Honeywell

VM3

Windows 8.1 | Windows 7 | Windows Embedded Standard 7

Network and Security Guide

Disclaimer

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

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

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

Web Address: www.honeywellaidc.com

Trademarks

Android is a trademark of Google Inc.

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

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

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

MITRE is a registered trademark of The MITRE Corporation.

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

UNIX is a registered trademark of The Open Group.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

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

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

Table of Contents

1 Introduction

This guide defines the security processes, both implemented and recommended by Honeywell, for using the VM3 Windows 8.1/ Windows 7/WES7 terminals.

Intended Audience

The target audience for this guide is the VM3 customer organization that identifies and manages the risks associated with the use of information processing equipment. This includes, but is not limited to, Information Technology (IT). Third party organizations delivering and installing turnkey systems should also follow the guidelines in this guide. The intent of this guide is to drive the discussion between the organization using the VM3 and the organization responsible for managing information technology risks.

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

- Microsoft Windows 8.1 Professional, Microsoft Windows 7 Professional, and Windows Embedded Standard 7 operating systems.
- Networking systems and concepts.
- Wireless systems.
- Security issues and concepts. In particular, the following systems need to be understood and properly setup:
  - Radius Server
  - Mobile Device Management Software
  - Application Server (such as a web server or terminal emulation server)

How to Use this Guide

Note: Win8/Win7/WES7 references in this guide refer to Windows 8.1 Professional, Windows 7 Professional, and Windows Embedded Standard 7 devices.

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

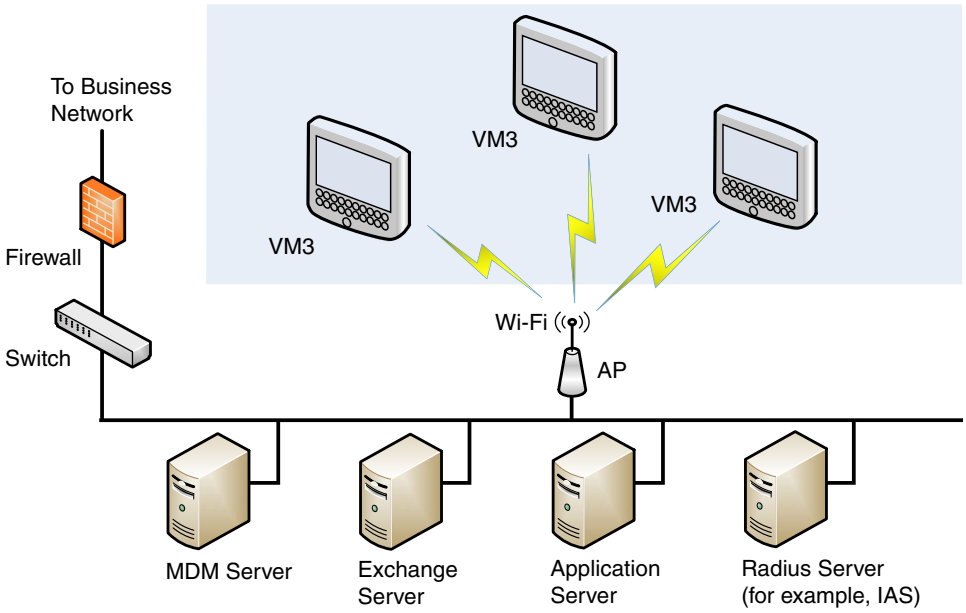
Product Detail

The Honeywell VM3 Win8.1/Win7/WES7/WEC7 solution is a device intended for use in in-premises Automatic Data Collection (ADC) systems. Most often, the system exists in a distribution warehouse. The VM3 is intended for mounting on a forklift or similar industrial vehicle, although some installations may require a stationary mount. This system typically uses terminal emulation servers or web servers to direct the VM3 to perform ADC operations, such as scanning during picking or placing of items. The VM3 uses either a web browser or terminal emulation software to interact with the server.

System Architecture

The system architecture includes VM3 devices and (typically) a wireless local area network (WLAN), a device management server such as Honeywell Remote MasterMind, and a server that supports the application, such as a web server or a terminal emulation server. A Microsoft Exchange Server may be present to allow security policies to be automatically supported by each VM3 in the system.

