

Experion
Server and Client Configuration Guide

EP-DSXX24

300

06/06

Release 300

Document	Release	Issue	Date
EP-DSXX24	300	1	June 2006

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 2006 – 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 and 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 About this guide	25
Before reading this guide	26
Prerequisite skills.	26
How to use this guide	27
2 Configuration overview	29
Configuration environment and tools	30
Configuration Studio	30
Server scripting	32
Using Experion data in other applications	33
Configuration procedures	34
3 Configuring your Enterprise Model	37
About the Enterprise Model	38
About the system model	39
About assets and the asset model	40
Asset model terminology.	40
Asset relationships/hierarchies	41
Naming rules for assets	42
About assignable assets.	44
About unassigned items.	45
Enterprise Model configuration tasks	46
About generic displays	48
4 Configuring the Network tree	49
About the Network tree	50
Network tree configuration tasks	52
Adding computers to the Network tree	52
Adding FTE communities to the Network tree	53
Adding a switch to the Network tree.	54
Loading the Network tree configuration	54
Removing items from the Network tree	55
Managing items in the Network tree	55
Providing access to the Network tree	56
5 Configuring system performance and event monitoring	57
About system performance and event monitoring	58

Enabling notifications using an Event Filter	59
About event filters	59
Setting up System Performance Server	60
Changing the System Performance Server scope	60
Adding system performance data to displays	61

6 Configuring Stations and printers 63

About Station.	64
What type of Station are you configuring?	64
About configuration	65
Station connections	66
Connection types	66
Connection methods	66
Station setup files	67
Customizing the initialization parameters of Station	68
Web access.	68
Specialized keyboards	68
Station scripting.	69
Printers	70
Configuring Station connection properties	72
Starting Station	72
Configuring Station connections	72
Customizing toolbars, menus and keyboard shortcuts	74
Multi-window toolbar and menu configuration	80
Controlling LEDs on a specialized keyboard	81
Configuring Station settings	83
Configuring timeouts.	83
Configuring startup displays	84
Setting the fast raise/lower step	85
Configuring alarm settings	86
Specifying associated Stations	87
Working with faceplates	89
Accessing Experion using Internet Explorer	91
Setting up Station Help	92
Setting up the server as a trusted site on the Station computer	94
Connection Properties	95
Customize dialog box	100
Menus tab	101
Toolbars tab	101
Keyboard Shortcuts tab	102
Command Properties dialog box	102
Server wide settings	107
Flex Station Configuration Display.	113
General tab	113
Assignment tab	115

Station.ini	116
Environment variables	120
7 Configuring Icon Series Console	121
About Icon Series Console	122
About multi-window Station	123
About multiple static Station	124
About master Station	124
Configuring Station for an Icon Series Console	125
Configuration tasks for multi-window Station	125
Configuration tasks for multiple static Station	126
Configuring setup files	127
Configuring a SafeView workspace configuration file	129
Controlling the location of faceplates	130
Controlling the location of Station command and status windows	131
Updating the page-level shortcut menu	132
Starting multi-window Station	133
Starting multiple static Station	134
Configuring a touch screen	136
Customizing keys	137
Adding manual input modules	138
8 Configuring point servers	139
About point servers and flexible points	140
Defining point servers in Station	142
Point server tuning	143
9 Configuring controllers	145
About controllers and channels	146
Connecting controllers to the server	146
Monitoring communications	146
Communications redundancy	148
Building channels	149
Defining redundant communication links	149
Configuring Stallion EasyConnection Adapter channel	150
Building controllers	155
Enabling and disabling channels and controllers	156
Enabling a channel	156
Enabling a controller	157
Monitoring channel and controller communications	158
Channel status and error statistics	158
Controller status and error statistics	158
Viewing channel and controller configuration information	159
Viewing channel configuration summary	159

Viewing the controller configuration summary	159
Viewing point names on a specific controller	160
Viewing controller configuration details	160

10 Understanding and configuring points 163

About points	164
Before you configure your points	164
After you configure your points	165
Point types	166
About flexible points	167
About derived points	168
Point names	169
Associating points with assets	171
Flexible point parameters	172
Standard point parameters	173
Summary of standard point parameters and addresses	174
Status point parameters	175
Analog point parameters	178
Accumulator point parameters	183
Summary of internal parameters	186
Source and destination addresses	195
Scanning and standard points	196
Control properties for flexible points	199
Control confirmation	199
Control modes	199
Control properties for standard points	200
Reverse output	200
Control confirmation	201
Control modes	201
Control level	202
Control properties for status points	203
Control properties for analog points	205
Configuring alarms for standard points	207
About alarms and events	207
Status point alarms	209
Specifying addresses for alarm acknowledgments	210
Analog point alarms	211
Accumulator point alarms	214
History collection and archiving	215
Types of history collection	215
History file sizes	216
Gating points, parameters and states	217
Viewing history collection configuration	218
History archiving	218
Configuring history archives	220

Configuring Station displays for points	222
Changing point configuration via Station displays	225
Calling up a point detail display	225
Advanced point configuration	226
Database addresses	226
Using auxiliary parameters	228
Building points off-scan	228
Creating user-defined data formats	229
Understanding internal point numbers	234
Configuring algorithms	235
PV algorithms	235
Action algorithms	236
Defining algorithms	237
Viewing algorithm configuration information	237
Finding free algorithm blocks	238
11 Configuring and customizing notifications	239
About notifications	240
Where do you configure notifications	241
Configuring system alarm priorities	242
Configuring messages	243
Enabling automatic message acknowledgement for confirmable messages	244
Configuring alerts	245
Connecting Experion and the User Alert application	246
Configuring external alarm notification	247
Configuring unanswered alarms	248
Customizing alarm behavior	249
Elevating the alarm priority	249
About the precedence of alarms in the alarm line	249
Disabling alarming	250
Customizing alarm behavior for Process alarms	251
Alarm Summary overflow	251
Configuring page acknowledgement	252
Customizing alarm colors	253
12 Configuring aggregate alarming	255
About aggregate alarming and alarm groups	256
Adding aggregated alarm information to custom displays	258
13 Configuring alarm paging	265
About alarm paging	266
Configuring alarm paging for pagers	267
Initial configuration	267
Supported service providers	269
Configuring alarm paging for email	270

Initial configuration	270
Configuring alarm paging for SNMP	272
Initial configuration	272
Configuring recipients, schedules and escalation	274
Nominating alarms to be sent	276
Nominating alerts to be sent	278
Viewing and clearing the message queue	279
Common settings	280
14 Configuring security and access	281
About security	282
Understanding Station security	283
About Station-based security	283
About operator-based security	283
Operator-based security and point control	285
About security levels	285
Using integrated security	287
About single signon	287
System configurations	287
User environments	297
Domain environments	299
About the Operator Management Service	299
Setting the Operator Management Service account	301
Configuring Station-based security	303
Using passwords in Station-based Station security	303
Configuring operator-based security	304
Adding an operator	306
Modifying operator configuration details	309
Deleting operator configuration details	310
Disabling an operator account	310
Converting traditional operator accounts to integrated accounts	311
Adding an Experion Windows group account	312
Determining the security settings for Windows group operators	312
Deleting an Experion Windows group account	316
Changing passwords	317
Setting and changing passwords for Station-based security	317
Changing password for traditional accounts	318
Changing passwords for integrated accounts	319
Defining sign-on restrictions	320
Configuring Sign-on administration	322
Configuring password administration for traditional operator accounts	322
Configuring Integrated Security policy	323
Using High Security Policy	324
About High Security Policy Workstation Package	325

Installing High Security Policy Domain Controller Package	327
Reviewing Group Policy Objects and Security Templates	329
Apply Group Policy objects to a global Windows group	330
Considerations for adding user accounts to Windows groups.	330
Linking the domain Windows groups to local Windows groups.	331
Enabling the Local Security Policy in a workgroup environment	332
Configuring profiles for scope of responsibility	333
Assigning scope of responsibility	336
Assigning scope of responsibility to Flex Stations	338
Assigning scope of responsibility to Console Stations	339
Assigning scope of responsibility to consoles.	339
Assigning scope of responsibility to operators or Windows group accounts	340
Assigning displays to assets	340
Actions permitted at each security level	341
Setting security levels for enabling/disabling channels and hardware	347
Changing the names of security levels	348
15 Signon Manager	349
About Signon Manager	350
Configuring Signon Manager	352
Using Signon Manager	353
16 Configuring Electronic Signatures	355
About Electronic Signatures	356
Considerations for Electronic Signatures and DSA	357
Customizing legal text.	358
Configuring Electronic Signature reason sets	359
17 Configuring group and trend displays	361
Configuring groups	362
About groups and displays	362
Creating groups	363
Modifying groups and points.	364
Deleting groups and points	364
Navigating to group displays.	364
Configuring trend displays	366
About trend displays	366
Configuring a trend	368
Changing trends.	370
Changing the scale on a trend	372
Changing the period on a trend	374
Adding a reference line to a trend	375
Viewing events with a trend	375
Zooming in on a trend	377
Saving your changes	377

Calling up trend displays	378
18 Template displays and container points	379
Engineering guidelines for container points	380
19 Customizing alarm, alert, event and message summaries	381
About the summary displays	382
Filtering the summaries	383
Filtering the Alarm Summary	383
Filtering the System Status display	385
Filtering the Alert Summary	386
Filtering the Event Summary	387
Filtering the Message Summary	389
Creating a custom filter	390
About Time Stamps	391
Sorting the summary displays	392
Customizing the layout of the summary displays	393
Creating a view	394
Changing the font size for the summary displays	396
Printing a summary as a report	397
Preventing operators from customizing the summary	398
20 Configuring reports	399
Report types	400
Pre-formatted	400
Additional custom reports	401
How reports are used	402
Configuring reports	403
Entering report content configuration details	406
Changing the date format for reports	407
Modifying report configuration details	408
Configuring field sizes	408
Alarm and Event reports	409
Alarm and Event DSA reports	411
Alarm Duration reports	413
Cross Reference reports	415
Point Attribute reports	417
Sequence of Events reports	418
Batch reports	419
Creating a points list	422
Batch report filenames	423
Starting and stopping a batch report	424
ODBC Data Exchange reports	425
Microsoft Excel reports	426

Creating custom reports with Microsoft Excel	427
Creating the report definition file	427
Saving the report definition file	428
Security issues	428
Configuring the Microsoft Excel report details	429
Configuring Free Format Reports	432
Free format reports	432
Creating a report definition file	432
Configuring the report details	433
Free Format report reference	434
Structure of a report definition file	434
Variable definition section	434
Saving report definition files	435
Variable definitions by functions	435
Using point values	436
Storing values in point parameters	436
Performing calculations	436
Working with historical data	437
Using server database and operating system file values	437
Formatting the report output	438
Free Format variables reference	439
A (Acquired Field Value)	440
B (Start of Report Body)	441
C (Calculated Variable Definition)	443
D (History Standard Deviation)	444
F (Fetch From Point)	445
G (Give to Point)	449
L (History Maximum and Minimum)	450
M (Operating System File Definition)	451
P (Perform Calculation)	452
R (Read From File)	453
T (Totalize History)	455
W (Write to File)	456
X (Demand Point Processing)	458
Free Format Report Example	459
Report output	460
21 Configuring and monitoring a redundant server system	463
About redundancy	465
Network redundancy	467
Network redundancy with FTE	467
Network redundancy without FTE	468
Station network redundancy	468
Redundant server network redundancy	469
Completing the TCP/IP configuration of the servers	470
Single network configuration	470

FTE configuration	472
Dual network configuration.	473
Checking network card settings	476
Defining the redundant connections	477
Redundant arbitration	477
Data links between primary and backup servers	479
Configuring Stations for server redundancy	481
Single network and FTE configuration	481
Dual network configuration.	481
Synchronizing the server databases.	483
Synchronizing the Engineering Repository database	484
Synchronizing the Enterprise Model database	485
Monitoring redundant servers	486
Using Station to monitor redundant servers	486
Using points to monitor redundant servers	487
Synchronizing other files	489
Changing the default transfer period	490
Failover of a redundant server system.	491
Manually failing over a redundant server system	493
Server redundancy fast failover configuration	494
Time until backup server becomes primary	494
Time until server disconnects Station	495
Time until stations fail over to backup network	496
Making IP address resolution faster	497
FTE-specific configuration	498

22 Configuring Distributed System Architecture 499

Overview	500
Requirements for implementing a DSA system	501
Data access	503
How remote points are located	503
Point IDs	503
Displays in a DSA system.	505
Displays locations	505
Consolidated Alarm Summary	505
Associated displays	506
Notifications	507
Alarms	507
Disabling alarms in a DSA system	507
Alarm and message acknowledgement policy	508
Message index	508
Journaled events	508
Journaled operator changes	509
Trends	510
Security	511

Working with DSA	512
Working with algorithms	512
Configuring hardware items	512
Performance considerations.	512
Multicasting.	513
Synchronization considerations.	513
Server redundancy and networks.	513
Operator keyboard support	514
Internationalization	514
Configuration for Distributed System Architecture	515
Configuring servers to subscribe to data and alarms.	516
Tuning your distributed system	517
23 Configuring Console Stations and consoles	521
About Console Station.	522
About Database and File Replication	524
Security	525
Configuring a Console Station	527
Configuring Console Station details	529
Configuring Console Station options	530
Assigning scope of responsibility to a Console Station	532
Configuring LEDs on operator keyboards for Console Stations.	533
Configuring the Station connection properties on the Console Station.	534
Deleting a Console Station	535
Adding Console Extension Stations	536
Configuring the connection properties on a Console Extension Station.	538
Configuring a Console Extension Station to access custom displays on the Console Station	538
About consoles	540
Configuring consoles.	543
Configuring a console	544
Configuring console options	545
Assigning scope of responsibility to a console	547
Configuring LEDs on operator keyboards for a console.	548
Adding Console Stations to a console	549
Deleting Console Stations from a console.	550
Deleting a console	551
About alarm and message acknowledgement/silence synchronization.	552
Alarm acknowledgement and consoles	552
Alarm silence and consoles	554
Sending displays to another Console Station	557
Sending displays using aliases.	559
24 Configuring eServer	563
About eServer	564

eServer configuration procedures	565
Setting up eServer access to Experion servers	566
Tuning eServer for standard access.	567
eServer security	569
Securing access to the eServer	569
eServer Stations and operators	569
Restricting access to assets	570
Considerations for Standard Access displays	571
Considerations for Premium Access displays	572
Setting up a home page for eServer.	574
25 Configuring Mobile Station	575
About Mobile Station	576
Using Mobile Access for eServer Standard	577
26 Configuring Remote Engineering and Station Server	579
About Remote Engineering and Station Server	580
Configuration and connection guidelines	581
Configuring and connecting to Mobile Access for Station	582
Remote Engineering and Station Server	582
Remote devices	583
Connecting to Station or to Configuration Studio	584
Configuring and connecting to Mobile Access for eServer Premium.	585
Remote Engineering and Station Server	585
Remote devices	586
Connecting to eServer Premium	586
Starting Microsoft Terminal Services Client or Remote Desktop Connection	588
27 Configuring File Replication	589
Understanding File Replication.	590
About replications	590
Configuring File Replication.	592
Configuring replications on an Experion server	595
Preparing the backup server	598
Configuring replications on a client computer	599
Using File Replication.	601
Running a replication manually	601
Running a replication automatically	602
Checking the status of a replication	602
Example scenarios.	603
28 Configuring schedules	609
About schedules	610
Point control schedules	610
Considerations when adding a Point Control Schedule	610

Configuring holiday and shift details	611
Configuring holidays	611
Configuring shifts	612
Configuring Point Control Schedules	613
Adding a schedule	613
Deleting a schedule	616
Updating or copying a schedule	616
Event log entries for schedules	617
Filtering the Point Control Scheduler	617
29 Configuring recipes	619
About recipe configuration	620
Configuring points for recipes	622
Configuring recipes	623
Defining a recipe	623
Defining the ingredients of the recipe	624
Chaining recipes	625
Configuring custom reports	626
Running custom reports automatically	626
Configuring a free format report	626
30 Configuring Event Archiving	629
About Event Archiving	630
Methods of archiving	630
Performance considerations	630
Estimating space requirements	631
Restoring events	631
Event tamper detection	632
Event Archiving system configuration	633
Event Archiving status	635
About Windows backup	636
31 Configuring Experion ODBC	637
About the Experion ODBC driver	638
Configuring the Experion ODBC driver	639
Configuring a data source	640
Connecting to the Experion server database	642
What data can you access with the Experion ODBC driver?	645
Case-sensitive searches	660
Searches Containing Special Characters	660
Using Experion ODBC driver and Microsoft Access	661
Using the Experion ODBC driver with Visual Basic and C++	668
ODBC Standard compliance	670
About Experion ODBC Data Exchange	671
Configuring ODBC Data Exchange Reports	673

Configuring the ODBC Data Source	674
Configuring the ODBC Data Exchange report	675
Creating the input reference file	679
Checking commands	681
ODBC Data Exchange report reference	682
Point reference type.	683
History reference type report	685
Table reference type report	687
SQL report example	690

32 Configuring OPC 695

Experion OPC Options	696
Experion OPC Client Interface	697
Experion OPC Advanced Client	698
Experion OPC Display Data Client.	699
Experion OPC Data Access Server	700
Experion OPC Historical Data Access Server	701
Experion OPC Alarm and Event Server	702
Experion OPC Integrator.	703
About OPC	704
About the OPC Data Access Standard	704
About Experion-to-OPC Server/Client communications	706
Configuring the Experion OPC Advanced Client.	709
Configuring the OPC server connection	710
Mapping OPC alarms/events to Experion alarms/events	714
Experion support for OPC event attributes	716
Configuring the Experion OPC Display Data Client	718
Configuring the Experion OPC Data Access Server.	720
Accessing Experion data	721
OPC-accessible point parameters	724
Error codes and qualities	737
Configuring the Experion OPC Historical Data Access Server	738
Supported interfaces and methods.	739
Supported aggregates	740
Configuring the Experion OPC Alarm and Event Server	741
Configuring Experion OPC Integrator	743
Recommended practices for configuring Experion OPC Integrator	744
Performance considerations	746
Bidirectional data transfer	752
Configuration tasks	753
Configuring OPC Integrator alarms	754
Configuring OPC groups.	755
Enabling OPC Integrator groups.	761
Checking the status of OPC Integrator groups	762
Location of OPC Integrator files.	763

OPC Integrator alarms and events	764
Monitoring the status of the Experion OPC Integrator	766
33 Configuring Microsoft Excel Data Exchange	769
Changing the read/write permissions for Microsoft Excel Data Exchange	770
Using the Microsoft Excel Data Exchange wizard	771
Retrieving point parameters	771
Retrieving historical information	772
Using cell formulas	774
Changing the data updating rate	775
Enabling Microsoft Excel Data Exchange under different user accounts	776
Interpreting Microsoft Excel Data Exchange errors	777
Using Experion parameters with Microsoft Excel Data Exchange functions	778
Microsoft Excel Data Exchange functions	779
Formula arrays	779
GetHistVal_Date	781
GetHistVal_Offset	782
GetHistValArray_Date	783
GetHistValArray_Offset	784
GetPointVal	785
GetPointValArray	786
PutPointVal_Number	787
NAPI_rGetdat_int, NAPI_rGetdat_double, NAPI_rGetdat_float and NAPI_rGetdat_long	788
NAPI_rGetdat_str	789
NAPI_rGethstpar_date	790
NAPI_rGethstpar_ofst	791
NAPI_rGetPnt_Num	792
NAPI_rGetPnt_Status	793
NAPI_rGetVal_Ascii	794
NAPI_rGetVal_History	795
NAPI_rGetVal_Number	796
NAPI_rPutdat_int, NAPI_rPutdat_double, NAPI_rPutdat_float, NAPI_rPutdat_long and NAPI_rPutdat_str	797
NAPI_rPutVal_Number	798
34 Developing custom applications	799
35 Integrating PHD	801
PHD integration architecture overview	802
PHD and Experion tag synchronization components	802
Data link and history	803
PHD point server	803
Configuring the Experion-PHD Link	804
Tuning the PHD point server	805

Changing PHD retrieval attributes	805
Changing history timeout	808
Changing the confidence value	808
Guidelines for optimizing performance	809
Assigning TPS point parameters to history	811
Importing HM history assignment into Experion	812
Creating an LCN-connected server point build file	814

36 Command reference 815

Running Experion commands/utilities	816
Installation/migration commands	817
sysbld	818
utbconv	820
Configuration commands	823
alglst	824
bckbld	825
dspbld	828
hdwbckbld	829
hdwbld	830
hscconfig	831
paswrld	832
pntbld	833
qckbld	834
rtusum	835
station	836
Experion PKS Server Configuration Panel	838
Controller configuration commands	839
hdwconfig	840
tdc_cl	841
Diagnostic commands	842
chkem	843
display	844
lissen	845
listag	846
tail	847
trace	848
Administration commands	850
hscserver /start	851
hscserver /stop	852
dspclr	853
hisint	854
usrlrn	855
tagflb	856
Database initialization commands	857
pntdel	858

almint. 859

Application development commands 860

Glossary

About this guide

1

This guide is intended primarily for engineers and system administrators who are responsible for configuring and supporting Experion Release 300.

It describes:

- The recommended order for configuring the server
- Mandatory and optional configuration procedures
- Administration procedures



Attention

This guide describes the configuration procedures for systems that are using Honeywell and third-party controllers such as Allen-Bradley, Series 9000, TDC 3000 Data Hiway, UDC, and so on.

It does not describe the configuration tasks for the Honeywell Experion Process Controller. For information about configuring the Experion Process Controller, see the *Experion Process Control Building Guide*.

Before reading this guide

Before using this guide to configure Experion, you need to:

- Understand basic Experion concepts such as “channel,” “controller,” “point,” and “Station,” as explained in the *Overview Guide*.
- Install the Experion and third-party software as described in the *Software Installation and Upgrade Guide*.

In following the procedures in this Guide, it is useful to have documented your site and processes (for example, in a single-line or process and instrumentation diagram) as suggested in the *Overview Guide*. This will help you to match it to the Experion database that you want to build.

Prerequisite skills

This guide assumes that you have a basic knowledge of the hardware you are using: that is, the computers, printers, network components, and especially the field devices and controllers, such as programmable logic controllers (PLCs).

It also assumes that you have a basic familiarity with the Microsoft Windows operating systems that you are using.

How to use this guide

“Configuration overview” on page 29 introduces you to the main configuration tasks and tools, and shows you where they are described in this Guide.

Configuring the server is described in the chapters listed below. These chapters do not, however, provide controller-specific configuration information. When configuring controllers for your system, you also need to see:

- The controller-specific online reference information that comes with Quick Builder
- The hardware documentation and third-party software documentation for the devices that you will be using in your system

For information about configuring the server, see:

- “Configuring your Enterprise Model” on page 37
- “Configuring Stations and printers” on page 63
- “Configuring Icon Series Console” on page 121
- “Configuring controllers” on page 145
- “Understanding and configuring points” on page 163
- “Configuring alarm paging” on page 265
- “Configuring security and access” on page 281
- “Configuring group and trend displays” on page 361
- “Template displays and container points” on page 379
- “Customizing alarm, alert, event and message summaries” on page 381
- “Configuring reports” on page 399
- “Configuring and monitoring a redundant server system” on page 463
- “Configuring Distributed System Architecture” on page 499
- “Configuring Console Stations and consoles” on page 521
- “Configuring eServer” on page 563
- “Configuring Mobile Station” on page 575
- “Configuring schedules” on page 609
- “Configuring recipes” on page 619
- “Configuring Event Archiving” on page 629
- “Configuring system performance and event monitoring” on page 57

For supplementary reference information, see:

- “Configuring Experion ODBC” on page 637
- “Configuring OPC” on page 695
- “Configuring Microsoft Excel Data Exchange” on page 769
- “Developing custom applications” on page 799
- “Command reference” on page 815

Configuration overview

2

This chapter introduces the configuration tasks and tools for Experion.

To configure Experion means to customize the Experion server database for your plant. It involves defining communication connections, and the data acquisition and control that you want to implement at your site.

Configuration also involves setting up standard displays and reports, and a range of optional features such as redundancy, point control scheduling, event archiving, recipes, and so on.

Assumptions and prerequisites

The configuration procedures described in this guide assume that you have already installed Experion software and third-party software as described in the *Software Installation and Upgrade Guide*.

Configuration environment and tools

A typical Experion environment features the following components:

- One or more servers.
- One or more Console Stations.
- One or more Flex Stations and printers connected to the server. (In most basic systems, the Station software and the server software run on the same computer.)
- One or more controllers connected to the server.

You use Configuration Studio to configure your system. From Configuration Studio, the following tools are launched:

- Enterprise Model Builder (for configuring your asset model)
- Quick Builder (for configuring Flex Stations, printers, channels, controllers other than the Experion Process Controller, and points on those controllers)
- Control Builder (for configuring control strategies on Experion Process Controllers)
- System displays

The configuration tools are described below.

Configuration Studio

Configuration Studio provides a central location from which you can configure your Experion system. The individual tools required to configure parts of your system are launched from Configuration Studio.

In Configuration Studio, you are provided with a customized list of tasks that you are required to complete to configure your System. When you click a task, the appropriate tool is launched so that you can complete the task.

Enterprise Model Builder

Enterprise Model Builder is a graphical tool for building your asset model.

The procedures you use to build your asset model are documented in the *Enterprise Model Builder User Guide*.

Quick Builder

Quick Builder is a graphical tool for building the hardware items (Flex Stations, printers, controllers), standard points in your system.

After building hardware and points with Quick Builder, you download these items from Configuration Studio to the server database.

The procedures you use to build items with Quick Builder are documented in the *Quick Builder Guide*.

Control Builder

Control Builder is a graphical tool for building your control strategy for Process controllers.

The procedures you use to build your control strategy are documented in the *Experion Process Control Building Guide*.

System displays

System displays, called up in Configuration Studio, are used to configure items such as reports, group display, trends, Station settings, Console Stations, and so on.

The procedures you use to configure these items are documented in this guide (*Server and Client Configuration Guide*).

Display Builder

The HMIWeb Display Builder allows you to create custom displays using Web-based features and save the displays in HTML format.

HMIWeb Display Builder can run on the server or on another computer in your system.

The procedures you use to build custom displays are documented in the *HMIWeb Display Building Guide*.

Experion server utilities

Utilities that run on the server are available to assist you in configuration and administration tasks. Utilities that apply to specific controllers, such as communications testing utilities, are described in the controller references. General utilities are described in “Command reference” on page 815, and referred to throughout this guide.

Server scripting

You can extend the functionality of Experion by creating *server scripts*. As you configure your system, you may want to create server scripts for:

- Servers
- Point servers
- Points
- Reports

The type of script you want to create determines the tool you use. For example, if you want to create a script that runs at specified times, you use Station to create the script. If you want to create a script that performs a task when the status of a point changes, you use Quick Builder to create the script. For more information about server scripting, see the *Server Scripting Reference*.

Using Experion data in other applications

Experion provides the following methods for accessing data:

- The Experion ODBC Driver option is designed for retrieving Experion data via ODBC-compliant applications such as Crystal Reports, Microsoft Access, or Microsoft Excel. See “About the Experion ODBC driver” on page 638.
- The Experion ODBC Data Exchange Report option enables you to transfer data between the Experion server database and an ODBC-compliant database. See “About Experion ODBC Data Exchange” on page 671.
- The Experion OPC options enable Experion to exchange point and alarm/event data with third-party OPC servers and clients. See “Configuring OPC” on page 695.
- The Experion Application Programming Interface (API) and Network API enable you to create custom applications that run on the server or on other computers on the network. You can also use these APIs if you want to configure reports that initiate application programs. See “Developing custom applications” on page 799.
- The Microsoft Excel Data Exchange option enables you to capture real-time point value and history information from Experion and display the data in an Excel spreadsheet. See “Configuring Microsoft Excel Data Exchange” on page 769.
- The Experion Free Format or Integrated Microsoft Excel reports also allow you to extract Experion data. For details on these reports, see “Configuring Free Format Reports” on page 432 and “Microsoft Excel reports” on page 426.

Configuration procedures

The table below shows the tasks for configuring Experion in their recommended sequence. The table also shows:

- Which procedures relate to licensable options (“Experion Option”).
- Which procedures are optional (“optional procedure”).
- Where to find the information you need to complete the procedures.



Attention

While configuring Experion, it is recommended that you make regular backups (preferably daily). After configuration is complete, make a full backup. For information on performing backups, see the Experion *Backup and Restore Guide*.

Table 1 Configuration procedures checklist

Task	Tool	For Details, See...
Add operators to Experion so that configuration engineers can log on to Configuration Studio.	Station	“Adding an operator” on page 306
Build your system model and asset model	Configuration Studio - Enterprise Model Builder	“Configuring your Enterprise Model” on page 37 and the Enterprise Model Builder User Guide
Build your Network tree	Configuration Studio	“Configuring the Network tree” on page 49
Configure performance monitoring (Experion Option)	Configuration Studio	“Configuring system performance and event monitoring” on page 57.
Build Flex Station	Configuration Studio - Quick Builder	“Configuring Stations and printers” on page 63. Quick Builder’s help.
Build printers	Configuration Studio - Quick Builder	“Configuring Stations and printers” on page 63. Quick Builder’s help.
Define Station setup details, and complete Station and printer configuration	Station	“Configuring Stations and printers” on page 63.
Configure server-wide Station settings	Configuration Studio	“Configuring Stations and printers” on page 63.

Table 1 Configuration procedures checklist (*continued*)

Task	Tool	For Details, See...
Define point servers to the server	Configuration Studio	“Configuring point servers” on page 139
Build flexible points (Experion Options) and, if required, create server scripts.	Appropriate point server tool Quick Builder Station	Device-specific documentation. <i>Server Scripting Reference</i> .
Build your control strategy		
Build a control strategy for Process Controllers.	Configuration Studio - Control Builder	See the Experion Process Software documentation.
Build SCADA controllers and the communications paths from the controllers to the server	Configuration Studio - Quick Builder	“Configuring controllers” on page 145. Quick Builder online help.
Test communications between the server and the controllers	Controller-specific test utilities	Help for your specific controller
Build SCADA points (analog, status and accumulator) on controllers and, if required, create server scripts.	Configuration Studio - Quick Builder	“Understanding and configuring points” on page 163. Quick Builder online help. <i>Server Scripting Reference</i> .
Configure history collection	Configuration Studio	“Viewing history collection configuration” on page 218
Configure system security	Configuration Studio - Quick Builder	For server system security, see “Configuring security and access” on page 281. For operating system security, see the Administration and Startup Guide.
Configure a Redundant Server system (Experion Option)	Configuration Studio	“Configuring and monitoring a redundant server system” on page 463.
Define the servers that will form a Distributed System Architecture (DSA) (Experion Option)	Configuration Studio - Enterprise Model Builder	“Configuring Distributed System Architecture” on page 499.
Configure Console Station (Experion Option)	Configuration Studio	“Configuring Console Stations and consoles” on page 521.
Configure eServer (Experion Option)	Station	“Configuring eServer” on page 563.
Configure Mobile Station (Experion Option)	Station	“Configuring Mobile Station” on page 575.

Table 1 Configuration procedures checklist (*continued*)

Task	Tool	For Details, See...
Configure groups and trends (optional procedure)	Configuration Studio	“Configuring group and trend displays” on page 361.
Configure pre-formatted reports and create server scripts to run on completion of reports (optional procedure)	Configuration Studio	“Configuring reports” on page 399. <i>Server Scripting Reference</i>
Configure Point Control Schedules (Experion option)	Configuration Studio	“Configuring schedules” on page 609.
Configure Recipes (Experion Option)	Configuration Studio	“Configuring recipes” on page 619.
Configure Event Archiving	Configuration Studio	“Configuring Event Archiving” on page 629.
Configure Microsoft Excel Data Exchange and the ODBC options. Develop applications that use the Application Programming Interface (API), and Network API, (Optional Procedure)	Microsoft application development tools	“Using Experion data in other applications” on page 33. <i>Application Development Guide</i>
If required, create server scripts.	Configuration Studio	<i>Server Scripting Reference</i>
Build custom displays and, if required, create display scripts (Optional Procedure)	Display Builder HMIWeb Display Builder	<i>Display Building Guide</i> <i>HMIWeb Display Building Guide</i>
Perform backups	Experion Backup and Restore (Experion option) or Microsoft Backup/Experion fullbkup	<i>Experion Backup and Restore Guide</i>

Configuring your Enterprise Model

3

This chapter describes:

- System model
- Asset model
- The tasks required to configure an Enterprise Model.

About the Enterprise Model

The Enterprise Model allows process and enterprise information to be integrated and organized in terms of a model of the important entities in your enterprise. It provides a more meaningful method of:

- Navigating through your Experion system
- Managing alarms
- Defining scope of responsibility
- Organizing such things as points, displays, and reports
- Viewing the status of system components such as channels, controllers, and system interfaces



Attention

Before you begin, you should have read the planning information in the section “Assets”, in the *Server and Client Planning Guide*.

In Experion Release 300, the Enterprise Model consists of a system model, a network model, an asset model, and an alarm group model.

To learn about	Go to:
The system model	page 39
Assets and the asset model	page 40
Alarm groups	page 256
Enterprise Model configuration tasks	page 46
The network model	page 49

About the system model

The system model represents the boundaries of your Experion system. It defines the Experion servers that comprise your system, as well as defining the servers that are external to your system.

A system can consist of several Experion servers connected using Distributed System Architecture (DSA), or a system can be a single Experion server.

If you have several servers connected using DSA, one server contains information about all of the servers that comprise your system, as well as information about any servers that are external to your system. This information is stored in the Enterprise Model database (EMDB). During installation, you choose which of your servers will contain the EMDB. After you have defined your servers, this information is loaded from the EMDB to all other servers in your system.

If you have a single server system, the server contains the EMDB which contains the information about itself, and any servers that are external to the system.

If you have two separate systems, there may be circumstances under which you want to share data between systems. In this situation, you would define an external server in your system model.

After you have configured your system and all of its components, you can see a graphical representation of your system using the System Status display. The System Status display shows the servers that make up your system as well as the Stations, channels, controllers, system interfaces, and printers that are connected to each server.

About assets and the asset model

Assets can represent entities such as fixed plant equipment, materials, and buildings. The Asset Model provides an organizational structure to enable you to engineer your Experion system in a hierarchical manner around the key entities in your organization.

A hierarchical asset model assists with alarm management. The location pane in the Alarm summary contains a graphical view of your asset model which provides:

- An easy way to navigate the asset model
- Alarm filtering capabilities
- Aggregated alarms counts

The asset model also provides an intuitive way of allowing or restricting access to parts of the plant, process, or equipment with the use of assignable assets.

Asset model terminology

The following table describes terms associated with the asset model.

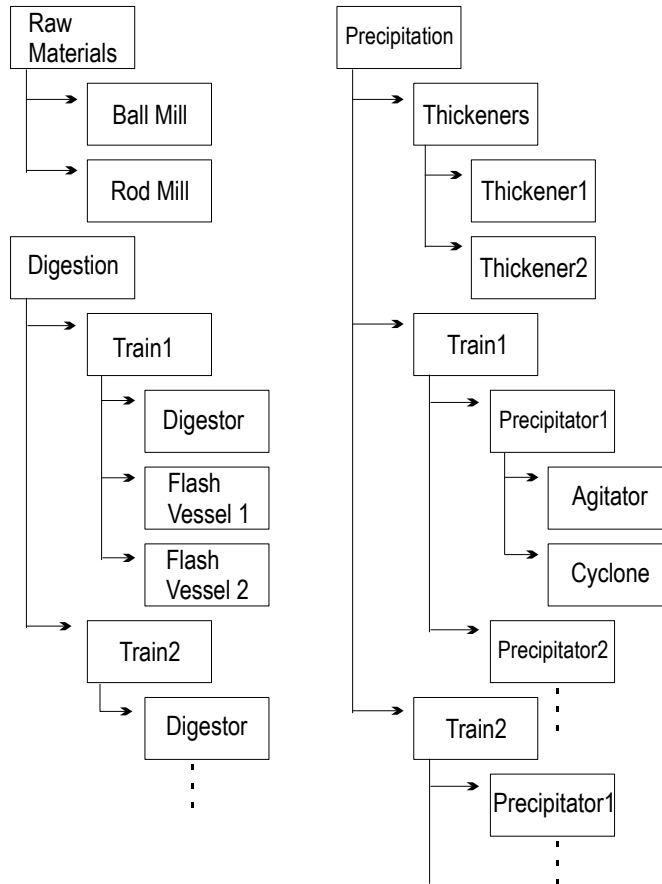
Term	Description
Asset	Represent entities such as fixed plant equipment, facilities, buildings.
Tag name	A unique identifier given to an entity, for example a point or an asset.
Assignable assets	An asset that can be assigned to an operator or Station for the purposes of controlling the scope of responsibility of an operator or Station and to enable or disable alarms for a particular asset.
Item name	An intuitive name given to an entity which can be used as an alternative to the tagname. The item name needs to be unique amongst entities with the same parent asset.
Full item name	Consists of the item name of the entity combined with the item name of its parent, and so forth, up to a top level node. A full item name uniquely identifies an entity within the system. For example, /assets/Plant/Filtration/Tank/FlowMeter. You cannot mix item names and tagnames to create a full item name.

Term	Description
Associated asset	An asset that is associated with an alarm group for scope of responsibility purposes.
Unassigned item	A point that is not associated with an asset. For example, if an asset has been deleted, points associated with the asset are considered unassigned items.

Asset relationships/hierarchies

The relationship or hierarchy you establish between your assets and entities essentially forms the asset model. The primary relationship in the asset model is that of asset containment, where one asset contains another.

Figure 1 on page 42 shows Raw Materials, Digestion, and Precipitation are all top level assets. The Raw Materials asset contains two assets, Ball Mill and Rod Mill. The Precipitation asset contains the Thickeners asset, which in turn contains Thickener1 and Thickener2.

Figure 1 Hierarchical asset model

Naming rules for assets

All entities in your system have a tag name and an item name. Tag names must be unique, whereas item names can be duplicated as long as the resulting full item name is unique. For example, in Figure 1 on page 42, there are two assets with the item name `Train1`. The full item name of these assets provides a unique name, `/Assets/Digestion/Train1` and `/Assets/Precipitation/Train1`.

Tag names and item names must follow the naming rules:

- Names must not be longer than 40 characters.
- Do not use the following characters:

- Tabs
 - Period (.)
 - Comma (,)
 - Forward slash (/)
 - Backslash (\)
 - Brackets []
 - Braces { }
 - Parentheses ()
 - Less than (<)
 - Greater than (>)
 - Single quote (')
 - Double quote (")
 - Asterisk (*)
 - Question mark (?)
 - Vertical bar (|)
 - Colon (:
 - Semi colon (;)
 - Space (tag names only)
 - The first character must not be any of the following:
 - Dollar sign (\$)
 - At sign (@)
 - Space
 - The last character must not be a space.
 - Names are not case-sensitive: `Cooling Tower1` and `cooling tower1` represent the same asset
 - An item name cannot match the item name of any other entity (including both points and assets) belonging to the same parent asset.
- A full item name:
- Must not be longer than 200 characters
 - Must be unique

About assignable assets

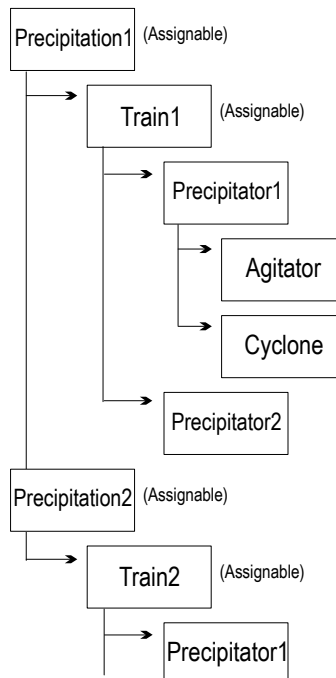
You use assignable assets so that you can:

- Assign appropriate scope of responsibility to operators or Stations.
- Enable or disable alarms for particular assets.

In the asset model structure, all top level assets are automatically set to be assignable. Below this top level, you can specify which assets are to be assignable.

If lower level assets are not configured to be assignable, the lower level assets inherit the assignment of the assets above them in the hierarchy.

In the following figure, the assets `Precipitation1`, `Train1`, `Precipitation2`, and `Train2` have been configured to be assignable. If an operator is assigned the asset `Precipitation1`, then the operator can view and control points, view and acknowledge alarms associated with the `Precipitation1` asset. The operator can only view and acknowledge alarms associated with the `Train1` asset and all assets below `Train1` if the operator is also assigned `Train1`. All points and alarms associated with `Train1` and any assets below are within the scope of responsibility of the operator who is assigned the asset `Train1`. If the operator is not assigned `Train2`, then any points or alarms associated with `Train2` and assets below are not included in the operator's scope of responsibility.



About unassigned items

Unassigned items are items that are not associated with an asset. For example, if you build a point but do not associate the point with an asset, when you download the point, the point is considered to be an unassigned item. Likewise, if you delete an asset but retain the points associated with the asset, those points become unassigned items.

Enterprise Model configuration tasks

To configure your Enterprise Model, complete the following tasks:

Task	Go to	Done
Plan your asset model. For considerations about planning an asset model.		
Set your system name using Configuration Studio. For instructions, see the following topic in Knowledge Builder: Experion R300 > Configuration > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Set system name (Rename System).		
Define your servers using Configuration Studio. For instructions, see the following topic in Knowledge Builder: Experion R300 > Configuration > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Add servers.		
Download the server definitions to all the Experion servers in your system.		
Create your assets and the asset model using Configuration Studio. For instructions, see the following topic in Knowledge Builder: Experion R300 > Configuration > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Creating and configuring assets.		
Download the asset model to all the Experion servers in your system. For instructions, see the following topic in Knowledge Builder: Experion R300 > Configuration > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Loading asset model and alarm groups.		
Build your points and assign parent assets to points by specifying the appropriate asset name when you define points in Quick Builder or Control Builder.		
Optionally, build alarm groups using Configuration Studio. For instructions, see the following topic in Knowledge Builder: Experion R300 > Configuration > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Creating and configuring alarm groups.		
Optionally, configure profiles.	page 333	

Task	Go to	Done
If you use Station-based security, assign assets to Stations for scope of responsibility.	page 338	
If you use operator-based security, assign assets to operators for scope of responsibility.	page 340	

About generic displays

By implementing a hierarchical asset model, you can create generic displays that can be used across your plant. For example, if you had a series of holding tanks within your plant, it is likely that the asset structure is repeated. A single display could be created that references this repeated structure and reused to display data for any of the holding tanks. Using the full item name (instead of just the tagname or point ID) in conjunction with system custom properties enables you to create generic displays.

System custom properties are like variables. Instead of binding an object on a display directly to a single point, you can bind the object to a system custom property.

At run time, the values of system custom properties can be stored in either the Station data repository or the display data repository. When you create the system custom property you set where the value of the property will be stored at run time by setting the scope.

If the scope of the system custom property is set to display, when you call up the display in Station, you set the value of the system custom property. The command for calling up a display containing a custom property is

displayname?custompropertyname=value, where *displayname* is the name of the display you are calling up, *custompropertyname* is the name of the custom property contained in the display, and *value* is the value you want to set for the custom property.

If the scope of the same system custom property was set to Station, you could create an application script to set the value of the system custom property when Station starts.

For more information about creating system custom properties, see the *HMIWeb Display Building Guide*.

Configuring the Network tree

4

This chapter describes the task required to add computers and devices to the network tree that is available on the System Status Display.

About the Network tree

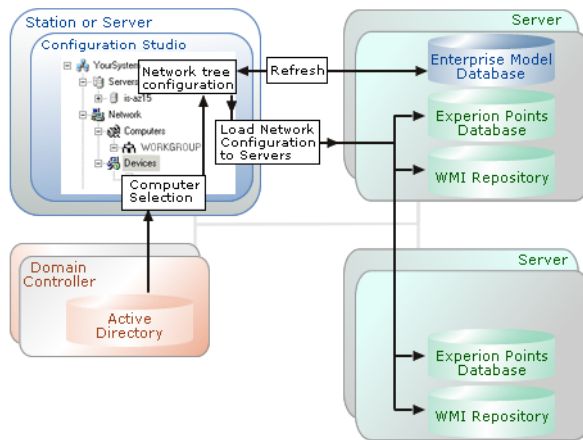
The Network tree is a graphical view of the nodes in your network, which can be viewed on the System Status display. (The System Status display also contains the System Components tree, which is automatically configured.)

