Honeywell

Experion
Network and Security Planning Guide

EP-DSX174
300
11/05

Release 300

Honeywell

Document	Release	Issue	Date
EP-DSX174	300	0	November 2005

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 Limited Australia.

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 2005 – Honeywell Limited Australia

Honeywell trademarks

PlantScape®, SafeBrowse®, **TotalPlant**® and TDC 3000® are U.S. registered trademarks of Honeywell International Inc.

Experion™ is a trademark of Honeywell International Inc.

Other trademarks

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

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

United States and Canada

Contact	Honeywell IAC Solution Support Center
Phone	1-800 822-7673. In Arizona: (602) 313-5558 Calls are answered by dispatcher between 6:00 am and 4:00 pm Mountain Standard Time. Emergency calls outside normal working hours are received by an answering service and returned within one hour.
Facsimile	(602) 313-5476
Mail	Honeywell IS TAC, MS P13 2500 West Union Hills Drive Phoenix, AZ, 85027

Europe

Contact	Honeywell TAC-EMEA
Phone	+32-2-728-2704
Facsimile	+32-2-728-2696
Mail	Honeywell TAC-EMEA Avenue du Bourget, 1 B-1140 Brussels, Belgium

Pacific

Contact	Honeywell Global TAC - Pacific
Phone	1300-300-4822 (toll free within Australia) +61-8-9362-9559 (outside Australia)
Facsimile	+61-8-9362-9169
Mail	Honeywell Global TAC - Pacific 5 Kitchener Way Burswood, WA, 6100, Australia
Email	GTAC@honeywell.com

India

Contact	Honeywell Global TAC - India
Phone	+91-20-2682-2458 / 1600-44-5152
Facsimile	+91-20-2687-8369
Mail	Honeywell Automation India Ltd. 56 & 57, Hadapsar Industrial Estate Hadapsar, Pune -411 013, India
Email	Global-TAC-India@honeywell.com

Korea

Contact	Honeywell Global TAC - Korea
Phone	+82-2-799-6317
Facsimile	+82-2-792-9015
Mail	Honeywell Korea, 17F, Kikje Center B/D, 191, Hangangro-2Ga Yongsan-gu, Seoul, 140-702, Korea
Email	Global-TAC-Korea@honeywell.com

People's Republic of China

Contact	Honeywell Global TAC - China
Phone	+86-10-8458-3280 ext. 361
Mail	Honeywell Tianjin Limited 17 B/F Eagle Plaza 26 Xiaoyhun Road Chaoyang District Beijing 100016, People's Republic of China
Email	Global-TAC-China@honeywell.com

Singapore

Contact	Honeywell Global TAC - South East Asia
Phone	+65-6580-3500
Facsimile	+65-6580-3501 +65-6445-3033
Mail	Honeywell Private Limited Honeywell Building 17, Changi Business Park Central 1 Singapore 486073
Email	GTAC-SEA@honeywell.com

Taiwan

Contact	Honeywell Global TAC - Taiwan
Phone	+886-7-323-5900
Facsimile	+886-7-323-5895 +886-7-322-6915
Mail	Honeywell Taiwan Ltd. 10F-2/366, Po Ai First Rd. Kaohsiung, Taiwan, ROC
Email	Global-TAC-Taiwan@honeywell.com

Japan

Contact	Honeywell Global TAC - Japan
Phone	+81-3-5440-1303
Facsimile	+81-3-5440-1430
Mail	Honeywell K.K 1-14-6 Shibaura Minato-Ku Tokyo 105-0023 Japan
Email	Global-TAC-JapanJA25@honeywell.com

Elsewhere

Call your nearest Honeywell office.

World Wide Web

To access Honeywell Solution Support Online, do the following:

1 In your web browser, type the address `http://www.honeywell.com/ps`.

2 Click **Login to My Account** and then log on.

3 Move the pointer over **Contacts & Support** in the top menu bar and then choose **Support** from the popup menu.

Training classes

Honeywell holds technical training classes on Experion. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see `http://www.automationcollege.com`.

Related documentation

For a complete list of publications and documents for Experion, see the *Experion Overview*.

Contents

1 Introduction 11

Assumptions and prerequisites 12
Important terminology 12
How to use this guide 14
Related documents 15

2 Security checklists 17

Infection by viruses and other malicious software agents 18
Unauthorized external access 19
Unauthorized internal access 20
Accidental system change 21
Protecting your Experion system components 22
System performance and reliability 23

3 Developing a security program 25

Forming a security team 26
Identifying assets 27
Identifying and evaluating threats 28
Identifying and evaluating vulnerabilities 29
Creating a mitigation plan 30
Implementing change management 31
Planning ongoing maintenance 32
Security response team 34

4 Disaster recovery 35

Formulating a disaster recovery policy 36
Backup and recovery tools for Experion 37
About Experion Backup and Restore 38
Planning considerations for Experion Backup and Restore 40
About Microsoft Backup 42

5 Physical and environmental considerations 43

Physical location 44
Protecting against unauthorized system access 45
Control room access 46
Network and controller access 47

Reliable power 48

6 Microsoft security updates and service packs 49

Security updates 50
Honeywell's qualification of Microsoft security updates 50
Service packs 52
Honeywell's qualification of Microsoft service packs 52
Distributing Microsoft updates and virus definition files 53

7 Virus protection 55

Choose supported antivirus software 56
Install antivirus software on process control nodes 57
Configure active antivirus scanning 58
Tune the virus scanning for system performance 59
Directories that can be excluded from scanning 59
About virus scanning and system performance 60
Ensure frequent updates to antivirus signature files 61
Test the deployment of antivirus signature files 62
Prohibit email clients on the process control network 63
Viruses and email 63
Instant messaging 63
Spyware 63

8 Network planning 65

9 Network security 67

High Security Network Architecture 68
Supported topologies 68
Connecting to the business network 72
The demilitarized zone 73
Configuring the DMZ firewall 74
Distributed System Architecture 76
File shares 79
Enterprise Model update 81
eServer 83
Remote access for Station and Configuration Studio 85
Experion Application Server 88
Microsoft Windows Software Update Services 89
Antivirus Update Server 91
PHD 93
Connecting other nodes to the process control network 100
Securing network equipment 102
Domain Name Servers 103
Remote access 104
Dual-homed computers 105

Port scanning 106

10 Securing wireless devices 107

About Experion wireless devices 108
Radio frequency survey 109
Configuring and securing WAPs 110
Connecting wireless devices 110
The domain controller and IAS 110
Firewalls 111
Configuring WAPs 111
Wireless network interface cards 111
Connecting wireless devices 113
IntelaTrac PKS 114
Mobile Access for eServer 116
Mobile Access for Station 119

11 System monitoring 121

Using Microsoft Baseline Security Analyzer 122
Setting up and analyzing audit logs 123
Detecting network intrusion 125
Setting up an event response team 127

12 Windows domains 129

About domains 130
Organization Units and Group Policy 130
Windows domains: forests, trees, and DNS 131
Workgroup limitations 132
Inter-domain trusts 133
Limiting inter-domain trust 133

13 Securing access to the Windows operating system 135

Windows user accounts and passwords 136
User account policies and settings 137
Password policies and settings 139
Honeywell High Security Policy 141
High Security Policy, domains, and workgroups 141
System services 143
Services required by Windows 2003 144
Services required by Experion 145
Services required by Experion Console Stations 146
File system and registry protection 147
Other Microsoft services 149
Internet Information Services 150
SQL Server 151
Windows Terminal Services 152

Remote Access Server 153
SMS Network Monitor 154
Windows XP SP2 and Windows Server 2003 SP1 security enhancements 155
Windows 2003 registry and other settings 156
Secure the desktop 156
Disable unused subsystems 157
Restrict anonymous logon 157
Use NTLM Version 2 158
Disable the caching of previous logons 158
Harden the TCP/IP stack 158

14 Experion security features 159

Windows accounts and groups created by Experion 160
Requirements for the Windows mngr account 160
Requirements for the Honeywell Administrators group 162
Experion group key 162
User accounts and Experion user roles 163
Station security 165
Station security choices 166
About Station-based security 166
About operator-based security 167
Integrated accounts 170
Single signon 171
Signon Manager 171
Windows group accounts 172
About security levels 173
Control levels 174
Securing Station displays 174
ODBC client authentication 175
Configuring a secure Station 176
Setting up a secure Station 176
Locking Station in full screen and disabling menus 177
Electronic signatures 178
Complying with 21 CFR Part 11 179

Glossary

Introduction

1

This guide contains networking and security information applicable to Experion.

It documents recommendations to assist you in planning, setting up, and maintaining a secure environment for your system.

For information about	Go to:
Assumptions and prerequisite skills	page 12
Using this guide	page 14
Related documents	page 15

Assumptions and prerequisites

This guide is primarily intended for engineers, system administrators, and other technical staff who are responsible for planning the configuration and maintenance of an Experion system.

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 derive a security program for your process control 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 Experion against viruses or preventing unauthorized access, you might like to start by consulting the checklists in the topic “Security checklists” on page 17.

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

For information about	Go to:
Developing a security program	“Developing a security program” on page 25.
A strategy for backups and recovery	“Disaster recovery” on page 35.
The physical security of your system	“Physical and environmental considerations” on page 43.
Measures for keeping security-related software up to date	“Microsoft security updates and service packs” on page 49.
Antivirus measures	“Virus protection” on page 55.
Network port access and connections through firewalls	“Network security” on page 67.
Securing wireless devices	“Securing wireless devices” on page 107.
Monitoring and auditing the security of your system	“System monitoring” on page 121.
Working with Windows domains	“Windows domains” on page 129.
Securing your operating system	“Securing access to the Windows operating system” on page 135.
Security issues specific to Experion	“Experion security features” on page 159.

Related documents

The following documents complement this guide.

Document	Description
Experion Overview	Provides a comprehensive overview of Experion, including basic concepts and terminology.
Fault Tolerant Ethernet Overview and Implementation Guide	Gives an overview and provides planning and implementation details of FTE.
Server and Client Planning Guide	Contains high-level planning and design topics for Experion servers and clients, as well as for controllers other than Process Controllers.
Server and Client Configuration Guide	Contains detailed configuration information about Experion security.
Control Hardware Planning Guide	Contains planning and design topics applicable to Process Controllers.
Software Change Notice (SCN)	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.

Security checklists

2

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 process control network and the steps that can be used to mitigate against them. They also provide an alternative way of navigating through this document, depending on your key concerns.

Issue	Go to:
Infection by viruses and other malicious software	page 18
Unauthorized external access	page 19
Unauthorized internal access	page 20
Accidental system change	page 21
Protecting your Experion system components	page 22

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

Mitigation steps	For more information, see
Ensure that your virus protection and Microsoft security hotfixes are up to date on all nodes in your process control network and the systems connected to it.	“Virus protection” on page 55
Ensure that there are no email clients on any nodes of your process control network.	“Prohibit email clients on the process control network” on page 63
Use a firewall and DMZ for the business network to process control network interface.	“Connecting to the business network” on page 72
Use Honeywell’s High Security Network Architecture.	“High Security Network Architecture” on page 68
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 141

Unauthorized external access

This threat includes intrusion into the process control 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 plant, or theft or contamination of product
- The capture, modification, or deletion of data
- Loss of prestige if the external access becomes public knowledge

Mitigation steps	For more information, see
Use a firewall/DMZ for the business network to process control network interface to restrict access from the business network to process control network.	“Connecting to the business network” on page 72
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	“Windows user accounts and passwords” on page 136
Monitor system access.	“System monitoring” on page 121
Use Honeywell’s High Security Network Architecture.	“High Security Network Architecture” on page 68
Securing wireless devices	“Securing wireless devices” on page 107.
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 141
Use the firewall on Windows XP SP2 and Windows Server 2003 SP1 machines	“Windows XP SP2 and Windows Server 2003 SP1 security enhancements” on page 155

Unauthorized internal access

This threat encompasses unauthorized access from systems within the process 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 plant, or theft or contamination of product
- The capture, modification, or deletion of data

Mitigation steps	For more information, see
Ensure Station security.	“Station security” on page 165
Use physical security for process control network systems.	“Physical and environmental considerations” on page 43
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 Experion system.	“Protecting against unauthorized system access” on page 45
Use strong passwords on network equipment.	“Securing network equipment” on page 102
Monitor system access.	“System monitoring” on page 121
Prevent the use of unauthorized laptops on the PCN.	“Connecting other nodes to the process control network” on page 100
Use and enforce a strong password policy.	“Windows user accounts and passwords” on page 136
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 141
Ensure strong access controls are in place on the file system, directory, and file shares.	“File system and registry protection” on page 147
Securing wireless devices	“Securing wireless devices” on page 107.

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

Mitigation steps	For more information, see
Set the minimum level of privilege for all accounts, and enforce a strong password policy.	“Windows user accounts and passwords” on page 136
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 141
Ensure strong access controls are in place on the file system, directory, and file shares.	“File system and registry protection” on page 147

Protecting your Experion system components

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

- Server(s), Stations, and domain controller
- Process control network components (including routers, switches, and firewalls)

Experion server

Protection measure	For more information, see
Take steps to implement and enforce physical security.	“Physical and environmental considerations” on page 43.
Set the minimum level of privilege, and enforce a strong password policy for all accounts.	“Windows user accounts and passwords” on page 136.
Ensure that your virus protection and Microsoft security hotfixes are up to date on all systems.	“Virus protection” on page 55.
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 141.

Experion Station

Protection measure	For more information, see
Take steps to implement and enforce physical security.	“Physical and environmental considerations” on page 43.
Set the minimum level of privilege, and enforce a strong password policy for all accounts.	“Windows user accounts and passwords” on page 136.
Ensure that your virus protection and Microsoft security hotfixes are up to date on all systems.	“Virus protection” on page 55.
Lock down the nodes in your system.	“Honeywell High Security Policy” on page 141.
Ensure Station security.	“Station security” on page 165

Domain controller

Protection measure	For more information, see
Take steps to implement and enforce physical security.	“Physical and environmental considerations” on page 43.
Set the minimum level of privilege, and enforce a strong password policy for all accounts.	“Windows user accounts and passwords” on page 136.

