Honeywell

THE POWER OF **CONNECTED**

Network and Security

Enterprise Provisioner and Staging Hub Server

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

Google, Google Play and Android are trademarks 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 and Miracast are registered trademarks 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 **Get Resources** > **Product Warranty**.

CHAPTER

1 INTRODUCTION

This document defines the security process implemented by Honeywell for using the Enterprise Provisioner and Staging Hub Server.

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) personnel responsible for planning the configuration and maintenance of the network infrastructure where the Enterprise Provisioner and Staging Hub Server system exist.

A high degree of technical knowledge and familiarity with the following is required:

- Microsoft Windows Operating Systems
- Networking Systems and Concepts
- Security Issues and Concepts

Definitions of terms can be found in the Glossary, beginning on page 67.

Product Detail

The Enterprise Provisioner and Staging Hub Server software uses commercial off-the-shelf computing and networking hardware with standard Microsoft Networking and Operating Systems.

Staging Hub Server provides a centralized platform to easily manage and monitor deployed Honeywell devices, such as mobile computers, printers, and RFID readers. Enterprise Provisioner is a standalone tool used to create and edit Android settings, provisioning commands, and barcodes.

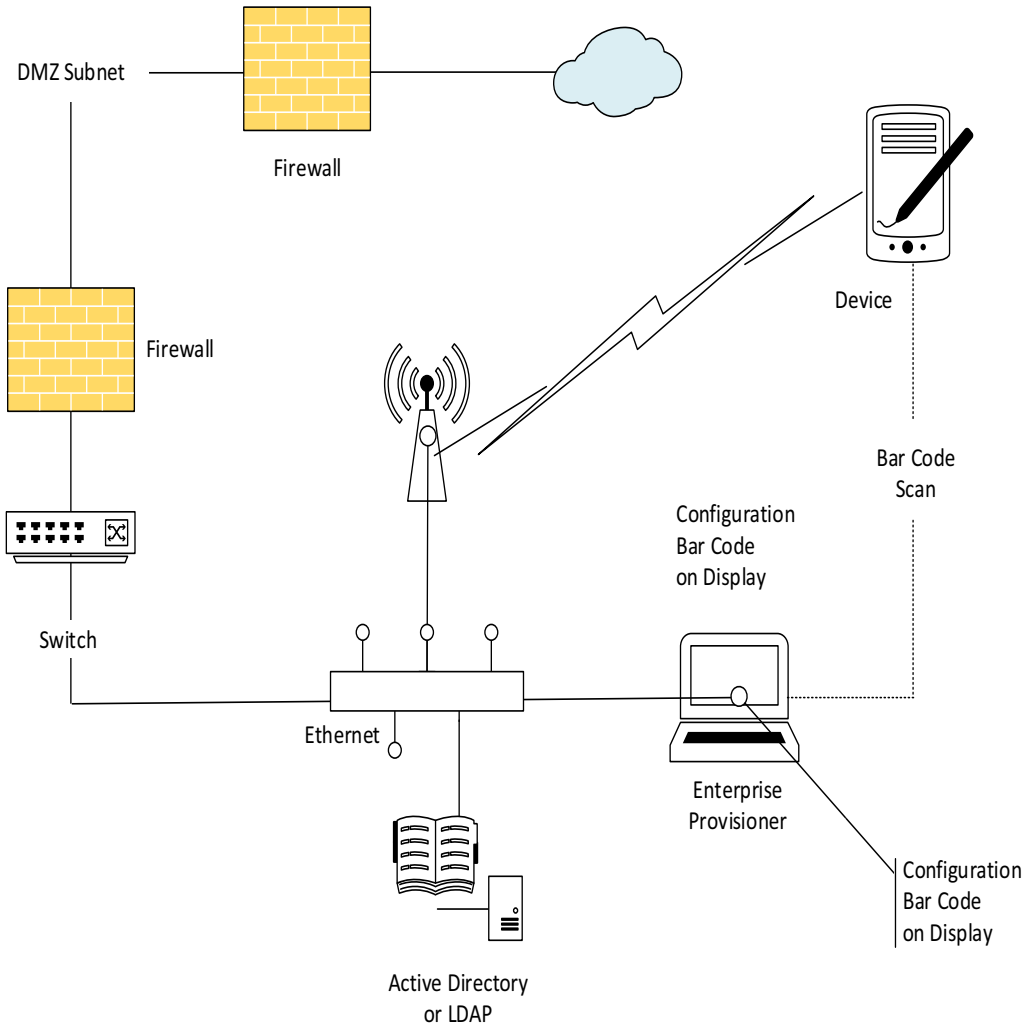
Enterprise Provisioner is located in the **Tools** menu and can run in different modes in Staging Hub.

- Settings tab exposed when editing a settings bundle
- Provisioning tab exposed when creating/editing Staging Hub Android software bundles
- Barcode tab exposed when creating barcodes from Android settings bundle

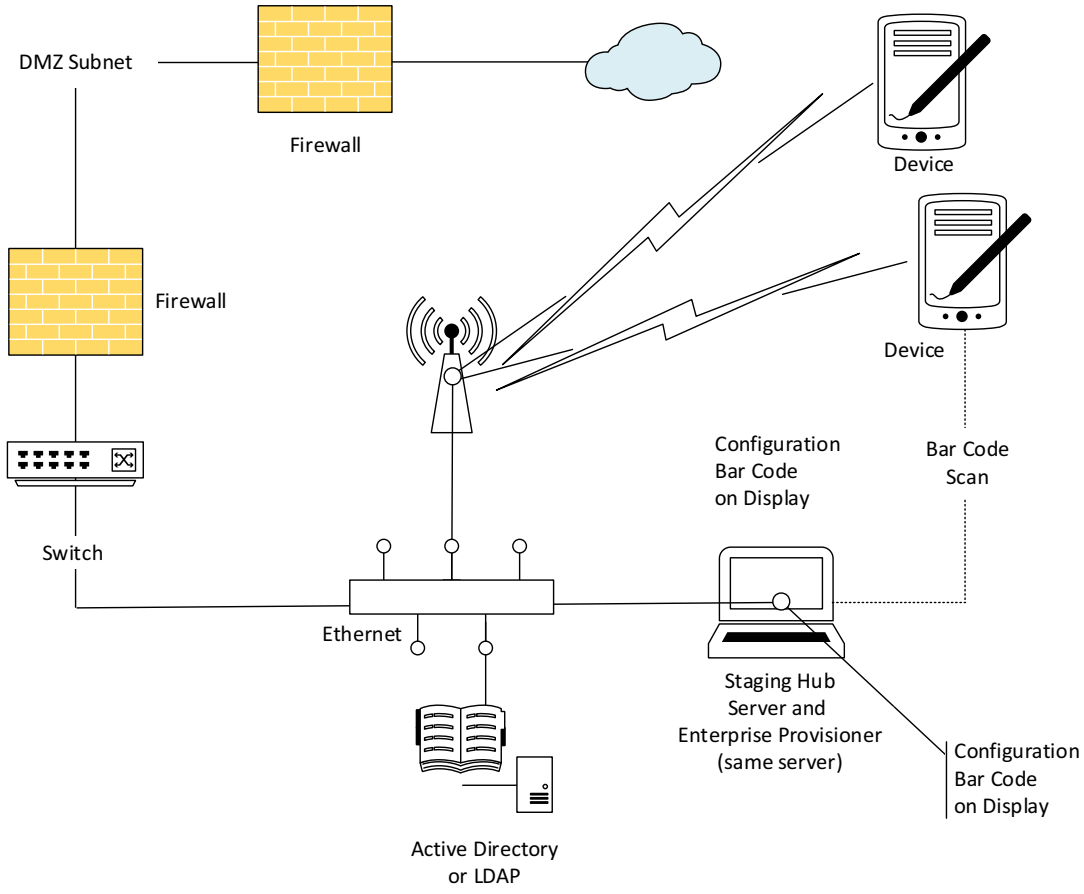
Enterprise Provisioner can be used alone or as a component of Staging Hub Server. It creates configuration bar codes that are printed, stored in a file, or displayed on the main screen. A Mobility Edge™ device can scan a barcode to provide a simple way to start the configuration process. Typically, the barcode will provide a URL of the Enterprise Provisioner web services where the device can finish configuration.

Staging Hub Server can use Enterprise Provisioner to create barcodes for completion of configuration and provides many additional device management functions such as organizing devices into groups, updating software, and keeping configuration up to date.

The following diagrams illustrate the architecture of these solutions:



Enterprise Provisioner (standalone)



Staging Hub with Enterprise Provisioner

Honeywell Service Limitations

Services **do not** include, and Honeywell is not responsible for providing, unless otherwise specifically agreed in writing with the customer Services to repair:

- System problems due to causes external to the System including but not limited to hardware or software components which do not form part of the System
- System problems caused by improper treatment or use of the System, or unauthorized attempts to repair or maintain the System
- Third party software upgrade releases beyond the control of Honeywell
- Installation visits by Honeywell

How to Use this Guide

If you have specific security concerns, such as protecting Enterprise Provisioner and Staging Hub Server systems against viruses or preventing unauthorized access, the following document complements this guide:

Document	Description
Enterprise Provisioner and Staging Hub Server Release Notes	Provides detailed instructions for how to install Enterprise Provisioner and Staging Hub Server products.

CHAPTER

2 SECURITY CHECKLIST

This chapter provides checklists covering some of the main threats that may exist on a network containing Enterprise Provisioner and Staging Hub Server as well as steps to mitigate those threats.

Infection by Viruses and Other Malicious Software Agents

This threat encompasses malicious software agents including viruses, spyware (Trojans), and worms.

The intrusion of malicious software agents can result in performance degradation, loss of system availability, and unwanted capture, modification, or deletion of data.