You configure a Network tree so that you can view the status and health of network items from the System Status Display. From the network tree in the System Status display, you can then access detail displays for the network tree items that display performance and configuration data. In the Network tree, you can configure the following to appear:

- Computers that host applications or software such as Station, Server, or ACE.
- Collections of computers such as workgroups, domains, and Organizational Units.
- Devices such as switches and routers.
- Collections of devices and computers called FTE Communities.

The Network tree works in conjunction with the System Event Server and the System Performance Server to display system errors on the System Status display. Operators and engineers can use this information to diagnose or troubleshoot faults within the system.

Details about the items in your Network tree, such as computers, devices, and FTE Communities, are stored in system databases. The initial definition of the tree (using the Computer Add/Remove task) displays the latest view of computers, workgroups, and domains from the Active Directory. The Network tree configuration, as displayed in the Configuration Explorer, resides in the Enterprise Model database (EMDB). When you add (or remove) Network tree items, you must also load the configuration to the servers in the system so that the tree items can be stored as points in the Experion point database, in addition, switch and FTE Community information is stored in the WMI Repository. The following figure shows the relationship of user configuration tasks to the databases you update or load so that you can support your Network tree configuration.



If there is an inconsistency of the Network tree configuration between the EMDB and the Experion database, icons appear in the Network tree in Configuration Studio. For more information about resolving inconsistencies, see the *Server and Client Troubleshooting Guide*.

Network tree configuration tasks

This section describes the procedures to add items to the Network tree so that they appear in the Network tree on the System Status display.

Prerequisites

- Before you can load your network tree configuration, you must first have added servers to your system. For information on adding servers, see the following topic in Knowledge Builder:
Experion R300 > Configuration > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Add servers.
- To view Network tree items from remote Experion servers, DSA must be enabled between the servers. When you first define a server and download this server definition to other servers in the system, the default subscription for the server is disabled and it does not participate in the DSA.

Adding computers to the Network tree

Prerequisites

- The computer must have system management software installed. This is installed by default on all Experion nodes, however, for non-Experion nodes you will need to install this software manually.
- The computer has the correct multicast address.
- One server node hosting SES per FTE community has been determined to be the SES for the FTE community.

To add a computer to the Network tree:

- 1 In the Configuration Explorer in Configuration Studio, expand the System tree you are configuring and click **Networks**.
- 2 Click the **Add/Remove Computers** task.
The Computer Selection dialog box opens.
- 3 Select the check box for each computer you want to add to the Network tree and click **Apply**.
The computers are added to the Network tree in Configuration Studio.
- 4 Click the Load Network Configuration to Servers task.
- 5 Select the servers you want to download to and click **OK**.
You should download the network tree to all servers in the system.

Adding FTE communities to the Network tree

Considerations

- Nodes planned for the FTE community have been identified.
- One server node hosting SES per FTE community has been determined to be the SES for the FTE community.
- The FTE community name you specify should be meaningful to your operators, for example, the name can identify the grouping of FTE devices.

Prerequisites

- Multicast address for the community has been defined using the Node Definition Tool.
- Nodes in the FTE community have been configured to use the same multicast address using the Node Definition Tool. For more information about specifying the multicast address, see the following section in Knowledge Builder:
Experion R300 > Configuration > Experion Node Definition Guide > Modifying node definitions > Change the node's multicast address.

To add an FTE community to the Network tree:

- 1 In the Configuration Explorer in Configuration Studio, expand the System tree you are configuring and click **Devices**.
- 2 Click the **Define FTE communities** task.
The FTE Definition display opens.
- 3 Type the FTE community name and click **Apply**.
The FTE community appears in the devices tree.
- 4 Select the server hosting the SES for the FTE community.
The System Event Server appears with its multicast address defined.
- 5 Select the nodes for the FTE community.
- 6 Click **Apply**.

Changing multicast settings

The multicast address is initially configured using the Node Definition Tool. For information about defining a multicast address, see the following section in Knowledge Builder:

Experion R300 > Configuration > Experion Node Definition Guide > Modifying node definitions > Change the node's multicast address.

Adding a switch to the Network tree

Considerations

- The switch has been configured.

To add a switch to the Network tree:

- 1 In the Configuration Explorer in Configuration Studio, select the system you want to configure.
The Network tree appears underneath the system item.
- 2 Expand the Network tree.
- 3 Select the **Devices** item.
- 4 Click the **Add Switch to the Network tree** task.
- 5 Type the switch name, which is to be displayed in the Network tree, and its IP address. The switch name must contain only standard alpha-numeric characters; no spaces are allowed.
The switch name is also used to create a WMI namespace used for accessing switch data.
- 6 Click **Apply**.

Changing router settings

For more information about changing switch or router settings, see the *Fault Tolerant Ethernet Overview and Implementation Guide*.

Loading the Network tree configuration

You load the Network tree configuration after you have initially configured your Network tree or after you have made adjustments to the Network tree, such as deleting items. An icon appears next to the Network tree item in Configuration Studio to indicate that a change has been made and you need to load the configuration.

To load the Network tree configuration:

- 1 In the Configuration Explorer in Configuration Studio, select the system you want to configure.
The Network tree appears underneath the system item.
- 2 Click the **Load Network Configuration to servers** task.
- 3 Select the servers you want to download to and click **OK**.
- 4 Click **OK** when the load is complete.

Removing items from the Network tree

To remove an item from the Network tree:

- 1 In the Configuration Explorer in Configuration Studio, select the system you want to configure.
The Network tree appears underneath the system item.
- 2 Expand the Network tree and select the item you want to delete.
- 3 Click the **Remove this item from the Network tree** task.
- 4 Click **Yes** to confirm you want to remove the item.
- 5 Click the **Load Network Configuration to servers task** to download this change.
- 6 Select the servers you want to download to and click **OK**.

Managing items in the Network tree

If you have an existing item in the Network tree and you change details about this item, for example, you rename a computer or reassign an item to another Windows domain or Organizational Unit, you need to re-add the item to the Network tree.

Providing access to the Network tree

If you have particular nodes included in the Network tree that you don't want visible to particular operators or Stations, you can control this by assigning the appropriate scope of responsibility to your operators or Station (depending on which type of security you use).

For more information about assigning scope of responsibility, see “Assigning scope of responsibility” on page 336.

Configuring system performance and event monitoring

5

This chapter describes the tasks required to enable system event and performance monitoring.

About system performance and event monitoring

The Windows environment contains event and performance information which can be used for the proactive and reactive management of your system. System events such as disk errors or a problem with the FTE network can be detected through performance and event monitoring.

You integrate Windows-based system event and performance information with Experion by using the System Event Server (SES), the System Performance Server (SPS), and System Management software components (which are installed automatically). You can enable specific notifications and performance data to be collected by the SES and the SPS using Configuration Studio. The SES and SPS then send these notifications and data to the Experion server as OPC events and data items using a system interface which is automatically configured. As a result, notifications are included in the System Status display and the Event Summary. You can also add Windows data to HMIWeb displays.

Enabling notifications using an Event Filter

When you install the System Event Server, a default filter is created that exposes only FTE events. You can create filters for other Windows events or share an existing filter.

About event filters

Event filters define a subset of Windows events that are collected by the SES. These events may be generated by the Windows system, Honeywell applications, or third-party applications.

So that the notifications collected by the SES are consistent with notifications in Experion, you need to specify more information than is initially generated for each Windows event. When you create an event filter, you specify extra information such as:

- Event type
- Event source
- Severity
- Category
- Condition and subcondition
- Active/acknowledge state
- Attributes



Attention

Do not edit the filters supplied by Honeywell. Create your own filter (by copying or using Save As) to supplement this set of filtered events.

If you need to create your own filters, see the following topic in Knowledge Builder: Experion R300 > Configuration > System Management Configuration Guide > 8. Configuring Event Filtering > 8.2 Event Filtering Configuration Procedures.

Setting up System Performance Server

This section describes enablers such as SNMP Monitoring for System Performance Server to provide you performance data. No user configuration is required on the System Performance Server itself unless you need to change default settings described in this section.

Changing the System Performance Server scope

In general the default scope of domain is sufficient. If errors are being generated in the event logs because of access problems to specific nodes, change the scope to exclude the problematic nodes. Changing scope limits OPC browsing of third-party OPC clients, however, it does affect access to data items.

To change the scope of the System Performance Server:

- 1 In the Configuration Explorer of Configuration Studio, click Network to expand the Network tree.
- 2 Click the computer hosting the System Performance Server.
- 3 Click the Configure HCI Component tasks.
The HCI Component display appears.
- 4 Select the component named SPS *computername* where *computername* is the name of the computer where the System Performance Server is installed.
- 5 Click Enter/Edit Server Specific configuration.
The SPS Server Configuration display appears.
- 6 Click Add Static Computer nodes to list all nodes.
- 7 Select or clear the Check boxes as appropriate to limit the SPS scope to any combination of OUs and computers.
- 8 Select the nodes you want to monitor.
- 9 Click **OK**.

Adding system performance data to displays

After you have checked the status of the System Performance Server, you can add system data to your custom displays.

To create a custom display and to display system data:

- 1 Start HMIWeb Display Builder:
 - If you are on the Experion server, choose **Start > Programs > Honeywell Experion PKS > Server > HMIWeb Display Builder**.
 - If you are on a client computer, choose **Start > Programs > Honeywell Experion PKS > Client Software > HMIWeb Display Builder**.
- 2 Choose **File > New > Display**.
A blank display appears.
- 3 Click the  (Alphanumeric) icon on the Toolbox toolbar and then drag the pointer on the display to define the size, shape and position of an alphanumeric.
- 4 Double-click the alphanumeric to open the Properties Window, which shows the alphanumeric's current properties.
- 5 Click the **Data** tab and make sure that **Point/Parameter** is selected in **Type of database link**.
- 6 Select **SYSMGT** from the point list.
- 7 In the **Parameter** box, type the alias for the data item you want to display in the format *computername.alias*, for example, `localhost.BiosVersion`.
To find the alias names defined on the System Performance Server (SPS), do the following:
 - a. Choose **Start > Programs > Honeywell Experion PKS > System Management > System Management Display**.
 - b. Locate the SPS in the domain and organizational unit tree.
 - c. Right-click on the SPS name and choose **Configure** in the popup menu.
 - d. Click the **Aliases** tab.

Configuring Stations and printers

6

This chapter describes how to configure Stations and printers.

To learn about	Go to:
Station	page 64
Printers	page 70
Setting up Station	page 72
Configuration tasks using Station	page 83

About Station

Station is Experion's user interface. You use Station to monitor and control your system. Station displays are used to notify operators of alarm conditions. Station works in conjunction with Experion server, which:

- Collects data from your system and displays it in a manner that you can easily understand
- Allows you to control your system by sending appropriate commands
- Automatically performs scheduled tasks
- Notifies you of system activities, including alarms and system events
- Generates comprehensive reports

What type of Station are you configuring?

There are several different types of Station and several different environments in which Station operates. The two main types of Station are Flex Station and Console Station.

A Flex Station is connected to an Experion server and is the interface an operator uses to interact with your plant, as described above. A Flex Station is generally installed on a computer other than the Experion server and can use either the rotary or static connection type, as described in "Station connections" on page 66.

A Console Station provides all of the functionality available on a Flex Station, however, a Console Station has direct access to Process controllers and ACE nodes and enables an operator to monitor and control the plant regardless of the state of the Experion server or redundant servers. For more information about Console Stations, see "Configuring Console Stations and consoles" on page 521.

A Console Station also differs from a Flex Station in the following ways:

- A Console Station has its own connection type.
- A Console Station is not built using Configuration Studio.
- A Console Station is installed differently from a Flex Station.

In this chapter, the generic term Station is used. The terms Flex Station and Console Station are used to indicate if a particular function is applicable only to that type of Station.

In addition to a single instance of Station appearing in a single monitor, there are two potential configurations of Station for use with multiple monitors on a single computer:

- **Multi-window Station.** Using a single instance of Station, you can view multiple displays at one time and manage where and how displays are placed on a desktop that spans up to four monitors. For more information, see “About multi-window Station” on page 123.
- **Multiple static Station.** Allows you to have up to four instances of Station running simultaneously. With this configuration, you can position an instance of Station in each monitor.

The multi-window Station configuration can be used with both a Flex Station and a Console Station. The multiple static Station can only be used with a Flex Station.

Both of these configurations can be used in the Icon Series Console environment.

About configuration

After you have installed the Station software and built a Station item in Configuration Studio (for Flex Stations), you can change the default configuration of Station to your site requirements. Some of the Station settings you can configure are:

- Station connections
- Menus, toolbars and keyboard shortcuts
- Sounds
- Web Access
- Station Appearance

For information about configuring Station security features, such as restricting access to Stations by assigning scope of responsibility and using passwords for logging on to Stations, see “Configuring security and access” on page 281.

Station connections

Connection types

Stations can be connected to a server as either:

Type	Description
Static	Provides a permanent, dedicated link to a specific Station. This is the recommended connection type for operators.
Rotary	Provides an “as required” link to a Station. This is the recommended connection type for staff who do not use Station full-time. Rotary connections are advantageous from a licensing point of view because your license only specifies the number of simultaneously connected Stations.

Regardless of whether you define a Station as static or rotary, the maximum number of Stations that you can have connected to the server (and running the Station software) at any one time is determined by your license. If you define some of your Stations as rotary, you can install and configure a larger number of Stations in your system, but they cannot all be connected to the server simultaneously.

Connection methods

You can set up a Station connection using one of the following methods:

Method	Description
Network	Connects the Station to the server via a network.
Remote Access Service (RAS)	Connects the Station to the server remotely. RAS can support connection via a modem or a serial link.

For information about using RAS, see the section on installing a modem and configuring RAS in the *Software Installation and Upgrade Guide*.

Station setup files

When Station software is installed on a computer, two types of configuration files are installed, Station setup files (.stn files) and toolbar, menu and keyboard shortcut definition files (.stb files). The .stn file references the .stb file. These files define:

- Connection properties from Station to the server
- The general appearance of Station
- Commands on the menus and toolbars
- Function key actions

Station automatically uses `default.stn` and `default.stb` unless you select another setup file. You might have several setup files for connections to more than one server, or setup files with specific user preferences.

After you have installed the Station software, the default settings contained in `default.stn` and `default.stb` can be reviewed and customized. For more information on customizing Station connections, see “Configuring Station connections” on page 72.

In addition to `default.stb` there are several other preconfigured .stb files containing information relevant to specialized keyboards and the Icon Series Console. These additional .stb files are:

- `12fn.stb`
- `12fn_multiwindow.stb`
- `icon.stb`
- `icon_multiwindow.stb`
- `ikb.stb`
- `ikb_multiwindow.stb`

You need to update your connection properties to reference the appropriate .stb file as follows:

If you have a:	Use the:
12 function keyboard	12fn.stb or default.stb
Integrated Keyboard (IKB)	ikb.stb
Icon Series Console	icon.stb

Customizing the initialization parameters of Station

You can customize initialization parameters of Station by editing the `station.ini` file. Use a text editor to open the file in `%systemroot%`, that is example, `C:\windows\station.ini` for Windows XP and Windows Server 2003. For details on what you can customize see “Station.ini” on page 116.

Web access

You can set up Station so that operators can call up Web pages that could, for example, contain operator procedures. You can also set appropriate security to prevent operators from calling up unauthorized Web pages or other documents in Station. To set the security you need to specify the Web pages or documents that operators can call up using the **Web Access** tab of the **Connection Properties** dialog box. (See “Web Access tab” on page 98.)

Specialized keyboards

You can use either the Integrated Keyboard (IKB) or the Operator Entry Panel keyboard (OEP) with your Station computer to control your plant.



Attention

The IKB and the OEP keyboard are not compatible with Electronic Signatures. You cannot use either of these keyboards if you use Electronic Signatures functionality.

Both keyboards have a set of shortcut keys with predefined actions assigned. You cannot reassign actions to these predefined shortcut keys. For a list of shortcut keys and the assigned actions see the reference chapter in the *Operators Guide*.

Both keyboards also have a set of keys to which you can assign actions, and LEDs that you can control. For example, you can set up a key so that the LED on a particular key is red, fast blinking when a point goes into alarm and when the operator presses the key, the associated display is called up for the point in alarm.

For information on customizing keys see “Customizing toolbars, menus and keyboard shortcuts” on page 74. For information on controlling LEDs see “Controlling LEDs on a specialized keyboard” on page 81.

Station scripting

You can implement more sophisticated Station customization by creating application scripts or Station scripting objects that can be run on Station. For example, you might want to configure Station so that a specific display is shown on operator changeover.

For more information on Station scripting objects and the Station object model, see the Automation Objects chapter in the *Application Development Guide*.

Printers

Printers that are intended for printing reports or alarms and events are defined with Configuration Studio. When you have defined your printers, you assign printers to specific tasks. For more information see “Printer Assignment” on page 114.

You can assign any printer as one of the following:

Property	Description
Report printer	Print reports requested by operators, generated as a result of a status change in the system, or generated on a periodic basis.
Alarm/event printer	Prints details of alarms that are configured to print on any printers associated with Stations assigned to the asset that contains the point in alarm. If you use operator-based security, the asset assignment and printer settings of the operator who is currently logged on to a Station determine which alarms are printed.

Considerations

- An alarm printer needs to be a line-by-line printer, because alarms and events must be immediately available to the operator as hard copy. Laser printers are not suitable because they either buffer a full page of events before printing or print only one line per page.
- Alarm/event printers can be segregated to print alarms and events associated with particular assets. (See “Assigning scope of responsibility” on page 336 for details.)
- Do not configure a printer as both a report printer and an alarm/event printer. Doing this causes report and alarm/event data to be mixed in together.
- When you configure reports, you can specify which printer is to be used for a given report.
- If you select a network printer for report printing, you must ensure that you create the network printer locally with the correct login account. See the *Installation Guide* for details.

Printing displays

When operators print displays, such as Trends and Point details displays (using the Action > Print menu option in Station), the display is printed using the Windows default printer defined for the Station computer.

The Windows default printer for a computer is defined in Windows (Start > Settings > Printers).

Configuring Station connection properties

This section describes how to start and configure Station.

To:	Go to:
Start Station	page 72
Configure Station's connections	page 72
Customize Station's toolbars, menus and keyboard	page 74

Starting Station

To start Station:

- 1 Choose **Start > Programs > Experion PKS Server > Station**.

To use a setup file other than default.stn:

- 1 Choose **Station > Connect**.
The **Connect** dialog box opens.
- 2 Select the required .stn file from the **Recent Connections** tab or the **Other Connections** tab.
- 3 Click **Connect**. Station connects to the server using the connection information contained in the setup file you specified.

Configuring Station connections

Considerations

- The **Connection Properties** menu item might be disabled on Stations that have had the startup command line modified for security reasons.
- The default behavior of selection on faceplates, including faceplates in detail and group displays is to timeout. (Note: You can set the time period after which this selection is removed. This is the system select timeout which is configurable on the System Configuration display.)

To ignore select timeouts on faceplates, open the Station connection properties dialog and view the advanced settings. In the grid find the entry for **IgnoreDeselectOnFacePlates** and set its value to 1. To allow select timeouts on faceplates, set this value to 0.

To create a new .stn file:

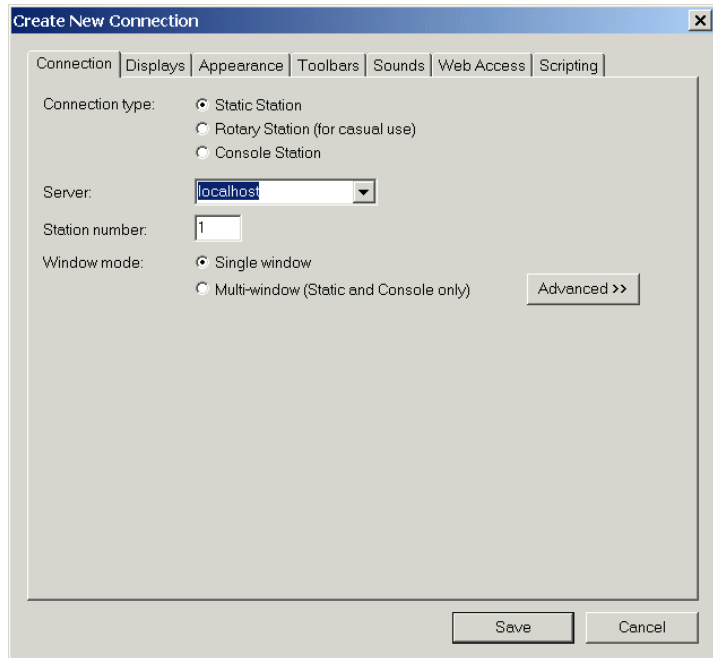
- 1 Choose **Station > Connect**.

The **Connect to** dialog box opens.

- 2 Click **New Connection**.

The **Create New Connection** dialog box opens.

Figure 2 Create New Connection dialog box



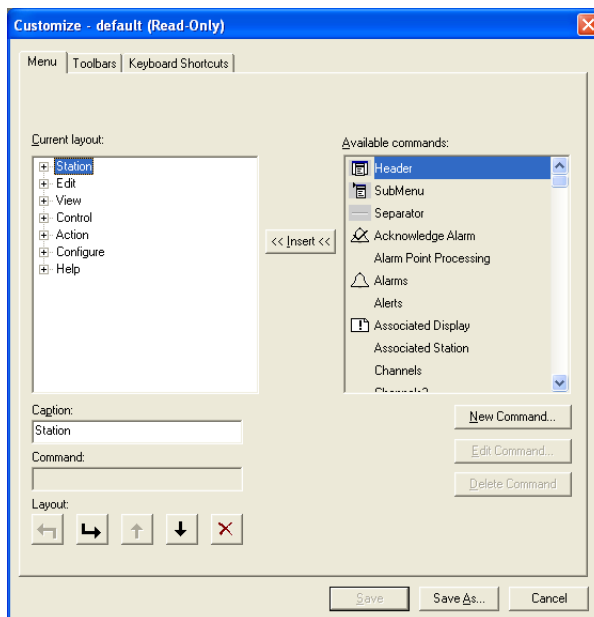
- 3 Use the tabs and options in the **Create New Connection** dialog box to review or modify the settings, as described in "Connection Properties" on page 95. For information on customizing menus, toolbars see "Customizing toolbars, menus and keyboard shortcuts" on page 74.
- 4 Click **Save** and specify a filename to save the settings to a new file.

Customizing toolbars, menus and keyboard shortcuts

You can create additional commands and add them to the toolbars, menus or assign keyboard shortcuts. You can also add new menus and submenus and you can add toolbars to Station.

Considerations

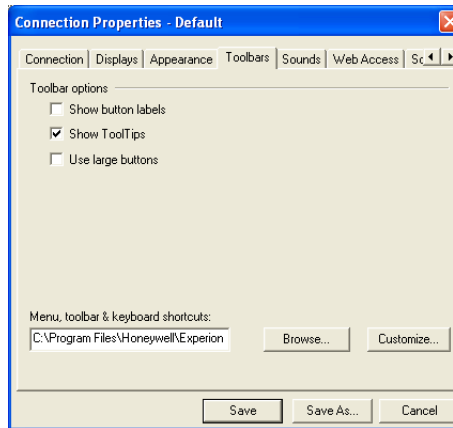
- When you create a command it appears in the list of available commands on the **Menus** tab and the **Toolbars** tab. If you assign a keyboard shortcut to the command, the command and the assigned keyboard shortcut then also appear in the list on the **Keyboard Shortcuts** tab.



- Toolbar button icons are stored in the Program Files\Honeywell\Experion PKS\client\system\R300\toolbar folder. If you have custom icons that you want to assign to a command, copy the icon to this folder.
- If you want to create icons or edit existing icons, you can use any drawing application, such as Microsoft Paint, that allows you to save the icon in bmp format.
- The default size of icons on the Station toolbar is 21 x 15 pixels. You can set Station to use large icons which are 32 x 32 pixels.

- Filenames for large icons have a prefix of `lrg_` and the suffix is the same as the filename for the small icons. For example, `lrg_tb015.bmp` is a large icon and `tb015.bmp` is the equivalent small icon.
- The preconfigured `.stb` files are read-only. If you are customizing a preconfigured `.stb` file, use the Save As option to create a new `.stb` file.
- When you customize the `.stb` file, you need to save the `.stn` file so that it references the customized `.stb` file.

To add a new command:



- 1 In the **Connection Properties** dialog box, click the **Toolbars** tab.
- 2 In the **Menu, toolbar & keyboard shortcuts** box, specify the `.stb` file you want to customize.
- 3 Click **Customize**.
The **Customize** dialog box opens.
- 4 Click **New Command**.
The **Command Properties** dialog box opens.
- 5 Type a name for the command.
- 6 If applicable, enter a tool tip.
- 7 If applicable, place the cursor in the **Enter keyboard shortcut** box and press the keyboard shortcut keys.
- 8 If applicable, click **Assign Icon** and select the appropriate icon.
- 9 Select the required action from the **Action** list.
For a list of actions and required information see “Command Properties dialog box” on page 102.

- 10 Specify any other required information for the action you have selected.
- 11 Click **OK**.

You can now add the command to a menu or to the toolbar.

To add a command to an existing menu:

- 1 In the **Connection Properties** dialog box, click the **Toolbars** tab.
- 2 In **Menu, toolbar & keyboard shortcuts**, specify the .stb file you want to customize.
- 3 Click **Customize**.
The **Customize** dialog box opens.
- 4 Click the **Menu** tab.
- 5 Select the command you want to add from **Available commands** and click **Insert**.
- 6 Use the arrows to move the new menu to the appropriate position.
- 7 Click **Save As** and specify a new .stb filename to save your settings.
- 8 Click **Save** to save the reference to the new .stb file in the current .stn file or click **Save As** and specify a new .stn filename to create a new .stn file.

To add a toolbar button to a toolbar:

- 1 In the **Connection Properties** dialog box, click the **Toolbars** tab.
- 2 In **Menu, toolbar & keyboard shortcuts**, specify the file you want to customize.
- 3 Click **Customize**.
The **Customize** dialog box opens.
- 4 Click the **Toolbars** tab.
- 5 Select the toolbar you want to which you want to add a button.
- 6 In **Available commands** select the command you want to add. (If you want to add a new command see the procedure for adding a new command on page 75)
- 7 If the command does not have an icon, click **Edit** and assign an icon.
- 8 Click **Insert**.
- 9 In the **Tooltip/Label** box, type in the appropriate tooltip.
- 10 Use the arrows to move the toolbar button to the required position.
- 11 Specify the required information for the action you have selected.
- 12 Click **Save As** and specify a new .stb filename to save your settings.

- 13 Click **Save** to save the reference to the new .stb file in the current .stn file or click **Save As** and specify a new .stn filename to create a new .stn file.

Considerations

- If you edit a command, all methods of invoking the command (menu, toolbar and keyboard shortcut) invoke the edited command.

To edit a command:

- 1 In the **Connection Properties** dialog box, click the **Toolbars** tab.
- 2 In the **Menu, toolbar & keyboard shortcuts** box, specify the .stb file you want to customize and click **Customize**.
- 3 In the **Available commands** list select the command you want to edit.
- 4 Click **Edit**.
The **Edit Command** dialog box opens.
- 5 Make the required changes.
For a list of actions and required information see “Command Properties dialog box” on page 102.
- 6 Click **OK**.

To add a new menu to the Station menu bar:

- 1 In the **Connection Properties** dialog box, click the **Toolbar** tab.
- 2 In **Menu, toolbar & keyboard shortcuts**, specify the .stb file you want to customize.
- 3 Click **Customize**.
The **Customize** dialog box opens.
- 4 Click the **Menu** tab.
- 5 In **Available commands** select **Header** and click **Insert**.
- 6 In the **Caption** box, type the menu name.
- 7 Use the arrows to move the new menu to the appropriate position.
- 8 Add menu items as required (see the procedure for adding a menu item on page 76).
- 9 Click **Save As** and specify a new .stb filename to save your settings.
- 10 Click **Save** to save the reference to the new .stb file in the current .stn file. or click the **Save As** button and specify a new .stn filename to create a new .stn file.

To add a new toolbar:

- 1 In the **Connection Properties** dialog box, click the **Toolbars** tab.
- 2 In the **Menu, toolbar & keyboard shortcuts** box, specify the file you want to customize.
- 3 Click **Customize**.
The **Customize** dialog box opens.
- 4 Click the **Toolbars** tab.
- 5 Click **New** and type the name in the **Toolbar Name** box.
- 6 Add toolbar buttons (see the procedure for adding a toolbar button on page 76).
- 7 Click **Save As** and specify a new .stb filename to save your settings.
- 8 Click **Save** to save the reference to the new .stb file in the current .stn file or click **Save As** and specify a new .stn filename to create a new .stn file.

Considerations

- You cannot use the same keyboard shortcut for more than one command. If you want to use a keyboard shortcut that is already assigned, you must overwrite the current assignment.

To assign keyboard shortcuts to an existing command:

- 1 In the **Connection Properties** dialog box, click the **Toolbar** tab.
- 2 In the **Menu, toolbar & keyboard shortcuts** box, specify the stb file you want to customize.
- 3 Click **Customize**.
The **Customize** dialog box opens.
- 4 In the Available commands list select the command and click **Edit**.
- 5 Click the **Keyboard Shortcut** box and press the relevant keys.
- 6 Click **Save As** and specify a new .stb filename to save your settings.
- 7 Click **Save** to save the reference to the new .stb file in the current .stn file or click **Save As** and specify a new .stn filename to create a new .stn file.

If you have a specialized keyboard and you also want to control the LED for a key you have assigned, see “Controlling LEDs on a specialized keyboard” on page 81.

Example Scenario

You have a custom display representing the cooling tower in your plant. The name of the display is `Cooling Tower`. You want your operators to be able to call up this display using:

- The View menu
- The toolbar with a custom icon that has been created
- Shortcut key CTRL + T

You have not customized the menus or toolbars before so the `default.stb` file is being used to define the menus, toolbars and shortcut keys.

You want the `default.stn` Station setup file to reference the custom `.stb` file.

Solution

Edit the `default.stb` file and create a new file that contains your customizations. Create a new command called `callup Cooling Tower` using the Callup page action. Create a custom icon by editing an existing icon in an application such as Microsoft Paint. Assign your custom icon and the keyboard shortcut to the command. Add the command to the View menu and add the toolbar button to the toolbar.

Prerequisites

- Place the custom icon in the `Program Files\Honeywell\Experion PKS\client\system\R300\toolbar` folder on every Station.

To create the command:

- 1 In the **Connection Properties** dialog box, click the **Toolbars** tab.
In the **Menu, toolbar & keyboard shortcuts** box, ensure that `default.stb` is specified.
- 2 Click **Customize**.
The **Customize** dialog box opens.
- 3 Click **New Command**.
The **Command Properties** dialog box opens.
- 4 In the **Name** box, type **callup Cooling Tower**.
- 5 Place the cursor in the **Enter keyboard shortcut** box and press the keys CTRL and T.
- 6 Click the **Assign Icon** button and select your custom icon and click **OK**.
- 7 In the **Action** box select Callup Page.
- 8 In the **Page** box type **Cooling Tower**.
- 9 Click **OK**. The command is now added to the **Available Command** list.

To add the command to the View Menu:

- 1 In **Current Layout**, select **View**.
- 2 In the **Available Commands** list, select your new command **Callup Cooling Tower**.
- 3 Click **Insert**. The Callup Cooling Tower command is added to the View menu.
- 4 In the **Caption** box type **Cooling Tower**.

To add the command to the toolbar:

- 1 Click the **Toolbars** tab.
- 2 In the **Available Commands** list select Callup Cooling Tower.
- 3 Click **Insert**.
- 4 In the **Tooltip/Label** box type **Callup Cooling Tower display**.
- 5 Click **Save As**.
The **Save As** dialog box opens.
- 6 In the **File name** box type **coolingtower.stb** and click **Save**.
- 7 In the **Connection Properties** dialog box click **Save** to save the reference to **coolingtower.stb** in **default.stn**.

Multi-window toolbar and menu configuration

Multi-window systems can have multiple command windows that display menus and toolbars. By default only one window is enabled and it displays the standard Station menu and toolbar. Up to four menu\toolbar windows can be used and each of these can have a custom menu and custom toolbars. The number of command windows is set on the **Appearance** tab of the **Connection Properties** dialog.

The toolbars and menu for each window is set through the normal Customize dialogs. The command window that is being configured is set in the **Window** combobox when working with toolbars and menus. Each command window can have multiple toolbars but only one menu bar—just like a single window Station.

To configure a SafeView workspace to control extra command windows see “Configuring a SafeView workspace configuration file” on page 129.

Controlling LEDs on a specialized keyboard

Each LED on the operator keyboard can be associated with a point. When the point goes into alarm, the associated operator keyboard LED changes state to show the highest priority alarm. The following table shows the default LED state and the corresponding alarm priority.

LED State	Alarm Priority
Red slow blink	There is at least one unacknowledged urgent priority alarm.
Yellow slow blink	There is at least one unacknowledged high priority alarm.
Yellow slow blink	There is at least one unacknowledged low priority alarm.
Red on (static)	There is at least one acknowledged urgent priority alarm. There are no unacknowledged urgent priority alarms.
Yellow on (static)	There is at least one acknowledged high or low priority alarm. There are no unacknowledged high or low priority alarms.
Off	No alarm exists.

You can change this default behavior of the LEDs.

To change the behavior of LEDs:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure server-wide Stations settings** task.
The Server Wide Settings display appears in the System Display tab in Configuration Studio.
- 3 Click the **IKB LED Settings** tab.
- 4 For each alarm priority, specify the LED color and the LED action.

Prerequisites

- You have installed the appropriate drivers and connected the keyboard. For these instructions, see the following topic in Knowledge Builder:
Experion R300 > Installation and Upgrades > Supplementary Installation Tasks Guide > Preparing a client computer for an Icon Console.

To associate points with LEDs:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Flex Stations** task.
The Flex Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Flex Station you want to configure. The Flex Station Configuration display appears.
- 4 Click the **Operator Keyboard** tab.
- 5 For every LED you want to associate with a point, enter the point ID in the corresponding LED key number box.

Figure 3 Operator Keyboard tab

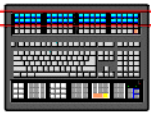
LED	Point ID	LED	Point ID	LED	Point ID	LED	Point ID
1	...	11	...	21	...	31	...
2	...	12	...	22	...	32	...
3	...	13	...	23	...	33	...
4	...	14	...	24	...	34	...
5	...	15	...	25	...	35	...
6	...	16	...	26	...	36	...
7	...	17	...	27	...	37	...
8	...	18	...	28	...	38	...
9	...	19	...	29	...	39	...
10	...	20	...	30	...	40	...

Operator Keyboard



1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40

IKB



1	2	3	4	5	6	7	8	9	10	21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20	31	32	33	34	35	36	37	38	39	40

Configuring Station settings

You use system displays in Configuration Studio to complete other Station-related configuration tasks that are not covered in Station connection properties or `station.ini`.

**Tip**

These tasks can also be done in Station, either a Flex Station or a Console Station, when the Experion server is available.

Configuring timeouts

You can specify a timeout period for:

- Alphanumeric objects on a Station display, known as Select timeout.
- Operator idle timeout on a server-wide basis, known as Idle timeout.
- Operator idle timeout on a per operator basis (used with operator-based security, see “Adding an operator” on page 306).

When the select timeout period is exceeded, the selected alphanumeric on a Station display is automatically deselected.

When the idle timeout period is exceeded without any operator activity:

- If you are using Station-based security with a static Station, the security level reverts to the lowest level of security and (optionally) a preconfigured display opens.
- If you are using operator-based security with a static Station, the operator is required to re-enter their password and (optionally) a preconfigured display opens.
- If you are using either operator-based or Station-based security with a rotary Station, Station is disconnected from the server and the operator is required to reconnect.

If you specify an operator idle timeout period and you use integrated security with single signon or Signon Manager, the operator is not required to re-enter their password. However, if you have a startup display specified, the startup display is called up when the idle timeout period is exceeded without operator activity. This may be an undesired effect. To avoid this either specify a timeout of 0 or do not select this option.

If you are using operator-based security and have specified an idle timeout period for each operator, these timeouts override the server-wide idle timeout when the corresponding operators are logged on to Station.

To specify idle timeout and select timeout:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure server-wide Stations settings** task.
The Server Wide Settings display appears in the System Display tab in Configuration Studio.
- 3 On the **General** tab, under Timeouts, enter the required timeout settings for Select timeout and Idle timeout.

For more information on Server Wide Settings see “Server wide settings” on page 107.

Configuring startup displays

The startup display is the display visible when Station first connects to the server. Where you specify the startup display depends on the connection type and the security type.

When you connect to the server using a rotary connection the startup display is specified in the connection properties. See “Connections tab” on page 95.

For a static connection the startup display is either:

- The display specified as the startup page on the Station Configuration display. See “General tab” on page 107.
- The display specified as the system startup display if there is no startup display specified for the Station.
- The display specified in the operator definition if you are using operator-based security.

However, for a static connection using Station-based security, when you reconnect to the server, Station opens with the last display that was open before Station was shutdown or disconnected.

To configure a system-wide default startup display:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure server-wide Stations settings** task.
The Server Wide Settings display appears in the System Display tab in Configuration Studio.
- 3 On the **General** tab, under Startup page, enter the required page name or number (see “General tab” on page 107).

To configure a startup display for a static Flex Station:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Flex Stations** task.
The Flex Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 In the **Flex Station Summary** display, click the number or title of the Station you want to configure. The **Station Configuration** display opens.
- 4 Under Start up/Idle Timeout Action, enter the required page name or number. (See “Start Up/Idle Timeout Action” on page 114).

The startup display for a rotary connection is specified on the **Connections** tab of the **Connection Properties** dialog box. For more information see “Connection Properties” on page 95.

To configure a startup display for a Console Station:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Console Station you want to configure.
- 4 Click the **Options** tab.
- 5 Under Start up/Idle Timeout Action, enter the required page name or number.

Setting the fast raise/lower step

You can set the percentage amount by which the value of a selected object can be raised or lowered in all Station displays when using the fast raise/lower function keys.

Considerations

- If an operator uses the fast raise/lower keys to change the value of a point beyond the configured limit, the result depends on the type of point being controlled:
 - For SCADA points, the value is set the configured limit.
 - For Process and TPS points, if clamping has been configured, the value is set to the configured limit. If clamping has not been configured, the command is ignored.

- You need to consider the tolerance levels that can be applied to outputs and setpoints. The tolerance level limits the size of changes made to the output and setpoint parameters so they cannot BUMP the process.
 - If an operator enters a value and the controller returns an “out of tolerance” error, the operator will be asked to confirm the value entered. If the value is confirmed, the value will be accepted. If the value is not confirmed, the control will be cancelled.
 - If an operator enters a value and the controller returns an “exceeds limit” error, the value is treated as an error and the control is cancelled.

The “out of tolerance” and “exceeds limit” errors are automatically handled by the raise/lower step so that you can exceed the tolerance level but the parameter value cannot be driven past at the limit.

To specify the fast raise/lower step:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure server-wide Station settings** task.
The Server-wide Station settings display appears in the System Display tab in Configuration Studio.
- 3 On the **General** tab, enter the required percentage increment/decrement in the **Fast raise/lower step** box.

Configuring alarm settings

To specify alarm settings for all Stations in your system:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm and event options** task.
The Server-wide Station Settings display appears in the System Display tab in Configuration Studio.
- 3 On the **Alarm/Event Options** tab, specify the required alarm settings as described in “Alarm/Event Options tab” on page 109.

To define Flex Station-specific alarm settings:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Flex Stations** task.
The Flex Station Configuration Summary display appears in the System Display tab in Configuration Studio.

- 3 Click the Flex Station you want to configure.
- 4 On the **General** tab, specify the required alarm settings as described in “Audible Alarm/Station Failure Alarm” on page 113.

To define Console Station-specific alarm settings:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Console Station you want to configure.
- 4 On the **General** tab, specify the required alarm settings as described in “Audible Alarm/Station Failure Alarm” on page 113.

If you enable the Station failure alarm for a Station, you can also configure the priority of the Alarm.

To configure the priority of the Station failure alarm:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm and Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Priorities** tab and select the appropriate priority for Station failure alarms.

Specifying associated Stations

You can configure a Flex Station so that particular displays are “sent” to one of three other Flex Stations. The Station to which the display is sent is known as an “Associated Station”. You can configure keyboard shortcuts to send the current display to the associated Stations or you can specify that Detail displays, Group displays, Trend displays and a point’s Associated display are always sent to one of the three associated Stations. By default the keyboard shortcut ALT+F8 is configured to send a display to the first associated Station. You need to configure two other keyboard shortcuts to send the current display to the second and third associated Stations.

Associated Stations are particularly useful when using the Icon Series Console with multiple instances of Station on a single computer.

To configure associated Stations:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Flex Station** task.
The Flex Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Flex Station you want to configure.
- 4 Enter the Station numbers for the first, second and third associated Stations.
- 5 If appropriate, select the associated Station that you want Detail, Group, Trend and Associated displays sent to.
- 6 Create a command using the action Request Task and set parameter 1 to 19 and parameter 2 to either 2 for associated Station 2 or 3 for associated Station 3.
- 7 Assign a keyboard shortcut to the command.

For more information about Station-specific settings, see “Flex Station Configuration Display” on page 113.

For details on creating a command see “Customizing toolbars, menus and keyboard shortcuts” on page 74.

Working with faceplates

A faceplate is a specialized type of popup that shows critical information about the point to which the object is linked. In most cases, a faceplate is similar to the left-hand portion of the matching point detail display.

Station can display up to four faceplates simultaneously. By default, faceplates are initially positioned in the bottom right-hand corner of Station. If there are four faceplates displayed, when you call up a fifth faceplate, it replaces the oldest faceplate using the position of the oldest faceplate.

Operators can move faceplates around the Station window and outside the Station window if the Station window is not maximized. The last position of the faceplates is persistent. That is, if the faceplate is closed and then re-opened, it opens in the same position it was in before it was closed.

Faceplates appear at the same zoom as the Station window, however an operator can resize the faceplate. The size of the faceplates is also persistent. That is, if the faceplate is closed and then re-opened, it opens at the same size it was before it was closed.

You can create a command for operators to use to easily reset the faceplates to the default size and position.

You can change the default behavior of persistent positioning, such that when an operator calls up a faceplate, it is positioned in relation to the object to which it is attached. When a fifth faceplate is called up, the oldest is closed and the newest appears in relation to its object.

This section describes:

- Creating a command to enable operators to reset the position of faceplates to the default position (if you have not changed the default behavior).
- Changing the default behavior of faceplates such that they appear in relation to the object to which they are linked by turning off persistent positioning.

To create a button to reset faceplate positions:

- 1 Create a new command as described in “Customizing toolbars, menus and keyboard shortcuts” on page 74.
- 2 From the Action list, select **Predefined action**.
- 3 From the Predefined action list, select **Reset Faceplate Positions**.



Caution

The following procedure involves editing the Windows registry. Incorrectly editing the registry may severely damage your system.

To turn off persistent positioning:

- 1 On the Station computer choose **Start > Run**.
- 2 Type `regedit` and click **OK**.
- 3 Locate the key:
**HKEY_LOCAL_MACHINE\software\Honeywell\Faceplates\
PersistentPositioning**
- 4 Set the value `Enable` to **0**.
- 5 Exit the registry.
- 6 Refresh the display or call up a new display.

Accessing Experion using Internet Explorer

If you have Station installed you can also access the Experion server using Internet Explorer. This allows the casual user to view Station displays from within Internet Explorer without having to start up an instance of Station.

For example, you may want to create a “home page” using HMIWeb Display Builder containing links to a set of displays relating to a specific part of your plant that casual users may want to access.