A firewall prevents direct access from the system to the rest of the Business Systems Network (such as financial, HR, or other systems), and prevents the business systems from accessing the VM3 system.



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 VM3 devices. You can mitigate the potential security risk to your site by following the steps listed under each threat.

Infection by Viruses and Other Malicious Software Agents

This threat encompasses malicious software agents, for example viruses, spyware (Trojans), and worms. The intrusion of malicious software agents can result in:

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

Mitigation Steps

Mitigation Steps	
Ensure virus protection is installed, signature files are up-to-date, and subscriptions are active.	
Allow only digitally signed software from trusted sources to run.	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 VM3 devices.	

Unauthorized External Access

This threat includes intrusion into the Honeywell VM3 system from the business network or other external networks including the Internet.

Unauthorized external access can result in:

- loss of system availability,
- the capture, modification, or deletion of data, and
- reputation damage if the external access security breach becomes public knowledge.

Mitigation Steps

Mitigation Steps	
Implement file system encryption.	
Use HTTPS or your VPN when using Web servers across untrusted networks.	http://msdn.microsoft.com/en-us/library/windows/apps/xaml/hh849625.aspx#require_https_connections
Use a firewall at the interface between your business network and the VM3 network. Enable the firewall with Advanced Security, choosing the most restrictive policy, and disallow HTTP connections.	
Secure wireless devices.	
Set the minimum level of privilege for all external accounts, and enforce a strong password policy. This is especially true for Mobile Device Management (MDM) systems.	Mobile Device Management (MDM) software

Mitigation Steps	
Disable all unnecessary access ports (such as FTP).	The construction of the OS does not allow an application to disable ports that another application may require. If an application cannot be removed because the port should not be used, then the way to restrict open ports is to restrict the available applications to users through Allow Listing (explained later).
Use the Windows VPN when the VM3 system requires data to traverse an untrusted network.	Mobile Device Management (MDM) software
Use HTTPS when using web servers across untrusted networks.	
Use 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 WLAN networks.	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 VM3. 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 USB drives) on VM3.	http://msdn.microsoft.com/en-us/magazine/cc982153.aspx
Monitor system access.	
Enable BitLocker on the SSD and all removable media used with the VM3. BitLocker is part of the Secure by Default configuration, but it is not enabled by default on the VM3.	http://windows.microsoft.com/en-us/windows-8/bitlocker-drive-encryption
Implement passwords on VM3 devices and use a strong password policy.	http://technet.microsoft.com/en-us/library/cc736605(v=WS.10).aspx

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 VM3 devices and infrastructure).
  - Business applications (for example, individuals responsible for applications interfaced to the Honeywell VM3 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 LAN and VM3 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 VM3 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 VM3 software and its infrastructure that could affect security, including configuration changes, the addition of network components, and the installation of software. Changes to policies and procedures might also be required.

Planning Ongoing Maintenance

Constant vigilance of your security program should involve:

- regular monitoring of your system.
- regular audits of your network security configuration.
- regular security team meetings where keeping up-to-date with the latest threats and technologies for dealing with security issues are discussed.
- ongoing risk assessments as new devices are placed on the network.
- the creation of an Incident Response Team.

Additional Security Resources

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

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

Information Technology - Security Techniques	
ISO 15408 - Evaluation Criteria for IT Security, Parts 1 - 3	http://www.iso.org
ISO 27002 - Code of Practice for Information Security Management	http://www.iso.org

4 Disaster Recovery Planning

Recovery Plan Recommendations

The VM3 devices should be considered part of the user's Disaster Recovery Plan. This plan could include maintaining an inventory of spare devices. Platform images should be backed up regularly to external media or network storage per corporate standards. Honeywell offers recovery images for the OS and built-in drivers. Additional Honeywell-provided drivers and applications may be obtained from Honeywell Technical Support.

5

Security Updates and Service Packs

As reported by the Open Web Security Project (OWASP), a common weakness of system management is the inability to keep software up-to-date. It is critical to keep the latest patches and software versions on your VM3 devices and supporting devices in the VM3 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.Use the Programs and Features control panel to determine what software has been installed on the terminal.

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.

6 Network Planning and Security

Connecting to the Business Network

The VM3 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 VM3 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 VM3 network and vice versa.

