Topic: Network and Security Planning Guide
Date: June 2009
Version: 3.0
Applicable Products: EBI R410
Notice

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2009 – Honeywell International Sàrl.

Honeywell trademarks

Honeywell Enterprise Buildings Integrator™ is a trademark of Honeywell, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

VMware is a registered trademark of VMware Inc.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Support and Other Contacts

For technical assistance or further information, call your nearest Honeywell office.

Training Classes

Honeywell holds technical training classes on Enterprise Buildings Integrator. These classes are taught by experts in the field of building control systems. For more information about these classes, contact your Honeywell representative.

Related documentation

For a complete list of publications and documents for EBI, see the EBI Overview.
ENSURE FREQUENT UPDATES TO ANTIVIRUS SIGNATURE FILES ................................................................. 52
TEST THE DEPLOYMENT OF ANTIVIRUS SIGNATURE FILES ......................................................................... 53
PROHIBIT EMAIL CLIENTS ON THE BUILDING CONTROL NETWORK .............................................................. 54
Viruses and email .............................................................................................................................................. 54
Instant messaging ............................................................................................................................................. 54
Spyware .............................................................................................................................................................. 54

NETWORK PLANNING AND SECURITY ........................................................................................................... 55

HIGH SECURITY NETWORK ARCHITECTURE ................................................................................................... 56
Supported topologies ......................................................................................................................................... 56
About Level 1 .................................................................................................................................................... 57
About Level 2 .................................................................................................................................................... 58
About Level 3 .................................................................................................................................................... 58
ABOUT DEMILITARIZED ZONES ...................................................................................................................... 58

CONNECTING TO THE BUSINESS NETWORK .............................................................................................. 59
THE DEMILITARIZED ZONE ............................................................................................................................ 60
CONFIGURING THE DMZ FIREWALL .............................................................................................................. 61
Distributed System Architecture ..................................................................................................................... 61
File shares .......................................................................................................................................................... 63
Remote access for Station and Quick Builder ................................................................................................. 65
Remote Access for HMIWeb Browser ............................................................................................................ 66
Mobile access for Honeywell EasyMobile .................................................................................................... 68
Remote Access for Enterprise Applications .................................................................................................. 69
Microsoft Windows Server Update Services .................................................................................................. 69
Honeywell Software Update Service ............................................................................................................... 70
Antivirus Update Server .................................................................................................................................. 71
Connecting other nodes to the Building Control Network ........................................................................... 73

SECURING NETWORK EQUIPMENT ............................................................................................................... 74
SECURING CONTROLLER NETWORK INTERFACES ....................................................................................... 75
NETWORK ENCRYPTION ................................................................................................................................. 76

NETWORK PLANNING ........................................................................................................................................ 78
Bandwidth requirements between Level 1 and Level 2 nodes ..................................................................... 78
Bandwidth requirements between Level 2 nodes ......................................................................................... 78
Bandwidth and latency requirements between HMIWeb browser and the EBI server ................................. 79

DOMAIN NAME SERVERS ............................................................................................................................... 81
REMOTE ACCESS ............................................................................................................................................. 82

COMPUTER NAMES ....................................................................................................................................... 83

REGISTERING EBI SERVERS ............................................................................................................................ 84
DUAL-HOMED COMPUTERS ........................................................................................................................... 85
PORT SCANNING ............................................................................................................................................ 86
THIRD-PARTY APPLICATIONS ........................................................................................................................ 87
REMOTE MONITORING APPLICATIONS ......................................................................................................... 88
MANAGED ETHERNET SWITCHES ................................................................................................................... 89

VIRTUAL ENVIRONMENTS ............................................................................................................................... 90
VIRTUAL ENVIRONMENT ARCHITECTURE ...................................................................................................... 91
DETERMINING THE REQUIREMENTS OF THE EBI SYSTEM ........................................................................ 92

SECURING WIRELESS DEVICES .................................................................................................................... 94
ABOUT EBI WIRELESS DEVICES .................................................................................................................. 95
RADIO FREQUENCY SURVEY .......................................................................................................................... 96
CONFIGURING AND SECURING WAPs .......................................................................................................... 97
CONNECTING WIRELESS DEVICES ............................................................................................................. 98
The domain controller and IAS ..................................................................................................................... 98
Firewalls ......................................................................................................................................................... 98
Configuring WAPs ......................................................................................................................................... 98
Wireless network interface cards ................................................................................................................ 99
Introduction
Intended Audience for this Document

This guide has been designed expressly for use by Information Technology (IT) personnel who are employed by customers who have a Honeywell Enterprise Buildings Integrator (EBI) software solution. EBI manages various building functions such as Heating Ventilation Air Conditioning (HVAC), Security, Surveillance, Life Safety (such as fire alarm systems) and Energy Management.

The EBI software utilizes commercial off the shelf computing and network hardware using standard Microsoft Networking and Operating Systems. The exception to this is when the system is required to meet Underwriters Laboratories (UL) listing requirements, primarily for but not limited to Life Safety systems involving fire alarm detection and notification systems. Under some conditions a high security system will also be required to meet UL listing requirements if a certificate is required for the security system. In applications where the system is going to require UL listing: Computing hardware, network hardware and other components will be required to have UL listing for the purpose of the application, which will preclude the use of off the shelf computing hardware and networking components. In UL applications it will be required that the computing hardware and network components be supplied by Honeywell. Contact your Honeywell Representative for more information. Except where noted the balance of this guide pertains to both UL and Non – UL installed systems.

<table>
<thead>
<tr>
<th>For information about</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Detail and Architectural Description</td>
<td>Page 9</td>
</tr>
<tr>
<td>System Architecture</td>
<td>Page 10</td>
</tr>
<tr>
<td>Assumptions and prerequisite skills</td>
<td>page 11</td>
</tr>
<tr>
<td>Using this guide</td>
<td>page 12</td>
</tr>
<tr>
<td>Related documents</td>
<td>page 13</td>
</tr>
</tbody>
</table>
Product Detail and Architectural Description

Honeywell EBI is a suite of applications that provide a complete solution for the information access and control needs of one or more buildings. EBI is targeted at key building functions. These requirements can be met by separate EBI systems or by a single, integrated EBI system. An EBI system can be comprised of one or more of the following applications in single server or network architecture of servers known as Distributed System Architecture (DSA):

- **Honeywell Building Manager** provides HVAC control. In addition to the traditional interfaces with Honeywell Excel 5000 controllers HBM also includes an interface to Honeywell R7044 controllers such as Excel Plus and HPEP. Open Systems include a direct LonWorks interface, OPC, Modbus, and BACnet capabilities. There is also support for numerous Programmable Logic Controllers (PLC) such as the Honeywell HC900 and Allen Bradley PLC control solutions.

- **Honeywell Security Manager** provides interfaces to Security Panels, Access Controllers and CCTV switchers. Advanced security features and options like Alarm Management, Deadman Timer and Guard Tour are available to provide a comprehensive security solution.

- **Honeywell Life Safety Manager** allows for monitoring and control for Fire Alarm Systems and Smoke Control. This system provides interfaces to Honeywell’s Excel Life Safety (XLS series) family of products as well as the Honeywell FS90 Plus Fire Panel. EBI has UL864 Listing for Ethernet based life safety control and monitoring. The UL Compliance option within Life Safety Manager is also used for High Security Applications where UL Security Listings are required.

- **Honeywell Energy Manager** is aimed at optimizing energy usage in your facility. The Energy Manager system monitors your energy meters, validates data, provides information for forecasting and load prediction and ultimately enables you to optimize the use of equipment to reduce energy costs.

- **Honeywell Digital Video Manager** is aimed at providing management of a digital video surveillance system consisting of a large number of cameras on a network that provides control, recording, viewing and playback through an EBI workstation or on a standalone Internet Explorer browser.
System Architecture

EBI is based on “client/server” architecture. The EBI Server runs on Windows XP or 2003 Server software. The EBI Station (client) runs on Windows XP, Windows Vista, and 2003 software.

The EBI server PC connects to a variety of controllers, which then connect to field devices such as HVAC sensors, and actuators, smoke sensors, card readers and cameras. The EBI software communicates to the controllers, providing system wide monitoring and control. These controllers can be HVAC controllers, programmable logic controllers (PLCs), access controllers, security controllers, fire panels and CCTV switchers.

Operators view and interact with the EBI server using an operator station client or a browser client. The proprietary client software is called “Station”. This software typically runs on one or more separate PCs, which are connected to the EBI server through a network connection. Station may also run on the same PC as the EBI software. The second option is to use an Internet Explorer browser to connect to the EBI Web Server. The EBI Web Server enables casual users to access specific EBI Server displays via an intranet.

Figure 1 gives an indication of the breadth of system architecture possibilities of EBI and subsystems–please refer to the specific device architectures in each section above for more detail. Please note that this diagram generalizes the network architecture, which will be described in detail in later sections.

For more information regarding EBI product specifications and hardware requirements please refer to the Honeywell Enterprise Buildings Integrator R410 Specification Data Brochure. This can be requested from your Honeywell Representative.
Assumptions and prerequisites

This guide is primarily intended for IT personnel who are responsible for planning the configuration and maintenance of the network infrastructure that the EBI system exists within. It therefore assumes a high degree of technical knowledge and familiarity with:

- Microsoft Windows operating systems
- Networking systems and concepts
- Security issues and concepts

Attention: As you develop a security program for your building management system you should be aware that detailed information, if not protected, can fall into the hands of organizations that could cause harm to your control system or process operations.

Important terminology

The following Microsoft terms are important when understanding security concepts and configuration. Definitions can be found on the Microsoft web site. See:

http://www.microsoft.com/resources/glossary/default.mspx

- Access control list (ACL)
- Access mask
- Access token
- Global group
- Group
- Group memberships
- Group Policy
- Group Policy object (GPO)
- Local group
- Organizational units (OU)
- Permission
- Privilege
- Universal group
- User account
- User rights
How to use this guide

If you have specific security concerns such as protecting your EBI against viruses or preventing unauthorized access, you might like to start by consulting the checklists in the topic “Security checklists” on page 14.

Alternatively, you can choose from the following list of topics.

<table>
<thead>
<tr>
<th>For information about</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing a security program</td>
<td>“Developing a security program” on page 21</td>
</tr>
<tr>
<td>A strategy for backups and recovery</td>
<td>“Disaster recovery” on page 31</td>
</tr>
<tr>
<td>The physical security of your system</td>
<td>“Physical and environmental considerations” on page 37</td>
</tr>
<tr>
<td>Measures for keeping security-related software up to date</td>
<td>“Microsoft security updates and service packs” on page 43</td>
</tr>
<tr>
<td>Antivirus measures</td>
<td>“Virus protection” on page 47</td>
</tr>
<tr>
<td>Network port access and connections through firewalls</td>
<td>“Network security” on page 55</td>
</tr>
<tr>
<td>Securing wireless devices</td>
<td>“Securing wireless devices” on page 90</td>
</tr>
<tr>
<td>Monitoring and auditing the security of your system</td>
<td>“System monitoring” on page 100</td>
</tr>
<tr>
<td>Working with Windows domains</td>
<td>“Windows domains” on page 107</td>
</tr>
<tr>
<td>Securing your operating system</td>
<td>“Securing access to the Windows operating system” on page 113</td>
</tr>
<tr>
<td>Security issues specific to EBI</td>
<td>“EBI security features” on page 132</td>
</tr>
</tbody>
</table>
## Related documents

The following documents complement this guide.

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBI Specification Data Sheet</td>
<td>Honeywell Enterprise Buildings Integrator R410 Specification Data Brochure. File name for this guide is EBI_R410_SpecTech_v1.PDF which is the current offering and can be requested from your Honeywell Representative.</td>
</tr>
<tr>
<td>EBI Overview And Planning</td>
<td>Provides a comprehensive overview of EBI, including basic concepts and terminology.</td>
</tr>
<tr>
<td>Installation Guide</td>
<td>Provides detailed instructions for installing EBI systems.</td>
</tr>
<tr>
<td>Configuration and Administration Guide</td>
<td>Provides information necessary for engineers and system administrators to configure and support a complete EBI system.</td>
</tr>
<tr>
<td>Software Release Bulletin (SRB)</td>
<td>Contains last-minute information that was not able to be included in the standard documents. It may include important details related to networking and security.</td>
</tr>
<tr>
<td>Compatibility Matrix</td>
<td>Provides a compatibility list of supported interfaces and options including hardware compatibility, software compatibility, operating systems and point servers.</td>
</tr>
<tr>
<td>Known Issues Bulletin</td>
<td>This document lists and summarizes issues that you may encounter in configuring or using this release of EBI.</td>
</tr>
<tr>
<td>Microsoft Hot Fix List</td>
<td>Provides the latest information regarding Microsoft Security Hot Fixes as they pertain to EBI. This is issued monthly.</td>
</tr>
</tbody>
</table>

The EBI Compatibility Matrix is available at the following location:

1. Go to Honeywell’s Service Online web site: https://www.honeywellserviceonline.com
2. Go to System Support and click on Knowledge Centre. Select Product Type as EBI and Category as Compatibility Matrix, and then click on Browse Documents. Look for Compatibility Matrix

The EBI Known Issues Bulletin is available at the following location:

1. Go to Honeywell’s Service Online web site: https://www.honeywellserviceonline.com
2. Go to System Support and click on Knowledge Centre. Select Product Type as EBI and Category as Known Issues Bulletin, and then click on Browse Documents. Look for Known Issues Bulletin

Note: A subscription to Honeywell Service Online (HSO) is required to view these documents. The Honeywell Service Online web site is not available to all regions of the world. Contact your Honeywell representative for further information.
Security checklists

This chapter provides a number of checklists to help you think about security issues that should be considered for your site.

The checklists cover some of the main threats that may exist on a Building Control Network and the steps that can be used to mitigate them. They also provide an alternative way of navigating through this document, depending on your key concerns.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infection by viruses and other malicious software</td>
<td>page 15</td>
</tr>
<tr>
<td>Unauthorized external access</td>
<td>page 16</td>
</tr>
<tr>
<td>Unauthorized internal access</td>
<td>page 17</td>
</tr>
<tr>
<td>Accidental system change</td>
<td>page 18</td>
</tr>
<tr>
<td>Protecting your EBI system components</td>
<td>page 19</td>
</tr>
</tbody>
</table>
Infection by viruses and other malicious software agents

This threat encompasses malicious software agents such as viruses, spyware (trojans), and worms. The intrusion of malicious software agents can result in:

- Performance degradation
- Loss of system availability
- The capture, modification, or deletion of data.

Mitigation Steps

<table>
<thead>
<tr>
<th>Mitigation steps</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that your virus protection and Microsoft Security Hot Fixes are up to date on all nodes in your Building Control Network and the systems connected to it.</td>
<td>“Microsoft Security updates and service packs” on page 43 and “Virus protection” on page 47</td>
</tr>
<tr>
<td>Ensure that there are no email clients on any nodes of your Building Control Network.</td>
<td>“Prohibit email clients on the building management network” on page 54</td>
</tr>
<tr>
<td>Use a firewall and DMZ for the business network to Building Control Network interface.</td>
<td>“Connecting to the business network” on page 59</td>
</tr>
</tbody>
</table>

Note: Use of spyware removal applications may cause unexpected results to your Building Control Network nodes. These applications may alter registry settings that are crucial to the operation of the software on these nodes.
Unauthorized external access

This threat includes intrusion into the building management system from the business network and possibly an intranet or the Internet.

Unauthorized external access can result in:

- Loss of system availability
- Incorrect execution of controls causing damage to the building,
- Theft or damage of its contents
- The capture, modification, or deletion of data
- Loss of prestige if the external access becomes public knowledge

<table>
<thead>
<tr>
<th>Mitigation steps</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a firewall/DMZ for the business network to Building Control Network interface to restrict access from the business network to Building Control Network.</td>
<td>“Connecting to the business network” on page 59</td>
</tr>
<tr>
<td>Set the minimum level of privilege for all accounts, and enforce a strong password policy.</td>
<td>“Windows user accounts and passwords” on page 114</td>
</tr>
<tr>
<td>Monitor system access.</td>
<td>“System monitoring” on page 100</td>
</tr>
<tr>
<td>Securing wireless devices</td>
<td>“Securing wireless devices” on page 90</td>
</tr>
<tr>
<td>Use the firewall on Windows XP SP2 and Windows Server 2003 SP1 machines</td>
<td>“Windows XP SP2 and Windows Server 2003 SP1 security enhancements” on page 126</td>
</tr>
</tbody>
</table>
Unauthorized internal access

This threat encompasses unauthorized access from systems within the Building Control Network. This threat is the most difficult to counter since attackers may well have legitimate access to part of the system and they simply want to exceed their permitted access.