When Internet Explorer loads this “home page”, a connection is made to the Experion server using connection properties defined in the `default.stn` file stored with the “home page”.

When a connection is made, Experion security works in the same manner as a Station connection. That is, if your system is set up to use Station-based security, the user is connected to the server at the oper security level. If operator-based security is used, the user is prompted for an operator ID and password.

Connecting to the server using Internet Explorer requires a rotary Station connection. The number of connections to the server at any one time is determined by your license.

Setting up Experion to enable access using Internet Explorer requires the following:

- Define a rotary Station in Configuration Studio.
- Use Station to define connection properties, in the same way you would for Station, and save them in an `.stn` to be stored with the displays to be accessed using Internet Explorer. (See “Configuring Station connection properties” on page 72.)
- Create a separate folder to store the `default.stn` and the relevant HMIWeb displays.
- If the Station computer only has web access to the server and does not have file share access to the server, the system displays need to be stored on the Station computer.
- Create an HMIWeb startup display or “home page”.
- Initiate a connection by navigating to “home page” by specifying the full path as a URL. For example, `file://c:/Program Files/Honeywell/Experion PKS/client/CustomWebDisplays/homepage.htm`.

Setting up Station Help

There are several help options available from the Station's **Help** menu:

- **Help for this display**—calls up the context-sensitive topic within Station Help. For example, if a user calls up the Alarm Paging display and selects this menu item, Station Help opens at a topic related to the Alarm Paging configuration.
(If there is no context-sensitive topic, Station Help opens at the first topic.)
- **Operators Guide**—calls up the Operators Guide.
- **Station Help**—calls up Station Help and opens it at the first topic.
- **Knowledge Builder**—Calls up Knowledge Builder, the Experion online documentation “library”.
- **Knowledge Builder Search**—Calls up the search function, which allows you to search the whole Knowledge Builder “library” for a particular word or phrase.

The following procedure describes how to configure a keyboard shortcut to invoke context-sensitive help.

Notes

- The help file that opens when a user presses the keyboard shortcut is specified by the HelpOperator parameter in `station.ini`. See “Station.ini” on page 116.
- The .stb files, supplied with Experion are read-only. If you are customizing a preconfigured file, use the Save As option to create a new .stb file.

To configure a keyboard shortcut for context-sensitive help:

- 1 Choose **Station > Connection Properties**.
The **Connection Properties** dialog box.
- 2 Click the **Toolbars** tab and then click **Customize**.
The **Customize** dialog box opens.
- 3 In the list of **Available commands** select [He1p]Page He1p and click **Edit Command**.
- 4 Click the **Keyboard shortcut** box and press the key (or key combination) you want to use to invoke the Help.
- 5 Click **OK**. If the key is already assigned to another command, a warning message appears. Click **Yes** to assign the key, or click **No** to assign another key.

- 6 Click **Save As** and specify a new filename to close the **Customize** dialog box.
- 7 Click **Save** to close the **Connection Properties** dialog box.

Setting up the server as a trusted site on the Station computer

If your Station computer does not reside in the same domain as the Experion server to which you are connecting, you need to define the Experion server as a trusted site in Internet Explorer.

Considerations

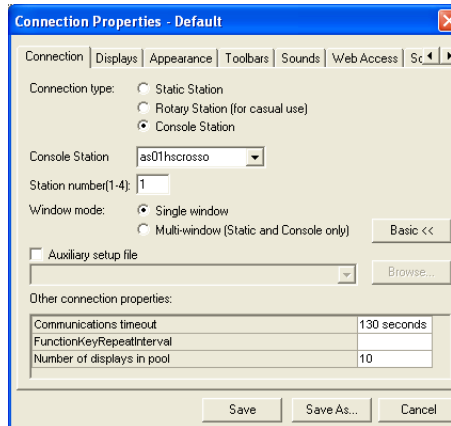
- If you have redundant servers, you need to add both server names to the list of trusted sites.

To make the server a trusted site:

- 1 Open Internet Explorer.
- 2 Choose **Tools > Internet Options**.
The **Internet Options** dialog box opens.
- 3 Click the **Security** tab.
- 4 Click the **Trusted Sites** icon.
- 5 Click **Sites**.
The **Trusted Sites** dialog box opens.
- 6 In **Add this Web site to the zone**, type **http://servername**, where *servername* is the name of the Experion server.
If you have redundant servers, type **http://servernamea**, where *servernamea* is the name of the primary Experion server and type **http://servernameb**, where *servernameb* is the name of the primary Experion server.
- 7 Clear the **Require server verification** check box.
- 8 Click **OK** to close the second dialog box and click **OK** again to save your changes.

Connection Properties

You use the Connection Properties to customize some of the Station settings. The dialog box contains a series of tabs relating to the Station settings you can customize. The settings are described in the sub-topics below.



Connections tab

You use the **Connection** tab in the **Connection Properties** dialog box to specify how the Station that you are currently using is connected to the server. The options you can specify are described below.

Click the **Advanced** button to display all properties.

Property	Description
Connection type	Specifies if this Station is a static Station, rotary Station, or Console Station.
Server	Specifies the name of the server to which this Station is to connect.
Console Station	Specifies the name of this Console Station. Visible only if the connection type is Console Station.
Station Number	Applicable to Flex Stations using a Static connection type. The number must match the Station number allocated for this Station in Quick Builder.
Window Mode	Specifies whether this Station uses multi-window mode or single window mode. For a description of these modes see “What type of Station are you configuring?” on page 64.

Property	Description
Auxiliary setup file	Specifies the auxiliary setup file that contains alternative connection properties to be used if: • A redundant server fails over to the backup server. • The Console Station fails. Applicable only if: • You have redundant servers and dual networks. See “Station network redundancy” on page 468. • Console Stations
Normal update rate	Applicable only to rotary connections. The rate, in seconds, at which dynamic values on displays at this Station are updated from the database.
Fast update rate	Applicable only to rotary connections. An optional fast update rate, in seconds, that can be invoked by function key for displays at this Station. For information about configuring the Fast Update Rate function key, see “Customizing toolbars, menus and keyboard shortcuts” on page 74
Communications timeout	How long the Station should wait for initial communications from the server before displaying an error message.
Startup display	Applicable only to a Flex Station using a rotary connection. The number or name of the startup display called up on connection to the server. Type 0 to use the System Startup display.
FunctionKeyRepeatInterval	Specifies the time during which repeat key strokes are ignored after the key has been initially pressed.
Number of displays in pool	Applicable only if you use multi-window mode. Specifies the maximum number of displays that can be visible simultaneously.

Displays tab

Use the Displays tab to define the paths and the order Stations uses to search for displays.

Property	Description
Search for displays in	Lists the paths and the order Station uses to look for displays and the .stb file. A search path can also be specified as an environment variable. See “Environment variables” on page 120.
Add	Adds a search path.

Property	Description
Remove	Deletes the selected search path from the list.
Up arrow	Move the selected search path up within the list. The order of the display paths determines the search order.
Down arrow	Moves the selected search path down within the list.
Search subdirectories for shapes	Indicates if the folders of the specified paths are searched.
DSP page background color	Specifies the color of the background visible when you change displays.

Appearance tab

Property	Description
Show Station menu	Specifies whether the Station menu is shown. If you hide the Station menu, you will need to provide an alternate method for operators to navigate to Station displays and to log on and log off.
Auto hide message zone	Specifies whether the message zone is always visible or only when a message is displayed.
Show alarm zone	Specifies whether the alarm zone is shown.
Show status zone	Specifies whether the status zone is shown.

Toolbars tab

Use the Toolbars tab to assign a different stb file, customize the menus, toolbars, and keyboard shortcuts that are available to Station.

Property	Description
Toolbar options	
Show button labels	Specifies if the button name is displayed with the icon.
Show ToolTips	Specifies if ToolTips are shown when you move the mouse over a toolbar button.
Use large buttons	Specifies if large buttons are used in the toolbar. The size of the large buttons is 32 x 32 pixels.
Appearance	
Menu, toolbar & keyboard shortcuts	The name of the file containing the menu, toolbar, and keyboard settings. If you specify the filename only, Station searches the paths specified on the displays tab.

Property	Description
Browse	Allows you to specify the specific file and location of the .stb file.
Customize	Allows you to customize the menu, toolbar, and keyboard settings. See “Customize dialog box” on page 100.

Sounds tab

Use the Sounds tab to configure audible alarms. These settings are used in conjunction with the audible alarm settings on the Station configuration display. See “Flex Station Configuration Display” on page 113.

Property	Description
Use PC Speaker	Specifies if the audible alarm is generated through the speakers on the computer Station is running on.
Event	Lists the events for which you can specify alarms.
Sound	Lists the sound specified for the event.
Sound for selected event	Specify the sound you want played for a particular event. Use the Browse button to locate the sounds. Use the Play button to test the sound.
Use external contact	Specifies if the audible alarm is generated through an external annunciator.
Use keyboard contact	Applicable only if you have a specialized keyboard. Specifies if the audible alarm is generated through an IKB.
Keyboard contact for selected event	Applicable only if you have a specialized keyboard. Specify the contact you want for a particular event.

Web Access tab

Use the Web Access tab to specify the Web pages an operator can navigate to using Station.

Any URL you specify must be less than 256 characters.

Click the **Advanced** button to display all properties.

Property	Description
No URLs	No Web pages or files can be displayed in Station.
All URLs	All Web pages or files can be displayed in Station.

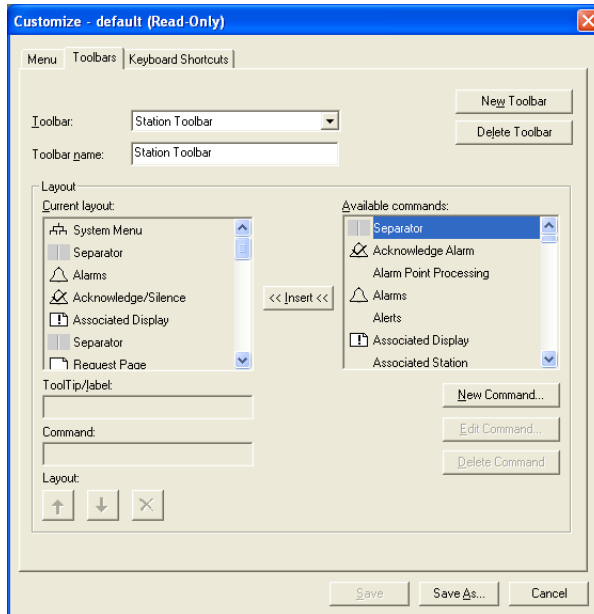
Property	Description
The following URLs only	Only the specified Web pages or files can be displayed in Station. Use an asterisk (*) to enable access to all pages of a website. For example <code>www.honeywell.com/*</code> enables operators to access all pages at this site. If you do not include the asterisk, operators can only access the home page.
Add	Enables you to add specific Web pages or files for display.
Remove	Removes the selected Web page or file.

Scripting tab

Use the scripting tab to specify the scripts that run with this Station connection.

Property	Description
Application Script	The filename and path of the application script. Use the Browse button to change the script. Use the Edit button to open the Station Script Editor.
Timeout after	The amount of time (in seconds) after which the script engine terminates the script.
Station scripting objects	The ID of the Station scripting object.
Add	Enables you to add scripting objects.
Remove	Enables you to remove scripting objects.

Customize dialog box



You access the **Customize** dialog box using the Customize button on the Toolbar tab, in the **Connection Properties** dialog box.

Use the **Customize** dialog box to:

- Create new commands to add to menus, toolbars and assign keyboard shortcuts.
- Add or delete a custom toolbar
- Add menu items to a menu
- Customize menu items
- Customize function keys and shortcut keys

There are three tabs in the **Customize** dialog box:

- Menus
- Toolbars
- Keyboard shortcuts

Menus tab

Property	Description
Current layout	Displays the current menu structure.
Available Commands	Lists all available commands that you can add to a menu.
Insert	Allows you to add the selected command to the menu.
Caption	Allows you to name of the menu item.
Command	Displays the name of the command.
Layout	Allows you to move the selected menu item.
New Command	Allows you to create a new command.
Edit Command	Allows you to edit the selected command.
Delete Command	Deletes the selected command.

Toolbars tab

Property	Description
Toolbar	Specifies the toolbar to edit.
Toolbar name	Allows you to specify the name of a custom toolbar.
New Toolbar	Allows you to add a new toolbar.
Delete Toolbar	Allows you to delete a toolbar.
Current layout	Displays the current layout of the selected toolbar.
Available Commands	Lists the commands or menu items available on the toolbar or menu bar currently selected in the Categories list.
Insert	Allows you to add the selected command to the selected toolbar.
Tooltip/Label	The tooltip that is visible when you place the mouse pointer over the toolbar button.
Command	The name of the command.
Layout	Allows you to move or delete the selected button in the layout view.
New Command	Allows you to create a new command.
Edit Command	Allows you to edit the selected command.
Delete Command	Allows you to delete the selected command.

Keyboard Shortcuts tab

Property	Description
Current keyboard shortcuts	Lists currently assigned keyboard shortcuts and the command to which they are assigned.
New Command	Allows you to create a new command.
Edit Command	Allows you to edit the selected command.
Delete Command	Allows you to delete the selected command.

Command Properties dialog box

The **Command Properties** dialog box is used to set the properties of a command you add to the toolbar, menubar or keyboard shortcut.

Property	Description
Name	The name of the menu item, toolbar button or keyboard shortcut.
Keyboard shortcut	The keyboard shortcut assigned to the menu item or toolbar button.
Icon	Enables you to specify an icon for a toolbar button.
Action	The action assigned to the menu item, toolbar button, or keyboard shortcut. See Actions for a list of actions.

Actions

You can specify the following actions for a menu item, toolbar button or keyboard shortcut.

Action	Description
Callup Page	The number or name of the display.
Callup Popup	The name of the popup and the position of the popup.
Current Display to	Applicable to Stations within a console only. The Station to which the current display is sent within the console.
Launch Application	The path of the executable file for the application to be launched. You can use environment variables to pass contextual information to the application when launching the application. See “Environment variables” on page 120.

Action	Description
Launch Help file	The path of the help file to be launched.
Next Display to	Applicable to Stations within a console only. The Station to which the next display to be called up is sent within the console.
Request Report	The report number.
Request Task	Task number, parameters, whether the task requires input from the Command Zone. For a list of parameters for LRN 21 see “Server Display Program” on page 103.
Server Pushbutton	Pushbutton interrupt code. See “Pushbutton interrupt codes” on page 105 for the appropriate code.
Predefined Action	A standard command. Select the command from the list.

Server Display Program

The Server Display program (LRN 21) is a common program assigned to user-definable function keys. It is the default option when you select a “Request Task” action for a command. The Server Display program performs a wide range of tasks, determined by the values of parameters 1 and 2, as described in the following table.

Table 2 Server Display Program parameters and actions

Parameter 1	Parameter 2	Action
1	<i>PageNumber</i>	Call up the specified numbered DSP display.
1	<i>PageName</i>	Call up the specified named DSP display.
1	<i>Page://pagename</i>	Call up the specified HMIWeb display.
2	N/A	Page forward
3	N/A	Page backward
4	Record #	Display the specified record
5	N/A	Record forward
6	N/A	Record backward
7	Page #	Call up display number or name with current file and record # offset.
8	Trend#	Call up the specified trend
9	Report #	Call up the specified report detail display
10	Report #	Peruse the report output
11	1	Prompt for password entry at the Station
11	2	Prompt for page # at the Station

Table 2 Server Display Program parameters and actions (*continued*)

Parameter 1	Parameter 2	Action
11	3	Prompt for trend # at the Station
11	4	Prompt for group # at the Station
11	5	Prompt for group trend # at the Station
11	6	Prompt for group history # at the Station
12	N/A	Message pad clear
13	N/A	Message pad save
14	History type#	Call up history type detail
15	0	Sends the current display to another Station in the console. You need a third parameter to specify the destination of the display. The destination can be an alias or in the format <i>CStnn-n</i> .
15	1	Sends the next display to another Station in the console. You need a third parameter to specify the destination of the display. The destination can be an alias or in the format <i>CStnn-n</i> .
17	N/A	Cancel
19	Associated Station number (either 1 for first, 2 for second or 3 for third))	Send current display to associated Station defined by parameter 2.
21	N/A	Call up the prior display
22	N/A	Cancel printing
24	N/A	Alarm silence/acknowledge
26	N/A	Control selected point to normal mode
27	N/A	Control selected status point to OFF
28	N/A	Control selected status point to ON
29	N/A	Control selected point to MAN mode
30	N/A	Control selected point to AUTO mode
31	N/A	Control selected point to CASC mode
32	N/A	Control selected point to COMP mode
37	N/A	Fast lower the selected value
38	N/A	Fast raise the selected value
39	N/A	Call up the point's associated display
40	N/A	Toggle the point's in-service status

Table 2 Server Display Program parameters and actions (*continued*)

Parameter 1	Parameter 2	Action
41	N/A	Select the point's OP
42	N/A	Select the point's SP
49	Group #	Call up the group display
50	Group #	Call up the group trend display
51	Group #	Call up the group history display
54	<i>n</i>	Invokes the password change request dialog box for the operator <i>n</i> .
61	N/A	Call up the previous point detail display.
73	N/A	Call up the point details display for the selected point.
78	N/A	Call up the Search display for cardholders/cards
79	N/A	Call up the current card download display

Pushbutton interrupt codes

Description	Pushbutton Interrupt	Description	Pushbutton Interrupt
Call up the System Status display	86	Call Up the Message Summary Display	115
Call up Station Status Display	87	Call Up the Alarm Summary Display	116
Toggle between normal update rate and fast update rate.	89	Call up page 80	119
Cancel Server Printing	90	Set Control to Manual Mode	121
Request the Server to Print the Display	91	Set Control to Automatic Mode	122
Call Up the System Menu Display	93	Set Control to Normal Mode	123
Enable/Disable	94	Select SP	124
Group	96	Select OP	125
Detail	97	Esc	126
Trend	99	Select	127
Page	102	Request a Server User Task	134-143

Description	Pushbutton Interrupt	Description	Pushbutton Interrupt
Send current page to Assoc Stn	104	Hit (select the nearest object)	144
Prior Display	106	Raise	148
Associated Display	107	Fast Raise	150
Page Backwards	110	Lower	152
Page Forwards	111	Fast Lower	154
Enter	112	Refresh Window	160
Acknowledge/Silence	113		

Server wide settings

Use the tabs on the Server Wide Settings display to define:

- General Station settings
- Station alarms
- Security level required for enabling and disabling hardware
- Alarm and event options

General tab

Use settings on the General tab to specify the following:

Property	Description
Startup Page	
Default system start up page	The default system startup display. This display is called up: • On initial connection to the server (that is, after server startup) for static Stations with Station-based security and there is no startup display specified for the Station. • On connection to the server for static Stations with operator-based security if there is no startup display specified for the Station or the operator.
Timeouts	
Select Timeout	The time, in seconds, an alphanumeric object on a Station display can remain selected before being automatically deselected.
Idle Timeout	The time, in seconds, a Station display remains active without any operator activity before reverting to the lowest level of security and (optionally) changing to a preconfigured display. For rotary Stations, the connection is closed so that it is available to another Station. Changes to the idle timeout value are not effective until Station reconnects to the server.
Operator Actions	

Property	Description
Slow raise/lower step	The percentage amount by which the value of a selected object can be raised or lowered in all Station displays when using the slow raise/lower function keys: Note that the Slow Raise/Slow Lower function key cannot be used to increase or decrease the field value of point parameters beyond their specified limits. For SCADA points, if the increase or decrease is beyond the limit, then the parameter is set to the specified limit. For Process and TPS points with clamping configured, if the increase or decrease is beyond the limit, the parameter is set to the specified limit; if clamping is not configured, then the change is rejected. You need to consider the tolerance levels that can be applied to outputs and setpoints. For more information on tolerance levels see “Setting the fast raise/lower step” on page 85.
Fast raise/lower step	The percentage amount by which the value of a selected object can be raised or lowered in all Station displays when using the fast raise/lower function keys: Note that the Fast Raise/Fast Lower function key cannot be used to increase or decrease the field value of point parameters beyond their specified limits. For SCADA points, if the increase or decrease is beyond the limit, then the parameter is set to the specified limit. For Process and TPS points with clamping configured, if the increase or decrease is beyond the limit, the parameter is set to the specified limit; if clamping is not configured, then the change is rejected. You need to consider the tolerance levels that can be applied to outputs and setpoints. For more information on tolerance levels see “Setting the fast raise/lower step” on page 85.
Point Value Error Indication	
Display as question marks	If selected, when a communications failure occurs point values on displays are replaced by question marks.
Display using inverse video	If selected, when a communications failure occurs the point value displayed (using reverse video) is the last scanned value before the communications error occurred.
OPC Server Option	
Use Enterprise Model hierarchy when OPC clients browse into an Experion address space	If selected, the enterprise model is presented to the OPC client in the browse address space. Otherwise the asset-point model is presented to the OPC client in the browse address space.

Alarm Colors tab

Use the settings on the Alarm Colors tab to specify:

Property	Description
Alarm colors	
Urgent priority	Specifies the color for urgent priority alarms.
High priority	Specifies the color for high priority alarms.
Low priority	Specifies the color for low priority alarms.
Unknown priority	Specifies the color for alarms of unknown priority.
Use these colors for points on display	If selected, specifies that the custom alarm colors are to be used on your displays for data objects that also display their alarm status and also for the Alarm indicator on the status line. If this option is not selected, the color specified for the alarm indicator is used in both instances.
Status Bar Indicator Colors	
Alarm	Specifies the color of the alarm indicator in the status line.
Communications	Specifies the color of the communications indicator in the status line.
Message	Specifies the color of the message indicator in the status line.
Alert	Specifies the color of the alert indicator in the status line.
Point State Colors	
Point off scan	Specifies the color used for points on displays if scanning is disabled.

Alarm/Event Options tab

Use Alarm/Event Options settings to specify:

Property	Description
Station Alarms	
Audible active time	The duration of audible alarms. For example, if you specify 10 seconds, the alarms sound for 10 seconds each, unless the operator silences the alarm by acknowledging it before the 10 seconds has passed. If the alarm is not silenced or acknowledged, the alarm will sound again when the Audible re-alarm time expires.

Property	Description
Audible re-alarm time	The period after which an audible alarm sounds again if the alarm has not been silenced or acknowledged by an operator. This setting is used in conjunction with the Audible active time.
Alarm line shows	Specifies whether the Alarm Line displays the newest or the oldest unacknowledged alarm of highest priority.
Silence action applies to	
Single Station only	If selected, silences the alarm on the Station where it is silenced. The alarm is not silenced on other Stations.
Single Station or single Console (all Stations in console)	If selected, silences an alarm on the Station where it is silenced. The alarm is not silenced on other Stations. If the alarm is silenced on a Station within a Console, the alarm is silenced on all Stations in the Console.
All Stations	If selected, silences the alarm on all Stations, including Flex Stations, Console Stations, and Console Extension Stations, that are connected to the same server.
Alarm/messages must be acknowledged:	
At each console	If selected, acknowledges the alarm on the Station where it is acknowledged and all other Stations that are not in a separate console. If the alarm was acknowledged on a Station in a console, the alarm is acknowledged on all Stations in the console.
Once (applies to all Stations)	If selected, acknowledges the alarm on all Stations including Flex Stations, Console Stations, and Console Extension Stations.
Event Summary Options	
Log NetServer and OPC server changes to the database as events	If selected, point parameter changes made via an OPC server or network API functions are logged as events.
Log NetServer changes with security information to the database as events	If selected, point parameter changes made using the network API functions <code>rhsc_param_value_put_sec_bynames</code> and <code>rhsc_param_value_puts_sec</code> are logged as events.
Show operator's full name in the Event Summary.	If selected, the operator's name is displayed with operator events in the Event Summary instead of just the operator ID.
Alarm, Alert, Event, SOE and Message Summary Restrictions	
Full page acknowledgement	The minimum security level required to be able to use the Acknowledge Page function on the summary displays.
Pausing	The minimum security level required to use the Pause function on the summary displays.

Property	Description
Filtering and sorting	The minimum security level required to be able to use the filtering and sorting functions on the summary displays.
Saving views	The minimum security level required to be able to save a view for the summary displays.
Organizing columns	The minimum security level required to be able to change the column layout (including hiding and changing the order) on the summary displays.
Print preview and printing	The minimum security level required to be able to see a report in print preview or to print a report.
Tamper Detection	
Check all event data returned from the event archives	If selected, events that have been restored from archived are checked for tampering whenever you query the event data. For more information see “Event tamper detection” on page 632.
Timeouts	
Event Queries	The time, in seconds, an event query is allocated to run. If the time expires before the event query is complete, the query is terminated and no event data is returned. The default is 15 seconds. Event queries include event reports, filtering the Event Summary or filtering the Recent Events display.
Event archive configuration	The time, in seconds, event archiving tasks are allocated to run. If the time expires before the event archiving task is complete, the task is terminated. The default is 60 seconds. Event archiving tasks include, performing an event archive and restoring an archive. If the task is terminated, an alarm is raised.

Security tab

Use the Security tab to specify:

Property	Description
Enabling and Disabling Hardware	
Minimum Security Level Required	The minimum security level for enabling and disabling channels, controllers, points and printers.
System Security Options	

Property	Description
Check both the Operators And the Stations asset assignment for access to a given asset.	Only applicable is the Station is configured for operator-based security. If selected, access to an asset is granted only if the both the operator and the Station have been assigned the asset.
User name and password required for Quick Builder and Control Builder downloads	If selected, operators require an integrated account with a security level of ENGR or MNDR to perform a download from Quick Builder or Control Builder. Download events in the event summary contain the full printed name of the operator who performed the download. The full printed name is included with operator-generated events. The Show operator's full name in the Event Summary option on the Alarm/Event options tab is automatically selected when you select this option. Point and hardware building is permitted only when the Experion server is running.

IKB LED Settings

Use the IKB LED Settings tab to specify:

Property	Description
LED color	Specify the LED color for urgent, high, and low priority alarms. The colors you can specify are red or yellow.
LED action	Specify the LED action for urgent, high, low priority alarms, messages, and system alarms. The actions you can specify are: • Off—The LED is off • Slow—The LED flashes slow. • Fast—the LED flashes fast. • On—the LED is static.

Flex Station Configuration Display

You use the Station Configuration Display to define settings for a particular Station.

General tab

The following sections describe settings you define on the General Tab of the Station Configuration display.

Associated Stations

Use the Associated Stations controls to specify:

Property	Description
First Station	Specifies the number or name of the first associated Station.
Second Station	Specifies the number or name of the second associated Station.
Third Station	Specifies the number or name of the third associated Station.
Send Detail to	Specifies which associated Station a Detail display is sent to when requested from the current Station.
Send Group to	Specifies which associated Station a Group display is sent to when requested from the current Station.
Send Trend to	Specifies which associated Station a Trend is sent to when requested from the current Station.
Send Associated to	Specifies which associated Station an Associated display is sent to when requested from the current Station.

Audible Alarm/Station Failure Alarm

Use the Audible Alarm/Station Failure Alarm controls to specify:

Property	Description
Activate for LOW Alarms	Controls whether an audible alarm is sounded for low priority alarms. You specify the particular sound when you configure the Station connection properties.
Activate for HIGH Alarms	Controls whether an audible alarm is sounded for high priority alarms. You specify the particular sound when you configure the Station connection properties.

Property	Description
Activate for URGENT Alarms	Controls whether an audible alarm is sounded for urgent priority alarms. You specify the particular sound when you configure the Station connection properties.
Activate for messages	Controls whether an audible annunciation is sounded for messages. If set, the sound specified for low alarms is used.
Activate for alerts	Controls whether an audible annunciation is sounded for alerts. If set, the sound specified for low alarms is used.
Also activate when Operator is signed off	Controls whether an audible alarm is sounded when, under alarm conditions, no operator is signed on to a Station configured for operator-based security.
Station failure Alarm	Controls whether an alarm is generated if communication to the Station is lost.

Start Up/Idle Timeout Action

Use the Start up/idle Timeout Action controls to specify:

Property	Description
Start up page	Specifies the display called up when connecting to the server with a static connection type and: - Operator-based security if there is no startup page specified in the operator definition. - Station-based security for an initial connection to the server (that is, after the server has been restarted). If you do not specify a display, the display specified as the default system display is called up. The default system display is specified on the Server Wide Settings display. See “General tab” on page 107.
Change to start up page on idle timeout	If selected, when the idle timeout timer for the Station expires the display specified as the startup display is called up.

Printer Assignment

Use the Printer Assignment controls to assign printers to specific tasks.



Attention

If you use operator-based security, the asset assignment and printer settings of the operator who is currently logged on to a Station determine which alarms are printed.

Property	Description
Alarm/Event Printer	Specifies the printer designated to print alarms and events.
Report Printer	Specifies the printer designated to print reports.
Print LOW alarms	Enables printing of alarms for points going in and out of low priority alarm conditions.
Print HIGH alarms	Enables printing of alarms for points going in and out of high priority alarm conditions.
Print URGENT alarms	Enables printing of alarms for points going in and out of urgent priority alarm conditions.
Print EVENTS	Enables printing of alarms for points going in and out of journal priority alarm conditions and other events.
Print Operator changes	Enables printing of all changes to points an operator has made from the Station.

Assignment tab

You use the controls on the Assignment tab to assign the scope of responsibility of the Station. For more information about scope of responsibility, see “Assigning scope of responsibility” on page 336.

Property	Description
Asset	The assets defined in the system.
Network	The nodes available on the Network tree in the System Status display
System Components	The system components, such as servers, in the System Components tree in the System Status display.

Station.ini

You can add or change the following parameters in %SystemRoot%\station.ini to customize the Station. (Where %SystemRoot% is C:\windows for Windows XP and Windows Server 2003.)

AllowRightMouseClickBrowserMenus=*n*

Controls whether the right mouse button menu is available in a SafeBrowse window. Valid values for *n* are:

- 0 Right mouse button menu is disabled. (Default)
- 1 Right mouse button menu is enabled.

BadStateColor=*RRGGBB*

Controls the color for a bad value. RR, GG, and BB are hex values from 00 through FF. For example, to set the message font color to red, use BadStateColor=FF0000.

CenterDSPDrawMode=*n*

Changes how DSP displays are drawn and positioned in Station. By default all displays are drawn from the top-left corner of the drawing area. However in some instances, this causes parts of custom DSP displays to be obscured. You can set this parameter so that DSP displays are drawn centered in the drawing area. HTML displays are still drawn from the top-left. Valid values for *n* are:

- 0 All displays are drawn from the top-left. (Default)
- 1 DSP displays are drawn centered in the drawing area.

ConnectTimeout=*n*

The amount of time (in tenths of seconds) allowed for Station to connect to the server before the connection attempt is cancelled. The default value is 150.

DefaultFont=*fontname*

Controls the font used for command bar and status bar where *fontname* is any font available on the computer.

DisableMaximizeButton=*n*

Allows or prevents users from maximizing the Station window. Valid values for *n* are:

- 0 Users can maximize the Station window. (Default)
- 1 Users cannot maximize the Station window.

DisablePingRequest=*n*

Enables or disables the ping request from the Station computer to a remote server. Ping requests are used to determine if the server you are attempting to connect to is available. If the server is not available, don't try to connect to it. This makes failover in a redundant system faster. However, if your server is behind a firewall, then clients that are outside the firewall will need port 80 open. If this is not desired, then disable the ping requests.

Valid values for *n* are:

- 0 The ping request is enabled.
- 1 The ping request is disabled.

DisableURLNavigationSubsystem=*n*

Allows or prevents the use of SafeBrowse. Valid values for *n* are:

- 0 SafeBrowse is enabled. (Default)
- 1 SafeBrowse is disabled.

FixedWindowSize=*n*

Allows or prevents users from resizing the Station window. Valid values for *n* are:

- 0 Users can resize the Station window. (Default)
- 1 Users cannot resize the Station window. This setting also ensures that a full page is automatically shown at every zoom level.

FlashWindowOnAlarm=*n*

Causes the Station taskbar icon to flash when an alarm is raised. Valid values for *n* are:

- 0 Off (Default)
- 1 On

IgnoreOperatorKeyboard=*n*

Prevents Station from taking full control of the IKB key and LED functions. Used in instances where Station is installed on a GUS node. If set, commands from the IKB are sent to the application with focus and the LEDs are controlled by GUS. If Station has focus then commands are sent to Station however LEDs are still controlled by GUS. Valid values for *n* are:

0

1 Commands from the keyboard are sent to the application with focus and LEDs are controlled by GUS.

KeepAliveTimeout

The time interval at which Station sends a messages to the server and waits for a reply. If the Server has not communicated with Station before the next KeepAliveTimeout period, Station starts the failover process.

You cannot change this without changes to the server, see “Server redundancy fast failover configuration” on page 494.

ManualFailRetry=*n*

The number of times to retry connection to backup on manual failover.

MessageFont=*fontname*

Controls the font used to display messages where *fontname* is any font available on the computer.

MessageFontColor=*RRGGBB*

Controls the message font color. RR, GG, and BB are hex values from 00 through FF. For example, to set the message font color to red, use MessageFontColor=FF0000.

MessageFontSize=*nn*

Controls the message font size where *nn* is any size applicable for the font.

MessageFontStyle=*n*

Controls the message font style where valid values for *n* are:

0 = normal

1 = bold

2 = italic

3 = bold italic

NanStateColor=*RRGGBB*

Controls the color for the NaN (not a number) condition. RR, GG, and BB are hex values from 00 through FF. For example, to set the NaN state color to red, use NanStateColor=FF0000.

UseHandIconOnbutton=*n*

Enables the mouse pointer to be context sensitive. The mouse pointer changes to a hand icon when moved over selectable items. Applicable to DSP displays only.

Valid values for *n* are:

0	Disabled
1	Enabled (Default)

Environment variables

Environment variables contain system related information such as drive, path and filename.

You can use either system or user environment variables to pass contextual information when:

- Launching an application using a toolbar button or script.
- Specifying a page to be displayed using a toolbar button or script.
- Specifying displays paths in Station connection properties.
- Calling up a page using the Station command zone.

When the task, application or script is run, the environment variables are expanded.

You can create and use the following variables:

Environment Variable	Values Called
%DISPLAYNAME%	The name of the page currently displayed.
%DISPLAYNUMBER%	The number of the page currently displayed.
%DISPLAYTITLE%	The title of the page currently displayed.
%HELPOPERATOR%	The document name of the Operator Help.
%HOSTIP%	IP address of the server you are connected to.
%HOSTNAME%	The name of the server you are connected to.
%NODE%	Node or Station number.
%POINTID%	Point ID of the selected point (only on custom displays).
%SERVERIP%	IP address of the server you are connected to.
%SERVERNAME%	The name of the server you are connected to.
%USERNAME%	For operator-based security, the operator ID of the operator logged on for the current session. For Station-based security, the security level of the current session.

Configuring Icon Series Console

7

This chapter describes configuration tasks for:

- The Icon Series Console
- Multi-window Station
- Multiple static Stations
- Touch screens

About Icon Series Console

The Icon Series Console provides you with the capability to use specialized furniture, specialized operator keyboards, Manual Input Modules and multiple monitors with a single computer.

In this environment you can use either the multi-window Station option or the multiple static Stations option. Multi-window Station is a single instance of Station used in conjunction with SafeView to manage the placement of multiple Station displays and Windows. Multiple static Stations allow you to run up to four instances of Station on a single computer.

The specialized operator keyboards are suited for use in harsh environments or where large numbers of function keys, in addition to a standard keyboard, are required. The operator keyboard supported in the Icon Console is the Operator Entry Panel (OEP).

About multi-window Station

With multi-window Station, you can have multiple Station displays visible at the same time, driven by one instance of Station.

Multi-window Station uses the SafeView application to manage the placement of displays and Station windows on the desktop. In SafeView, you create a workspace and configure various window parameters that define the initial location and size of application windows, and limit subsequent changes to the position or size of the windows.

One of the window parameters that you can define is a category. You can then assign this category to your custom displays. For example, you can define a category called `plant_equipment`. You assign this category to all your custom displays that represent your plant equipment so that they always appear in a certain place on your desktop without obscuring other important Station displays such as the Alarm Summary.

You are provided with some sample workspace configuration files with predefined window categories. In addition, the system displays have been assigned window categories.

About multiple static Station

With multiple static Station, you can have up to four instances of Station running simultaneously on the one computer.

About master Station

The master Station is the instance of Station that was started first. If you close the instance of Station that was started first, the instance of Station that was started second then becomes the master Station, and so on.

In the Icon Series Console environment you have the one set of input devices to control each instance of Station. The Station that has “focus” receives the control commands from the input devices. If none of the Stations have focus when an operator issues one of a subset of commands, the master Station receives the command. The subset of commands are:

- CONS STATS—Console Status key
- ALM SUMM—Alarm Summary key
- MSG SUMM—Message Summary key
- SYST MENU—System Menu key

For example, if you have three instances of Station and another application in the fourth monitor has focus, if you press the Alarm Summary keyboard shortcut, the Alarm Summary appears in the master Station.

If the command issued is not one of the commands listed above, none of the Stations receives the command.

Configuring Station for an Icon Series Console

The steps you are required to complete to make your Icon Series Console operational depend on whether you are using multi-window Station or multiple static Stations.

For the list of configuration tasks for multi-window Station, see “Configuration tasks for multi-window Station” on page 125.

For the list of configuration tasks for multiple static Station, see “Configuration tasks for multiple static Station” on page 126.

Configuration tasks for multi-window Station

Prerequisites

- You have prepared the Station computer. For these instructions, see the following topic in Knowledge Builder:
Experion R300 > Installation and Upgrades > Supplementary Installation Tasks Guide > Preparing a client computer for an Icon Console.

Task	Go to	Done
Configure Station setup files and if you have redundant Experion servers and/or redundant networks, configure auxiliary setup files.	page 127	
If you have redundant Experion servers and/or redundant networks specify the auxiliary setup file in each setup file. (For information on redundancy see “Station network redundancy” on page 468.)	page 128	
Honeywell recommends using one of the supplied workspace configuration files in SafeView. However, if you want to create a custom workspace configuration file, see “Configuring a SafeView workspace configuration file” on page 129.	page 129	
Update the page-level shortcut menu.	page 132	
Assign SafeView window categories to custom displays. For more information, see the <i>HMIWeb Display Building Guide</i> and <i>Display Building Guide</i> .	<i>Knowledge Builder</i>	
Provide a shortcut to start SafeView, load the workspace, and start Station.	page 133	
Customize LEDs on the specialized keyboard.	page 81	
Add manual input modules.	page 138	

Configuration tasks for multiple static Station

Prerequisites

- You have prepared the Station computer as described in the “Preparing a Station Computer for an Icon Console” section of the *Supplementary Installation Tasks Guide*.

Task	Go to	Done
Configure Station connections for each instance of Station and if you have redundant Experion servers and/or redundant networks configure auxiliary connections for each instance of Station.	page 127	
Specify the auxiliary files in each Station connection.	page 128	
Provide a shortcut or other method to start multiple instances of Station.	page 134	
Customize LEDs on the specialized keyboard.	page 81	
Add manual input modules.	page 138	

Configuring setup files

After you have installed the Station software, you need to configure the Station connection properties. The Station connection properties identify:

- Station as a multi-Window Station or a single window Station.
- For a Flex Station, the Experion server you are connecting to.
- The type of keyboard you use.

Considerations

- If you are configuring a Flex Station and have redundant Experion servers and/or redundant networks, use this procedure to create auxiliary setup files.
- This procedure is specific to the Icon Console connection properties. See “Configuring Stations and printers” on page 63 for other Station details.

To configure the Station connection properties:

- 1 Start Station.
- 2 Choose **Station > Connection Properties**.
The **Connection Properties** dialog box opens.
- 3 Click the appropriate connection type, either **Static Station** or **Console Station**.
- 4 If you are configuring a Flex Station, do the following:
 - a. In the **Server** box, type the name of the Experion server to which you are connecting.
 - b. In the **Station number** box, type the number of this Station. The number must match the Station number allocated for this Station in Quick Builder.
- 5 Click the appropriate window mode; **Multi-window** for multi-window Station or **Single window** for multiple static Stations.
- 6 Click **Advanced** to expand the options.
- 7 If you are configuring a multi-window Station, specify the maximum number of displays in a pool in the **Other connection properties** list.
- 8 Click the **Toolbars** tab.
- 9 Click **Browse** and navigate to Program Files\Honeywell\Experion PKS\client\System\R300.
- 10 If you are configuring a multi-window Station, select the `ICON_multiwindow.stb` file.
- 11 If you are configuring a multiple static Station, select the `ICON.stb` file.

12 Click **Open**.

13 Click **Save As** and specify a filename.



Stop

You have completed this task. Return to the checklist that led to this task.

Specifying auxiliary setup files

Prerequisites

- You have configured all of your required setup files.

Considerations

- Complete this procedure only if you have a Flex Station with redundant Experion servers and/or redundant networks.

To specify the auxiliary setup file:

- 1 Choose **Station > Connect**.
- 2 Select the appropriate .stn file and click **Edit Properties**.
- 3 If the advanced properties are not visible, click **Advanced**.
- 4 Select the **Auxiliary setup file** check box and specify the appropriate .stn file.
- 5 Click **Save**.



Stop

You have completed this task. Return to the checklist that led to this task.

Configuring a SafeView workspace configuration file

This section provides a high-level overview of the tasks required to configure a workspace configuration file. For detailed instructions, see the *SafeView User's Guide* in Knowledge Builder.

Experion is supplied with sample workspace configuration files that have been designed for dual- and quad-screen Icon Consoles. You might find these samples useful as a starting point when designing your own workspace. The sample workspace configuration files are located in the Program Files\Honeywell\Experion PKS\Client\Station\Samples folder.

Considerations

- Total screen resolution. This determines how much real estate you have and will influence how you size and position windows.
- The number of windows you want visible simultaneously.
- The Command window and the Status Window have their own window categories, HSC_Station_MainWindow and HSC_Station_StatusWindow. You should not use these window categories for any other displays.
- The number of groups and subgroups you need and the types of displays that appear in each group.
- How you want groups to behave, do you want first match, round robin or manual select behavior.
- The Station displays that you want to appear when Station starts.

Tasks

The following is a suggested high-level procedure for configuring a workspace:

- 1 Determine your total screen resolution.
- 2 Determine the main group and subgroups.
- 3 Determine your SafeView window categories. If you have custom HMIWeb displays, you need to update the `windowCategories.xml` file that defines the window categories in HMIWeb Display Builder. For more information, see the “Display/shape properties” section of the *HMIWeb Display Building Guide*.
- 4 Use the SafeView text editor or graphical workspace editor to configure the workspace.

- 5 Add a startup specification so that Station starts automatically when the workspace is loaded. For example:

```
STARTUP
"C:\Program Files\HONEYWELL\Client\Station\Station.exe"
END STARTUP
```
- 6 Apply the window categories to your custom displays.
- 7 Ensure that the Station connection file specifies a sufficient number of windows in the pool. Count the number of windows in your SafeView desktop (include faceplates but not menu or status windows) and then add 3. Then in the **Advanced** section of Station **Connection Properties** dialog make sure the value for **Number of displays in Pool** is at least this figure. This ensures Station had enough windows to handle your SafeView configuration
- 8 Test the workspace and modify as required.

Controlling the location of faceplates

Your SafeView workspace can be configured to display faceplates in the same monitor as they were invoked. This improves the usability of the system by keeping faceplates close to where operators work.

When a faceplate is registered with SafeView it adds an extra hint to the category. This can be used in the match expression of a SafeView placeholder to only match with faceplates from a particular monitor. A normal Experion faceplate match expression would be:

```
category("?*HW_System_Faceplate?*")
```

To check for a specific monitor this expression becomes:

```
category("?*HW_System_Faceplate_Monitor=3?*")
```

The monitor numbers used are the ones assigned by the Windows operating system.

To display the monitor number:

- 1 Choose **Start > Control Panel**.
- 2 Double-click **Display**.
- 3 Click the **Settings** tab.

Controlling the location of Station command and status windows

When configuring a SafeView workspace for Station you will need to create placeholders for the Station command window(s) and status window.