Mitigation Steps

Mitigation Steps	For more information see:
Ensure that your virus protection and Microsoft security hotfixes are up to date on all computers in your Enterprise Provisioner and Staging Hub Server system and in the systems connected to it.	Security Updates And Service Packs, beginning on page 21 and Virus Protection, beginning on page 25
Ensure that there is no email or instant messaging clients on any Enterprise Provisioner and Staging Hub Server machine.	Prohibiting Email and Messaging Clients, beginning on page 28.
Use a firewall and DMZ at the interface between your Internet access and Enterprise Provisioner and Staging Hub Server network, if such connectivity is required.	Section The Demilitarized Zone, beginning on page 31 and Configuring The DMZ Firewall, beginning on page 32

Note: *The use of spyware removal applications may cause unexpected results if run on Enterprise Provisioner and Staging Hub Server or workstation computers. These applications may alter registry settings that are crucial to the operation of the software.*

Unauthorized External Access

This threat includes intrusion into the Enterprise Provisioner and Staging Hub Server system from the business network and possibly an intranet or the Internet.

Unauthorized external access can result in:

- Loss of system availability
- Theft or damage of system contents
- Capture, modification, or deletion of data
- Damage to reputation if the external access becomes public knowledge.

Mitigation Steps

Mitigation Steps	For more information see:
Use a firewall and DMZ at the interface between your Internet access and Enterprise Provisioner and Staging Hub Server network, if such connectivity is required.	The Demilitarized Zone, beginning on page 31 and Configuring The DMZ Firewall, beginning on page 32
Set the minimum level of privilege for all accounts, and enforce a strong password policy, both for Windows user accounts and Enterprise Provisioner and Staging Hub Server user accounts.	Windows User Accounts and Passwords, beginning on page 45
Monitor system access	System Monitoring, beginning on page 35
Use the Windows Firewall	Windows Security Features, beginning on page 53

Unauthorized Internal Access

This threat encompasses unauthorized access from people or systems within the Enterprise Provisioner and Staging Hub Server Network. 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
- Incorrect execution of controls causing the failure of Enterprise Provisioner and Staging Hub Server system
- Capture, modification, or deletion of data
- Theft or damage of system contents

Mitigation Steps

Mitigation Steps	For more information see:
Ensure Enterprise Provisioner and Staging Hub Server security	Security Features, beginning on page 59
Ensure Enterprise Provisioner and Staging Hub Server workstation security	User Roles, beginning on page 59
Use physical security for Enterprise Provisioner and Staging Hub Server systems	Physical and Environmental Considerations, beginning on page 18
Do not allow the use of unauthorized removable media (for example, DVDs or memory sticks) on any computer in (or connected to) your Enterprise Provisioner and Staging Hub Server system.	Protecting Against Unauthorized System Access, beginning on page 19
Use strong authentication (strong passwords) on network equipment.	Securing Network Equipment, beginning on page 32
Monitor system access	System Monitoring, beginning on page 35
Use and enforce a strong password policy	Windows User Accounts and Passwords, beginning on page 45
Ensure strong access controls are in place on the file system, directory, and file shares.	File System and Registry Protection, beginning on page 50

Accidental System Change

This threat encompasses inadvertent changes to executables or configuration files. Accidental system change can result in loss of system availability and data.

Mitigation Steps

Mitigation Steps	For more information see:
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	Windows User Accounts and Passwords, beginning on page 45
Ensure strong access controls are in place on the file system, directory and file shares.	File System and Registry Protection, beginning on page 50
Ensure user account control is enabled on relevant Operating Systems.	Windows Security Features, beginning on page 53
Ensure a system backup and recovery system is in place.	Disaster Recovery Plan, beginning on page 17

Protecting Enterprise Provisioner and Staging Hub Server System

The following tables list the steps you can take to secure Enterprise Provisioner and Staging Hub Server on Windows Server 2016 OR Windows 10 desktops:

- Servers
- Domain controller and network components (routers, switches, and firewalls)

Enterprise Provisioner and Staging Hub Server

Protection Measure	For more information, see
Take steps to implement and enforce physical security	Physical and Environmental Considerations, beginning on page 18
Set the minimum level of privilege, and enforce a strong password policy for all accounts	Windows User Accounts and Passwords, beginning on page 45
Ensure that your virus protection and Microsoft security hotfixes are up to date on all systems.	Security Updates And Service Packs, beginning on page 21 and Virus Protection, beginning on page 25
Ensure EnterpriseProvisioner and Staging Hub Server workstation security	Enterprise Provisioner and Staging Hub Server Operator Accounts, beginning on page 45
Ensure user account control is enabled on relevant Operating Systems	Windows Security Features, beginning on page 53

Network Components

Protection Measure	For more information, see
Take steps to implement and enforce physical security	Physical and Environmental Considerations, beginning on page 18
Set the minimum level of privilege, and enforce a strong password policy for all accounts.	Windows User Accounts and Passwords, beginning on page 45

System Performance and Reliability

Protection Measure	For more information, see
Do not allow port scanning on Enterprise Provisioner and Staging Hub Server computers	Port Scanning, beginning on page 33
Do not automatically schedule full system antivirus scans on Enterprise Provisioner and Staging Hub Server computers	Tuning Antivirus Scanning for System Performance, beginning on page 27

CHAPTER

3 DEVELOP A SECURITY PROGRAM

A security program is a risk-analysis driven, life-cycle approach to secure Enterprise Provisioner and Staging Hub Server Systems. This chapter describes the key components of a security 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 (those responsible for running and maintaining Enterprise Provisioner and Staging Hub Server and its infrastructure)
    - Business applications (those responsible for applications interfaced to the Enterprise Provisioner and Staging Hub Server 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 team. 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
- Equipment and assets
    - Site equipment: network equipment including routers, switches, firewalls, and ancillary items used to build the system
    - Network configuration information including routing tables and access control lists
- Intangible assets such as security policies, bandwidth, and speed
- Computer equipment including servers, cameras, and streamers
- Information stored on computer equipment, such as databases and other intellectual property

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 both within and outside the Enterprise Provisioner and Staging Hub Server deployment team and 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 Enterprise Provisioner/Staging Hub 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 to be sensitive such as personal passwords, email accounts, phone numbers, or permissions 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 Enterprise Provisioner and Staging Hub Server 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.

Performing risk assessments to evaluate the potential impact of threats and keeping a full inventory of your assets will help you to identify threats and vulnerabilities. Performing these tasks will help you decide 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 Enterprise Provisioner and Staging Hub Server network 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 Enterprise Provisioner and Staging Hub Server 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
- Ongoing risk assessments as new devices are placed on the network (see Develop a Security Program, beginning on page 11)
- The creation of an Incident Response Team (see Security Response Team, beginning on page 16)

Additional Security Resources

Operating System Security Information	
Microsoft Security Overview	http://technet.microsoft.com/en-us/security/default.aspx
National Cyber Security Partnership	https://national-cyber.org/
SANS Internet Storm Center	https://isc.sans.edu/
CERT	http://www.cert.org/
CanCERT	http://www.ewa-canada.com/cancert/

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

Security Response Team

The responsibilities of a SRT can include:

- Monitoring the Microsoft update sites
- Monitoring the availability of antivirus software updates
- Risk assessment of each security update, antivirus update, and any other update as it is made available
- Determining the amount of verification required for any update and how the verification is to be performed
    - In extreme cases, it may helpful to have an offline system available so that full functionality testing is possible. This would be particularly useful where it is normal practice to install hotfixes as soon as they are announced, rather than waiting for Honeywell qualification
- Determining when the update is to be installed
    - There may be times when the SRT determines that an update is so important that you cannot wait for Honeywell's verification cycle and you need to verify and install it early on all your systems
- Ensuring the deployment of qualified security updates on the Honeywell Enterprise Provisioner and Staging Hub Servers
- Checking that Microsoft Baseline Security Analyzer is run periodically to ensure that security updates have not need missed. For details, see Using Microsoft Baseline Security Analyzer, beginning on page 35
- Reviewing network infrastructure patches and configuration changes that will help to secure the network against the latest methods of attack

CHAPTER

4 DISASTER RECOVERY PLAN

This section describes planning considerations for backup and restoration policies and the tools that are supported for backing up and restoring your Enterprise Provisioner and Staging Hub Server system.

Formulating a Disaster Recovery Policy

As part of your security strategy you should define a comprehensive backup and restore policy for disaster recovery purposes. In formulating this policy you need to consider:

- How quickly data or the system needs to be restored
    - This will indicate the need for a redundant system, spare offline computer, or simply good file system backups
- How long data needs to be kept
- The frequency of changes to critical data and configuration settings
    - This will dictate the frequency and completeness of backups
- The safe onsite and offsite storage of full and incremental backups
- The safe storage of all Microsoft Operating System and Enterprise Provisioner and Staging Hub Server related installation media, license keys, and configuration information
- Who will be responsible for backups and testing as well as storing/restoring of backups

Backup

Recovery from a disaster requires that you can restore you system quickly. Thus backing up the system is recommended. No particular tool is recommended, but using the Microsoft backup tools is a good start. In addition, the Microsoft Security Baseline tool can be used to save the current security settings of a properly running system and be used to restore after a failure.

In addition, the baseline tool should be used after updates to the system to keep the baseline data up to date.

Availability of Spare Equipment

It is recommended to maintain a supply of spare workstation computers and associated peripheral hardware (mouse, speakers, monitors etc.) to provide for quick replacement in the case of workstation hardware failure.

Disaster Recovery Testing

Disaster recovery plans should be tested at least once per year (or more often) to confirm that the current steps are valid and working as expected. This can detect if the backup plan is not working and will detect the lack of a functional backup.