Unauthorized internal access can result in:

- Loss of system availability
- Incorrect execution of controls causing damage to the building
- Theft or damage of its contents
- The capture, modification, or deletion of data

<table>
<thead>
<tr>
<th>Mitigation steps</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure Station security.</td>
<td>“Station security” on page 138</td>
</tr>
<tr>
<td>Use physical security for Building Control Network systems.</td>
<td>“Physical and environmental considerations” on page 37</td>
</tr>
<tr>
<td>Do not allow the use of unauthorized removable media (for example, CDs, floppy disks, and memory sticks) on any node in (or connected to) your EBI system.</td>
<td>“Protecting against unauthorized system access” on page 17</td>
</tr>
<tr>
<td>Use strong passwords on network equipment.</td>
<td>“Securing network equipment” on page 74</td>
</tr>
<tr>
<td>Monitor system access.</td>
<td>“System monitoring” on page 100</td>
</tr>
<tr>
<td>Prevent the use of unauthorized laptops on the BCN.</td>
<td>“Connecting other nodes to the Building Control Network” on page 73</td>
</tr>
<tr>
<td>Use and enforce a strong password policy.</td>
<td>“Windows user accounts and passwords” on page 114</td>
</tr>
<tr>
<td>Ensure strong access controls are in place on the file system, directory, and file shares.</td>
<td>“File system and registry protection” on page 122</td>
</tr>
<tr>
<td>Securing wireless devices</td>
<td>“Securing wireless devices” on page 90</td>
</tr>
</tbody>
</table>
Accidental system change

This threat encompasses inadvertent changes to executables or configuration files.
Accidental system change can result in:

- Loss of system availability
- Loss of data

<table>
<thead>
<tr>
<th>Mitigation steps</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the minimum level of privilege for all accounts, and enforce a strong password policy.</td>
<td>“Windows user accounts and passwords” on page 114</td>
</tr>
<tr>
<td>Ensure strong access controls are in place on the file system, directory, and file shares.</td>
<td>“File system and registry protection” on page 122</td>
</tr>
</tbody>
</table>
Protecting your EBI system components

The following tables list steps you can take towards securing your EBI:

- Server(s), Stations, and domain controller

- Building Control Network components (including routers, switches, and firewalls)

### EBI server

<table>
<thead>
<tr>
<th>Protection measure</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take steps to implement and enforce physical security.</td>
<td>“Physical and environmental considerations” on page 37</td>
</tr>
<tr>
<td>Set the minimum level of privilege, and enforce a strong password policy for all accounts.</td>
<td>“Windows user accounts and passwords” on page 114</td>
</tr>
<tr>
<td>Ensure that your virus protection and Microsoft Security Hot Fixes are up to date on all systems.</td>
<td>“Microsoft Security updates and service packs” on page 43 and “Virus protection” on page 47</td>
</tr>
</tbody>
</table>

### EBI Station

<table>
<thead>
<tr>
<th>Protection measure</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take steps to implement and enforce physical security.</td>
<td>“Physical and environmental considerations” on page 37</td>
</tr>
<tr>
<td>Set the minimum level of privilege, and enforce a strong password policy for all accounts.</td>
<td>“Windows user accounts and passwords” on page 114</td>
</tr>
<tr>
<td>Ensure that your virus protection and Microsoft Security Hot Fixes are up to date on all systems.</td>
<td>“Microsoft Security updates and service packs” on page 43 and “Virus protection” on page 47</td>
</tr>
<tr>
<td>Ensure Station security.</td>
<td>“Station security” on page 138</td>
</tr>
</tbody>
</table>

### Domain controller

<table>
<thead>
<tr>
<th>Protection measure</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take steps to implement and enforce physical security.</td>
<td>“Physical and environmental considerations” on page 37</td>
</tr>
<tr>
<td>Set the minimum level of privilege, and enforce a strong password policy for all accounts.</td>
<td>“Windows user accounts and passwords” on page 114</td>
</tr>
<tr>
<td>Ensure that your virus protection and Microsoft Security Hot Fixes are up to date on all systems.</td>
<td>“Microsoft Security updates and service packs” on page 43 and “Virus protection” on page 47</td>
</tr>
</tbody>
</table>

### Network components

<table>
<thead>
<tr>
<th>Protection measure</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take steps to implement and enforce physical security.</td>
<td>“Physical and environmental considerations” on page 37</td>
</tr>
</tbody>
</table>
System performance and reliability

To ensure the continued reliability of your system, you should also attend to the following factors that can impact system performance.

<table>
<thead>
<tr>
<th>Protection measures</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not allow port scanning within the BCN.</td>
<td>“Port scanning” on page 86</td>
</tr>
<tr>
<td>Do not automatically schedule full system antivirus scans on EBI nodes.</td>
<td>“Configure active antivirus scanning” on page 50</td>
</tr>
</tbody>
</table>
A security program is a risk-analysis driven, life-cycle approach to securing the Building Control Network. This chapter describes the key components of a security program.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forming a security team</td>
<td>page 22</td>
</tr>
<tr>
<td>Identifying assets that need to be secured</td>
<td>page 23</td>
</tr>
<tr>
<td>Identifying and evaluating threats</td>
<td>page 24</td>
</tr>
<tr>
<td>Identifying and evaluating vulnerabilities</td>
<td>page 25</td>
</tr>
<tr>
<td>Implementing change management</td>
<td>page 28</td>
</tr>
<tr>
<td>Creating and implementing a mitigation plan</td>
<td>page 27</td>
</tr>
<tr>
<td>Planning ongoing maintenance</td>
<td>page 29</td>
</tr>
</tbody>
</table>
Forming a security team

In forming a 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 cross-functional security core team consisting of representatives from:
  - Building management (those responsible for running and maintaining the building HVAC, fire and security subsystems)
  - Business applications (those responsible for applications interfaced to the Building Management system such as Human Resources, Physical Security etc.)
  - IT system administration
  - IT network administration
  - IT security

Executive sponsorship and a formal team structure is a recommendation for the security program. The actual process steps that follow are more critical to the success of the program.
Identifying assets

In this context the term asset implies anything of value to the company. The term includes equipment, intellectual property such as historical data and algorithms, and infrastructure such as network bandwidth and computing power.

In identifying assets that are at risk you need to consider:

- People, for example, your employees and the broader community to which they and your enterprise belong.

- Equipment and assets, for example control system equipment
  - Plant equipment: network equipment (routers, switches, firewalls) and ancillary items used to build the system
  - Network configuration information (such as routing tables and ACL’s)
  - Intangible assets such as bandwidth and speed
  - Computer equipment
  - Information on computing equipment (databases) and other intellectual property
Identifying and evaluating threats

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

Potential threats to be considered include:

- People, for example, malicious users outside the company, malicious users within the company, and uninformed employees.

- Inanimate threats, for example, natural disasters (such as floods, earthquakes, fire) or malicious code such as a virus or denial of service.
Identifying and evaluating vulnerabilities

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

- The absence of security policies and procedures
- Inadequate physical security
- Gateways from the Internet to the corporation
- Gateways between the business LAN and Building Control Network
- The improper management of modems
- Out-of-date virus software
- Out-of-date security patches or inadequate security configuration
- Inadequate or infrequent backups

You might also want to use failure mode analysis to assess the robustness of your network architecture.
Identifying and evaluating privacy issues

You need to consider the potential for unauthorized access to personal data stored within your system. Any information which may be considered sensitive by an individual such as home address, tax number, religion etc; should be protected and all their access methods reviewed to ensure correct authorization is applied. The Cardholder System is a prime example of a database holding personal information.
Creating a mitigation plan

As part of your plan of defense you need to write policies and procedures to protect your assets from threats. The policies and procedures should cover your networks, your Windows nodes, and any other operating systems.

You should also perform risk assessments on your building management system equipment. A full inventory of your assets will help you to identify threats and vulnerabilities.

You are then in a better position to decide whether you can ignore, mitigate, or transfer the risk.
Implementing change management

A formal change management procedure is vital for ensuring that any modifications to the Building Control Network meet the same security requirements as the components that were included in the original asset evaluation and the associated risk assessment and mitigation plans.

Risk assessment should be performed on any change to the Building Control Network that could affect security, including configuration changes, the addition of network components and installation of software. Changes to policies and procedures might also be required.
Planning ongoing maintenance

Constant vigilance of your security position should involve:

- Regular monitoring of your system.
- Regular audits of your network security configuration.
- Regular security team meetings whose role it is to stay up to date with the latest threats and with the latest technologies for dealing with security issues.
- Ongoing risk assessments as new devices are placed on the network (see “Implementing change management” on page 28).
- The creation of an Incident Response Team (see “Security response team” on page 30).

Additional security resources

You should also be proactive about security by reviewing additional security resources, for example:

- Microsoft: http://www.microsoft.com/technet/security
- Cisco: http://www.cisco.com
- Computer Security Institute: http://www.gocsi.com
- SANS Internet Storm Centre: http://isc.sans.org
- CERT: http://www.cert.org
- AusCERT: http://www.auscert.org.au

Refer to Information Security Standards

- European Network and Information Security Exchange: http://www.enisa.eu.int/
- British Standards Institution – Information Security: http://www.bsi-global.com
- ISO: http://www.iso.org

Refer to Information Technology - Security Techniques:

- ISO 15408 Evaluation Criteria for IT Security parts 1-3
- ISO 17799 Code of practice for information security management
- The Instrumentation, Systems, and Automation Society: http://www.isa.org
  Choose Standards > Committees
  Then choose ISA-SP99, Manufacturing and Control Systems Security
  More detailed information on creating a security program can be found in the ISA document Integrating Electronic Security into the Manufacturing and Control System Environment, which includes a detailed life-cycle approach similar to the approach developed for safety-related system in the IEC 61508.
Security response team

The responsibilities of a security response team (SRT) might include:

- Monitoring the Microsoft and Honeywell software update sites.
- Monitoring the 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 be 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 hot fixes 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 so you need to verify and install it early on all of your systems.
- Ensuring the deployment of qualified security updates on the EBI servers and dedicated (control room) Station clients. Note that the corporate IT policy for updating Windows computers should be sufficient for the rotary Station and engineering computers.
- Checking that Microsoft Baseline Security Analyzer is run periodically to ensure that security updates have not been missed. For details, see “Using Microsoft Baseline Security Analyzer” on page 101.
- Review network infrastructure patches and configuration changes that will help to secure the network against the latest methods of attack.
Disaster recovery

This section describes planning considerations for backup and restoration policies and the tools that are supported for backing up and restoring your EBI system.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formulating a disaster recovery policy</td>
<td>page 32</td>
</tr>
<tr>
<td>Overview of backup and recovery tools</td>
<td>page 33</td>
</tr>
<tr>
<td>About Acronis True Image</td>
<td>page 35</td>
</tr>
<tr>
<td>Important planning considerations for Acronis True Image</td>
<td>page 36</td>
</tr>
</tbody>
</table>
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 frequently critical data and configuration is changing. 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 EBI related installation media, license keys, and configuration information.

- Who will be responsible for backups, and the testing, storing, and restoring of backups?
Backup and recovery tools for EBI

The recommended method of backing up your EBI system is the EBI fullbkup utility in conjunction with Acronis True Image software.

Acronis True Image software has been qualified for use with EBI products. If you want to use other third-party backup software, contact your Honeywell representative for the latest information about qualified backup software.

For detailed information about backup strategies, and specific instructions for backing up your EBI system using Acronis True Image, see the *EBI Backup and Restore Guide*.

The following table lists some of the key features of Acronis True Image.

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backs up the entire drive.</td>
</tr>
<tr>
<td>Backups can be saved to an internal hard drive, a USB or FireWire drive, a network drive or Acronis Secure Zone (protected partition on the local drive).</td>
</tr>
<tr>
<td>Performs full and incremental backups</td>
</tr>
<tr>
<td>Backs up local and remote computers</td>
</tr>
<tr>
<td>Performs on demand or scheduled backups</td>
</tr>
<tr>
<td>Rapidly restore from catastrophic failure.</td>
</tr>
<tr>
<td>Bootable restore CD/DVD for restore management.</td>
</tr>
<tr>
<td>Minimal user intervention to schedule and run backups.</td>
</tr>
<tr>
<td>Single management console for control of local and remote nodes.</td>
</tr>
<tr>
<td>Supports backing up RAID drive arrays.</td>
</tr>
</tbody>
</table>

Notes:

- The Windows Operating System and EBI cannot be restored to the system partition from a remote location using Acronis Management Console. This must be performed locally via the bootable recovery CD.

- Note that CD and DVD are not considered a reliable backup medium.

- Acronis True Image Enterprise Server is required for remote management of computers.

- The Acronis Management Console cannot connect to its Remote Agent without modifying Honeywell SUS port configurations. The default SUS policy enforcement rules blocks the following ports that Acronis requires to communicate with its agent:
  
  For the server computer:
  - Acronis True Image Agent - UDP port: 9876
  - Acronis True Image Agent - TCP port: 9876, if busy chose randomly
For the client computer:
- Acronis True Image Management Console - UDP port: 9877, if busy chose randomly
About Acronis True Image

A key feature of Acronis True Image is the ability to provide an image-based backup while the node is operational. The backup image can then be the basis for a rapid node recovery.

With Acronis True Image, you can perform partial or total restores of your disk images as required by your system condition. The backup image can be used to return your computer to a previous working state with the operating system, applications and data files intact.

With Acronis True Image, you can perform the following tasks:

- Remotely initiate a backup of any EBI nodes on the network such as Point Servers and Stations. Acronis True Image Enterprise Server is required for remote management of computers.

- Determine what is backed up on an EBI node and where the backup image is stored in the EBI system.

- Configure backups, backup schedules, and options.

- Direct the backup to various storage media/devices such as USB drive, NAS, CD, and DVD to allow you to store backup images and data in a secure, temperature controlled location.

- Manually initiate a backup.

- Monitor the status of backup jobs.

- Manage the backup repository.

- Restore drive images, files, and folders.

- Restore archived images from an internal hard drive, Acronis Zone, External USB or FireWire drive, CD, DVD, tape device or a network drive.
Planning considerations for Acronis True Image

When planning the implementation of Acronis True Image you need to bear in mind the following rules and guidelines:

- The network location used as the destination for backup images should not be an EBI server.

- Have enough file storage space to hold all of the planned backups.

- LonWorks credit backup requires a full disk backup. A partition backup does not save the LonWorks credit data. Be sure to size your file storage space accordingly.

- You should also ensure that verification is performed upon the backup’s completion to ensure that the data was backed up correctly.
Physical and environmental considerations

Although the security issues for EBI are generally the same as for any IT server, the physical security of a Building Control Network is particularly important. If the hardware is rendered inoperable, then the operations of the entire facility can be compromised.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical location</td>
<td>page 38</td>
</tr>
<tr>
<td>Protecting against unauthorized system access</td>
<td>page 39</td>
</tr>
<tr>
<td>Control room access</td>
<td>page 40</td>
</tr>
<tr>
<td>Network and controller access</td>
<td>page 41</td>
</tr>
<tr>
<td>Reliable power</td>
<td>page 42</td>
</tr>
</tbody>
</table>
In 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 located 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 located in an area that is not susceptible to flood or liquid seepage situations. It should be elevated above the base floor level either by a raised floor or mounting pad. It should be located in area with no overhead piping that could break or otherwise leak into the equipment.

- **Temperature and Humidity** – The server should be located 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 computers or of individual components such as disks and memory chips. At the very least, the computer and monitor should be chained 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 they have a floppy disk or CD drive, you might also consider fitting locks to floppy and CD drives, or (in extreme cases) removing the floppy and CD drives from the computers altogether. If the server or control room Stations have 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. You should also consider disabling or physically protecting the power button to prevent unauthorized use.

For maximum security, the server, any PC workstation with access to the EBI Server 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 individuals who accessed the room.
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 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 therefore of critical importance in relation to the nodes in your Building Control Network that you do not allow (and prevent) the use of all unauthorized removable devices and media such as CDs, DVDs, floppy disks, and USB memory sticks.

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.
- 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 drives.
- Removing (in extreme cases) the floppy and CD drives from the computer.
- Disabling USB ports and other ports capable of being used for memory sticks and other portable storage devices.
- Group policy may be used to prevent certain drive letters (floppy drive and CD drive) from being visible to Microsoft Windows Explorer. For instructions on how to do this, see the Microsoft article 278295 “How to lock down a Windows Server 2003 Terminal Server session”. Note, however, that hiding the drives in Windows Explorer does not prevent those drives from being accessed via a Command prompt.
Control room access

Providing physical security for the control room is essential to reduce the potency of many threats. Frequently control rooms will have Stations continuously logged onto the EBI server, with speed of response and continual view of the building considered more important than secure access. The area will also often contain the servers themselves, other critical computer nodes and controllers. Limiting those who can enter this area, using smart or magnetic identity cards, biometric readers and so on is essential. In extreme cases, it may be considered necessary to make the control room blast-proof, or to provide a second off-site emergency control room so that control can be maintained if the primary area becomes uninhabitable.
Network and controller access

Many building, fire, security and access controllers are intelligent programmable devices, with the ability to be manipulated through loader software running on a laptop or similar computer connected directly to them. In order to prevent unauthorized tampering, the controllers and network equipment should be physically protected in locked cabinets, and logically protected with passwords or other authentication techniques. Network cables are also 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 uninterruptible power supply (UPS). If the site has an emergency generator, the UPS battery life may only need to be a few seconds; however, if you rely on external power, the UPS probably needs several hours supply.

Note that where you have redundant equipment such as redundant servers or redundant switches, you should also ensure that each unit in a redundant pair is on a different UPS or power source.
Microsoft™ security updates and service packs

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

At the same time, it is important to bear in mind that frequent updates to critical building management system nodes can be error prone, and may, over time, destabilize your system so they should be undertaken judiciously and with care.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft security updates</td>
<td>page 43</td>
</tr>
<tr>
<td>Microsoft service packs</td>
<td>page 45</td>
</tr>
<tr>
<td>A secure process for distributing Microsoft hot fixes and virus definition files</td>
<td>page 46</td>
</tr>
</tbody>
</table>
Microsoft Security updates

Microsoft releases a range of security updates and other operating system and software updates. Note that only Honeywell-qualified Microsoft updates are supported. You should therefore wait until Honeywell has validated Microsoft updates before installing them (see “Honeywell’s qualification of Microsoft security updates” on page 44). It is also recommended that you implement a controlled system for the distribution of all updates (see “Distributing Microsoft updates and virus definition files” on page 46).

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

Attention: Before installing security updates on the critical nodes in your Building Control Network, you should refer to Honeywell’s HBS Product Technical Support web site (see “Honeywell’s qualification of Microsoft security updates” on page 44 for instructions on navigating to the site). This site provides information on the status of qualified updates and Hot Fixes for Honeywell Building Solutions (HBS) products (that is, EBI).

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

Honeywell’s qualification of Microsoft security updates

In this context, qualification means that Honeywell sells and supports the product, or has tested a product for use in conjunction with its own products or services. Honeywell qualifies Microsoft security updates and other updates for operating systems, Internet Explorer, and SQL Server products within a short period of time but generally only qualifies updates denoted as “Critical”.

Customers may choose to enlist the assistance of Honeywell in the management of Microsoft Hotfixes as well as other critical security related services such as virus protection and backup solutions. Honeywell Service Technicians, the Technical Assistance Center and even the subscription based Honeywell Software Update Service are valuable resources available for systems management. With a subscription to Honeywell Server Online (HSO), update information may be found at the HSO website by following these steps:

Go to Honeywell’s Service Online web site: https://www.honeywellserviceonline.com

Go to System Support and click on Knowledge Center. Select Product Type as EBI and Category as Compatibility Matrix, and then click on Browse Documents. Look for Microsoft Security Hot Fix titles for the latest Microsoft Update Listings.

Honeywell’s Microsoft Security Hot Fix Information web page will contain the latest monthly update of Hot Fixes that have been tested and qualified with EBI.

The Microsoft web site is a prime source of information on current and past Hot Fixes. Go to:

Microsoft Service packs

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

Honeywell’s qualification of Microsoft service packs

Microsoft performs full integration testing of their service packs against the operating system and their own applications. Honeywell will follow that with system integration testing of the service pack which in most cases will be part of a scheduled and planned release.

Note that only Honeywell-qualified Microsoft service packs are supported and you should therefore wait until Honeywell has qualified the service pack prior to your own qualification testing.

You may wish to contact your Honeywell representative for advice in relation to Microsoft service packs or check the Honeywell Service Online web site:

2. Go to System Support and click on Knowledge Center. Select Product Type as EBI and Category as Compatibility Matrix, and then click on Browse Documents. Look for Microsoft Security Hot Fix titles for the latest Microsoft Update Listings.