The status window registers with the SafeView category “HSC_Station_StatusWindow”. The main command window uses “HSC_Station_MainWindow” and each extra command window uses “HSC_Station_CommandWindow2”.

To configure the menus and toolbars used in extra command windows see, “Multi-window toolbar and menu configuration” on page 80.

To take advantage of multiple command windows and SafeView’s new focus based matching it is best to organize placeholders into groups that match up with the areas of your screens. Each group will likely be a work area with a command window and faceplates and schematic placeholders. For more information refer to the SafeView documentation and look at the multiple command zone example connection file, toolbar menu file and SafeView workspace (multiplecommand.stn, multiplecommand.stb and multiplecommand.wdl).

Updating the page-level shortcut menu

When you right-click the background of a display in Station, that is, not on any object, the page-level shortcut menu is displayed. The Page forward command in this shortcut menu is not applicable to multi-window Station. You can remove this command from the shortcut menu.

Considerations

- Ensure the sysdefault_sm.xml does not have read-only properties set.

To remove the page forward command:

- 1 Open the C:\Program Files\Honeywell\Experion PKS\Client\System\R300\sysdefault_sm.xml file in a text or XML editor.
- 2 Locate and delete the following node in the file:

```
<menuitem id="mnu_grp" acceleratorKey="">
  <script type="onclick">
    window.external.application.InvokeMenu2(' [Navigation]
    Forward');
    window.external.ClosesShortcutMenu();
  </script>
  <text>Page Forward</text>
  <image>.\Toolbar\tb008.bmp</image>
</menuitem>
```
- 3 Save the file.

Starting multi-window Station

To start a multi-window Station, you must follow a certain startup sequence.

To start multi-window Station:

- 1 Start SafeView.
- 2 Load a workspace configuration file.
- 3 Start Station.

You should consider providing an easy method for operators to start multi-window Station. For example, in the workspace configuration file, you can specify Station to start automatically and load Station displays. You could also create a shortcut which starts SafeView and loads the appropriate workspace.

To create a shortcut that starts SafeView and loads a workspace:

- 1 In Windows Explorer, browse to the following folder:
C:\Program Files\Honeywell\Safeview
- 2 Right-click the safeview.exe file and choose **Send To > Desktop (create shortcut)**.
- 3 On the Windows Desktop, right-click the shortcut to safeview.exe file, and choose **Properties**.
- 4 In the **Target** box, add the /f option to specify the path and file name of the workspace to load.

For example:

```
"C:\Program Files\Honeywell\Safeview\safeview.exe" /f"C:\Program Files\Honeywell\Experion PKS\Client\Station\Samples\workspace1.wdl" /cp
```

The /cp option suppresses the display of the SafeView control panel.

If you want to load Station displays, use Station's /window option. The sample workspaces supplied with Experion contain examples of how to do this.

- 5 Click **OK**.

Starting multiple static Station

If you are starting multi-window Station, you do not need to complete this procedure.

If your operators are required to start multiple instances of Station, consider providing an easy method to start Station in the appropriate monitor. The `station` command has an option `-d[n]` that allows you to specify in which monitor the instance of Station appears. You can use this command option in:

- Desktop shortcuts in each of the four monitors.
- A batch file in the startup folder of the Icon Console computer.

Identifying monitor numbers

You use the Windows Display Properties to identify which monitor number relates to which physical monitor.

- 1 Choose **Start > Settings > Control Panel**.
- 2 Double-click the **Display** icon.
The **Display Properties** dialog box opens.
- 3 Click the **Settings** tab.
- 4 Click the **Identify** button to indicate monitor numbers.

To create a shortcut:

- 1 On the desktop in the monitor in which you want to create the shortcut, right-click and choose **New > Shortcut**. The Create Shortcut wizard starts.
- 2 Type the path and filename of Station and parameters to start Station using the appropriate stn file, in the appropriate monitor.

The following example starts Station in monitor 4 using the `monitor4.stn` file.

```
c:\Program Files\Honeywell\Experion PKS\client\station\
station.exe c:\Program Files\Honeywell\Experion PKS\client\
station\monitor4.stn -d4
```

Use a text editor, such as Notepad, to create the batch file:

```
rem *****
rem   change to station directory
rem *****
cd \Program Files\Honeywell\Experion PKS\client\station
rem *****
rem   start first instance of Station
rem   in monitor 1 with iconstn1.stn.
```

```

rem *****
start station.exe iconstn1.stn -d1
rem *****
rem   start second instance of Station
rem   in monitor 2 with iconstn2.stn.
rem *****
start station.exe iconstn2.stn -d2
rem *****
rem   start third instance of Station
rem   in monitor 3 with iconstn3.stn.
rem *****
start station.exe iconstn3.stn -d3
rem *****
rem   start fourth instance of Station
rem   in monitor 4 with iconstn4.stn.
rem *****
start station.exe iconstn4.stn -d4
rem *****

```

Configuring a touch screen

If you are using the NEC 2010X touch screen monitor, it is recommended you configure your system to use the following settings:

- Monitor resolution set to 1280 by 1024 pixels.
- Windows font size set to extra large fonts.
- Station configured to use the zoom setting of **Zoom to fit**.
- Station configured to use the large toolbar buttons.
- Touch screen configured to operate in **Mouse click on release** mode.
- If you use shortcut menus in Station, operators require the Touch Screen Control Panel to set the right-click function.

Touch screen limitations

If you are configuring a touch screen, consider the following limitations:

- You cannot scroll the Alarm Summary using a click and drag method as this method is not supported by the Mouse click on release mode.
- There is no keyboard emulation with the NEC 2010X touch screen, therefore you need to provide a keyboard for data entry.
- Displays with small targets are difficult to use because touch screen resolution is limited.
- Zooming on a trend requires the touch screen to operator in Mouse Emulation mode. The recommended mode is Mouse click on release.

Considerations for building displays for use with a touch screen

When building custom displays for use with a touch screen, consider the following points:

- Any targets or objects that require interaction from the operator should be large enough to allow for ease of operation.
- Provide enough space between objects to avoid operators touching the wrong object.
- Avoid building displays that require the operator to click and drag.

Customizing keys

The OEP keyboard has a set of preconfigured keys which invoke specific actions or commands. There is also a set of keys which you can customize to invoke actions and commands, and control the LEDs, referred to as relegendable keys.

For details on customizing keys see “Customizing toolbars, menus and keyboard shortcuts” on page 74 and “Controlling LEDs on a specialized keyboard” on page 81.

To support mode changes using either keyboard, the server must have the default mode acronym set (MAN, AUTO, and so on) installed. The default mode acronyms are located in Program Files\Honeywell\Experion PKS\server\data\defmodes.src. This file is added during server installation by selecting **Default Acronyms**, or can be added later by opening a Command Prompt window on the server computer and running the command:

```
filres defmodes.src
```

Adding manual input modules

You can add the following modules to your console:

- Keypad
- Thumbwheel
- Trackball

As you add these modules and connect them to your computer, the Windows operating system detects that you have added new hardware and installs the appropriate drivers.

The keypad module is the same as the number keypad on a standard keyboard, with the addition of the operator keys:

- MAN
- AUTO
- NORM
- SP
- OUT
- CLR

The trackball operates in the same manner as a standard mouse. However, the operation of the buttons on the trackball is dependant on the side of the console the trackball is installed.



Attention

If you change the configuration of your standard mouse to left-handed use, this will effect the trackball. Do not change the configuration of your standard mouse.

If the trackball is	Use the
Installed on the left-hand side of the console	Right button (inner button) for click and select functions. Left button (outer button) for context menus.
Installed on the right-hand side of the console	Left button (inner button) for click and select functions. Right button (outer button) for context menus.

The thumbwheel is used for fast raise and fast lower and slow raise and slow lower functions.

Configuring point servers

8

This chapter discusses point servers. It provides introductory information on point servers and shows you how to:

- Define a point server in Station
- Tune point servers

About point servers and flexible points

A *point server* is a software component that interfaces between the Experion server and devices and channels that are represented in Experion as flexible points.

This section discusses configuration tasks in Experion that apply to any point server. For information about a particular point server, see the documentation supplied with the field devices represented within it.

You can run a point server on the same computer as the Experion server, or on a separate computer. Depending on the point server type, you can run more than one point server on a computer, but each point server communicates with only one Experion server.

Point servers read data directly from the field when required. When a display containing the flexible point is called up, the server creates the point if it does not already exist. The point's parameter values are read from the field via the point server, and then shown on the display. The value of a flexible point parameter is stored in the Experion server while the point parameter is being accessed (e.g. the point parameter is assigned to history collection, on a display that is currently shown in Station, being accessed through the Experion OPC server, etc.).

Parameter values are updated and cached by the Experion server for a configurable period after a point is accessed.

Flexible points can be added to groups, trends, history collection, point control schedules, reports, and displays.

Considerations

- Flexible points do not support algorithms. A *derived* point must be used whenever a server algorithm is required to be configured on a flexible point parameter. (See “About derived points” on page 168.)
- Flexible points are not processed by the Experion server's alarm subsystem. For most point servers this is not an issue, because the controller or point server generates alarms on the point. However, if you are using a point server that does not support alarming, you must use derived points to do the alarming. See the reference for the particular point server for more information.
- Flexible points may not have standard parameters PV, OP and SP. You need to consider this when you are creating custom displays with flexible points or adding flexible points to trends.
- Flexible point data can be accessed using ODBC and the OPC Server.
- You need to know the numeric representation of state descriptors if you are using gating points or algorithms.

- If you have a redundant system you must install your point server on a stand-alone computer.
- If the point server supports channels, they are not shown on the System Status displays. You need to build custom displays to show the status of point server channels.
- Not all point servers use channels to communicate with Experion.
- The status of point server controllers can be viewed on the Controller Status summary.

Defining point servers in Station

After you have installed the point server software you need to define the point server to the Experion server.

To define a point server:

- 1 On the System Configuration Menu display click **System Interfaces**. The System Interface Configuration Summary display opens.
- 2 In an empty row select the Server Type and click the server alias. The Point Server Configuration display opens.
- 3 Configure the point server properties as appropriate:

Property	Description
Network Name	The point server computer name. Can be localhost or the network name of a stand-alone point server computer, but cannot be an IP address.
Alias	The name that server use for the point server. This name appears in the alarm and event summaries.
Point Server connected via dual network	Select this check box if your system uses dual networks. Leave this check box clear if you use FTE.
Allow remote servers to query for new points	If selected, enables DSA servers to query the point server for new points.

- 4 Use Configuration Studio to define the required assets for the point server.
- 5 Complete this step if your point server does not have assets defined (assets are defined in Configuration Studio). Return to Point Server Configuration display and click the **Asset Mapping** tab and select a default asset for this point server.
- 6 On the Point Server Configuration display, click the **Status** tab to check that point server is communicating with Experion server.

Point server tuning

The Tuning tab contains Cache and Communications Settings for the point server. These settings should only be changed by experienced technical personnel in consultation with your local Technical Assistance Center.

To set tuning settings:

- 1 On the System Configuration Menu display, click **System Interfaces**. The System Interface Configuration Summary opens.
- 2 Click the server alias name. The **Point Server Configuration** tab opens.
- 3 Click the **Tuning** tab.

Tune the following settings:

Property	Description
Connection timeout	The amount of time (in seconds) a packet of data can remain on the network without being acknowledged. When the timeout period expires, the connection is broken and communication is initiated again. The default value varies depending on the type of point server.
Cache flush time	The intervals (in milliseconds) that the subscription list is checked for references to old data. The default value is 60 seconds.
Cache age time	The amount of time (in milliseconds) old data remains in the dynamic cache. The default value is 10 minutes.
Maximum subscription time	The slowest subscription time (in milliseconds). The default value varies depending on the type of point server. If the subscription time is slower than that specified, the Experion server switches from subscription to synchronous read (polls). Maintaining a slow subscription is not efficient.
List fragment size	The size of data packets sent over the network. The default is 100 parameter values. This is tuned for optimal performance on low bandwidth links.
Synchronization time	The time of day that time synchronization occurs.
Notification buffer interval	The maximum amount of time (in seconds) a notification can be delayed on the point server before being sent to the Experion server. The default value is 2 seconds.

Property	Description
Notification keep alive interval	The maximum amount of time (in seconds) the point server does not send packets to the Experion server. If Experion does not receive an alarm or an alarm keep alive packet from the Point Server within this time the connection is broken and communication is initiated again. The default value is 15 seconds.

Configuring controllers

9

This chapter describes how you configure controllers in your system. It provides introductory information on controllers and channels, and shows you how to:

- Build a channel
- Build a controller
- Test the communications
- Monitor the status of system communications



Attention

The information in this chapter applies to configuring controllers other than Experion Process Controllers, point servers, and TPS.

For information on configuring Experion Process Controllers, see the *Experion Process Control Building Guide*.

For point servers, see the documentation specific to your point server.

For TPS systems, see your TPS documentation.

About controllers and channels

In Experion, the term “controller” is the generic term for devices such as loop controllers, and so on, which are used to monitor and control one or more processes and items of field equipment.

In an Experion system, controllers are connected to the server so that the server can co-ordinate the monitoring and supervising of all your plant processes.

The communication links that connect controllers to the server are known as “channels.” Every controller in your system (other than the Experion Process Controllers and point servers) must be associated with a channel. Depending on the type of controllers and the type of communications line you used to connect them to the server, you may have more than one controller on a channel.

After installing the server software and setting up your controllers, you need to:

- 1 Build your channels.
- 2 Build your controllers.
- 3 Download the channel and controller configuration data from Configuration Studio to the Experion database.
- 4 Enable each channel as described in “Enabling and disabling channels and controllers” on page 156.

Connecting controllers to the server

Depending on the capability of controllers, they connect to the server in one or more of the following ways.

- LAN (Ethernet/vendor proprietary network)
- Serial line (RS-232, RS-422, and RS-485)
- Serial line to LAN using a terminal server

Details of these connections are given in the *Installation Guide* and the Controller References (which are accessed via Quick Builder’s help).

Monitoring communications

Before you start defining controllers and channels, it is useful to understand a number of concepts that are used in Experion to flag communications failures and help you to monitor the state of your system.

After the connections between the server and the controllers have been physically set up, defined, and enabled, the server starts to record channel and controller

communications statistics. These statistics can be viewed using the channel and controller communications displays at a Station. For information on calling up these displays, see the section “Monitoring channel and controller communications” on page 158.

The server maintains the following communications statistics for each channel. If there is more than one controller on a channel, the channel values represent the sum of all of the controller values on that channel.

Total requests

Indicates the number of requests for data that have been sent to the channel or controller.

Total errors

Indicates the number of times the controller did not respond or the response was incorrect (for example, due to a bad checksum).

Barometer

Indicates the condition of the channel or controller. Every time an error occurs, the barometer is incremented by 2 or more, depending on the type of error. Every time a good call is made it is decremented by 1. If the number of errors is relatively large, the barometer value will tend to increase. If the number of errors is relatively small, the barometer value will tend to decrease. The minimum value of the barometer is not allowed to be less than zero.

Marginal and fail limit alarms

You can specify a “marginal” and a “fail” barometer limit for channels and controllers.

When the barometer reaches the marginal limit, an alarm is generated and the channel or controller communication is declared to be “marginal.” If the barometer continues to increase and the “fail” limit is reached, an alarm is generated, the channel or controller communication is declared to be “failed,” and scanning of points on that channel or controller ceases. You can specify the priority of the alarms generated using the Alarm Priority tab of the Alarm & Point Processing display.

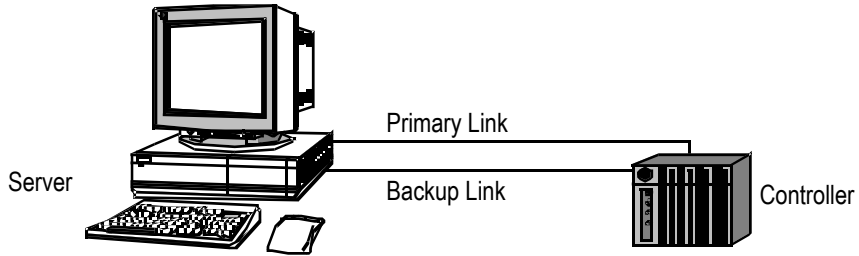
For most types of controllers, the server will try to re-establish communications every 60 seconds, using a diagnostic scan.

For some types of controllers, it is necessary to disable and then re-enable the channel or controller in order to re-establish communications after the problem has been rectified. For details of these procedures, see “Enabling and disabling channels and controllers” on page 156.

Communications redundancy

With some types of controllers, Experion provides the option of defining redundant communications links to provide a safety net in the event of communications link failures.

Figure 4 Communications redundancy architecture



Attention

If a single channel is later changed to a redundant configuration (or vice versa), then all controllers that are on that channel will need to be rebuilt to ensure that the controllers will connect to the alternate link if the primary link is disconnected or severed.

Building channels

To build channels:

- 1 In the Configuration Explorer of Configuration Studio, click **Control Strategy**.
- 2 In the SCADA Control list, click the **Build channels** task.
Quick Builder appears.
- 3 Create a channel item for each channel in your system.
When you create a channel item, you need to select a controller type; for example, Allen-Bradley, LCS620 and so on.
- 4 Select the channel item(s) in the item list and complete the relevant options on each tab.
- 5 Download the items to the server.

The information you need to specify depends on the type of channel. For details, see Quick Builder's help.

Defining redundant communication links

For devices that support communications redundancy, Quick Builder displays a Redundant Port tab, where you can configure the redundant link if you require it.

The options in the Redundant Port tab are identical to those in the Port tab. However, when you first display the Redundant Port tab, it shows only the **Port Type** and **Port Name** options. The appropriate additional options are displayed after you select a port type. For details, see Quick Builder's help for the device.

To set up redundant communications links you need to:

- 1 Define the redundant channels in the appropriate Quick Builder property tab for each controller.
- 2 On the **Channel Configuration Summary**, select the **Show Redundant Link Status** check box.
- 3 On the **Channel Status Summary**, ensure that check boxes, **A** and **B** are selected for the channels that use redundant communications links.

Configuring Stallion EasyConnection Adapter channel

The Stallion EasyConnection Adapter is used to provide up to eight RS-232, RS-422, and RS-485 serial ports for connection to appropriate controllers. In order to use these ports in channel configuration you need to make a note of which logical Windows ports relate to which physical ports on the Stallion EasyConnection board. To do this:

- 1 Choose **Start > Settings > Control Panel > Administrative Tools > Computer Management**.
- 2 Select **Device Manager**.
- 3 Expand the Ports tree to view a list of Stallion EasyConnection ports versus Windows COM ports.

Further information on the setting up of each port can be obtained by double-clicking the required port and viewing the properties, which can then be adjusted if required.

To build a channel using the Stallion EasyConnection ports, first use Quick Builder to create a new channel of the correct device type.

Configure the port for the channel using the COM port number from step 3 above.

Setting flow control

Because of limitations on how quickly they can process serial data, some computers and other devices implement flow control strategies to ensure that data is neither received nor transmitted at a rate faster than the device can process. Flow control is also used by industrial devices to interface with modems or half-duplex radio systems. Flow control strategies are also known as “handshaking”.

For controllers, flow control is usually only required when communicating through a half-duplex radio link or a modem connected to the device. Flow control is necessary for half-duplex radio systems to ensure that the radio link is “keyed” to receive or transmit data in the correct direction. Note that cabling requirements for devices that use flow control and those that do not are different. See “Cabling for Stallion EasyConnection” on page 152.

With the Stallion EasyConnection Serial Adapter different ports can be configured to use different flow control strategies. Before using the Stallion EasyConnection Serial Adapter, find out what flow control strategies are used by your devices, including any intervening modems or half-duplex radio systems.

Software flow control (XON/XOFF)

Software flow control uses special characters in the data stream to control the transmission and reception of data. These characters are called “XON” and “XOFF”. Because they interfere with the data flow, these characters should not appear in the normal data transmitted in the data stream. XON/XOFF flow control is therefore normally used only to transmit ASCII characters. Transmission of ASCII characters ensures that the XON and XOFF characters will not appear within the normal data stream. Software flow control is also called XON/XOFF handshaking.

It is possible to use software flow control in addition to hardware flow control, but this is very uncommon.

To configure your channel to use software flow control, on the Quick Builder Port tab for serial ports, choose either Input or Output from the XON/XOFF list:

- **Input** uses XON/XOFF to control the flow of data on the receive line
- **Output** uses XON/XOFF to control the flow of data on the transmit line

RS-232 hardware flow control (RTS/CTS)

Hardware flow control uses specialized RS-232 lines of the serial cable to determine whether the device is ready to process incoming data. These lines are called RTS (Request to Send) and CTS (Clear to Send). This form of flow control is often called RTS toggle/CTS handshaking.

Using this form of flow control, the server (data terminal equipment or DTE) will raise the RTS line when it wants to transmit data. The device (data communications equipment or DCE) will raise its CTS line when it is ready to receive data. When both the RTS and CTS lines are raised, the server will transmit data. After the server has finished sending data, it lowers the RTS line. The device will then lower its CTS line. The device might also lower its CTS line if its input buffer becomes full. If this occurs the server will stop transmitting data and will wait until the device raises its CTS line again before recommencing transmission. Hardware flow control has special cabling requirements. Please see “Cabling for Stallion EasyConnection” on page 152 more details.

To configure your channel to use hardware flow control, on the Quick Builder Port tab for serial ports, ensure **Enable RTS/CTS** flow control is selected.

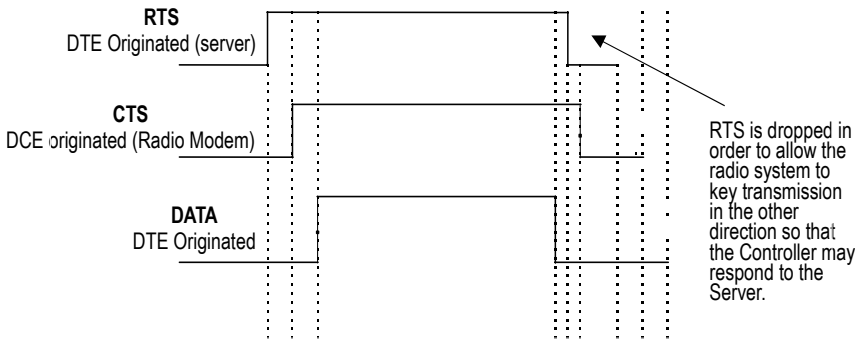


Attention

Because hardware flow control uses special RS-232 lines, this type of flow control is unavailable for RS-422 and RS-485 communications.

The following timing diagram shows how this works with a radio system.

Figure 5 Timing diagram for RTS/CTS flow control



RS-232 modem and radio link support

Some devices, such as modems and radio links, are limited not only by the rate at which they process data, but by whether their links (radio or telephone) are currently good. These devices sometimes use extra RS-232 lines to signal whether the device has a good connection.

Modems typically use DCD (Data Carrier Detect) to signal that they have a good connection. Other devices sometimes use DSR (Data Set Ready). The server can be configured to watch either or both of these lines. If the lines go down, the channel will fail.

To configure your channel to use these settings, on the Quick Builder Port tab for serial ports, ensure the appropriate Detect DCD or Detect DSR is selected.

Cabling for Stallion EasyConnection

RS-232 requirements

Most devices have their own particular RS-232 cabling requirements. See the documentation for your device to determine how to wire your RS-232 cable.

The lines from the Stallion EasyConnection board use the standard RS-232 pin assignments. The following table lists the standard RS-232 pin assignments.

Table 3 Stallion RS-232 pin assignments

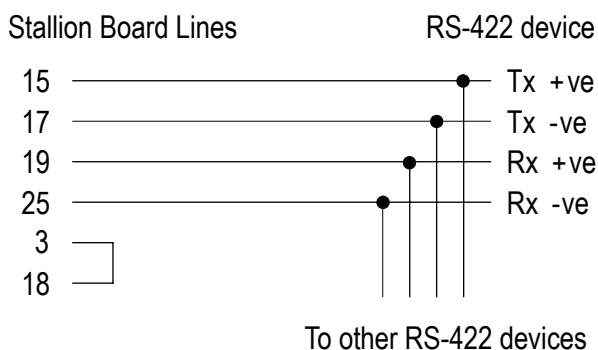
Pin Number	Data Line	Description
1	Shield	Signal Shield
2	TXD	Transmit serial data
3	RXD	Receive serial data

Table 3 Stallion RS-232 pin assignments (*continued*)

Pin Number	Data Line	Description
4	RTS	Request to Send
5	CTS	Clear to Send
6	DSR	Device (DCE) ready
7	GND or COM	Signal common (ground)
8	DCD or RLSD	Carrier Detect (Received line signal detector)
20	DTR	Server (DTE) ready
22	RI	Ring Indication

RS-422 requirements

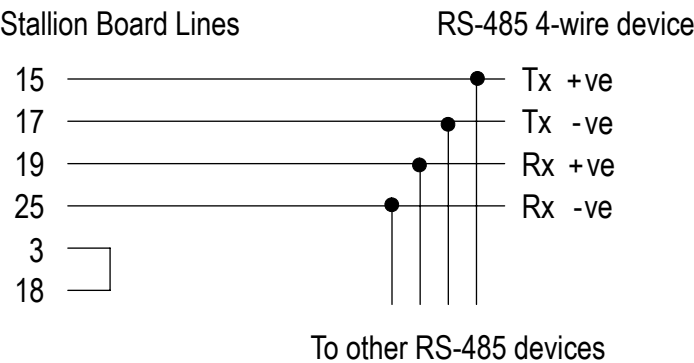
There are no special settings required in Quick Builder for a RS-422 setup. The following figure shows the wiring requirements.

Figure 6 RS-422 wiring diagram**RS-485 port configuration and wiring requirements**

To use the Stallion EasyConnection board with RS-485, select **Enable Stallion RS-485 Half Duplex** on the serial port tab for the channel properties in Quick Builder.

4-wire configuration

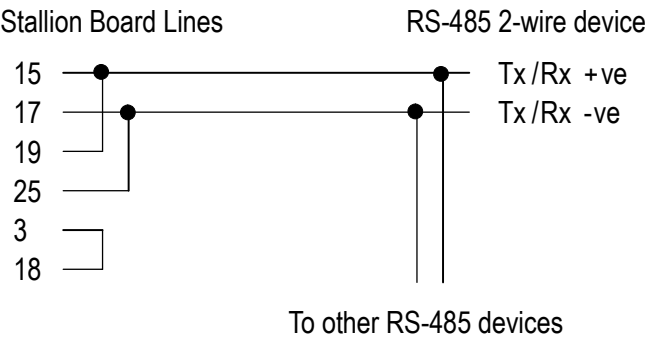
Figure 7 RS-485 wiring diagram for 4-wire configuration



2-wire configuration

To use the Stallion EasyConnection board with a 2-wire RS-485 configuration, select **Echo (Required for Stallion RS-485 ports)** on the serial port tab for the channel properties in Quick Builder.

Figure 8 RS-485 wiring diagram for 2-wire configuration



Building controllers

To build controllers in Quick Builder:

- 1 In the Configuration Explorer of Configuration Studio, click **Control Strategy**.
- 2 In the SCADA Control list, click the **Build controllers** task.
Quick Builder appears.
- 3 Create a controller item for each controller in your system. Note that when you create a controller item, you need to specify the controller type; for example, an Allen-Bradley, a Series 9000, and so on.
- 4 Select one (or more) of the controller items in the item list and then complete the relevant options on each tab. For more information, see Quick Builder's help.
- 5 Download the items to the server.

Enabling and disabling channels and controllers

After you have downloaded the channels and controllers to the server, you need to “enable” them so that the system can send and receive data.

To enable or disable channels and controllers, you need to be using Station with a security level of SUPV or higher. Security levels are described in “About security levels” on page 285.

Enabling a channel

By default, all channels are initially disabled.

To enable a channel:

- 1 Call up the System Status–Channels display as follows. Either:
 - Select **View > System Status > Channels** from the Station menu bar and scroll to the required channel.
 - Click the System box in the Status Line to call up the System Status display and ensure the Location and Status panes are open. In the System Components tree in the Location pane, expand Controllers and select the required channel.
- 2 Select the **Enable** check box.
- 3 If you are using redundant communications links select both **A** and **B** check boxes.

If you are using redundant communications links and you cannot see two check boxes, you need to show redundant links. See “Defining redundant communication links” on page 149.



Attention

The **Hiway** column in the System Status–Channels display only applies to channels for TDC 3000 Data Hiway controllers.

Enabling a controller

By default all controllers are initially enabled.

Considerations

- Even if a controller is enabled, it is only scanned by the server if the corresponding channel is also enabled.

To enable or disable a controller:

- 1 Call up the System Status–Controllers display as follows. Either:
 - Select **View > System Status > Controllers** from the Station menu bar,
 - Click the System box in the Status Line to call up the System Status display and ensure the Location and Status panes are open. In the System Components tree in the Location pane, expand Controllers and select the required controller.
- 2 If the **Enable** check box is selected the controller is enabled. Clear the **Enable** check box to disable the controller.



Attention

The **Hiway** column is applicable only to TDC 3000 Data Hiway controllers.

Monitoring channel and controller communications

You can monitor your Experion system communications by checking on the status and error statistics of each channel and each controller in your system.

Channel status and error statistics

To view status and error statistics information:

- 1 Call up the System Status–Channels display as described in “Enabling a channel” on page 156.
- 2 To view the status and error statistics of an individual channel, click its name. This displays the Channel Status Detail display for the selected channel.

The Channel Status Detail display shows the current status of the selected channel and a range of error statistics as described in “Monitoring communications” on page 146.

If you have defined redundant communications links for any of your channels, the Channel Status Detail display works like the display for a single link, except that there are two columns of information: one for link A, and one for link B.

Controller status and error statistics

To view the status and error statistics of a controller:

- 1 Call up the System Status–Controllers display as described in “Enabling a controller” on page 157.
- 2 Click the name of a controller. This displays the Controller Status display for the selected controller.

The Controller Status Detail display shows the current status of the selected controller and a range of error statistics as described in “Monitoring communications” on page 146.

If you have defined redundant communications links for any of your controllers, and you have enabled the Redundant Communications Links displays (as described in “Communications redundancy” on page 148), the Controller Status Detail display works like the display for a single link, except that there are two columns of information: one for link A, and one for link B.

Viewing channel and controller configuration information

You can call up System Configuration displays to view information about the channels and controllers that have been defined and enabled for your system.

Viewing channel configuration summary

To call up the Channel Configuration Summary display, which lists all the channels configured for your system, either:

- Choose **Configure > System Hardware > Controller Interfaces > Channels** from the Station menu bar.
- Press F1 to call up the System Menu display, and click **System Configuration**. From the System Configuration Menu display click **Channels**.

To call up the Channel Configuration display for a channel, click its number or title in the Channel Configuration Summary display.



Attention

The **Hiway** identifier and the **Enable Hiway Switching** check box under **TDC Channel Options** apply only to channels for TDC 3000 Data Hiway controllers.

The **Enable Hiway Switching** check box is used to enable and disable automatic switching by the server to the backup TDC 3000 Data Hiway when the channel fails. See the online reference module for the TDC 3000 Data Hiway controller interface for more details.

Viewing the controller configuration summary

To call up the Controller Configuration Summary display, which lists all the controllers defined to your system, either:

- Choose **Configure > System Hardware > Controller Interfaces > Controllers** from the Station menu bar.
- Press F1 to call up the System Menu display, and click **System Configuration**. On the System Configuration Menu display click **Controllers**.

For each controller in your system, the Controller Configuration Summary display shows:

- Whether or not the controller is enabled
- The channel/point server name
- The Hiway identifier (only applicable to TDC 3000 Data Hiway controllers)
- The controller ID

This information is also available on the System Status–Controllers display, and you can enable or disable controllers on both displays.

The **Configuration Upload** and **Configuration Download** columns only apply to TDC 3000 Data Hiway or UDC controllers, and are described in the individual controller configuration reference guides.

Viewing point names on a specific controller

After you have downloaded your points to the system, you can view a list of points defined for each controller in the server database. On the **Controller Configuration Summary** display, click **View Points** to display a list of the point parameters that have addresses defined for the chosen controller.

The points listed are those that have an address that refers to a real location within the controller. Points that have been associated with the controller for scanning purposes, but have addresses that reference other points or locations in the database, are not included.

Viewing controller configuration details

Considerations

- This procedure can be used only for the following controllers:
 - 7800 Burner
 - Allen-Bradley PLC5
 - Bristol Babcock
 - FSC
 - Series 9000
 - Safety Manager
 - TDC 3000
 - UDC

To view information about a specific controller:

- 1 Call up the Controller Configuration Summary display by following the instructions in “Enabling a controller” on page 157.
- 2 Click the name of a controller listed in the display. This opens the Controller Status Detail display for that controller.
- 3 Click the **Details** button. This opens the Controller Status display for that controller.

Understanding and configuring points

10

The information in this chapter applies to configuring points on controllers other than Experion Process Controllers. For information on points on Experion Process Controllers, see the *Experion Process Control Building Guide*.

This chapter provides an overview of the different types of points you can configure and how they can be used.

This chapter assumes that you have:

- A basic understanding of the various point types and how they are used in Experion. (If not, you should read the general information about points in the Overview and Planning documentation before continuing with the procedures in this chapter.)
- Followed the instructions in “Configuring Stations and printers” on page 63 and “Configuring controllers” on page 145 for configuring your controllers and channels.

About points

Experion uses points to store information about field values or devices, for example, the state of a pump, a temperature sensor, the process variable of a control loop.

Experion records each significant change in the values for a point as an event, which operators can see on the Event Summary display. Point events can also be treated as alarms, for which you can configure a priority that determines whether it is included in the Alarm Summary. For more information about point events and alarms, see “Customizing alarm behavior” on page 249.

Depending on your data acquisition and control requirements, you might only need to define very simple points. For example, you might only need to define points that are going to be used in simple processes or applications, such as monitoring an oven temperature or monitoring the state of a pump.

On the other hand, your data acquisition and control requirements might be more sophisticated. For example, you might want to use a point to:

- Monitor and provide access to a PID loop in a controller
- Generate an alarm
- Collect historical data
- Start an application
- Run a server script to perform a task on point change

Before you configure your points

Before you configure your points you should understand the following topics:

- Point types
- Point names
- Associating points with assets
- Standard point parameters
- Source and destination addresses
- Scanning and standard points
- Control properties for standard points
- History collection and archiving

After you configure your points

Once you have configured your points you might want to consider the following topics:

- Configuring Station displays for points
- Changing point configuration via Station displays
- Advanced point configuration
- Configuring algorithms

Point types

Experion provides the following point types:

Type	Description
Process	A point on an Experion Process Controller, which is accessed via the Control Data Access Server.
Status	Represents digital inputs or outputs. For example, the on and off states of a pump or light. It is a <i>standard</i> point type with a fixed data structure.
Analog	Represents continuous values. For example, pressures in a boiler or temperatures in a blast furnace. It is a <i>standard</i> point type with a fixed data structure.
Accumulator	Represents total values. For example, the volume of water that has flowed into a tank or through a turbine. It is a <i>standard</i> point type with a fixed data structure.
Database	A standard point that accesses data from parameters of other points, or from user files. See “Database addresses” on page 226.
Container	A point that ties together a set of related standard points so that you can manage them as if they were one point. A container point is, in effect, a user-defined point type that matches your data requirements for a particular device type or scenario. For more information, see “Template displays and container points” on page 379.

About flexible points

The value of a flexible point parameter is read directly from the field when required. The value of a flexible point parameter is not stored in the Experion server unless the point is configured in history collection. When a display containing a flexible point parameter is called up, the server creates the point if it does not already exist. The point's parameter values are read from the field via the system interface or point server, and then shown on the display. Parameter values are updated and cached by the Experion server for a configurable period after a point is accessed.

Flexible point parameters can be added to groups, trends, history collection, point control schedules, reports, and displays.

Considerations

- Flexible points do not support algorithms. A *derived* point must be used whenever a server algorithm is required to be configured on a flexible point parameter. (See “About derived points” on page 168.)
- Flexible points are not processed by the Experion server's alarm subsystem. For most system interfaces or point servers this is not an issue, because the controller or point server would generate alarms on the point. However, if you are using a system interface or point server that does not support alarming, you must use derived points to do the alarming. See the reference for the particular system interface or point server for more information.
- Flexible points might not have standard parameters PV, OP and SP. You need to consider this when you are creating custom displays with flexible points or adding flexible points to trends.
- Flexible point data can be accessed using ODBC and the OPC Server.
- If you have a system with redundant servers you must install your system interface or point server on a computer that is not one of the servers.

About derived points

A *derived* point is a point whose parameters are mapped to another point's parameters or a user table. Derived points are typically used to perform a function that the referenced point or user table cannot perform. For example, you build derived points if you have flexible points and want to use algorithms.

Derived points are built as standard points. You also need to build a user scan task channel and a user scan task controller.

Considerations

- Use a separate channel and controller for your derived points.
- User tables 1, 2, and 3 (Files 251, 252 and 253) are configured by default in all Experion servers. It is convenient to build a channel and controller referring to File 251, Record 1 (unless this has been used for another purpose)

To build a derived point:

- 1 Add a user scan task controller and channel and configure them as appropriate. See Quick Builder's help.
- 2 Add a point of the appropriate type, that is, status, analog or accumulator.
- 3 Enter the appropriate **Parent Asset**.
- 4 Set the **PV Scan Period** to a suitable value, such as 60 seconds.
- 5 Click the button to the right of **PV Source Address** to open the Address Builder and then:
 - a. Set **Address Type** to **Point**.
 - b. Type the name of the flexible point in **Point Name**.
 - c. Type the name of the flexible point's parameter in **Parameter**.
 - d. Select the user scan task controller from the **Controller Name** list.
 - e. Click **OK**.
- 6 Configure the point's remaining properties as appropriate.
- 7 Download the point to the server.

Point names

When a point is created, it is given a unique name, for example, POINT01, POINT02. This identifier, known as the point ID or tag name, is used in Experion whenever it is necessary to refer to a point in the server (for example, on a custom display or in a report). A point is also given an item name, for use in the context of the Enterprise Model. An item name is an intuitive name given to a point which can be used as an alternative to the tag name.

When you are creating tag names and item names, consider the following:

- Names must not be longer than 40 characters
- Tag names must contain at least one alpha character
- Do not use the following characters:
 - Space (tag name only)
 - Tab
 - Period (.)
 - Comma (,)
 - Forward slash (/)
 - Backslash (\)
 - Less than (<)
 - Greater than (>)
 - Single quote (')
 - Double quote (")
 - Asterisk (*)
 - Question mark (?)
 - Vertical bar (|)
 - Colon (:
 - Semi colon (;)
 - Brackets [] (item names only)
 - Braces { } (item names only)
 - Parentheses () (item names only)

- The first character must not be any of the following:
 - Dollar sign (\$)
 - At sign (@)
 - Space
- Names are *not* case-sensitive; POINT01 and point01 represent the same point
- If you are using a point in a recipe, the first two characters of the point name must be the descriptor of the unit that contains the point. For details about Recipes and units, see “Configuring recipes” on page 619.
- Point IDs cannot match the item name of any other point belonging to the same asset.

Associating points with assets

By associating points with assets, the point becomes an entity within the asset model. As a result points can be more easily located within the asset model because the asset model is a representation of your system. After you have created assets, you then associate points with the appropriate asset when you build your points.

An asset model is used to represent your process. It is a hierarchical arrangement of entities that represent assets, such as individual pieces of equipment in your organization. You create assets and the asset model using Configuration Studio. For more information see “About assets and the asset model” on page 40.

Assets can be assignable, enabling you to control access to assets. By associating points with assignable assets, you can control access to those points. For more information see “Assigning scope of responsibility” on page 336.

Flexible point parameters

Flexible point parameters represent the data structures and applications existing in a particular controller or device. Flexible points can have the equivalent of PV, OP and SP parameters, however they may have different names and different data structures. Flexible points are accessed via a point server interface.

For more information about the parameters used by flexible points in your system, see the relevant *Controller Reference* for the interface being used.

Standard point parameters

Each point type has a different set of parameters available. The main parameter types for standard points are summarized in Table 4 on page 174.

The following sections discuss:

- Summary of standard point parameters and addresses
- Status point parameters
- Analog point parameters
- Accumulator point parameters
- Source and destination addresses

Summary of standard point parameters and addresses

The names of the parameters reflect their most common usage. They can, however, be used to hold any controller values.

Because Experion can store and manage multiple values in the one point, you can use a single point to monitor and control a complete loop.

Not all parameters need to be configured for each point. In many cases, the only parameter of a point that needs to be configured is the PV to show the current value of a given location within a controller.

The following table summarizes the addressable parameters of the standard point types.

Table 4 Summary of point parameter types

Parameter Types	Status Points	Analog Points	Accumulator Points
SP (Set Point)		Yes	
PV (Process Variable)	Yes	Yes	Yes
OP (Output)	Yes	Yes	
MD (Mode)	Yes	Yes	
A1 (Auxiliary #1)		Yes	
A2 (Auxiliary #2)		Yes	
A3 (Auxiliary #3)		Yes	
A4 (Auxiliary #4)		Yes	

Except for the PV parameter, the input/output point parameters listed in Table 4 on page 174 can all be configured to have a source address, or a destination address, or both. The PV parameter can only be configured to have a source address, as it is used for the measured value of some element of the process, such as a temperature, that cannot be changed directly by the operator.

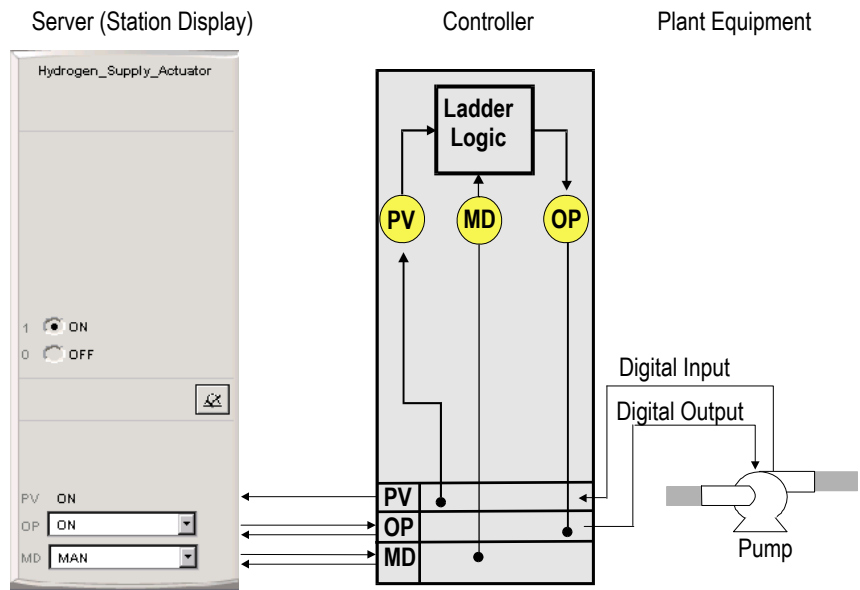
Status point parameters

A status point has three parameters which can address field values:

- Process Variable (PV)
- Output (OP)
- Mode (MD)

The following figure, Status point representing a pump, shows the relationship between a field value and a status point.

Figure 9 Status point representing a pump



Status point process variable (PV)

For every point in your system that is to be used in monitoring a process or value, you need to define the “input” (for example, the reading from a field device) so that the server knows what kind of information it has to read from the controller that is regulating that process or value.

This input is known in Experion as the “process variable” (or PV) of a point, because it represents values that are a function of the process itself (or the controller or both). Process variables cannot be changed by an operator.

When you define the PV you need to know the:

- Number of states
- State descriptors

Number of states

Status point PVs are used to represent the current “state” of the field device or process. For example, you could define four distinct states for a valve that has two limit switches: TRAVEL, CLOSED, OPEN, and FAIL. The PV for a status point in Experion can be used to represent up to eight discrete states.

Status points represent these states by reading up to three consecutive discrete values from an address in the controller. You will need two states to monitor 1 bit, up to four states to monitor 2 bits, and up to eight states to monitor 3 bits.



Attention

Bits are numbered from the least significant to the most significant.