Protection measure	For more information, see
Ensure that your virus protection and Microsoft security hotfixes are up to date on all systems.	“Virus protection” on page 55.

Network components

Protection measure	For more information, see
Take steps to implement and enforce physical security.	“Physical and environmental considerations” on page 43.
Set the minimum level of privilege, and enforce a strong password policy for all accounts.	“Securing network equipment” on page 102.

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.

Protection measures	For more information, see
Do not allow port scanning within the PCN.	“Port scanning” on page 106
Do not automatically schedule full system antivirus scans on Experion nodes.	“Configure active antivirus scanning” on page 58

Developing a security program

3

A security program is a risk-analysis driven, life-cycle approach to securing the process control network. This chapter describes the key components of a security program.

Issue	Go to:
Forming a security team	page 26
Identifying assets that need to be secured	page 27
Identifying and evaluating threats	page 28
Identifying and evaluating vulnerabilities	page 29
Implementing change management	page 30
Creating and implementing a mitigation plan	page 31
Planning ongoing maintenance	page 32

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:
  - Process control (for example, the process control network administrator)
  - Business applications
  - IT system administration
  - IT network administration

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 ACLs)
  - 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 process 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.

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 process control 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 process 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 process 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 31).
- The creation of an Incident Response Team (see “Security response team” on page 34).

Additional security resources

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

- Honeywell’s Process Solutions web site

  `http://www.honeywell.com/ps`

  (In particular, go to **Quick Links** and click **Microsoft Security Information**.)
- Microsoft

  `http://www.microsoft.com/technet/security`
- US Government Accountability Office

  `http://www.gao.gov/`
- Process Control Security Requirements Forum (PCSRF)

  `http://www.isd.mel.nist.gov/projects/processcontrol/`
- National Cyber Security Partnership

  `http://www.cyberpartnership.org/`
- Cisco

  `http://www.cisco.com`
- Computer Security Institute

  `http://www.gocsi.com`
- The National Institute of Standards and Technology document *System Protection Profile - Industrial Control Systems*

  `http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc`

- The Instrumentation, Systems, and Automation Society

  Go to: `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 hotfixes as soon as they are announced, rather than waiting for Honeywell qualification.
- Determining when the update is to be installed. There may be times when the SRT determines that an update is so important that you cannot wait for Honeywell's verification cycle and so you need to verify and install it early on all of your systems.
- Ensuring the deployment of qualified security updates on the Experion 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 122.
- Review network infrastructure patches and configuration changes that will help to secure the network against the latest methods of attack.

Disaster recovery

4

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

Issue	Go to:
Formulating a disaster recovery policy	page 36
Overview of backup and recovery tools	page 37
About Experion Backup and Restore	page 38
Important planning considerations for Experion Backup and Restore	page 40
About Microsoft Backup and Restore	page 42

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 installation media, licence keys, and configuration information.
- Who will be responsible for backups, and the testing, storing, and restoring of backups.

Backup and recovery tools for Experion

To back up your Experion system, you will need to use one of the following tools:

- Experion Backup and Restore (EBR), a separately licensable Experion option
- The Experion `fullbkup` utility in conjunction with the Microsoft Windows Backup and Restore utility. (If you want to use other third-party backup software, contact your local Honeywell Technical Assistance Center for the latest information about qualified backup software.)

For detailed information about backup strategies and specific instructions for backing up your Experion system using these tools, see the *Experion Backup and Restore Guide*.

The following table compares the features of Experion Backup and Restore and Microsoft's Backup and Restore utility.

Experion Backup and Restore	Microsoft Backup Utility
Backs up the entire drive.	You can choose the files and folders to backup
Backups can be saved to hard drive, a USB or FireWire drive, a network drive or DVD.	Backups can be saved to hard drive, a network drive, floppy disk or tape.
Performs full and incremental backups	Performs normal, copy, incremental, differential and daily backups.
Backs up local and remote computers.	Backs up only the local computer
Performs on demand or scheduled backups	Performs on demand or scheduled backups
Rapidly restore from catastrophic failure.	
Bootable restore CD/DVD for restore management.	Can create a bootable floppy disk.
Minimal user intervention to schedule and run backups.	Minimal user intervention to schedule and run backups.
Performance can be adjusted to minimize impact on nodes.	
Single management console for control of local and remote nodes.	

About Experion Backup and Restore

A key feature of the Experion Backup and Restore option 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.

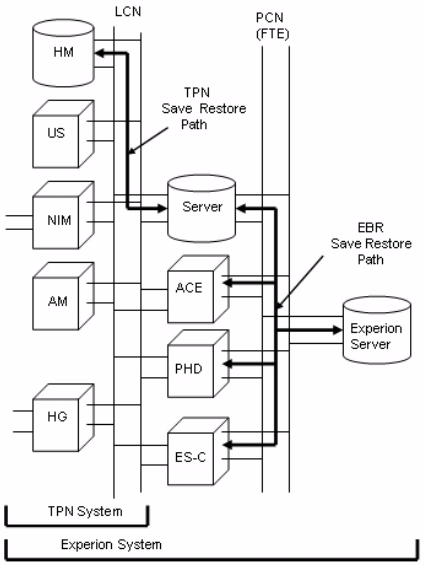
With Experion Backup and Restore, you can perform partial or total restores of your disk images as required by your system condition. Experion Backup and Restore can also be used to restore individual folders and files. The backup image can be used to return your computer to a previous working state with the operating system, applications and data files intact.

With Experion Backup and Restore, you can perform the following tasks:

- Select nodes and databases that are part of the Experion Backup and Restore backup and restore environment.
- Determine what is backed up on a node and where the backup image is stored in the Experion system.
- Configure backups, backup schedules, and options.
- Manually perform a backup.
- Monitor the status of backup jobs.
- Manage the backup repository.
- Archive/export backup images to CD, DVD, or a network drive to allow you to store backup images and data in a secure temperature controlled location.
- Restore drive images, files, and folders.
- Restore archived images from CD, DVD, or a network drive.

Figure 1 on page 39 is a simplified diagram that shows the relationship between the Experion system, and the Experion Backup and Restore save and restore path. In this illustration the information from the Experion nodes is backed up onto a server. Using the Experion Backup and Restore tool, you can specify the drive images of the Experion nodes that will be stored in the Experion server.

Figure 1 Experion Backup and Restore backup and restore path



Planning considerations for Experion Backup and Restore

When planning the implementation of Experion Backup and Restore you need to bear in mind the following rules and guidelines:

- The network location used as the destination for the backup images must not be an Experion server or PHD server.
- If you have a redundant server system but you only have one Experion Backup and Restore license, then you should install Experion Backup and Restore on server B of the redundant pair, as this is where the primary Engineering Repository Database and primary Enterprise Model Database are located.
- Experion Backup and Restore supports only Honeywell nodes or Windows domain controllers for an Experion platform. If you need to back up non-Honeywell nodes, you should purchase separate Symantec LiveState Recovery licenses. Your Experion Backup and Restore license is only for Honeywell nodes and Windows domain controllers used on an Experion platform.

  You must not use separately licensed versions of Symantec LiveState Recovery to back up and restore Honeywell nodes. While the Experion Backup and Restore product is based on Symantec LiveState Recovery technology, it includes additional components and it has also been carefully tested to ensure backup integrity of Honeywell nodes. Separately licensed versions of Symantec LiveState Recovery will not correctly back up and restore Experion nodes.
- If you intend to use both Experion Backup and Restore and Symantec LiveState Recovery in your system, you will need to run a separate Management Console on a separate server for each agent. Nodes with the Experion Backup and Restore agent installed and nodes with the Symantec LiveState Recovery agent installed (which have been separately licensed) should never be managed by the same Management Console. The Management Console does not support these two different agents. This configuration is not supported and its use may result in backup images that cannot be restored.
- The EBR Management Console needs to be installed on a computer that:
  - Is running either Windows 2000 Server or Windows Server 2003.
  - Has enough file storage space to hold all of the planned backups.
- The node running EBR Management Console node should preferably not be an Experion server, PHD server or APP node. Instead, Honeywell

recommends that EBR Management Console be installed on a file server that is also the repository for the backup images.

Backing up TPS/TPN systems

If your system contains Local Control Network (LCN) nodes, you must use the TPS/TPN Save Restore tool to back up the LCN History Module (HM) to an LCN-connected server as shown in Figure 1 on page 39 before you attempt to use Experion Backup and Restore to back up the remainder of the system. Using the TPS/TPN Save Restore tool as the first part of your backup strategy ensures that you will have a complete backup of your system.

The TPS/TPN Save Restore tool can perform automatic check pointing before the tool begins backing up the HM to ensure that you have the latest information. For a description of the TPN Save Restore tool, refer to the *TPS/TPN Backup and Restore User's Guide*.

About Microsoft Backup

The Microsoft Backup Utility helps you create a copy of the information on your hard disk using the Backup or Restore Wizard. The Wizard guides you step-by-step through the process of creating a backup. The Backup utility helps to protect your data if your hard disk fails or your files are accidently erased or damaged.

The Backup utility allows you to copy the files from your hard drive and then archive them onto another hard disk, floppy disk or a tape. You can then copy the resulting .bkf file to CD or DVD if necessary.

Microsoft Backup options

There are five different types of backups available using the Advanced Mode of the Backup or Restore Wizard:

- **Normal**. Copies the selected files and marks each file that has been backed up. You only need the most recent copy of the backup to restore the files.
- **Copy**. Copies all the selected files, but doesn't mark them as being backed up. This option is useful if you want to back up files between your normal or incremental backups as the copy doesn't affect them.
- **Incremental**. Backs up only the files that have been created or changed since the last normal or incremental backup. This option marks the files as backed up.
- **Differential**. Copies the files that have been created or changed since the last normal or incremental backup. It doesn't mark the files as backed up.
- **Daily**. Copies all the files that have been created or modified today. It doesn't mark the files as backed up.

You can also use the Backup utility to verify the data on the backup's completion to ensure that the data was backed up correctly.

Physical and environmental considerations

5

Although the security issues for Experion are generally the same as for any IT server, the physical security of a process control network is particularly important. If the hardware is rendered inoperable, the entire system (and hence the plant) is rendered inoperable.

Issue	Go to:
Physical location	page 44
Protecting against unauthorized booting	page 45
Control room access	page 46
Network and controller access	page 47
Reliable power	page 48

Physical location

In addressing the security needs of your system and data, it is important to consider environmental factors.

For example, if a site is dusty, you should place the server and network equipment in a filtered environment. This is particularly important if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron. And if vibration is likely to be a problem, you should mount the server on rubber to prevent disk crashes and wiring connection problems. In addition, you should provide stable temperature and humidity for the server and network equipment, as well as for network backup tapes and floppy disks.

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. To prevent this, the computer and monitor should be chained to the furniture, and the case locked and closed.

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. These suggestions apply to both the main server and to the control room computers running Station.

Depending on your security needs and risks, you should also consider disabling or physically protecting the power button to prevent unauthorized use. For maximum security, the server should be placed in a locked area and the key protected. Network equipment should be placed in a cabinet or locked closet to protect against unauthorized access to the power, console ports, and network ports.

In addition, 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.

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 or CD drive, 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 process 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 or Windows 2000 Terminal Server session”.
  Note, however, that hiding the windows in Windows Explorer does not prevent those drives from being accessed via a Command window.

Control room access

Providing physical security for the control room is essential to reduce the potency of many threats. Frequently control rooms will have consoles continuously logged onto the primary control server, with speed of response and continual view of the plant considered more important than secure access. The area will also often contain the servers themselves, other critical computer nodes and plant 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 plant 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. For maximum protection, cabling should be duplicated and laid 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

6

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 process control system nodes can be error prone, and may, over time, destabilize your system so they should be undertaken judiciously and with care.

Issue	Go to:
Applying Microsoft security updates and other updates	page 50
The installation of service packs	page 52
A secure process for distributing Microsoft hotfixes and virus definition files	page 53

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 50). 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 53).

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

- If you have PHD nodes in your Experion system, you can (and should) install security updates and hotfixes on those nodes as soon as they are available.
- Before installing security updates on the critical nodes in your process control network, you should refer to Honeywell’s Solution Support On-Line site (see “Honeywell’s qualification of Microsoft security updates” on page 50 for instructions on navigating to the site). This site provides information on the status of qualified updates and hotfixes for Honeywell Process Solutions (HPS) products (that is, Experion, TPS, and Uniformance). For non-HPS products, you will need to refer to the supplier’s security update rules.

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”.

You may wish to contact your local Honeywell Technical Assistance Center (TAC) for advice in relation to Microsoft security updates, or go to the Honeywell ACS Web site for a list of Microsoft security updates that have been qualified by Honeywell:

1 Go to: `http://www.honeywell.com/ps`

2 In the **Quick Links** column select **Microsoft Security Information**.

Honeywell’s **Microsoft Security Information** web page also provides links to a number of Microsoft sites that have information related to security hotfixes.

In any case, before implementing any updates, it is best to verify them on a non-production computer, or when the plant or building is not active, to ensure that there are no unexpected side effects.

The Microsoft web site is a prime source of information on current and past hotfixes. Go to: `http://www.microsoft.com/technet/security/current.aspx`

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 local Honeywell Technical Assistance Center (TAC) for advice in relation to Microsoft service packs or look up the Honeywell ACS web site:

1 Go to: `http://www.honeywell.com/ps`

2 In the **Quick Links** column select **Microsoft Security Information**.

In any case you should verify service packs on a non-production computer, or when the plant or 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 nodes (including non-Experion nodes such as PHD servers) in your Experion 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 process 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 73). Both roles can be performed by a single server. Honeywell provides a service to design and configure nodes in a DMZ: contact Honeywell Network Services on 1-800-822-7673 (USA) or +1 602-313-5558 (outside the USA).

Implementing a Microsoft update and antivirus management system that is dedicated to the process control network helps to ensure more controlled and secure updates, which sites can also tailor for the unique needs of their particular process control environment. It also helps address the issues that arise when an antivirus product that is supported by the process control 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 50 and "Honeywell's qualification of Microsoft service packs" on page 52).

