Honeywell

Network and Security

Honeywell Mobile Computers

with Windows™ 10 Operating System

User Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

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

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

Web Address: www.honeywellaidc.com

Trademarks

Microsoft, Windows, Windows 10 and the Windows logo are registered trademarks of the 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 the Wi-Fi Alliance.

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

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

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

TABLE OF CONTENTS

Customer Support

Technical Assistance

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

Product Service and Repair

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

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

Limited Warranty

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

CHAPTER

1 INTRODUCTION

This guide defines the security processes, both implemented and recommended by Honeywell, for using Honeywell mobile computers with Windows™ 10.

Intended Audience

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

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

- Windows 10 operating system
- Networking systems and concepts
- Wireless systems
- Security issues and concepts. In particular, the following systems need to be understood and properly set up:
    - Identity and access management (IAM) server
    - Mobile device management (MDM) software
    - Application server (such as a web server or terminal emulation server)

How to Use this Guide

Note: *Windows references in this guide refer to devices with Windows 10 operating system.*

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

- Develop a Security Program, page 9
- Disaster Recovery Plan, page 13
- Security Updates And Service Packs, page 15
- Secure Wireless Devices, page 19
- System Monitoring, page 23
- Secure Access to the Windows Operating System, page 27

Product Detail

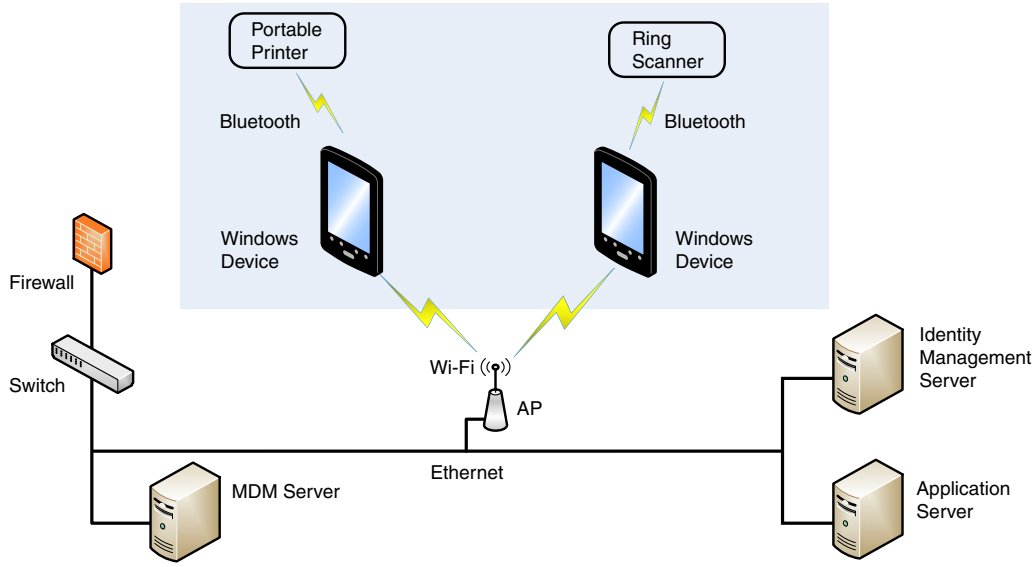
Honeywell mobile devices are intended for use in in-premise Automatic Data Collection (ADC) systems and for field ADC applications. In-premise systems typically exist in establishments such as distribution warehouses or retail stores. This type of system often uses terminal emulation servers or web servers 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 on page 3 illustrate sample architecture for in-premise and field system Windows 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 Windows system.

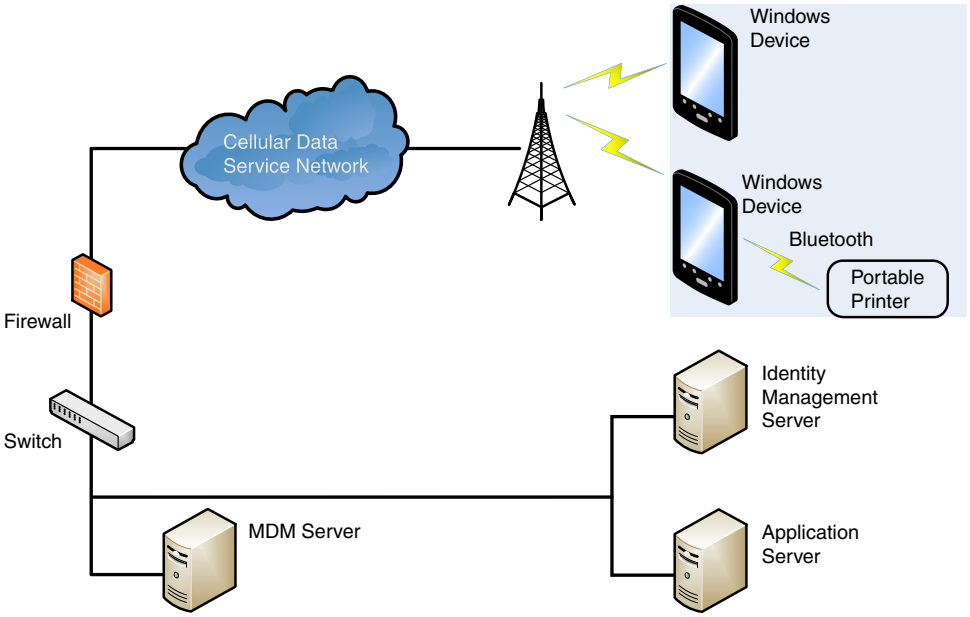
Architecture of an In-Premise Windows System

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



Architecture of a Field Service Windows System

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



Related Documents

Go to www.honeywellaidc.com to download the user guide specific to your computer model.