For 2- and 3-bit addresses, the bits are assumed to have contiguous controller addresses.

State descriptors

For each state you want to use, you need to define a short alphanumeric descriptor (8 characters maximum). The number of descriptors you enter must match your selected number of states.

For example, if you wanted to use a point to monitor and control a valve, the PV might be used to represent 4 states of that valve and the descriptors might be: TRAVEL, CLOSED, OPEN, and FAIL.

Status point output (OP)

OP is the opposite of PV, that is, OP represents values that can be changed by an operator, or by another component of the system, when performing supervisory control. The OP of a point can usually only be changed by an operator if the mode of that point is set to “manual.” (For details of point modes, see “Status point mode (MD)” on page 177.)

For points in your system that are to be used in controlling a process or value, you need to define the available states that can be controlled.

For a status point, you can define up to four output states, which correspond to four of the input states for that point. In the valve example, you might define CLOSED, and OPEN as the two controllable output states.

Status point mode (MD)

The mode of a status point is used to determine whether or not an operator is permitted to control the output value. The two most common modes are: “manual” and “automatic”.

The MD state is usually determined by addressing a single bit in the controller, however some controller types support 2 bit modes.

For information about control modes, see “Control modes” on page 201.

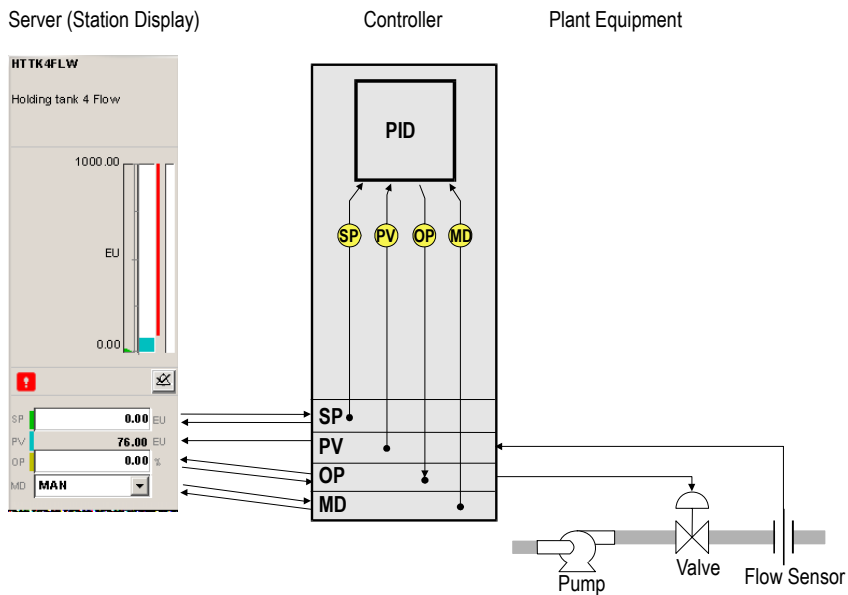
Analog point parameters

An analog point can represent the following different types of field values:

- Process Variable (PV)
- Output (OP)
- Mode (MD)
- Setpoint (SP)
- Up to four auxiliary values (A1, A2, A3, A4)

Analog points represent continuous values such as pressures or temperatures. The following figure, Analog point representing a flow control loop, shows the relationship between field values and an analog point.

Figure 10 Analog point representing a flow control loop



Analog point process variable (PV)

The PV of an analog point represents the current “reading” (represented in engineering units) of the field device or process. PVs are often used to represent the process variable of a control loop.

When you define the PV you need to specify the:

- Engineering units
- Range high value and range low value
- Drift deadband
- Clamp point

Engineering units

In defining the PV of an analog point, you need to specify the engineering units used in representing the PV value; for example, Deg. K, ohms, ML/min. The maximum length is 8 characters.

Range high value and range low value

You also need to specify the highest and the lowest valid values of the range for this point. For example, if the maximum output of a temperature transmitter represents 600 degrees celsius, and the minimum is zero degrees celsius, you need to enter the value 600 as the **Range High Value** and 0 as the **Range Low Value** so that the server can correctly “scale” or convert the raw data captured from the controller.

Drift deadband

In defining the parameters of an analog point you can specify a “drift deadband” to eliminate unnecessary point processing and therefore reduce system load.



Tip

The processing power available in a computer qualified to run Experion server software makes it unnecessary to set a value of greater than 0% for the drift deadband in most applications.

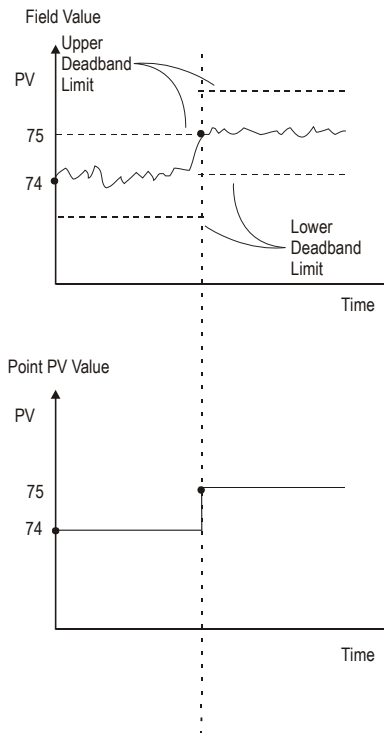
Whenever a new parameter value is scanned from a controller, further point processing is only performed if the value has changed by more than the configured drift deadband amount since processing last occurred. The deadband value is expressed as a percentage of the point range.

Further point processing includes:

- Updating the parameter value
- Processing point alarms

The following figure, Drift deadband, shows how drift deadbands work in relation to PV.

Figure 11 Drift deadband



Clamp point

When defining an analog point you can indicate whether you want the PV to be clamped to 0% if it is less than the PV clamp low limit, and 100% if it is greater than the PV clamp high limit.

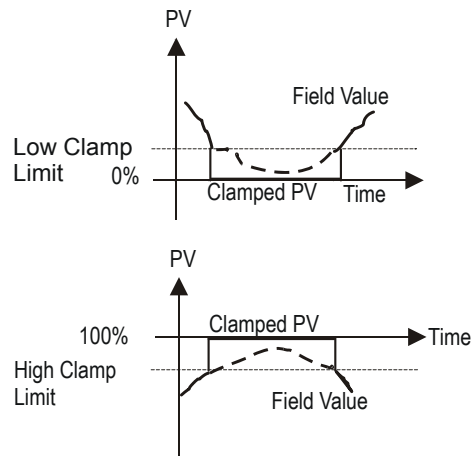
For example, because of instrumentation inaccuracies or anomalies, a controller might give a reading of 9 units, when in fact you know that the reading should be zero. By setting a PV clamp limit of 10, you can force the reading from the controller to be read as zero whenever it is less than 10. This can be useful when integrating a value over time.

The high and low limits for the PV clamp are defined on Point Processing tab on the Alarm & Point Processing display. The values are entered as a percentage of the point range.

Leaving the clamp limits at the default values of -10% (low) and 110% (high) makes them essentially ineffective.

The following figure, Effects of PV clamping shows how PV clamps work.

Figure 12 Effects of PV clamping



Analog output (OP)

The output (or “OP”) can be used to read and write an analog value. It can only be changed by an operator if the mode is set to MANUAL (see “Analog mode (MD)” on page 181).

The OP value is always in the range of 0% to 100% and is intended to indicate “% open” of a valve. If the valve is reverse acting, for example, 4 mA represents valve fully open and 20 mA represents valve fully closed, then the OP Reverse parameter should be enabled so that the OP indicator still shows “% open”.

Analog mode (MD)

The mode (or “MD”) is used to determine whether or not an operator is permitted to control the output value. The two most common modes are: “manual” and “automatic.” For more details about control modes, see “Control modes” on page 201.

Analog setpoint (SP)

The setpoint (or “SP”) can be used to read and write an analog value in a controller. Set points are represented in engineering units and are often used to represent the required operating value for a control loop.

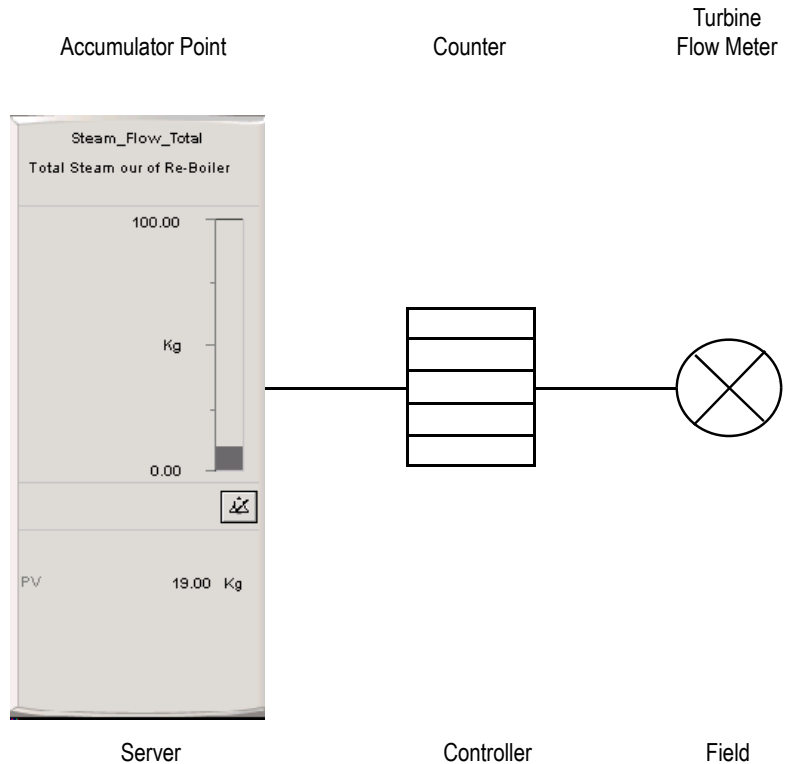
Analog auxiliary values (A1, A2, A3, and A4)

Up to four additional values can be used to read and write four analog values in a controller. These auxiliary values are given names A1 to A4 and are represented in engineering units. Auxiliary values can be used to display the tuning constants of a control loop, or any other addressable parameters in the controller.

Accumulator point parameters

Accumulator points represent totalizers. The following figure, Accumulator point, shows the relationship between a field value and an accumulator point.

Figure 13 Accumulator point



An accumulator point can access a single counter input value.

Accumulator point process variable (PV)

The PV for an accumulator point is used to read a value from a counter (in a controller) that continues to increment until it reaches its rollover value, at which time it resets.

When you define the accumulator point you specify:

- Engineering units
- Rollover value of controller counter

- Range high value (used for the PV indicator and RSHI alarm only)
- Scale factor
- Meter factor

The following example describes how accumulator process variables work and illustrates some of the concepts used in defining the PV of an accumulator point.

Example

Suppose there is a server accumulator point named AZGALLONS and that this point is connected to a field value that is a counter that counts from 0 to 4095. At 4096, the counter's value rolls over to 0. Suppose also that the AZGALLONS scale and meter factors are set to 1 and that the values of AZGALLONS and the field values are both 4000:

If the Field counter increases by:	The field value of the counter is:	And the value of AZGALLONS is:
50	4050	4050
50	4	4100
50	54	4150

The value of AZGALLONS will continue to increase either until it is reset by an operator, or until it reaches the maximum value that it can display (in which case it will display a series of asterisks).

Engineering units

In defining the PV of an accumulator point, you need to specify the engineering units used in representing the PV value for an accumulator point; for example, ML, Kwh. The maximum length is 8 characters.

Rollover value

In defining an accumulator point you need to specify the value at which the “physical” counting or totalizing mechanism on the device or controller rolls over.

Note that, regardless of this “physical” rollover value, the accumulator point PV continues to increase indefinitely until it reaches its maximum value or until it is reset by an operator.

Range high value

You also need to specify the value that represents the highest available range for this point. This is only used to scale the height of the PV indicator and for the RSHI alarm.

Scale factor

The scale factor is a multiplier (usually close to 1) that is used to convert the raw counts of the totalizing device into engineering units. For example, if you are measuring totals in megalitres, and the counting device uses 1 count to indicate 1 megalitre, the scale factor would be 1; if it uses 1 count to indicate 2 megalitres, the scale factor would be 2.

Meter factor

A meter factor is a multiplier that is used for calibration purposes.

Every time the controller's counter value is scanned, the PV value is determined by the following formula:

$$PV_{new} = PV_{old} + (SF \times MF \times Rawcounts)$$

Part	Description
<i>PV_{new}</i>	The new PV
<i>PV_{old}</i>	PV at the last scan
<i>SF</i>	The scale factor
<i>MF</i>	The meter factor
<i>Rawcounts</i>	The change in the counter value since the last scan. If the new raw count is less than the old raw count, the counter is assumed to have rolled over.

Summary of internal parameters

The following table shows the internal parameters for the point types status, analog and accumulator.

Internal Parameter	Description	Status	Analog	Acc.
PointID	The name of the point. This name identifies the point.	Yes	Yes	Yes
Description	The description of the point.	Yes	Yes	Yes
ItemName	An alternative name for the point that is used in the context of the asset mode.	Yes	Yes	Yes
FullItemName	The item name of the point combined with the item name of its parent asset, and so forth, up to a top level node in the asset model.	Yes	Yes	Yes
LocationTagName	The tag name of the point's parent asset.	Yes	Yes	Yes
LocationFullItemName	The full item name of the point's parent asset.	Yes	Yes	Yes
EULO	0% range	Yes	Yes	
EUHI	100% range	Yes	Yes	
AlarmLimit1	The value at which alarm 1 is tripped.		Yes	Yes
AlarmLimit2	The value at which alarm 2 is tripped.		Yes	Yes
AlarmLimit3	The value at which alarm 3 is tripped.		Yes	Yes
AlarmLimit4	The value at which alarm 4 is tripped.		Yes	Yes
AlarmLimit5	The value at which alarm 5 is tripped.		Yes	Yes
AlarmLimit6	The value at which alarm 6 is tripped.		Yes	Yes
AlarmLimit7	The value at which alarm 7 is tripped.		Yes	Yes
AlarmLimit8	The value at which alarm 8 is tripped.		Yes	Yes
AlarmType1	The type of alarm 1, for example, PVHI		Yes	Yes
AlarmType2	The type of alarm 2, for example, PVHI		Yes	Yes
AlarmType3	The type of alarm 3, for example, PVHI		Yes	Yes
AlarmType4	The type of alarm 4, for example, PVHI		Yes	Yes

Internal Parameter	Description	Status	Analog	Acc.
AlarmType5	The type of alarm 5, for example, PVHI		Yes	Yes
AlarmType6	The type of alarm 6, for example, PVHI		Yes	Yes
AlarmType7	The type of alarm 7, for example, PVHI		Yes	Yes
AlarmType8	The type of alarm 8, for example, PVHI		Yes	Yes
RollOver	Accumulator input rollover value, for example, a 12 bit counter rolls over at 4095.			Yes
MeterFactor	The accumulator meter factor. Normally 1.0, is adjusted after meter proving.			Yes
ScaleFactor	The accumulator scale factor, for example, 1 pulse.count = 5.678 liters.			Yes
RawPV	The value of the accumulator raw input (the counter it is reading).			Yes
SetpointLowLimit	Data entry of Setpoint values below this value will be rejected.		Yes	
SetpointHighLimit	Data entry of Setpoint values above this value will be rejected.		Yes	
OutputLowLimit	Data entry of Outpoint values below this value will be rejected.		Yes	
OutputHighLimit	Data entry of Outpoint values above this value will be rejected.		Yes	
LastProcessedDate	The day when the value of the PV last changed.	Yes	Yes	Yes
LastProcessedTime	The time of day when the value of the PV last changed.	Yes	Yes	Yes
H1M	History Standard 1 min	Yes	Yes	Yes
H6M	History Standard 6 min	Yes	Yes	Yes
H1H	History Standard 1 hour	Yes	Yes	Yes
H8H	History Standard 8 hour	Yes	Yes	Yes
H24H	History Standard 24 hour	Yes	Yes	Yes
H5SF	History Fast, configurable between 1 and 30 seconds.	Yes	Yes	Yes
H1HE	History Extended 1 hour	Yes	Yes	Yes

Internal Parameter	Description	Status	Analog	Acc.
H8HE	History Extended 8 hour	Yes	Yes	Yes
H24HE	History Extended 24 hour	Yes	Yes	Yes
OnScan	0=off, 1=on	Yes	Yes	Yes
AlarmValue	If the point is not in alarm, the AlarmValue parameter has a value of 0. Otherwise the value is equal to the alarm type as defined in the alarm limit. For example, if the point is in the PV LO state the AlarmValue parameter is 6.	Yes	Yes	Yes
ControlLevel	The operator must have this control level or better to be able to control the point.	Yes	Yes	Yes
AlarmDisabled	Alarming is disabled for the point. (0=enabled. 1=disabled)	Yes	Yes	Yes
PVInError	The Process value is unreliable. (0=ok, 1=error)	Yes	Yes	Yes
ModeInError	The Mode value is unreliable. (0=ok, 1=error)	Yes	Yes	
SetPointInError	The Setpoint value is unreliable. (0=ok, 1=error)		Yes	
OutputInError	The Output value is unreliable. (0=ok, 1=error)	Yes	Yes	Yes
A1InError	The A1 value is unreliable. (0=ok, 1=error)		Yes	
A2InError	The A2e value is unreliable. (0=ok, 1=error)		Yes	
A3InError	The A3 value is unreliable. (0=ok, 1=error)		Yes	
A4InError	The A4 value is unreliable. (0=ok, 1=error)		Yes	
Units	The engineering units for the point, for example, Liters, The PV is 3.45 Liters.		Yes	Yes
State0Descriptor	The text that describes PV state 0, for example, Travel.	Yes		
State1Descriptor	The text that describes PV state 1, for example, Open.	Yes		
State2Descriptor	The text that describes PV state 2, for example, Closed.	Yes		

Internal Parameter	Description	Status	Analog	Acc.
State3Descriptor	The text that describes PV state 3, for example, Invalid.	Yes		
State4Descriptor	The text that describes PV state 4, for example, Stopped.	Yes		
State5Descriptor	The text that describes PV state 5, for example, Stopped.	Yes		
State6Descriptor	The text that describes PV state 6, for example, Stopped.	Yes		
State7Descriptor	The text that describes PV state 7, for example, Stopped.	Yes		
TargetPVforOPState0	The PV state that is expected for OP state 0, for example, 0=Travel.	Yes		
TargetPVforOPState1	The PV state that is expected for OP state 1, for example, 1=Open.	Yes		
TargetPVforOPState2	The PV state that is expected for OP state 2, for example, 2=Closed.	Yes		
TargetPVforOPState3	The PV state that is expected for OP state 3, for example, 3=Invalid	Yes		
PVAlgoNumber	The number of the algorithm used during PV processing.	Yes	Yes	Yes
PVAlgoBlock	The number of the algorithm block used by the PV algorithm.	Yes	Yes	Yes
ActionAlgoNumber	The number of the algorithm used during PV change processing.	Yes	Yes	Yes
ActionAlgoBlock	The number of the algorithm block used by the PV change algorithm.	Yes	Yes	Yes
UnackAlarmExists	The point has alarmed and the alarm has not been acknowledged.	Yes	Yes	Yes
Alarm1Priority	The alarm priority of alarm 1, for example, Urgent.		Yes	Yes
Alarm2Priority	The alarm priority of alarm 2, for example, Urgent.		Yes	Yes
Alarm3Priority	The alarm priority of alarm 3, for example, Urgent.		Yes	Yes
Alarm4Priority	The alarm priority of alarm 4, for example, Urgent.		Yes	Yes
Alarm5Priority	The alarm priority of alarm 5, for example, Urgent.		Yes	Yes

Internal Parameter	Description	Status	Analog	Acc.
Alarm6Priority	The alarm priority of alarm 6, for example, Urgent.		Yes	Yes
Alarm7Priority	The alarm priority of alarm 7, for example, Urgent.		Yes	Yes
Alarm8Priority	The alarm priority of alarm 8, for example, Urgent.		Yes	Yes
State0AlarmPriority	The alarm priority of state 0, for example, Urgent.	Yes		
State1AlarmPriority	The alarm priority of state 1, for example, Urgent.	Yes		
State2AlarmPriority	The alarm priority of state 2, for example, Urgent.	Yes		
State3AlarmPriority	The alarm priority of state 3, for example, Urgent.	Yes		
State4AlarmPriority	The alarm priority of state 4, for example, Urgent.	Yes		
State5AlarmPriority	The alarm priority of state 5, for example, Urgent.	Yes		
State6AlarmPriority	The alarm priority of state 6, for example, Urgent.	Yes		
State7AlarmPriority	The alarm priority of state 7, for example, Urgent.	Yes		
AlarmPriority	The alarm priority of unreasonable alarm.		Yes	Yes
AlarmSubPriority	The alarm subpriority of unreasonable alarm.		Yes	Yes
ControlFailAlarmPriority	The alarm priority at which a control failure is alarmed.	Yes	Yes	Yes
ControlFailAlarmSubPriority	The alarm subpriority at which a control failure is alarmed	Yes	Yes	Yes
Alarm1SubPriority	The alarm subpriority of alarm 1. (0-15)		Yes	Yes
Alarm1SubPriority	The alarm subpriority of alarm 1. (0-15)		Yes	Yes
Alarm2SubPriority	The alarm subpriority of alarm 2. (0-15)		Yes	Yes
Alarm3SubPriority	The alarm subpriority of alarm 3. (0-15)		Yes	Yes

Internal Parameter	Description	Status	Analog	Acc.
Alarm4SubPriority	The alarm subpriority of alarm 4. (0-15)		Yes	Yes
State0AlarmSubPriority	The alarm subpriority of state 0. (0-15)	Yes		
State1AlarmSubPriority	The alarm subpriority of state 1. (0-15)	Yes		
State2AlarmSubPriority	The alarm subpriority of state 2. (0-15)	Yes		
State3AlarmSubPriority	The alarm subpriority of state 3. (0-15)	Yes		
State4AlarmSubPriority	The alarm subpriority of state 4. (0-15)	Yes		
State5AlarmSubPriority	The alarm subpriority of state 5. (0-15)	Yes		
State6AlarmSubPriority	The alarm subpriority of state 6. (0-15)	Yes		
State7AlarmSubPriority	The alarm subpriority of state 7. (0-15)	Yes		
AssociatedDisplay	When the associated display key is pressed, this display is called up.	Yes	Yes	Yes
AlarmMessageIndex	A point can be configured to generate a message. This is the message number.	Yes	Yes	Yes
REALARM	If set (=1), the point in alarm transitions between alarm states.	Yes		
PVExternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the PV changes.	Yes	Yes	
MDEternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the MD changes.	Yes	Yes	
OPEternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the OP changes.	Yes	Yes	
SPEternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the SP changes.		Yes	
A1ExternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the A1 changes.		Yes	
A2ExternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the A2 changes.		Yes	
A3ExternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the A3 changes.		Yes	
A4ExternalChangeAlarmEnable	If enabled (=1), an alarm is generated if the A4 changes.		Yes	
InUserAlarm1	If enabled (=1), an alarm is generated		Yes	
InUserAlarm2	If enabled (=1), an alarm is generated		Yes	
InUserAlarm3	If enabled (=1), an alarm is generated		Yes	
InUserAlarm4	If enabled (=1), an alarm is generated		Yes	

Internal Parameter	Description	Status	Analog	Acc.
State0AlarmEnabled	State 0 is an alarm state.	Yes		
State1AlarmEnabled	State 1 is an alarm state.	Yes		
State2AlarmEnabled	State 2 is an alarm state.	Yes		
State3AlarmEnabled	State 3 is an alarm state.	Yes		
State4AlarmEnabled	State 4 is an alarm state.	Yes		
State5AlarmEnabled	State 5 is an alarm state.	Yes		
State6AlarmEnabled	State 6 is an alarm state.	Yes		
State7AlarmEnabled	State 7 is an alarm state.	Yes		
NumberOfInputStates	Number of Status PV states (2, 4, or 8)	Yes		
NumberOfOutputState	Number of Status OP states (2 or 4)	Yes		
NormalMode	The normal mode of the point, for example, Auto.	Yes	Yes	
PulseWidthSecs	For a status OP, if this is non zero, the OP will be reset to zero after this time.	Yes		
OPReverse	The OP value is reversed.	Yes	Yes	
ControlConfirmRequired	If enabled (=1), the operator must confirm all changes to the point.	Yes	Yes	
ControlTimeout	An index to a system table that specifies the time in seconds that a control takes to complete.	Yes	Yes	
DriftDeadbandPercent	The value must change by more than this amount to be considered a change.		Yes	
AlarmDeadbandPercent	The value must drop below the alarm limit by this amount before the alarm is returned.	Yes	Yes	Yes
ControlDeadbandPercent	The value gets this close to the target value, the control is considered complete.		Yes	
PVClampingEnabled	If enabled (=1), the PV will be clamped between the high and low clamp limits.		Yes	
PointDetailDisplayDefault	The default detail display for the point type.	Yes	Yes	Yes
GroupDetailDisplayDefault	The default group display for the point type.	Yes	Yes	Yes
PVAlgoExists	If set (=1), a PV algorithm has been built on the point.	Yes	Yes	Yes

Internal Parameter	Description	Status	Analog	Acc.
ActionAlgoExists	If set (=1), an Action algorithm has been built on the point.	Yes	Yes	Yes
PointInAlarm	The point is in alarm (0=no alarm, 1=in alarm)	Yes	Yes	Yes
InRateOfChangeAlarm	If set (=1), a Rate of Change alarm exists.		Yes	Yes
InDeviationLowAlarm	If set (=1), a Deviation Low alarm exists.		Yes	
InDeviationHighAlarm	If set (=1), a Deviation High alarm exists.		Yes	
InTransmitterLowAlarm	If set (=1), a Transmitter Low alarm exists.		Yes	
InTransmitterHighAlarm	If set (=1), a Transmitter High alarm exists.		Yes	
InLowAlarm	If set (=1), a PV Low alarm exists.		Yes	
InHighAlarm	If set (=1), a PV High alarm exists.		Yes	Yes
InLowLowAlarm	If set (=1), a PV Low Low alarm exists.		Yes	
InHighHighAlarm	If set (=1), a PV High High alarm exists.		Yes	Yes
InUnreasonablyLowAlarm	If set (=1), an Unreasonably Low alarm exists.		Yes	
InUnreasonablyHighAlarm	If set (=1), an Unreasonably High alarm exists.		Yes	Yes
ModeCheckDisabled	If set (=1), the mod is not checked before doing a control.	Yes	Yes	
A1AssociatedParameter	If non zero, the A1 value is store to this parameter.		Yes	
A2AssociatedParameter	If non zero, the A2 value is store to this parameter.		Yes	
A3AssociatedParameter	If non zero, the A3 value is store to this parameter.		Yes	
A4AssociatedParameter	If non zero, the A4 value is store to this parameter.		Yes	
State0InAlarm	If set (=1), a State 0 alarm exists.	Yes		
State1InAlarm	If set (=1), a State 1 alarm exists.	Yes		
State2InAlarm	If set (=1), a State 2 alarm exists.	Yes		
State3InAlarm	If set (=1), a State 3 alarm exists.	Yes		

Internal Parameter	Description	Status	Analog	Acc.
State4InAlarm	If set (=1), a State 4 alarm exists.	Yes		
State5InAlarm	If set (=1), a State 5 alarm exists.	Yes		
State6InAlarm	If set (=1), a State 6 alarm exists.	Yes		
State7InAlarm	If set (=1), a State 7 alarm exists.	Yes		

Source and destination addresses

To define the main properties and control properties of a point, you need to understand source and destination addresses and how they are used. (See “Control properties for standard points” on page 200 for information about defining control properties.)

Address types

Points are generally used to read values from and write values to an address in a controller.

Locations (usually in the memory of the controller) that are to be read (or “scanned”) by the server are referred to as the *source address* for a point parameter.

Locations that are to be written to (or “controlled”) by the server are referred to as the *destination address* for a point parameter.

Source and destination addresses generally refer to locations within real controllers. These addresses are known as *hardware addresses*.

Experion uses “control confirmation” scans to ensure that controls are actually performed by a controller. When a point parameter has both a source and a destination address, the source address is scanned immediately after the destination address is written to. An alarm is generated if the scanned value does not match the controlled value, indicating that an attempted operator action did not actually occur.

The formats of hardware source and destination addresses depend on the type of controller. Details about the format of these addresses can be found in Quick Builder’s help for each controller.

It is also possible to address information in the server database, for example, the parameter of another point. These are known as *database addresses* (see “Database addresses” on page 226).

Scanning and standard points

This section is applicable to standard points only.

Scanning is the process by which the server reads values from locations in controllers, specified by the source addresses, and stores them in point parameters.

The server uses the scanning process for status, analog, and accumulator points.

To minimize the load on the whole system, it is important to plan for and implement an efficient scanning strategy. A point can have multiple parameters associated with it and all point parameters must be considered when analyzing the point scan load of a system.

The methods of scanning are:

- Periodic
- Exception
- Demand

Periodic scanning

Periodic scanning is the regular scanning of a point parameter at specified time intervals.

You can choose from several scan periods, ranging from seconds to minutes, and you can assign a different scan period to each input/output point parameter when you configure each point. For example, if you assign a scan period of 15 seconds to the PV parameter of a point, the server scans the value in the controller every 15 seconds.

When choosing a scan period, consider the following factors:

- Whether the controller automatically reports changes of state. If so, periodic scanning might not be necessary (see “Exception scanning” on page 197).
- The rate of change of the value. If a value only changes once an hour, it is inefficient to scan that value every five seconds.
- The rate at which history needs to be collected for the parameter. A point requiring one minute snapshots to be recorded would not necessarily require a scan period less than 60 seconds. (For details of point history collection, see “History collection and archiving” on page 215.)
- How quickly field changes need to be available on a Station display. Dynamic values on a display are updated from the database at the configured update rate of the Station.

- The number of values that can be scanned from a controller at a particular scan rate. For example, it is unlikely that 2000 analog values could be scanned every second from a controller connected to server via a serial line operating at 1200 baud. Many factors influence this value; see “Scan packets” on page 198 for more details.

Some experimentation might be required to arrive at optimum scanning periods. See “Analyzing the scanning load with lisscn” on page 198 for information on analyzing scanning performance.

Exception scanning

Exception scanning is only available for those controllers that support the reporting of significant events to the server.

Significant events can include such things as:

- Changes in a status point
- Significant changes in an analog point
- Analog alarms

For more information about configuring this type of scanning, see the controller-specific help in Quick Builder.

Demand scanning

Demand scanning provides a one-shot scan of a point parameter in response to a request. Two main types of demand scanning are used:

- Scan Point Special
- Control Confirmation

A Scan Point Special is a forced scan of point parameters. Whenever scanning of a point is disabled and then re-enabled (for example using the Point Detail display), a Scan Point Special is performed. Application programs and free format reports can request a Scan Point Special demand scan of a point. See “Configuring reports” on page 399 and the *Application Development Guide* for more information.

After an OP, SP, MD, or an auxiliary parameter control is issued, a demand scan is issued on the source address (if configured). This is to confirm that the control took place correctly. If the scanned value does not match the controlled value (within the deviation deadband), a control fail alarm may be generated.

See “Analog point alarms” on page 211 for more information on control fail alarms for analog points.

See “Status point alarms” on page 209 for more information on control fail alarms for status points.

Scan packets

The basic unit of scanning used by the server to acquire data from a controller is referred to as a *scan packet*. One scan packet represents a single transaction with a controller; that is, every time the server sends a request to a controller for data, one scan packet is used.

A scan packet can access several addresses within a controller to provide values for several server points. Because the number of requests per second is generally a limiting factor, the scanning strategy should attempt to obtain the maximum number of point parameter values in the minimum number of scan packets.

The basic requirements for points to be in the same scan packet are as follows:

- Parameters should be at the same scan period.
- Parameters should have source addresses that reference the same controller and are contiguous.
- The number of values to be acquired does not exceed the scan packet size for the particular controller.

Every time points are configured, the server rebuilds the scan packets in order to re-optimize scanning. For example, the server will ensure that:

- If there are multiple references to an address at the same scan rate, there will be only one entry in the scan packet.
- If there are multiple references to an address at different scan rates, a single entry will be made at the fastest rate.

A separate scan packet is created for each database address. Database addresses are used to scan information from other point parameters or from files in the server database. For details, see “Database addresses” on page 226.

It is strongly recommended that you follow the instructions for optimizing scan packets (and hence maximizing scanning performance) as described in Quick Builder’s help for each controller interface.

Analyzing the scanning load with **lisscn**

The **lisscn** utility that comes with Experion can be used to list the details about the currently configured scan packets in the server database.

Use the **lisscn** utility program to list the currently configured:

- Scan packets in each scan period (interval)
- Number of scan packets per period
- Scan packets per period per second

For details of how you run the **lisscn** utility, see “lisscn” on page 845.

Control properties for flexible points

Control confirmation

When an operator performs a control action on a point for which control confirmation has been specified, a prompt is displayed to the operator to confirm control. The operator must respond yes before the control action is carried out or no to abort the command.

Control modes

The current control mode of a point determines whether or not an operator is permitted to control the certain parameters of the point.

The available control modes are defined by the type of controller or device you are using.

Control properties for standard points

When you create a point you specify properties relating to how the point is controlled.

When specifying control properties for a point you need to consider:

- Source and destination addresses
- Scanning and standard points
- Control confirmation
- Control modes
- Control timeout for status points
- Reverse output
- Control level

For status points you also need to consider:

- Output states
- Pulsing

For analog points you also need to consider:

- Low and high control limit for OP and SP
- Control deadband for analog points

Reverse output

Reverse output for an analog point is used to allow the OP parameter to always indicate “% open” regardless of the control valve action. If the valve is forward acting (for example, 4 mA is closed, 20 mA is open) then leave Reverse Output deselected. If the valve is reverse acting (for example, 4 mA is open and 20 mA is closed) then ensure Reverse Output is selected.

Reverse output for a status point can be used to correct incorrect (or reversed) output wiring. However, it is advisable to physically correct the wiring as soon as possible and deselect Reverse Output.

Control confirmation

When an operator performs a control action on a point for which control confirmation has been specified, a prompt is displayed to the operator to confirm control. The operator must respond “yes” before the control action is carried out or “no” to abort the command. If electronic signatures has been specified in conjunction with control confirmation, the operator must enter an authorized ID and password before the action is carried out. For more information on electronic signatures see “Configuring Electronic Signatures” on page 355.

Control modes

The current control mode of a point determines whether or not an operator is permitted to control the OP or SP of the point.

The available control modes are: manual, automatic, cascade, and computer although cascade and computer are only available with specific controllers. Most Experion device interfaces support just single bit modes (that is, values of **0** and **1**, displayed by default as **MAN** and **AUTO**).

For PLC devices this is used to scan/control a bit within the controller that can then be used for mode control within its logic. Other device interfaces define specific behavior for the mode values (for example, S9000 supports this feature).

Property	Description
Man	When the manual mode is set, an operator is permitted to change either the set point or the output value.
Auto	When the automatic mode is set, the controller itself (or sometimes the server) controls the output and operators cannot change the output value, unless “Disable mode checking on output” is set (see “Control confirmation” on page 201).
Casc	Cascade mode is specific to S9000, TDC, and UDC controllers. The cascade mode is used when the SP is coming from the output of another PID loop within the controller (that is, PID loops are cascaded together). When the mode is set to cascade, operators cannot change either the set point or the output value.
Comp	This mode is specific to TDC controllers. The computer mode is used when the SP is coming from a computer that is performing automatic control. When the mode is set to computer, operators can change either the set point or the output values.

Normal mode

When defining a point that includes a control you can specify what is to be the “normal mode” for that point. The normal mode applies:

- By default for this point.
- When an authorized operator presses the appropriate function key(s) to reset the mode after manual intervention. (For details, see the *Operators Guide*.)

For most points, the normal mode is **Auto**.

Mode checking

Normally, the server checks that the mode of the point is set to MAN before it allows an operator to change the OP for that point. In some circumstances (for example, you might not want to implement modes for that point), you might want to disable this mode-checking by the server.

Control level

Using the control level provides an additional form of security on individual points. For each point, you can specify a control level between 0 and 255. At Stations using operator-based security, operators can only control a point if they are defined with a control level equal to or higher than the point’s control level. (See “Configuring security and access” on page 281 for information about operator-based security.)

Control properties for status points

This section discusses control properties specific to status points.

Output states

The OP parameter can address 1 or 2 bits in the controller; the corresponding number of OP states is 2 or 4.

Target input state associations

For each OP state, you define the PV state you expect to see when that particular OP state is selected.

Pulsing

Pulsing is an action that is performed by the server. When an operator issues a control, one pulse width later the server issues the reverse control. For example, if the operator switches an output ON the server switches the output OFF one pulse width later.

When you configure your point you can specify the period of the pulse width.

By default pulsing is disabled.

Considerations

- Where feasible, the controller should perform pulsing in preference to the server.
- Critical applications should not use server pulsing.

Control timeout for status points

You use control timeout to specify the maximum allowable time for the PV of the point to reach the target state for the OP action, before a PV Fail alarm is generated.

For example, if an operator has used Station to set the OP of a pump to the ON state, the server then reads the controller every 10 seconds to determine whether the pump PV is in fact ON or OFF. If the ON state is not achieved before the control timeout period expires, an alarm is raised to indicate that the control has failed.

To configure the generation of control timeout alarms for status point outputs or modes, as described in the previous examples, you must:

- Specify the target input states for the point.
- Enable the control failure alarm option (as described in “Status point alarms” on page 209).

Control fail alarms for status points

When a status point control is issued, the server tests for control failure as follows:

- After an OP or MD parameter control is issued, a demand scan on the source address is performed by the server. If the scanned value does not match the controlled value, a control fail alarm is generated.
- If a control timeout value has been defined, a PV Fail Alarm is generated when the PV fails to match the OP. (See the description of “Control timeout for status points” on page 203.)

Control properties for analog points

This section discusses control properties specific to analog points.

Low and high control limit for OP and SP

You can set limits to specify the lowest and highest value that can be set for the OP or SP of a point. These limits are called Low Control Limit and a High Control Limit.

These limits do not apply to the actual values that the controller is capable of registering or controlling, only to the control limits set for performing supervisory control from the server.

Control deadband for analog points

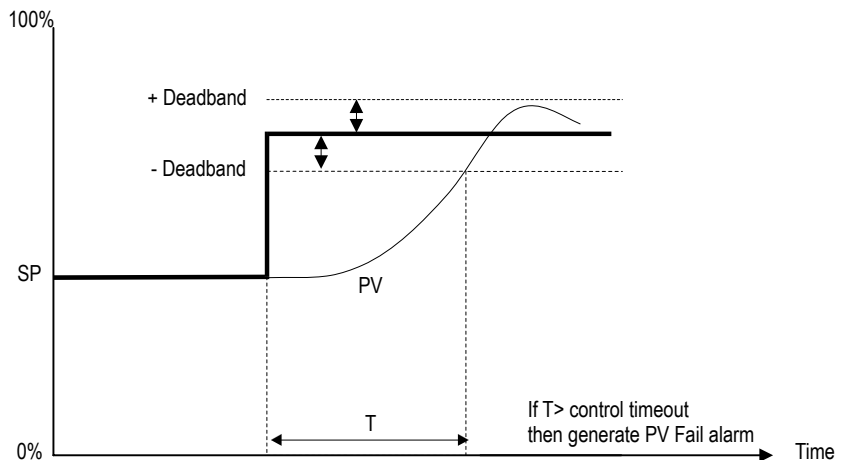
You can specify a percentage value that is used in determining what constitutes a good control. This is called control deadband.

A control deadband works as follows. If the PV signal, read back after an SP control is issued, does not reach the following value within the period specified for the **Control Timeout** option, a PV Fail alarm is generated:

$$\text{New SP value} \pm \text{Deadband Percentage}$$

This check is performed every 10 seconds (from when the control is performed) until good control has been achieved or the control timeout period has elapsed (whichever happens first).

Figure 14 Control deadbands



Control fail alarms for analog points

When an analog point control is issued, the server tests for control failure as follows:

- After an OP, SP, MD, or auxiliary parameter control is issued, a demand scan on the source address is performed by the server. If the scanned value does not match the controlled value, a control fail alarm is generated.
- If a control timeout and control deadband value have been defined, a PV Fail Alarm is generated when the PV fails to match the SP. (See the description of “Control deadband for analog points” on page 205.)

You select an alarm priority and sub-priority for the control fail alarm on the Alarms tab in Quick Builder.

Configuring alarms for standard points

Alarms are primarily used to notify operators of conditions that might call for intervention or supervisory control.

For information on how alarms work with respect to points on Experion Process Controllers, see the *Experion Process Control Building Guide*.

This topic describes how alarms for status, analog, and accumulator points work, and how to define alarms.

Alarms for standard points are specified when you configure your points in Quick Builder.

You use the Alarms tab in Quick Builder to specify which changes in a standard point's values are recorded as events, and which point events generate alarms.



Attention

The priority of alarm for system events, such as communications failures, and operator-events, Station, and printer alarms are configured using Station. See "Configuring system alarm priorities" on page 242.

About alarms and events

Experion records each significant change in the values for a point as an event, which is written to the Events file and which operators can see on the Event Summary display.

You use Quick Builder to configure:

- When a change is to be considered as significant and therefore generates an event (see "Status point alarms" on page 209, "Analog point alarms" on page 211, "Accumulator point alarms" on page 214).
- Selected point events to be treated as alarms (see "Customizing alarm behavior" on page 249).

Every time a point PV changes, the server checks to see whether an alarm should also be generated for the new value. If the server determines that an alarm condition exists, it sends an alarm to the appropriate Stations or printers, depending on how the Station has been configured (as described in "Configuring alarm settings" on page 86).

For each point in your system you can define a range of properties that are used to determine the types of conditions or events that should generate alarms and how those alarms should be prioritized.

The priority determines whether the server treats a change as an event or an alarm:

Priority	Description
Journal	The change is written to the event file, where it can be accessed for alarm and event reports, or event displays on a Station. Journal priority alarms do not appear in the Alarm Summary.
Low, High or Urgent	The change is displayed in Station's Alarm Line to bring new alarms to the attention of operators and/or directed to an alarm/event printer. It also appears in the Alarm Summary.

Within each alarm priority level, you can classify alarms as having sub-priorities between 0 and 15, where 0 represents the lowest sub-priority and 15 the highest.

Alarm priorities (and their sub-priorities) are used in determining which alarms will take precedence in the alarm line of a Station display.

You can define alarm properties for status, analog, and accumulator points, but the types of alarms and how they are used vary according to the point type.

To define conditions that generate an event or an alarm for a point:

- 1 Select the point in the Quick Builder item list.
- 2 Click the Alarms tab and complete the options on the Alarms tab.

Status point alarms

You can define the following types of alarms for a status point:

- State alarms
- Alarms on transition
- Control failure alarms
- External change alarms

When you configure alarms for status points consider the following topics:

- “State alarms for status points” on page 209.
- “Customizing alarm behavior” on page 249.
- “External change alarms for status points” on page 210.
- “Control fail alarms for status points” on page 204.
- “Configuring messages” on page 243.
- “Specifying addresses for alarm acknowledgments” on page 210.
- “Disabling alarming” on page 250.
- “Change of state events” on page 209.

State alarms for status points

Any of the PV states of a status point can be defined to be an alarm state. For example, you might define an alarm for the FAILED state of a valve so that the operator can be alerted as soon as there is a problem.

As well as defining which state(s) should generate an alarm, you can also define the priority of each alarm.

To associate a PV state with an alarm:

- 1 Select the **Enable** check box for each PV state that is to be used in generating an alarm.
- 2 For each state that is to generate an alarm, select an alarm priority from the **Priority** selection list, and specify an alarm sub-priority in the **Sub-Priority** box.

Alarm priorities and sub-priorities are described in “Customizing alarm behavior” on page 249.

Change of state events

You can also configure events to be generated if the PV of a status point changes from one state to another. To do this ensure that alarms are enabled for the point and all alarm states are disabled.