Virus protection

7

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

Recommendations	Go to:
Choose antivirus software that has been tested (and is supported) by Honeywell.	page 56
Install antivirus software on each node connected to the process control network.	page 57
Configure active virus scanning.	page 58
Tune the virus scanning for system performance.	page 59
Ensure that signature files are updated on a regular basis.	page 61
Test antivirus signature files offline before deploying them to process control nodes.	page 62
Prohibit email clients on nodes in the process control network.	page 63

Choose supported antivirus software

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

Honeywell Services has an offering to qualify other third party packages.

Attention

Virus scanners other than McAfee VirusScan and Norton Anti-Virus may not be supported and may not work on Experion. For more information contact your Honeywell service center or TAC.

Install antivirus software on process control nodes

Install antivirus software on every node in the process control network. This should include:

- In an Experion system
  - Experion Stations (Flex Stations, Console Stations and Console Extension Stations, LCN-connected Stations)
  - Experion Server, LCN-connected servers, eServers
  - Application Control Environment (ACE) node
- In a TPS system
  - GUS nodes
  - Application Processing Platform (APP) nodes
- Other nodes
  - Process History Database (PHD) servers
  - Advanced control nodes
  - Honeywell and third party application nodes
  - Non-Windows nodes
  - Subsystem interface nodes (for example, tank gauging)

It is recommended that you set up special servers for the controlled distribution of antivirus signature files to the PCN as outlined in “Distributing Microsoft updates and virus definition files” on page 53.

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 Process Solutions web site:
`http://www.honeywell.com/ps`

2 Choose **Quick Links** and click **Microsoft Security Information**.

Here you will find information about:

- Antivirus software that has been qualified by Honeywell
- 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 Experion is experiencing problems due to low system resources, you may need to:

- Ensure that antivirus software (and other third party applications) are only run 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 60.

Attention

Do not automatically schedule full system scans on any Experion node as this can result in severe degradation of performance, and could therefore:

- Impact the ability of operators to respond to a situation, or
- Result in execution cycle overruns on an ACE node.

Directories that can be excluded from scanning

Experion creates many files during normal operations and the system resource overhead of scanning each of these files for viruses is extremely high. Honeywell tests anti-viral software with the following directories excluded from scanning:

```
\Documents and Settings\All Users\Application Data\Honeywell\
\Program Files\Honeywell\Experion PKS\server\data
\Program Files\Honeywell\Experion PKS\Engineering Tools\system\
   er
```

About virus scanning and system performance

The Experion 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.

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 53.

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 process 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 53.

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 process control network

Do not install email clients on any node connected to the process control network. Honeywell does not support email clients on the process 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 PCN.

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 that Honeywell does not support internet and email access from the PCN.

Network planning

8

General network planning issues for an Experion process control network are described in the following documents:

- *Experion Overview* describes the basic concepts and terminology as well as the capabilities of an Experion process control network.
- *Control Hardware Planning Guide* provides detailed planning information for all aspects of Experion process control network planning. It also describes ControlNet, Ethernet, and FTE networks as well as PLC connections.
- *Fault Tolerant Ethernet Overview and Implementation Guide* includes information about configuring a system that conforms to Honeywell's High Security Network architecture. It contains information about network equipment specifications, configuration, IP addressing, and network topologies.
- The *Experion Server and Client Planning Guide* contains planning information for Experion, including information about distributed systems architecture (DSA), server redundancy, and data exchange. See the chapter on "Networks".

Network security

9

This chapter describes key network security considerations for Experion systems.

Issue	Go to:
Honeywell's High Security Network Architecture	page 68
Connecting to the business network	page 72
The demilitarized zone (DMZ)	page 73
Configuring the DMZ firewall	page 74
Securing network equipment	page 102
Domain Name Servers	page 103
Remote access	page 104
Dual-homed computers	page 105

High Security Network Architecture

Honeywell's High Security Network Architecture is recommended for Fault Tolerant Ethernet based systems using Experion Release 200 and later. It comprises a specific set of qualified network components, including switches and routers, and template configuration files to assist with the setup of switches and routers.

To implement Honeywell's High Security Network Architecture, complete the instructions in the following topics in Knowledge Builder:

- Experion R300 > Configuration > Fault Tolerant Ethernet Overview and Implementation Guide > Planning a Honeywell FTE Network.
- Experion R300 > Configuration > Fault Tolerant Ethernet Overview and Implementation Guide > Use of IP Addresses in an FTE Network.

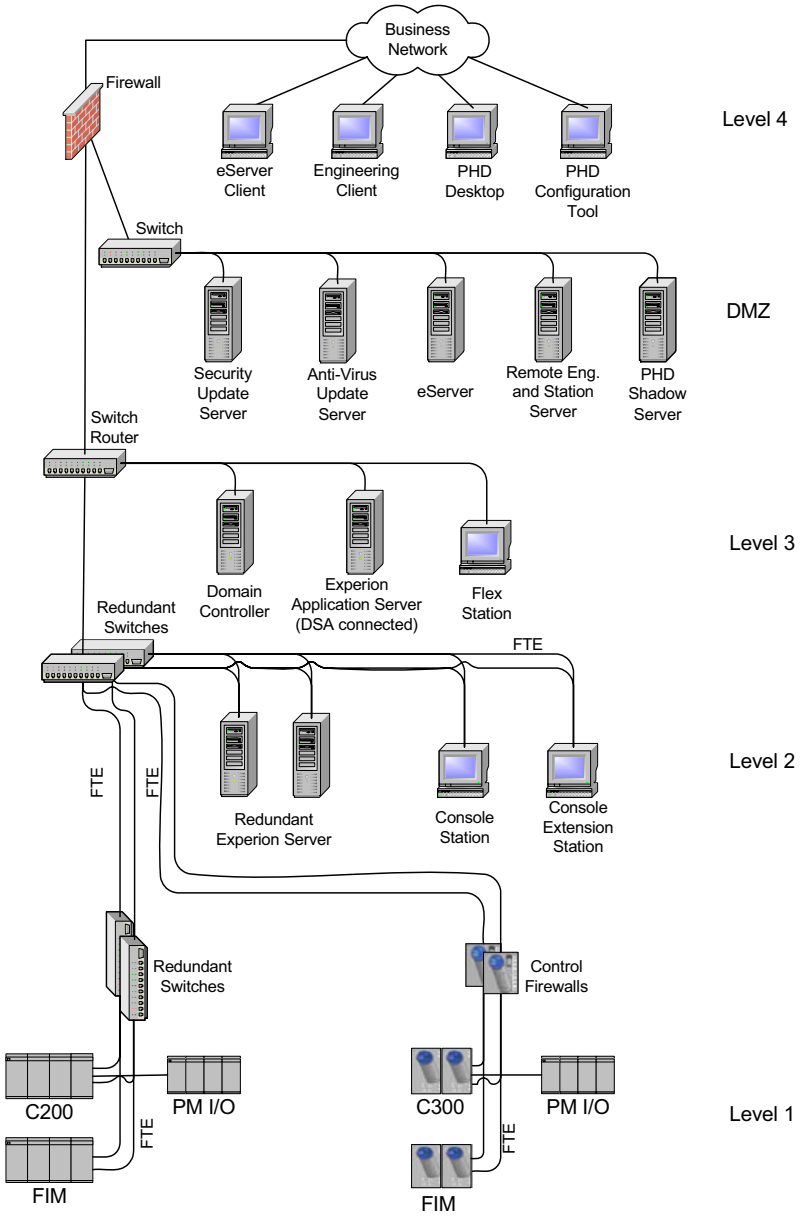
A summary of the key security-related features of Honeywell's High Security Network Architecture follows.

Supported topologies

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

Level	Function of this level	Go to:
Level 1	Real time control (controllers and input/output)	page 70
Level 2	Supervisory control and the operator interface	page 70
Level 3	Advanced control and advanced applications (non-critical control applications)	page 71
Demilitarized Zone (DMZ)	Nodes that access the process control network as well as the business network	page 73
Level 4	Business network applications such as Manufacturing Execution Systems (MES) and Manufacturing Resource Planning (MRP) solutions	page 71

Figure 2 The levels in an Experion system



Topologies other than that shown in “The levels in an Experion system” on page 69 are supported.

For small scale networks you can also connect:

- Level 1 and Level 2 devices using a single switch.
- Console Stations directly to the Level 1 switches where the geography of the plant dictates this.

About Level 1

At Level 1, controllers (C300 and C200) and Fieldbus Interface Modules (FIM) connect to redundant Level 1 switches.

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. The network should be configured so that all Level 1 devices that control a given area of the plant 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 Experion servers and Stations at Level 2. Network traffic on the Level 1 network is also prioritized such that CDA traffic is highest priority.

About Level 2

At Level 2 Experion servers, Stations, and other nodes connect to Level 2 switches. There are also uplink connections from the Level 1 switches.

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

IP subnetting of nodes, priority queuing, and access lists in the switches are 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 2 and Level 1 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 (and higher) nodes and Level 1 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.

About Level 3

At Level 3 domain controllers, plant-wide applications, DSA-connected Experion servers, Stations, and other nodes are connected to a Level 3 router, which may also have switch functionality. 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.

A failure of the Level 3 network can result in a loss of advanced control.

IP subnets, access lists, filtering, and virtual LANs are used to control network communication as follows:

- Access from Level 3 to Level 2 nodes is only enabled if it is required.
- In addition, the type of communication is limited; for example, if authentication of Level 2 nodes by the domain controller at Level 3 is the only communication required, traffic is limited to this type.

If the nodes at Level 2 are part of a Microsoft Windows domain, these nodes will have to communicate with the domain controller which should be part of the Level 3 network.

About demilitarized zones

A demilitarized zone (DMZ) serves as a buffer zone between the process 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 4, permitting the supply of data but preventing nodes at Level 4 from having direct access to any systems on the levels below. For more information, see “The demilitarized zone” on page 73.

About Level 4

Level 4 is the business network (see “Connecting to the business network” on page 72). 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 process control network and business network be kept separate as shown in “The levels in an Experion system” on page 69.

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

Ideally there should be no direct communication between the process control network and the business network. However, practical considerations often mean that a connection is required between these networks. This may be because the process control network requires data from the business network or because certain business applications need access to data from the process 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 73.

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 69) and provides a buffer between the process control network (PCN) and the business network. Servers containing data from the process control 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 PCN 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 74. For more detailed information on firewall configuration, contact Honeywell Network Services.

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 PCN 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 PCN 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).

Honeywell provides a service to design and configure firewalls. Contact Honeywell Network Services on 1-800-822-7673 (USA) or +1-602-313-5558 (outside the USA).

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, PCN 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 129.
- Firewall filtering requirements, refer to the relevant Microsoft documentation.

Issue	Go to:
Distributed System Architecture	page 76
File shares	page 79
Enterprise Model Builder Database runtime update	page 81
eServer	page 83
Mobile Access for Station	page 85
Experion Application Server	page 88
Microsoft Security Update server	page 89
Antivirus Update server	page 91
PHD	page 93

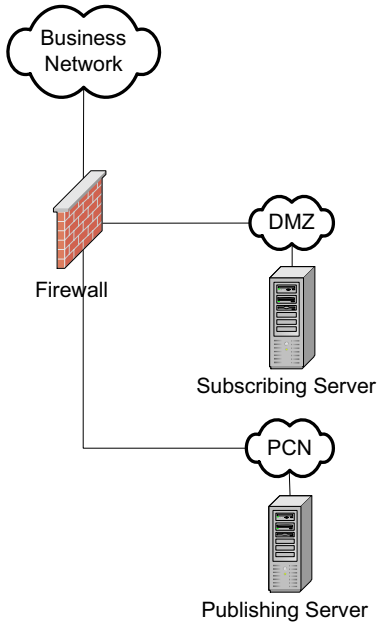
Issue	Go to:
Mobile Access for eServer	page 116

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 Experion 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 “Servers” in the *Server and Client Planning Guide*. The following diagram shows one publishing and one subscribing node. DSA supports networks of nodes, any of which can be publishing, subscribing, or both.



The following table shows the firewall access requirements if both servers are running Experion R300 or later.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Subscribing server	Publishing server	DMZ	2911/UDP	Connection must be configured to use Unicast. Do not use the “Link Supports Multicast Traffic” option.
Publishing server	Subscribing server	PCN	2911/UDP	
Subscribing server	Publishing server	DMZ	50001/TCP	
Subscribing server	Publishing server	DMZ	50003/TCP	
Publishing server	Subscribing server	PCN	50002/TCP	
Publishing server	Subscribing server	PCN	50004/TCP	

If either of the servers are running a release earlier than Experion R300, firewall access needs to be configured as follows.

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

Honeywell strongly recommends that IP to IP access be granted between pre-R300 DSA servers.

Note that the password for the Windows mngr local account must be the same on all servers in a DSA system.

File shares

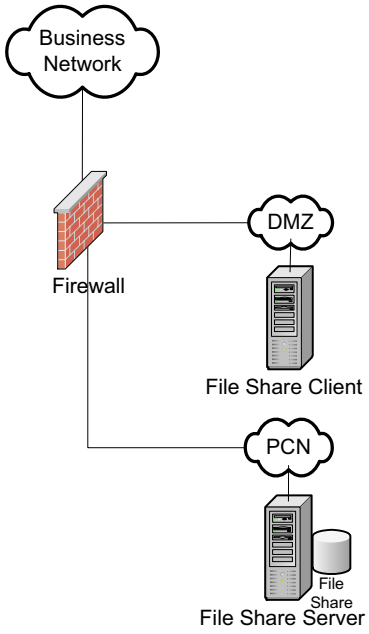
This section describes the firewall access and account requirements for file shares.

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

Note also that the directory `Program Files\Honeywell\Experion PKS\Server\reports` has a file share configured that is used by the “Alarm and Event DSA” report:

- To allow the report output to be viewed from a remote Station. Read permissions are granted to the generic Windows Users group for this purpose. If all operator accounts are contained within the same group, then access can be further reduced by only giving that group read access this directory.
- To allow all temporary information to be retrieved from remote servers when running a report across multiple servers. Read and Write permissions are granted to the Windows Honeywell Administrators group for this purpose.

In the example shown below, a server in the DMZ accesses files from a server in the PCN.