In any case you should verify service packs on a non-production computer, or when the building is not active, 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 nodes (including non-EBI nodes) in your EBI 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 nodes on the Building Control Network as this is contrary to the goal of minimizing direct communication between nodes on these networks. Honeywell therefore recommends that an update manager and an antivirus server be located in the DMZ (see “The demilitarized zone” on page 60). Both roles can be performed by a single server. Contact your Honeywell representative if you need assistance configuring nodes in a DMZ.

Implementing a Microsoft update and antivirus management system that is dedicated to the Building Control Network helps to ensure more controlled and secure updates, which sites can also tailor for the unique needs of their particular building management environment. It also helps address the issues that arise when an antivirus product that is supported by the building management equipment vendor is not the same as the antivirus product supported by the corporate IT department.

Attention: Honeywell qualifies Microsoft security updates and other updates. It is strongly recommended that Microsoft updates are not implemented until this qualification has been carried out (see “Honeywell’s qualification of Microsoft security updates” on page 44 and “Honeywell’s qualification of Microsoft service packs” on page 45).
Antivirus measures are an essential element of a comprehensive building management security strategy.

<table>
<thead>
<tr>
<th>Recommendations</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose antivirus software that has been tested (and is supported) by Honeywell.</td>
<td>page 48</td>
</tr>
<tr>
<td>Install antivirus software on each node connected to the Building Control Network.</td>
<td>page 49</td>
</tr>
<tr>
<td>Configure active virus scanning.</td>
<td>page 50</td>
</tr>
<tr>
<td>Tune the virus scanning for system performance.</td>
<td>page 51</td>
</tr>
<tr>
<td>Ensure that signature files are updated on a regular basis.</td>
<td>page 52</td>
</tr>
<tr>
<td>Test antivirus signature files offline before deploying them to building management nodes.</td>
<td>page 53</td>
</tr>
<tr>
<td>Prohibit email clients on nodes in the Building Control Network.</td>
<td>page 54</td>
</tr>
</tbody>
</table>
Choose supported antivirus software

Honeywell has tested (and supports) both McAfee VirusScan and Norton AntiVirus for use in conjunction with EBI.

The EBI Compatibility Matrix lists the versions of McAfee VirusScan and Norton AntiVirus that are supported for EBI.

Attention: Virus scanners other than McAfee VirusScan and Norton Anti-Virus may not be supported and may not work on EBI. For more information contact your Honeywell representative.
Install antivirus software on building management nodes

Install antivirus software on every node in the Building Control Network. This should include:

- EBI Servers
- EBI Point Servers
- EBI Stations

It is recommended that you set up special servers for the controlled distribution of antivirus signature files to the BCN as outlined in “Distributing Microsoft updates and virus definition files” on page 46.
Configure active antivirus scanning

It is recommended that you adopt an active virus scanning strategy. For guidance on antivirus measures:

1. Go to Honeywell’s Service Online web site: https://www.honeywellserviceonline.com
2. Go to System Support and click on Knowledge Center. Select Product Type as EBI and Category as Product Bulletins, and then click on Browse Documents. Look for PB-363 Important information when considering antivirus software for the server.

Here you will find information about:

- Recommended antivirus strategies.

The recommended strategies include ensuring that:

- Virus scan reports are regularly reviewed.

- Antivirus software is 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.
Tune the virus scanning for system performance

In formulating your virus scanning strategy you may also need to take into account the potential impact on critical system resources.

For example, if your EBI is 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 node are adequate to meet system needs.

- Consider limiting the system resources that are used by antivirus software during scanning. Honeywell has tested anti-viral software successfully on extremely large systems by limiting the CPU utilization of anti-viral 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.

  For more information about virus-scanning and system performance, see “About virus scanning and system performance” on page 51.

  Attention: Do not automatically schedule full system scans on any EBI node as this can result in severe degradation of performance, and could therefore impact the ability of operators to respond to a situation.

Directories that can be excluded from scanning

EBI creates many files during normal operations and the system resource overhead of scanning each of these files for viruses is extremely high. Performance degradation can occur when the \Honeywell\Server\Data directory is not excluded from scanning. If this, or other, directories are excluded, their file permissions should be modified to ensure that only authorized accounts (such as Honeywell Administrator group) have write access.

By default, the \Honeywell\Server\Data directory has write access only for the Honeywell Administrators and Administrators groups.

About virus scanning and system performance

The EBI system requires a certain amount of system resources (including CPU, memory, disk access), in order 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 node 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, look up the web-site for your antivirus software.

McAfee VirusScan version 8 performs checking of any scripts that are run and will affect the performance of any Station displays that use scripting. This feature is recommended to be disabled.
Ensure frequent updates to antivirus signature files

Non-directed virus and worm attacks are common attacks on a control system. A virus that is deemed low risk for corporate systems may pose a high risk to a control 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

Where it is not practical to do this daily, it is worth monitoring those Web sites which publish information about new virus attacks so that the system can be isolated if a specific threat appears. For recommendations on distributing antivirus updates, see “Distributing Microsoft updates and virus definition files” on page 46.
Test the deployment of antivirus signature files

It is important to test antivirus signature files offline before deploying them. This helps to ensure that the signature file does not break the antivirus software or cause problems on the computer. For example, you could first test the signature files on:

- A staged test system
- One or two nodes

In line with the best practice of minimizing communication between the business network and the Building Control 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” on page 46.

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

- Stagger automatic deployment to eliminate the potential for common cause failure. For example, deploy to no more than three or four nodes per hour.
- Follow the recommendations of your antivirus software vendor for distribution server/services.
- Stage the distribution on a test system.
Prohibit email clients on the Building Control Network

Do not install email clients on any node connected to the Building Control Network. Honeywell does not support email clients on the Building Control Network.

Viruses and email

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

Instant messaging

An emerging trend is the use of instant messaging (IM) as a transport mechanism for malware. Targeting MSN clients in particular, the malware sends messages to all contacts on an infected machine, thereby increasing network traffic uncontrollably. This message itself, apparently from a trusted source, usually tells the recipient to browse to a malicious web site which will then download more serious malware, opening back doors or otherwise allowing takeover of the machine. It is possible that IM will replace email as the prime carrier of malware in the near future.

Honeywell strongly advises against supporting instant messaging on nodes within the BCN.

Spyware

An increasingly common threat is that posed by spyware, also known as “bots.” These 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 propagated via email or inadvertently downloaded in the course of Internet access.

Note: Honeywell does not support internet and email access from the BCN. Use of spyware removal applications may cause unexpected results to your Building Control Network nodes. These applications may alter registry settings that are crucial to the operation of the software on these nodes. If spyware is detected, and a spyware removal application needs to be used, ensure that the nodes are backed up prior to the installation of the spyware removal application. Refer to page 33 for details on backing up the nodes.
Network planning and security

This chapter describes key network security considerations for EBI systems. The network security model described herein takes the position that security of the Building Control Network (BCN) and EBI applications are critical. Installations where there is regulation by agencies or compliance to specific government requirements may need to follow the recommendations and the architecture in the absolute sense. Customers with Pharmaceutical applications who are complying to CFR 21/11 or who have requirements to protect information under the Sarbanes Oxley Act or for other reasons may need to follow a stringent and securely enforced architecture. Customers need to evaluate their business, the compliances required and the risks posed, then deploy the EBI applications in a manner that is consistent with their risks and business policies for security in their IT organization. What follows are recommendations for a secure network, not a depiction of the only way EBI may be properly installed.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honeywell’s High Security Network Architecture</td>
<td>page 56</td>
</tr>
<tr>
<td>Connecting to the business network</td>
<td>page 59</td>
</tr>
<tr>
<td>The demilitarized zone (DMZ)</td>
<td>page 60</td>
</tr>
<tr>
<td>Configuring the DMZ firewall</td>
<td>page 61</td>
</tr>
<tr>
<td>Securing network equipment</td>
<td>page 74</td>
</tr>
<tr>
<td>Securing controller network interfaces</td>
<td>page 75</td>
</tr>
<tr>
<td>Network Encryption</td>
<td>page 76</td>
</tr>
<tr>
<td>Network Planning</td>
<td>page 78</td>
</tr>
<tr>
<td>Domain Name Servers</td>
<td>page 81</td>
</tr>
<tr>
<td>Remote access</td>
<td>page 82</td>
</tr>
<tr>
<td>Computer Names</td>
<td>page 83</td>
</tr>
<tr>
<td>Registering EBI Servers</td>
<td>page 84</td>
</tr>
<tr>
<td>Dual-homed computers</td>
<td>page 85</td>
</tr>
<tr>
<td>Port Scanning</td>
<td>page 86</td>
</tr>
<tr>
<td>3rd Party Applications</td>
<td>page 87</td>
</tr>
<tr>
<td>Remote Monitoring Applications</td>
<td>page 88</td>
</tr>
<tr>
<td>Managed Ethernet Switches</td>
<td>page 89</td>
</tr>
</tbody>
</table>
High Security Network Architecture

Honeywell’s High Security Network Architecture is a concept for secure and reliable Ethernet based systems. It is comprised of a tiered network architecture of switches, routers, and firewalls to protect and isolate critical building operational levels from less secured network levels.

A summary of the key security-related features of Honeywell’s High Security Network Architecture follows.

Supported topologies

Honeywell’s High Security Network Architecture has the following levels. At each level the node membership, IP subetting, and switch configuration are different.

<table>
<thead>
<tr>
<th>Level</th>
<th>Function of this level</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Controller interfaces</td>
<td>page 57</td>
</tr>
<tr>
<td>Level 2</td>
<td>Supervisory control and the operator interface</td>
<td>page 57</td>
</tr>
<tr>
<td>Demilitarized Zone (DMZ)</td>
<td>Nodes that access Level 2 as well as the business enterprise network</td>
<td>page 58</td>
</tr>
<tr>
<td>Level 3</td>
<td>Business Enterprise network applications that access data such as alarms, events, history and cardholder information</td>
<td>page 58</td>
</tr>
</tbody>
</table>

The Building Control Network (BCN) comprises of Level 1 and Level 2.
Figure 2: Figure 2 EBI High Security Network Architecture

Topologies other than that shown in Figure 2 “EBI High Security Network Architecture” are supported.

For small scale networks you can also connect:

- Level 1 and level 2 devices using a single switch
- Level 1 and level 2 using a flat switched network topology.

About Level 1

At Level 1, building controller busses, access and security controller busses connect to the Level 1 network switches via network interfaces and terminal servers.

The Level 1 network is the most critical network in the system as a failure or loss of service on this network can result in loss of control/view. The network should be configured so that all Level 1 devices that control a given area of the building are connected together in the same secured network.
Traffic on the Level 1 network is limited to communication with other Level 1 nodes and with the EBI Servers and Point Servers at Level 2.

About Level 2

At Level 2 EBI Servers and Point Servers connect to Level 2 switches. There are also uplink connections from the Level 1 switches. If the nodes at Level 2 are part of a Microsoft Windows domain, these nodes will have to communicate with the domain controller.

If you want to virutalize EBI Servers and point servers, the ESX host would be at Level 2. For more information about virtualization, see Virtual environments on page 90.

The Level 2 network must be a highly reliable and highly available network to maintain constant view to the building controllers, access and security controllers. A failure of the Level 2 network can result in a loss of view of the building.

IP subnetting of nodes, priority queuing, and access lists in the switches can be used to control network traffic between Level 2 and Level 1 as follows:

- Internal Level 1 traffic has a higher priority than traffic between Level 1 and Level 2 nodes. Peer-to-peer controller communication will not be disrupted by other network traffic.

- Only Level 2 nodes that need to communicate with Level 1 nodes are permitted to do so. No communication between Level 3 nodes and Level 1 or Level 2 nodes is permitted.

- Bandwidth limits are configured for Level 2 nodes to protect against broadcast, multicast, and unicast storms. If these thresholds are set for low tolerance of high traffic bursts, then problems may be encountered with traffic between redundant servers being interpreted as an attack.

There are also uplink connections from the Level 2 switches and, if required, a connection to a firewall that serves as the gateway to the business network.

About demilitarized zones

A demilitarized zone (DMZ) serves as a buffer zone between the Building Control Network and the business network. It is a separate network segment connected directly to the firewall.

Servers placed in the DMZ can be accessed by nodes at Level 3, permitting the supply of data but preventing nodes at Level 3 from having direct access to any systems on the levels below. For more information, see “The demilitarized zone” on page 60.

About Level 3

Level 3 is the business network (see “Connecting to the business network” on page 59). It is generally administered by the corporate IT department and is outside the scope of these guidelines.
Connecting to the business network

It is recommended that the Building Control Network and business network be kept separate as shown in “The levels in an EBI system” on page 56.

The nature of network traffic on these two networks is different:

- Internet access, FTP, email, and remote access will typically be permitted on the business network but not on the Building Control Network.

- Rigorous change control procedures for network equipment, configuration, and software changes may not be in place on the business network.

- Building management network traffic should not go on the business network as it could be intercepted. Security and performance problems on the business network should not be able to affect the Building Control Network.

Ideally there should be no direct communication between the Building Control Network and the business network. However, practical considerations often mean that a connection is required between these networks. This may be because the Building Control Network requires data from the business network or because certain business applications need access to data from the Building Control Network.

However such a connection represents a significant security risk and therefore careful consideration should be given to the design. Because of this, it is strongly recommended that only a single connection be allowed and that the connection is through a firewall and a DMZ as described in “The demilitarized zone” on page 60.
The demilitarized zone

A demilitarized zone (DMZ) is a separate network segment that connects directly to the firewall (as shown in Figure 2 on page 57) and provides a buffer between the Building Control Network (BCN) and the business network. Servers containing data from the building management system that needs to be accessed from the business network are put on this network segment.

It is recommended that direct access between the two networks is avoided by having each network only access nodes in the DMZ. By eliminating the direct connection between the nodes in the BCN and the business network, the security of each network is increased.

With any external connections the minimum access should be permitted through the firewall. Only identified ports required for specific communication should be opened.

The access required for specific node types is described in “Configuring the DMZ firewall” on page 61. For more detailed information on firewall configuration, contact your Honeywell representative.
Configuring the DMZ firewall

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

Filtering is used to permit only specific nodes on the business network, DMZ and BCN to communicate. TCP port filtering should be used to stop denial-of-service attacks to well-known ports.

The following topics describe the firewall access and account requirements for an arrangement where nodes on the business network, DMZ, and BCN are separated by a firewall. While other topologies are possible, you need to consider their security implications (for example, if a DMZ is not used).

The sections referred to below describe the firewall access requirements for Honeywell-supplied applications. In addition to the requirements documented, access may be required for Windows authentication of accounts and synchronization between domain controllers. The precise access requirements will depend upon:

- The domain membership of the nodes in the DMZ (business, BCN or other).
- The domain membership of accounts used.
- The location of domain controllers and which, if any, trusts exist between domains.

For more information on:
- Domains refer to “Windows domains” on page 107.
- Firewall filtering requirements; refer to the relevant Microsoft documentation.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed System Architecture</td>
<td>page 61</td>
</tr>
<tr>
<td>File shares</td>
<td>page 63</td>
</tr>
<tr>
<td>Remote access for Station and Quick Builder</td>
<td>page 65</td>
</tr>
<tr>
<td>Remote access for HMIWeb Browser</td>
<td>page 65</td>
</tr>
<tr>
<td>Mobile access for Honeywell EasyMobile</td>
<td></td>
</tr>
<tr>
<td>Remote access for Enterprise Applications</td>
<td>page 69</td>
</tr>
<tr>
<td>Microsoft Windows Security Update Server</td>
<td>page 69</td>
</tr>
<tr>
<td>Honeywell Software Update Service</td>
<td>page 70</td>
</tr>
<tr>
<td>Antivirus Update server</td>
<td>page 70</td>
</tr>
</tbody>
</table>

Distributed System Architecture

This section describes the firewall access and account requirements for Distributed System Architecture (DSA) nodes.

DSA is an option that supports the sharing of information between EBI servers, and is used by a number of the systems described in the following sections.

DSA nodes have publishing and subscribing roles. Publishing servers provide data to subscribing servers. For more details see “Distributed System Architecture” in the chapter “Configuring Distributed System Architecture” in the Configuration and Administration Guide. Also see “Distributed System Architecture” in the Access Control and Security Guide for EBI Security Cardholder Management database requirements.
The following diagram shows one publishing and one subscribing node. DSA supports networks of nodes, any of which can be publishing, subscribing, or both.

![Diagram of Distributed Server Architecture](image)

The following table shows the firewall access requirements.

<table>
<thead>
<tr>
<th>Source Host/ Network</th>
<th>Destination Host/ Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribing server</td>
<td>Publishing server</td>
<td>DMZ</td>
<td>2911/UDP</td>
<td>Connection must be configured to use Unicast. Do not use the “Link Supports Multicast Traffic” option.</td>
</tr>
<tr>
<td>Publishing server</td>
<td>Subscribing server</td>
<td>BCN</td>
<td>2911/UDP</td>
<td></td>
</tr>
<tr>
<td>Subscribing server</td>
<td>Publishing server</td>
<td>DMZ</td>
<td>135/TCP/UDP</td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td>Subscribing server</td>
<td>Publishing server</td>
<td>DMZ</td>
<td>1024-65535/TCP/UDP</td>
<td>Used by RPC. The port range can be restricted by registry settings.</td>
</tr>
<tr>
<td>Publishing server</td>
<td>Subscribing server</td>
<td>BCN</td>
<td>135/UDP</td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td>Publishing server</td>
<td>Subscribing server</td>
<td>BCN</td>
<td>1024-65535/TCP/UDP</td>
<td>Used by RPC. The port range can be restricted by registry settings.</td>
</tr>
</tbody>
</table>

Notes:
- Honeywell strongly recommends that IP to IP access be granted between DSA servers
• The password for the Windows MNGR local account must be the same on all servers in a DSA system.

• DSA by default uses multi-casting for distributing status information between servers. Multi-casting is not supported through firewalls; as well many routers also disable it by default. If DSA is to be used through a firewall then the connection needs to have the multi-casting option disabled, and hence uni-casting enabled. Please refer to the Configuration and Administration Guide for details on how to do this.

• DSA also requires that the Honeywell Servers are time synchronized. In a Microsoft Windows Active Directory domain environment this time synchronization is provided automatically by the Windows Operating System. If Time Synchronization between domains or time synchronization to an external source is required, then you will need to consult Microsoft documentation for the appropriate ports used for Time Synchronization.

**File shares**

This section describes the firewall access and account requirements for file shares.

File shares provide access to files for remote systems, and are used by a number of the systems described in the following sections.