Ideally, there should be no direct communication between the VM3 network and the business network. However, practical considerations often mean a connection is required between these networks. The VM3 network may require data from the servers in the business network or business applications may need access to data from the VM3 network. A connection between the networks represents a significant security risk; therefore, careful consideration should be given to the system architecture design. Due to the security risk, it is strongly recommended that only a single connection is allowed and that the connection is through a firewall.

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

Third Party Applications

Honeywell provides most of the applications that meet the needs of the VM3 customer. When a third-party application must be added to the device, always verify the following with the vendor:

- Secure Development Lifecycle (SDL) practices were used when writing the software.
- The proper means and security controls to mitigate any threats to the VM3 system are provided.

In addition, evaluate additional risks to the VM3 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 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 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.

Telnet Security

By default, Telnet does not encrypt any data sent over the connection. To mitigate risks caused by using Telnet, Honeywell recommends the following steps:

- Use Telnet only with SSH enabled.
- Change the default Telnet password to a strong password. For more information, see http://technet.microsoft.com/en-us/library/cc736605(v=WS.10).aspx.
- Enable IPSec on computers running Telnet and on Telnet servers.
- Use a TelnetClients local group to allow standard users to use Telnet.
- Require the use of NTLM authentication, so that the username and password are encrypted.

FTP Security

For computers running an FTP client or server, IPSec should be enabled, or FTP should be used over a VPN. The FTP server should disable anonymous and basic authentication. The server should create allow/deny rules and require TLS 1.0 (or greater) connections. Use SFTP instead of FTP.

7 Securing Wireless Devices

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

VM3 terminals 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 VM3 device connects through a wireless access point (AP) to an organization's server on a wired network, specific security precautions are required to mitigate the significant security risk the WLAN wireless AP connection represents for the servers and devices on the wired network.

Limit the SSIDs to which the VM3 can be connected.

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: WPA2 EAP-TTLS, WPA2 EAP-TLS, WPA2 PEAP-MSCHAP, WPA2 PEAP-GTC, WPA2 EAP-FAST, WPA2 PSK.
- Configure the RADIUS server address.
- Configure all user accounts with full security in Enterprise mode for WPA2:
  - Enable validation of the server certificate.
  - Define the server address.
  - Select the root CA certificate.
  - Disable prompting the user to trust new CAs.
  - Do not use WEP or LEAP security because of their vulnerability to attacks.
- 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 wireless AP supplier. Also, refer to the detailed Wi-Fi documentation in the User Guide.

Secure VM3 WLAN Configuration

Honeywell recommends the following when configuring the VM3 for WLANs:

- Honeywell supports and approves these security methods: WPA2 EAP-TTLS, WPA2 EAP-TLS, WPA2 PEAP-MSCHAP, WPA2 PEAP-GTC, WPA2 EAP-FAST, WPA2 PSK.
- Configure the proper SSID.
- Configure 802.1x authentication.
- Configure Protected EAP 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 VM3 device. Additional information on configuring Wi-Fi security can be found in the Thor VM3 User's Guide.

Bluetooth™ Wireless Technology Security

All VM3s are equipped for short-range wireless communication using Bluetooth wireless technology.
For secure Bluetooth communications, follow these security recommendations and precautions:

- Set the Bluetooth stack to "non-discoverable" on the VM3.
- Set the Bluetooth stack to stop arbitrary pairings on the VM3.
- Disable unused Bluetooth profiles on the VM3.
- When available, use Bluetooth 2.1 Secure Simple Pairing.
  Note: Honeywell recommends that you do ***not*** *use the "just works" mode.*
- Use a strong PIN or Password.
- If possible, pair devices ONLY when in a physically secure area.

Additional information on configuring Bluetooth security can be found in the Bluetooth Wizard User Guide, or at http://msdn.microsoft.com/en-us/library/windows/hardware/dn133844(v-vs.85).aspx.

Wireless Wide Area Network (WWAN) Security

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

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

GPS Security

GPS is susceptible to denial of service when an attacker sends GPS signals and data to the target at increasing power levels, eventually overpowering the real GPS signal.