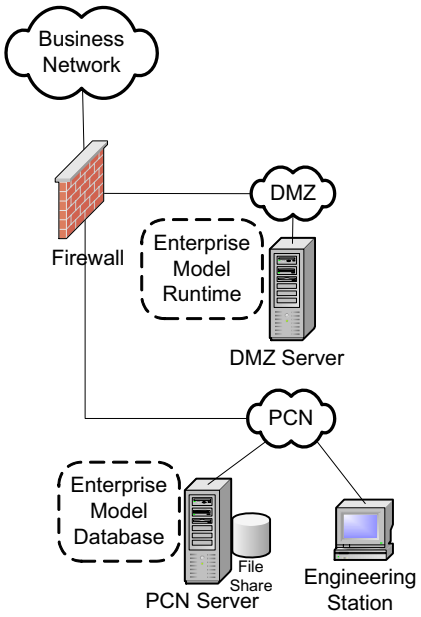


The following table shows the firewall access requirements if both systems are running Windows 2000 or later.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
File share client	File share server	DMZ	445/TCP	

Enterprise Model update

The Enterprise Model Builder Database (EMDB) is a system-wide database that stores information on assets, system alarms and alarm groups.



In the example shown, the server in the PCN stores the Enterprise Model database, but changes are made from an engineering Station in the PCN, and a server in the DMZ uses the Enterprise Model runtime. Changes are made in the offline database and downloaded to servers using the Enterprise Model runtime.

The following firewall access is required to download the Enterprise Model runtime.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Engineering Station	DMZ server	PCN	2909/TCP	
Engineering Station	DMZ server	PCN	2910/TCP	

In addition to this access, the DMZ server needs access to the file share on the PCN server. The DMZ server is the file share client and the PCN server is the file

share server. Firewall access requirements are described in “File shares” on page 79.

Note the following account requirements:

- The Windows `mngr` local account on the DMZ server and PCN server must have the same password.
- The DMZ server needs to authenticate against the Engineering Station. If the System Wide Settings option **Require user name and password for Quick Builder and Control Builder downloads** is:
  - Selected

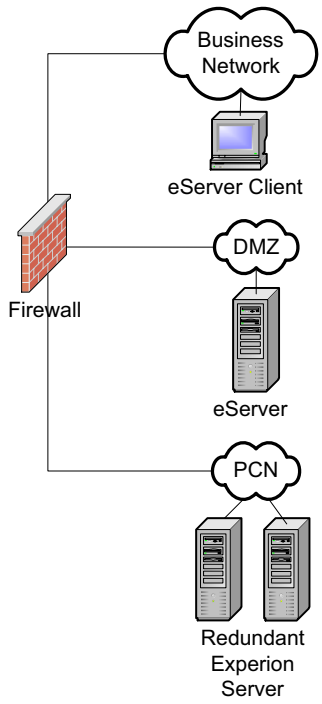
    You need to ensure that both machines have the same account and password configured. The account name needs to be the same account name that was used to log into Configuration Studio. The account also needs to belong to the “Honeywell Administrators” group on the DMZ server, and be configured as an operator account with at least ENGR access rights.
  - Not selected

    You need to ensure that the password for the Windows mngr local account is the same on the DMZ and PCN servers

eServer

An eServer provides read-only access to Experion graphics from a web client.

There are two types of eServer clients: Premium Access and Standard Access. Both provide read-only process graphics without the need for any re-engineering. Premium access provides graphics with data that updates as well as active navigation links. Standard Access graphics do not support data updates or any other type of user interaction.



In the example shown, the eServer client is in the business network, connecting to an eServer in the DMZ.

The following table shows the firewall access requirements for eServer.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
eServer client	eServer	Business network	80/TCP	HTTP

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
eServer client	eServer	Business network	50000/TCP	Premium Access client only

In addition to these access requirements, the eServer is a DSA node that subscribes to the publishing redundant Experion server. Firewall access and Windows account requirements are described in “Distributed System Architecture” on page 76.

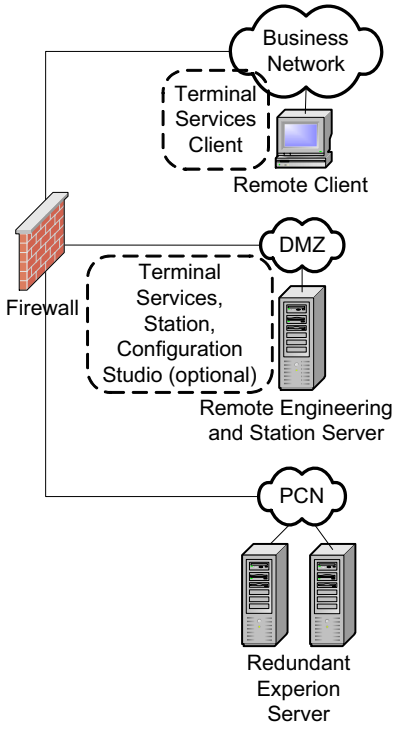
The default eServer configuration allows anonymous access for clients. If authentication is required for access to eServer, the interactive account being used on the eServer client needs to be authenticated on eServer.

Optionally eServer might use the Enterprise Model runtime, with the Enterprise Model database on the redundant Experion server. Firewall access and account requirements are described in “Enterprise Model update” on page 81.

Remote access for Station and Configuration Studio

If business network access is required to Configuration Studio or Station, you should set up a Remote Engineering and Station Server and use Microsoft Terminal Services. For details, see “Configuring Remote Engineering and Station Server” in the *Server and Client Configuration Guide*.

Because of the security risks and firewall access requirements, Honeywell does not support Station or Configuration Studio connected directly to the PCN or DMZ. Running Terminal Services directly on the Experion server is also not supported because Terminal Services consumes a significant portion of the fixed size operating system “session space” resource. Exhausting this resource can stop the Experion server from starting correctly.



In the example shown a remote client connects to Terminal Services running on the Remote Engineering and Station Server in the DMZ, which obtains information from a redundant Experion server in the PCN.

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

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Engineering client	Remote Engineering and Station Server	Business network	3389/TCP	Microsoft Terminal Services

The user on the remote client needs to log on to the Remote Engineering and Station Server with an account that can be authenticated in the Remote Engineering and Station Server's domain.

If Station access is required on the business network, Station runs on the Remote Engineering and Station Server, connecting to the redundant Experion server in the PCN.

If Configuration Studio access is required, both Station and Configuration Studio run on the Remote Engineering and Station Server. The firewall access requirements are described in the following table.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Remote Engineering and Station Server	Redundant Experion server	DMZ	Echo/ICMP	Optionally used to verify which server is currently active. It can be disabled by a configuration option.
Redundant Experion server	Remote Engineering and Station Server	PCN	Echo/ICMP	
Remote Engineering and Station Server	Redundant Experion server	DMZ	1433/TCP	SQL Server access (Configuration Studio only).
Remote Engineering and Station Server	Redundant Experion server	PCN	2909/TCP	
Remote Engineering and Station Server	Redundant Experion server	PCN	2910/TCP	Configuration Studio only.
Remote Engineering and Station Server	Redundant Experion server	PCN	50000/TCP	

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 *Server and Client Configuration Guide.*

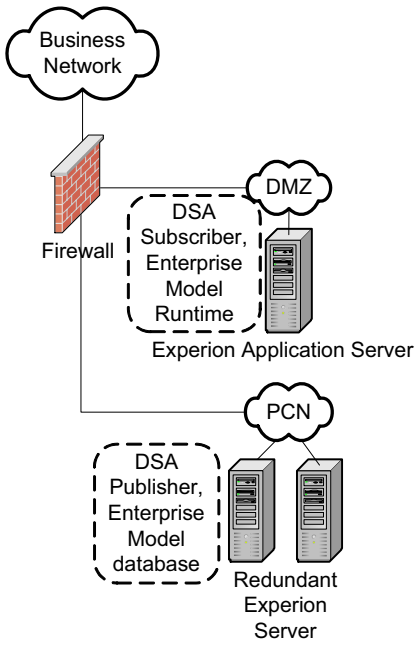
If Configuration Studio is used on the Remote Engineering and Station Server, access to a file share on the redundant Experion servers is required. The Remote Engineering and Station Server is the file share client and the redundant Experion servers are the file share servers. For details of the firewall access requirements, see “File shares” on page 79.

When users of Configuration Studio connect to Experion, they must use an account that correlates to an operator on that Experion server.

Experion Application Server

Experion Application Server is a platform for applications.

In the following example, the Experion Application Server is in the DMZ, getting information via DSA and sharing the Enterprise Model with the Experion server in the DMZ.



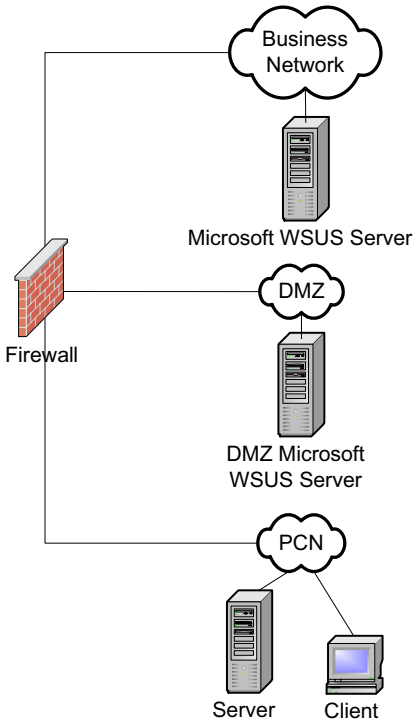
The Experion Application Server is the DSA subscriber to the publishing redundant Experion server. The firewall access and account requirements are described in “Distributed System Architecture” on page 76.

The Experion Application Server uploads the Enterprise Model runtime from the redundant Experion server. The firewall access and account requirements are described in “Enterprise Model update” on page 81.

Microsoft Windows Software Update Services

A Microsoft Windows Software Update Services (WSUS) server provides Microsoft Security Hotfixes to nodes on the PCN.

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



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

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
DMZ Microsoft WSUS server	Microsoft WSUS server	DMZ	80/TCP	HTTP

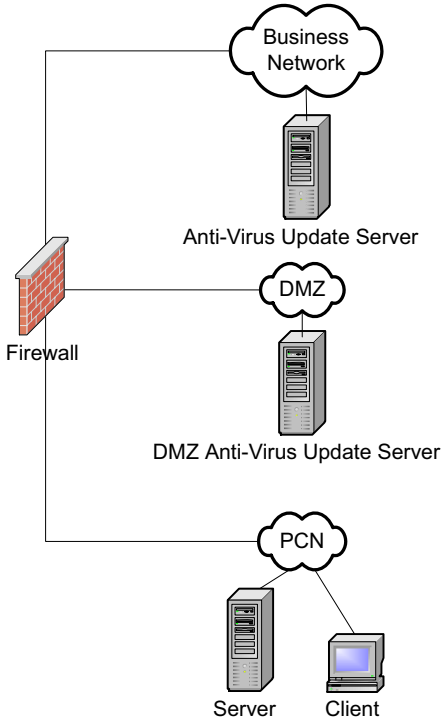
The firewall access required between the Microsoft SUS in the DMZ and the server and client nodes in the PCN is shown in the following table.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PCN server or client	DMZ Microsoft WSUS server	PCN	80/TCP	HTTP

Antivirus Update Server

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

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 PCN. Under no circumstances should the DMZ server access the internet to get the updates to propagate to the PCN.



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.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
DMZ Antivirus Update server	Antivirus Update server	DMZ	80/TCP	HTTP
DMZ Antivirus Update server	Antivirus Update server	DMZ	21/TCP	FTP

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

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PCN server or client	DMZ Antivirus Update server	PCN	80/TCP	HTTP
PCN server or client	DMZ Antivirus Update server	PCN	21/TCP	FTP

PHD

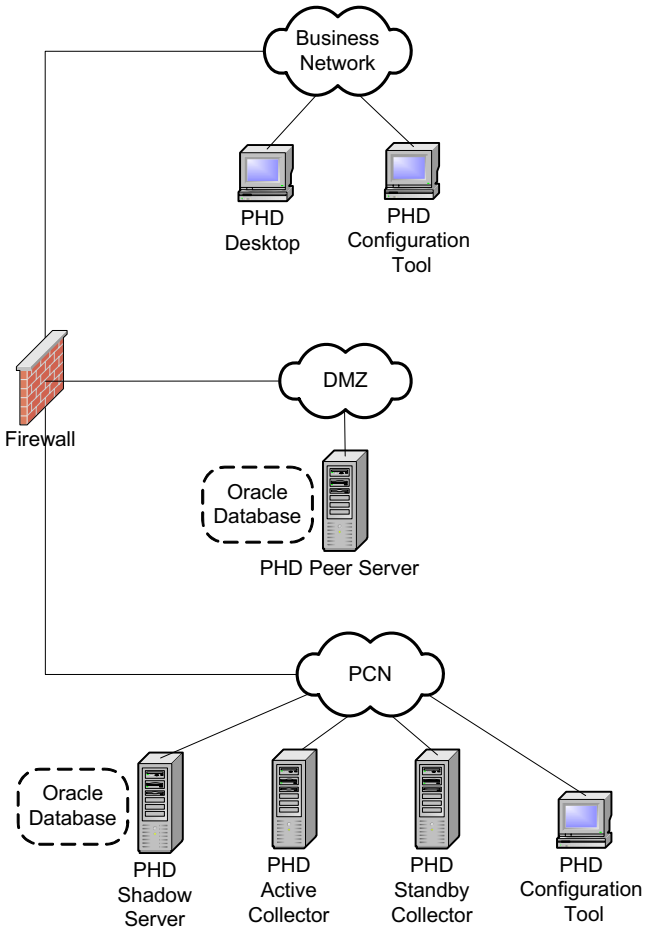
PHD is Honeywell's advanced historian, providing distributed data collection, and data consolidation. PHD supports a wide range of network topologies. This section describes the firewall access and account requirements of two possible topologies with different levels of complexity and security.

The firewall access requirements shown in this section apply to PHD Release 202 and later only. Earlier versions of PHD have different firewall access requirements.

High security configuration: PHD Peer Server in DMZ

In the following example, a PHD Peer Server in the DMZ gets data from a PHD Shadow Server in the PCN. The PHD Peer and PHD Shadow servers each have an Oracle database. A PHD Configuration Tool in the business network is used to configure the PHD Peer Server, while a PHD Configuration Tool in the PCN is used to configure the PHD Shadow Server and Collectors.