Note: *Testing of the restore from backup must be done on an alternate server machine, not on a production server.*

Physical and Environmental Considerations

Physical Location

When addressing the security needs of your system and data, it is important to consider the following environmental factors:

- Dust: The server and network equipment should be in a filtered environment to prevent the infiltration of dust, dirt and other contaminants
- Vibration: The server or server rack should be mounted on rubber isolation pads to prevent disk drive damage and wiring connection problems in environments with structural vibration
- Water: The server or server rack should be in an area that is not susceptible to flood or liquid seepage. It should be elevated above the base floor level either by a raised floor or mounting pad. It should be in an area with no overhead piping that could break or otherwise leak into the equipment
- Temperature and humidity: The server should be in an appropriately conditioned space with stable temperature and humidity conditions appropriate for the server, network equipment and stored backup media

A major cause of downtime in the IT world is hardware theft, either of whole computer or individual components such as disks and memory chips. At the very least, the computer and monitor should be secured to the furniture, and the case locked and closed. Network equipment should be placed in a cabinet or locked closet to protect against unauthorized access to the power, console ports, and network ports.

If computers are readily accessible and have a CD or DVD drive, you may also consider fitting locks to the drives, or removing the CD and DVD drives from the computers altogether. If the server has unused USB ports, they should be disabled to

prevent memory sticks or other uncontrolled devices from being connected to the system. Such devices may be used to introduce virus or other malware applications. You should also consider disabling or physically protecting the power button to prevent unauthorized use.

For maximum security, the Enterprise Provisioner and Staging Hub Servers, computers with access to Enterprise Provisioner and Staging Hub Servers, and all network equipment should be placed in a secured area. The area or room should be under electronic access control security with full audit capabilities and digital video surveillance. Audit trail data should include the date, time, and personnel access logs.

Protecting Against Unauthorized System Access

External media drives can enable anyone to bypass Windows security and gain access to your system.

If there is easy access to a computer, and it has a floppy disk, CD/DVD drive or a USB port, it can be booted from an alternative operating system. This can be used to circumvent file system security, and could be used to install damaging software, or even to reformat the hard disk.

It is critical that you do not allow (and you actively prevent) the use of all unauthorized removable devices and media such as CDs, DVDs, floppy disks, and USB memory sticks on Enterprise Provisioner and Staging Hub Server computers.

There are several other steps that can be taken to reduce the risk of unauthorized access, including:

- Setting the BIOS to boot only from the C: drive (or the equivalent Operating System partition on the onboard hard disk drive)
- Setting a BIOS password (check that this does not prevent automatic startup)
- Physically securing the computer (for example, in a locked room or cabinet) or fitting locks to the floppy and CD/DVD drives
- Removing (in extreme cases) the floppy and CD/DVD drives from the computer
- Disabling USB ports and other ports capable of being used for memory sticks or portable storage devices
- Group policy may be used to prevent certain drive letters (e.g. DCD/DVD drive) from being visible to Microsoft Windows Explorer. For instructions on how to do this for Windows, see http://support.microsoft.com

Note: *Hiding the drives in Windows Explorer does not prevent those drives from being accessed via Command Prompt. Another option is to remove the drive letter using* ***Administrative Tools > Computer Management > Disk Management****.*

Network and Device Access

To prevent unauthorized tampering, the devices and network equipment should be physically protected in locked cabinets, and logically protected with passwords or other authentication techniques.

Default passwords for hardware devices should be changed from their default settings. This includes default passwords for Enterprise Provisioner and Staging Hub Servers, default passwords for attached devices, and default passwords for UPS hardware.

Network cables are vulnerable to damage or unauthorized connection. Where communication redundancy is required, cabling should be run in separate hardened cable runs.

Reliable Power

Reliable power is essential, so you should provide an uninterrupted power supply (UPS). If the site has an emergency generator, the UPS battery life needs to be at least long enough for the generator to come online; however, if you rely on external power, the UPS probably needs several hours supply. Other considerations are to have enough time to shut the server down properly in preparation for a switchover/move to a backup server/location.

Note: *When there is redundant equipment (redundant servers or redundant switches), you should ensure each unit in a redundant pair is on a different UPS or power source.*

CHAPTER

5 SECURITY UPDATES AND SERVICE PACKS

An important part of your overall security strategy is to set up a process that ensures that the operating system software is kept up to date.

It is important to recognize that frequent updates to critical Enterprise Provisioner and Staging Hub Server computers can be error prone and may destabilize your system over time. Updates should be undertaken judiciously and with care.

Microsoft Security Updates

Microsoft regularly releases a range of security updates and other operating system and software updates. Timely information on security updates can be obtained by subscribing to the Microsoft Security Bulletin Summary at: http://www.microsoft.com/technet/security/bulletin/notify.mspx

For information on current and past hotfixes, see: http://www.microsoft.com/technet/security/current.aspx

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.

Once system functionality has been confirmed after an update, to ensure that closed security holes are not inadvertently or maliciously re-opened, uninstall of the update should be disallowed.

To prevent inadvertent uninstall of Windows updates via Control panel, the **Hide Installed Updates' page** group policy should be enabled. This can be found in **Local Group Policy Editor > User Configuration > Administrative Templates > Control Panel > Programs**.

Note: *This setting does not prevent users from using other tools and methods to install or uninstall programs.*

Microsoft Service Packs

A service pack is a tested, cumulative set of security and other updates. Service packs may also contain additional fixes for problems that have been found since the release of the product, and a limited number of customer-requested design changes or features.

Microsoft performs full integration testing of their service packs against the operating system and their own applications. Before you deploy the Microsoft Service Packs to Enterprise Provisioner and Staging Hub Server computers, you should verify service packs on a non-production computer, or in a scheduled maintenance period, to ensure that there are no unexpected side effects.

Distributing Microsoft Updates and Virus Definition Files

It is important to install Microsoft security updates and updates to virus definition files on all network computers (including non-Enterprise Provisioner and Staging Hub Server computers) in your Enterprise Provisioner and Staging Hub Server system and the systems connected to it.

It is, however, not best practice to distribute Microsoft security updates and updates to virus definition files directly from the business network to computers on the Enterprise Provisioner and Staging Hub Server as this is contrary to the goal of minimizing direct communication between computers on these networks. Honeywell therefore recommends that an update manager and an antivirus server be in the DMZ (see The Demilitarized Zone, beginning on page 31). Both roles can be performed by a single server. Contact your Honeywell representative if you need assistance configuring computers in a DMZ.

Implementing a Microsoft update and antivirus management system that is dedicated to the Enterprise Provisioner and Staging Hub Server Network helps to ensure more controlled and secure updates, tailored for the unique needs of the particular environment.

The following Windows Policy setting recommendations should be considered for the computers in the Enterprise Provisioner and Staging Hub Server Network which connect to the update management server in the DMZ:

Policy	Setting	Comment
Allow automatic updates immediate installation	Disabled	Ensures that updates are not installed prior to any predetermined schedule
Allow non-administrators to receive update notifications	Disabled	Ensures that only administrators are privileged to install updates
Configure automatic updates	Enabled	Ensures that computers check for updates from the update management server on a schedule determined by you

Policy	Setting	Comment
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled	Ensures that installation of updates is a considered choice when shutting down a computer
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Disabled	Ensures that computer users are not prevented from installing updates when made available from your management server
No auto-restart with logged on users for scheduled automatic updates installations	Enabled	Ensures that operators are not interrupted by a computer reboot for Windows updates while they are in the middle of critical activities
Specify intranet Microsoft update service location	Enabled	Ensures that the computer uses your specified update management server for downloading updates
Turn off Automatic Root Certificates Update	Enabled (for computers on isolated networks with no internet access)	Prevents computers from trying to access the Microsoft Windows Update Web site to check for trusted authorities

CHAPTER

6 VIRUS PROTECTION

Antivirus measures are an essential element of a comprehensive security strategy.

Choosing Antivirus Software

There is no specific Antivirus Software that has been tested for Enterprise Provisioner and Staging Hub Server in Release 1.0. Honeywell recommends that you use an anti-virus package to protect the Enterprise Provisioner and Staging Hub Server system.

When choosing an antivirus product, please consider the following:

- Template files need to be updated frequently without Administrator action
- The package should be capable of being configured to manage exclusions
    - Exclusion offers the ability to skip directories or specified file types during the scanning process
    - Small independent software packages are less likely to offer these abilities and as such are not a recommended solution

Installing Antivirus Software

If your Enterprise Provisioner and Staging Hub Server software is already installed, then you should backup your Enterprise Provisioner and Staging Hub Server system prior to installing any third-party software, including antivirus software. A full system backup, including the registry and details of directory security for Enterprise Provisioner and Staging Hub Server install directories, is the preferred approach.

After installing the antivirus software, check through the Windows Event Logs, and the Enterprise Provisioner and Staging Hub Server logs (if Enterprise Provisioner and Staging Hub Server is already installed on the computers), and ensure no obvious errors are being reported.

If the system starts experiencing failures, or if the logs show deadlock errors, the inability to read or write files, or any other unusual behavior, disable the antivirus software to see if the failures continue. Note that some antivirus software may need to be completely uninstalled to be disabled.

Ensuring Frequent Updates to Antivirus Signature Files

Non-directed virus and worm attacks are common attacks on a system. A virus that is deemed low risk for corporate systems may pose a high risk to a Enterprise Provisioner and Staging Hub Server system if it causes a denial of service. It is therefore essential to update antivirus signature files frequently by:

- Subscribing to the updates of your antivirus software vendor(s)
- Leveraging enterprise antivirus policies and practices

Since new viruses are being released every day, the system will remain vulnerable to attack if the signature files are not updated at the same rate. Where it is not practical to perform updates daily, it is worth monitoring reputable Web sites which publish information about new virus attacks so that the system can be isolated if a specific threat appears.

Receipt of new signature files generally requires Internet access so that the files can be downloaded from the antivirus software vendor. It is recommended that you set up special servers for the controlled distribution of antivirus signature files to the Enterprise Provisioner and Staging Hub Server network as outlined in Section Distributing Microsoft Updates and Virus Definition Files, beginning on page 22 *Distributing Microsoft updates and virus definition files*.