Secure Browsing

Enterprise Browser is a secure, lockdown web browser created for customers who wish to use web-based applications but do not want to allow complete Internet access to users. Enterprise Browser restricts user access to other applications, websites, and components of the operating system. The browser has no address bar, so users can only access the links provided on the home page. Also, users are unable to exit the browser to access other applications or the Start menu. Companies have more control over program flow to create directed applications with Enterprise Browser, resulting in less end-user confusion.

Securing Direct Connections via USB, RS-232 Serial, or CAN/Audio

Restrict devices and drivers that users can install by using a Group policy manager.

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 VM3. Early detection of an attack and/or system breach is essential to preventing further damage. The earlier a system intrusion is detected and the more evidence that is captured, the less damage is likely to occur and the greater the chances of identifying the intruder.

Providing a means to detect and document system exploits is vital.

For example, the anti-virus package used should provide a method to collect logs created by the package. The log should be available for retrieval via the package and a related console application on a server, or via a remote device management system. Periodic collection of additional logs (for example, VPN connection information or login access failures) should also be implemented.

Intrusion Detection

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

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

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

9 Securing Access to the Windows Operating System

An essential component of any security strategy for computers in the VM3 network is to secure access to the operating system to ensure that:

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

The following links will provide information about the security features of the Windows 7 / WES7 operating environment:

- http://www.microsoft.com/security/pc-security/windows7.aspx
- http://windows.microsoft.com/en-us/windows7/security-checklist-for-windows-7

Security Settings

This section defines security settings related to security policies on VM3 Windows 8.1, Windows 7 and WES 7.

Configuring Security Policies

On Windows 8.1, Local Security Policy settings can be viewed and modified using secpol.msc (select the run app and enter secpol.msc).

On Windows 7, Local Security Policy settings can be viewed and modified using secpol.msc (Start | run secpol.msc).

On both Windows 7 and WES7, Local Security Policy tab of the Administrative Tools control panel can be used to view and modify the settings.

The Local Security Policy categories are listed below:

- Account Policies
  - Password Policies
  - Account Lockout Policy
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
  - Encrypting File System
  - BitLocker Drive Encryption
- Software Restriction Policies
- Application Control Policies
  - Intermec Launcher
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

The applet contains built-in Help as well as links to the Microsoft web site for further explanation. To access Help, double-tap the desired policy setting and select the Explain tab. Some key settings to consider are discussed in the following section.

Recommended Settings for Local Security Policies

Password

Account Policies->Password Policy->Password must meet complexity requirements
Recommended Value is **Enabled.** When set to Enabled, the following criteria are enforced:

- The password may not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- The minimum password length is 6 characters.
- The password must contain characters from three of the following four groups:
  - Alpha uppercase
  - Alpha lowercase
  - 0-9

– Non-alpha (!, @, #, $, etc.)

Account Policies->Password Policy->Minimum password length
Recommended Value is **8**

Account Policies->Password Policy->Enforce password history
Prohibit the same password from being used for the previous N password changes.
Recommended Value is **10**

Account Policies->Password Policy->Maximum password age
Specifies the time period (in days) for password expiration
Recommended values are indicated in the next table:

Days	Recommended Usage
30	Critical usage cases or when VM3 users might change frequently
42 (default)	Typical usage cases
90	Less critical usage cases
120	Very low security requirements

Account Lockout Policy

Account Policies->Account Lockout Policy->Account lockout duration
This setting defines the number of minutes a locked-out account remains locked before automatically becoming unlocked.
Recommended Value is **30 minutes**

Account Policies->Account Lockout Policy->Account lockout threshold
This setting defines the number of failed login attempts that causes a user account to become locked-out.
Recommended Value is **5**

Account Policies->Account Lockout Policy->Reset account lockout counter after
This setting defines the number of minutes that must elapse before the failed login counter is reset to 0.
Recommended Value is **30 minutes**

Admin Account

The Admin Account should be used for administrative purposes only. A general user should not run out of the admin account.

Disable Unused Services

Windows provides many services that may not be needed. One security control is to turn off anything that is not going to be used.

Intermec Launcher

Use Intermec Launcher to restrict application use. Malware detection should also be installed and run on the VM3.