The following file shares are configured by default:

- **\Honeywell\Server\data\Views**
  This file share is set for read access only for the Everyone group

- **\Honeywell\Server\sqlrep**
  This file share is set for full control to the Honeywell Administrators group.

- **\Honeywell\Client\abstract (shared as CustomDisplays)**
  All custom displays can be located in this directory. This file share is set for full-control for the Honeywell Users group to allow remote Stations to access a central graphic repository.

- **\Honeywell\Server\setup (shared as hwConfig)**
  Set to full control for the Honeywell Administrators group to allow remote Quick Builder operations.

- **\Honeywell\client\system\rXXX (shared as RXXX)**
  System displays located in this directory. This file share is for full control for Honeywell Users to allow remote Stations to access a central graphic repository.

- **\Honeywell\Pointservers\LPS\templates (shared as templates).**
  This file share is set for full-control Honeywell Administrators full control and Honeywell Users Read only

The following additional file shares can be configured:

- **\Honeywell\EBI\Server\cms\PhotoID**
  This file share can be set for full for the Honeywell Users group to allow cardholder images to be replicated by sqlrep.

In the example shown below, a server in the DMZ accesses files from a server in the BCN.
The following table shows the firewall access requirements if both systems are running Windows XP or Windows 2003.

<table>
<thead>
<tr>
<th>Source Host/ Network</th>
<th>Destination Host/ Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>File share client</td>
<td>File share server</td>
<td>DMZ</td>
<td>88/TCP/UDP</td>
<td>Required when using domain accounts with Kerberos</td>
</tr>
<tr>
<td>File share client</td>
<td>File share server</td>
<td>DMZ</td>
<td>137/TCP/UDP</td>
<td></td>
</tr>
<tr>
<td>File share client</td>
<td>File share server</td>
<td>DMZ</td>
<td>138/UDP</td>
<td></td>
</tr>
<tr>
<td>File share client</td>
<td>File share server</td>
<td>DMZ</td>
<td>139/TCP</td>
<td></td>
</tr>
<tr>
<td>File share client</td>
<td>File share server</td>
<td>DMZ</td>
<td>445/TCP</td>
<td></td>
</tr>
</tbody>
</table>

Notes:

- If the Honeywell servers are in a domain then they should be able to communicate to the appropriate domain controllers on all of these ports.

- When using file shares the client machine will need to be able to communicate to the machine providing the file share on all ports except 88. For machines providing the file share, if using domain accounts these machines will need to be able to communicate with the domain controller on all of these ports.

- The Kerberos security port may be utilized by the machine providing the file share to its domain controller when it needs to authenticate a client accessing this share. It is not required when simply signing on to a Station.
Remote access for Station and Quick Builder

If business network and offsite access is required to Station or Quick Builder applications, you should set up a Remote Station Radmin Server and use the Radmin client on the business client PC(s). The Honeywell High Security Network Architecture does not recommend Station or Quick Builder connections directly to the BCN or DMZ from the business network side of the firewall because of the security risks.

Running Terminal Services directly on the EBI server is not supported because Terminal Services consumes a significant portion of the fixed size operating system “session space” resource. Exhausting this resource can stop the EBI server from starting correctly.

In the example shown a remote client PC connects to the Remote Station Radmin Server in the DMZ using the Radmin client. Station runs on the Remote Station Radmin Server connecting to the redundant EBI server pair in the BCN. In the same manner, Quick Builder runs on the Remote Station Radmin Server connecting to the servers in the BCN.

The firewall access requirements between the remote client PC and the Remote Station Radmin Server are shown in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering client</td>
<td>Remote Station Radmin Server</td>
<td>Business network</td>
<td>4899/TCP</td>
<td>Port can be changed.</td>
</tr>
</tbody>
</table>

The user on the remote client needs to log on to the Remote Station Radmin Server with an account that can be authenticated in the Remote Station Radmin Server’s domain.
The firewall access requirements between the Remote Station Radmin server and the EBI server pair is described in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Station Radmin Server</td>
<td>Redundant EBI server</td>
<td>DMZ</td>
<td>Echo/ICMP</td>
<td>Optionally used to verify which server is currently active. It can be disabled by a configuration option.</td>
</tr>
<tr>
<td>Redundant EBI server</td>
<td>Remote Station Radmin Server</td>
<td>BCN</td>
<td>Echo/ICMP</td>
<td></td>
</tr>
<tr>
<td>Remote Station Radmin Server</td>
<td>Redundant EBI server</td>
<td>DMZ</td>
<td>1433/TCP</td>
<td>SQL Server access (Quick Builder only).</td>
</tr>
<tr>
<td>Remote Station Radmin Server</td>
<td>Redundant EBI server</td>
<td>BCN</td>
<td>2910/TCP</td>
<td>Quick Builder only.</td>
</tr>
<tr>
<td>Remote Station Radmin Server</td>
<td>Redundant EBI server</td>
<td>DMZ</td>
<td>50000/TCP</td>
<td></td>
</tr>
<tr>
<td>Redundant EBI server</td>
<td>Remote Station Radmin Server</td>
<td>BCN</td>
<td>50000/TCP</td>
<td></td>
</tr>
</tbody>
</table>

Notes:
- If the firewall has been configured to disable ICMP traffic, Station will not be able to connect to the server unless the “ping” setting in the station.ini file has been disabled. For information on changing station.ini file settings, see the “Station.ini” section in the chapter “Configuring Stations and printers” in the *Configuration and Administration Guide.*
- If Quick Builder is used on the Remote Station Radmin Server, access to a file share on the redundant EBI servers is required. The Remote Station Radmin Server is the file share client and the redundant EBI servers are the file share servers. For details of the firewall access requirements, see “File shares” on page 63.
- When users of Quick Builder connect to EBI, they must use an account that correlates to an operator on that EBI Server.

**Remote Access for HMIWeb Browser**

HMIWeb Browser allows remote users to connect to the EBI server over an Internet or Intranet environment using only Internet Explorer.

To allow this to work, there are several things that need to be done:
- Port 80 must be opened in the firewall. Any organizations with existing web servers will already have this port opened.
- Port 80 must also be port forwarded to the EBI server if NAT is used.

HMIWeb Browser also allows secure connections using SSL technology. To configure this (in addition to the points above):
- Port 443 must be opened in the firewall.
• Port 443 must also be port forwarded to the EBI server if NAT is used

• Port 443 can be changed if desired, but port 80 must remain open in the firewall in order for secure connections to be used.

To modify the SSL port for HMIWeb browser:

1. Choose Start > Run and type inetmgr.

2. Expand Web Sites and right click on Default Web Site and select Properties.

3. Substitute the new port number in the SSL port section and configure the firewalls and routers to allow through and port forward the new ports.

![Diagram of HMI Web Browser setup]

Figure 6: HMIWeb Browser

The following table shows the firewall access requirements between the HMIWeb Browser and the EBI server:

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote HMIWeb browser client</td>
<td>EBI server</td>
<td>80/TCP</td>
<td>HMIWeb browser – non-secure connection</td>
</tr>
<tr>
<td>Remote HMIWeb browser client</td>
<td>EBI server</td>
<td>80 and 443 TCP</td>
<td>HMIWeb browser – Secure connection</td>
</tr>
<tr>
<td>Remote HMIWeb browser client</td>
<td>EBI server</td>
<td>2910/TCP</td>
<td>Required if the point browser is required</td>
</tr>
</tbody>
</table>
Notes:

- Some system displays require the use of DCOM which utilizes a random port assignment and as such, it will not be possible to predetermine and configure the port configuration.

- If the HMIWeb browser client is on a different domain, then the EBI Server will need to be added to its list of trusted sites.

- For more information on the HMIWeb Browser configuration, see the “Configuring the EBI Web Server” chapter in the Configuration and Administration Guide.

Mobile access for Honeywell EasyMobile

Honeywell EasyMobile provides access to HVAC information in EBI from PDAs, mobile phones with web browsers, as well as browser access from a computer.

Honeywell EasyMobile can be used in the following network topologies:

- Through an Internet service provider (ISP)

- Through internal wireless access points (WAP)

![Diagram of network topologies]

Figure 7: Honeywell EasyMobile connecting through an ISP

To allow connections using Honeywell EasyMobile:

- It is recommended that HTTPS is used for both the internal and external firewall communications. Therefore the configured HTTPS port (443 by default) must be open.

- Set up a reverse proxy application in the DMZ.

- Configure rules on the internal firewall to allow traffic between the reverse proxy and the EBI server only.
Remote Access for Enterprise Applications

The following table shows the firewall access requirements between the Client applications and the subscribing server:

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Toolkit client</td>
<td>Subscribing server</td>
<td>50000/UDP</td>
<td></td>
</tr>
<tr>
<td>WebPoint Control client</td>
<td>Subscribing server</td>
<td>50000/UDP</td>
<td></td>
</tr>
<tr>
<td>Cardholder Services</td>
<td>Subscribing server</td>
<td>50200/TCP</td>
<td></td>
</tr>
</tbody>
</table>

The firewall access requirements between the Subscribing Server and the Publishing Server is as per the “Distributed Server Architecture” configuration as described on page 61.

Microsoft Windows Server Update Services

A Microsoft Windows Server Update Services (WSUS) server provides Microsoft Security Hot Fixes to nodes on the BCN.

In the following example the Microsoft WSUS in the DMZ gets Security Hot Fixes from the Microsoft WSUS in the business network, and provides these updates via Windows Update to servers and clients.
in the BCN. Under no circumstances should the DMZ server access the internet to get the updates to propagate to the BCN.

The firewall access required between the Microsoft WSUS server in the business network and DMZ is shown in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ Microsoft WSUS server</td>
<td>Microsoft WSUS server</td>
<td>DMZ</td>
<td>80/TCP</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

The firewall access required between the Microsoft SUS in the DMZ and the server and client nodes in the BCN is shown in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCN server or client</td>
<td>DMZ Microsoft WSUS server</td>
<td>BCN</td>
<td>80/TCP</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

**Honeywell Software Update Service**

Honeywell provides a solution for managing Microsoft Hotfixes, EBI software updates as well as policy enforcement as related specifically to EBI systems. This service, called Honeywell Software Update Service or SUS, provides a unified application for managing these security related components. SUS allows users to manage updates through a single interface. Users can configure download methods and times, notifications, and other settings to support the update process. Further, the Microsoft Hotfixes are made available through SUS as they are qualified by Honeywell. This
eliminates the guess work in determining what updates can be safely applied. In addition, SUS provides for the management of EBI updates.

SUS also provides a set of pre-defined Windows policies to harden systems against potential threats. Taken as a whole, SUS provides a useful and effective tool for systems management of EBI.

Note: Honeywell’s Service Online web site is not available to all regions of the world.

![Honeywell SUS Diagram](image)

**Figure 10: Honeywell Software Update Service**

A File Server in the DMZ connects to the Honeywell SUS Central server over the internet and downloads files from HSO. These files are then made available on the network via a network share. The SUS enabled nodes will connect to this file share and install the software updates.

The firewall access required between the Honeywell SUS Server central in the business network and the File Server in the DMZ is shown in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ File Server</td>
<td>Honeywell SUS Central Server</td>
<td>DMZ</td>
<td>80/TCP</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

The firewall access required between the File Server in the DMZ and the server and client nodes in the BCN is as per the “File Shares” configuration as described on page 63.

**Antivirus Update Server**

The Antivirus Update Server provides DAT file updates to nodes on the BCN.

In the following example the Antivirus Update Server in the DMZ gets antivirus DAT file updates from the Antivirus Update Server in the business network. In this way updated DAT files are provided to servers and clients in the BCN. Under no circumstances should the DMZ server access the internet to get the updates to propagate to the BCN.
There are two supported methods for distributing the DAT files: FTP and HTTP. You can use either of these methods. The firewall access requirements for both are shown below.

The firewall access required between the Antivirus Update Server in the business network and DMZ is shown in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ Antivirus Update server</td>
<td>Antivirus Update server</td>
<td>DMZ</td>
<td>80/TCP</td>
<td>HTTP</td>
</tr>
<tr>
<td>DMZ Antivirus Update server</td>
<td>Antivirus Update server</td>
<td>DMZ</td>
<td>21/TCP</td>
<td>FTP</td>
</tr>
</tbody>
</table>

The firewall access required between the Antivirus Update Server in the DMZ and the server and client nodes in the BCN is shown in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCN server or client</td>
<td>DMZ Antivirus Update server</td>
<td>BCN</td>
<td>80/TCP</td>
<td>HTTP</td>
</tr>
<tr>
<td>BCN server or client</td>
<td>DMZ Antivirus Update server</td>
<td>BCN</td>
<td>21/TCP</td>
<td>FTP</td>
</tr>
</tbody>
</table>
Connecting other nodes to the Building Control Network

There may be a requirement to connect non-Honeywell nodes to the BCN. This includes permanently connected computers associated with equipment such as analyzers, turbines, compressors, or metering systems, as well as laptop computers that are temporarily connected to the Building Control Network for configuration purposes such as CARE, LonMaker and LincNet.

Laptop computers

The portability of laptops poses a particular risk, as they can become infected elsewhere with malicious agents such as viruses or worms and spread these to the BCN.

As it is not possible to completely mitigate against this risk, Honeywell recommends that laptop computers not be connected to the BCN. Instead, you should adopt other approaches such as using the Radmin Server in the DMZ when you need to make configuration changes.

If this is not possible, you should check the state of a laptop before allowing it to be connected to the BCN. As a minimum you should do the following:

- Check the patch level of the operating system. If it is running Microsoft Windows, ensure that all current security Hot Fixes have been installed.
- Check the antivirus software on the laptop. The latest antivirus engine and virus definition files must be installed and properly configured.
- Perform a full system virus scan and view the log file to check that no files or directories were skipped, and that the virus scan successfully completed.
- Audit the software on the laptop to ensure compatibility of the laptop software with the control system software.

These audits and checks must be performed by a qualified independent person. The audit should not be undertaken by the user of the laptop. Standards for security Hot Fixes, antivirus software and compatible software must be in place before the audit is performed.

Once the state of the laptop has been verified, it can be connected to the BCN. If the laptop is disconnected from the BCN at any time and connected elsewhere, it must be checked again prior to reconnecting. It is strongly recommended that laptops not be used for web browsing prior to connection to the BCN.

Permanently connected non-Honeywell computers

Non-Honeywell computers connected to the BCN should conform to the recommendations in this document. This includes at a minimum:

- Up-to-date antivirus software
- Up-to-date Microsoft security Hot Fixes
- Strong passwords for all accounts
- A “least privilege” access model for users of the computer: users should only have access to resources required to perform their task.
Securing network equipment

The configuration of network equipment such as switches, routers, and firewalls is a critical part of the security for a Building Control Network. Each piece of this equipment should have a unique name and be secured by a strong password.

During normal operation, do not enable HTTP 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 Building Control Network’s infrastructure equipment (for example, switches and routers) should be disabled and then only enabled when needed through your site’s change management procedure.
Securing controller network interfaces

The configuration of controller network interfaces such as BNAs, LonWorks network interfaces and terminal servers are a critical part of the security for a Building Control Network. Each controller network interface that features a network based terminal session should be secured by a strong password.
Network Encryption

Honeywell network encryption implementations meet some US Government security requirements, specifically, those requirements coming from DCID 6/9 requiring 128 bit AES encryption.

The simplest methods of encryption are provided directly by specialized hardware, typically arranged in matched sets and configured for this application. The following diagram shows the system architecture with several hardware components that are appropriate for EBI network encryption and listed by UL for Honeywell use.
EBI Server PC – W7053H or W7054A Series
• Configurable for single or dual Ethernet networks, single or redundant or Distributed Server Architecture
• Supports AES Encryption of network data using NIST approved AES algorithms embedded in software for controller communications.

Network Router - 14507744 Series
74-3487 Specification Data
- Ethernet and T1 Interfaces
- UL864 Listed
- Supports AES encryption capability

Network Switch - 14507722 Series
74-3487 Specification Data
- 10/100 MB Ethernet
- 100BaseFX Fiber Optic Adapters
- UL864 Listed
Specify 14507725-001 (2 port fiber) OR 14507725-002 (4 port fiber) as additional options for each switch.

EBI Station PC – W7053H or W7054A Series
• Configurable for single or dual Ethernet networks, single or redundant or Distributed Server Architecture

Intelliguard 9000
74-3035 Specification Data
• Cost Effective Security Solution
• Meets UL Grade A A requirements.
• AES Line security with 14006700 series network adapter.

Deltanet FS90 Fire and Security Controller
74-3154 Specification Data
• Conventional and intelligent detection and signaling
• Stand-alone operation and/or integration with higher order systems
• Function boards for configuration to site requirements
• Grade AA High Security interface when AH High

Figure 12: Network Encryption
Network Planning

The following topics describe the bandwidth requirements of EBI system components within the Building Control Network. This information can be used for decisions on IP subnetting and switch/router configuration.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth requirements between Level 1 and Level 2 nodes</td>
<td>page 78</td>
</tr>
<tr>
<td>Bandwidth requirements between Level 2 nodes</td>
<td>page 78</td>
</tr>
<tr>
<td>Bandwidth and latency requirements between HMIWeb Browser and the EBI server</td>
<td>page 79</td>
</tr>
</tbody>
</table>

Bandwidth requirements between Level 1 and Level 2 nodes

EBI Server/Point Servers to Terminal Servers

To connect controllers to the EBI server, some controllers have their own Ethernet connection (e.g. the Honeywell XLS LAN Interface and Honeywell Excel Web controller), but many controllers only support serial communications. It is possible however, to connect some serial controllers to the Ethernet network with the aid of a device called a Terminal Server. This has the advantage of using existing Network infrastructure instead of having to run many serial cables.

The Terminal Server device has one network port and a number of serial or parallel connections. The controller communicates with the Terminal Server serially and then the Terminal Server communicates with the EBI via the network. A Terminal Server connects directly to the network so it does not need a network interface card. However, it may need a transceiver - a device that converts from one network cable type to another. Terminal Servers used with EBI must be both TCP/IP and Ethernet compliant. A number of terminal servers have been qualified for use with EBI. Please refer to the EBI Compatibility Matrix for a list of these devices.

*Required Network Bandwidth:* 80 Kbps per populated channel on the terminal server.

EBI Server/Point Servers to BNA

Each device has a different protocol and exchanges a different amount of information with the EBI Server but some testing has been done with R7044 connections and Excel 5000 interfaces.

*Required Network Bandwidth:* During testing of a representative configuration, the following bandwidth observations were made:

Between BNPS point server and BNA: Average 32kbps

Between Excel 5000 point server and BNA: Average 64kbps

Bandwidth requirements between Level 2 nodes

Station to EBI Server

This is the most typical use of networking in an EBI system. Station is client software that provides a graphical user interface to the EBI server. Any information entered by the operator is passed from Station to EBI. EBI passes system information back to Station via the network, which Station displays graphically to the operator.