Testing the Deployment of Antivirus Signature Files

It is important to test antivirus signature files offline on non-production servers before deploying them to the live Enterprise Provisioner and Staging Hub Server system. This helps to ensure that the signature file does not compromise the antivirus software or cause problems on the computer. This recommendation is based on known examples of antivirus software affecting its operating environment. As an example, see: http://support.microsoft.com

In line with the best practice of minimizing communication between the business network and the Enterprise Provisioner and Staging Hub Server network, it is recommended that updates to antivirus signature files be distributed from a server located in a DMZ as outlined in Distributing Microsoft Updates and Virus Definition Files, beginning on page 22.

When implementing the automatic deployment of signature files, it is also important to:

- Stagger automatic deployment (deploy to no more than three or four computers per hour) to eliminate the potential for common cause failure
    - This is especially important if you are not able to test files in a non-production environment prior to their roll-out
- Follow the recommendations of your antivirus software vendor for distribution server/services
- Stage the distribution on a test system

Configuring Active Antivirus Scanning

It is recommended that you adopt an active virus scanning strategy. Honeywell recommends an on-access scanning strategy, as this provides the best real-time protection for your system. You should additionally consider running on-demand scans during regular, scheduled maintenance windows however, to catch any malicious files or programs which may be currently dormant on a computer.

Both on-access and on-demand scanning should be configured to:

- Scan the boot sectors of all floppy disks
- Move infected files to a quarantine directory and notify the user that an infected file was found. The user should be allowed to clean up the infection
- Virus scan reports should be regularly reviewed as part of your active scanning strategy

Tuning Antivirus Scanning for System Performance

In formulating your virus scanning strategy you may need to consider the potential impact on critical system resources.

For example, if your Enterprise Provisioner and Staging Hub Servers are experiencing problems due to low system resources, you may need to:

- Ensure that antivirus software (and other third party applications) only runs when system resources on the computer are adequate to meet system needs
- Limit the system resources that are used by antivirus software during scanning. Honeywell has tested antivirus software successfully on extremely large systems by limiting the CPU utilization of antivirus software to as low as 10%

To find the proper balance between server performance and virus protection, you may need to make configuration choices such as disabling scanning on reading of files and changing the default process-based scanning to per-process scanning.

Note: *Do not automatically schedule full system scans on any Enterprise Provisioner and Staging Hub Server as this can result in severe degradation of performance, and could impact the ability of operators to respond to an incident.*

Virus Scanning and System Performance

The Enterprise Provisioner and Staging Hub Server system requires a certain amount of system resources (2GHz or faster processor and 4GB RAM), to perform reliably. Shortages of these resources may lead to decreased system performance.

When tuning antivirus software, consider balancing performance against risk. On some systems, the high performance of the server computer is balanced against the performance of the scanning engine. Some antivirus scanners allow you to set maximum CPU usage.

The default installation of antivirus software will generally meet the demands of most customers. However, for systems with extremely high CPU usage and input/output demands, the default installation of antivirus software may impose system limitations. Please refer to your antivirus software documentation for specific procedures on how to limit CPU utilization.

If your system is experiencing continued resource-related performance problems, there are further steps that you can take to limit the resources consumed by antivirus software. For up-to-date and specific information, consult the Web site for your antivirus software.

Note: *Some failures which appear to be resource problems may be an action taken by the antivirus software to try and protect the computer from a suspected threat.*

For example, Symantec Endpoint Protection antivirus software can limit the bandwidth for TCP/IP sessions and/or disable the Network Card temporarily to prevent perceived Denial of Service Attacks due to heavy network traffic. This feature, and similar features of other antivirus products, has potential to cause communication failures with the affected computer.

It is strongly recommended that limiting the bandwidth for TCP/IP sessions and/or disabling the Network Card temporarily feature be disabled or uninstalled when you use the antivirus software.

For an example of how the Symantec antivirus package accomplishes this, see: http://www.symantec.com/endpoint-protection

Prohibiting Email and Messaging Clients

Do not install email clients on any Enterprise Provisioner and Staging Hub Server. Honeywell does not support email clients.

Viruses and Email

Many viruses and malware are spread via email. Not only do these viruses cause damage to computers, often rendering them inoperable, they also cause significant network traffic by mass-mailing to other addresses, which may prevent the timely delivery of alerts.

Instant Messaging

Instant messaging (IM) software can be used as a transport mechanism for malware. The malware sends messages to all IM contacts on an infected computer, thereby increasing network traffic uncontrollably. This message itself, seemingly from a trusted source, usually tells the recipient to browse to a malicious website which will then download more serious malware, opening back doors or otherwise allowing takeover of the computer.

Honeywell strongly advises against supporting instant messaging on a Enterprise Provisioner and Staging Hub Server.

Spyware

An increasingly common threat posed by spyware, also known as “bots” are typically small modules that do not in themselves cause damage, but record keystrokes and other user actions, and then transmit this information to a remote host, where passwords, account, and other information can be extracted.

Conventional antivirus checkers do not look for spyware. Like viruses and other malware, spyware can be spread via email or inadvertently downloaded during Internet access.

Note: *Honeywell does not support internet and email access from the Enterprise Provisioner and Staging Hub Server. Use of spyware removal applications may cause unexpected results if run on your Enterprise Provisioner and Staging Hub Server or workstation computers. These applications may alter registry settings that are crucial to the operation of the software. If spyware is detected, and a spyware removal application needs to be used, ensure that the computers are backed up prior to the installation of the spyware removal application. Refer to Backup, beginning on page 17 for details on backing up the Enterprise Provisioner and Staging Hub Server computers.*

CHAPTER

7 NETWORK PLANNING AND SECURITY

This chapter describes key network security considerations for the Enterprise Provisioner and Staging Hub Server systems.

The network security model described herein takes the position that security of the Enterprise Provisioner and Staging Hub Server Network and Enterprise Provisioner and Staging Hub Server applications are critical.

What follows are recommendations for a secure network, not a depiction of the only way Enterprise Provisioner and Staging Hub Server may be properly installed.

Customers need to evaluate their business, required compliance, and potential risks before deploying the Enterprise Provisioner and Staging Hub Server application. Once those factors have been determined, customers should deploy the Enterprise Provisioner and Staging Hub Server applications in a manner that is consistent with the IT security regulations and policies in their organization.

Installations where there are regulations, policies, or compliance to specific government requirements, may need to follow the recommendations and architecture in the absolute sense.

The Demilitarized Zone

A Demilitarized Zone (DMZ) is a separate network segment that connects directly to the firewall and provides a buffer between the Enterprise Provisioner and Staging Hub Server network and the Internet. The DMZ can be used to access the Internet to download updated anti-virus updates, Microsoft software updates and services packs and any other activities required to access the Internet.

It is recommended that direct access between the Enterprise Provisioner and Staging Hub Server network and the Internet is avoided by having each network only access computers in the DMZ. By eliminating the direct connection between the devices in the Enterprise Provisioner and Staging Hub Server Network and the Internet network, the security of Enterprise Provisioner and Staging Hub Server network is increased.

In the DMZ, any external connections should be permitted through the firewall and only identified ports required for specific communication should be opened.

Configuring The DMZ Firewall

Honeywell recommends that the firewall use a restrictive security policy; that is, all access should be denied unless explicitly permitted.

Filtering should be used to permit only specific computers on DMZ and Enterprise Provisioner and Staging Hub Server network to communicate. TCP port filtering should be used to stop denial-of-service attacks to well-known ports.

Securing Network Equipment

The configuration of network equipment such as switches, routers, and firewalls is a critical part of the security for a Enterprise Provisioner and Staging Hub Server Network. Each piece of equipment should have a unique name and be secured by a strong authentication (password).

During normal operation, do not enable HTTP, FTP, or Telnet on devices that support these features. However, if substantial re-configuration is needed, they may be enabled for the duration of the maintenance.

Unused physical ports on the Enterprise Provisioner and Staging Hub Server Network's infrastructure equipment (switches and routers) should be disabled and only enabled when needed through your site's change management procedure.

It is recommended that you choose intelligent switches for use in your network, as the features available on these devices can help to prevent Denial of Service (DOS) attacks.

Domain Name Servers

Whenever a TCP connection is made, the system must convert the user-provided host name into an IP address. This is usually performed by the Domain Name Server (DNS), a service generally hosted by the domain controller. In turn, this DNS will consult other DNS systems, both internal and external on the Internet to resolve unknown names.

There is a well-known attack method, known as cache poisoning, which results in incorrect resolution, generally aimed at leading Web browsers to rogue sites which will cause malware to be downloaded.

A possible side effect will be that clients are unable to find the host, resulting in Enterprise Provisioner and Staging Hub Server workstation computers being unable to connect to the local Enterprise Provisioner and Staging Hub Server.

Mitigating Actions:

- Hardening the DNS: Windows Server operating systems have a registry setting which will cause the DNS to reject some false updates
- Using the local hosts file on each workstation computer in place of a DNS to perform the resolution. Use of the hosts file provides protection from DNS

poisoning attacks, but has some administrative disadvantages in that each workstation must be manually updated if IP addresses change. One approach is to have a central copy of hosts which is copied to each computer when required. This will also act as a backup should an individual hosts file become corrupted.

- If possible, use secure DNS services that authenticate the DNS servers

Unfortunately, some malware also target the host file, usually by adding its own entries. This threat is greatly reduced by the presence of antivirus software, using strict file permissions (by default, only Administrators can modify it), and by marking the file as read-only. Should corruption still occur, only one computer will be affected. If DNS corruption occurs, then all computers will be affected.

Remote Access

Remote access allows connection to the Enterprise Provisioner and Staging Hub Server from the outside the DMZ including the Internet using a customer's corporate WAN or a direct Internet connection. A client should connect to the corporate WAN via a VPN client tunnel. Authentication occurs when the client's VPN connection is established with the corporate VPN server. Once authenticated, the client can connect to the Enterprise Provisioner and Staging Hub Server via Windows Remote Desktop or other remote access system required by the specific customer.