Configuration Data

Access to the configurations of the following components should be restricted to Admin users:

- Remote Desktop
- Touch Screen
- Screen Blanking
- Remap Keys
- RFTerm
- ReM Agent
- WLAN
- WWAN
- Bluetooth

Installation Restrictions

Use the Group Policy Manager to restrict users on the devices and drivers that they can install.

Remote Access

When accessing the VM3 remotely through apps such as Remote Desktop and ReM, use a secure VPN or enable TLS1.2 to improve security. Also, use a 2-factor authentication.

10 Using Honeywell Applications Securely

This chapter describes Honeywell applications that may be present on the VM3 computer, and recommends methods for using these applications securely in the VM3 network.

Securing Honeywell Launcher

Launcher is a Honeywell application that provides the following features:

- Provides a configurable locked-down menu program that prevents end-users from accessing the start menu and other non-authorized applications.
- Allows end-users to log in and access only authorized programs.
- Password-protected operating system environment.
- Hot key access to the Launcher main menu from within authorized programs.
- Auto-start feature which opens to the main menu.
- Configurable main menu can include up to five buttons, which launch unique mission critical application programs.
- Can be used in conjunction with Honeywell Browser (IB). With Honeywell Launcher and Honeywell Browser running together, the end-user is unable to navigate outside the designated applications.

Security Recommendations for Launcher

To use Honeywell Launcher securely, Honeywell recommends the following:

- Launcher should be set to auto run to provide security benefits, and to prevent system access.
- Change the default password to prevent access to the system.
- Do not use blank passwords.
- Change the Launcher password every 90 days, if not sooner, to help mitigate the risk of password discovery by unauthorized persons.
- Configure Launcher to display only the applications that are required for use on the device.
- Use of the 'whitelist' functionality that allows customer applications to run. This can be configured though EZConfig for the Enterprise Settings. Customers should take care with what applications they allow to run.
- All files used with the application, including the application executable, should be protected with the operating system file access controls so that only the application and its administrators have access to the files.

Securing Enterprise Terminal Emulation

Enterprise Terminal Emulation (ETE) is a Honeywell application (part of the Intermec Client Pack) that provides the following features:

- Leverages WMS investment with support for all major emulation protocols
- Improves productivity with multiple sessions and session persistence
- Enhances operator experience with industry leading terminal emulation performance
- Enables security compliance via enhanced, secure communications
- Lowers operational costs with remote management and configuration capability
- Expands potential for new uses of data through remote procedure calls
- Minimizes support expense through available maintenance plans

Security Recommendations for ETE

To use ETE securely, Honeywell recommends the following:

- Configure the ETE password to a non-default value. Apply all standard password security measures, such as prohibiting the use of words, or using a mix of alphabetic and numeric characters. The password configuration entry can be found in the ETE configuration under each session.
- Use a separate exit password (available in the root of the configuration) that allows users to exit ETE without the ability to launch Enterprise Settings. This allows users to exit ETE, but prevents them from changing the device settings by opening Enterprise Settings.
- Only allow secure data transmission. Data transmitted through Telnet, non-SSL TGAP, or no-security SPS/UDP+ connections is not secure and can be seen by anyone on the same network. If a wireless connection is used, anyone nearby can detect and read the transmissions if the network is not properly encrypted. For any potentially sensitive data, use SSH or SSL connections to prevent unauthorized access to the data.
- All files used with the application, including the application executable, should be protected with the operating system file access controls so that only the application and its administrators have access to the files.

Securing RFTerm

RFTerm is a Honeywell application that provides the following features:

- Terminal Emulation, supported on a variety of HSM terminals with various operating systems. Enables the use of three terminal emulations: VT220, IBM 5250, and IBM 3270.
- Auto launched when the terminal is powered up.
- Supports Secure Shell (connections) using PuTTY.
- Provides a restricted access menu settings through password access. This password is encrypted and stored in the registry.

Security Recommendations for RFTerm

To use this product security, Honeywell recommends the following:

- Enable password protection on every connection access via RFTerm to their host applications.
- Enable password protection for the menu settings. Use robust (non-simple) passwords, such as a mix of upper and lower case letters, some use of numbers and special characters other than @ or *. Change the password periodically (such as every 90 days or sooner).
- Secure the network from the HSM terminal to the host by encryption. If the network is not otherwise secured in this way, then Honeywell recommends that SSH is enabled between the terminal and the host application. This requires a compatible SSH shell/tunnel running on the Host side.
- All files used with the application, including the application executable, should be protected with the operating system file access controls so that only the application and its administrators have access to the files.