All the required networking software to support a TCP/IP connection in the EBI server is included in the operating system software - no additional software is required.
**Required Network Bandwidth:** For systems using access control which requires the EBI Cardholder Management System (CMS), the bandwidth required for a station connection should be at least 256Kbps. This is because the CMS pages must be downloaded across the network every time they are used.

For systems not requiring the use of the Cardholder Management system (for example Building Management only systems), the minimum network bandwidth can be much lower as long as all display files are stored locally.

A Station needs to be able to access a set of display files, which define how each EBI display appears. There are two options for storage and maintenance of these files:

- Display files can be stored centrally on the EBI server. This is the more usual option for display file storage. Station PCs then map the EBI server disk drive, and load the display files dynamically as they are needed. This method reduces maintenance, but can increase display call up time on busy systems or over low speed network connections.

- Display files can be stored locally on each Operator Station. This method optimizes the speed of file loading, but adds some maintenance overhead - whenever a display is modified, the display file then needs to be updated on each machine.

**Required Network Bandwidth:** The average EBI display is between 100k bytes and 200k bytes. If you assume that an operator calls up 5 displays in a minute then the required bandwidth for serving displays would be approximately 16 Kbps per station. The other consideration is communications protocol. In an idle state, Station uses anywhere between 8 Kbps and 32Kbps. The recommendation is for a minimum of 256 Kbps to sustain a Station to EBI server connection. In practice, Stations are LAN-based so bandwidths of 10 – 100 Mbps (or more) are commonplace. For an optimal user experience these bandwidths are required.

**Required Network Latency:** Typically Stations are LAN-based so latencies of 10ms are commonplace. For an optimal user experience, a latency of 10ms is required. The larger the latency, the greater the impact on Station performance.

**HMIWeb browser to EBI Server**

The topology diagram shows HMIWeb browser at level 3 however it is possible (and valid) to have an HMIWeb browser at level 2. Regardless of what level the HMIWeb browser is in, the requirements are the same. For information about the bandwidth and latency requirements see Bandwidth and latency requirements between HMIWeb browser and the EBI server on page 79.

**Bandwidth and latency requirements between HMIWeb browser and the EBI server**

This type of access is useful to casual users who don’t need frequent access or require offsite access to EBI. For a connection to operate optimally there are minimum bandwidth and latency requirements.

A Browser needs to be able to access a set of display files which define how each EBI display appears. In general, these displays are hosted on the EBI Web Server. For normal usage, the displays should remain on the EBI Web Server. Under certain circumstances it may be required to host displays locally; this should only be done after consultation with support personnel. This is not generally recommended.

Tools are available to determine the latency between the computer where HMIWeb browser is installed and the EBI server. In general, the more hops that are involved in the communications path, the greater the latency and the less performant the connection will be.

**Minimum Required Network Bandwidth:** 256Kbps. Optimal usage is via a broadband connection of between 1.5Mbps and 8 Mbps.

**Network latency:** 300msec. Anything more than this may result in any of the following symptoms:

- Poor page callup performance
- Abnormally slow responses to user actions
• Script errors on system and custom displays.
Domain Name Servers

Whenever a TCP connection (that is, a DSA node, Station or other client tool) is made the system has to 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. Since users should not be web browsing from within the control network, the intended attack will not be successful, but a possible side affect will be that clients are unable to find the host, resulting in Station or DSA nodes being unable to connect.

Mitigating actions include:

1. Isolating the BCN DNS from the business LAN using firewall protection
2. Hardening the DNS, W200x has a registry setting which will cause the DNS to reject some false updates.
3. Using the local hosts file on each client machine 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 client must be manually updated if IP addresses change. One approach is to have a central copy of hosts which is copied to each node when required. This will also act as a backup should an individual hosts file become corrupted.

Unfortunately some malware also targets the hosts file, usually adding its own entries. This threat is greatly reduced by the presence of antivirus software, by setting tight file permissions on the file (by default only Administrators can modify it), and by marking the file as read-only. Should corruption still occur, then only one machine will be affected; if DNS corruption occurs, then all nodes will be affected.
Remote access

Remote access allows connection to the BCN from outside the business network using a customer’s corporate WAN or a direct Internet connection. The client typically connects 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 Remote Station Radmin Server located in the DMZ, and then uses various tools to reach the target system. Security aspects of the Remote Station Radmin Server configurations are discussed in “Remote Access Server” on page 125.

Such access may be used to:

- Perform remote control from home after normal hours or for emergency situations. In this case the client would connect to the Remote Station Radmin Server and would run Station on it.

- Perform engineering tasks on an EBI system in a remote building. In this case the client would connect to the Remote Station Radmin Server described in “Remote access for Station and Quick Builder” on page 65) and then run Station or Quick Builder as required.

- Perform remote support by Honeywell engineers or other support staff. In this instance more direct access to the target machine is needed and Remote Administrator (Radmin) would be used to reach the target machine.

- Remote direct machine 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.
Computer Names

All EBI server and client computers must have a unique name and IP address.

- The following restrictions apply when naming server and client computers:
  - The name must be 14 characters, or less, in length.
  - The name cannot contain spaces, hyphens (-), underscores (_), or other non-standard characters.
  - If you have a non-redundant server, avoid names (server and client) that end with "A" or "B". Although this is not mandatory, it makes it easier if you later want to upgrade to redundant servers.
  - If you have redundant servers, the names of the server computers have a common base name, plus a single-letter suffix. In the case of the primary server, the suffix is "A", and in the case of the backup server, the suffix is "B". For example, if the base name is HSSERV:
    - The primary server name would be HSSERVA
    - The backup server name would be HSSERVB
  - If you have redundant servers with a dual network configuration, the hostname that is used for each of the network interfaces will use the names of the server computers plus a zero (0) or a one (1) suffix. For example, if the base name is HSSERV, in the hosts file:
    - The primary server’s 1st network interface name would be HSSERVA0
    - The primary server’s 2nd network interface name would be HSSERVA1
    - The backup server’s 1st network interface name would be HSSERVB0
    - The backup server’s 2nd network interface name would be HSSERVB1

Notes:
The computer name is typically used for the hostname and SQL instance name.

Underscores (_) are prevented as they are not valid TCP/IP host names:
Hyphens (-) are prevented as they are not valid SQL instance names:
http://support.microsoft.com/default.aspx?scid=kb;en-us;257716

Attention: Renaming the EBI server computer has consequences for SQL Server. If you need to rename your server computer please refer to the section “Renaming the server computer” in the Configuration and Administration Guide.
Registering EBI Servers

In addition to the system number and license number entered during the EBI server installation, the EBI server requires a registration code. You request the registration code after installing the EBI server. Amongst other things, the registration code is associated with the MAC address of the computer on which the EBI server is installed. As such, if the computer or network interface is replaced, then the registration process will need to be carried out again. If a computer or network interface is required to be replaced on an EBI server, then it is advisable to plan in advance that the registration process will need to be carried out.
Honeywell recommends not allowing any system to have a network connection to both the building control and business networks. All connections between the Building Control Network and the business network should be through the firewall.
Port scanning

Only allow port scanning at the perimeter of your BCN, that is, from outside the firewall, pointing into the DMZ. Do not allow port scanning of online systems within the BCN, as this could lead not only to performance degradation but to system failure.
Third-party Applications

Honeywell does not recommend the installation and use of Third-party Applications on any BCN computers. This includes the EBI Server, point servers and Stations. 3rd party applications may affect the performance of these computers and perhaps even result in a loss of view of the building. Only those applications listed in the compatibility matrix, which have been tested and qualified should be installed on these computers.
Remote Monitoring Applications

Honeywell does not recommend the installation and use of remote monitoring and control applications, such as LANDesk Remote Control, on any BCN computers. This includes the EBI Server, point servers and Stations. These applications may affect the performance of these computers and perhaps even result in a loss of view of the building. Only those applications listed in the compatibility matrix, which have been tested and qualified should be installed on these computers.
Managed Ethernet Switches

Honeywell strongly recommends the use of managed Ethernet switches within the BCN, and that the port settings be manually configured based on the node type, as follows:

- 10MB Half Duplex: BNA-I (Q7750A)
- 100MB Full Duplex: Computers, BNA-II (Q7750B), Excel Web, LonWorks network interfaces and IP-852 routers, 10MB Terminal Servers
EBI has been qualified to operate on a VMware ESX and ESXi platform. This section describes considerations for hosting EBI in a virtual environment.

*Attention:* The information provided here is not designed to replace formal training on VMware. To successfully set up a virtual environment, we recommend that you receive formal training from an authorized VMware trainer.
Virtual environment architecture

Figure 13: shows an EBI server, point server and Station virtualized on an ESX host, as well as a Honeywell Digital Video Manager (DVM) database and DVM camera server virtualized on a separate ESX host, removing the need for six separate physical computers. Note that there are two networks shown. We recommend having a separate management network to isolate management operations such as cloning, creating snapshots and backup operations. This helps ensure that network performance is not degraded.

Attention: Where ESX host is used, this could be an ESX host or ESXi host.

The preceding figure shows a simple example of hosting EBI and DVM in a virtual environment. There are many options to consider when planning to host EBI in a virtual environment such as:

- Shared or network storage of images
  For more information about options for storing images, we recommend that you undertake VMware training.

- EBI redundancy
  Having redundancy ensures there is no loss of view of the facility if one of the servers fails. If you are hosting redundant EBI servers in a virtual environment, be aware that hosting redundant EBI server images on the same ESX host can create a point of failure for EBI if the ESX host becomes unavailable.

- EBI DSA
  If you are hosting an EBI server that is part of a DSA, the EBI server image/ESX host must be able to communicate with the other EBI servers in the DSA.

- UL security and fire systems
  Any systems requiring UL listing must be excluded from a virtual environment. Systems requiring UL listing must be installed on physical hardware that is UL listed.
Determining the requirements of the EBI system

To prepare a virtual environment that is suitable to host EBI, you need to work with the Honeywell representative to understand the type of EBI system that is being installed. The specifications you use to set up a virtual environment must be at least equivalent to the physical computer that can host EBI.

You should ask the following questions to help determine how to prepare the image that EBI is to be installed on:

- What is the required operating system?
- How many network cards are required?
- How many CPUs are required?
  The number CPUs required is determined by the performance requirements of the system. The EBI compatibility matrix lists the number of CPUs for each type of system.
- How much RAM is required?
  The amount of RAM required is determined by the performance requirements of the system. The EBI compatibility matrix lists guidelines for RAM requirements for each type of system.
- How much storage is required?
  The amount of storage required is determined by the performance requirements of the system. The EBI compatibility matrix lists the amount of storage for each type of system.
- Is the EBI server part of a DSA system?
  Are all of the EBI server images to be hosted on the same ESX host?
- Are the EBI servers redundant?
  Separate images are required for redundant servers. You need to determine if they will be hosted on the same ESX host and understand the implications if the ESX host becomes unavailable. Avoid creating a single point of failure.
- Are there any standalone point servers to be virtualized?
  A standalone point server requires a separate image and requires one CPU.
- Are Stations to be hosted in a virtual environment? If so, how many Stations are to be virtualized?
  The EBI compatibility matrix lists the hardware and software requirements for EBI servers, Stations, and point servers.

When you have determined the image requirements, you need to ensure that the ESX hardware can accommodate these requirements. The ESX hardware should have at least the equivalent processing power and RAM as all of the computers being virtualized.

The following requirements that apply to EBI installed on a physical computer also apply to EBI in a virtual environment:

- Computer names, see Computer Names on page 83.
- Bandwidth requirements, see Network Planning on page 78.
- Protection against viruses, see Virus protection on page 47.
- Microsoft Windows Updates, see Microsoft™ security updates and service packs on page 43.

We recommend that you reserve CPU and memory in the resource pool settings to ensure that the EBI server has the required resources to run correctly. If you are virtualizing an existing EBI system, it is a
good idea to work with the Honeywell representative to monitor the system and determine CPU usage and memory usage.

**Backup considerations**

Implement a backup strategy using the planning considerations in this guide. Do not use the VMWare snapshot function as a backup strategy. (Creating snapshots increases the amount of hard disk space used and can hinder performance.)

**Security considerations**

For EBI to be successfully installed on an image you have prepared, the Honeywell representative responsible for installing EBI must have administrative privileges for that image.

The Honeywell representative also needs to connect to the ESX from a laptop or computer. A thin client cannot be used to install the EBI software.

Other security considerations that apply to EBI installed on a physical computer also apply to EBI in a virtual environment.
Securing wireless devices

When planning to connect wireless devices to your EBI system, you need to consider the following:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless devices</td>
<td>page 95</td>
</tr>
<tr>
<td>Conducting a radio frequency survey</td>
<td>page 96</td>
</tr>
<tr>
<td>Configuring and securing wireless access points (WAPs)</td>
<td>page 97</td>
</tr>
<tr>
<td>Connecting wireless devices</td>
<td>page 98</td>
</tr>
</tbody>
</table>

The information in this guide on securing wireless devices is intended to provide high-level guidance for users with knowledge of, and experience with, installing wireless systems. It is therefore assumed that readers will be familiar with terminology such as MAC address, PEAP, RADIUS, and SSID.
About EBI wireless devices

The EBI system can be configured to work with wireless mobile productivity devices. These devices connect through commercially available wireless access points (WAP). WAPs are typically connected to a wired network, which connects the wireless devices and servers on the wired network.

Because this connection can represent a significant security risk for the servers and other parts of the wired network, it is essential that the recommendations for connecting the WAPs in this guide are followed.
Radio frequency survey

Prior to deploying wireless devices, a radio frequency (RF) survey should be carried out to determine:

- Areas of the facility where wireless access is needed
- Areas of the facility where wireless access should not be allowed or made available.
- The number and placement of Wireless Access Points (WAPs)
- Antenna strengths for each WAP.
Configuring and securing WAPs

The basic implementation of a wireless device connection is shown in the diagram below. This shows the components of the network used to secure the wireless access point (WAP). Components that communicate with the wireless devices for data are described in subsequent sections.

Figure 14: Wireless Point Device
Connecting wireless devices

The wireless device should not connect directly to the BCN. It is recommended that the WAP be connected to a separate network segment, separated from the network by a firewall. The WAP must have access to a Microsoft Windows domain controller which is running Microsoft’s Internet Authentication Service (IAS). IAS supports the 802.1x RADIUS protocol, which is used to securely authenticate the wireless device. This can be a domain controller in the BCN or the business networks.

The domain controller and IAS

The domain controller provides an additional layer of protection for the network. Traffic from the wireless device is blocked until the user has authenticated with the domain controller using RADIUS. Microsoft supports RADIUS in Windows Server 2003 as part of the Internet Authentication Services (IAS) package. For detailed guidance on configuring wireless access with RADIUS see the Windows Server 2003 documentation.

Information on RADIUS is available in RFCs 2138, 2139, 2865 and 2866 of the IETF http://www.ietf.org

Firewalls

When wireless devices are used on an EBI network, the firewall should be configured to only allow traffic between:

- The domain controller running RADIUS (see “The domain controller and IAS” on page 98).
- The nodes being accessed by the wireless devices
- The WAP(s)

The firewall access required between the WAP in the wireless network and domain controller running IAS is shown in the following table.

<table>
<thead>
<tr>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Interface</th>
<th>Ports/Service</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Access Point</td>
<td>Domain Controller IAS</td>
<td>Wireless Network</td>
<td>1812/UDP</td>
<td>RADIUS 802.1x</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>Domain Controller IAS</td>
<td>Wireless Network</td>
<td>1813/UDP</td>
<td>RADIUS 802.1x</td>
</tr>
</tbody>
</table>

Configuring WAPs

When configuring a wireless access point (WAP) it is recommended that you:

- Configure a unique SSID. Do not use the default SSID.
- Disable SSID broadcast.
- Configure authentication for EAP authentication to the Network. PEAP is preferred.
- Configure the RADIUS server address.
- Configure for dynamic WEP.
- Configure 802.1x authentication.
- Enable MAC filtering and enter MAC addresses for wireless Stations.

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

**Wireless network interface cards**

The wireless device will contain a wireless network interface card. The following configuration recommendations should be followed:

- Configure the proper SSID
- Configure 802.1x authentication
- Configure WEP with key supplied from WAP
- Configure Protected EAP authentication Note: both PEAP-TLS and PEAPMS-CHAP are supported.
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.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Microsoft Baseline Security Analyzer</td>
<td>page 101</td>
</tr>
<tr>
<td>Setting up and analyzing audit logs</td>
<td>page 102</td>
</tr>
<tr>
<td>Detecting network intrusion</td>
<td>page 104</td>
</tr>
<tr>
<td>Setting up an event response team</td>
<td>page 106</td>
</tr>
</tbody>
</table>
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 other installation components such as Internet Information Services (IIS) and SQL Server. It also checks whether or not 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 in order to download the latest information on Hot Fixes, service packs, and so on. However, MBSA2.0 can be configured to use its registered Update Services server for this purpose, see Microsoft Windows Server Update Services on page 69. It only takes a few minutes to run and generates a series of reports on the security health of a system.

Attention: Do not run the IIS Lock Down Tool from Microsoft™ which the MBSA tool will recommend. Doing so will damage the system and render EBI inoperable. Please contact your Honeywell representative for more information.
Setting up and analyzing 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.

Once auditing is enabled, the audit logs should be reviewed frequently by a responsible person, who can take action 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, select Log > Security and then select Log > Log Settings. Then change either the Maximum Log Size, or the Event Log Wrapping options.

You should ensure that the audit log is regularly inspected and cleared, or else disable the security option “Audit: shut down system immediately if unable to log security audits”.

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.

To enable auditing:

Either:

- Set the appropriate Group policy, or

- Log on as the Local Administrator and
  - Start the User Manager tool.
  - Select Policies > Audit and enable options of interest.

The most useful options are likely to be:

- Logon and Logoff - success and failure
- Process Tracking - success and failure
- Object access - success and failure

This enables the auditing of file system and registry access. It is then necessary to choose the objects of interest and the user (or groups) whose actions are to be audited. Note that since it is necessary to specify an identity to audit (and by definition, it is not known who the intruder is), you should specify the group “Everyone”.

To configure the auditing of file access:

1. Go to Windows Explorer and select the directory or file of interest.
2. Select Properties > Security > Advanced > Auditing.
3. Then add a user, for example, “Everyone” and the access to be audited; for example, “Open failure”.

To configure the auditing of registry keys:

1. Run regedt32.
2. Select the key for which you want to set up auditing.
3. Select Permissions > Advanced > Auditing and add users as above.