Such access may be used to:

- Perform remote support by Honeywell engineers or other support staff. In this instance, more direct access to the target computer is needed and Windows Remote Desktop would be used to reach the target computer.

Remote direct computer access will require ports in the firewall to be opened to allow direct access. These ports should be shut off as soon as the support project is complete. It may also be beneficial to have a special account that is used only by the remote support user and is disabled when connection is not expected. You can achieve this automatically by specifying a short password age time.

Port Scanning

Only allow port scanning at the perimeter of your Enterprise Provisioner and Staging Hub Server Network, that is, from outside the firewall, pointing into the DMZ. Do not allow port scanning of online systems within the Enterprise Provisioner and Staging Hub Server network, as this could lead to performance degradation and to system failure. For the ports used in Enterprise Provisioner and Staging Hub Server system, please refer to Network Ports Summary, beginning on page 65.

Third-Party Applications

Honeywell does not recommend the installation and use of third-party applications on any Enterprise Provisioner and Staging Hub Server computers. Third-party applications may affect the performance of these computers. Only those applications used by the Enterprise Provisioner and Staging Hub Server system which have been tested and qualified, should be installed on these computers.

If third-party software is necessary, all third-party software should be patched and kept up to date to protect against security vulnerabilities. As noted above, changes should only be tested on test servers before distributing to Honeywell systems.

Remote Monitoring Applications

Honeywell does not recommend the installation and use of remote monitoring and control applications, such as LANDesk Remote Control, on any Enterprise Provisioner and Staging Hub Server Network computers. This includes Enterprise Provisioner and Staging Hub Servers . These applications may affect the performance of these computers and perhaps even result in a loss of data process and security.

CHAPTER

8 SYSTEM MONITORING

If all the steps outlined in this document are followed, then a secure system should result. However, there is always the possibility that an attacker will succeed in circumventing all the safeguards and break in. In this case it is important to discover the break in and prevent further damage as rapidly as possible. The earlier a system break is detected, the more evidence that is captured, the less damage is likely to occur and the greater the chances of identifying the intruder.

Using Microsoft Baseline Security Analyzer

It is recommended that you download and run Microsoft Baseline Security Analyzer (MBSA) on your system.

MBSA is a tool that you can run on Windows-based computers to check for common problems with security configuration. MBSA checks the operating system as well as installed components like Internet Information Services (IIS) and SQL Server. It also checks whether security updates are current.

MBSA is freely available for download from the Microsoft Web site. By default, MBSA attempts to connect to the Microsoft Web site to download the latest information on hotfixes, service packs, and so on. However, MBSA can be configured to use its registered Update Services server for this purpose. It only takes a few minutes to run and generates a series of reports on the security health of a system.

Setting Up and Analyzing Windows Audit Logs

It is recommended that you enable the auditing of your file system and registry access. If there is a suspicion that the system is being misused, then Windows auditing provides a useful tool to track who has done what and when. If possible, the logging should be centralized, that is automatically collected on a central log service.

Once Windows auditing is enabled, the Windows audit logs should be reviewed frequently by a responsible person who can act if unexpected activity is seen.

Considerations

The default action is to halt the system if the security log becomes full. This is to prevent activity occurring without any traceability. However, it also provides an opportunity for a denial of service attack.

To prevent this, either increase the log file size and review the log before it fills up, or set one of the overwrite options (for example, Overwrite events as needed), and check the log frequently enough to prevent loss of events.

To view the log settings, start the Event Viewer tool, and select Windows Logs Security and then select to open the Log Properties. From here you can change the Maximum Log Size, and the action to take when the maximum event log size is reached.

Configuring the log settings to overwrite will ensure that the system never stops when the log is full but this can also be used to hide events of interest by falsely filling the log with other events. This highlights the need for regular monitoring.

You should ensure that the audit log is regularly inspected and cleared, or else disable the security policy **Local Policies>Security Options>Audit**: shut down system immediately if unable to log security audits.

To Enable Auditing:

Either:

Set the appropriate Group policy, or

Log on as the Local Administrator and:

- Open the Local Security Policy editor by typing **secpol.msc** at a command prompt.
- Select **Local Policies>Audit Policy** and enable the appropriate options.

The most useful options are likely to be:

Policy	Security Setting
Audit account logon events	Success and Failure
Audit account management	Success and Failure
Audit directory services access	Failure (for domain controllers)
Audit logon events	Success and Failure
Audit object access	Failure
Audit policy change	Success and Failure
Audit privilege use	Failure
Audit process tracking	Success and Failure
Audit system events	Success and Failure

Choosing to audit object access enables the auditing of file system and registry access. Once enabled, it is necessary to subsequently choose the objects of interest and the user (or groups) whose actions are to be audited. Since it is necessary to specify an identity to audit (and it is not known who the intruder is), you should specify the group Everyone.

To configure the auditing of file access:

Open Windows Explorer and select the directory or file of interest.

1. Right-click on the file or folder and select **Properties > Security > Advanced> Auditing**
2. If you are prompted with a warning about being an administrative user with privileges to view the object's auditing properties, select to continue
3. If you are prompted by User Account Control, select **Yes** to continue
4. In the Advanced Security Settings dialog, select **to Add a user or group** (for example, Everyone) and configure the access to be audited (for example, Open failure).

To configure the auditing of registry keys:

1. Choose **Start>Run** to open the Run window.
2. Type **regedit** and click **OK**.
3. Right-click the key you want to audit and select **Properties > Security > Advanced > Auditing**.
4. If you are prompted with a warning about being an administrative user with privileges to view the object's auditing properties, select to continue
5. If you are prompted by User Account Control, select **Yes** to continue
6. In the Advanced Security Settings dialog, select to Add a user or group (for example, Everyone) and configure the access to be audited (for example, Open failure)

Auditing Enterprise Provisioner and Staging Hub Server Database Access

Rather than enabling auditing of Enterprise Provisioner and Staging Hub Server database access, Honeywell recommends blocking all direct access to the databases from machines other than the server itself and other Enterprise Provisioner and Staging Hub Servers on the local Enterprise Provisioner and Staging Hub Server network.

Restricting Access to Event Logs

By default, anonymous accounts and guest accounts can view the Windows Event Logs when logged in to a Windows computer. It is recommended that this be restricted on Enterprise Provisioner and Staging Hub Server computers, as the System, Application and Security logs can contain information about your system and its operations.

To restrict access to administrators and system accounts only:

1. Choose **Start>Run** to open the Run window.
2. Type **regedit** and click **OK**.
3. Expand the HKEY_LOCAL_MACHINE tree until you open the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog registry key.
4. Select the Security subkey.
5. Right-click in the right-hand window and choose **New>DWORD Value** to create a new registry value.
6. Name the new value **RestrictGuestAccess**.
7. Right-click **RestrictGuestAccess** and select **Modify**.
8. Type **1** into the RestrictGuestAccess value data field and click **OK**.
9. Repeat steps 5 through 8 for the Application and System subkeys.
10. Close the Registry editor.

Detecting Network Intrusion

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 (most of these are aimed at the UNIX world), 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 act such as raising alerts or even disconnecting the computer from the network. The latter is a dangerous option which causes its own denial of service while preventing damage from occurring to the system, by closing network ports, and so on.

Most firewalls, switches, and routers have reporting facilities that can report various levels of events, ranging from debugging to emergency failure. These reports can be viewed via telnet, collected by a central logging server, or be 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.

Syslog servers commonly exist on Unix systems, but third party syslog services are available for Windows. Some of these vary in functionality and cost, from freeware, which simply writes to a log file, to sophisticated NIDS systems which analyze the logs in detail.

As well as being able to control the level of severity of events, the PIX firewall allows the suppression of individual messages. This can significantly reduce the clutter and provides some ability to recognize common attack signatures and to raise appropriate alarms.

When configuring the logging of these network events, a balance must be kept between collecting too many acceptable events (and missing something important) and filling storage disks and deleting information (which is subsequently needed for an intrusion investigation).

The following is a typical log from a firewall.

Jun 03 14:17:44 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code 0) by access-group "outside_access_in"

Jun 03 14:17:49 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny tcp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX by access-group "outside_access_in"

Jun 03 14:17:51 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp src outside:XXX.XXX.XXX.XXXX dst inside:XXX.XXX.XXX.XXX (type 0, code 0) by access-group "outside_access_in"

Jun 03 14:17:51 XXX.XXX.XXX.XXX local4.err %PIX-3-305005: No translation group found for tcp src inside:XXX.XXX.XXX.XXX dst outside:XXX.XXX.XXX.XXX

Jun 03 14:17:57 XXX.XXX.XXX.XXX local4.err %PIX-3-305005: No translation group found for tcp src inside:XXX.XXX.XXX.XXX dst outside:XXX.XXX.XXX.XXX

Jun 03 14:18:01 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code 0) by access-group "outside_access_in"

Jun 03 14:18:11 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code 0) by access-group "outside_access_in"

Jun 03 14:18:23 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny icmp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX (type 0, code 0) by access-group "outside_access_in"

Other forms of intrusion detection will search event logs looking for unusual events, or will compare the current file system to a known good image. Care must be exercised when running such tools to prevent them using too many resources and interfering with the control system.

Setting Up An Event Response Team

An event response team should be ready to handle any security breach as it occurs. Their role is to identify the attack, prevent further damage, recover from the damage and capture evidence which could be used in prosecutions. In many instances the IT department will already have such a team; they simply need to be made aware of any specific requirements of the control system.

Many Government and industry bodies and computer vendors have published good papers on this topic, which should be reviewed when building the team.

Useful references include:

http://technet.microsoft.com/en-au/security/default.aspx
http://www.sans.org/security-resources/
http://csrc.nist.gov/

CHAPTER

9 WINDOWS DOMAINS

When planning your system, you need to consider how the Windows-based computers in the Enterprise Provisioner and Staging Hub Server Network will fit into the IT infrastructure, and how users will be given access to both the Enterprise Provisioner and Staging Hub Server Network and the business network. This is generally achieved using Windows domains and workgroups.