Return-to-Normal alarms for status points

For status points configured with multiple alarm states and re-alarm on state transition, when the point moves between alarm states, the previous alarm is set to return-to-normal.

If it is appropriate for your system, you can prevent the alarms from being set to return-to-normal when the point moves between alarm states. In this case the alarms are only set to return-to-normal when the point changes to a non-alarm state.

To prevent the alarms from being set to return-to-normal on alarm state transition:

- 1 Call up the Point Processing tab on the Alarm and Point Processing tab.
- 2 Select **Alarm return-to-normal only on non-alarm states**.

External change alarms for status points

An external change is a change in the value of a parameter that is not caused directly by an operator control issued through the server. An alarm is issued when the value referenced by the parameter is changed in the field device.

For status points, you can enable alarms for external changes in PV, OP and MD.



Attention

The external change alarm setting applies only to the parameter being directly controlled. For example:

- Point1 and Point2 are built with their OPs viewing the same field location and with external change alarms enabled on their OPs. An operator control to the OP of Point1 is an external change to the OP of Point2, so Point2 issues an external change alarm.
 - Point3 is built with its PV and OP viewing the same field location and with external change alarms enabled for the PV. An operator control to the OP is an external change to the PV, so the point issues an external change alarm.
-

Specifying addresses for alarm acknowledgments

For status points, you can use Quick Builder to specify an address (for example, in a controller) to which the alarm acknowledgment can be written.

The address is shown on the Alarms tab of the Status Point Detail display, in the Controller Destination Address box.

You might use this feature, for example, if the controller on which this point is built cannot continue normal functioning until the alarm state is acknowledged. For further details, see Quick Builder's help.

Analog point alarms

When you configure alarms for analog points consider the following:

- “PV limit alarms for analog points” on page 211.
- “Alarm deadband for analog points” on page 212.
- “External change alarms for analog points” on page 212.
- “Unreasonable low and unreasonable high alarms for analog points” on page 212.
- “Control fail alarms for analog points” on page 206.
- “Configuring messages” on page 243.
- “Customizing alarm behavior” on page 249.
- “Disabling alarming” on page 250.

PV limit alarms for analog points

You can configure up to eight alarms for each analog point to indicate when the PV goes beyond the limit you specify. You can also define the same types of alarms for accumulator points.

The types of PV limit alarms for analog points are:

- PV High
- PV High High
- PV Low
- PV Low Low
- Deviation High and Deviation Low (Note that Deviation Low must be a negative value, for example, -5.)
- Rate Of Change
- Transmitter Low
- Transmitter High



Attention

When a point is off scan you can manually change the PV. However:

- You cannot set a value that is higher than the PV High limit.
- You cannot set a value that is lower than the PV Low limit.

As a result, you cannot enter a PV value outside of the alarm limits that would cause an alarm.

See Quick Builder's help for descriptions of these alarm types.

For each alarm, you can also specify the alarm priority, sub-priority and the specific limit. Alarm priorities and sub-priorities are described in "Customizing alarm behavior" on page 249. Alarm limits are described below.

Unreasonable low and unreasonable high alarms for analog points

In addition to the previous alarm types, you can also configure a pair of alarms for an unreasonable high value and an unreasonable low value for the PV of an analog point. This one pair of alarms apply to all the analog points in the server.

Unreasonable low and unreasonable high alarms appear as RSLO and RSHI alarms in the Alarm Summary.

To define these alarms you define the:

- Unreasonable high and unreasonable low limit values (Point Processing tab of the Alarm & Point Processing display). The default values are 110% and -10%.
- Alarm priority and sub-priority for unreasonable values for each point (Analog Point Alarms tab) when you build the point.

Alarm deadband for analog points

When defining your analog point in Quick Builder you can specify an alarm deadband so that an analog value that is oscillating around an alarm limit will not generate unwanted alarms.

To define a deadband, select a percentage value from the **Alarm Deadband** list.

External change alarms for analog points

An external change is a change in the value of a parameter that is not caused directly by an operator control issued through the server. An alarm is issued when the value referenced by the parameter is changed in the field device.

For analog points, you can configure alarms for external changes in PV, OP, MD, and SP.

User alarms for analog points

If you have applications such as OPC Integrator, or if you use server scripting, you can generate additional alarms for your analog points. Analog points have parameters InUserAlarm1, InUserAlarm2, InUserAlarm3, InUserAlarm4 which are used to generate alarms.

When the InUserAlarm parameter value is set to 1, an alarm is generated. The default priority of the user alarm is urgent.

The default alarm condition text that appears in the alarm summary is User1. To change the condition text, you change acronyms 143 to 146 as shown in the following table:

Parameter	Acronym	Default value
InUserAlarm1	143	User1
InUserAlarm2	144	User2
InUserAlarm3	145	User3
InUserAlarm4	146	User4

Accumulator point alarms

When you configure alarms for analog points consider the following:

- “Accumulator point alarm types” on page 214.
- “Accumulator point alarm types” on page 214.
- “Customizing alarm behavior” on page 249.
- “Disabling alarming” on page 250.

Accumulator point alarm types

For each accumulator point you can define up to four alarms for indicating when the PV has gone beyond certain limits.

You can choose from three alarm types for an accumulator point when defining an alarm to indicate when the PV has gone beyond certain limits:

Property	Description
Rate Of Change	The rate of change of the PV, in engineering units per second, exceeds the limit.
PV High	The PV rises above the PV High limit.
PV High High	The PV rises above the PV High High limit (which must be greater than the PV High limit).

For each alarm, you can also specify the alarm priority, sub-priority, and the specific limit. Alarm priorities and sub-priorities are described in “Customizing alarm behavior” on page 249. Alarm limits are described below.

Alarm limit

You use the **Limit** option for each alarm type to specify the value (in engineering units) at which the alarm should be generated.

History collection and archiving

Experion can be configured to store the values of points at predetermined intervals to create a history of process values. This process is known as history collection and archiving.

This historical information can then be called up on a Station Trend display so that operators can monitor the trends in the processes represented by those points.



Attention

You might also want to use the event archiving option for event collection, storage, and retrieval. For information about the event archiving system, see “Configuring Event Archiving” on page 629.

You can use Station to configure history collection for points. For details, see “Viewing history collection configuration” on page 218.

You use Quick Builder to define history collection for status, analog, or accumulator points on other types of controllers. You use Control Builder to define history collection for process points.

When configuring history collection and archiving for a point you need to know about:

- Types of history collection
- History file sizes
- Gating points, parameters and states
- Viewing history collection configuration
- History archiving

Types of history collection

When you configure a point to store historical values, the server scans the point parameters at pre-determined intervals according to the following choices for history collection:

- Standard
- Extended
- Fast

To define the type of history to be collected for a point, select one or more history collection type check boxes for the parameters defined for a point. The choices are described below.

Standard history

When you configure Standard History collection for a point, the following snapshots and averages are stored:

- 1-minute snapshots
- 6-minute averages of the 1-minute snapshots
- 1-hour averages of the 1-minute snapshots
- 8-hour averages of the 1-minute snapshots
- 24-hour averages of the 1-minute snapshots

The averages are calculated using the 1-minute base interval. That is, 6-minute averages are calculated on six 1-minute values. If you change the 1-minute base interval the averages are still calculated from the base interval. For example, if you change the base interval to 30 seconds, 6-minute averages are calculated on twelve 30-second values.

Extended history

When you configure Extended History collection for a point, the following process history snapshots are stored:

- 1-hour snapshots
- 8-hour snapshots
- 24-hour snapshots

Fast history

When you configure Fast History collection for a point, snapshots are stored at a period between 1 and 30 seconds, depending on what you selected during installation.

History file sizes

The duration and the number of samples for each history interval are shown in the table below.

Table 5 Default history file sizes

History Types		Intervals	File Sizes	
			Duration	Number of Samples
Standard History	1	1-minute snapshot	24 hours	1442
	2	6-minute average	7 days	1682
	3	1-hour average	7 days	170

Table 5 Default history file sizes (*continued*)

History Types		Intervals	File Sizes	
			Duration	Number of Samples
	4	8-hour average	3 months	281
	5	24-hour average	1 year	368
Fast History	6	1 to 30-second snapshot	2 hours - 72 hours	8652
Extended History	7	1-hour snapshot	7 days	170
	8	8-hour snapshot	3 months	281
	9	24-hour snapshot	1 year	368

Gating points, parameters and states

To avoid collecting inaccurate historical data (for example, a zero error on a flow transmitter when the associated valve is closed or the pump off), you can define the conditions under which data should be collected.

To define a gating point:

- 1 Select a gating point from the list of points.
- 2 Select a parameter from the list of parameters.
- 3 Specify the state for that gating point in the **State** box.

For example, for a point monitoring a flow, you would probably only want to collect history when the pump is running. In this case you would define:

- The gating point as the point ID of the point that monitors the pump
- The state of the gating point as ON (or whichever wording you have configured for that state of the PV)



Attention

A history sample is still collected regardless of the gating state. When the gate point is not in the gate state, the history samples for the point are saved as “bad values” or “0.0”. Use “bad values” if you want these periods to be excluded from subsequent average calculations. Use “0.0” if you want average calculations to include all history values.

Viewing history collection configuration

To view the points configured for history collection choose **Configure > History > History Assignment** to call up the History Collection displays.

You can also use these displays to add points and parameters for history collection.



Attention

Changes to history collection that are made using the History Collection displays are not reflected in the point definitions in Quick Builder or Control Builder unless the point definition is uploaded to Quick Builder or uploaded to Control Builder. Consequently if you download points from Quick Builder or Control Builder, changes to history collection that have not been uploaded are overwritten.

History archiving

The number of samples that can be stored, and the number of points that can be assigned to have history collected for them, depend on database sizing.

When the number of samples stored equals the maximum number that can be stored, the oldest history sample is discarded in order to store a new sample. (For details about database sizing, see the *Installation Guide*.)

If you need to keep point history data for future use, you can archive the online history files. When you archive online history files, the history files for the nominated history intervals are copied to a default folder on the hard disk of the server.

When you configure history archives you need to know about:

- Specifying folders for history archives
- Determining space requirements for a history archive
- Moving history archives

To learn how to configure history archives, see “Configuring history archives” on page 220.

Specifying folders for history archives

During installation you specified the default folder for saving history archives and the default folder for restoring history archives. These folders are also the default starting point for history archive searches.

You can specify additional history archive folders for use in archive searches. The additional folders are automatically included in history archive searches, or you can specify one as the starting point of a search.

Considerations

- Because archive searches scan all subfolders under an additional history restore search path, you should not specify the root folder of the server hard disk as a history archive folder. If you do, the search will scan the entire hard disk before it returns any information.

To change the default history archive folder:

- 1 Open the Experion Server Configuration Panel.
- 2 Click **Edit**.
- 3 For the History archive directory, click **Browse**.
- 4 Locate the new archive folder and click **OK**.
- 5 Click **OK** to close the Configuration Panel.

To specify additional history restore search paths:

- 1 Open the Experion Server Configuration panel.
- 2 Click **Edit**.
- 3 For the Additional history restore search paths, type in any additional paths, separating them with semi-colons.
- 4 Click **OK** to close the Configuration Panel.

Each history archive is created in a new subfolder under the default history archive folder, or the folder specified in its configuration. The files in an archive folder should not be changed.

The name of each history archive subfolder indicates when the archive was made. The name format is:

ayYYYYmMMdDDhHHmNNtTT

Where	Is...
YYYY	The year that the archive was made.
MM	The month that the archive was made (for example, 01 for January, 02 for February, and so on).
DD	The day that the archive was made (for example, 03 for the 3rd day of the month, and so on).
HH	The hour that the archive was made (for example, 13 for 1 pm).
NN	The minute the archive was made.
TT	The history type. (See “Default history file sizes” on page 216.)

Determining space requirements for a history archive

To calculate the space required for a history archive, add up the space requirements for each history interval to be included in the archive.

To calculate the disk space required for a history interval, you need to know:

- The maximum number of point parameters (P) that can be collected for that interval.
- The maximum number of samples (N) that can be collected for the interval.
The maximum number of point parameters and samples is determined by the server database size. For details, see “Default history file sizes” on page 216.

Use the following formula to calculate disk space in bytes:

$$\text{Space (bytes)} = (P + 2) * (N + 2) * 4$$

Example

If 1-minute history can store samples for 24 hours for 2000 point parameters, the size of the history file would be:

$$(2000 + 2) * (1442 + 2) * 4 = 11,563,552 \text{ bytes (11 MB)}$$

Configuring history archives

History archives are created using the History Archiving display. History Archives created using the History Archive report are supported for backward compatibility.

The History Archiving display allows you to:

- Enable history archiving for each history type
- Check the time of the last archive
- Force an archive to be run

To configure history archives:

- 1 From the System Configuration Menu display, click **History Archiving**.
- 2 Using the check boxes under **History Types to Archive**, select the history types you want to archive. (See “Types of history collection” on page 215 for a detailed description of history types.)
- 3 Enter the minimum free disk space that must be available for this archiving job to run. This prevents all of the free disk space on the server from being used for history archive files. (If the disk becomes full, system performance will be severely degraded.)

Moving history archives

You can move history archives from the default history archive folder. You want to do this to prevent the minimum free disk space value being reached and causing history archiving to stop.

Considerations

- Moving history archives has implications for trends. If a trend requires data from an archive that has been moved, you need to restore the archive. (The archive should be restored to the restored archives folder, c:\Program Files\Honeywell\Experion PKS\server\RestoredArchives, or the folder you specified during installation. Do not restore archives to the default history archive folder.)
- As an alternative to restoring moved history archives you can add a path to the new location of the archives using the Experion Server Configuration Panel. However, specifying a network path to access archives that no longer exist or cannot be found can affect system performance when viewing trends.

To automatically remove history archives:

- 1 On the History Archiving display, select the required archive management option for each history type. The options you can select are Retain, Move, or Delete.
- 2 If you select Move or Delete, specify the number of days until the archive is moved or deleted. If you specify 0 the archives are not moved or deleted.
- 3 If you select Move, specify the location to which the archives are to be moved.

Configuring Station displays for points

As part of points configuration you can:

- Associate a display with each point (see “Associated displays” on page 222)
- Group related points to form:
 - Groups
 - Trends (see “Groups and trends” on page 222)

For any point in your system, you can also specify:

- A user-defined Point Detail display, instead of the standard Point Detail display (see “User-defined point detail displays” on page 223)
- A user-defined Group Faceplate Template display, instead of the standard Group Faceplate Template display (see “Group faceplate templates” on page 223)

Associated displays

If you define an associated display for a point, operators can select a point (for example, on a custom display or in the Alarm Summary) and call up the Associated display (by pressing F2 or clicking the associated display button on the toolbar); the display that has been defined as the associated display for that point is then called up.

You can define an associated display for a point by using the following methods:

- Using Quick Builder or Control Builder to specify the associated display
- Using the Point Detail display on Station to specify the associated display. For information on calling up Point Detail displays, see “Changing point configuration via Station displays” on page 225.

Groups and trends

You can configure up to 16000 groups and up to 3000 trends.

Groups enable users to view the current operating data (or configuration data) for up to eight points of any type on a single group display.

Trends enable users to view trend information for up to eight point parameters. For examples of group and trend displays, see “Configuring group and trend displays” on page 361.

You can use Quick Builder or Control Builder to configure points to form groups or trends. You can also use Station displays, as described in “Configuring group and trend displays” on page 361. If you assign a point to a group or trend in Station, this is not reflected in the point definitions in Quick Builder or Control Builder unless the point definition is uploaded to Quick Builder or uploaded to Control Builder. Consequently if you download points from Quick Builder or Control Builder, changes to trends and groups that have not been uploaded are overwritten.

**Attention**

When you use Quick Builder to configure groups and trends, you can only assign a point to one group and one trend. When you use Station to configure groups and trends, you can assign a point to as many groups or trends as you want.

If you assign a point to more than one group or trend on Station, and then upload your configuration data from the server to Quick Builder, this information about the multiple groups and trends will not be present in Quick Builder because Quick Builder can only handle a single group and a single trend per point.

User-defined point detail displays

You are supplied with a set of pre-defined displays that are used to show point detail data.

You can create custom Point Detail displays using Display Builder and then use Quick Builder to specify the custom Point Detail display for particular points.

Group faceplate templates

You are supplied with a set of pre-defined “faceplates” or templates that are used for status, analog, or accumulator points in a Group Detail display.

For example, the following figure shows a Group Detail display for a group consisting of various types of points using the standard faceplates for the point type.

Figure 15 Group display



You can create custom Group Faceplate Template displays using Display Builder and then specify the template for particular points when you build the point.

Changing point configuration via Station displays

After a point definition has been loaded to the server database, you can use the Point Detail display on Station to view configuration details for the point.

You can also use a Point Detail display to change point configuration information, but you must be using Station at a security level of SUPV or higher.

Most point configuration information can be changed in Point Detail display however there are various items of data that can only be changed from within Quick Builder or Control Builder and downloaded to the server database.



Attention

When you use a Point Detail display to change the point configuration data in the server database, the configuration data in the Quick Builder project file or the Control Builder project file will no longer match the server database.

It is good practice to keep the Quick Builder and Control Builder data synchronized with the server data by using the upload function to upload point data from the server database to the Quick Builder and the Control Builder project file databases.

Calling up a point detail display

To call up a Point Detail display in Station, in the command zone on any Station display, type the point ID, then select the Detail button on the tool bar, or press F12.

Advanced point configuration

This section is only applicable to standard points.

The configuration tasks described in this topic relate to functions that are not essential to implement for the successful running of your system, but rather allow you to take advantage of some advanced features of point configuration.

The following topics discuss:

- Defining points to represent an address in the database, rather than an address in a controller (see Database addresses)
- Using auxiliary parameters (see Using auxiliary parameters)
- Building points off-scan (see Building points off-scan)
- Creating user-defined data formats (see Creating user-defined data formats)
- Using point internal reference numbers (see Understanding internal point numbers)



Attention

To check the scanning performance of your system, see the *Troubleshooting Guide*.

Database addresses

You can configure points to access addresses in the database, rather than addresses in controllers. Such points are sometimes known as “derived points” or “database points”, but they have the characteristics of the type of fixed point they are accessing.

The database addresses can be either point parameters or user files. For details about user files, see the *Application Development Guide*.

To configure a “derived point”, you specify that the address type for its PV Source Address is “Point”.

For the syntax for accessing a database address for a point parameter see “About derived points” on page 168 and the chapter on configuring points in *Quick Builder*.

When a source address is configured for a database type address, an equivalent destination address is automatically defined. Destination addresses cannot be explicitly configured for database addresses.

Internal point parameters

Apart from the standard point parameters (described in “Standard point parameters” on page 173) there is a range of other parameters to store internal information for the point. Examples of these types of parameters are alarm limits and ranges for an analog point.

Whenever an item of information in a point needs to be referenced in another part of the server (for example, when building custom displays), you identify that item by specifying the point ID and the parameter name. For details of the internal point parameters available, see “Summary of internal parameters” on page 186.

Using auxiliary parameters

For an analog point you can define up to four auxiliary parameters for general purpose use. For example, you might want to define auxiliary parameters to represent the proportional, integral, and derivative parameters of a PID loop. Auxiliary parameters can also be used for tracking and modifying alarm limits that are held in a controller.



Attention

Auxiliary parameters are disk-resident and therefore should not be configured for scan rates faster than 60 seconds. (For more information about scanning rates, see “Scanning and standard points” on page 196).

For each auxiliary parameter, you can configure:

Property	See:
Source Address	“Source and destination addresses” on page 195.
Destination Address	“Source and destination addresses” on page 195.
Scan Period	“Scanning and standard points” on page 196.

Using auxiliary parameters to track controller alarm limits

If you set the auxiliary parameter name to match the name of an internal point parameter, then the internal point parameter’s value will track the value in the controller at the auxiliary parameter’s source/destination address. If the internal point parameter value is changed, the value will also be written to the auxiliary parameter’s destination address.

This is especially useful for keeping alarm limits in a controller synchronized with point alarm limits. For example, if a name of AlarmLimit1 was given to an auxiliary parameter, then the first alarm limit for the point would follow the controller value addressed by the auxiliary parameter.

Building points off-scan

If you are adding points, and you do not want point processing (such as algorithm or alarm processing) while you are implementing your system, you can build your points “off-scan” by ensuring that the **Scanning Enabled** check box is cleared as you define them with Quick Builder.

After completing your points configuration, you can call up the Point Detail display for each point on Station (as described in “Changing point configuration via Station displays” on page 225), and use the **Scanning and control enabled** check box under **Services** to enable scanning and control for that point.

Creating user-defined data formats

Data formats convert field values into values that are more useful for operators and other applications.

You can create user-defined data formats for the following types of controllers:

- Allen-Bradley
- OPC Client Interface
- Modicon
- GE Fanuc Series 90
- DNP3

You can create:

- *Unscaled formats*, which converts (but does not scale) a field value before loading it into the parameter.

With an unscaled format, you need to define the scaling for each parameter that uses the format.

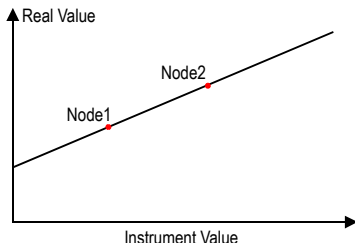
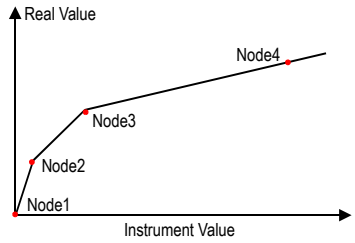
- *Scaled formats*, which converts and scales a field value before loading it into the parameter.

With a scaled format, parameters that use this format are automatically scaled.

To create a user-defined data format:

- 1 On the **System Configuration Menu** display click **User-defined Data Formats**.
- 2 Click the **Unscaled** or **Scaled** tab, as appropriate.
- 3 Click an empty data format row.
- 4 Type the name for the data format. (Do not use any name listed in “Reserved Data Format Names” on page 233.)
- 5 Type the details as appropriate.

Property	Description
Name	The unique name of the data format. A maximum of 10 alphanumeric characters (no spaces, underscores or double quotes). Do not use any name listed in “Reserved Data Format Names” on page 233.

Property	Description
Data type	The data format of the field value, which can be: • INT2 (16-bit integer). If you select this, you can specify the Start bit and Width of the field value. (By default these are 0 and 16 respectively). • INT4 (32-bit integer) • REAL4 (single-precision IEEE floating point)
Signed Value	If selected, indicates that the field value could be either negative or positive.
Minimum Maximum	Specifies the minimum and maximum field values. Type NaN if you do not want to specify a value.
Swap bytes Swap words	Specifies whether the bytes/words of the field value are swapped during conversion. Field values are assumed to be big-endian (high order byte first). For example, if a device uses big-endian storage and the field value is INT4 in two 16-bit registers with the least significant 16-bits first, you would select Swap words. If the device used little-endian storage, you would also select Swap bytes.
Type	The type of conversion, which can be either: • Linear. A conversion ratio defined by Node 1 and Node 2. Note that the nodes only define the conversion ratio, not the minimum/maximum values.  • Piecewise Linear. Approximates a conversion curve that can have up to seven nodes. 

Property	Description
Node 1 to Node 7	Each node specifies a Field value and its corresponding Converted value . For a scaled data format, the converted values must be between 0.0 and 1.0.

Example

Example 1

A device stores values in a 16-bit register in big-endian format. Additionally, the value stored ranges from 10 to 60, but you want that value represented in Expon as 0 to 1000 regardless of what the point's range is.

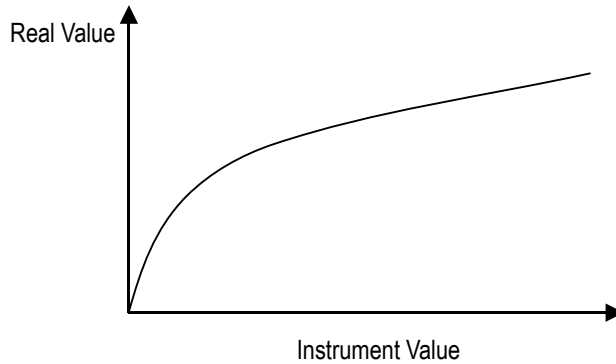
To define a format for this:

- 1 Define an unscaled data format.
- 2 In the **Field Value** section select **INT2** from **Data type**, and set the **Start bit** to 0 and **Width** to 16.
- 3 Select **Signed value**. (Do not select **Swap words** or **Swap bytes**.)
- 4 Type **NaN** in **Minimum** and **Maximum**.
- 5 In the **Conversion** section select **Linear**. Set the node values as follows.

Node	Field value	Converted value
1	10	0
2	60	1000

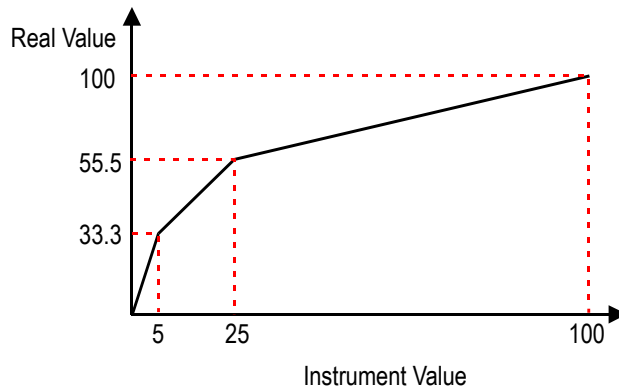
Example 2

A device stores values in two 16-bit registers in little-endian format. The value stored is an IEEE floating point number. However, the response curve of the instrument that generates the value is shown in the following figure.



To define a data format for this:

- 1 Determine the nodes you need to define to obtain the desired accuracy. In this example, you decide to define four nodes, as shown in the following figure. (The first node is at 0,0.)



- 2 Define an unscaled data format.
- 3 In the **Field Value** section select **REAL4** from **Data type**.
- 4 Select **Swap bytes**. (Do not select **Swap words**.)
- 5 Type **NaN** in **Minimum** and **Maximum**.
- 6 In the **Conversion** section select **Piecewise linear curve**.

7 Set the **Node** values as follows.

Node	Field value	Converted value
1	0	0
2	5	33.3
3	25	55.5
4	100	100
5 to 7	NaN	NaN

Reserved Data Format Names

B0	DPS6I4	HIGHWORD	LOWWORD	S8B	U32BS
B12	E3BCD	IEEEFP	LREAL	S9999	U32BSB
B12E	FENUM	IEEEFPBB	MFCFP	SCALED	U3BCD
B12ES	FS90DC	IEEEFPL	MFCTM	SLC_AI	U4095
B12S	FS90DS	IEEEFPLB	MMU	SLC_AO	U4BCD
B15	FS90PVA	LCN0	MMUS	SREAL	U6BCD
B4	FS90RDR	LCN1	MODE	T1	U8B
B7	FS90SEC	LCN10	PIUOP	T2	U8BCD
C16	FSC0TO10V	LCN2	PMXFP	TD	U999
C3BCD	FSC0TO20MA	LCN3	R32	U100	U9998
C4BCD	FSC0TO5V	LCN4	REVWD	U1023	U9999
C8BCD	FSC1TO5V	LCN5	S16B	U14B	UBCD12
D9999	FSC2TO10V	LCN6	S32B	U15B	UBCD16
DPR3V	FSC4TO20MA	LCN7	S32BB	U16B	VAXFP
DPS6DP	FTEXT	LCN8	S32BS	U32B	XLPC
DPS6FP	HALFWD	LCN9	S32BSB	U32BB	XLPRH
DPS6I2					

Understanding internal point numbers

The maximum number of flexible, status, analog, accumulator and other points you can create is determined by the size of your database.

When you download point data from Quick Builder to the server database, each point is assigned a unique *point number* in the range from 1 to 65000. These numbers are used to uniquely identify points within the server. They are internal numbers that are not displayed in Quick Builder.

When a point is deleted from the server, the internal number for that point is freed, and is available to be allocated to another point.

If you need to know which internal point numbers are currently in use, you can use the **listag** utility to list the points currently configured in the database. For details of running the **listag** utility, see “Command reference” on page 815.



Attention

All references to points in the server database use the internal point number. If you reload a point, the point will retain its internal point number. However, if you delete a point and then add the point some time later, it might be allocated a different internal point number. This means that the point is no longer available to custom displays currently being displayed, or to standard displays such as trends, that accessed it. You need to:

- Re-enter the point on standard displays (such as trends).
 - Re-load into Station any currently displayed custom displays that reference the point (from the Station menu, choose **View > Reload Page**).
-

Configuring algorithms

Algorithms perform additional point processing or initiate actions when standard point values change.



Attention

- For information about constraints on configuring algorithms in a DSA system, see “Working with algorithms” on page 512.
- You cannot configure algorithms for points on Experion Process Controllers. However, you can reference Process Controller points in algorithms that are attached to other point types.

A number of standard algorithms are available, each performing a different function. These algorithms are available for alarm processing, data analysis, value transportation, action requests, and application task requests.

Each type of algorithm has a different number. This number is specified when the algorithm is configured for a point. For example, the value transportation algorithm is algorithm number 68.

Two classes of algorithm are available:

- PV algorithms (see PV algorithms)
- Action algorithms (see Action algorithms)

PV algorithms

PV algorithms perform data gathering or data manipulation. The result of the algorithm operation is usually stored in the PV of the point to which it is attached. PV algorithms are processed whenever the raw PV changes from its previously scanned value.

For example, say you needed to determine the number of hours that a pump has been running and to store this value in a point’s PV. You could attach the “run hours” algorithm to a “dummy” analog point, gate it from the pump’s status point, which indicates whether or not the pump is running, and this would give a “run hours” reading in the analog point’s PV.

The following PV algorithms are available:

- General Arithmetic (Algo#4)
- Production (Algo#5)
- Run Hours (Algo#7)
- General Logic (Algo#10)

- Composite Alarm Processing (Algo#12)
- Integration (Algo#15)
- Cyclic Task Request (Algo#16)
- Piecewise Linearization (Algo#22)
- Maximum/Minimum (Algo#64)

Action algorithms

Action algorithms initiate some action when the PV of the point to which they are attached changes. Action algorithms are processed whenever the PV of a point changes by more than the drift deadband for the point.

For example, say you needed to run a report when a status point changes to a certain state. You could attach the Status Change Report Request algorithm to the status point, and the report would be requested when the status point changed to the nominated state.

The following action algorithms are available:

- Composite Alarm Initiation (Algo#11)
- Value Transportation (Algo#68)
- Status Change Task Request (Algo#69)
- Status Change Report Request (Algo#70)
- Queued Task Request (Algo#71)
- Status Point Notification (Algo#75)
- Analog Point Notification (Algo#76)
- Status Change Display Request (Algo#77)
- Group Control of Points (Algo#78)
- Status Change Alarm Group Inhibit (Algo#79)
- Status Change Alarm Area Inhibit (Algo#80)



Attention

If you want to configure Algo#11, consider using alarm groups and the aggregate alarming capabilities. For more information about alarm groups, see “Configuring aggregate alarming” on page 255.

Sources of information on algorithms

For information on algorithms, see:

- Quick Builder's help for each Algorithm, or
- The *Hardware and Point Build Reference*.

Algorithms #16 and #69 are also documented in the *Application Development Guide*.

Defining algorithms

To define an algorithm for a point:

- 1 Select the point item in the Quick Builder item list.
- 2 In the PV Algo box or the Action Algo box, select the type of algorithm you need to configure.
- 3 Select the PV Algo tab or the Action Algo tab and complete the options.

Quick Builder's help describes how to configure each algorithm.

Viewing algorithm configuration information

After an algorithm has been configured for a point, you can view the algorithm details at a Station via the Point Detail display.

Considerations

- When you use an Algorithm Detail display to change the point configuration data in the server database, the configuration data in the Quick Builder project file no longer matches the server database.

It is good practice to keep the Quick Builder data synchronized with the server data by using the Quick Builder upload function to upload point data from the server database to the Quick Builder project file database.

To call up the Algorithm Detail display:

- 1 Call up the Point Detail display for a point (as described in “Changing point configuration via Station displays” on page 225). The currently configured PV or Action algorithm number is under **Algorithms** at the bottom of the display.
- 2 Click the algorithm number and then press F12 or go to the **View** menu and select **Detail**. The Algorithm Detail display for the selected algorithm appears, with the algorithm block number shown in the title bar of the display.

Finding free algorithm blocks

Algorithm blocks are used to store the algorithm configuration as well as working values required by the algorithm. Algorithm blocks are part of the database.

Details of the number of blocks available can be found in the *Installation Guide*.

Algorithm blocks are generally not shared between algorithms so each algorithm attached to each point should be assigned a unique block number, unless you are using algorithms 11 and 12, which need to share common block numbers.

To find out which algorithm blocks have been used and which are free, you can run the Point Cross Reference report. This report is described in “Cross Reference reports” on page 415.

Alternatively, you can use the **alg1st** utility to list the free algorithm blocks in the database. For details of running **alg1st**, see “alg1st” on page 824.

Configuring and customizing notifications

11

This chapter describes how you can configure and customize the behavior of notifications.



Attention

For information on configuring alarms for points see “Configuring alarms for standard points” on page 207.

About notifications

Notifications alert operators of changes in the system. Some notifications require operator intervention, such as changing the value of a point parameter and acknowledging the associated alarm. Other notifications are informational only and do not require any operator action.

Notifications include point alarms, system alarms, messages and alerts.

Where do you configure notifications

The different types of notifications are configured using various tools. The following table describes where each notification is configured.

Notification type	Configured using
Standard point alarms	Quick Builder when you configure your standard points
Process point alarms	Control Builder when you configure your process points
Flexible point alarms	System interface or point server software
Standard point messages	Configuration Studio
Process point messages	Control Builder
TPS point messages	TPS configuration tool
Alerts	User Alert application and Station Control Builder when you configure your sequential control module.

Configuring system alarm priorities

You can configure the priority for the following system alarms:

- **Communications diagnostic.** An alarm of the specified priority is raised if a controller diagnostic check finds a problem. Only certain types of SCADA controllers, such as TDC, perform diagnostic checks.
- **Comms marginal.** An alarm of the specified priority is raised if the marginal barometer level specified for a SCADA channel or controller is reached.
- **Comms fail.** An alarm of the specified priority is raised if the fail barometer level for a SCADA channel or controller is reached.
- **Redundancy.** An alarm of the specified priority is raised if redundant server lose synchronization.
- **Station.** If Station failure alarms are enabled, an alarm of the specified priority is raised when communication to the Station is lost.
- **Operator logon.** An alarm of the specified priority is raised when an operator attempt to log on has failed.
- **Operator lockout.** An alarm of the specified priority is raised when an operator exceeds the specified number of logon attempts.
- **Printer fail.** An alarm of the specified priority is raised when Windows print queue cannot be located.
- **Printer marginal.** An alarm of the specified priority is raised when an error is received from the Windows printer.

Configuring messages

Messages can be generated to provide additional information to an operator, for example when a point goes into alarm, a message can provide an explanatory note or a procedure.

There are four types of messages:

- Informational
- Confirmable (available if you have Process Controllers or a TPS system)
- Single signature (available if you have Process Controllers)
- Double signature (available if you have Process Controllers)

Informational messages are defined in:

- Station if you have standard points and are associated with a point.
- Control Builder if you have process points.
- TPS if you have a TPS system.

Single signature and double signature messages are configured in Control Builder. Confirmable messages are configured in Control Builder or TPS.

For status, analog, and accumulator points you can specify a predefined message to be displayed in the Message Summary when the point goes into alarm.

Each Station displays the message text defined on its local server. If you have a DSA system, the message indexes and text should be the same on all servers to ensure that appropriate messages are displayed for remote points.

To define an informational message:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm and Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Messages** tab.
- 4 In an empty line, type the message text.
- 5 Note the line number. This is the number you specify as the message index for your point.

Enabling automatic message acknowledgement for confirmable messages

If your system has an IKB or OEP keyboard and you have confirmable messages, you can configure your system such that when an operator selects a confirmable message and presses the MSG CNFM button (message confirm), the message is acknowledged and confirmed at the same time.

To enable automatic message acknowledgement for confirmable messages:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm and Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Processing** tab.
- 4 Select the **Perform Auto Acknowledge when Confirm Message key pressed (IKB only)** option.

Configuring alerts

There are several types of alerts:

- Interactive Instruction alerts
- User-generated alerts
- System-generated alerts

Interactive Instruction alerts indicate to the operator that there are tasks that they must complete so that a sequential control module can continue executing. These types of alerts are configured when the sequential control module is configured. For more information on sequential control modules and alerts, see the *Sequential Control User's Guide*.

A user-generated alert could be a reminder to an operator to schedule maintenance for a piece of equipment.

A system-generated alert is a notification of an abnormal condition in the system that could cause problems if the condition is not fixed. However, the priority of the condition is not high enough to be an alarm.

For example, the gas pressure in Pipe A has been rising steadily over the last couple of days, most probably due a build-up of waste particles on the inner lining. This is leading to a degradation in process performance. An alert is raised to indicate that pipe cleaning must take place in the next week.

User-generated alerts and system-generated alerts are configured by the user alert application. The user alert application exists in a Unified Real Time environment (URT).

The steps required to incorporate user-generated and system-generated alerts into Experion are:

Task	See	Done
Install and set up the URT environment	URT documentation	
Install the User Alert Server.	User alert documentation	
Identify which conditions will trigger an alert using User Alert application.	URT documentation	
Install the User Alert Explorer on Experion Stations.	URT documentation	
Configure a URT connection between Experion and the User Alert application.	page 246	
Map URT areas to Experion assets.	page 246	

Connecting Experion and the User Alert application

User-generated alerts and system-generated alerts are incorporated into Experion from the User Alert application using a URT connection.

To configure the connection:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure system interfaces** task to call up the System Interfaces display.
- 3 In an empty row select **URT** from Type and click **URT** in the Alias column to call up the System Interface configuration displays.
- 4 Under Notification Sources, in the **Network Name** box, type the name of the computer where the URT and user alert application are installed.
- 5 In the **ServerProgID** list, ensure that `Hci.URTOpcServer` is selected.
- 6 Click the **Asset Mapping** tab and specify how the OPC areas are mapped to Experion assets.

Configuring external alarm notification

You can specify up to four standard points to receive alarm notifications and control an external device, such as a siren, that attracts attention even if no one is logged into a Station.

Notifications are issued according to the priority of the alarm. You can specify an external alarm notification point ID and parameter for Low, High, Urgent, and Any priority alarms.

When external alarm notification is enabled, the specified point parameter is controlled to:

- 1, when an alarm occurs
- 0, when an alarm is acknowledged or returns to normal

You cannot specify active times or re-alarm times for external alarm notifications, as you can for Stations audible alarms.

To configure external alarm notification:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm & Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Processing tab**.
- 4 Under External Alarm Notification, select the appropriate alarm priority check box.
- 5 For each alarm priority you have selected, enter the name of the point and the parameter for which you want to raise an external alarm.

To enable or disable external alarm notification for any of the four priority choices, select or clear the appropriate check box.

Configuring unanswered alarms

You can configure Experion to raise a further alarm if an existing alarm is not acknowledged within a specified time. This type of alarm is called an unanswered alarm.

To configure unanswered alarms:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm & Point Processing display appears in the System Display tab in Configuration Studio.
- 3 On the Alarm and Point Processing display click the **Alarm Processing** tab.
- 4 Select the **Unanswered alarms enabled** check box.
- 5 Specify the asset for which the unanswered alarm is to be raised.
- 6 In the **Alarm Acknowledgement period** box, specify the time in minutes that an alarm can remain unacknowledged before an unanswered alarm is raised.

Customizing alarm behavior

Elevating the alarm priority

You can specify a change in alarm priority for alarms that are unacknowledged for a configured amount of time.

To elevate the alarm priority:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm & Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Priorities** tab.
- 4 Select the **Alarm Priority Elevation enabled** check box.
- 5 In the **Low to High** box specify the time period after which unacknowledged low priority alarms are elevated to high priority.
- 6 In the **High to Urgent** box specify the time period after which unacknowledged high priority alarms are elevated to urgent priority.

About the precedence of alarms in the alarm line

In Station, one alarm appears in the alarm line. The alarm that appears in the alarm line is determined as follows:

- 1 Unacknowledged
- 2 Highest priority
- 3 Highest sub-priority
- 4 Newest/oldest. The default setting is newest, but you can set your preference on the System Wide Configuration display.
- 5 The order in which they appear on the alarm summary

For example, with the alarm precedence set to newest, and the following alarms having occurred:

10:18 unacknowledged, urgent, sub-priority 13
 10:19 unacknowledged, urgent, sub-priority 13
 10:20 unacknowledged, urgent, sub-priority 11
 10:30 unacknowledged, low, sub-priority 15
 10:30 unacknowledged, low, sub-priority 12
 10:31 acknowledged, urgent, sub-priority 15

The alarm that is shown in the alarm line is:

10:19 unacknowledged, urgent, sub-priority 13

Disabling alarming

You might need to temporarily disable alarming in the following circumstances:

- When you are building your system
- When equipment needs to be repaired or replaced

For example, if you need to temporarily disable alarming on a set of points when a status point changes to a nominated state, you can use the Status Change Alarm Group Inhibit algorithm (#79) or the Status Change Alarm Area Inhibit algorithm (#80). The configuration of algorithms is described in “Configuring algorithms” on page 235.

You can also enable or disable alarms:

- Server-wide using the Alarm and Point Processing display. (By default, **Alarms enabled server-wide** is selected.)
- For assets by using the Enable Alarms display.
- For individual points using the Point Detail display.

When you are configuring a standard point, you can disable its alarms in Quick Builder (see “Configuring alarms for standard points” on page 207).

To disable alarms server-wide:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
 The Alarm & Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Processing** tab.
- 4 Clear the **Alarms enabled server-wide** check box.

To disable alarms for a particular asset:

- 1 Call up the **Alarm Enable/Disable** display.
- 2 Clear the check box for the required asset.

To disable alarms for individual points:

- 1 Call up the Point Detail display for the point.
- 2 In the **Services** group, deselect **Alarms Enabled**.

Customizing alarm behavior for Process alarms

If you have Process controllers and Process points, by default, alarms are enabled at the block level. If a block goes into alarm, other blocks in the same control module do not automatically go into alarm at the same time.

You can change this behavior so that alarms are enabled at the module level.

To enable alarms at the module level:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm & Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Processing tab**.
- 4 Clear the **Maintain alarm state for each Control Module Function Block** check box.

Alarm Summary overflow

The Alarm Summary and the Alert Summary have a combined limit of 2000 alarms and alerts. When this limit is reached, an algorithm is run which replaces alerts or particular alarms.

The algorithm searches for any alerts and replaces alerts before replacing alarms. The oldest alert is replaced with the new alert or alarm.

If no alerts are found, the algorithm searches for an alarm that is similar to the alarm being added. A similar alarm must be of equal or lower effective priority. If a similar alarm is found, it is replaced with the new alarm. An alarm is considered similar if the associated asset, condition, point, and parameter are the same. The effective priority is a combination of the priority, sub-priority, and additional alarm state information such as whether the alarm has been acknowledged. An

existing alarm of urgent priority that has been acknowledged or has returned to normal has a lower effective priority than a new alarm that has low priority.

If a similar alarm is not found, the algorithm searches for the oldest alarm of equal or lower effective priority. If found, the oldest alarm of equal or lower effective priority is replaced with the new alarm.

If there is no older alarm of equal or lower effective priority, then the oldest alarm in the summary is replaced with the new alarm.

Configuring page acknowledgement

If you have an IKB or OEP keyboard, you can configure your system such that an operator can acknowledge all alarms on a display, without any items selected, by pressing the acknowledge button (ACK) on the keyboard or using the Acknowledge toolbar button. The page acknowledgement behavior is applicable to system displays and custom displays.

Considerations

- Page acknowledgement may take one to two minutes to complete in situations where the Alarm Summary consists mainly of alarms for points on SCADA devices that are configured to have alarm acknowledgement registered on the controller using the Ack Destin setting.

To configure page acknowledgement:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm & Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Processing** tab.
- 4 Select the **Perform Page Acknowledge when no items selected (IKB only)** option.