To enable the auditing of EBI database access:

1. Before starting the database service, give the “Everyone” account “Generate security audits” rights.
2. Enable audit object access. This will ensure that any attempt by an executable to open the EBI database will also generate a security log entry.
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 take action 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 whereby they can report various levels of events, varying from debugging to emergency failure. These reports can be either viewed via telnet, collected by a central logging server, or be sent via e-mail 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 be detected.

Syslog servers commonly exist on UNIX systems, but third party syslog services are available for Windows. They vary in functionality and cost from freeware, which simply writes to a log file, to sophisticated IDS 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 also 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 between 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.xxx dst inside:xxx.xxx.xxx.xxx (type 0, code 0) by access-group "outside_access_in"
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://www.microsoft.com/technet/security/guidance
http://www.sans.org/resources
http://csrc.nist.gov
In planning your system, you also need to consider how the Windows-based nodes in the Building Control Network will fit into the IT infrastructure, and how users will be given access to both the Building Control Network and the business network. This is achieved through the use of Windows domains and workgroups.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>About domains</td>
<td>page 108</td>
</tr>
<tr>
<td>Domain forests and trees, and DNS</td>
<td>page 110</td>
</tr>
<tr>
<td>Domains and Building Control Networks</td>
<td>page 110</td>
</tr>
<tr>
<td>Domains vs. workgroups</td>
<td>page 111</td>
</tr>
<tr>
<td>Inter-domain trusts</td>
<td>page 112</td>
</tr>
</tbody>
</table>
About domains

A Windows *domain* is a collection of computers that share a common domain database and security policy. A domain is managed by a *domain controller*, the server that authenticates domain logons and that maintains the security policy and the master database for a domain. Each domain, and each computer within that domain, has a unique name. A *Domain Name Server* (DNS) is used for the transparent translation of computer names to IP addresses when connections are made.

The operating system for domain controllers in an R410 EBI system can be either Windows Server 2003 R2 or Windows XP Professional SP2.
Organizations and Group Policy

Windows domains also use Organization Units (OU). An OU is a group of objects (for example, 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:

- Microsoft Windows 2003 Deployment Kit (see the topic “Designing and Deploying Directory and Security Services”)
Windows domains: forests, trees, and DNS

Domains in Windows Server 2003 are significantly more flexible and more complex than in Windows NT 4.0. Domain concepts such as forests, trees, and dynamic DNS allow users to closely integrate Windows 2003 domains in IT and building management.

It is important to understand and be familiar with these concepts before installing a new Windows 2003 domain, or upgrading existing Windows NT 4.0 domains, 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. Honeywell recommends that the building management and IT departments liaise closely to determine the best method of integrating the business IT infrastructure with the building management domain architecture.

Domain membership and Building Control Networks

Active Directory’s scalability allows the largest of organizations to utilize a single domain implementation. At this time, however, Honeywell recommends that customers maintain a separate Windows domain for Building Control Network systems in order to accommodate building management requirements.

A separate domain for the Building Control Network has the following advantages:

- Increased security and reliability
- Centralized and independent management of security
- The ability to customize security policies for the Building Control Network
- Changes to the business domain do not affect the Building Control Network

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 Building Control Network not be in a forest or tree that includes the business network domain.
Workgroup limitations

A workgroup, or peer-to-peer network, is a low-cost option commonly used for small business networks. In this model, computers directly communicate with each other and do not require a domain controller to manage network resources. In general, a peer-to-peer network is most appropriate for networks with a small number of computers (say, less than five), all located in the same general area. The computers in a workgroup are considered peers because they are all equal and share resources among each other without requiring a server. Users determine which data on their computer will be shared with the network. Sharing common resources allows users to print from a single printer, to access information in shared folders, and to work on a single file without transferring it to a floppy disk.

The main disadvantages of workgroups are:

- The requirement to manually configure user accounts on all participating nodes
- The low security protocol used for authentication between nodes
Inter-domain trusts

Inter-domain trusts are used to allow users in one domain to access resources on a different domain. Native Windows Server 2003 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 Building Control Network and business network domains. If 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 2003 domains.

Note that this does not prevent users from the business domain making Station connections if they provide credentials (user name and password) that are valid on the EBI server in the Building Control Network domain.

If Stations do reside on the same domain as the EBI server then single signon for operators is possible; that is, Station will be able to automatically connect to EBI using the same credentials as those used when the operator logged onto the Station computer. For more information, see “Single signon” on page 141.
An essential component of any security strategy for a Building Control 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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows user accounts and passwords</td>
<td>page 114</td>
</tr>
<tr>
<td>System services</td>
<td>page 119</td>
</tr>
<tr>
<td>File system and registry services</td>
<td>page 122</td>
</tr>
<tr>
<td>Other Microsoft services</td>
<td>page 124</td>
</tr>
<tr>
<td>Windows XP SP2 and Windows Server 2003 SP1 security enhancements</td>
<td>page 126</td>
</tr>
<tr>
<td>Windows 2003 registry and other settings</td>
<td>page 129</td>
</tr>
</tbody>
</table>
Windows user accounts and passwords

Access is gained to the Windows operating system by logging onto the system 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.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>User account policies and settings</td>
<td>page 115</td>
</tr>
<tr>
<td>Password policies and settings</td>
<td>page 117</td>
</tr>
</tbody>
</table>
User account policies and settings

As a general rule you should:

• Review user accounts on a regular basis.

• Disable or delete all unused accounts.

• Disable all guest accounts.

EBI operator accounts

EBI operator accounts should be set up as follows:

• Enable them to log in only to operator Stations.

• 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 nodes for maintenance activities should be enabled to log in to all building management nodes.

New accounts

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

Where EBI operator-based security is configured, similar care must be taken in choosing passwords. For more information about operator-based security see the topic “Adding an operator” in the chapter “Configuring system security and site parameters” of the Configuration and Administration Guide.

Administrator accounts

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

Note also 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 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.

For more information about Administrator accounts, see “Administrators” on page 136.
Service and server accounts

Windows 2003 services and COM servers should run under an account with the lowest possible set of
privileges. The account should not have the “Logon Interactively permitted” permission set.

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

- Local “service” account (valid on Windows XP and Windows 2003 only)
- Local accounts with minimum rights. Most EBI services run under the local account MNGR.
- Domain accounts with minimum rights
- “Network Service” account (valid on Windows XP and Windows 2003 only)
- Local or domain user belonging to the Local Administrators group
- Local “system”

Running services under the local “system” should be avoided if at all possible as compromised
processes running under this account have rights to “act as part of the operating system” and can do
anything they wish on the computer. In Windows Server 2003 a new account, “local server” 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.

#### Password settings

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

The following settings are suggested.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum password age</td>
<td>45 to 90 days</td>
<td>Forces the choice of a new password after this time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The setting for the Administrator account should be shorter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A maximum of 30 is recommended.</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 to 5 days</td>
<td>Prevents too rapid cycling of passwords.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>8 characters</td>
<td>Improves encryption and makes guessing harder.</td>
</tr>
<tr>
<td>Password uniqueness</td>
<td>8 to 13 old</td>
<td>Prevents reuse of the same password too quickly.</td>
</tr>
<tr>
<td></td>
<td>passwords</td>
<td></td>
</tr>
<tr>
<td>Account lockout</td>
<td>10 attempts</td>
<td>Prevents continual password guessing by disabling account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>after the specified number of attempts. Consider disabling account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lockout for operator (or other user) accounts where denial of service or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>loss of view would be detrimental to safety or the continued operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of the plant.</td>
</tr>
<tr>
<td>Lockout duration</td>
<td>30 minutes</td>
<td>Specifies the period of time during which a user will not be able to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>log on following an account lockout. (Note that the administrator can</td>
</tr>
<tr>
<td></td>
<td></td>
<td>re-enable the account before the expiration of the specified lockout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>period.)</td>
</tr>
<tr>
<td>Lockout counter</td>
<td>29 minutes</td>
<td>The time before the account lockout is reset to zero.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, with the account lockout set at 10, and the lockout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>counter set at 29 minutes, lockout will occur if there are 10 invalid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon attempts within 29 minutes. Note that the lockout counter must be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>less than the lockout duration.</td>
</tr>
</tbody>
</table>

The following settings are configured by default by the Honeywell SUS:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password age</td>
<td>15 days</td>
<td></td>
</tr>
<tr>
<td>Account lockout</td>
<td>3 attempts</td>
<td></td>
</tr>
<tr>
<td>Lockout duration</td>
<td>5 minutes</td>
<td></td>
</tr>
</tbody>
</table>
**Strong passwords**

It is recommended that you enforce strong passwords, that is, passwords consisting of at least 8 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 through Z)
- English lowercase characters (a through z)
- Numbers (0 through 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.

An alternative way of increasing password complexity is to recommend the use of a pass phrase, for example, “the cow jumped over the moon” 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.

**Account lockout**

The lockout values shown in Table on page 117 are those suggested by Microsoft and are discussed in their white paper “Account Lockout Best Practices”

- Account Lockout Best Practices.doc is available from:

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, who will capture logon packets and use 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 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 EBI itself runs as a set of these services, many of the system default services are not needed by EBI. They do, however, provide avenues for malicious network attack and should be disabled. This can be performed through the Services tool by choosing Control Panel > Administrative Tools > Services.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services required by Windows 2003</td>
<td>page 119</td>
</tr>
<tr>
<td>Services required by EBI</td>
<td>page 120</td>
</tr>
<tr>
<td>Services required by antivirus Programs</td>
<td>page 121</td>
</tr>
</tbody>
</table>

Services required by Windows 2003

The following table lists required services on Windows 2003. Depending on your EBI license options, all other services should be disabled.

<table>
<thead>
<tr>
<th>Display Name / Core System</th>
<th>Service</th>
<th>Required?</th>
<th>Dependent on?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Browser</td>
<td>browser</td>
<td>Y</td>
<td>lanmanserver, lanmanworkstation</td>
</tr>
<tr>
<td>COM+ Event System</td>
<td>eventsystem</td>
<td>Y</td>
<td>rpcss</td>
</tr>
<tr>
<td>Distributed Link Tracking Client</td>
<td>Trkwks</td>
<td>Y</td>
<td>rpcss</td>
</tr>
<tr>
<td>Distributed Transaction Coordinator</td>
<td>Y(ii)</td>
<td>Rpcss, lsass</td>
<td></td>
</tr>
<tr>
<td>DNS Client</td>
<td>dnscache</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Event Log</td>
<td>eventlog</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>IIS Admin Service</td>
<td>iisadmin</td>
<td>Y (ii)</td>
<td>rpcss, protectedstorage, lsass</td>
</tr>
<tr>
<td>IPSEC Policy Agent</td>
<td>Policyagent</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Logical Disk Manager</td>
<td>dmserver</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>MSSQLSERVER</td>
<td>MSSQLSERVER</td>
<td>Y (ii)</td>
<td></td>
</tr>
<tr>
<td>Net Logon</td>
<td>Netlogon</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Network Connections</td>
<td>netman</td>
<td>Y</td>
<td>rpcss</td>
</tr>
<tr>
<td>Routing and Remote Access</td>
<td>RemoteAccess</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Remote Procedure Call (RPC)</td>
<td>rpcss</td>
<td>Y</td>
<td>rpcss</td>
</tr>
<tr>
<td>Plug and Play</td>
<td>plugplay</td>
<td>Y</td>
<td>rpcss</td>
</tr>
<tr>
<td>Protected Storage</td>
<td>protectedstorage</td>
<td>Y</td>
<td>rpcss</td>
</tr>
<tr>
<td>Print Spooler</td>
<td>spooler</td>
<td>Y</td>
<td>rpcss</td>
</tr>
<tr>
<td>Security Accounts Manager</td>
<td>lsass</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>lanmanserver</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>simple mail service (optional for pager)</td>
<td>smtpsvc</td>
<td>Optional (iv)</td>
<td></td>
</tr>
<tr>
<td>System Event Notification</td>
<td>sens</td>
<td>Y</td>
<td>EventSystem</td>
</tr>
</tbody>
</table>
The installation instructions for Internet Information Services (IIS) are documented in the EBI Installation Guide.

Not required for client nodes.

Required for Event Archiving/Email notification for Alarm Pager

Pager may be configured to use a mail server. This could be SMTP, but other mail servers are possible.

**Services required by EBI**

The following table lists services that run on an EBI server. Depending on your EBI license options, other services may be disabled.

<table>
<thead>
<tr>
<th>Display Name / Core System</th>
<th>Service</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aegis Central Service</td>
<td>AegisCentralService</td>
<td>Optional</td>
</tr>
<tr>
<td>Axcess</td>
<td>Axcess Point Server</td>
<td>Optional</td>
</tr>
<tr>
<td>Axcess DCFR</td>
<td>DCFR</td>
<td>Optional</td>
</tr>
<tr>
<td>BACnet Point Server</td>
<td>BACnet point server</td>
<td>Optional</td>
</tr>
<tr>
<td>BACstac Protocol</td>
<td>BACstac</td>
<td>Optional</td>
</tr>
<tr>
<td>Building Network Point Server</td>
<td>SDA</td>
<td>Optional</td>
</tr>
<tr>
<td>BNPS Redundancy Service</td>
<td>BNSPSRDN</td>
<td>Optional</td>
</tr>
<tr>
<td>Central Event Programs</td>
<td>EBIEventProg</td>
<td>Optional</td>
</tr>
<tr>
<td>Crypkey License</td>
<td>Crypkey License</td>
<td>Optional</td>
</tr>
<tr>
<td>EBI Server Daemon</td>
<td>hscserver_daemon</td>
<td>Y</td>
</tr>
<tr>
<td>EBI Server Database</td>
<td>hscserver_database</td>
<td>Y</td>
</tr>
<tr>
<td>EBI Server Desktop</td>
<td>hscserver_desktop</td>
<td>Y</td>
</tr>
<tr>
<td>EBI Server Logger</td>
<td>hscserver_serverlogger</td>
<td>Y</td>
</tr>
<tr>
<td>EBI Server Operator Management</td>
<td>hscserver_oprmgmt</td>
<td>Y</td>
</tr>
<tr>
<td>EBI Server System</td>
<td>hscserver_system</td>
<td>Y</td>
</tr>
<tr>
<td>Echelon LNS Server</td>
<td>lnssrv</td>
<td>Optional</td>
</tr>
<tr>
<td>Energy Manager Analysis</td>
<td>EMAnalysis</td>
<td>Optional</td>
</tr>
<tr>
<td>Energy Manager Data Import</td>
<td>EMDDataImport</td>
<td>Optional</td>
</tr>
<tr>
<td>Energy Manager Internet RTP</td>
<td>EMInternetRTP</td>
<td>Optional</td>
</tr>
<tr>
<td>Energy Manager Internet Weather</td>
<td>EMInternetWeather</td>
<td>Optional</td>
</tr>
<tr>
<td>Energy Manager Point Build</td>
<td>EMPPointBuild</td>
<td>Optional</td>
</tr>
<tr>
<td>Energy Manager Point Server</td>
<td>EMPPointServer</td>
<td>Optional</td>
</tr>
<tr>
<td>Service</td>
<td>Display Name / Core System</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Energy Manager Rates Engine EMRates</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Energy Manager Server EMServer</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Excel 5000 Direct Excel 5000 direct</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Fire Point Server FEA</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Fire Point Server Redundancy SRDN</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>HDX Browser Service HDXBrowserService Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Schedules Download Manager GSDownloadManager</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Honeywell Integrated Maintenance Manager IMMmgr</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Honeywell Server OPC Data Transfer HscOpCIEngine</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Honeywell Service Framework ServiceFramework Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Honeywell SUS Agent Honeywell SUS Agent</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Honeywell SUS Framework Honeywell SUS Framework</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Honeywell Web Point Control ScheduleService</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>LCBS Point Server LCBS PS</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>LonWorks Point Server LonWorks Point Server</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>MSSQL Server OLAP Service MSSQLServerOLAPService</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Network DDE NetDde</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Network DDE DSDM NetDcDsDM</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Remote Sync Server Remote Sync Server</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Rslinx</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Temaline Service TemaService</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>XL5000 OpenViewNet OVNRouter</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>XLNET Daemon HSCSERVER_XLNET_Daemon</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

**Services required by antivirus Programs**

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

<table>
<thead>
<tr>
<th>Display Name / Core System</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Associates McShield</td>
<td>McShield</td>
</tr>
<tr>
<td>Network Associates Task Manager</td>
<td>McTaskManager</td>
</tr>
<tr>
<td>McAfee Framework Service McAfFeFramework</td>
<td></td>
</tr>
<tr>
<td>Norton AntiVirus Server Norton AntiVirus Server</td>
<td></td>
</tr>
</tbody>
</table>
File system and registry protection

Windows protects objects, including files, directories and registry keys, with Access Control Lists (ACLs). An ACL is a list of user accounts and groups, in which each entry specifies a set of allowed or disallowed actions.

- In the case of a file, actions include open, read, write, modify permissions, and so on.

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

ACLs are discretionary in that they 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 node. 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 EBI installation will apply ACLs to its directories and registry tree.

ACL protection can only be applied to files and directories if the containing file system is in NTFS format. EBI 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 configuration files such as those used by qckbld, and archived data such as history 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.

Managing file system ACLs

As installed, the file system ACLs provide good security. Access to the \Honeywell\Server subtree is set up as follows:

- Administrators are given full access.

- Honeywell Administrators are given full access.

- All other users have no access.

Attention: 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 EBI from operating correctly.

To manage file system ACLs:

1. In Windows Explorer, select the file or directory.
2. Right-click and select Properties > Security. This will show a list of users and groups for which access is specified.
3. Selecting a specific user will show their access permissions. You can change these if necessary.
Managing registry ACLs

Attention: 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.

To manage registry ACLs:

1. Using regedt32, select the registry key that you want to protect.
2. Choose Edit > Permissions. A dialog box similar to that provided by Windows Explorer will appear.

Managing file shares

File shares should also 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.

EBI uses file shares as follows:

- Distributing reports to Station users requires read access by Station users
- Distributing Station displays requires:
  - “read” access by Station users
  - “write” access if users need to build displays
- Quick Builder uploads and downloads require “write / file create” access by building engineers.

Thus EBI file shares should be set up to give the Honeywell Administrators group (engineers) “change access” and the Station users group “read access”.

Other Microsoft services

EBI relies on the presence of several Microsoft services that need to be configured securely.