The firewall access requirements for this configuration are minimal. A less complex topology that balances ease of configuration with somewhat less network security (because more ports need to be opened in the firewall) is shown in "Typical configuration: PHD Shadow Server in DMZ" on page 95.



The firewall access requirements for communicating with the PHD Peer Server are as follows. The port numbers shown in the following table indicate default settings, which can be modified.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Peer Server	PHD Shadow Server	DMZ	49500/TCP	1st RDI. Each RDI has a port.
PHD Peer Server	PHD Shadow Server	DMZ	49501/TCP	2nd RDI

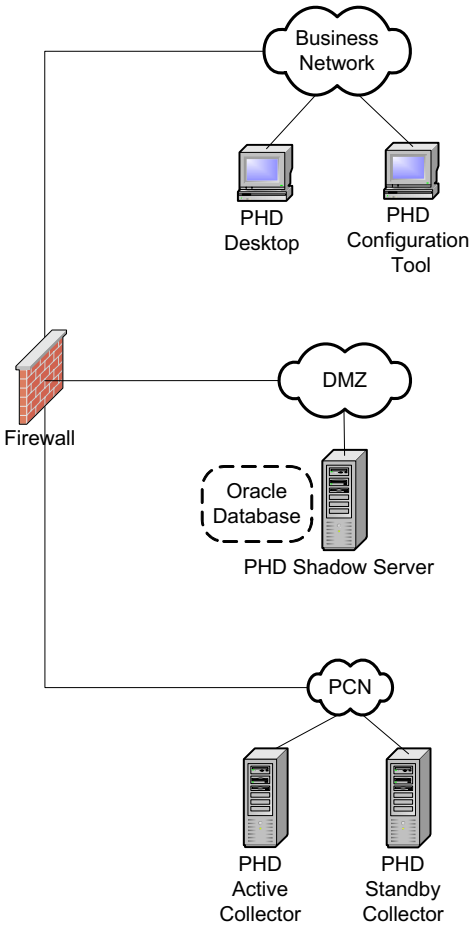
The firewall access requirements for the connection between the PHD Desktop and the PHD Peer Server are as follows. The port numbers shown in the following table indicate default settings, which can be modified. The exception is port 445, which is fixed.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Desktop	PHD Peer Server	Business Domain	3100/TCP	Process Trend, Automation Object via Standard PHD API
PHD Desktop	PHD Peer Server	Business Domain	3150/TCP	
PHD Desktop	PHD Peer Server	Business Domain	445/TCP	
PHD Desktop	PHD Peer Server	Business Domain	1521/TCP	Tag Explorer.

Typical configuration: PHD Shadow Server in DMZ

In the following example, a Shadow Server in the DMZ gets data from redundant PHD Collectors in the PCN. The PHD Configuration Oracle database is on the Shadow Server. The PHD Configuration Tool is used to configure PHD in the PCN.

This configuration has reduced Oracle database license and system administration requirements relative to the topology shown in “High security configuration: PHD Peer Server in DMZ” on page 93. However, additional ports need to be opened in the firewall to support communication with the Oracle database. Furthermore, tag and user updates from the Shadow to the Collectors require specific NT authentication ports to be open.



The firewall access requirements for the PHD Configuration Tool to do an update are as follows. Ports are required for communication with the Oracle database and for sending tag and user updates from the PHD Shadow server to both PHD Collectors. The port numbers shown in the following table indicate default settings, which can be modified. The exception is port 445, which is fixed. Note that port 3100 can be modified but must be the same on the PHD Shadow Server and both PHD Collectors.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Configuration Tool	PHD Shadow Server	Business Network	1521/TCP	Oracle
PHD Configuration Tool	PHD Shadow Server	Business Network	3100/TCP	
PHD Configuration Tool	PHD Shadow Server	Business Network	445/TCP	
PHD Shadow Server	PHD Active Collector	DMZ	3100/TCP	
PHD Shadow Server	PHD Active Collector	DMZ	445/TCP	
PHD Active Collector	PHD Shadow Server	PCN	1521/TCP	Oracle
PHD Shadow Server	PHD Standby Collector	DMZ	3100/TCP	
PHD Shadow Server	PHD Standby Collector	DMZ	445/TCP	
PHD Standby Collector	PHD Shadow Server	PCN	1521/TCP	Oracle

Port 445 is used for many Windows functions, including authentication and Named Pipes. See Microsoft Knowledgebase Article Q179442 for additional information. Starting with Release 210, PHD can be configured to use either Named Pipes, the default method, or Secure Sockets to pass authentication information. Both methods require communication using port 445. Named Pipes will use port 445 for both authentication and data transfer. Secure Sockets will use port 445 for authentication.

The firewall access requirements for the connection between the PHD Desktop and the PHD Shadow Server are as follows. The port numbers shown in the following table are default settings, which can be modified. The exception is port 445, which is fixed.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Desktop	PHD Shadow Server	Business Domain	3100/TCP	Process Trend, Automation Object via Standard PHD API
PHD Desktop	PHD Shadow Server	Business Domain	3150/TCP	
PHD Desktop	PHD Shadow Server	Business Domain	445/TCP	See above comments.
PHD Desktop	PHD Shadow Server	Business Domain	1521/TCP	Tag Explorer (optional).

Two approaches can be used for communication between a PHD Collector and a PHD Shadow Server: the Gateway RDI, which supports peer-to-peer communication, or the Shadow RDI.

- The Gateway RDI firewall access requirements are shown in the PHD Peer Server access table in “High security configuration: PHD Peer Server in DMZ” on page 93.
- The Shadow RDI is used in conjunction with Robust Data Collection (RDC) as shown in this topology. The firewall access requirements for the Shadow RDI are as follows. The port numbers shown in the following table are default settings, which can be modified.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
PHD Active Collector	PHD Shadow Server	PCN	54000/TCP	1st RDI, each RDI has a separate set of ports.
PHD Active Collector	PHD Standby Server	PCN	54000/TCP	
PHD Standby Collector	PHD Shadow Server	PCN	54001/TCP	
PHD Active Collector	PHD Shadow Server	PCN	54002/TCP	2nd RDI
PHD Active Collector	PHD Standby Server	PCN	54002/TCP	
PHD Standby Collector	PHD Shadow Server	PCN	54003/TCP	

PHD security account requirements

There are two client security models for PHD: standard and integrated NT security:

- With standard security, separate logins are required for the PHD Configuration Tool, PHD Data Access, and Oracle.
- With integrated NT security, the Windows login is assigned to a Windows local group that is granted permissions to Oracle. A secondary login is not required.

The service log on account used by the PHD Server and RDI Server services on the PHD Shadow and PHD collectors must be an account that belongs to the Administrators and PHD_MANAGER local groups of the machine. For ease of administration it is recommended that this be a domain account.

Connecting other nodes to the process control network

There may be a requirement to connect non-Honeywell nodes to the PCN. 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 process control network for configuration purposes.

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 PCN.

As it is not possible to completely mitigate against this risk, Honeywell recommends that laptop computers not be connected to the PCN. Instead, you should adopt other approaches such as using the Terminal 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 PCN. Aa 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 hotfixes 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 hotfixes, 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 PCN. If the laptop is disconnected from the PCN 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 PCN.

Permanently connected non-Honeywell computers

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

- Up-to-date antivirus software
- Up-to-date Microsoft security hotfixes
- 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 process 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 process 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.

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 PCN 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 anti-virus 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 PCN from outside the business network using a corporate WAN, the Internet, or a dial-up connection. The client connects to a Remote Access Service (RAS) server placed on the business LAN or in the DMZ, where authentication occurs, then uses various tools to reach the target system. Security aspects of RAS configurations are discussed in “Remote Access Server” on page 153.

Such access may be used to:

- Perform remote control from home after normal hours or for emergency situations. In this case the client would run Station as if it were an in-house Level 4 user. This would either be through a DSA node in the DMZ (assuming there is one and that the server allows the required access) or directly to the Level 2/3 server that owns the points to be controlled.
- Perform engineering tasks on an Experion system in a remote plant. In this case the client would connect to the Engineering Terminal Services Server (the RESS described in “Remote access for Station and Configuration Studio” on page 85) and then proceed as a normal Level 4 user.
- Perform remote support by Honeywell engineers or other support staff. In this instance more direct access to the target machine is needed and tools such as Altiris Carbon Copy or Remote Administrator (Radmin) will be used.

  If an RAS server outside the PCN is used then additional ports need to be opened in the firewall to allow the Carbon Copy (or other tool) client and server to communicate. These ports would be shut off as soon as the support project was complete. An alternative, and simpler, method is to connect a modem directly to the target machine. This limits the remote access to the target, but places a modem within the protected PCN area, which must then be carefully managed and disconnected when not in use. 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.

Where modems are used regularly for dial-in purposes, they should be set for auto re-dial if possible. This only allows calls to pre-configured phone numbers, thereby preventing attacks from unknown sources.

Dual-homed computers

Honeywell recommends not allowing any system to have a network connection to both the process control and business networks. All connections between the process control network and the business network should be through the firewall.

Port scanning

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

Securing wireless devices

10

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

Issue	Go to:
Wireless devices supported by Experion	page 108
Conducting a radio frequency survey	page 109
Configuring and securing wireless access points (WAPs)	page 110
Connecting wireless devices	page 113

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 Experion wireless devices

The Experion system includes wireless mobile productivity devices. These are:

- IntelaTrac PKS for collecting field data
- Mobile Station for allowing remote access to the control system.

These mobile productivity 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.

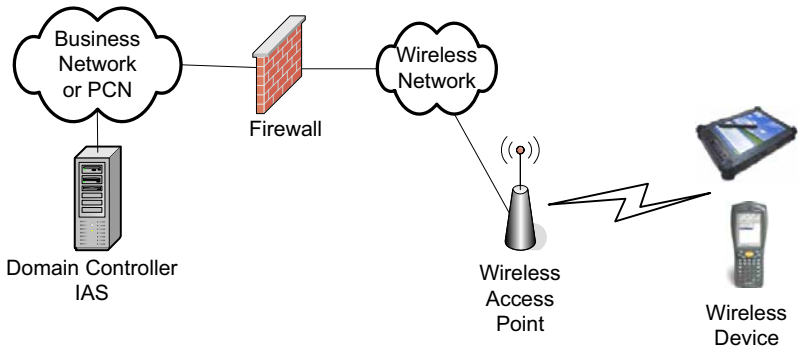
Radio frequency survey

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)
- Antennae 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.



Connecting wireless devices

The wireless device should not connect directly to the PCN. 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 PCN 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 both Windows 2000 Server and Windows Server 2003 as part of the Internet Authentication Services (IAS) package. For detailed guidance on configuring wireless access with RADIUS see the Windows 2000 Server and 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 Experion network, the firewall should be configured to only allow traffic between:

- The domain controller running RADIUS (see “The domain controller and IAS” on page 110).
- 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.

Source Host/ Network	Destination Host/ Network	Interface	Ports/Service	Comments
Wireless Access Point	Domain Controller IAS	Wireless Network	1812/UDP	RADIUS 802.1x
Wireless Access Point	Domain Controller IAS	Wireless Network	1813/UDP	RADIUS 802.1x

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, IntelaTrac PKS or Mobile Station, 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 PEAP-MS-CHAP are supported.

For more information on wireless security recommendations see:

- http://cnscenter.future.co.kr/resource/hot-topic/wlan/1350.pdf
- http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html (Download the Cisco Aironet Wireless LAN Security Overview document.)
- http://www.microsoft.com/technet/community/columns/cableguy/cg1202.mspx
- http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/understanding_8021x.asp

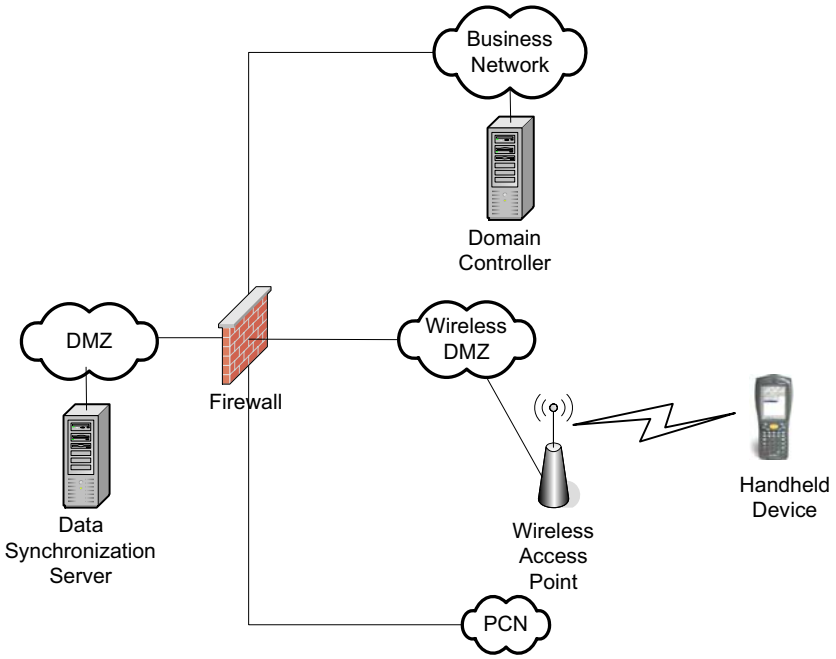
Connecting wireless devices

This section describes the connections for wireless access in an Experion system.

Issue	Go to:
IntelaTrac PKS	page 114
Mobile Access for eServer	page 116
Mobile Access for Station	page 119

IntelaTrac PKS

The IntelaTrac PKS hand-held wireless device connects to the data synchronization server. The IntelaTrac PKS interface does not require access to the PCN. It is recommended to place the data synchronization server in the wireless DMZ (Level 3.5). If no DMZ is present, then the data synchronization server should be placed on the Business Network. The diagram below shows the best practice for IntelaTrac.