Domains

A Windows domain is a collection of computers that share a common network directory database and security policy. A domain is managed by a domain controller, the server that authenticates domain logons and maintains the security policy and master database for a domain. Each domain, and each computer within that domain, has a unique name.

Domains typically use a DNS for the transparent translation of computer names to IP addresses when connections are made.

Organization Units and Group Policy

Windows domains also use Organization Units (OU). An OU is a group of objects (users) to which common Group Policy can be applied. It is the smallest unit to which administration rights can be granted. An OU enables an administrator to manage operator accounts independently of the overall domain administration. OUs also allow the application of Group Policy to users and computers within the OU. This is useful for controlling dedicated operator computers so that they all have common security settings, as well as a common appearance and execution environment.

For more information on OUs and Group Policy, see the appropriate Active Directory documentation provided by Microsoft.

Windows Domains: Forests, Trees, and DNS

Domain concepts such as forests, trees, and dynamic DNS allow users to closely integrate Windows domains in IT and building management.

It is important to understand and be familiar with these concepts before installing a new Windows domain, or upgrading your Windows domain, as it is not easy to modify these constructs after a domain has been established. If you establish a domain and then subsequently decide on a different architecture, a significant amount of manual work may be required to migrate to the new architecture.

For Enterprise Provisioner and Staging Hub Servers, it is recommended to set up in the same domain and without sharing domains with outside networks.

Domain Membership

Active Directory's scalability allows the largest of organizations to utilize a single domain implementation. Honeywell recommends that customers maintain a separate Windows domain for Enterprise Provisioner and Staging Hub Server Network systems in order to accommodate management requirements.

A separate domain for the Enterprise Provisioner and Staging Hub Server Network has the following advantages:

- Increased security and reliability
- Centralized and independent management of security
- The ability to customize security policies for the Enterprise Provisioner and Staging Hub Server Network
    - Changes to the business domain will not affect the Enterprise Provisioner and Staging Hub Server Network

Honeywell recommends that the Enterprise Provisioner and Staging Hub Server software is installed on a computer and checked for correct operation before being added to a domain. This can help in troubleshooting issues caused by group policies that may interfere with the Enterprise Provisioner and Staging Hub Server software.

Active Directory Forests and Trees

Active Directory forests and trees are hierarchical organizations of domains. Domains configured in forests and trees share a common schema and all domains within a forest or tree have automatic two-way transitive trusts between them. Honeywell recommends that the Enterprise Provisioner and Staging Hub Server Network not be in a forest or tree that includes the business network domain.

Inter-Domain Trusts

Inter-domain trusts are used to allow users in one domain to access resources on a different domain. Native Windows Server 2012 domains have implicit two-way trust relationships called transitive trusts between domains within a forest, and may have explicit trusts between domains in different forests.

Limiting Inter-Domain Trust

It is important to limit inter-domain trust, that is, not to trust other domain users to log on unless absolutely necessary. It is recommended that you do not permit trusts between the Enterprise Provisioner and Staging Hub Server Network and business network domains. If no trusts exist, administrators can be assured that no access to Windows resources can be configured for users from other domains.

If trusts are necessary, then the “least access” principle should be followed: that is, only have the trusts that are required. Use a one-way trust if possible. Explicit trusts can be configured between Windows domains. Note that if Enterprise Provisioner and Staging Hub Servers and Enterprise Provisioner and managed devices are on different domains, two-way trust between these two domains is required.

CHAPTER

10 SECURING ACCESS TO WINDOWS OS

An essential component of any security strategy for computers in the Enterprise Provisioner and Staging Hub Server 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 those necessary for the performance of their duties.

Windows User Accounts and Passwords

Access is gained to the Windows operating system by logging onto the computer using a user account name and password. This is true for both local and remote terminal services access. Because user accounts may be well known or easily guessed within an organization, the password becomes the prime vehicle for authentication. User account and password policies are therefore important security measures.

User Account Policies and Settings

As a general rule Honeywell recommends:

- Review user accounts on a regular basis
- Disable or delete all unused accounts
- Disable all guest accounts

Enterprise Provisioner and Staging Hub Server Operator Accounts

Enterprise Provisioner and Staging Hub Server operator accounts should be set up as follows:

- Enable operator accounts to log in only to servers
- Do not use a shared operator account if individual accountability is required

Non-Operator User Accounts

Accounts for engineers and others who need interactive access to server computers for maintenance activities should be enabled to log in to all Enterprise Provisioner and Staging Hub Server Network computers.

New Accounts

To prevent the use of default passwords, new accounts should have the *User must change password option* set until their first login.

Administrator Accounts

It is essential that the password for the Administrator account be changed from the default set at installation.

Please note that the Administrator account cannot be locked out and is therefore vulnerable to continual attacks with random passwords.

A suggested practice is to use Group Policy to modify the Administrator user name. Renaming the local Administrator account does not, however, provide complete protection from attack as there are tools that attempt to break into the server using the Security Identifier (SID) of the Administrator account. The SID of the local Administrator account cannot be changed.

On Windows Server 2012, Windows 7 and Windows 10, the built-in Administrator account is disabled by default and should be kept disabled. A separate Administrator account should be created for performing admin activities on all Enterprise Provisioner and Staging Hub Servers.

Service and Server Accounts

Windows services and COM servers should run under an account with the lowest possible set of privileges. The account should not have the login interactively permitted permission set.

The following classes of accounts are suggested in order of preference:

- Local service accounts
- Domain accounts with minimum rights
- The Network Service account
- Local or domain user accounts belonging to the Local Administrators group
- The local system account

Running services under the local system account should be avoided as compromised processes running under this account have rights to act as part of the operating system and can gain full control over the computer. From Windows Server 2003, a new Local Service account has been added to reduce the security risk.

Password Policies and Settings

The most popular technique for breaking into a system is to guess user names and passwords. Consequently, it is essential that passwords are difficult to guess and that they are changed often.

Additionally, Honeywell recommends implementation of biometric and/or two-factor authentication instead of standard one-factor password authentication for Windows login on all Enterprise Provisioner and Staging Hub Server and workstation computers.

Password Settings

You can apply system-wide control of passwords using Group Policy. Alternatively, you can apply individual control to each account.

Parameter	Setting	Comment
Maximum password age	45 to 90 days	Forces the choice of a new password after this time. The setting for the Administrator account should be shorter. A maximum of 30 days is recommended.
Minimum password age	1 to 5 days	Prevents too rapid a cycling of passwords.
Minimum password length	12-14 characters	Improves encryption and makes guessing harder.
Enforce password history	24 passwords remembered	Prevents reuse of the same password too quickly.
Password must meet complexity requirements	Enabled	Improves encryption and makes guessing harder.
Store passwords using reversible encryption	Disabled	Prevents passwords from being stored in (the equivalent of) clear-text.
Account lockout threshold	5 invalid login attempts	Prevents continual password guessing by disabling an account after the specified number of attempts. Consider disabling account lockout for operator (or other user) accounts where denial of service or loss of view would be detrimental to safety or the continued operation of the facility.
Account lockout duration	15 minutes	Specifies the period of time during which a user will not be able to log on following an account lockout. (Note that the administrator can re-enable the account before the expiration of the specified lockout period.)
Reset account lockout counter after	14 minutes	The time before the account lockout is reset to zero. For example, with the account lockout set at 10, and the lockout counter set at 29 minutes, lockout will occur if there are 10 invalid logon attempts within 29 minutes. Note that the lockout counter must be less than the lockout duration.

Strong Passwords

It is recommended that you enforce strong passwords, that is, passwords consisting of at least 12-14 characters including one numeric. If you enforce password complexity, a strong password must contain at least three of the following four character groups:

- English uppercase characters (A-Z)
- English lowercase characters (a-z)
- Numbers (0-9)
- Special characters (such as !, $, #, &)

Weak passwords that are easy to guess provide an opportunity for unauthorized access. Minimum password complexity can be enforced by Group Policy or local password policy. Microsoft provides tools that can check your passwords to determine if they are easily guessable. If possible, such tools should be used.

An alternative way of increasing password complexity is to recommend the use of a pass phrase, for example, “the cow can eat the mountain” rather than a password. The extra characters dramatically increase the difficulty for a hacker attempting to crack the password. It is also much easier to remember than a random collection of letters, numbers, and other characters.

Note: *While pass phrases can be more difficult to guess, common phrases should not be used.*

Account Lockout

The lockout values shown in the Password Policies and Settings, beginning on page 47, are those suggested by Microsoft and are discussed in their white paper “Account Lockout Best Practices” available here: http://www.microsoft.com/downloads/details.aspx?FamilyID=8c8e0d90-a13b-4977-a4fc-3e2b67e3748e

Account lockout policy must be used with caution. Although it will slow down an attempted password guessing attack, it will not prevent a determined attacker from capturing login packets and using cryptographic tools to break the password offline. It may also lead to a Denial of Service, where authorized users find themselves unable to log on. It is generally better to rely on strong authentication (strong passwords) and system audit log monitoring to prevent and detect password cracking attempts.

System Services

System services are background processes started by the system at boot time to provide functionality independently of any logged on user. While Enterprise Provisioner and Staging Hub Server itself runs a set of these services, many of the system default services are not needed by Enterprise Provisioner and Staging Hub Server. They do, however, provide avenues for malicious network attack and should be disabled. This can be performed using the Windows Services utility found under **Control Panel >Administrative Tools>Services** on each computer.

Required Windows Services

The following table lists required services on Windows computers running Enterprise Provisioner and Staging Hub Server software. Depending on your Enterprise Provisioner and Staging Hub Server license options, all other Windows services should be disabled.

Display Name/Core System	Service	Required (Y/N)	Dependent On
Event Log	eventlog	Y	

Services Required by Antivirus Programs

The following table lists services that may run on server or workstation computers for each respective antivirus protection program.