<table>
<thead>
<tr>
<th>Service</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Information Services</td>
<td>page 124</td>
</tr>
<tr>
<td>SQL Server</td>
<td>page 124</td>
</tr>
<tr>
<td>Remote Access Server</td>
<td>page 125</td>
</tr>
</tbody>
</table>

Internet Information Services

Attention: Internet Information Services (IIS) is mandatory for EBI

IIS 6.0, as installed on Windows 2003, has most options disabled by default, unlike IIS 5.0 which had to have unwanted options disabled by use of the IIS Lockdown tool. The installation instructions for IIS 6.0 and details of the components required for EBI are documented in the EBI Installation Guide.

It is strongly recommended that you run the Microsoft Baseline Security Analyzer (see “Using Microsoft Baseline Security Analyzer” on page 101).

In setting up and maintaining IIS you should also:

• Keep the number of virtual directories to a minimum. These are the access points used by the outside world, and will therefore be the target for hackers.

• As a general rule do not place executable .asp or .aspx files and read only .html files in the same directory:
  – Directories containing HTML should have read-only permission
  – Directories containing ASP files should have execute-script permission only

• Never have network share directories within a virtual directory tree. If a user can write an .html or .asp file within a virtual directory, then that page can be executed by a browser and, with the help of scripting, can do untold damage to the system; for example they can delete files. File and directory permissions may be further contained with NTFS security options. IIS will compare its own permissions with those of NTFS and use the most restrictive.

SQL Server

The following information details EBI requirements in relation to SQL Server. If other databases are hosted by the EBI SQL Server, then their own security model must also be applied.

EBI processes use integrated authentication to access the SQL database through the Honeywell Administrators group account.

The following security recommendations apply to SQL Server:

• Where possible, do not give users access to multiple databases.

• Run Microsoft Baseline Security Analyzer (see “Using Microsoft Baseline Security Analyzer” on page 101) on your SQL Server.

• It is recommended that the default passwords for SQL logins be changed as soon as possible after installation.
Note that EBI installation process sets authentication to “Windows only” and ensures that the sa password is not blank.

Microsoft CALs (Client Access Licenses)
A Microsoft SQL CAL is required for each number of the following connections to the EBI Server:
- Station
- HMIWeb Browser
- WebPoint control client

The EBI software license indicates how many Microsoft SQL CALs that the system is licensed for.

Remote Access Server
The Remote Access Service (RAS) allows remote workstations to establish a dial-up connection to a LAN and access resources on the LAN as if the remote workstation were on the LAN; that is to provide “terminal services” like functionality over a dial-up line.

It is important to secure RAS if it is available and configured in your system. RAS can be used to allow dial-up access for engineers running a remote Station, or for an administrator when performing remote diagnostics, but can also be a significant security risk.

Follow these guidelines:
- Only give dial-in access to those users who need it.
- Revoke this right as soon as the need has passed.
- Ensure that their passwords are strong, and are changed frequently.
- Configure RAS to use encrypted authentication to prevent password stealing.
- If the computer is connected directly to a modem, consider limiting the valid TCP/IP ports available for connection.
- Configure RAS to use the Caller ID or the callback function
Windows XP SP2 and Windows Server 2003 SP1 security enhancements

Microsoft Windows XP SP2 and Windows Server 2003 SP1 add significant security enhancements to the operating system. These include the following:

- **DCOM**
  Permissions for launching and accessing DCOM servers have changed.
  It is necessary to add the Honeywell Administrators group to the machine wide COM ACL to allow members launch and access permissions.
  In addition, it is necessary to give Honeywell Administrators activation permission to the following COM servers:
  - GDA Notification Client
  - GDA Notification Server
  - GDA Manager
  - HSC Operator Management

- **RPC (the DCOM transport mechanism)**
  The most significant changes are that all anonymous connections are refused, and authenticated RPC over UDP connections are also refused.
  While these security enhancements are supported by EBI R410, some of the changes may cause problems in some EBI systems where there are:
  - Pre-R400 EBI DSA servers
  - OPC connections (for example, Honeywell OPC Server, OPC Data Transfer, or other third party OPC connections)

In these cases, it will be necessary to disable the new security settings. This is achieved by creating two registry keys and setting the value as described below:

<table>
<thead>
<tr>
<th>Type</th>
<th>Location</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DWORD</td>
<td>HKLM\Software\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients</td>
<td>0</td>
</tr>
<tr>
<td>DWORD</td>
<td>HKLM\Software\Policies\Microsoft\Windows NT\RPC\EnableAuthEpResolution</td>
<td>0</td>
</tr>
</tbody>
</table>

The EnableAuthEpResolution key will make the endpoint mapper service perform authenticated calls if its value is set to 1.
The RestrictRemoteClients key will cause the node to only accept authenticated RPC/TCP calls if the value is set to 1.
Therefore if RestrictRemoteClients = 1, then EnableAuthEpResolution should be 1 as well.

- **Host firewall**
  Under Windows XP SP2 and Windows Server 2003 SP1 the host-based firewall will by default reject any incoming connections. (Note that this is not the case when SP1 is applied to an existing Windows Server 2003 installation. Installing EBI will, however, enable the Windows host firewall.)
The Windows Firewall has an exception list where executables or ports can be registered to bypass any filtering. The executables and ports will be set dependant on the licensed EBI options. The hsconfig tool will automatically configure the required firewall settings, and is performed as part of the EBI installation, but may be run again afterwards.
The following table lists the core EBI executables that are added by fwconfig:

<table>
<thead>
<tr>
<th>Executable</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bacnet Point Server</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>BACnet Utilities</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>BACSTAC</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>cfgsum</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>confd.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dbrepsrv.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>DLL Host</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dsacksync.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dsdc.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dsredcli.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dsredsrv.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dual_flsrv.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dual_linkd.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dual_onsrv.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>dual_pswd.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>eventsdc.exe</td>
<td>EBI pointserver component</td>
</tr>
<tr>
<td>Excel 500 Daemon</td>
<td></td>
</tr>
<tr>
<td>Excel 500 Firmware Download</td>
<td></td>
</tr>
<tr>
<td>Excel 500 Scan Task</td>
<td></td>
</tr>
<tr>
<td>Excel 500 Time Schedules</td>
<td></td>
</tr>
<tr>
<td>Excel 5000 Point Server</td>
<td></td>
</tr>
<tr>
<td>filerep.exe</td>
<td></td>
</tr>
<tr>
<td>gdamngr.exe</td>
<td></td>
</tr>
<tr>
<td>gdanotcli.exe</td>
<td></td>
</tr>
<tr>
<td>gdanotsrv.exe</td>
<td></td>
</tr>
<tr>
<td>gdaserver.exe</td>
<td></td>
</tr>
<tr>
<td>HMIWeb Station</td>
<td></td>
</tr>
<tr>
<td>hscodebn.exe</td>
<td></td>
</tr>
<tr>
<td>iLON Configuration Server</td>
<td></td>
</tr>
<tr>
<td>Inetinfo</td>
<td></td>
</tr>
<tr>
<td>LNS Server</td>
<td></td>
</tr>
<tr>
<td>LonMaker for Windows</td>
<td></td>
</tr>
<tr>
<td>Lonworks POET DB Server</td>
<td></td>
</tr>
<tr>
<td>Lonworks Point Server</td>
<td></td>
</tr>
<tr>
<td>ms_dfid</td>
<td></td>
</tr>
<tr>
<td>Program</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>nifd.exe</td>
<td></td>
</tr>
<tr>
<td>opcscn.exe</td>
<td></td>
</tr>
<tr>
<td>PointServer DC</td>
<td></td>
</tr>
<tr>
<td>Quick Builder</td>
<td></td>
</tr>
<tr>
<td>ripsd.exe</td>
<td></td>
</tr>
</tbody>
</table>
**Windows 2003 registry and other settings**

Windows 2003 has many registry settings that can be used to increase the overall security of a system. Note, however, that extreme caution needs to be exercised when making any changes to the registry. For more information, see “Managing registry ACLs” on page 123.

The following table lists the main settings and recommendations. For further information see Microsoft’s white paper, *Windows Server 2003 Security Guide*.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure the desktop</td>
<td>page 129</td>
</tr>
<tr>
<td>Disable unused subsystems</td>
<td>page 130</td>
</tr>
<tr>
<td>Restrict anonymous logon</td>
<td>page 130</td>
</tr>
<tr>
<td>Use NTLM Version 2</td>
<td>page 130</td>
</tr>
<tr>
<td>Disable the caching of previous logons</td>
<td>page 130</td>
</tr>
<tr>
<td>Harden the TCP/IP stack</td>
<td>page 130</td>
</tr>
<tr>
<td>Security Templates</td>
<td>page 131</td>
</tr>
</tbody>
</table>

**Secure the desktop**

The following recommendations apply to desktop policy settings:

- Configure Windows to display a warning against unauthorized use of the computer.
  
  With Windows Server 2003 you can configure computers to display a message when someone logs on. A typical message would be:

  **It is an offense to continue without proper authorization**

  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 Server 2003 domain) or the local registry to:
  
  - Hide the last user’s name on the logon window. By default, the Windows Server 2003 Logon 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 logon has been attempted, but provides useful information to a would-be attacker: they only have to guess the password. Honeywell SUS will automatically configure this by default.

  - Disable the default Windows Server 2003 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.

- 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 (say 10 minutes) so that unattended logged-on sessions cannot be high-jacked. Note that in a control room with dedicated Stations, this may not be desirable, in which case an alternative method is to configure Station idle...
time-outs to reduce the Station security level to “view only”. The Honeywell SUS will automatically configure this with a 15 minute default.

Disable unused subsystems

Windows Server 2003 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. Honeywell SUS will automatically configure this by default.

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.

Restrict anonymous logon

By default, anonymous NetBIOS connections can be made to the server 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.

Where file share connections need to cross insecure networks, such as into the DMZ (see “Supported topologies” on page 56), 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

Use 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 and clients to accept and transmit NTLM Version 2 only.

Disable the caching of previous logons

Windows remembers the credentials of previous logged on users so that in the event of the domain server being unavailable, those users can continue to log on. Some security experts recommend that this caching be disabled to prevent sensitive information remaining in memory and hence being vulnerable to attack.

Attention: This can, however, lead to a denial of service. Should the control room become disconnected from the domain server; no more user logons will be possible until re-connection occurs.

Harden the TCP/IP stack

Windows supports a number of 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 in the Microsoft Knowledge Base article: Q315669: How To Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000.
Security Templates

Once the EBI has been installed, Microsoft security templates may be applied to harden the system. These are found in the `\windows\security\templates` directory.

`securews.inf` is recommend, and on more sensitive systems `hiseews.inf` can be used.

**To apply security templates:**

1. Open the local security settings window
2. Right-click and select Import Policy. This will show a list of policies in the `\windows\security\templates` directory
3. Select the required security template
EBI security features

This chapter describes security features specific to EBI.
EBI security is based on operators and locations:

- Operators are individual users or users grouped by role.

- Operators are assigned various degrees of access to locations through access levels. These allow restrictions varying from “view only” to “full control”. Note that in the context of this chapter, the term “locations” refers specifically to physical locations in a facility as defined by EBI. For information on EBI locations, see “Understanding, Planning and Building a Facility Model” in the Configuration and Administration Guide.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Go to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows accounts and groups created by EBI</td>
<td>page 133</td>
</tr>
<tr>
<td>User accounts and EBI user roles</td>
<td>page 136</td>
</tr>
<tr>
<td>Station security</td>
<td>page 138</td>
</tr>
<tr>
<td>Integrated accounts</td>
<td>page 141</td>
</tr>
<tr>
<td>Security levels</td>
<td>page 142</td>
</tr>
<tr>
<td>Configuring a secure Station</td>
<td>page 144</td>
</tr>
<tr>
<td>Electronic signatures</td>
<td>page 146</td>
</tr>
</tbody>
</table>
Windows accounts and groups created by EBI

EBI users fall into several roles, which can be reflected in the Windows user groups to which their account belongs. The main roles are: operators, building engineers, system administrators, and in some cases, application developers. Each role needs different account characteristics and privileges.

On installation, EBI adds a number of local groups and accounts to existing Windows groups and accounts.

Attention: With the installation of EBI R400, the Windows account EBIAdmin will be removed. OPER and ENGR accounts, which were available in previous versions, will still work with sites that use them but are no longer set up when installing EBI.

<table>
<thead>
<tr>
<th>Name</th>
<th>Account type</th>
<th>Description</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNGR</td>
<td>Local account</td>
<td>EBI MNGR account. EBI processes run under this account. It is the operator ID used to log on to Station.</td>
<td>“Requirements for the Windows MNGR account” on page 134</td>
</tr>
<tr>
<td>ADMINISTRATOR</td>
<td>Local account</td>
<td>EBI administrator account.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Group type</th>
<th>Description</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honeywell Administrators</td>
<td>Local group</td>
<td>Members of this group have direct access to the EBI database, file system sub-tree containing EBI executable and data files, and to the EBI registry keys. Engineers, administrators, and developers must belong to this group.</td>
<td>“Requirements for the Honeywell Administrators group” on page 135</td>
</tr>
<tr>
<td>Honeywell Users</td>
<td>Local group</td>
<td>A group, created for convenience, which may be used to group building engineers. If single signon is required (see “Single signon” on page 141), this local group should be changed to a domain group.</td>
<td></td>
</tr>
<tr>
<td>Honeywell Station Users</td>
<td>Local group</td>
<td>This group is created on an EBI client computer, where Station, HMIWeb Display Builder, or Quick Builder are installed on the Windows Vista operating system. This group has the required privileges that users of these applications require.</td>
<td></td>
</tr>
</tbody>
</table>
Requirements for the Windows MNGR account

The Windows MNGR account has a number of specific requirements:

- Password should never expire.
- The following settings should be applied:
  - Deny logon locally
  - Deny logon through terminal services
  - Logon as a batch job
  - Logon as a service
  - Replace a process token
- Where a DSA environment is geographically compact it may be possible to have all the computers in a single domain. The MNGR account must, however, be a local account rather than a domain account.
- To prevent access from external DSA systems it is necessary to change the Windows MNGR account password as described below.
- As installed, the MNGR account must be a member of either the Administrators or Power Users groups in order to start the hscopciengine service.

About changing the Windows MNGR password

The MNGR account is used by:

- All EBI core processes
- Certain EBI Windows services
- Certain EBI COM servers
- DSA node authentication
- Stations

Notes

- Because the MNGR password is used when configuring these services and COM servers, you need to exercise caution in changing this password. Incorrectly changing the password can render the system inoperable.
- If the MNGR password is changed on a DSA node, then this account’s password must also be changed to the new value on all other DSA nodes.
- The EBI server and all Stations synchronized with that server must have the same MNGR password.
- As best practice requires frequent password changes, it is important to use the password utility hscconfig.exe to ensure that the change is made consistently. The system administrator should run this periodically but with care as an invalid password could prevent EBI from operating correctly. For information about using hscconfig.exe see the topic “Windows MNGR Account and EBI Services and Processes” in the Configuration and Administration Guide.
Requirements for the Honeywell Administrators group

The Honeywell Administrators group should be given the following privileges:

- Debug programs
- Profile single process
- Shut down the system

Note that the Honeywell Administrators group also needs permission to execute `%windir%\system32\cmd.exe`, otherwise the EBI server cannot run.

EBI group key

EBI restricts access to its database by placing ACLs on various securable shared objects which it creates (these include shared memory segments, semaphores, Mutexes and other kernel objects). These ACLs grant access to one or more user groups nominated in the following registry key:

```
LOCAL_MACHINE\software\Honeywell\EBI server\group
```

You can specify multiple account groups by separating them with semicolons (;). This allows several user groups to access EBI but have different access permissions to other areas of the server. The group specified must be a local group, not a global group, that is, it must be defined on the EBI server, not a domain server.

Note, however, that extreme caution needs to be exercised when making any changes to the registry. For more information, see “Managing registry ACLs” on page 123.

By default the Honeywell Administrators, Honeywell Users and the Administrator groups are given access, and normally there would be no need to change this.

Attention: A user whose account is a member of the Honeywell Administrators group has extensive access to EBI files, executables, and registry keys. Only provide this access to those who require it. For more information, see “User accounts and EBI user roles” on page 136.
# User accounts and EBI user roles

The users in an EBI system generally fall into one of the four following user roles:

- Engineers
- Administrators
- Operators

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

## Engineers

Engineers need access to configuration tools such as Quick Builder, HMIWeb Display Builder, and Display Builder. They also need to view the system log and to run Station. This requires an account with more flexibility than the operator.

In addition, if they need to stop and start the EBI services, or run utilities with direct access to the database such as trace or dct, then their Windows user account must be part of the Honeywell Administrators group.

If a site wishes to change the name of this group, or to give additional groups direct access to the database, then the following registry key may be changed (see the instructions in “EBI group key” on page 135 for changing or adding user groups to a registry key):

```
HKLM\Software\Honeywell\EBI server\group
```

You can reduce the management load if all engineers use the same logon. However, this is not recommended as it becomes impossible to trace an individual’s activities in audit trails.

## Administrators

Administrators generally have two roles:

- Doing backups, and undertaking performance monitoring, diagnostic investigation and software configuration tasks for the EBI system. They must belong to Honeywell Administrators group and the Backup Operators group for these activities.

- Managing user accounts, performing audits, and undertaking operating system upgrades and similar tasks. They must belong to the Windows Administrators group for these tasks.

Best practice requires that administrators have two accounts, and that they only use the account belonging to the Windows Administrators group when absolutely 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.

## Operators

While every user logging onto a Windows computer needs their own Windows user account, it may not be necessary to configure individual operator accounts in EBI. Depending on the EBI security model you choose, operators may be:

- Defined only within the EBI database, or

- A separate Windows account.
If all operators are placed in a single Windows account group, then that group can be used to provide read-only access to the file shares exposing display files and reports (see “Managing file shares” on page 123).

Note that operator accounts would not normally belong to the Honeywell Administrators group since they do not need the level of access this would provide.

For more information, see “Station security” on page 138 and “Integrated accounts” on page 141.
Station security

In deciding on the kind of Station security to implement you need to consider the following:

- What type of Station security do you want to use:
  - Operator-based security, or
  - Station-based security?

- If you choose operator-based security, do you want to use:
  - Traditional operator accounts?
  - Integrated accounts using either domain-based Windows accounts or local Windows accounts?
  - Electronic signatures?
  - Single signon?

- What type of access do operators require within EBI?

- How do you want to implement Windows security?

- What type of Windows accounts do you require?

<table>
<thead>
<tr>
<th>To learn more about</th>
<th>Go to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Station-based security</td>
<td>page 138</td>
</tr>
<tr>
<td>Operator-based security</td>
<td>page 139</td>
</tr>
<tr>
<td>Integrated security</td>
<td>page 141</td>
</tr>
</tbody>
</table>

Station security choices

EBI offers two types of security:

- Station-based security
- Operator-based security

This allows you to configure security levels, control levels, and scope of responsibility for individual operators or alternatively for individual Stations.