Note in this diagram that the WAP resides in the Wireless DMZ and IntelaTrac PKS Data Synchronization Server resides in the DMZ. IntelaTrac PKS users are authenticated with the domain controller IAS in the business network. Additional nodes are included in an IntelaTrac system, the Database Server and Decision Support Systems. It is recommended that these nodes be located in the DMZ or on the business network. For more information, refer to the *IntelaTrac PKS System Installation Guide, IntelaTrac PKS Version 2.4*.

Authentication, firewall access and wireless device configuration are described in “Configuring and securing WAPs” on page 110.

The firewall configuration for Data Synchronization Server and other IntelaTrac PKS system components, such as the IntelaTrack PKS database and PHD will

depend upon what options are being used. Details are contained in the two following documents:

- *IntelaTrac PKS System Installation Guide, IntelaTrac PKS Version 2.4*
- *Administration User's Guide, IntelaTrac PKS Version 2.4*

Please refer to these documents for detailed information on the port configuration required.

Further reference information is available in:

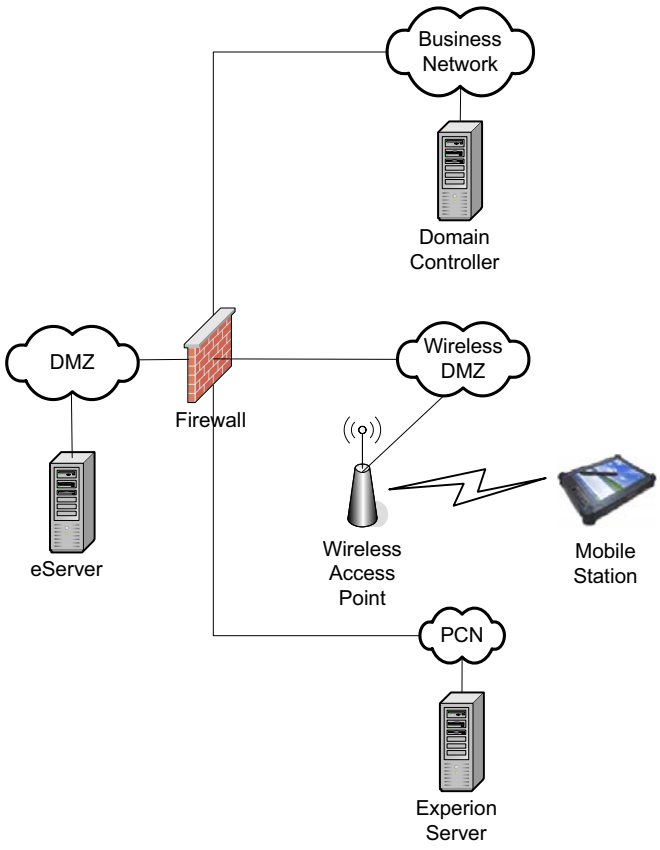
- *Mobile Manager for Pocket PC User's Guide, IntelaTrac PKS Version 2.4*

Mobile Access for eServer

Mobile Station devices have three ways of connecting to Experion. Two of these provide access through an eServer. For this type of access, the eServer resides in the Level 3.5 DMZ.

Mobile Access for eServer Standard

The diagram below shows Mobile Station Access for eServer Standard.

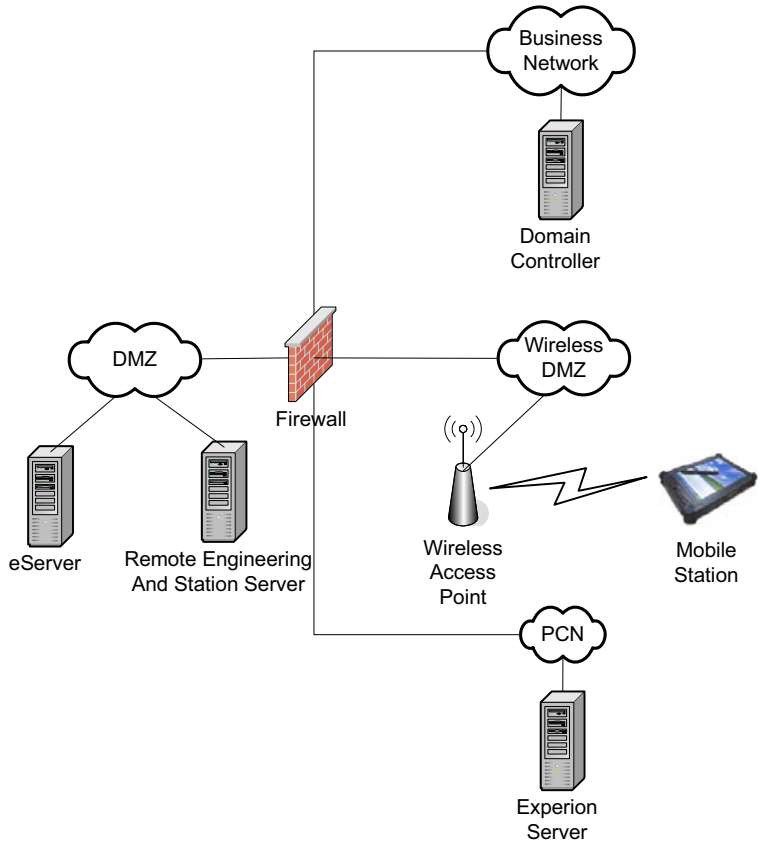


Note in this diagram that the WAP resides in the wireless DMZ. The domain controller with IAS is in the business network. In general it is a better practice to use the domain controller in the business network.

Authentication, firewall access and wireless device configuration are described in “Configuring and securing WAPs” on page 110. Firewall access between the eServer and Experion server is shown in the eServer topics of “Configuring the DMZ firewall” on page 74.

Mobile Access for eServer Premium

The diagram below shows Mobile Station Access for eServer Premium.



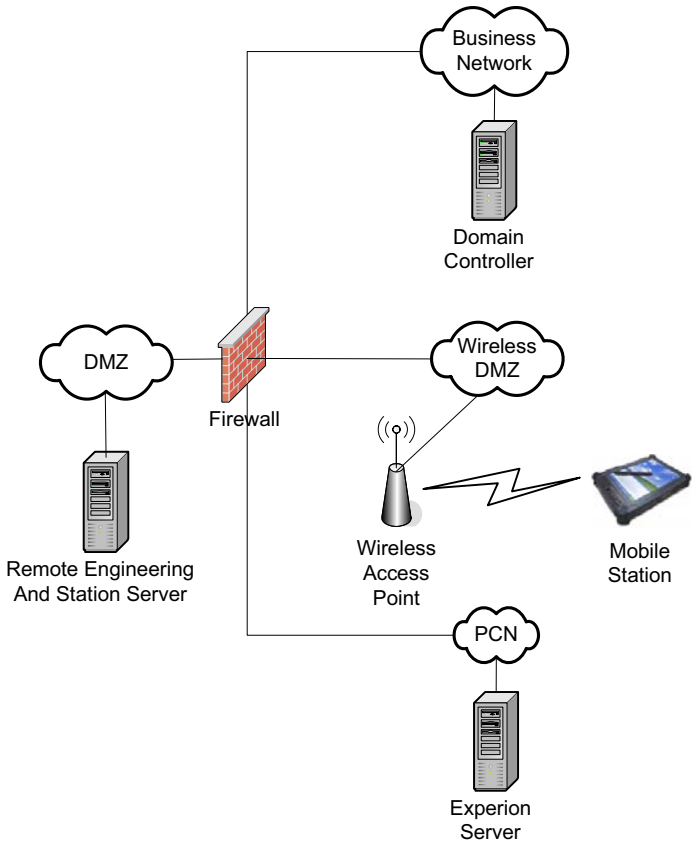
Note in this diagram that the WAP resides in a wireless DMZ. The domain controller with IAS is in the PCN.

The eServer obtains information from the Experion server in the PCN via DSA. The firewall access and account requirements for DSA are described in “Distributed System Architecture” on page 76.

Authentication, firewall access and wireless device configuration are described in “Configuring and securing WAPs” on page 110. Firewall access between the eServer and Experion server is shown in the eServer topics of “Configuring the DMZ firewall” on page 74.

Mobile Access for Station

The diagram below shows Mobile Access for Station.



Note in this diagram that the WAP resides in a wireless DMZ. The domain controller with IAS is in the business network.

Authentication, firewall access and wireless device configuration are described in “Configuring and securing WAPs” on page 110. Firewall access between the eServer and Experion server is shown in “Remote access for Station and Configuration Studio” on page 85.

System monitoring

11

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 more evidence that can be captured, the less the damage is likely to be and the greater the chances of identifying the intruder.

Issue	Go to:
Using Microsoft Baseline Security Analyzer	page 122
Setting up and analyzing audit logs	page 123
Detecting network intrusion	page 125
Setting up an event response team	page 127

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. When run, MBSA attempts to connect to the Microsoft Web site in order to download the latest information on hotfixes, service packs, and so on. It only takes a few minutes to run and generates a series of reports on the security health of a system.

Setting up and analyzing 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.

You can also configure the System Event Server to send system events to the Experion alarm and event subsystem when certain thresholds are reached in the audit logs. For more information, see the chapter “Configuring system performance and event monitoring” in the *Server and Client Configuration Guide*.

To enable auditing:

Either:

- Set the appropriate Group policy, or
- Log on as the Local Administrator and
  a. Start the User Manager tool.
  b. 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 Experion 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 Experion 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 licences (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.XXXX dst inside:XXX.XXX.XXX.XXX
   (type 0, code 0)
   by access-group "outside_access_in"
Jun 03 14:17:51 XXX.XXX.XXX.XXX local4.err %PIX-3-305005: No
   translation group found for tcp src inside:XXX.XXX.XXX.XXX
   dst
   outside:XXX.XXX.XXX.XXX
```

```
Jun 03 14:17:57 XXX.XXX.XXX.XXX local4.err %PIX-3-305005: No
   translation group found for tcp src inside:XXX.XXX.XXX.XXX
   dst
   outside:XXX.XXX.XXX.XXX
Jun 03 14:18:01 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny
   icmp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX
   (type 0, code 0)
   by access-group "outside_access_in"
Jun 03 14:18:11 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny
   icmp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX
   (type 0, code 0)
   by access-group "outside_access_in"
Jun 03 14:18:23 XXX.XXX.XXX.XXX local4.warn %PIX-4-106023: Deny
   icmp src outside:XXX.XXX.XXX.XXX dst inside:XXX.XXX.XXX.XXX
   (type 0, code 0)
   by access-group "outside_access_in"
```

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

Setting up an event response team

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

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

Useful references include:

- http://www.microsoft.com/technet/security/guidance
- http://www.sans.org/resources/
- http://csrc.nist.gov/

Windows domains

12

In planning your system, you also need to consider how the Windows-based nodes in the process control network will fit into the IT infrastructure, and how users will be given access to both the process control network and the business network. This is achieved through the use of Windows domains and workgroups.

Issue	Go to:
About domains	page 130
Domain forests and trees, and DNS	page 131
Domains and process control networks	page 131
Domains Vs workgroups	page 132
Inter-domain trusts	page 133

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 R300 Experion system can be either Windows 2000 Server or Windows Server 2003.

Organization Units 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.

The Honeywell High Security Policy is an example of Group Policy which can be used to implement a secure environment. For information on High Security Policy see “Honeywell High Security Policy” on page 141.

For more information on OUs and Group Policy see:

- Microsoft Windows 2000 Server Resource Kit (see the topic “Deployment Planning Guide: AD Infrastructure”)
- Microsoft Windows 2000 Server Resource Kit (see the topic “Distributed Systems: Desktop Configuration Management”)
- Microsoft Windows 2003 Deployment Kit (see the topic “Designing and Deploying Directory and Security Services”)

Windows domains: forests, trees, and DNS

Domains in Windows 2000 Server and 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 2000 or Windows 2003 domains in IT and process control.

It is important to understand and be familiar with these concepts before installing a new Windows 2000 or 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 process control and IT departments liaise closely to determine the best method of integrating the business IT infrastructure with the process control domain architecture.

Domain membership and process 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 process control network systems in order to accommodate process control requirements.

A separate domain for the process control network has the following advantages:

- Increased security and reliability
- Centralized and independent management of security
- The ability to customize security policies for the process control network
- Changes to the business domain do not affect the process 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 process 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 2000 Server and 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. By default, all domains within a Windows 2000 domain have two-way trusts enabled. This dramatically simplifies trust relationship management, but may provide more access than is desirable.

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 process 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 2000 and 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 Experion server in the process control network domain.

If Stations do reside on the same domain as the Experion server then single signon for operators is possible; that is, Station will be able to automatically connect to Experion using the same credentials as those used when the operator logged onto the Station computer. For more information, see “Single signon” on page 171.

Securing access to the Windows operating system

13

An essential component of any security strategy for a process 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

Issue	Go to:
Windows user accounts and passwords	page 136
Honeywell High Security Policy	page 141
System services	page 143
File system and registry services	page 147
Other Microsoft services	page 149
Windows XP SP2 and Windows Server 2003 SP1 security enhancements	page 155
Windows 2003 registry and other settings	page 156

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.

Issue	Go to:
User account policies and settings	page 137
Password policies and settings	page 139

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.

Experion operator accounts

Experion 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.

You can use Signon Manager to modify user credentials without loss of view.

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 process control 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 Experion operator-based security is configured, similar care must be taken in choosing passwords. For more information about operator-based security see the topic "Administering users" in the chapter "System administration" of the *Server and Client System 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 164.

Service and server accounts

Windows 2003 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 Experion 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. Note, however, that in Windows 2000 certain Windows services must be run under the local "system" account. 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 1 Password settings

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

Strong passwords

It is recommended that you enforce strong passwords, that is, passwords consisting of at least 8 characters including one numeric. 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 1 on page 139 are those suggested by Microsoft and are discussed in their white paper “Account Lockout Best Practices - White Paper” (Account Lockout Best Practices.doc) available from:

```
http://www.microsoft.com/downloads/
   details.aspx?familyid=8c8e0d90-a13b-4977-a4fc-
   3e2b67e3748e&displaylang=en
```

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.

Honeywell High Security Policy

The Honeywell High Security Policy leverages the Microsoft Windows Group Policy security model to enable you to control how programs, network resources, and the operating system behave for users and computers in your organization.

The High Security Policy provides an appropriate security configuration for each user type: operator, supervisor, engineer, and so on. The High Security Policy is based on the Windows security model, but has been optimized for use with Experion and related products with the addition of specialized security templates, accounts, and groups.

Attention

High Security Policy blocks a number of groups like the Windows-created group “Users” from logging in to the desktop. Only members of the following Local Windows groups can log in to the desktop after High Security Policy is installed:

- Administrators
- Engineering Repository Administrators
- Honeywell Administrators
- Local Ack View Only Users
- Local Engineers
- Local Operators
- Local Supervisors
- Local View Only Users

You should consider re-running High Security Policy if significant changes are made to your system. This will ensure that those changes do not undo or adversely affect the security settings created by High Security Policy.

See the topic “Using High Security Policy” in the chapter “Configuring security and access” of the *Server and Client Configuration Guide*. for detailed information on:

- Implementing and configuring the Honeywell High Security Policy
- The groups and users created by Honeywell High Security Policy

High Security Policy, domains, and workgroups

You can use the High Security Policy in a domain or a workgroup environment but as you can only implement Windows Group Policy in a domain environment, you cannot install all the components of High Security Policy in a workgroup environment. High Security Policy is therefore best implemented in a domain environment.

If you implement the High Security Policy in:

- A domain environment, you can implement security settings at the group level. The security settings then apply to every user in the group regardless of the computer they are logged on to.
- A workgroup environment, the settings are applied to every user who logs on to the computer regardless of which local groups they belong to. If you are using a workgroup environment, you need to ensure that the Administrator account can still perform administrative functions.

System services

System services are background processes started by the system at boot time to provide functionality independently of any logged on user. While Experion itself runs as a set of these services, many of the system default services are not needed by Experion. 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**.

Issue	Go to:
Services required by Windows 2003	page 144
Services required by Experion	page 145
Services required by Experion Console Stations	page 146

Services required by Windows 2003

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

Display Name / Core System	Service	Required?	Dependent on?
Computer Browser	browser	Y	lanmanserver, lanmanworkstation
Logical Disk Manager	dmserver	Y	
DNS Client	dnscache	Y	
Event Log	eventlog	Y	
COM and Event System	eventsystem	Y	rpcss
IIS Admin Service[i]	iisadmin	Optional[ii, iii]	rpcss, protectedstorage
Server	lanmanserver	Y	
Workstation	lanmanworkstation	Y	
TCP/IP NetBIOS Helper Service	lmhosts	Y	
MSSQLSERVER	MSSQLSERVER	Y[ii]	
Network Connections	netman	Y	rpcss
Remote Procedure Call (RPC)	rpcss	Y	
Plug and Play	plugplay	Y	rpcss
Protected Storage	protectedstorage	Y	rpcss
Print Spooler	spooler	Y	rpcss
Security Accounts Manager	samss	Y	
System Event Notification	sens	Y	EventSystem
SQLSERVERAGENT	SQLSERVERAGENT	Y[ii]	MSSQLSERVER
Windows Time	w32time	Y	rpcss
World Wide Web Publishing	w3svc	Optional[ii, iii]	IIS Admin
simple mail service (optional for pager)	smtpsvc	Optional[iv]	
Windows Management Instrumentation (needed by FTE)	winmgmt	Optional[v]	rpcss
Windows Management Instrumentation Driver Extensions	wmi	Optional[v]	

i The installation instructions for Internet Information Services (IIS) are documented in the *Experion Software Installation and Upgr Tasks Guide.*

ii Not required for client nodes.

iii Required for Event Archiving/Email notification for Alarm Pager.

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

v Windows Management Instrumentation is needed if Fault Tolerant Ethernet (FTE) is in use.

Services required by Experion

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

Display Name / Core System	Required?
Experion PKS BOOTP Server	Y
Experion PKS Checkpoint Service	Y
Experion PKS Configuration Studio Information Service	Y
Experion PKS Control Data Access Server	Y
Experion PKS DTLR Server	Y
Experion PKS EMDB Server	Y
Experion PKS ER Server	Y
Experion PKS GCL Name Server	Y
Experion PKS HART Multiplexer	Y
Experion PKS Server Daemon	Y
Experion PKS Server Database	Y
Experion PKS Server Desktop	Y
Experion PKS Server Logger	Y
Experion PKS Server Operator Management	Y
Experion PKS Server Replication	Y
Experion PKS Server System	Y
Experion PKS System Repository	Y
sm-Component Admin Service (cas.exe)	Y
sm-Fte Provider (HeartBeatProvider) (fteprovider.exe)	Y
sm-Name Service Provider	Y
sm-Remote Configuration Service	Y
sm-System Event Provider (sysevtprov.exe)	Y
IKB	Experion optional[i]
Signon Manager	Experion optional[i]
GUS TimeSyncClerk Service	Installed for LCN-connected Experion server[ii]
TDC Emulators Service	Installed for LCN-connected Experion server[ii]

i If installed, should not be disabled.

ii Only required on an LCN-connected Experion server accessing TPS data and alarms.

Services required by Experion Console Stations

The following table lists services that run on an Experion Console Station: other services may be disabled.

Display Name / Core System	Required?
Experion PKS Console Station Daemon	Y
Experion PKS Console Station Database	Y
Experion PKS Console Station Desktop	Y
Experion PKS Console Station Logger	Y
Experion PKS Console Station Operator Management	Y
Experion PKS Console Station Replication	Y
Experion PKS Console Station System	Y
Experion PKS Control Data Access Server	Y
Experion PKS GCL Name Server	Y
Experion PKS System Repository	Y
sm-Component Admin Service (cas.exe)	Y
sm-Fte Provider (HeartBeatProvider) (fteprovider.exe)	Y
sm-Name Service Provider	Y
sm-Remote Configuration Service	Y
sm-System Event Provider (sysevtprov.exe)	Y
IKB	Experion optional[i]
Signon Manager	Experion optional[i]
GUS TimeSyncClerk Service	Installed for LCN-connected Console Station[ii]
TDC Emulators Service	Installed for LCN-connected Console Station[ii]

i If installed, should not be disabled.

ii Only required on an LCN-connected Console Station accessing TPS data and alarms.

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 Experion 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. Experion 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 Program Files\Honeywell\Experion PKS subtree is set up as follows:

- Users are given “read only” permission.
- Power Users are given “read/write” access.
- Honeywell Administrators are given full 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 Experion 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

Caution

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. For detailed information about backing up and restoring system data like registries, see the *Backup and Restore Guide*.

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.

Experion 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
- Configuration Studio uploads and downloads require “write / file create” access by plant engineers.

Thus Experion 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

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

Service	Go to:
Internet Information Services	page 150
SQL Server	page 151
Windows Terminal Services	page 152
Remote Access Server	page 153
SMS Network Monitor	page 154

Internet Information Services

Internet Information Services (IIS) is needed for the following Experion functionality:

- Event Archiving System displays
- Alarm Pager option (e-mail notification)
- eServer

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 Experion are documented in the *Experion Software Installation and Upgrade Guide*.

It is strongly recommended that you run the Microsoft Baseline Security Analyzer (see "Using Microsoft Baseline Security Analyzer" on page 122).

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.
- Do not place executable `.asp` 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.
- Where possible do not allow anonymous connections, since there is no indication who is calling. Where access is intranet, that is, from trusted domains, enable NT challenge/response so that IIS can determine the callers identity. Mixed mode connections can be allowed by enabling both anonymous and NT challenge connections and using NTFS to prevent access to those directories requiring client identity checking.

SQL Server

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

Experion 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 122) on your SQL Server.

Note that Experion installation process sets authentication to "Windows only" and ensures that the `sa` password is not blank.

Windows Terminal Services

Windows Terminal Services allows you to run Microsoft Windows-based programs on a server and display them remotely on client computers connected to the LAN. This can be a useful facility for remote administration, engineering and monitoring activities, but does provide an additional avenue for attack.

Several levels of protection are available which are detailed in Microsoft documentation. The fewer people given Terminal Services access the better, and logon rights should be removed as soon as access is no longer needed. Communications should be set to be encrypted.

The easiest way of allocating Terminal Services access to users is to place all such users in a special group and use the Terminal Services session manager to give that group, rather than the “Everyone” group, Terminal Services logon rights.

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.

SMS Network Monitor

The SMS Network Monitor is a very useful tool which intercepts and displays network packets. Access to the tool should be controlled by password. In addition, both Windows 2003 servers and Windows XP workstations have a Network Monitor agent which allows a remote monitor to intercept packets to or from that computer. The agent should also be password-protected using the Monitor Agent panel applet.

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.

- 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.

- 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 Experion will, however, enable the Windows host firewall.)

While these security enhancements are supported by Experion R300, some of the changes may cause problems in some Experion systems where there are:

- Pre-R300 Experion DSA servers
- Windows 2000 DSA nodes (for example, a Windows 2000 EAS node)
- OPC connections (for example, HSC OPC Server, OPC Integrator, or other third party OPC connections).

Because of this, the Experion R300 installation process modifies some of the default Windows security settings. You can, however, subsequently tighten this initial Experion security setting with the Experion Node Security wizard on individual Experion servers or Console Stations that meet all of the following conditions:

- The node is not connected to any pre-R300 Experion DSA servers
- The node is not connected to any Windows 2000 DSA nodes (for example, a Windows 2000 EAS node)
- There are no OPC connections (for example, HSC OPC Server, OPC Integrator, or other third party OPC connections) on this node.

The instructions for using the Experion Node Security wizard are documented in the *Experion Supplementary Installation Tasks Guide*.

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 148.)

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

Issue	Go to:
Secure the desktop	page 156
Disable unused subsystems	page 157
Restrict anonymous logon	page 157
Use NTLM Version 2	page 158
Disable the caching of previous logons	page 158
Harden the TCP/IP stack	page 158

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 pre-canned banner when someone logs on. A typical message would be:

  ```
  It is an offence 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 2000 Server or Windows Server 2003 domain) or the local registry to:

  - Hide the last user’s name on the logon window.

    By default, the Windows 2000 Server and 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.

  - 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”.

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.

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 or across the Level 3/Level 4 boundary (see “Supported topologies” on page 68), 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.

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.

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.*

Experion security features

14

This chapter describes security features specific to Experion.

Experion security is based on *operators* and *assets*:

- Operators are individual users or users grouped by role.
- Operators are assigned various degrees of access to assets through access levels. These allow restrictions varying from “view only” to “full control”.

  Note that in the context of this chapter, the term “assets” refers specifically to the Experion assets that comprise your asset model. For information on the Experion asset model, see “Assets and asset models” in the *Server and Client Planning Guide*.

Issue	Go to:
Windows accounts and groups created by Experion	page 160
User accounts and Experion user roles	page 163
Station security	page 165
Integrated accounts	page 170
Windows group accounts	page 172
Security levels	page 173
Restricting access to the operating system	page 176
Electronic signatures	page 178

Windows accounts and groups created by Experion

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

On installation, Experion adds a number of local groups and accounts to existing Windows groups and accounts. These include:

Name	Account / group	Description	Go to:
mngr	Local account	Experion processes run under this account.	"Requirements for the Windows mngr account" on page 160
Honeywell Administrators	Local group	Members of this group have direct access to the Experion database, file system sub-tree containing Experion executable and data files, and to the Experion registry keys. Engineers, administrators, and developers must belong to this group.	"Requirements for the Honeywell Administrators group" on page 162
Engineering Repository Administrators	Local group	Members of this group have permission to administer the engineering repository database. The `mngr` must belong to this group.	
Engineers	Local group	A group, created for convenience, which may be used to group plant engineers. If single signon is required (see "Single signon" on page 171), this local group should be changed to a domain group.	

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 above.

About changing the Windows mngr password

The `mngr` account is used by:

- All Experion core processes
- Certain Experion Windows services
- Certain Experion COM servers
- DSA node authentication
- Console 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 Experion server and all Console 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 `pwdutil.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 Experion from operating correctly.

For information about using `pwdutil.exe` see the topic "Changing the Windows mngr account password" in the *System Administration GuideAdministrative Topics*.

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 Experion server cannot run.

Experion group key

Experion 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\Experion PKS server\group
```

You can specify multiple account groups by separating them with semicolons (;). This allows several user groups to access Experion 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 Experion 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 148.)

By default the Honeywell Administrators group is the only group 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 Experion files, executables, and registry keys. Only provide this access to those who require it. For more information, see "User accounts and Experion user roles" on page 163.

User accounts and Experion user roles

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

- Engineers
- Programmers
- Administrators
- Operators

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

Engineers

Engineers need access to configuration tools such as Configuration Studio, 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 Experion 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 “Experion group key” on page 162 for changing or adding user groups to a registry key):

```
HKLM/software/Honeywell/Experion PKS 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.

Programmers

Programmers should not develop on the live system because of the risk of disruption due to the excessive use of resources (CPU, memory, and disk throughput), and because of problems associated with untested code.

Development should occur on a second computer, and new executables should only be allowed on the live system after they have been thoroughly tested.

Sensitive sites may use file permissions to prevent changes and additions to the executables in the `run` directory by anyone other than an authorized administrator. Anyone who adds or removes processes running under the Experion umbrella must belong to Honeywell Administrators group. Typically, they also belong to the Power Users group.

Administrators

Administrators generally have two roles:

- Doing backups, and undertaking performance monitoring, diagnostic investigation and software configuration tasks for the Experion 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 Experion. Depending on the Experion security model you choose, operators may be:

- Defined only within the Experion database, or
- A member of a Windows group, 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 148).

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 165 and “Integrated accounts” on page 170.

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?
  - Windows group accounts using either domain-based Windows groups or local Windows groups?
  - Electronic signatures?
  - Single signon?
- What type of access do operators require within Experion?
- How do you want to implement Windows security?
- What type of Windows accounts do you require?
- Do you want to use the Honeywell High Security Policy?

To learn more about	Go to:
Station-based security	page 166
Operator-based security	page 167
Group accounts	page 172
Integrated security	page 170
Honeywell High Security Policy	page 141

Station security choices

Experion offers two types of security:

- Station-based security
- Operator-based security

This allows you to configure security levels, control levels, and asset assignments for individual operators (or groups of operators) or alternatively for individual 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`).
- Asset assignment applies to the Station, not to the operator. (For more information on asset assignment, see the topic "About assignable Assets" in the chapter "Assets and asset models" in the *Server and Client Planning Guide*.)