Securing Honeywell Browser

Honeywell Browser is a Honeywell application that provides the following features:

- Lockdown browser for control over program flow
- Optimization for Web-based data collection applications
- Supports remote configuration and cold boot assistance
- Supports HTML, XML and JavaScript
- Provides more screen real estate for applications
- Controls on-screen keyboard
- Available maintenance plan for ongoing support
- Part of Enterprise Client Pack

Security Recommendations for Honeywell Browser

To use this product security, Honeywell recommends the following:

- Configure Browser to auto-run to provide security benefits and prevent system access.
- Do not use blank passwords.
- Remove the Exit button from the user interface.
- Change the Browser password periodically (such as every 90 days or sooner) to help mitigate the risk of password discovery by unauthorized persons.
- Set the home page to a work-related site.
- Do not disable ActiveX security (enabled by default).
- Disable JavaScript if it is not required for any work. Malicious attacks may be attempted using JavaScript.
- Disable browser plugins (if not required by the application) to help prevent any unwanted plugins from running.
- Use SSL Encryption along with certificates to help prevent any data from being seen by others.
- All files used with the application, including the application executable, should be protected with the operating system file access controls so that only the application and its administrators have access to the files.

Securing Enterprise Data Collection

Enterprise Data Collection is a Honeywell component (part of the Enterprise Client Pack) that includes the following features:

- Manages the connections between data collection devices, such as scanners and imagers (serial, Bluetooth, USB), and their software clients.
- Executable (DataServer.exe) is always running on a Honeywell mobile device with data collection enabled. On Windows 7, Windows 8.1, and WES 7 devices, it runs as a service. As DataServer runs automatically after a reboot and is always running, there is no password.

- Configuration of Data Collection settings can be done via Enterprise Settings, which can require password access to menu settings.

Security Recommendations for Enterprise Data Collection

To use this product securely, Honeywell recommends the following:

- Enable the Enterprise Settings password to prevent unauthorized access to configuration settings.
- Do not use blank passwords.
- Change the Enterprise Settings password every 90 days (or sooner) to help mitigate the risk of password discovery.
- All files used with the application, including the application executable, should be protected with the operating system file access controls so that only the application and its administrators have access to the files.

Securing Enterprise Bluetooth

Enterprise Bluetooth is a Honeywell component (part of the Enterprise Client Pack) that includes the following features:

- Connects Bluetooth scanners and printers to Honeywell mobile computers.
- Configures Bluetooth settings including Device Name (“friendly name”), Device Address, Discoverable, Connectable, and Class of Device.
- Configurable one-time passcode (if required).
- Configured through Enterprise Settings, which can require password access to menu settings.

Security Recommendations for Enterprise Bluetooth

To use this product securely, Honeywell recommends the following:

- Enable the Enterprise Settings password to prevent unauthorized access to configuration settings.
- Do not use blank passwords.
- Change the Enterprise Settings password every 90 days (or sooner) to help mitigate the risk of password discovery.
- All files used with the application, including the application executable, should be protected with the operating system file access controls so that only the application and its administrators have access to the files.

11 Network Ports Summary

Network Port Table

Port Used	Connection	Task	Comments
80	HTTP		Web Pages
443	HTTPS		Secure Web Pages
3790	SSL	RemoteMasterMind	Application used for remote device management. Manages software updates and settings on the VM3