CHAPTER

2 SECURITY CHECKLIST

This chapter identifies common security threats that may affect networks containing Windows devices. You can mitigate the potential security risk to your site by following the steps listed under each threat. For more information, refer to https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines.

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
- Capturing, modifying, or deleting data

Mitigation Steps

Honeywell recommends that the latest version of software native protections within the operating system are kept in place and that back-end infrastructure/ systems are upgraded to current standards to match.

Note: *For optimal security, Honeywell recommends aligning back-end infrastructure to current operating system protections.*

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

Unauthorized External Access

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

Unauthorized external access can result in:

- Loss of system availability
- Capturing, modifying, or deleting data
- Reputation damage if the external access security breach becomes public knowledge

Mitigation Steps

Mitigation Steps	
Implement file system encryption.	
Use HTTPS when using web servers across untrusted networks.	
Use a two-factor authentication method when the Honeywell device is connecting to web applications.	
Use a firewall at the interface between your other networks and Windows devices.	
Secure wireless devices.	For information, see Secure Wireless Devices on page 19.
Set the minimum level of privilege for all external accounts, and enforce a strong password policy.	
Disable all unnecessary access ports, such as FTP.	
Use a VPN when the Windows system requires data to traverse an untrusted network.	
Use SSL for communication between native applications and specialty servers.	
Use intrusion detection on WLAN networks.	See Intrusion Detection, page 23, or http://www.sans.org/security-resources/idfaq/
Use an MDM solution to retrieve Windows system and application logs for centralized analysis.	
Use an MDM solution to permit only the use of trusted applications whitelisted by your organization as well as manage the device.	
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

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. Alternatively, you can use a locked-down menu program (such as Launcher for Windows or Enterprise Launcher) to prevent users from accessing specific applications.

Unauthorized Internal Access

This threat encompasses unauthorized access from people or systems with direct access to a Windows 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
- Capturing, modifying, or deleting data
- Theft or damage of system contents

Mitigation Steps

Mitigation Steps	
Do not allow the use of unauthorized removable media, such as microSD™ or microSDHC™ cards, on Windows devices.	http://msdn.microsoft.com/en-us/magazine/cc982153.aspx
Implement password protection on Windows devices.	Refer to https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
Monitor system access.	Use an MDM solution or SIEM utility for gathering and centralizing system logs.
Add other mitigations for disabling radios, (such as 802.11, location services, camera).	MDM software

CHAPTER

3 DEVELOP A SECURITY PROGRAM

Honeywell uses Building Security In Maturity Model (BSIMM) as our chief assessment tool for continuously improving the security maturity for our products and solutions. BSIMM https://www.bsimm.com/framework.html is a maturity framework which organizations can use to help understand the maturity of their product security process and practice. The model is based on observational science around software security and is continuously being updated and evolving. It is conducted on organizations across many different industries.

Note: *Honeywell recommends making use of such frameworks to gauge the maturity and progress needed in the user's own cybersecurity program.*

Form a Security Team

When forming a security team, you should:

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

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

Identify Assets to be Secured

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

When identifying assets at risk, you should consider:

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

Identify and Evaluate Threats

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

Potential threats to be considered include:

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

Identify and Evaluate Vulnerabilities

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

- The absence of security policies and procedures
- Inadequate physical security
- Gateways from the Internet to the corporation
- Gateways between the business LAN and Windows network

- Improper management of modems
- Out-of-date virus software
- Out-of-date security patches or inadequate security configuration
- Inadequate or infrequent backups

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

Identify and Evaluate Privacy Issues

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

Create a Mitigation Plan

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

Implement Change Management

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

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

Plan Ongoing Maintenance

Constant vigilance of your security program should involve:

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

CHAPTER

4 DISASTER RECOVERY PLAN

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

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

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

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

External Storage

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

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

Mobile Device Management Software

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

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

Disaster Recover Testing

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

CHAPTER

5 SECURITY UPDATES AND SERVICE PACKS

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

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

Caution: Before installing any critical updates or making any system changes, ALWAYS back up the system. This will provide a safe and efficient recovery path if the update fails. See the External Storage, page 13.