The security levels and their associated functions are described in "About security levels" on page 173.

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 Experion installation process), be changed as soon as possible after installation.

The `paswrd` 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. 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.
- Assignable assets 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 operator-based security if you want to use:

- Single signon
- Electronic Signatures

Operator-based security variations

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

Account type	Description
Traditional operator account	An account whose definition exists in the Experion server database. Authentication and authorization is done by the Experion server.
Integrated account	A combination of a Windows user account and an Experion operator account. Authentication is done by Windows, authorization is done by the Experion server.
Windows group account	An integrated account that allows you to add multiple users by adding the Windows group to the Experion server. Authentication is done by Windows, authorization is done by the Experion server.

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 Experion server against credentials stored in Experion. Authorization is also controlled by Experion using security levels and, if applicable, assignable assets.
- 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 Experion server using security levels and, if applicable, assignable assets.

By using Windows group accounts you can add multiple users to Experion 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.

Disabling an operator account

If you want to remove access to Experion 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 security and access” in the *Server and Client Configuration 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 security and access” in the *Server and Client Configuration Guide*.

Integrated accounts

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

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 security and access" in the *Server and Client Configuration 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 security and access" in the *Server and Client Configuration 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 Experion, 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.
- You then need to add the Windows accounts to the appropriate Honeywell Experion Windows group, that is, add accounts for operators to the Honeywell Experion Users group. If the operator also needs to use configuration tools such as Configuration Studio, add the Windows account to the Honeywell Administrators group.

Single signon

If you are using integrated accounts you can set up single signon. Single signon enables operators to log on to the Station computer and start Station by providing their operator ID and password only once when they log on to the computer. This is a configurable option that requires the use of operator-based security integrated with Windows accounts.

Signon Manager

Signon Manager is an application that provides a point of single signon on a particular computer to applications that use this facility. Users can:

- Sign on to any applications that are “Signon aware” through Signon Manager.
- Change the current user without having to shut down and restart any applications or the computer.
- Temporarily override the current user security credentials without having to shut down and restart any applications or the computer.

Signon Manager is optional and can be used with Station if the security type is operator-based and integrated with Windows accounts.

The benefit of using Signon Manager is that operators can sign on and off without losing view of the plant or critical processes. When a different user signs on to Signon Manager, any instances of Station that are running receive notification of the change of user. The Experion server then verifies the authority of the user in the normal manner and changes to the appropriate security level for the user who is currently signed on.

Example scenario

An operator is logged on to Signon Manager and is running multiple instances of Station on their workstation. At the end of the shift, the next operator needs to sign on with their security credentials. The operator for the next shift calls up Signon Manager and enters their user name and password. All instances of Station are notified of the change of operator and the new operator is now effectively logged on to all Stations with the correct security credentials.

Windows group accounts

If you are using integrated Windows and Experion accounts (see “Integrated accounts” on page 170), and you have also set up Windows group accounts, you can add Windows group accounts to Experion. This enables all members of that Windows group to log on to Station.

The benefits of using Experion Windows group accounts are that you:

- Only have to configure one account in Station for every Windows group. This reduces the number of accounts required in Experion.
- Can leverage any existing Windows security policies and settings.
- Can apply any Experion security and access restrictions at the group level.

The Windows group can be a local Windows group or a domain Windows group. For information about the use of local or domain Windows groups, see the topic “Using Integrated Security” in the chapter “Configuring security and access” in the *Server and Client Configuration Guide*.

For more information about using Windows group accounts in Experion, see the topic “Adding an Experion Windows group account” in the chapter “Configuring security and access” in the *Server and Client Configuration Guide*.

About security levels

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

Table 2 Security levels

Default Security Level Acronym	Default Meaning
View Only previously called Lvl1 (Available with operator-based security only)	View-only mode
Ack Only previously called Lvl2 (Available with operator-based security only)	Alarm acknowledgement mode
OPER	Operator mode
SUPV	Supervisor mode
ENGR	Engineer mode
MNGR	Manager mode

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 Experion.

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 *Server and Client Configuration 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 *Server and Client Configuration Guide.*

Attention

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

Setting security levels for downloading from Configuration Studio

As an option, security levels can also be used to control who can upload and download changes to the engineering database made via Configuration Studio. An Experion global setting requires that the Configuration Studio user is running under a Windows account known to Experion (that is, an integrated account) and configured to have mngr access level.

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 assets 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 an asset, so that the operator has to have View access to that asset 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 Experion data source are authenticated when they first establish a connection. Asset 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, a Windows integrated account or group. Single signon will take effect 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 goes beyond that applied by the High Security Policy to server and non-dedicated clients, and 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. The procedures for securing Station described in this section can be used in conjunction with the Experion High Security Policy.

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 176
- Remove access to the operating system and applications other than Station. See “Locking Station in full screen and disabling menus” on page 177.
- Remove the link from the System Menu display to Knowledge Builder which uses Internet Explorer and can therefore be used to access other files.

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 *Server and Client System 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 176 and use the High Security Policy.

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 *Server and Client System 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 *Server and Client System Configuration Guide*.

Electronic signatures

Electronic signatures are the legally binding equivalent of an operator's handwritten signature.

With Experion's Electronic Signatures option, you can configure operator actions (such as acknowledging a message or controlling a point) to require one or two electronic signatures before the action is performed. You can also configure a set of reasons that require operators to choose from a pre-configured set of reasons before they perform the 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.
- A time-out has been set for the action, and the time has been exceeded before the signing was complete.
- The operator does not have the appropriate security level required for the action.

Notes

- The Electronic Signatures option requires the use of integrated accounts. See "Integrated accounts" on page 170, and the topic "Using integrated security" in the chapter "Configuring security and access" in the *Server and Client Configuration Guide*.
- The IKB and the OEP keyboard are not compatible with Electronic Signatures. You cannot use either of these keyboards with Electronic Signatures.

For more information about electronic signatures, see the chapter "Configuring electronic signatures" in the *Server and Client Configuration Guide*.

Complying with 21 CFR Part 11

The Experion 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.

Applying the Honeywell High Security Policy will restrict the ability to make system time changes to users belonging to the Administrators group. For information on Honeywell High Security Policy, see “Honeywell High Security Policy” on page 141.

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.

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 123.

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 process controls what a known user can do within the system. See also “authentication”.

business network

A collective term for the network and attached systems at Level 4. See also “Levels 1 through to 4.”

Configuration Studio

Configuration Studio is an Experion tool that provides a central location from which you can configure your Experion system. Configuration Studio 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 licence details. When you click a task, the appropriate tool is launched so that you can complete the task.

Console

A logical grouping of Console Stations and Console Extension Stations.

Console Extension Station

A Station that provides similar functionality to a Flex Station but is hosted by a Console Station rather than an Experion server.

Console Station

A Station that has direct access to Process Controllers in addition to the server. Consequently, there is no loss of view of critical process data if the server fails.

Compare with a Flex Station.

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 (ACLs) that let a subset of services be visible from the Internet.

Distributed Systems Architecture

An option that enables multiple Experion 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

One of the options available with the Microsoft Windows Backup utility is the creation of an Emergency Repair Disk that can help you to fix damaged system files or repair a computer that will not start.

ERD

The abbreviation for “Emergency Repair Disk”.

FIM

The abbreviation for “Fieldbus Interface Module”.

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;en-us;832017`

Flex Station

A Station that is generally installed on a computer other than the server computer, and which is connected to the server using either a static or rotary connection.

Compare with a Console Station.

FTE

The abbreviation for “Fault Tolerant Ethernet,” the control network of Experion.

GUS

The abbreviation for “Global User Station,” a TPS node.

IP

The abbreviation for “Internet Protocol.”

Knowledge Builder

An online library that contains the complete Experion documentation set.

LAN

The abbreviation for “Local Area Network.”

Levels 1 through to 4

The location of a node within an Experion network and attached systems are often categorized in terms of a series of levels.

- Level 1 is where real time control takes place
- Level 2 is where supervisory control takes place
- Level 3 is where advanced control and advanced applications reside
- Level 4 is where the business network resides

Levels 1 to 3 inclusive constitute the “process control network.” Between Levels 3 and 4 you might have a demilitarized zone to help restrict unauthorized access to the process 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.

MES

The abbreviation for “Manufacturing Execution Systems.”

MRP

The abbreviation for “Manufacturing Resource Planning.”

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.

PCN

The abbreviation for “process control network.”

PHD

An abbreviation for “Process History Database.” PHD is Honeywell’s advanced historian, providing distributed data collection, and data consolidation.

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.

Process Controller

Experion’s controller, which can handle all possible control requirements—whether for continuous processes, batch processes, discrete operations, or machine control needs. The term is used to refer to all control hardware (chassis, power supply, Control Processor, and ControlNet bridge) as a single entity.

Points on a Process Controller are called *process points*.

process control network

A collective term for the network and connected systems at Levels 1 through to Level 3. See also “Levels 1 through to 4.”

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.

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.

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 Experion 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.

TPS

The abbreviation for TotalPlant® Solutions.

uninterruptible power supply

For a process 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.”

WSUS

The abbreviation for Microsoft Windows Software Update Services.

Index

Numerics

21 CFR Part 11 compliance
    electronic signatures 178

A

access
    dial-in 104
accounts
    Administrator 137
    engineer 137
    integrated 170
    new 137
    service and server 138
    user 160
ACLs 147
Administrator
    accounts 137
anonymous logon 157
antivirus measures 55
AntivirusUpdate Server
    firewall access requirements 91
audit log 123
auditing 123

B

backing up
    TPS systems 40
Backup and Restore 37
backups 35
    Microsoft utility 42
bots 63

C

computers
    dual-homed 105
Configuration Studio
    firewall access requirements 85
control levels 174

D

Demilitarized Zone 68, 72, 73, 74
desktop policy 156
dial-in access 104
disabling channels and controllers
    security level required 174
disaster recovery 35
Distributed System Architecture 76
DMZ 68, 72, 73, 74
DNS 103, 129, 131
documents
    related 15
domain controller
    and IAS 110
Domain Name Servers 103
domains 129, 131
DSA 76
dual-homed computers 105

E

EAS
    firewall access 88
electronic signatures 178
    21 CFR Part 11 compliance 178
email
    viruses 63
enabling
    channels and controllers 174
engineer
    accounts 137
engineering Station 85
Enterprise Model
    update 81
eServer
    firewall access 83

event response team 127
Experion Application Server
  firewall access requirements 88
Experion Backup and Restore 37

F

Fault Tolerant Ethernet 68
file shares 79
file system protection 147
firewall 68, 72, 73, 74
  Antivirus Update Server 91
  Configuration Studio access requirements 85
  DSA access requirements 76
  Enterprise Model update access requirements 81
  eServer access requirements 83
  Experion Application Server access requirements 88
  file share access requirements 79
  IntellaTrac PKS access requirements 114
  Microsoft Windows Software Update Services 89
  Mobile Access for eServer access requirements 116
  Mobile Access for Station access requirements 119
  PHD access requirements 93
  remote access for Station 85
forests 131
FTE 68
fullbkup 37

G

group accounts
  Windows 172
groups 130

H

High Security Network Architecture 68
High Security Policy 141
HTTP
  do not enable 102

I

IAS
  and domain controller 110
IIS 122, 150
IIS Lockdown Tool 150
Instant Messaging 63
integrated accounts 170
IntelaTrac PKS
  connecting 113
  firewall access requirements 114
  securing 108
inter-domain trusts 133
Internet Information Services 122, 150
intrusion detection 125, 127

L

LCN-connected nodes
  backups 40
levels
  network 68
locking Station 177
logon
  anonymous 157

M

MBSA 122
messaging 63
Microsoft Backup utility 37, 42
Microsoft Baseline Security Analyzer (MBSA) 122
Microsoft terms, important 12
Microsoft Windows Software Update Services
  firewall access requirements 89
mngr account 160
Mobile Access for eServer
  connecting 113
  firewall access requirements 116
Mobile Access for Station
  connecting 113
  firewall access requirements 119
Mobile Station
  securing 108
modems
  securing 104
monitoring

system 121

N

network
business
business network 72
planning 65
security 67
network equipment
securing 102
network interface card
wireless 110
network intrusion detection 125
networks
wired 108
NIDS 125
NTLM 158

O

ODBC client authentication 175
operating system
restricting access to 176
securing 135
operator-based security 167
Signon Manager 171
organizational units 130
Overview document 15

P

PHD
firewall access requirements 93
physical security 43
port scanning 106
process control network
connecting to business network 72
Process Controllers
planning documentation for 15

R

RADIUS protocol 110
RAS 153
recovery tools 35
registry protection 147
remote access 104
firewall access requirements 85
Remote Access Service (RAS) 153

S

scanning
ports 106
securing
network equipment 102
Station 176
wireless devices 108, 109, 110
securing networks 67
security
electronic signatures 178
levels 173
operating system 176
physical and environmental 43
Signon Manager 171
Station-based
configuring 166
Windows 176
security program 25
Security Response Team 34
security team 25
security updates 49
service and server accounts 138
service packs 49, 52
Signon Manager 171
Single signon 171
SMS Network Monitor 154
Software Change Notice (SCN) 15
spyware 63
SQL Server 151
Station
disabling menus 177
engineering 85
locking in full screen 177
restricting access 176
securing 176
security levels 173
Station security 165
electronic signatures 178
operator-based 167
Signon Manager 171
Single signon 171
system monitoring 121
system services 143

T

Telnet
    do not enable 102
Terminal Services 152
terminology 12
TPS
    backups 40
trees 131
trusts
    interdomain 133

U

updates
    security 49
user accounts 160
users 130

V

viruses 55
    email 63

W

WAPs 108, 109, 110
    firewall access 110
Windows
    securing 176
    Terminal Services 152
    user accounts 160
Windows group accounts 172
Windows security 171
wired networks 108
wireless devices
    connecting 113
    securing 108, 109, 110
wireless network interface card 110

Honeywell Process Solutions
2500 West Union Hills Drive
Phoenix AZ 85027
USA
www.honeywell.com

EP-DSX174
11/05
© 2005 Honeywell International Inc

Honeywell