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

12 Glossary

General Terms and Abbreviations

ACL	An Access Control List (ACL) is a list of user accounts and groups with each entry specifying a set of allowed, or disallowed actions. When applied to a firewall, an ACL is a list of device addresses and ports that may (or may not) pass through the device.
Authentication	When a user logs on to a system, the authentication process verifies the user is known to the system. See also "authorization".
Authorization	When a user logs on to a system, the authorization result dictates what a known user can do within the system. See also "authentication".
Business network	A collective term for the network and attached systems.
Digital signature	Using the private key of a digital certificate to encrypt the digital hash (digest) of an electronic document, code file, etc.
DMZ	Demilitarized zone (DMZ) is an area with some firewall protection, but which is visible to the outside world. This is where business network servers for Web sites, file transfers, and email are located.
Firewall	A firewall is a software or hardware barrier that sits between two networks, typically between a LAN and the Internet. A firewall can be a standalone network appliance, part of another network device such as a router or bridge, or special software running on a dedicated computer. Firewalls can be programmed to block all network traffic from coming through except that which has been configured to be allowed. By default, a firewall should block all 65,536 ports and open up only the ports you need. If you need to browse the Web, then it should allow "outgoing" traffic on port 80. If you would like DNS lookups to work for you, port 53 needs to be opened up for "outgoing" traffic. If you want to access your Internet mail server through POP3, open up port 110 for outgoing traffic. Firewalls are directional. They monitor where the traffic originates for both "incoming/inbound" and "outgoing/outbound" traffic. Quite frequently you will not want any unsolicited inbound traffic unless you have specific reasons (for example, you might have a Web server that you want people to access). However, in most cases, a Web server would probably be located outside your firewall and not on your internal network. This is the purpose of a demilitarized zone. The following Microsoft reference is a useful source of information about well known TCP/IP ports: http://support.microsoft.com/kb/832017.
IAS	Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy.
LAN	Local Area Network
Locking down	The procedure whereby a given user is given access to only one or a few specific programs is known as "locking down" a desktop or computer.
MAC	Media Access Control (MAC) is the lower level of the Data Link Layer (under the IEEE 802.11-1997 standard). In Wireless 802.11, MAC stands for "Medium Access Control". MAC can also be an abbreviation for "Message Authentication Codes", a cryptographic hash added to a message to enable the detection of tampering.
MDM	Mobile Device Management (MDM) technology provides the ability to deploy, secure, monitor, integrate, and manage mobile devices across multi-site enterprises. MDMs help manage the distribution of software updates, data, and configuration information across multiple devices or groups of devices. MDMs are also used to enforce security policies. An example of MDM is the Remote MasterMind software.
PEAP	Protected Extensible Authentication Protocol (PEAP) is a protocol proposed for securely transporting authentication data, including passwords, over 802.11 wireless networks.
Port	A port is a logical endpoint on a network computer or device used for communications. There are approximately 65,536 ports on which any one IP address can communicate. Some are dedicated to specific well-known services; some are used by application services; and some will be dynamically allocated to clients as they connect to remote services. A service listens on a known port for client connections, if the connection is accepted, the client will address messages to that port, and the server will send responses to the dynamically allocated client port.
RADIUS	Remote Authentication Dial In User Service (RADIUS) is a protocol that enables centralized authentication, authorization, and accounting for dial-up, virtual private network, and wireless access.
Remote MasterMind	Device management software available from Honeywell to facilitate the management of mobile computers, smartphones, and bar code scanners across multi-site enterprises.

SDL	Security Development Lifecycle (SDL) is a software development process that helps developers to build more secure software and to address security requirements while reducing development cost.
SNMP	Simple Network Management Protocol (SNMP) is a protocol used to manage devices on IP networks.
SSID	Service set identifier (SSID) is a unique identifier for a wireless network.
Subnet	A group of hosts that form a subdivision of a network.
Subnet mask	A subnet mask identifies which bits of an IP address are reserved for the network address. For example, if the IP address of a particular computer or device is 192.168.2.3 with a subnet mask of 255.255.255.0, this subnet mask indicates the first 24 bits of the address represent the network address and the last 8 bits can be used for individual computer or device addresses on that network.
Switch	A switch is a multi-port device that moves Ethernet packets at full wire speed within a network. A switch may be connected to another switch in a network. 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.

13 Customer Support

Product Service and Repair

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

For ongoing and future product quality improvement initiatives, the VM3 terminal comes with an embedded device lifetime counter function. Honeywell may use the lifetime counter data for future statistical reliability analysis as well as ongoing quality, repair, and service purposes.

Technical Assistance

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

Knowledge Base: www.hsmknowledgebase.com

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

Technical Support Portal: www.hsmsupportportal.com

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

Web form: www.hsmcontactsupport.com

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

Telephone: www.honeywellaidc.com/locations

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

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

www.honeywellaidc.com