Display Name/Core System	Service
McAfee Engine Service	EngineServer
McAfee Framework Service	McAfeeFramework
McAfee McShield	McShield
McAfee Task Manager	McTaskManager
McAfee Validation Trust Protection Service	mfevtps
Norton AntiVirus Server	Norton AntiVirus Server

File System and Registry Protection

Windows protects objects, including files, directories and registry keys, with ACLs. In the case of a file, actions include open, read, write, and modify permissions.

When applied to a directory, the default permissions are inherited by all subordinate files and directories. The inheritance can be broken if required.

ACLs are discretionary and need not exist for an object, but once they do exist, all access to the object will be subject to the access control specified. New directories, files, or registry keys will inherit ACLs from their parent computer. If the inheritance is broken, or a new directory is created under the root, there will be no ACLs and hence no protection. It is then up to the site to apply appropriate protection.

When installed, Windows applies default ACLs to its system directories and registry trees to prevent malicious or accidental damage. Similarly, the Enterprise Provisioner and Staging Hub Server installation will not apply ACLs to its directories and registry tree. Honeywell recommends that access controls are applied after installation.

ACL protection can only be applied to files and directories if the containing file system is in NTFS format. Enterprise Provisioner and Staging Hub Server application binaries can only be installed on a disk partition with NTFS and so ACLs should be applied as described.

NTFS also supports the ability to encrypt files. Runtime data and executables are not suitable for encryption for performance reasons, but static files like Enterprise Provisioner and Staging Hub Server database backups may be encrypted if the additional level of protection is required. Note however that file encryption requires additional administrative work in the form of key management.

Note: *Enterprise Provisioner and Staging Hub Server directories can be configured on non-NTFS volumes. Honeywell strongly recommends against using such file system. The lack of ACL protection for these volume types (like FAT32) versus alternative available security for the file system should be considered when choosing database and backup storage volumes.*

Managing File System ACLs

As installed, the file system ACLs provide good security. Access to the Enterprise Provisioner and Staging Hub Server application directories is set up as follows:

Administrators are given full access to server install directories. The Users group is given read-only access to server install directories.

Note: *A site may wish to tighten these permissions by applying more specific ACLs to files and directories, but should do so under Honeywell's guidance. Incorrect permissions may prevent Enterprise Provisioner and Staging Hub Server from operating correctly.*

In Windows Explorer, select the file or directory.

1. Right-click and select **Properties>Security**. This will show a list of users and groups for which access is specified.

Selecting a specific user will show the access permissions. You can change these if necessary.

Managing Registry ACLs

Note: *Incorrect changes to the registry may create problems or cause severe damage to your system. Changes made to the Windows registry happen immediately, and no backup is automatically made. Before making changes to the registry, you should back up any valued data on your computer.*

1. Choose **Start>Run** to open the Run window
2. Type **regedit** and click **OK**
3. Select the registry key that you want to protect
4. Choose **Edit>Permissions**. A dialog box like that provided by Windows Explorer will appear.

Managing File Shares

The use of file shares in the Enterprise Provisioner and Staging Hub Server Network is not recommended, though in some circumstances they may be necessary. Any file shares should be protected. By default, any directory which is made available for network access will give “read access” to the “Everyone” group, that is, anyone on the network can read any file under the shared directory tree. This is generally too permissive and should be changed. Only required accounts should be configured for share access, and “read only” permission should be applied where possible.

Where file share connections need to cross insecure networks, such as into the DMZ, consider enforcing the digital signing of SMB packets. This will prevent packet spoofing or session hijacking, at the expense of up to 15% CPU overhead. This option may be set either through the computer’s Group Policy (if the computer belongs to a Windows domain) or through the local registry. Note: this setting must be used on all computers using that file share

Note: *Enterprise Provisioner and Staging Hub Server does not require any file shares for operation.*

SNMP Configuration

The Simple Network Management Protocol (SNMP) is a protocol used to manage devices on IP networks. It may be used by, for example, servers, switches, routers, storage devices, UPS devices, network printers, cameras and/or streamers on the network. Much information pertaining to system configuration and network activity can be polled or reported via SNMP and enabling its use should be carefully considered.

In SNMP version 1 and SNMP version 2, authentication is performed through supply of a “community string” and encryption of SNMP traffic is not implemented. Accordingly, SNMP versions 1 and 2 are vulnerable to packet sniffing, where an attacker reviews the contents of information being transferred over the network in order to find authentication information that can be used in impersonation attacks.

SNMP version 3 introduced the use of user names and passwords, as well as support for encryption, among other security enhancements. Accordingly, if SNMP is enabled in your Enterprise Provisioner and Staging Hub Server network, Honeywell recommends that SNMP version 3 should be used to provide greater security with confidentiality, integrity and authentication. Even with the additional protections of SNMP version 3, public Community Strings should always be removed and replaced with read-only private Community Strings. In addition, enable version 3 encryption whenever possible.

Remote Access Configuration

If Enterprise Provisioner or Staging Hub Server must be accessed remotely, then the use of a VPN and Microsoft Remote Desktop should be used as described Remote Access, beginning on page 33.

CHAPTER

11 WINDOWS SECURITY FEATURES

Certain Windows security features have an impact on Enterprise Provisioner and Staging Hub Server. This section lists security features that impact Enterprise Provisioner and Staging Hub Server and Honeywell recommends the use of these features.

Hardening the Operating System to Local Threats

Windows has many registry settings, policy settings and configuration options that can be used to increase the overall security of a system, especially where threats present themselves as users of the system.

Note that extreme caution needs to be exercised when making any changes to the registry.

The following sections lists the main settings and recommendations. For further information see Microsoft's Windows Server 2012 Security Guide (available as part of the Microsoft Security Compliance Manager 3.0 (SCM 3.0) tool).

Securing the Desktop

The following recommendations apply to desktop policy settings:

- Configure Windows to display a warning against unauthorized use of the computer.
    - You can configure computers to display a message when someone logs on. A typical message would be: *Only authorized users may use this system*
    - Historically, legal prosecutions of intruders have failed because no such warning was displayed. The banner can be defined using Group Policy or the local registry
- Use Group Policy (if the computer is part of a Windows domain) or the local registry to:
    - Hide the last user's name on the login window. By default, the login dialog box displays the name of the last user to log on. This saves time if the same user is logging on again, and provides a quick indication if an unauthorized login has been attempted, but provides useful information to a would-be attacker: they only must guess the password

- Disable any setting which allows anyone with access to the system console (whether logged on or not) or a Terminal Services session to shut down the system without trace
- Disable the “Shutdown: Allow system to be shut down without having to log on” group policy setting, which could allow attackers to shut down a server from the login screen without requiring any system credentials
- If the system console is not locked away with the server, then you should disable *automatic Administrator logon for the Recovery Console* option, which is used to troubleshoot a booting problem. Without this change, it would be possible for anyone with physical access to reboot the system and obtain Administrator access
- Configure a password-protected desktop screen saver with a short time-out (10 minutes) so that unattended logged-on sessions cannot be hijacked

Restricting Anonymous Logon

By default, anonymous NetBIOS connections can be made to servers and used to obtain information about domain accounts, computer names, file shares, and so on. Although it does not directly allow the computer to be compromised, it provides valuable information which can be used for other attacks.

See the registry key *HKLM\system\CurrentControlSet\control\lsa* for details on disabling anonymous logon.

Disabling Unused Subsystems

Windows provides support for running executables intended for Windows, POSIX (UNIX) and OS/2 environments. The POSIX and OS/2 support is not required and should be disabled as they offer an increased attack surface to malicious users.

These subsystems can be disabled with local registry settings. For more information, see the Microsoft Knowledge Base article 320869, *How to Prevent Windows from Loading the Optional OS/2 and POSIX Subsystems*.

Using NTLM Version 2

The NTLM protocol, which is used for authentication in Windows domains, provides encryption for credential exchange. For maximum security, configure the server to accept and transmit NTLM Version 2 only.

Hardening the TCP/IP Stack

Windows supports several options to help TCP/IP defend itself from well-known network attacks. Although it is recommended that these options be set for maximum protection, care must be taken to allow for the characteristics of individual LANs. Details can be found at https://support.microsoft.com (note: this does not apply to Windows Server 2012).

As of Windows Server 2008, the TCP/IP stack has been redesigned. For more information about changes to the TCP/IP stack, see https://support.microsoft.com

Disabling the Use of Removable Storage

USB ports and other removable storage devices on a computer provide an entry point for viruses and malicious software to be loaded on to the system. They also provide a means for attackers to copy sensitive data from the system.

Removable storage devices can be disabled using local registry settings. For more information, see https://support.microsoft.com/en-us/help/823732

Alternately, removable storage devices can be disabled with policies on Windows Vista or later. The following policies manage read and write permissions for removable storage devices:

1. **Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access**
2. **User Configuration > Policies > Administrative Templates > System > Removable Storage Access**

The following policy restricts installations of removable storage devices:

- **Computer Configuration > Policies > Administrative Templates > System > Device Installation > Device Installation Restrictions**

Disabling Auto Run Functionality

Autorun functionality in Microsoft Windows allows for an automatic software response to hardware actions taken on a computer. Typically, Autorun commands are used on removable media and can automatically launch applications of install programs when the removable media is inserted into a computer.

On operating systems earlier than Windows Vista, the default behavior is to execute Autorun commands without requiring any user intervention After Windows Vista, the system will prompt the user to accept the execution of an Autorun command.

Since Autorun can allow code to be executed without proper consent, Honeywell recommends that Autorun is disabled for all drives. This will reduce the risk of suspicious files being launched automatically and/or without user interaction.

For more information, and for instructions on disabling Autorun, see: http://support.microsoft.com

Removing Access to Task Manager and Windows Explorer

You can prevent operators from accessing applications through Task Manager and Windows Explorer by removing access to Task Manager and Windows Explorer. Note: disabling access to Windows Explorer is recommended only if operators do not require it for Enterprise Provisioner and Staging Hub Server activities.