Customizing alarm colors

Experion has predefined colors for alarms in the alarm summary, the status line indicators, off-scan points. If these colors are not suitable for your site, you can customize these colors.

To customize alarm colors:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm colors** task.
The Alarm Colors tab of the Server Wide Station Settings display appears in the System Display tab in Configuration Studio.
- 3 Under Alarm Colors select the appropriate color for each alarm priority you want to change.
- 4 Select **Use these colors for points on displays** if you want the custom alarm colors to be used on your displays for data objects that also display their alarm status.

To customize status line indicator colors:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm colors** task.
The Alarm Colors tab of the Server Wide Station Settings display appears in the System Display tab in Configuration Studio.
- 3 Under Status Line Indicator Colors select the appropriate color for each indicator you want to change.

To customize the color of points off-scan:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm colors** task.
The Alarm Colors tab of the Server Wide Station Settings display appears in the System Display tab in Configuration Studio.
- 3 Under Point State Colors select the appropriate color.

To customize the color of points bad state:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm colors** task.
The Alarm Colors tab of the Server Wide Station Settings display appears in the System Display tab in Configuration Studio.
- 3 Under Point State Colors select the appropriate color.

To customize the color of points NaN:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm colors** task.
The Alarm Colors tab of the Server Wide Station Settings display appears in the System Display tab in Configuration Studio.
- 3 Under Point State Colors select the appropriate color.

Configuring aggregate alarming

12

This chapter describes aggregate alarming and alarm groups.

About aggregate alarming and alarm groups

Custom operating displays are often organized hierarchically to provide an overview of the process being monitored and controlled. Aggregate alarming and alarm groups enhance this display hierarchy by enabling you to group your points into alarm groups and add aggregated alarm counts from the alarm groups to your displays so that operators can see alarms in particular parts of the plant at a glance.

The asset model also makes use of aggregate alarming. The asset tree in the location pane on the Alarm Summary contains aggregated alarm counts for each asset that contains a point that is in alarm. There is no configuration required to make use of aggregate alarming for assets.

Alarm groups provide an alternative way of viewing assets and alarms associated with assets. By using alarm groups, you can create a group of assets and points that are otherwise unrelated to one another in the asset model. For example, you may be interested in all mechanically agitated tanks in the plant for the purposes of monitoring agitator-related alarms across the entire plant.

The set of alarm groups defined in your system effectively forms an alarm group model, which is distinct from the asset model.

The benefits of using alarm groups are:

- Additional filtering capabilities on the Alarm Summary.
- Aggregated alarm counts for alarm groups. The alarm counts of all the points within the alarm group are aggregated.
- Aggregate alarming parameters which you can add to custom displays so you can see the number of alarms in each section of the plant at a glance.

The visibility of alarm groups within the Alarm Summary can be controlled by asset assignment if you associate an alarm group with an asset. If the asset is within the operator's (or Station's) scope of responsibility, then the alarm group is visible to the operator.

Alternatively, if you do not associate alarm groups with assets, you can make alarm groups visible in the Alarm Summary by assigning the alarm group model to an operator or Station.

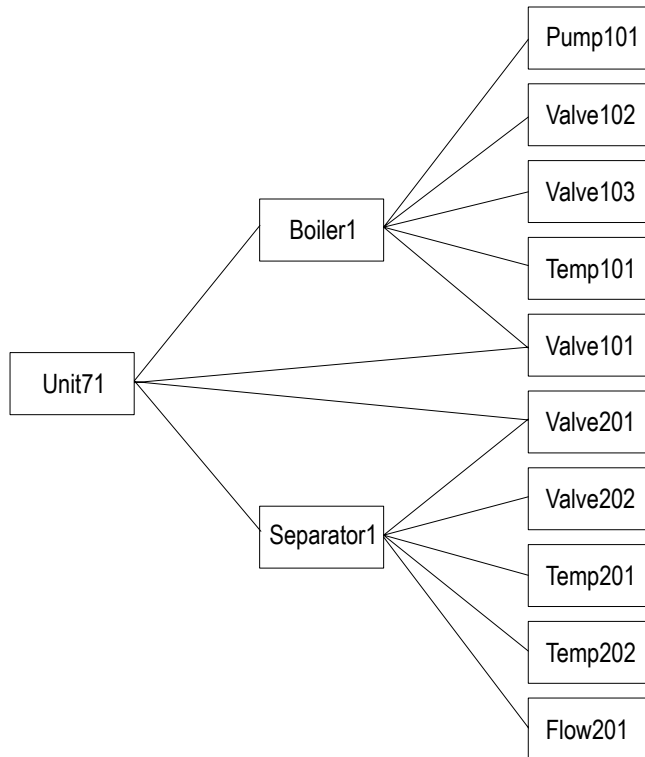
The aggregated alarm count for an alarm group that is visible to a particular operator or Station is determined by the scope of responsibility of the operator or Station. If an alarm group contains a point that belongs to an asset that has not been assigned to the operator or Station viewing the alarm group, then the alarms for this point are not included in the aggregated alarm count for the alarm group.

You create alarm groups using Configuration Studio. For instructions on creating an alarm group, see the following topic in Knowledge Builder:

Experion R300 > Configuration > Enterprise Model Builder User's Guide > Creating and configuring alarm groups.

The following figure shows an example alarm group model. `Unit71` is an alarm group which contains alarm groups `Boiler1` and `Separator1` and points `Valve101` and `Valve201`. `Boiler1` contains the points `Pump101`, `Valve102`, `Valve103`, `Temp101`, and `Valve101`. `Separator1` contains the points `Valve201`, `Valve202`, `Temp201`, `Temp202`, and `Flow201`.

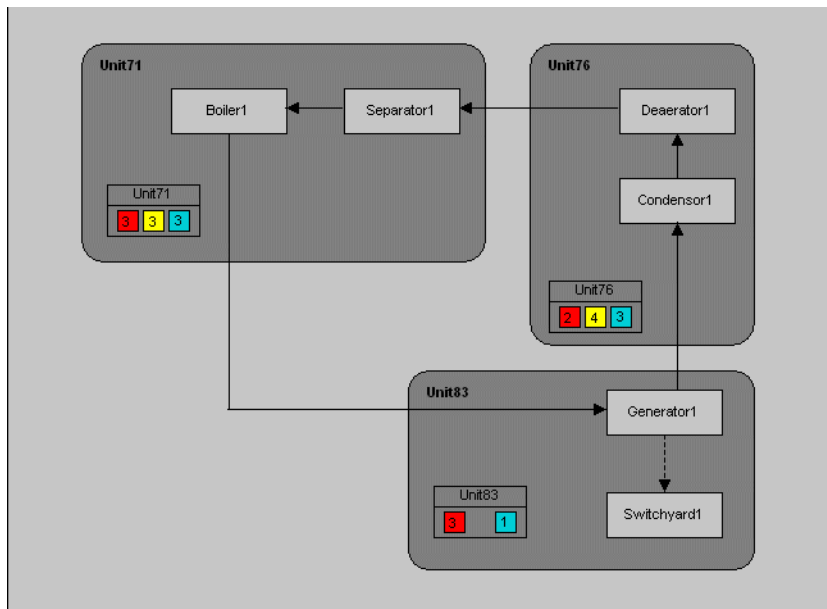
Points `Valve101` and `Valve201` are included in two alarm groups however alarms for these points are counted only once in the aggregate alarm parameters for alarm group `Unit71`.



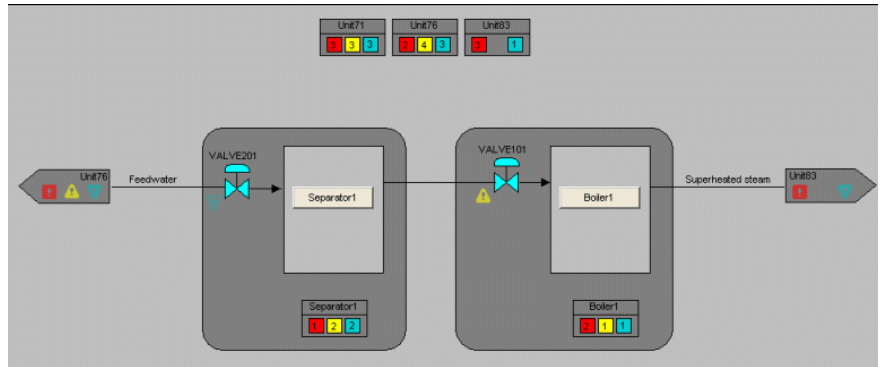
Adding aggregated alarm information to custom displays

You can add aggregated alarm information for your alarm groups to custom displays and create a hierarchy of displays that reflect the structure of your alarm groups. The “higher level” display can provide aggregated alarm counts for the points within the alarm group. Operators can then “drill down” the display hierarchy to find more detail about current alarms.

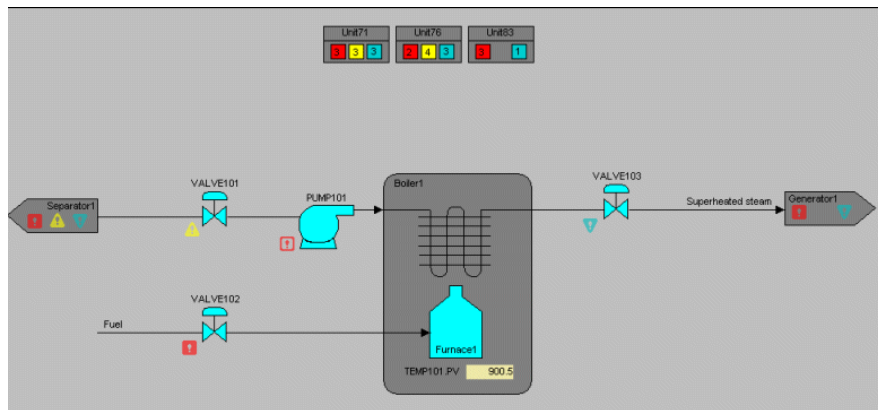
The following figure shows a custom display which incorporates aggregated alarm information for alarm groups Unit71, Unit76, and Unit83.



An operator notices that Unit71 is in alarm. The operator clicks the Unit71 display object which calls up a more detailed custom display of Unit71.



From this more detailed custom display, the operator can see that the alarm group Boiler1 has several alarms. The operator clicks the Boiler1 display object which calls up a custom display for Boiler1.



From this custom display for Boiler1, the operator can see which particular piece of equipment is in alarm and take action to manage the alarm.

The aggregated alarm counts are added to a display by creating an alphanumeric which is linked to the alarm group and the aggregate alarm count parameters (see Table 6).

The following table lists the aggregate alarm and alert count parameters that are available for alarm groups as well as standard point types.

Table 6 Aggregate alarm and alert count parameters

Parameter	Alarm Priority			Active State		Acknowledge State		Disabled
	Urgent	High	Low	Active	RTN	Unack	Ack	
TotalAckAlarms	X	X	X	X	X		X	
TotalAckAlerts	N/A	N/A	N/A	X	X		X	
TotalActiveAckAlarms	X	X	X	X			X	
TotalActiveAckAlerts	N/A	N/A	N/A	X			X	
TotalActiveAlarms	X	X	X	X		X	X	
TotalActiveAlerts	N/A	N/A	N/A	X		X	X	
TotalActiveUnackAlarms	X	X	X	X		X		
TotalActiveUnackAlerts	N/A	N/A	N/A	X		X		
TotalAlarms	X	X	X	X	X	X	X	
TotalAlerts	N/A	N/A	N/A	X	X	X	X	
TotalDisabledAlarms	X	X	X	X	X	X	X	X
TotalDisabledAlerts	N/A	N/A	N/A	X	X	X	X	X
TotalHighAckAlarms		X		X	X		X	
TotalHighActiveAckAlarms		X		X			X	
TotalHighActiveAlarms		X		X		X	X	
TotalHighActiveUnackAlarms		X		X		X		
TotalHighAlarms		X		X	X	X	X	
TotalHighRTNAckAlarms		X			X		X	
TotalHighRTNAlarms		X			X	X	X	
TotalHighRTNUnackAlarms		X			X	X		
TotalHighUnackAlarms		X		X	X	X		
TotalLowAckAlarms			X	X	X		X	
TotalLowActiveAckAlarms			X	X			X	
TotalLowActiveAlarms			X	X		X	X	
TotalLowActiveUnackAlarms			X	X		X		
TotalLowAlarms			X	X	X	X	X	
TotalLowRTNAckAlarms			X		X		X	
TotalLowRTNAlarms			X		X	X	X	
TotalLowRTNUnackAlarms			X		X	X		

Table 6 Aggregate alarm and alert count parameters (*continued*)

Parameter	Alarm Priority			Active State		Acknowledge State		Disabled
	Urgent	High	Low	Active	RTN	Unack	Ack	
TotalLowUnackAlarms			X	X	X	X		
TotalRTNackAlarms	X	X	X		X		X	
TotalRTNackAlerts					X		X	
TotalRTNAlarms	X	X	X		X	X	X	
TotalRTNAlerts					X	X	X	
TotalRTNUnackAlarms	X	X	X		X	X		
TotalRTNUnackAlerts					X	X		
TotalUnackAlarms	X	X	X	X	X	X		
TotalUnackAlerts				X	X	X		
TotalUrgentAckAlarms	X			X	X		X	
TotalUrgentActiveAckAlarms	X			X			X	
TotalUrgentActiveAlarms	X			X		X	X	
TotalUrgentActiveUnackAlarms	X			X		X		
TotalUrgentAlarms	X			X	X	X	X	
TotalUrgentRTNackAlarms	X				X		X	
TotalUrgentRTNAlarms	X				X	X	X	
TotalUrgentRTNUnackAlarms	X				X	X		
TotalUrgentUnackAlarms	X			X	X	X		

The following table lists aggregate message count parameters that are available for alarm groups as well as standard point types.

Table 7 Aggregate message count parameters

Parameter	Message Type		Acknowledge State	
	Informational	Confirmable	Unack	Ack
TotalAckConfMessages		X		X
TotalAckInfoMessages	X			X
TotalAckMessages	X	X		X
TotalConfMessages		X	X	X
TotalInfoMessages	X		X	X
TotalMessages	X	X	X	X

Table 7 Aggregate message count parameters

Parameter	Message Type		Acknowledge State	
	Informational	Confirmable	Unack	Ack
TotalUnackConfMessages		X	X	X
TotalUnackInfoMessages	X		X	
TotalUnackMessages	X	X	X	

The following table shows the options describing how the alphanumeric with the **Show alarm state with color** check box will behave:

Table 8 Show alarm state with color check box options

Point state	System-defined color
In alarm and unacknowledged	Red and blinking
In alarm and acknowledged	Red
Returned to normal but alarm not acknowledged	Normal color, but blinking
Point off-scan (scanning disabled)	White

To add an aggregated alarm count to a display:

- 1 Start HMIWeb Display Builder:
 - If you are on the Experion server, choose **Start > Programs > Honeywell Experion PKS > Server > HMIWeb Display Builder**
 - If you are on a client computer, choose **Start > Programs > Honeywell Experion PKS > Client Software > HMIWeb Display Builder**
- 2 Choose **File > Open**.
Select the display you to which you want to add an alarm count.
- 3 Click the  (Alphanumeric) icon on the Toolbox toolbar and then drag the pointer on the display to define the size, shape and position of the alphanumeric.
- 4 Double-click the alphanumeric to open the Properties Window, which shows the alphanumeric's current properties.
- 5 Click the Data tab and make sure that Point/Parameter is selected in **Type of database link**.

- 6 Select alarm group from the point list.
- 7 Select the required aggregate alarming parameter from the Parameter list.
- 8 Save the display.

The custom display for `Boiler1` also contains alarm state icons that indicate the state and priority of the alarm for `Boiler1`. The following table indicates the order of priority of the alarm state icon.

Priority	Active	Acked	Symbol	
Urgent	Yes	No	flashing	
High	Yes	No	flashing	
Low	Yes	No	flashing	
Urgent	No	No	flashing	
High	No	No	flashing	
Low	No	No	flashing	
Urgent	Yes	Yes	static	
High	Yes	Yes	static	
Low	Yes	Yes	static	
Disabled	-	No	flashing	
Point Disabled	No	No	Static	
No alarm	-	-	-	-

For more information on the Point Disabled alarm state refer to the section on “Setting Alarm States” in the *HMIWeb Display Building Guide*.

To add an alarm state icon to a display:

- 1 Start HMIWeb Display Builder:
 - If you are on the Experion server, choose **Start > Programs > Honeywell Experion PKS > Server > HMIWeb Display Builder**.
 - If you are on a client computer, choose **Start > Programs > Honeywell Experion PKS > Client Software > HMIWeb Display Builder**.
- 2 Choose **File > Open**.
Select the display you to which you want to add an alarm state icon.
- 3 Click the  (Alarm State) icon on the Toolbox toolbar and then move the pointer on the display to define the position of the alarm state icon.
- 4 Double-click the alarm state icon to open the Properties Window.
- 5 Click the Data tab and make sure that Point/Parameter is selected in **Type of database link**.
- 6 Select alarm group from the point list.
- 7 Save the display.

Configuring alarm paging

13

The alarm pager licensable option is a background task that monitors Station alarms and alerts to determine which alarms or alerts meet the criteria for sending messages to the appropriate recipient. There are three ways of transporting the messages to recipients:

- pagers (including SMS)
- email
- SNMP

This chapter describes configuring alarm paging for pagers, SMS, email and SNMP; and alert paging for pagers, SMS and email.

For information about	Go to:
Alarm paging	page 266
Initial configuration of the pager subsystem	page 267
Initial configuration of the email subsystem	page 270
Initial configuration of the SNMP subsystem	page 272
Configuring recipients, schedules and escalation for pagers, SMS, email and SNMP	page 274
Nominating alarms to be sent	page 276
Viewing and clearing the message queue	page 279
Message configuration common to messages sent by all subsystems	page 280

About alarm paging

Paging starts when messages are placed in the alarm pager queue. A paging message is placed in the queue when an alarm or alert is received. If the alarm or alert is acknowledged before being sent out, the message is removed from the queue. The system checks where the alarm or alert is being sent and carries out various tasks depending on where the alarm or alert is being sent.

When communications are complete, the alarm paging system waits for new messages to be placed in the queue. Each message that is sent is logged as an event in the event file. The event file also logs any communication failures or similar problems.

The alarm paging system checks its queue every 5 seconds for alarms or alerts that need to be sent.

The alarm paging options allow you to:

- Configure communications settings.
- View the alarm paging status.
- Enable or disable the paging service.
- View the number of alarms and alerts in the alarms queues and clear the queue if necessary.
- Set up escalation, so that paged alarms and alerts are automatically sent to another recipient if they are not acknowledged within a specified time.
- Determine the information you include in the messages you want the recipients to receive.
- Configure the escalation delay and the delay to send times, to allow additional time for alarms or alerts to be acknowledged before they are sent out or escalated.

To configure alarm paging, first perform the initial configuration for each of the subsystems you want to use, then configure the recipients in the tabs corresponding the subsystems you configured.

Configuring alarm paging for pagers

When sending alarms or alerts to a pager, there are two methods of connection that can be used. The methods of connection are:

- Direct connection to a paging system
- Connection by modem to a service provider

When an alarm or an alert is being sent to a pager, the system checks which connection method is being used. It then checks that there is communication with the paging system or modem. If the connection method is through a modem, the system dials the service provider number and logs on to the provider's network. If the connection method is by direct connection to a paging system, the alarm paging system logs directly onto that paging system.

Once a successful connection is made, alarm paging attempts to send the unacknowledged alarms and alerts to all of the recipients nominated for each individual alarm or alert. Each paging message in the queue can be sent out to up to 100 pagers. Message 'blocks' are sent to each pager in turn, until all messages are sent. If the provider allows it, alarm paging sends multiple message blocks at the same time, reducing the number of times it has to call the provider.

You need a security level of SUPV or higher to configure or change the settings for alarm paging.

Initial configuration

Prerequisites

- You have a modem attached to the Experion computer. Or, for redundant servers, you have a modem attached to each Experion server computer.
- The modem(s) are configured within the operating system.
- The Dialing Rules have been configured correctly within the operating system.

To configure:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and alert notification settings** task.
- 3 Click on the **General** tab.
- 4 Select the **Pagers** check box.

- 5 Review the fields described in “Common settings” on page 280, making any changes to meet your requirements.
- 6 If you want to send alarms or alert paging to pagers or SMSs through a direct connection:
 - a. Click on the **Pager Settings** tab.
 - b. Select the **Direct connection** radio button.
 - c. Enter into the **Port** field the port name.
- 7 If you want to send alarms or alert paging to pagers or SMSs through a modem:
 - a. Click on the **Pager Settings** tab.
 - b. Select the **Modem** radio button.
 - c. Check the **Pager Settings** tab to see if your modem is listed in the **Modem** drop down list box.
 - d. If your modem is not listed, the **Modem** drop down list box can be refreshed by clicking the **Refresh List** button.
 - e. If you have a redundant Experion system, fail over to the backup computer, repeating steps c. through d.
 - f. Fail over to the preferred Experion server.
 - g. Enter the telephone number of the service provider into the **Provider telephone number** field.
 Include the external access number if required. For example, if you dial 0 to access an outside telephone line from your building, and the service provider’s telephone number is 9500 1000, you type 095001000, that is, 0 followed by the service provider’s telephone number.
 - h. Set each of the redial parameters that appear in the following table.

The parameters you enter should follow those provided by the local communications authority. The values in parentheses in the table are Australian requirements. Alarm paging defaults to these values if the entered values are above maximums or below minimums.

Property	Description
Initial retry attempts	The number of automatic redials before message failure (maximum 9).
Retry interval	The delay between redials (minimum 2 seconds).
Start retrying again after	The delay before dialing again after the maximum number of automatic redials has been reached (minimum 30 minutes).
Repeat	The number of times the cycle of dialing and retrying is repeated.

- 8 Configure the specific baud rate, data bits, parity, stop bits and flow control settings required by the serial device or provider.
- 9 Select the protocol from the **Protocol** drop down list.
- 10 If your service requires a password, click the **Set Password** button and enter a password in the dialog box that appears.
The password is usually supplied by the service provider. For example, for PET protocol the password usually has the format “PG1xxxxxx”, where xxxxxx is the password supplied by the service provider. (If the provider does not supply a password, you might still need to set the alarm paging password to PG1. Check with your provider for details.)
- 11 If the **Multiple messages** drop down list is enabled, determine whether you want to send multiple messages.

Supported service providers

The service providers supported by the alarm paging system must use one of the following protocols:

- Paging entry terminal (PET)
- Telocator alphanumeric protocol (TAP)
- UCP protocols UCP 01, UCP 30, or UCP 51

Service providers in the USA generally use the PET or TAP protocols.

Service providers in the Europe mainly use the UCP protocol. The two-digit suffixes refer to the EMI command numbers being used by the provider.

Configuring alarm paging for email

To set up email to receive paged alarms or alerts, configure the SMTP relay restrictions and then configure the email details.

Initial configuration

Prerequisites

- Install Internet Information Services (IIS) with SMTP active as described in “Installing Internet Information Services 6.0” in the *Software Installation and Upgrade Guide*.

To configure SMTP relay restrictions:

- 1 On the Experion server, choose **Start > Administrative Tools > Computer Management**.
- 2 In the tree pane, expand **Services and Applications**.
- 3 Expand **Internet Information Services**.
- 4 Right-click **Default SMTP Virtual server** and select **Properties**.
- 5 Click the **Access** tab.
- 6 Click **Relay**. The **Relay Restrictions** dialog box opens.
- 7 Select **All except the list below** and click **OK**.
- 8 Click **Apply**.
- 9 Ensure that SMTP is started and set to start automatically.

To configure email details:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and alert notification settings** task.
- 3 Click on the **General** tab.
- 4 Select the **Emails** check box.
- 5 Review the fields described in “Common settings” on page 280, making any changes to meet your requirements.
- 6 Configure each of the email-specific properties.

Property	Description
Email Settings	
Sender	An email address to be used in the “From” or “Sender” box of each alarm message email sent by Alarm Paging.
Include the standard email subject message	When selected, includes the standard message in the email’s subject line: <code>Alarm alert from SERVERNAME.</code>
Include description in email subject	When selected, includes the alarm description in the email’s subject line. (When both the standard and the description check boxes are selected, both are included in the email subject line.)

Configuring alarm paging for SNMP

To set up SNMP to receive paged alarms or alerts, install SNMP and then configure it.



Attention

You cannot set up SNMP to receive paged alerts.

Initial configuration

To enable alarm paging to communicate with your SNMP manager you need to install and configure SNMP.

To install SNMP:

- 1 Choose **Start > Settings > Control Panel > Add/Remove Programs**.
- 2 Click **Add/Remove Windows Components**.
- 3 Select **Management and Monitoring Tools**.
- 4 Click **Details** and ensure that Simple Network Management Protocol is selected. Click **OK**.
- 5 Click **Next**.
- 6 When prompted, insert the Windows Server 2003 CD and click **OK**. Alternatively, click **OK** and specify where to copy files from, such as a network server, and click **OK**.

To configure SNMP:

- 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.
- 2 Right-click **SNMP Service** and choose **Properties**.
- 3 Click the **Agent** tab.
- 4 In the **Contact** box type the user name or administrator for this computer.
- 5 In the **Location** box type the physical location of this computer.
- 6 Under Service, select **Applications** and any other appropriate service.
- 7 Click the **Traps** tab.
- 8 Type a community name to which this computer sends trap messages, and click **Add to list**. The community name is case-sensitive and must be the same as the community name on the SNMP client.

- 9 Under Trap destinations click **Add**.
- 10 Type the appropriate host name, IP address or IPX address and click **Add**.
- 11 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 12 Click the **Configure alarm and alert notification settings** task.
- 13 Click the **General** tab.
- 14 Select the **SNMP** check box.
- 15 Review the fields described in “Common settings” on page 280, making any changes to meet your requirements.

Configuring recipients, schedules and escalation

The Paging, Email and SNMP tabs provide the means to specify which messages get sent to whom and when. And if they don't respond, to whom to escalate the message.

Considerations

- Holiday availability is linked to the server's Holiday Schedule. An SNMP recipient that has this availability selected receives alarms and alerts on those dates that are defined as holidays in the server Holiday Schedule.

Considerations (pagers only)

- Do not enter the phone number of the Pager Service Provider on this display. The service provider's number is entered on the **Pager Settings** tab.
- A pager's availability times also apply to escalated alarms and alerts. For example, if pager 1 receives alarms from 4:00 p.m. to midnight, Monday to Friday and pager 2 receives alarms from noon to 8:00 p.m. Monday to Friday and pager 1's alarms escalate to pager 2, pager 2 only receives alarms escalated from pager 1 between 4 p.m. and 8:00 p.m.

To configure:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and alert notification settings** task.
The Alarm and Alert Notification display appears in the System Display tab in Configuration Studio.
- 3 Click the **Paging, Email** or **SNMP** tab.
- 4 In the **Name** box, type the name of the recipient.
- 5 Enter the destination address:
 - For **Email**, enter the recipient's email address.
 - For **Pagers** (including SMS), enter the pager ID number.
Pager Service Providers specify a unique identifier as the pager ID.
For mobile phones, enter the mobile phone number.
 - For **SNMP**, no destination address is necessary.

- 6 Select the time and day of week the recipient is required to receive alarms and alerts. If both the Start and Stop times are zero, the recipient will not receive alarms or alerts at any time.
If a recipient is required to receive alarms and alerts between midnight and 8:00am, set the Start Time to 0:00 and the Stop Time to 8:00. If a SNMP recipient is required to receive alarms and alerts all day, set the Start Time to 0:00 and the Stop Time to 24:00.
- 7 Select the holiday schedule that the recipient is to follow for receiving alarms and alerts.
- 8 If you are nominating alarms and alerts by asset, select the operator ID with the appropriate assets assigned and select the check boxes to receive alarms, alerts, or both. For alarms, select the minimum alarm priority for these alarms.
- 9 Select the recipient to whom unacknowledged messages are escalated and select the check boxes to escalate alarms, alerts, or both. You can select a minimum priority for alarm escalation, which means that alarms of the minimum priority or higher are escalated.
- 10 Select the **Enable** check box to enable the recipient to receive alarms and alerts.

To cease sending alarms and alerts to a recipient, clear the **Enable** check box beside that recipient.

Nominating alarms to be sent

There are two ways to nominate the alarms to be sent to each recipient. One way is to individually specify every point that is to have its alarms paged. The other way is to nominate the alarms by assets assigned to operators.

Nominating individual point alarms

You use the Specific Alarms tab on the Alarm Paging display to specify the point points that are to have alarms sent out. Up to 10 recipients can be specified to receive the alarm messages for each point. Alarms of the specified priority or higher are sent.

To nominate individual point alarms:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and alert notification settings** task.
The Alarm and Alert Notification display appears in the System Display tab in Configuration Studio.
- 3 Click the **Specific Alarms** tab.
- 4 In the **Point ID** box, enter the point ID.
- 5 Select the minimum alarm priority.
- 6 Use the lists to nominate the recipients you want assigned to this point.

Nominating system alarms

You can nominate to which paging subsystem system alarms, such as communication failure alarms, can be assigned.



Attention

You must use the Specific Alarms tab to assign system alarms to be sent to a paging subsystem. If you make a system alarm a part of an operator's asset profile, the alarm will not be sent to a pager.

To nominate system alarms:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and alert notification settings** task.
The Alarm and Alert Notification display appears in the System Display tab in Configuration Studio.
- 3 Click the **Specific Alarms** tab.
- 4 Select the **System Alarms** check box.
- 5 Select the minimum priority of system alarms you want paged.
- 6 Use the list to nominate the recipient you want to assign to the System Alarms. Up to 10 recipients can be nominated.

Nominating alarms by assets

If you are using operator-based security, you can also use assets to control which alarms are paged. Alarms are only sent to the recipient for the assets assigned to the nominated operator.

For example, a Station operator named Norm Smith may be assigned to assets A1, A2, and A3. Only alarms from assets A1, A2, and A3 are sent to any recipient configured with Norm Smith's operator ID.

You nominate the required operator ID on the corresponding tab for each alarm paging recipient. For example, to nominate an operator ID for pagers, click the Pagers tab.

For information on setting up an operator's profile, see "Configuring operator-based security" on page 304.

**Attention**

To set up alarm paging, you must be using a Station with a security level of SUPV (or higher). Security levels are described in "Configuring security and access" on page 281.

Nominating alerts to be sent

There are two ways to nominate the alerts to be sent to each recipient. One way is to individually specify every alert condition that is to have its alerts paged. The other way is to nominate the alerts by assets assigned to operators.

Nominating individual alert conditions

You use the Specific Alerts tab on the Alarm Paging display to specify the alert conditions that are to have alerts sent out. Up to 10 recipients can be specified to receive the alert messages for each alert condition.

To nominate individual alert condition:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and alert notification settings** task.
The Alarm and Alert Notification display appears in the System Display tab in Configuration Studio.
- 3 Click the Specific Alerts to Page section of the tab, type the alert source into the **Source** box.
- 4 In the **Condition** box, enter the alert condition which will generate the alert.
- 5 Use the lists to nominate the recipients you want assigned to this point.

Nominating alerts by assets

If you are using operator-based security, you can also use assets to control which alerts are paged. Alerts are only sent to the recipient for the assets assigned to the nominated operator.

For example, a Station operator named Norm Smith may be assigned to assets A1, A2, and A3. Only alerts from assets A1, A2, and A3 are sent to any recipient configured with Norm Smith's operator ID.

You nominate the required operator ID on the corresponding tab for each alert paging recipient. For example, to nominate an operator ID for pagers, click the Pagers tab.

For information on setting up an operator's profile, see "Configuring operator-based security" on page 304.



Attention

To set up alert paging, you must be using a Station with a security level of SUPV (or higher). Security levels are described in "Configuring security and access" on page 281.

Viewing and clearing the message queue

You monitor the alarm subsystems and message queues from the **General** tab.

To view:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and alert notification settings** task.
The Alarm and Alert Notification display appears in the System Display tab in Configuration Studio.
- 3 Click the **General** tab.
- 4 Enabled message subsystems have a selected check box.
- 5 The **Current Status** describes the status of each subsystem. Each status is defined in this table.

Table 9 Alarm paging status definitions

Status	Description
Disabled	Alarm paging system has been disabled by clearing the Enabled check box.
Running	Enters the Running state while processing and searching for alarms to page.
Dialing	Changes to Dialing when trying to contact the provider's phone number.
Paging	Applicable only when paging to pagers, not email or SNMP. After connecting to the provider the system goes into the paging state until it disconnects.
Failed	Failed state indicates an error in communications. (This is usually indicated by a message in the system log.)
Waiting	Enters the Waiting state when the number of automatic redials has been exceeded. (Redial information is as configured in the Alarm Paging display.)

- 6 The **Queued Messages** displays the number of messages in the **Main Queue** and the number of messages in the **Escalation Queue**.

To clear the message queues:

- 1 On the **General** tab, click the **Clear Queues** button.
The **Main Queue** and **Escalation Queue** values are reset to zero.

Common settings

Settings common to all message transports are located on the **General** tab.

Property	Description
Include in message	
Sequence Number	The message number, incremented for each message generated by alarm paging.
Date	Date of the alarm.
Time	Time of the alarm.
Source	Source of the alarm. (Usually a point, but could be a Station number or a printer number.)
Condition	The condition field from the alarm acknowledgement display.
Priority	The priority field from the alarm acknowledgement display.
Description	The description field from the alarm acknowledgement display.
Value	The value field from the alarm acknowledgement display.
Units	Describes how to interpret the value.
Delays	
Delay to notify	The time (in minutes) between the raising of an alarm and the alarm being sent out.
Escalation delay	The time (in minutes) between alarm being sent out and the alarm being escalated.

Configuring security and access

14

This chapter describes how to configure security for your Experion system. It describes:

- How you configure each type of security
- How to use assignable assets to limit access and distribute alarms accordingly

Before you begin configuring security, you should read the *Network and Security Planning Guide*.

About security

System security enables you to control who has access to the system and to control what users can do within the system when access is granted.

The security required for your Experion system can be considered as follows:

- Windows operating system security
- Station security—Station-based or operator-based

When planning security for your site you need to consider the following:

- What type of Station security do you want to use.
- What type of access do operators require within Experion.
- If you choose operator-based Station security, do you want to use:
 - Traditional operator accounts
 - Integrated accounts using either domain Windows accounts or local Windows accounts
 - Windows group accounts using either domain Windows groups or local Windows groups
- How you implement Windows security.
- What type of Windows accounts do you require.

To learn more about	Go to:
Station security	page 283
Planning considerations to use Windows accounts	page 287

Understanding Station security

When you build a Station, you define the security method that will control access to functions at that Station. You choose between:

- Station-based security
- Operator-based security

In Station-based security there are security levels which are used to restrict operator authority within Station.

Station-based security and operator-based security are discussed further in this chapter.

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.
- Asset assignment applies to the Station, not to the operator.

The security levels and their associated functions are described in “About security levels” on page 285.

About operator-based security

Operator-based security provides a higher level of security than Station-based security. In general, Operator-based security with traditional operator accounts works as follows:

- You assign a specific security level to each user.
- Users cannot access any Station functions unless they enter a valid ID and password.

- To access a higher security level than the one they are currently using, users need to sign off and 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.

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 only 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. The Windows user account can be a local account or a domain account. For information to consider when deciding to use local or domain accounts, see “Using integrated security” on page 287. Authentication is done by Windows, authorization is done by the Experion server.
Windows group accounts	An integrated account that allows you to add multiple operators by adding the Windows group to the Experion server. The Windows group can be a local Windows group or a domain Windows group. For information to consider when deciding to use local or domain Windows groups, see “Using integrated security” on page 287. 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.

You can further restrict operator authority by restricting the level of access to assets. Access to assets uses a separate set of security levels.

For more information see “Using integrated security” on page 287.

Operator-based security and point control

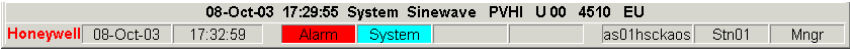
You can specify a **control level** for a point when it is configured in the server database. (Control levels for points are described in “Control properties for standard points” on page 200.)

When Operator-based security is used at a Station, an operator must have a control level greater than or equal to the control level defined for a selected point in order to be able to control that point.

About security levels

The current security level of a Station is displayed in Status Line (right-hand side). If no operator is signed on to the Station, this part of the Station Line is blank.

Figure 16 Status line showing the current security level setting (“Mngr”)



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 10 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

Table 10 Security levels (*continued*)

Default Security Level Acronym	Default Meaning
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, Engr, or Mngr.

For a list of the actions permitted at each security level, see the section “Actions permitted at each security level” on page 341.

Using integrated security

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

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 create an operator definition in Experion, so that the users 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. See “System configurations” on page 287.
- You need to decide if your system will use single signon. See “User environments” on page 297.

About 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.

System configurations

The benefits and impact of integrated accounts vary depending on your logical network configuration. This section discusses a number of typical topologies. In all these scenarios users can be configured as traditional Experion operators, in which case they will log onto Station with a user name, password and domain of <None>.

In the following scenarios, multiple solutions are presented. Your chosen solution may be a combination of these.

Scenario—single node system

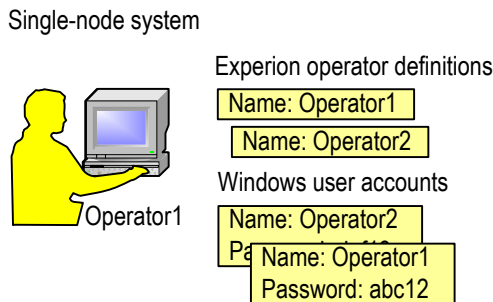
You have a single Experion server with no network connections. Operators require access to Station and other client applications on this computer.

Solution incorporating local Windows user accounts

Set up local Windows user accounts for each operator who requires access to Experion. Create operator definitions for each operator in Experion that reference the relevant Windows user account.

You can also set up Experion to use single signon. That is, when operators log on to the computer, they provide their user name and password. When the operator starts Station, they are not required to re-enter their user name or password.

Figure 17 Single node system with local Windows user accounts

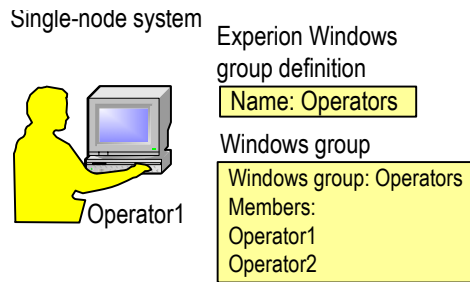


In Figure 17 operator1 and operator2 both have integrated accounts and can both use single signon since they have a Windows user account and a related operator definition.

Solution incorporating local Windows groups

Set up local Windows user accounts for each operator who requires access to Experion. Create Windows groups and add the Windows user accounts to the appropriate Windows group. Create an Experion Windows group definition that references the relevant Windows group.

You can also set up Experion to use single signon. That is, when operators log on to the computer, they provide their user name and password. When the operator starts Station, they are not required to re-enter their user name or password.

Figure 18 Single node system with local Windows groups

In Figure 18 operator1 and operator2 can both use single signon since they have a Windows user accounts belonging to a Windows group that has a related Experion Windows group definition.

Scenario—client server system (Windows workgroup environment)

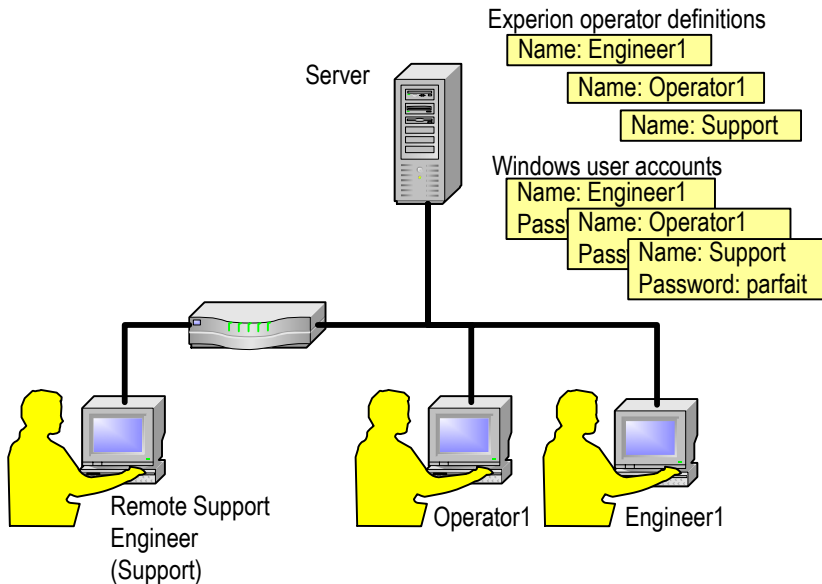
You have a client server system consisting of an Experion server and a number of Stations operating in a Windows workgroup environment. A Windows Workgroup typically consists of a small number of machines (typically less than 5), networked together. They are not part of a wider corporate network, and there is no external, Internet or other access.

Solution incorporating local Windows user accounts

To use integrated accounts and single signon, you need to manually configure identical Windows user accounts on all computers to enable network access. You also need to create operator definitions on the Experion server that reference the relevant Windows user accounts. If this account duplication has been done and each operator has the same Windows user account on the Station and the server, then Single Signon is possible.

You may also want to provide access to a support engineer. If the support engineer is not part of the workgroup, use traditional operator accounts to provide access and set the appropriate authority levels.

For a larger system, this solution is inefficient as it requires manual replication of accounts. Consider using a domain controller to reduce the overhead of manually replicating accounts.

Figure 19 Client server system with local accounts

In Figure 19 on page 290 operator1, Engineer1 and support can use integrated accounts and single signon only if they have local Windows accounts and passwords on their client computers that match the Windows accounts and passwords on the server computer.

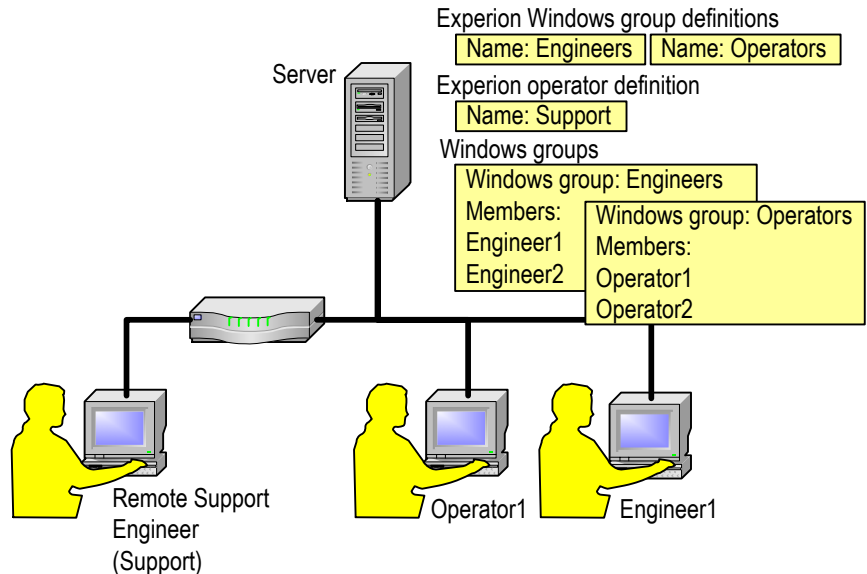
Figure 19 also illustrates the use of a guest Support account to allow access to a support engineer. In this case, it is unlikely that the support engineer's computer is part of the same workgroup as the Experion system or that the support engineer has a matching Windows account and password, and hence single signon is not available. The use of integrated accounts does not offer any advantage over traditional operator accounts.

Solution incorporating local Windows groups

To use integrated accounts and single signon, you need to manually configure identical Windows user accounts and identical Windows groups on all computers to enable network access. You also need to create Experion Windows group definitions on the Experion server that reference the relevant Windows groups. If this account duplication has been done and each operator has the same Windows user account belonging to the same Windows group on the Station and the server, then Single Signon is possible.

For a larger system, this solution is inefficient as it requires manual replication of accounts. Consider using a domain controller to reduce the overhead of manually replicating accounts.