Additional Resources

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

CHAPTER

6 NETWORK PLANNING AND SECURITY

Connect to the Business Network

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

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

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

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

Third Party Applications

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

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

- Secure Development Lifecycle (SDL) practices were used by the vendor when developing the software
- The proper means and security controls to mitigate any threats to the Windows system are provided by the vendor
- Secure network practices were used by the vendor for APIs to prevent accidental access to insecure networks

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

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

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

Note: *Install only signed software from a trusted vendor or authority.*

CHAPTER

7 SECURE WIRELESS DEVICES

Wireless Local Area Networks and Access Point Security

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

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

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

Secure Wireless AP Configuration

Honeywell recommends the following when configuring a wireless AP:

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

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

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

Secure Windows WLAN Configuration

Honeywell recommends the following when configuring the Windows for WLANs:

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

Bluetooth™ Wireless Technology Security

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

- Set the Windows stack to non-discoverable
- Set the Windows stack to stop arbitrary pairings
- Use a strong PIN or password
- If possible, pair devices ONLY when in a physically secure area
- If simple secure pairing is used, Honeywell recommends that “just works” pairing is disabled

Wireless Wide Area Network Security

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

- Use HTTPS with web applications and white listing to ensure only specific URLs are accessed. 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

CHAPTER

8 SYSTEM MONITORING

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

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

Intrusion Detection

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

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

Most firewalls, switches, and routers have reporting facilities whereby they can report various levels of events, varying from debugging to emergency failure. These reports can be viewed via secure shell (SSH), collected by a central logging server, or sent via email to an administrator. For example, the Cisco® PIX firewall and Catalyst® 4500 switches can be configured to send selected levels of events to a central syslog server where further analysis can occur and significant events can be detected.

Remote Device Management

Honeywell recommends using an MDM solution to provision Windows-powered devices. The system should be used to monitor device software versions, applications and control any upgrade and/or downgrade processes.

To learn more about policy control for improved security, see https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/agpm/step-by-step-guide-for-microsoft-advanced-group-policy-management-30.

Honeywell recommends using the MDM solution to retrieve Windows system and application logs for centralized analysis. The MDM solution can help detect attempted abuse of the Windows device and applications.

Operational Technology Security

Honeywell recommends these cybersecurity best practices when implementing devices and solutions.

Best Practice	Description
Application Whitelisting	This practice aligns with a key cybersecurity principle of “least privilege”, where a user should only have the capabilities needed to perform their job function. Limiting the number of applications installed on a device greatly reduces the attack surface against the device and an intentionally malicious user.
Ensuring Asset Visibility	Knowing the assets in your infrastructure and where they are located is critical to keeping an organization safe and secure in a connected world.
Vendor Partnerships	Working together with your vendor in a close partnership is crucial in keeping up with the complexity of deploying Operational Technologies to enable your workforce. Technology is quickly evolving and so are threat agents. Honeywell looks forward to working with our customers to keep them secure.
Staying Up-to-Date	Work with vendors who take cybersecurity seriously and respond quickly to constantly evolving threats around the world. Honeywell recommends developing a cadence on patching and updating your devices, as well as using the latest operating system to leverage new security features and enhancements.
Be diligent and aware of Regulatory Frameworks	The regulatory environment around cybersecurity and data privacy is quickly adapting to the demands of a connected and digitized business environment (GDPR and CCPA). Working with a vendor that can provide you an “out-of-the-box” compliance and assurance is important. It is also imperative to develop your own framework around data privacy to ensure applications running your infrastructure are compliant.

CHAPTER

9 SECURE ACCESS TO THE WINDOWS OPERATING SYSTEM

Windows 10 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
- SmartScreen filter provides anti-phishing protection
- Remote data removal for Enterprise data
- Virtual smart cards for two-factor authentication (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, see https://docs.microsoft.com/en-us/windows/windows-10.

Many of the above features are capable of being managed by MDM software. System provisioning is used to enable and provide the level of enterprise security needed by your Windows 10 users.

Internal Firewall

By default the internal firewall of Windows 10 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. Customers can then migrate from the Honeywell defined security settings to their enterprise needs through their own MDM policy choices and customization.

APPENDIX

A GLOSSARY

General Terms and Abbreviations

ACL	An Access Control List (ACL) is a list of user accounts and groups with each entry specifying a set of allowed, or disallowed actions. When applied to a firewall, an ACL is a list of device addresses and ports that may (or may not) pass through the device.
Authentication	When a user logs on to a system, the authentication process verifies the user is known to the system. See also “authorization”.
Authorization	When a user logs on to a system, the authorization result dictates what a known user can do within the system. See also “authentication”.
Business network	A collective term for the network and attached systems.
Digital signature	Using the private key of a digital certificate to encrypt the digital hash (digest) of an electronic document, code file, etc.
DMZ	Demilitarized zone (DMZ) is an area with some firewall protection, but which is visible to the outside world. This is where business network servers for web sites, file transfers, and email are located.
Firewall	A firewall is a software or hardware barrier that sits between two networks, typically between a LAN and the Internet. A firewall can be a standalone network appliance, part of another network device such as a router or bridge, or special software running on a dedicated computer. Firewalls can be programmed to block all network traffic from coming through except that which has been configured to be allowed. By default, a firewall should block all 65,536 ports and open up only the ports you need. If you need to browse the web, then it should allow “outgoing” traffic on port 80. If you would like DNS lookups to work for you, port 53 needs to

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

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

Honeywell
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com

ALLSKU-W-EN-SG-01 Rev B
07/20