To remove access to Task Manager and Windows Explorer

1. In Windows Explorer, right-click the file windows\system32\taskmgr.exe
2. Select **Properties → Security**
3. Click **Add**
4. Select the user you want to modify, click **Add** and **OK**
5. Select the user you added, click **Deny** for full control
6. Click **OK**
7. Select **Yes** in response to the 'Do you wish to continue?' prompt
8. Repeat steps 1 through 7 of this task for the file \%windir%\explorer.exe

Preventing Operators From Shutting Down the Server Computer

Operators can shut down a computer in several ways. E.g. from the Start Menu by pressing **Ctrl+Alt+Del** at the logon screen.

To prevent operators from shutting down the computer, you need to change the local policies and edit the registry.

To change the local policies to prevent shut down

1. Select **Start Settings > Control Panel > System and Maintenance > Administrative Tools > Local Security Policy**
2. Select **Local Policies > User Rights Assignment**
3. Double-click **Shutdown the system**
    a. The Local Security Policy Setting dialog box opens
    b. Deselect Local Policy Setting for the group or operator that you are modifying and click **OK**. Close Local Security Settings

To edit the registry to prevent operator shut down

1. Select **Start All programs > Accessories > Run**, type **regedit** and click **OK**.
    a. The Registry editor opens
2. Locate the key:
    a. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\ShutdownWithoutLogon
    b. Set value to **0**
    c. Exit the Registry editor

CHAPTER

12 SECURITY FEATURES

This chapter describes security features of the software provided by Honeywell.

User Roles

The users in a Enterprise Provisioner and Staging Hub Server system generally fall into one of the following user roles:

- System Administrator/Installer
- Enterprise Provisioner and Staging Hub Server Administrator
- Enterprise Provisioner and Staging Hub Server Device Managers

The user account and access requirements of each role are described below.

Administrators/Installers

Tasks include system installation and initial configuration, creating backups, undertaking performance monitoring and diagnostic investigation tasks for the Enterprise Provisioner and Staging Hub Server system, and managing Windows accounts and permission settings.

Best practice requires that administrators have two Windows user accounts, and that they only use the account belonging to the Windows Administrators group when necessary. This reduces the risk of accidental damage, and of leaving a highly-privileged account logged on and liable to hijacking.

Where possible, the built-in Administrators account should not be used directly if the site has several administrators, since actions will not be attributable to any individual.

Enterprise Provisioner and Staging Hub Server Administrator

Tasks for this Enterprise Provisioner and Staging Hub Server user role include operational configuration of devices, adding devices, managing groups and content thereof and Device Manager account management. Server Administrators who also use Enterprise Provisioner and Staging Hub Server device activities should have two user accounts – one with Server Administration role and one with Device Manager role. They should only log in to Enterprise Provisioner and Staging Hub Server as System Manger to perform configuration and user account management tasks.

Enterprise Provisioner and Staging Hub Server Device Managers

This role should have a separate windows account from the Server or System Administrator to prevent privilege escalation when using the Device Manager role. This role should only be granted to those corporate users that need to enable Staging Hub Server to update devices that are being managed.

Security Settings for Staging Hub Server

The following security settings within Staging Hub Server should be assured. Many are set automatically upon installation, but since they can be changed, they should be checked. Microsoft Baseline security tool will not capture all of these recommended settings.

- Recommended value for the inactivity timeout is 30 minutes
- Honeywell recommends that the Honeywell Android Network and Security Guide be used for security settings in Android devices that are being managed by Staging Hub Server
- Recommend security for Microsoft SQL Server: https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/sql-server-security

Honeywell recommends that any Windows SafeDllSearchMode is enable to restrict loading DLLs used by Enterprise Provisioner or Staging Hub Server to the system path before the local directory to prevent DLL malware being loaded. In addition, as noted in other sections, only the Staging Hub user account or system administrator should have read/write access to the current directory.

Barcodes should be encrypted by a passphrase used post initial provisioning, enforced where possible on the device (this applies to new versions on Mobility Edge), and AES should be used as the encryption technology if the device supports (this applies to new versions on Mobility Edge).

Note: *The passphrase must be changed from the default.*

Honeywell recommends the use of **HTTPS** server with an inactivity timeout of 30 minutes in Enterprise Provisioner, for secure communication over a computer network. This can protect against man-in-the-middle attacks.

The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication. In practice, this provides a reasonable assurance that one is communicating without interference by attackers with the website that one intended to communicate with, as opposed to an impostor.

CHAPTER

13 SECURE WIRELESS DEVICES

Security for Wireless LAN Networks

Most devices that connect to Enterprise Provisioner and Staging Hub Server will use a WiFi wireless network. For initial provisioning, Enterprise Provisioner will create a barcode (or barcodes) that specify the proper WiFi settings as described below. Staging Hub Server will use Enterprise Provisioner to create such barcodes. The recommended settings are in the following sections.

WLAN and AP Security

When a device connects through a wireless access point to an organization's server on a wired network, specific security precautions are required to mitigate the significant security risk the Wireless Local Area Network (WLAN) wireless Access Point (AP) connection represents for the servers and devices on the wired network. Therefore, you should consider the following steps to secure and protect the data transmissions. Refer to manufacturer documentation as needed.

Wireless devices not used with Enterprise Provisioner or Staging Hub Server 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.

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 using one of TLS, PEAP, TTLS, or FAST. If possible, the RADIUS server should use a directory service (such as LDAP or Active Directory) for user names and passwords
- Configure the RADIUS server address

- Configure for WPA2 Enterprise
- Change the WAP RADIUS password. Do not use the default password
- Configure 802.1x authentication
- Enable MAC filtering and enter the MAC addresses for all the wireless devices. This helps prevent unauthorized devices from connecting to the wireless network

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

Secure Device Configuration

Honeywell recommends the following when configuring mobile devices for WLANs:

- Configure the proper SSID
- Configure 802.1x authentication
- Configure Protected EAP authentication using one of TLS, PEAP, TTLS, or FAST
- If possible, configure the 802.1x supplicant (client) to prompt for the any password needed by the EAP method

If EAP-TLS or EAP-PEAP-TLS are in use, a client certificate must be available on the device.

CHAPTER

14 NETWORK PORTS SUMMARY

Network Port Table

- "Internal use" means that a firewall rule allowing traffic on the port is only required for communication between multiple Enterprise Provisioner and Staging Hub Servers. Access should be restricted by IP address to those servers. If there is only a single server, no firewall exceptions are needed for these.
- Ports for which "client access" is indicated should be restricted by IP address to known workstations that are expected to require access to the application.
- Ports for which "MCC access" is indicated should be restricted to be accessible to/from the MCC/OCC machine.
- Ports for which "external provider" is indicated should be restricted by IP address to the specific external data provider(s) (WMS, weather, etc.) that are expected to be accessed by the application for the specified data type.

Port Used	Connection Type	Task	Comments
8998 or 80	HTTP	Web page server for main application	Web page port (client access)
9000	HTTP	API Gateway	API port (client access)
8080	TCP	Map Server (GeoServer)	GeoServer port (client access)
9018	TCP	UI Notification (SSN)	UI Notification port (client access)
5601	HTTP	Web page server for error logs	Kibana (internal use; client access is optional)
4369, 5671, 5672 and 25672	TCP	Inter-service messaging	Rabbit MQ ports (internal use)
5432	TCP	Database	PostGreSQL database (internal use)
9200	HTTP	Database	Elasticsearch HTTP (internal use)
9300	TCP	Error logging	Logstash port (internal use)
27017	TCP	Database	MongoDB (internal use)
3306	TCP	Database	MySQL (internal use)

Port Used	Connection Type	Task	Comments
8080	HTTP	Eureka, Enterprise Provisioner and Staging Hub Server Config. Manager (hosted under Tomcat)	Tomcat port (internal use)
9001 – 9017 and 9019 - 9033	TCP	Web services	Enterprise Provisioner and Staging Hub Server micro-services (internal use) (additional ports may be used if multiple instances of any service are run)
21 (inbound)	FTP	Beacon alert message reception	FTP Server (FTP Traffic-In) (MCC access) (required only if beacon alert feed is via FTP)
1024 - 65535	FTP	Beacon alert message reception	FTP Server Passive (FTP Passive Traffic-In) (MCC access) (required only if beacon alert feed is via passive FTP)
20 (outbound)	FTP	Beacon alert message reception	FTP Server (FTP Traffic-Out) (MCC access) (required only if beacon alert feed is via FTP)
123	UDP	NTP	Time synchronization (external provider)
80	HTTP	External weather data service APIs	Weather Underground (http://api.wunderground.com)
80	HTTP	External weather data service APIs	PlanetOS (http://api.planetos.com)
80 (provider-specific)	HTTP	External WMS	Example: http://ows.terrestris.de/osm/service?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetCapabilities

Firewall Configuration

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 then open only the ports you need (see above). So, 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 then you would need to open port 53 for “outgoing” traffic. If you want to access your internet mail server through POP3, then you would open port 110 for outgoing traffic. Firewalls are directional, that is, they pay attention to where the traffic originates, that is, whether it is “incoming/inbound” and “outgoing/outbound”.

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 be able 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.

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".
BIOS	Basic Input/Output System
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.
DOS	Denial Of Service
DNS	Domain Name Server
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.
MBSA	Microsoft Baseline Security Analyzer
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.
NIDS	Network Intrusion Detection System
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.
SID	Security Identifier
SNMP	Simple Network Management Protocol (SNMP) is a protocol used to manage devices on IP networks.
SRT	Security Response Team
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
VPN	Virtual Private Network

WAN	Wide Area Network
WAP	Wireless Access Point
WLAN	Wireless Local Area Network
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

EPSH-W-EN-SG Rev B
02/19