*Attention: You must use operator-based security for HMIWeb Browser Stations*

About Station-based security

Station-based security works as follows:

- Station starts without prompting users to enter any form of operator ID or password.

- The initial security level setting allows users to perform the basic operating functions associated with the user level of OPER (for example, acknowledging alarms and controlling points).
• Users only need to use a password if they want to change to a higher level of security (that is, to SUPV, ENGR, or MNGR).

• Scope of responsibility applies to the Station, not to the operator. (For more information on assignable locations, see the topic “About assignable locations in a Facility Model” in the Configuration and Administration Guide.)

The security levels and their associated functions are described in “About security levels” on page 142.

Attention: If you opt for the Station-based security method, it is recommended that the default passwords for ENGR, SUPV, and MNGR security levels (that were installed as part of the EBI installation process), be changed as soon as possible after installation. The passwd utility used for this change may be run by anyone belonging to the Honeywell Administrators group. Additional file system ACLs may be used to further constrain the use of this tool.

About operator-based security

Operator-based security provides a higher level of security than Station-based security. Operator security is generally used for rotary stations, where the connection to EBI is short term. In general, operator-based security works as follows:

• You assign a specific security level to each user.

• Users cannot access any Station functions unless they enter a valid user ID and password.

• To access a higher security level than the one they are currently using, users need to sign off and then sign on again as a different operator who has the higher security level.

• Locations are assigned to the operator, irrespective of which Station they are currently logged on to.

Operator-based security is appropriate if you need to specify each user’s access and control rights, or where an operator remains at the Station throughout a shift.

Attention: You must use integrated operator-based security if you want to use the Single signon or Electronic Signature options.

Operator-based security variations.

If you choose operator-based security, there are several alternatives that you can use:

<table>
<thead>
<tr>
<th>Account type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional operator account</td>
<td>An account whose definition exists in the EBI server database. Authentication and authorization is done by the EBI server.</td>
</tr>
<tr>
<td>Integrated account</td>
<td>A combination of a Windows user account and an EBI operator account. Authentication is done by Windows; authorization is done by the EBI server.</td>
</tr>
<tr>
<td>Windows group accounts</td>
<td>An integrated account that allows you to add multiple operators by adding a Windows group to the EBI server.</td>
</tr>
<tr>
<td>LDAP accounts</td>
<td>A combination of an LDAP account and an EBI operator account. Authentication is done by an LDAP server; authorization is done by the EBI server.</td>
</tr>
</tbody>
</table>
There are two aspects to operator-based security: authentication and authorization. Authentication is the process of verifying that a user is known to the system, while authorization controls what a known user can do within the system. Accounts are used to restrict access and authority within Station.

- For traditional operator accounts, authentication of the user is done by the EBI server against credentials stored in EBI. Authorization is also controlled by EBI using security levels and, if applicable, locations.

- For integrated accounts and Windows group accounts, authentication of the user is done by Windows on the server computer against the Windows user account. Authorization is then controlled by the EBI server using security levels and, if applicable, assignable locations.

- By using Window group accounts, you can add multiple users to EBI simply by adding the Windows group. All users within the Windows group can then log on to Station in the same manner as traditional operator accounts or integrated accounts.

- You can further restrict operator authority by restricting the level of access to locations. Access to locations uses a separate set of security levels. For detailed procedures, see the topic “Assigning scope of responsibility” in the chapter “Configuring system security and site parameters” in the Configuration and Administration Guide.

Disabling an operator account

If you want to remove access to EBI for a particular operator but want to keep the operator account, you can disable the operator access rather than deleting the operator account. For detailed procedures, see the topic “Disabling an operator account” in the chapter “Configuring system security and site parameters” in the Configuration and Administration Guide.

About traditional operator passwords

For security reasons:

- An operator password consists of a minimum of 5 alphanumeric characters and is stored using one-way encryption.

- Operators may change their own passwords, but a new password cannot be the same as the last 10 passwords used in the previous 3 months. The validity period for passwords defaults to one month, but this setting can be configured as required.

- When signing on, three unsuccessful attempts will lock the operator out for a configurable lockout period. Note that making the retry count too small, or the lockout time too great could lead to a denial of service if a malicious person attempts numerous consecutive failed logons.

- Note that this lockout functionality is unrelated to the Windows account lockout mechanism.

- Once logged on an operator can log off at any time, or they will be automatically logged off after a defined period of inactivity. This will result in the same page, or if configured, an idle page, being displayed in view only mode. Any attempt to change pages, or perform data entry, will cause a logon dialog box to appear.

For more information, see the topic “Changing passwords” in the chapter “Configuring system security and site parameters” in the Configuration and Administration Guide.
Integrated accounts

You can control operator access to EBI using an integrated account. An integrated account is a combination of a Windows user account and an EBI operator definition. The security credentials stored in the Windows user account are used to authenticate the user, while the security details in the EBI operator definition are used to control the authority the user has within EBI.

Using integrated accounts enables you to:

• Use existing enterprise-wide security policies

• Use single signon

• Minimize the number of accounts required for operators

• Use Windows auditing to track user activities

The benefits and impact of integrated accounts vary depending on your logical network configuration. For guidance, see the detailed scenarios in the topic “Using Integrated Security” in the chapter “Configuring system security and site parameters” in the Configuration and Administration Guide.

If you already have traditional operator accounts, you can convert these accounts to integrated accounts. For detailed procedures, see the topic “Converting traditional operator accounts to integrated accounts” in the chapter “Configuring system security and site parameters” in the Configuration and Administration Guide.

Considerations and prerequisites

When deciding how to implement integrated accounts, consider the following:

• You need to set up a Windows user account, so that the user can be authenticated, and then create an operator definition in EBI, so that the user’s authority can be controlled.

• You need to decide what type of Windows user accounts you use: either local or domain accounts. Different account types will suit different site requirements.

• You need to decide if your system will use single signon.

Single signon

If you are using integrated accounts you can set up single signon. Single signon enables EBI to automatically authenticate Station operators using the credentials used to log onto Windows. It is not necessary to supply additional account names and passwords. This is a configurable option that requires the use of operator-based security integrated with Windows accounts.
About security levels

You can use up to six different security levels in EBI. These levels are shown in the following table in ascending order of access.

<table>
<thead>
<tr>
<th>Default Security Level Acronym</th>
<th>Default Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lvl1 (Available with operator-based security only)</td>
<td>View-only mode</td>
</tr>
<tr>
<td>Lvl2 (Available with operator-based security only)</td>
<td>Alarm acknowledgement mode</td>
</tr>
<tr>
<td>OPER</td>
<td>Operator mode</td>
</tr>
<tr>
<td>SUPV</td>
<td>Supervisor mode</td>
</tr>
<tr>
<td>ENGR</td>
<td>Engineer mode</td>
</tr>
<tr>
<td>MNGR</td>
<td>Manager mode</td>
</tr>
</tbody>
</table>

If you have configured a Station to use operator-based security:

- The Station prompts you to sign on, and you cannot access any Station functions until you have successfully signed on.

If you have configured a Station to use single signon (available only if you are using Windows accounts):

- The Station starts with the credentials of the current Windows account if the equivalent operator definition exists in EBI.

If you have configured a Station to use Station-based security:

- The Station starts at a security level of OPER, but you need to enter a password if you want to access a higher level of security.

The security levels OPER through MNGR can be assigned to server functions. In order to use the function, the current security level used to run Station must be equal to or greater than the security level assigned to the function. For example, a push button on a display might be assigned a security level of SUPV when a custom display is built. In order for an operator to use the push button, the Station security level must be either SUPV or MNGR.

For a detailed listing of actions permitted at each security level, see the topic “Actions permitted at each security level” in the chapter “Configuring security and access” in the Configuration and Administration Guide.

Setting security levels for enabling or disabling channels and controllers

Security levels are also used to define which level of security is required to enable or disable hardware items.

For detailed procedures, see the topic “Enabling and disabling channels and controllers” in the chapter “Configuring controllers” in the Configuration and Administration Guide.

Attention: This enable/disable security level setting applies to every Station in your system.

Setting security levels for downloading from Quick Builder

As an option, security levels can also be used to control who can upload and download changes to the engineering database made via Quick Builder. An EBI global setting can be used to require that the
Quick Builder user is running under a Windows account that is a member of the Honeywell Administrators group, and that has been given MNGR security level in the EBI database.

**Control levels**

Operator-based security provides up to 255 control levels to further refine operator control access to individual items of plant and equipment. Any control action to a given point is only allowed if the control level configured in the operator or profile exceeds the level assigned to the point. Any actions initiated by an operator are logged in the Event database against an operator identifier.

**Securing Station displays**

The data that can be viewed on a Station display is primarily controlled by assigning to operators the locations that contain the data. Values can be seen if the access level is View only or higher. Values can be changed if the access is OPER or higher. However, additional constraints can be defined for an individual display.

- A display may be assigned to a location, so that the operator has to have View access to that location in order to call up the display at all.

- An individual database link can have data entry permissions set. Data entry can be totally prevented, that is, the field is read only, or a security level may be applied, allowing an operator with lower level to see the data, but not modify it. This technique is used on many system pages to restrict data entry to Admin level only.

**ODBC client authentication**

ODBC clients using the EBI data source are authenticated when they first establish a connection. Scope of responsibility assignments are used to limit access to data, unless the user has MNGR access level. An operator name may be specified as part of the data source definition, or may be supplied via a dialog box on connection. Authentication can be as a traditional operator-based account, or as a Windows integrated account, with single signon active if permitted.
Configuring a secure Station

A secure Station is one that can only be used to run the Honeywell Station functionality. This level of security is appropriate for dedicated static Stations used in a control room environment.

Setting up a secure Station involves securing the operating system and non-Station software as well as securing Station.

To restrict access to the operating system and non-Station applications, you need to:

• Set up a secure Station. See “Setting up a secure Station” on page 144

• Remove access to the operating system and applications other than Station. See “Locking Station in full screen and disabling menus” on page 144.

Setting up a secure Station

Locking down (that is, securing) Station involves the following tasks.

Attention: If you want an operator to print, you need to set up access to the printers for the operator before you complete the tasks in this section.

1. Creating a batch file which starts Station automatically.

2. Specifying the batch file as a logon script to the user account.

3. Preventing operators from shutting down their computer.

4. Removing access to applications via Task Manager and Windows Explorer.

5. Setting up automatic logon (optional). If you set up automatic logon, to log on as Administrator you need to press the Shift key to prevent automatic logon.

6. Preventing users from locking the computer.

For detailed instructions on completing each of these tasks, see the topic “Setting up a secure Station” in the chapter “System administration” in the Configuration and Administration Guide.

Locking Station in full screen and disabling menus

You can restrict access to non-Station software on a computer by changing the Station command line.

If you want to completely restrict access to the Station computer, use the procedure in the section “Configuring a secure Station” on page 144.

Changing the Station command line allows you to:

• Lock the Station window in full screen so that users cannot resize the window or access operating system functions and non-Station applications.

• Disable the Exit menu choice so users cannot close down this Station.

• Disable the Setup menu choice so that users cannot change the connection or display settings for this Station.

• Disable the Connect menu choice so that users cannot attempt to connect to a different server and disconnect from the current server.

For detailed instructions, see the topic “Changing the Station command line” in the chapter “System Administration” in the Configuration and Administration Guide.
Access to Intranet and Internet sites is disabled by default on Station. For information on enabling full or restricted access see the topic “Web access” in the chapter “Configuring Stations and printers” in the *Configuration and Administration Guide*. 
**Electronic signatures**

With EBI’s Electronic Signatures option, you can configure operator actions, such as controlling a point, to require one or two electronic signatures before the action is performed. You can also configure a set of reasons from which operators must choose before they perform an action.

Each time an action requiring an electronic signature is performed, the events database is updated with:

- The name of the operator(s) who initiated the action
- The specified reason
- The date and time.
- An event is also generated, if:
  - The user name or password provided by the operator is invalid.
  - The operator cancels the Electronic Signature dialog box.
  - The operator does not have the appropriate security level required for the action.

**Notes**

- An event will not be generated if the electronic signature process is cancelled on the first signature step.

- The Electronic Signatures option requires the use of integrated accounts. See “Integrated accounts” on page 141, and the topic “Using integrated security” in the chapter “Configuring security and access” in the *Configuration and Administration Guide*.

For more information about electronic signatures, see the chapter “Configuring electronic signatures” in the *Configuration and Administration Guide*.

**Complying with 21 CFR Part 11**

The EBI Electronic Signatures option is specifically designed to support users (such as the pharmaceutical industry) that must meet the requirements of 21 CFR Part 11, but it is also useful to any organization requiring the ability to trace all operator actions.

Compliance with 21 CFR Part 11 also requires that computer systems audit all logon attempts and all (manual) changes to system time.

Controlling access to the system clock is important because the FDA requires all electronic records to be time-stamped. This means any change to the system clock will affect the audit trail.

To enable audit logging of user logons and system time changes:

- In a domain, you use Group Policy
- In a workgroup, you set the local audit policy

System time changes will be logged if “Audit system events” is enabled for “Success”. As a minimum, therefore, audit settings should log successful attempts, but if attempted intrusion is suspected then failed attempts should also be logged.

*Attention: Note, however, that the default setting for audit logs is to halt the system if the security log becomes full. This is to prevent activity occurring without any traceability but it can also provide an opportunity for a denial of service attack. For information on setting up audit logs to mitigate this kind of attack, see “Setting up and analyzing audit logs” on page 102.*
Glossary

Access Control List
A list of user accounts and groups, each entry specifying a set of allowed, or disallowed actions. When applied to a firewall, an ACL is a list of node addresses and ports that may (or may not) pass through the device.

ACL
The abbreviation for “Access Control List.”

Authentication
When a user logs on to a system the authentication process verifies that a user is known to the system. See also “authorization”.

Authorization
When a user logs on to a system, the authorization building managements what a known user can do within the system. See also “authentication”.

BCN
The abbreviation for “Building Control Network.”

BNA
The abbreviation for “building network adapter.”

BNPS
The abbreviation for “building network point server.”

Business network
A collective term for the network and attached systems at Level 3. See also “Levels 1 through to 3.”

Building Control Network
A collective term for the network and connected systems at Levels 1 through to Level 2. See also “Levels 1 through to 3.”

Controller
Generic term for a device that is used to control and monitor one or more processes in field equipment. Controllers include Programmable Logic Controllers (PLCs), loop controllers, bar code readers, and scientific analyzers.

Demilitarized zone
A demilitarized zone (or DMZ), is an area with some firewall protection, but which is visible to the outside world. This is where public servers for Web sites, file transfers and email are located. More sensitive, private services such as internal company databases, intranets and so on are placed behind a further firewall and have all incoming access from the Internet blocked. You can also create an effective DMZ with just one firewall by setting up access control lists (ACL’s) that let a subset of services be visible from the Internet.

Distributed Systems Architecture
An option that enables multiple EBI systems to share data, alarms, and history.
DMZ
The abbreviation for “demilitarized zone.”

DSA
The abbreviation for “Distributed Systems Architecture.”

Electronic signature
A combination of a user ID and password which are used as the legally binding equivalent of a handwritten signature.

Emergency Repair Disk
Bootable media with the standalone Acronis True Image Enterprise Server version.
The Acronis ERD allows you to run Acronis True Image Enterprise Server on a bare metal or on a crashed computer that cannot boot. You can also back up disks on a non-Windows computer, copying all its data sector-by-sector into the backup archive.

ERD
The abbreviation for “Emergency Repair Disk”.

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 then open up only the ports you need. 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 up port 53 for “outgoing” traffic. If you want to access your internet mail server through POP3, then you would open up 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/default.aspx?scid=kb%3en%3enus%3a832017

HMI
The abbreviation for “Human Machine Interface.”

IP
The abbreviation for “Internet Protocol.”

LAN
The abbreviation for “Local Area Network.”

Levels 1 through to 3
The location of a node within an EBI network and attached systems are often categorized in terms of a series of levels.
• Level 1 represents controller interfaces where building controller busses, access and security controller busses connect to the network.

• Level 2 is where the EBI server and point servers reside

• Demilitarized Zone is the buffer between the Building Control Network and the business enterprise network

• Level 3 is the business network.

Levels 1 to 2 inclusive constitute the “Building Control Network.” Between Levels 2 and 3 you might have a demilitarized zone to help restrict unauthorized access to the Building Control 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**

The abbreviation for “Media Access Control,” 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.

**NAS**

The abbreviation for “Network-attached Storage.”

**NAT**

The abbreviation for “Network Address Translation.”

**Network address translation**

This is a protocol that enables networks to access the Internet by translating private IP addresses.

**Node**

A node is a processing location within a network. It can be a computer or some other device, such as a printer.

**Port**

A port is a logical endpoint on a network node 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 then the client will address messages to that port, the server will send responses to the dynamically allocated client port.

**Quick Builder**

Quick Builder is an EBI tool that provides a central location from which you can configure your EBI system. Quick Builder presents a customized list of tasks that you are required to complete to configure your system. The list of tasks is automatically generated based on your license details. When you click a task, the appropriate tool is launched so that you can complete the task.
**Redundant server**

In a redundant server system, the backup server is actively linked to the primary (running) server, so that it can take immediate control if the primary server fails or is shut down. When synchronized, any change made to the primary’s database will be automatically reflected in the backup’s database.

**SP**

The abbreviation for “Service Pack.”

**Subnet**

A group of hosts that form a subdivision of a network.

**Subnet mask**

A subnet mask identifies which bits of a IP address are reserved for the network address. For example, if the IP address of a particular node 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 node addresses on that network.

**SUS**

Honeywell Software Update Service for EBI.

**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).

**Station**

The EBI operator interface.

**TCP/IP**

The abbreviation for “Transmission Control Protocol/Internet Protocol.”

**Terminal server**

A terminal server allows you to connect several controllers and Stations to a network even though they only have serial or parallel ports. Most terminal servers also provide a range of serial connection options, such as RS-232, RS-422 and RS-485.

**Uninterruptible Power Supply**

For a Building Control Network, reliable power is essential, so it is important to provide an uninterruptible power supply (UPS). If the site has an emergency generator, the UPS battery life may only need to be a few seconds; however, if you rely on external power, the UPS probably needs several hours supply.

**Uplink**

Any interface that connects switches to switches or switches to routers.

**UPS**

The abbreviation for “uninterruptible power supply.”

**WAN**

The abbreviation for “Wide Area Network.”
**Web Toolkit**

The Web toolkit allows users to develop Web pages which incorporate live EBI data.

**WebPoint Control**

Provides web access to after hours lighting and air-conditioning controls.

**WSUS**

The abbreviation for Microsoft “Windows Server Update Services.”