Figure 20 Client server system with local groups



In Figure 20 operator1 and Engineer1 can single signon only if they have local Windows accounts and passwords belonging to a Windows group on their client computers that match the Windows accounts and passwords belonging to a matching Windows group on the server computer.

Figure 20 also illustrates the use of a guest Support account to allow access to a support engineer. In this case, it is unlikely that the support engineer's computer is part of the same workgroup as the Experion system or that the support engineer has a matching Windows account and password, and hence single signon is not available. The use of integrated accounts does not offer any advantage over traditional operator accounts.

Scenario—client server system (domain environment)

You have a large network of computers, included several Experion servers and client computers. The Experion servers and client computers belong to a domain. The domain controller can be using the Windows 2000 or Windows 2003 operating system.

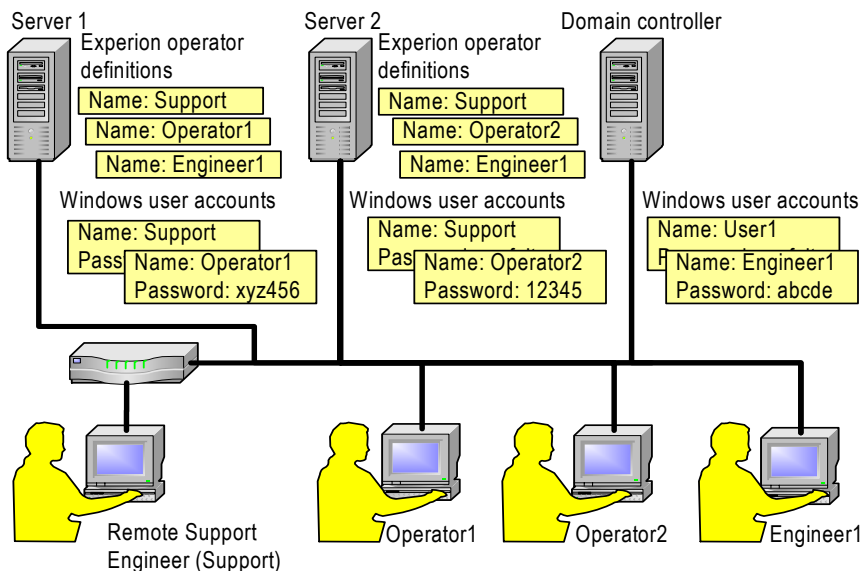
Although Windows user accounts can be local, the advantage of using a domain is that accounts are known to all computers in the domain, and account

configuration need only be done once. Account management is performed by the domain administrator, who can be a privileged Experion engineer, or may belong to the company's IT department.

Solution incorporating domain Windows accounts

Create Windows user accounts on the domain controller so that users are known to all computers within the domain. Create operator definitions for each operator on the Experion servers the operators need to access. Ensure that the operator definitions reference the relevant Windows domain account. You can then take advantage of using single signon.

Figure 21 Client server system with domain accounts



In Figure 21 two client server systems consisting of two servers and a number of operator Stations operate in a domain environment. The servers and client computers belong to a single domain, or set of trusted domains.

Engineer1 has a Windows domain account and can use the domain account to log onto Windows on any computer in the domain. Both servers have an operator definition for Engineer1 therefore Engineer1 can use an integrated account to access the two Experion systems. Engineer1 can also use single signon.

operator1 and operator2 do not have Windows domain accounts and therefore can only access computers where they have a local account. operator1 has a local Windows account and operator definition on server 1 and can gain access to this server by entering the user name operator1, password xyz456 and the

server machine name at the Station logon dialog. operator2 can gain access to server 2 in a similar manner.

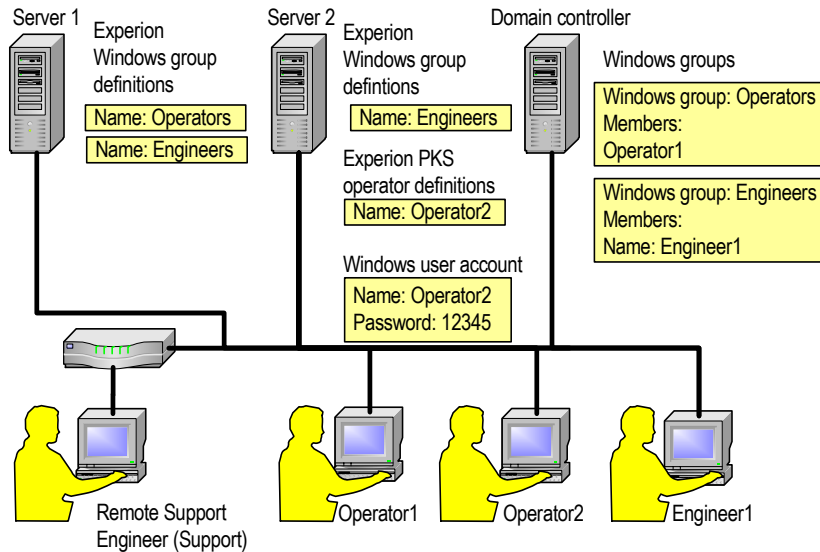
Single signon could be available for operator1 or operator2 if their accounts are moved to the domain controller or if they have matching Windows accounts and passwords created on the client computer.

Both servers have a local Support account, but the password is different on each system. This might be done to in order to control access to the various Experion systems on site. There is no real advantage to using integrated accounts for the support engineer's access.

Configurations where the server is not in the same domain as the client computer are quite valid, but add to the complexity of account configuration. In particular, it should be noted that the authentication is done by the server's domain, not the client's domain. Even if the domains do not trust each other, it is possible for an operator to log on to the server providing the account is known to the server domain. Note that the server domain does not appear in list of domains in the Station logon dialog if it is not trusted by the client. In this case the domain needs to be typed in.

Solution incorporating domain Windows groups

Create Windows user accounts and add these accounts to Windows groups on the domain controller so that users are known to all computers within the domain. Create Experion Windows group definitions for each Windows group on the Experion server the operators need to access. Ensure that the Experion Windows group definitions reference the relevant domain Windows group. You can then take advantage of using single signon.

Figure 22 Client Server system with domain Windows groups

In Figure 22 two client server systems consisting of two servers and a number of operator Stations operate in a domain environment. The servers and client computers belong to a single domain, or set of trusted domains.

Engineer1 has a Windows domain account which belongs to the domain Windows group Engineers. Engineer1 can use the domain account to log onto Windows on any computer in the domain. Both servers have an Experion Windows group definition for Engineers therefore Engineer1 can access the two Experion systems. Engineer1 can also use single signon.

operator1 has a Windows domain account which belongs to the domain Windows group Operators. Server 1 has an Experion Windows group definition for Operators therefore operator1 can access the Experion system on Server 1 using the domain account. operator1 can also use single signon. operator2 does not have a domain account and therefore can only access computers where there is a local account. In this case, Server 2 has a local Windows account and an operator definition for operator2.

Configurations where the server is not in the same domain as the client computer are quite valid, but add to the complexity of account configuration. In particular, it should be noted that the authentication is done by the server's domain, not the client's domain. Even if the domains do not trust each other, it is possible for an operator to log on to the server providing the account is known to the server domain. Note that the server domain does not appear in list of domains in the

Station logon dialog if it is not trusted by the client. In this case the domain needs to be typed in.

Scenario—redundant server system (domain environment)

You have redundant Experion servers and several client computers on a network. The Experion servers and client computers belong to a domain.

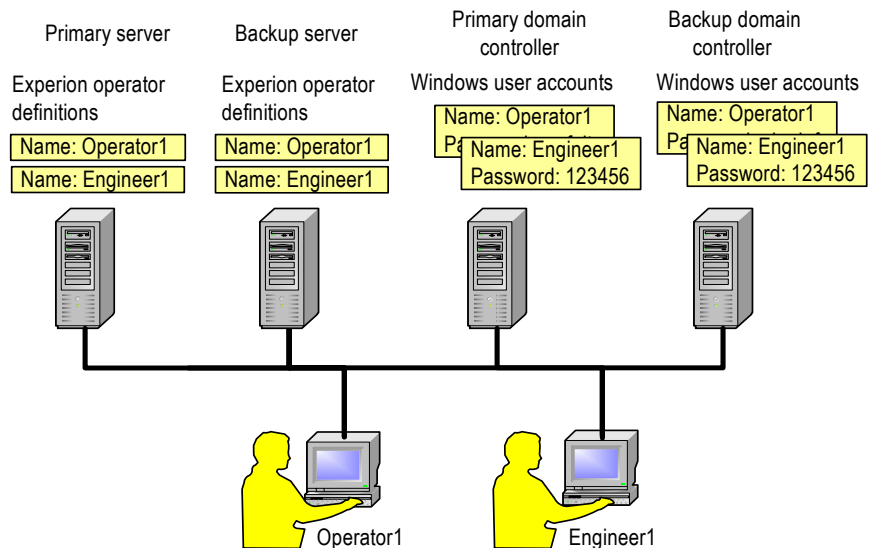
Solution incorporating domain Windows accounts

Create Windows user accounts on the domain controller to ensure consistency of Windows accounts during a failover. This eliminates any problems caused by differences in local accounts on the server computers. Create operator definitions on the primary Experion server that reference the relevant Windows domain account. The operator definitions are automatically replicated to the backup Experion server.

The use of local Windows user accounts in a redundant server system is not recommended because they need to be manually replicated, including any password changes, to the backup server.

If you cannot set up a domain, use traditional operator accounts.

Figure 23 Redundant servers with domain accounts



In Figure 23 on page 295 operator1 and Engineer1 have domain accounts and can access any computer in the domain. During failover operator1 and Engineer1 will continue to have access to the servers. Operator1 and Engineer1 can both use single signon.

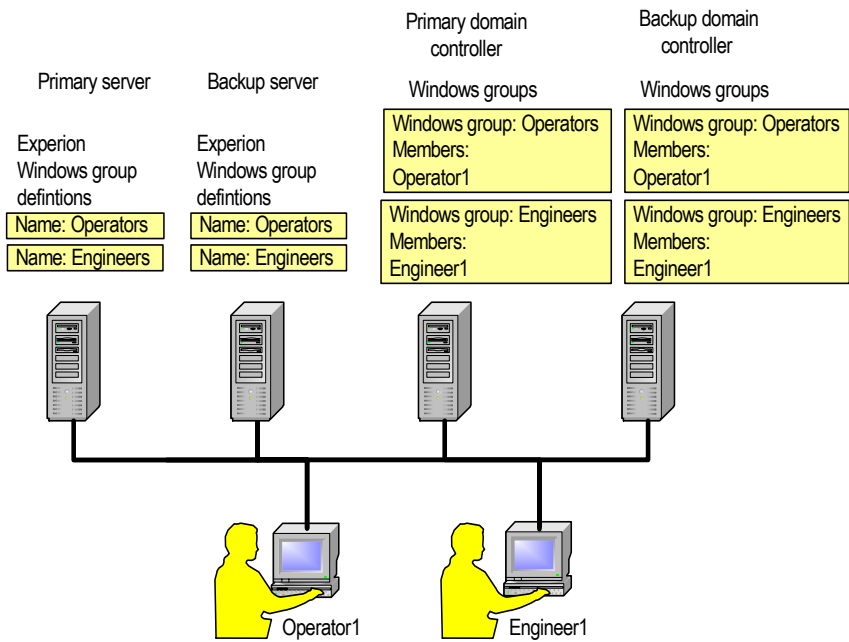
Solution incorporating domain Windows groups

Create Windows user accounts and add these accounts to Windows groups on the domain controller to ensure consistency of Windows accounts during a failover. This eliminates any problems caused by differences in local accounts on the server computers. Create Experion Windows group definitions on the primary Experion server that reference the relevant Windows domain group. The Experion Windows group definitions are automatically replicated to the backup Experion server.

The use of local Windows user accounts and groups in a redundant server system is not recommended because they need to be manually replicated, including any password changes, to the backup server.

If you cannot set up a domain, use traditional operator accounts.

Figure 24 Redundant servers with domain groups



In Figure 24 operator1 and Engineer1 have domain accounts which belong to domain groups and can access any computer in the domain. During failover operator1 and Engineer1 will continue to have access to the servers. operator1 and Engineer1 can both use single signon.

User environments

As well as deciding the best implementation of security for your system configuration, you also need to consider the best implementation of security for your work environment.

This section discusses the following environments:

- Control room
- Desktop
- Configuration

Scenario—control room environment

You have a control room where Station computers must be strictly controlled. Computers in the control room are used solely for the purpose of managing and interacting with the facility. Multiple applications can be used on a single computer to provide multiple views of the site. For example you can run several instances of Station running on the one computer, displayed on several monitors.

The primary concern in this environment is continual visibility of the facility. To facilitate this you need to minimize disruptions due to:

- Administrative tasks where engineers make changes.
- Shift change where operators log on and off.

Other applications such as Configuration Studio or third-party applications exchanging server data, may also run on these computers.

Solution

To improve operator productivity, use integrated accounts or Experion Windows group accounts and single signon so that operators provide their credentials once when they log on to the computer. This is particularly useful where you start multiple instances of Station.

In this environment it is useful to have a default “view-only” operator account so that Station remains connected to the server. This way alarms are evident at all times. To do this:

- Create a generic Windows user account.
- Create an operator definition in Experion that references the generic Windows account and assign the lowest security level.
- Set up the computer so that it starts with this account and Station starts automatically.

Scenario—desktop environment

You have a conventional office computing environment involving a wide range of applications, including Station. This environment is much less structured than the control room environment.

Users in this environment have a casual interest in the entire site or multiple sites and need to connect to several different Experion systems, sometimes simultaneously.

The primary concerns in this environment are:

- Flexibility
- A high level of integration of process views with the desktop computing environment

Site managers spend most of their working time in this environment. They often have multiple instances of Station connected to different Experion servers.

Typically, domain accounts are used in this environment.

Solution

To remove the need to repeatedly provide credentials whenever the manager logs on to Station, use integrated accounts or Experion Windows group accounts and single signon.

Create an operator definition or Windows group definition on each Experion server referencing the domain Windows account or Windows group for the manager.

Scenario—remote user

You need to provide access to a technical support engineer who needs to investigate problems from time to time. This user is an infrequent user outside of your domain environment.

Solution

On the Experion server create a local Windows user account and an operator definition referencing the Windows account. The account name and password are encrypted on the network.

The Windows account and operator definition can be disabled when they are not required.

Domain environments

The operating system for your domain controllers can be either Windows 2000 or Windows 2003. The difference is described in this section.

In Windows 2000 and Windows 2003 domains the account information is held within the Active Directory infrastructure (AD) and security information is transported by Kerberos, a more secure protocol than NTLM.

The Windows 2000 and Windows 2003 domains also use Organization Units (OU). An OU is a group of objects, for example, users, to which common Group Policy can be applied, and 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 within the OU. This is useful for controlling dedicated operator computers so that they all have a common appearance, security settings and execution environment. You can use the High Security Policy to implement a secure environment.

For more information on OUs and Group Policy see:

- Windows 2000 Server Resource Kit/Deployment Planning Guide/AD Infrastructure
- Windows 2000 Server Resource Kit/Distributed Systems/Desktop Configuration Management
- Windows Server 2003 Deployment Kit/Designing and Deploying Directory and Security Services

About the Operator Management Service

The Operator Management Service is a Windows service that is installed when you install Experion. The service provides a central point for:

- Checking the existence of Windows accounts and groups for operator-based security.
- Retrieving details for use by the server, for example full name.
- Password changes in Station

Because the Operator Management Service is not used as part of the logon process for any Station or other clients that log on to the server, the service must run under an account that has the appropriate permissions to perform the required functions. If the account does not have permission to query the local account database or a domain based account database, then a user account that does exist may be reported as not being found, with errors reported in the server log.

The default account under which the Operator Management Service runs is the System account. You should use the information in this section to determine the most appropriate account for your topology.

The Operator Management Service running under the System account supports:

- Local Windows accounts
- Windows 2000/2003 Active Directory domain accounts running with the **Allow pre-Windows 2000 servers to access Active Directory** option set in either **Mixed Mode** or **Native Mode**.

Password changes are available only for:

- Local accounts (regardless of whether the old password is known)

The System account does not support the High Security Policy.

Choosing an appropriate account

To determine the appropriate Windows account under which the Operator Management Service needs to run, you need to know the location of Windows accounts and the facilities required for these accounts. The following sections describe possible scenarios and the account requirements.

Notes

- If the **chgpsw** command is used, an operator can change their own password for integrated accounts regardless of whether the account is a local account or a domain account.
- If you have a combination of local Windows accounts and domain accounts, the Operator Management service must run under an account that has all the permissions listed in the following section. To achieve this you may have to use trust relationships between your domains.
- The Operator Management service account needs to be added to the Honeywell Administrators group on all servers and Console Stations utilizing the account for the Operator Management Service.

Local Windows accounts

- If you need to change the password in Station for other users then the account must be a member of the local Administrators group. The System account satisfies this requirement.
- If you do not need to change passwords in Station for other users, then the account can be a domain account or a local account. It does not need to be a member of the local Administrators group. The System account satisfies this requirement.

Windows 2000/2003 Active Directory domain in any mode

- If you need to change passwords in Station for other users, the account must be a member of the domain Administrators group or the account must be delegated the **Create, delete, and manage user accounts** role and the **Reset passwords on user accounts** role for the entire domain or the Organizational Unit (OU) containing the accounts.
- If users need to be able to change their own password in Station, the account must be known to the domain. It can be a domain account or it can be an account from a trusted domain.
- If there are no password change requirements in Station and the Allow pre-Windows 2000 servers to access Active Directory was chosen when the Active Directory was installed, then the account can be a domain account or a local account. The System account satisfies this requirement.
- If there are no password change requirements in Station and the Allow pre-Windows 2000 servers to access Active Directory was not chosen when the Active Directory was installed, then the account must be known to the domain. It can be a domain account or it can be an account from a trusted domain.

High Security Policy

- If you have implemented the High Security Policy, the Windows account must be a member of a High Security Policy group on the domain controller. The Windows account can be a member of any High Security Policy group.

Setting the Operator Management Service account

After you have determined the account under which the Operator Management service needs to run, you need to set the service to run under this account on all Experion servers and Console Stations.

To set the account for the Operator Management service:

- 1 Log on to the server computer using an account that is a member of the Administrators group.
- 2 Choose **Start > Control Panel**.
- 3 Double-click **Administrative Tools**.
- 4 Double-click **Services**.
- 5 Locate the Operator Management Service.
- 6 Right-click the server and choose **Properties**.
- 7 Click the **Log On** tab.

- 8 Type the account name and password.
- 9 Confirm the account name and password.
- 10 Click **OK**.
- 11 Click **OK** to subsequent messages.
- 12 Right-click the service and choose **Restart**.

Configuring Station-based security

Station-based security is the default security type for all types of Station. If you want to use Station-based security, there is no special configuration required.

Using passwords in Station-based Station security

If you have chosen the Station-based security method, it is recommended that you change the default passwords (one each for ENGR, SUPV, and MNGR security levels) that were installed as part of the Experion installation process.

Under Station-based security, only levels SUPV, ENGR, and MNGR require passwords because:

- View Only and Ack Only are not available.
- Users can access OPER level without entering a password.

To access functions associated with security levels higher than OPER:

- 1 Start up Station if it is not already running.
- 2 Type **psw** in the command zone and press ENTER (or click the Security Level displayed in the Status Line).
The **Station Logon** dialog box opens.
- 3 Type the password for the desired security level and click **OK**.

Configuring operator-based security

If you want to use operator-based security, you need to:

- Specify operator-based security for each Station that is to use this security method.
- Define each operator (or Experion Windows group account) who needs to access these Stations.

You specify operator-based security for a Flex Station when you build the Flex Station. You specify operator-based security for a Console Station (and Console Extension Stations) when you configure the Console Station.

The procedures for building a Flex Station are described in Quick Builder's help. If necessary, see Quick Builder's help for assistance in completing the following instructions.

The procedures for configure Console Stations and Console Extension Stations are described in the section, "Configuring Console Stations and consoles" on page 521.

To specify operator-based security for one or more Flex Stations:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Build Flex Stations** task.
Quick Builder appears.
- 3 In the item list, select all the Station items that are to have operator-based security.
- 4 Go to the **Main** tab, and select the **Operator-Based Security** check box.
A check mark in the box means that operator-based security is enabled for the selected Station(s).

Considerations

- The security type you choose for a Console Station also applies to the Console Extension Stations connected to the Console Station.

To specify operator-based security for a Console Station:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Station Configuration display appears in the System Display tab in Configuration Studio.

- 3 Click the name of the Console Station to which you want to specify operator-based security.
- 4 Select **Operator sign-on required**.

Considerations

- You only need to configure the type of security for a console if you want the console settings to apply to the Console Stations and Console Extension Stations within the console. For more information about consoles, see “About consoles” on page 540.

To specify operator-based security for a console:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Consoles** task.
The Console Configuration display appears in the System Display tab in Configuration Studio.
- 3 Click the name of the Console to which you want to specify operator-based security.
- 4 Select **Operator sign-on required**.

Adding an operator

The server software is installed with a default traditional operator account of `mngr`. The security level for this account is `MNGR` and the default password is `mngr1`. You use this default operator account and password to set up access for all other users. You should check the password for the `mngr` operator account as it may have been changed.

If you are using integrated accounts you still need to create an operator definition in Experion and assign access rights within Experion.

Prerequisites

- If you are using integrated accounts, ensure that the Windows account exists before you define the operator in Experion.
- Add the Windows accounts to the appropriate Honeywell Experion Windows group. For example, if the operator needs to use configuration tools, add the Windows account to the Honeywell Administrators group.

To define an operator:

- 1 In the Configuration Explorer in Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click an empty row. This opens the **Operator Configuration** display.
- 4 Click the **Operator Definition** option.
- 5 For the operator you are adding, type the appropriate information.

You can use the list at the top of the Operator Configuration display to view or change the details of any operator who has already been entered into the system.\

The Operator Configuration display is used to define the details for a new operator or to amend the details for an existing operator. Specify the information as follows:

Property	Description
Username	A unique identifier for the operator. You can use a maximum of 20 alphanumeric characters. If you are using Windows accounts, the user name specified here must be exactly the same as the Windows account. Whenever an operator makes a change at a Station (for example, to control a point, acknowledge an alarm) and that change is logged as an event, the operator user name is recorded with the event in one of the following formats: • user name—for traditional operator accounts • .\user name—for local integrated accounts • domain\user name—for domain integrated accounts If Show operators full name in the event summary on the Server Wide Settings display is selected, then the Full name is recorded with events instead of the user name.
Use Windows account	If selected indicates that the operator account is using a corresponding Windows account. If the corresponding Windows account does not exist or is configured differently to how it is referenced, the error message, “The Windows account could not be found”, is displayed.
Domain	Available only if Use Windows account check box is selected. The name of the domain where the Windows accounts exists. If the Windows account is a local account, leave blank.
Full name	The operator’s name. If you are using Windows accounts, this information is updated automatically from the Windows account and is read-only. The full name is recorded with events if the Show operators full name in the event summary on the Server Wide Settings display is checked. (See “Alarm/Event Options tab” on page 109.)
Job title	The operator’s title, if applicable.
Asset	Use this option to specify the asset that must be assigned for viewing this operator’s configuration details. Only Stations or operators with this asset assigned are permitted to view the details display for this operator.

Property	Description
Password	Click the Change Password button to change the operator's password. For information relating to changing passwords for integrated accounts see "Changing passwords for integrated accounts" on page 319, Note: Passwords are case-sensitive.
Security Level	Select the security level assigned to the operator.
Control level	Defines the control level assigned to the operator (from 0 to 255). The default is 255. The operator's control level determines whether or not the operator is permitted to control a point. (For more about point control, see "Control properties for standard points" on page 200.)
Multi-user	If selected, this operator ID can log on concurrently on multiple Stations using the same user name and password. If this option is not selected and you have Console Stations, this operator can log on concurrently to a single Flex Station and a Console Station or one of its Extension Stations.
Access for this operator is disabled	If selected, indicates the operator details are retained however operator access using the account is disabled for this server or redundant server pair.
Ignore any Windows Group settings for this Operator	If selected, ignores any of the Windows groups settings if the operator is also a member of an Experion Windows group account.
The following alarms will be printed on this Operator's Alarm/Event printer	• Print LOW priority alarms. Enables printing of low alarms and points going out of low priority alarm conditions to Station's printer when the operator is logged on to the Station. • Print HIGH priority alarms. Enables printing of high alarms and points going out of high priority alarm conditions to Station's printer when the operator is logged on to the Station. • Print URGENT priority alarms. Enables printing of urgent alarms and points going out of urgent priority alarm conditions to Station's printer when the operator is logged on to the Station. • Print journal alarms/events. Enables printing of events and journal alarms and points going out of journal priority alarm conditions when the operator is logged on to the Station. • Print Operator changes. Enables printing of all changes to points an operator has made from the Station. Note: When the operator logs on to Station, these settings override the default Station settings (see "Flex Station Configuration Display" on page 113). The printer assigned to the Station as the alarm/event printer is used to print the alarms and events.

Property	Description
Operator idle timeout	If selected, the specified time is the idle timeout value, in seconds, for this operator. When this time is exceeded without any operator activity, the operator has to re-enter their password. This idle timeout overrides the idle timeout specified for server-wide Station settings. If you use Signon Manager, consider setting this timeout to 0. If you specify a timeout and you use Signon Manager, if the timeout is exceeded, the startup display is called up.
Operator start up page	If selected, the specified display is the startup display for this operator. This setting overrides the start up display defined for the Station (as described in “Configuring startup displays” on page 84).

Modifying operator configuration details

Considerations

- If you are using Windows accounts, do not change the Username or Domain unless you have already made the corresponding changes to the Windows account.

To modify operator account details:

- 1 In the Configuration Explorer in Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click the Operator ID you want to change.
- 4 Change the details as required.

Any changes made to the configuration details of an operator are not effective until the next time the operator signs on to Experion.

Deleting operator configuration details

Considerations

- Deleting an operator ID deletes all the details of the operator such, as user name and domain, and sets security attributes, such as security level, to the default settings.

To delete an operator account:

- 1 In the Configuration Explorer in Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click the Operator ID you want to delete.
- 4 Click **Clear Details**.

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.

To disable an operator account:

- 1 In the Configuration Explorer in Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click the Operator ID you want to disable.
- 4 Select the **Access for this operator is disabled** check box.

Converting traditional operator accounts to integrated accounts

If you already have traditional operator accounts, you can convert these accounts to integrated accounts. You need to complete the following tasks:

- If you have existing Windows accounts, modify your operator accounts by changing the user name of the operator account to exactly match the user name of the existing Windows accounts.
Alternatively, create Windows accounts for each operator account, ensuring that the user name is exactly the same for both the Windows account and the operator account.
- Add the Windows accounts to the appropriate Honeywell Experion Windows group. For example, if the operator needs to use configuration tools, add the Windows account to the Honeywell Administrators group.
- In Station, modify each operator configuration details and select **Use Windows accounts**.
- Enter the domain name if the Windows accounts belong to a domain.

Adding an Experion Windows group account

If you use integrated security and you use Windows groups, you can create Experion Windows group accounts.

By using an Experion Windows group account, you only have to configure one account in Station for every Windows group, which enables members of the Windows group to log on to Station.

The benefits of using Experion Windows group accounts are:

- Ease of configuration
- Reduces the number of accounts required in Experion
- You can leverage any existing Windows security policies and settings
- You can apply any Experion security and access restrictions at the Windows group level

Determining the security settings for Windows group operators

An operator can be a member more than one Experion Windows group. The security settings of the first 10 groups (as they are stored in the server database) to which an operator belongs are used to determine the security settings for the operator.

If an operator is a member of an Experion Windows group as well as being defined as a single operator, the security settings for the Experion Windows group are ignored unless the **Ignore Windows groups for this operator** option is disabled.

The following table describes how the combined security settings of each Experion Windows group are used to determine the security settings for a particular operator belonging to more than one Experion Windows group.

Security setting	Applied security setting
Security level	The highest level of all Experion Windows group accounts is applied.
Control level	The highest level of all Experion Windows group accounts is applied.
Alarm/Event print settings	A union of all settings is applied. For example, Group1 prints urgent and high alarms, Group2 prints low alarms and events. An operator belonging to both Windows groups can print urgent, high, and low alarms and events.

Security setting	Applied security setting
Idle timeout	The longest timeout period is applied. If a value of 0 is specified for any of the Experion Windows group accounts, then no timeout is applied. If no idle timeout is specified for any of the Experion Windows group accounts, the system wide idle timeout is used.
Startup page	Experion searches the Experion Windows group accounts to which the operator belongs in the order listed in the Operator Summary display. It chooses the first of those Experion Windows group accounts that has a startup page defined and uses this startup for the operator. If there is no startup page configured for any of the Experion Windows group accounts, the system wide startup page is used.
Asset assignment	The highest permission for each asset is applied. If an asset profile is used, the profile is calculated and merged with the permissions of the other Experion Windows group accounts. For example, if one Experion Windows group account has view only permission and another Experion Windows group account has view and acknowledge permission, a member of both will have view and acknowledge permission.
Time access	Time access is checked only at logon. If the Experion Windows group account has access at the current time, then all of the settings in the Experion Windows group account are considered in determining the settings for the operator. If the Experion Windows group account does not have access at the time, then all of the settings in the Experion Windows group account are ignored when determining the settings for the operator.
Flex Station access	Flex Station access is checked only at logon. If the Experion Windows group account has access at the current time, then all of the settings in the Experion Windows group account are considered in determining the settings for the operator. If the Experion Windows group account does not have access at the time, then all of the settings in the Experion Windows group account are ignored when determining the settings for the operator.

Security setting	Applied security setting
Console Station access	Console Station and Console Extension Station access is checked only at logon. If the Experion Windows group account has access at the current time, then all of the settings in the Experion Windows group account are considered in determining the settings for the operator. If the Experion Windows group account does not have access at the time, then all of the settings in the Experion Windows group account are ignored when determining the settings for the operator.

If the user logging in with an integrated account is also a member of a Windows group configured in Experion, then care needs to be taken when using the **Multi-User** and **Ignore any Windows Group settings for this Operator** options:

- If the **Ignore** flag is off and **Multi-user** is off, then this user can log in to more than one Flex Station. However, the first Flex Station they log into will have a Scope of Responsibility that is based on the operator's record and also all of the relevant Windows Group records. For subsequent logins the Scope of Responsibility will be determined completely by the relevant Windows Group records.
- If **Multi-User** is enabled then all logins will have their Scope of Responsibility determined by the operator's record and all relevant Windows Group records.
- If the **Ignore** option is enabled, all relevant Group records are always ignored for all login attempts by this user.

Prerequisites

- If you are using Experion Windows group accounts, ensure that the Windows group exists before you define the account in Experion.

To create an Experion Windows group account:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click an empty row. This opens the **Operator Configuration** display.
- 4 Click the **Windows Group Definition** option.
- 5 Specify the appropriate information for the Windows group you are adding as follows:

Property	Description
Windows Group name	A unique identifier for the Experion Windows group. You can use a maximum of 32 alphanumeric characters. The name specified here must be exactly the same as the Windows group.
Domain	The name of the domain where the Windows group exists. If the Windows group is a local group, leave blank.
Description	This information is updated automatically from the Windows group and is read-only.
Asset	Use this option to specify the asset that must be assigned for viewing this Experion Windows group's configuration details. Only Stations or operators with this asset assigned are permitted to view the details display for this Experion Windows group.
Security Level	Select the security level assigned to the Experion Windows group.
Control level	Defines the control level assigned to the Experion Windows group (from 0 to 255). The default is 255. The control level determines whether or not the operator is permitted to control a point. (For more about point control, see "Control properties for standard points" on page 200.)
Access for this Windows Group is disabled	If selected, when an operator belonging to this Windows group logs on, the settings of this Windows group are ignored. If the operator is not a member of any other Windows group, and is also not defined as a single operator, then the operator has no access. If the operator belongs to other Windows groups that do not have access disabled, then the security settings of the other Windows groups are used to determine the security settings of the operator.
Printer Assignment	Select the classes of alarms and events that are printed this Experion Windows group's alarm/event printer.
Windows Group idle timeout	If selected, the specified time is the idle timeout value, in seconds, for this Experion Windows group. When this time is exceeded without any operator activity, the operator has to re-enter their password. This idle timeout overrides the idle timeout specified for server-wide Station settings. If you use Signon Manager, consider setting this timeout to 0. If you specify a timeout and you use Signon Manager, if the timeout is exceeded, the startup display is called up.
Windows Group start up page	If selected, the specified display is the startup display for this Windows group. This setting overrides the start up display defined for the Station (as described in "Configuring startup displays" on page 84).

Deleting an Experion Windows group account

Considerations

- Deleting an Experion Windows group account deletes all the details of the group such, as name and domain from the Experion server, and sets security attributes, such as security level, to the default settings.

To delete an Experion Windows group account:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click the Windows group you want to delete.
- 4 Click **Clear Details**.

Changing passwords

The procedure you use to change a password depends on the type of Station security you use or the type of operator account you have.



Attention

You cannot use Station to change the password for an operator who belongs to an Experion Windows group unless that operator also has an individual Experion operator definition.

If you have	See
Station-based security	page 317
Traditional operator accounts	page 318
Integrated accounts	page 319

Setting and changing passwords for Station-based security

Default passwords are set for ENGR, SUPV, and MNGR at each Station as part of the installation process. These default passwords are the same as the acronym used for that security level; for example, the default password for MNGR security level is mngr.

Considerations

- Passwords are case-sensitive.
- The scope of the password change on a Console Station includes Console Extension Stations.

To change a Station password for ENGR, SUPV, or MNGR:

- 1 Log on to the Experion server with a Windows account that belongs to the Honeywell Administrators group.
- 2 Open a **Command Prompt** window.
- 3 Type **paswr**

- 4 If you are changing passwords for a Flex Station, specify the Flex Station number as follows:
Fnn
 where nn is the number of the Station for which you want to change the password(s)
 If you are changing passwords for a Console Station, specify the Console Station number as follows:
Cnn
 where nn is the number of the Console Station for which you want to change the password(s)
- 5 Type the number for the security level for which you want to change the password:
 - 1 for SUPV
 - 2 for ENGR
 - 3 for MNGR
- 6 Type the new password. The password can be either 5 or 6 alphanumeric characters.
- 7 Type **Q** (for quit).

Changing password for traditional accounts

Considerations

- Operator passwords are encrypted.
- The 10 most recently used passwords cannot be re-used within a configurable time period.
- The validity period for passwords defaults to one month, but this setting can be configured as required. For details, see “Configuring Sign-on administration” on page 322.

To change your password:

- 1 Type **chgpsw** in the Command Zone and press ENTER.
 The **Change Password** dialog box opens.
- 2 Type your old password and press TAB.
- 3 Type your new password and press TAB.
- 4 Re-type your new password and click **OK**. (The new password is only accepted if the new password entries are identical.)

Changing passwords for integrated accounts

As with traditional operator accounts, operators can use the **chgpsw** Station command to change their own password for integrated accounts. Operators with **mng**r security level can also change passwords for integrated accounts using the Operator Configuration display. Operators with **supv** security level or higher can change their own password on the same display.



Attention

You cannot use Station to change the password for an operator who belongs to an Experion Windows group unless that operator also has an individual Experion operator definition.

To change a password using the **chgpsw** command:

- 1 Type **chgpsw** in the Command Zone and press ENTER.
The **Change Password** dialog box opens.
- 2 Type your old password and press TAB.
- 3 Type your new password and press TAB.
- 4 Re-type your new password and click **OK**. (The new password is only accepted if the new password entries are identical.)

The same dialog box appears when you change a password from the Operator Configuration display.

Defining sign-on restrictions

The Sign-On Restriction display is used to define the time and Station Sign-on access for a new or existing operator or an Experion Windows group account.

Considerations

- Any restrictions you specify for a Console Station also apply to any Console Extension Stations connected to the Console Station.

To define sign-on restrictions:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows Group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click the name of the operator or Experion Windows group for which you want to define sign-on restrictions.
- 4 Click the **Sign-On Restriction** tab and specify the appropriate restrictions as described in the following sections.

Restricting Station access

The default setting is for all Flex Stations and all Console Stations to be accessible to new operators.

The settings you specify for a Console Station apply to the Console Extension Stations connected to the Console Station.

To give an operator access to a Flex Station or a Console Station, select the check box next to the Flex Station name or the Console Station name.

To restrict an operator from signing on to a Flex Station or a Console Station, clear the check box next to the Flex Station name or the Console Station name.

Time restrictions

To restrict an operator to signing on only between certain times of day, set the start and finish times of the operator's valid access period.



Attention

The default setting is for all days to be enabled (checked), with no restrictions on time access (that is, from 0:00 to 24:00). To restrict an operator for the entire day, clear the box next to the name of the day.

Holiday access times

Holiday access times are only applied on the days that have been defined as a holidays.



Attention

On holidays, the holiday start and finish times override the normal Sunday to Saturday times.

For more information about configuring holidays, see “Configuring holidays” on page 611

Configuring Sign-on administration

This section describes:

- Configuring password administration parameters for traditional operator accounts.
- Configuring integrated security policy, such as single signon and password administration for integrated accounts.

Configuring password administration for traditional operator accounts

To configure password administration for traditional operator accounts:

- 1 In the Configuration Explorer of Configuration Studio click **Security**.
- 2 Click the **Administer Operator Sign-on** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Set the administration properties as appropriate:

Property	Description
Password Expiry Period	Operator passwords for traditional operator accounts will expire after this number of days, and a new password will be required.
Password Validation Period	Expiration does not allow operators with traditional operator accounts to reuse any of their 10 most recently used passwords unless the password was changed at least as many days ago as specified in this option.
Change Operator Configuration Security Level	Defines the security level required to change operator configuration.
Number of failed logins before lockout	Specifies the number of unsuccessful login attempts permitted before Station lockout.
Lockout time	The Station will stay locked out for this period of time after the specified number of failed logins.

Operator failed login alarms

An alarm is raised when an operator enters an incorrect password or when the number of specified login attempts is exceeded. You can set the priority of these alarms. You might want to set the priority of an operator lockout alarm to Urgent while you might want to set the priority to journal when an operator enters an incorrect password.

To set the priority of operator alarms:

- 1 In the Configuration Explorer of Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Configure alarm and point processing** task.
The Alarm and Point Processing display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Priorities** tab.
- 4 On the **Alarm Priorities** display, set the required priorities for **Operator Logon**. The Operator Logon alarm indicates when an operator has entered an incorrect password.
- 5 On the **Alarm Priorities** display, set the required priorities for **Operator Lockout**. The Operator Lockout alarm indicates the operator has exceeded the number of login attempts and does not have access to the Experion system.

Configuring Integrated Security policy

If you are using integrated accounts you can configure your system to allow

- Single signon
- Password changes in Station

To configure integrated security policy:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 Click the **Administer operator sign-on** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Set the options as required.

Property	Description
Allow Single Signon	If selected, operators provide their user name and password only once when they log on to the Station computer.
Allow password changes in Station	If selected, operators can change the password for their Windows account in Station. Note, passwords for Experion Windows group accounts cannot be changed in Station.

Using High Security Policy

The 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.

You can use the High Security Policy in a domain or a workgroup environment however, Group Policy is best implemented in a domain environment.

The following table lists the various components associated with High Security Policy and where they are installed.

Component	Installed
Group Policy Objects (GPOs)	A GPO for each user type is created on the domain controller.
Global Windows groups	A global group for each user type is created on the domain controller. These groups are used as filters on the GPOs.
Global accounts	User accounts created on the domain controller
Local Windows groups and users	A local group for each user type is created on each computer when you install the workstation security package.
Local computer policy settings	Created on each computer where you install the workstation security package.
Linkdomaingroups.vbs	A script to link global groups with local groups for computers participating in a domain.
Local user policy template	A local policy for computers not participating in a domain.
Lockdownlocalusers.bat	A script to enable the local policy on computers not participating in a domain.

Implementing the High Security Policy in a domain environment allows you to 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.

About High Security Policy Workstation Package

The High Security Policy Workstation Package is automatically installed with Experion software. The following modifications are made after the High Security Policy Workstation Package is installed:

- Several local user accounts are created.
- Several local Windows groups are created.
- A local policy is installed.
- Some modifications to registry permissions and file permissions are made.

The following tables list the local Windows groups and users that are created.

Windows Group name
Local Ack View Only users
Local Continuous Controls
Local Engineers
Local Intimate Users
Local Operators
Local Point Builders
Local Programs
Local Servers
Local Supervisors
Local View Only Users

User account name
GUS
LocalCOMServer
TPSLocalServer

Domain environment task list

The following table lists the steps required to install and implement High Security Policy in a domain environment.

Prerequisites

- You must have the System Management software installed before you install High Security Policy. For instructions on installing the System Management software on a domain controller, see the following topic in Knowledge Builder:
Experion R300 > Configuration > System Management Configuration Guide > Installing System Management Tools > System Management Installation - Domain Controller.

Task	Go to	Done
Install High Security Policy Domain Controller Package from the Experion Application DVD on to your domain controller	page 327	
Decide if you need to customize the Group Policy objects and perform any customization.	page 329	
Create and add users accounts to the appropriate Windows groups on the domain controller. For example, administrator accounts should be added to the DCS Administrators group and the Engineering Repository Administrators group, and so on.		
Apply the Group Policy to the Windows groups.	page 330	
On each computer where you want to implement the Global Policy, link the domain groups to the local Windows groups, run the <code>LinkDomainGroups.cmd</code> .	page 331	
Create logon scripts to start the required applications automatically, for example, Station. For more information, see the “Restricting access to operating systems and non-Station software” section in the <i>Administration and Startup Guide</i> .	<i>Knowledge Builder</i>	
Assign the script to user accounts where appropriate. For more information, see the “Restricting access to operating systems and non-Station software” section in the <i>Administration and Startup Guide</i> .	<i>Knowledge Builder</i>	

Workgroup environment task list

The following table lists the steps required to implement High Security Policy in a workgroup environment.

Task	Go to	Done
Decide if you need to customize the <code>wksta_lo.inf</code> template and perform any required customization.	page 329	
Create and add user accounts to the appropriate Windows group. Users that have not been added to a Windows group will not be able to log on to a computer that has had the High Security Policy Workstation package installed.	Microsoft Windows Help	
Enable local security policy on each computer, run the <code>Lockdownlocalusers.bat</code> batch file	page 332	
Create logon scripts to start the required applications automatically, for example, Station. For more information, see the “Restricting access to operating systems and non-Station software” section in the <i>Administration and Startup Guide</i> .	<i>Knowledge Builder</i>	
Assign the script to user accounts where appropriate. For more information, see the “Restricting access to operating systems and non-Station software” section in the <i>Administration and Startup Guide</i> .	<i>Knowledge Builder</i>	

Installing High Security Policy Domain Controller Package

Prerequisites

- Experion Application DVD.
- Your domain controller is installed using the mixed mode option.

To install High Security Policy on a domain controller

- 1 Insert the Experion Application DVD into the DVD drive of the domain controller.
- 2 In Windows Explorer, browse to the Packages folder on the DVD and double-click the `Install.exe` file
- 3 On the Welcome screen, read the instructions and click **Next**.
- 4 On the End User License Agreement screen, read the agreement and click **Next**.
- 5 On the Third-party Software Compatibility Policy screen, read the instructions and click **Next**.

- 6 On the User Information screen, type your details and click **Next**.
- 7 On the Package Selection screen, select Domain Security and click **Install Package**.

Results

The following modifications are made when you install the High Security Policy Domain Controller Package:

- Several user accounts are created.
- Several Windows groups are created.
- Group Policy objects are installed.

The following tables list the Windows groups and users that are created.

Windows Group name
Ack View Only Users
Continuous Ctrls
DCS Administrators
DCS Domain Servers
Engineering Repository Administrators
Engineers
Intimate Users
Operators
Point Builders
Programs
Supervisors
View Only Users

User account name
DCSComServer
TPSApp
TPSComServer

Reviewing Group Policy Objects and Security Templates

Before you implement High Security Policy, you may want to review the settings and make any customizations for your site.

Domain environment

Considerations

- If you want to customize the Group Policy, make a copy and edit the copy.

To view Group Policy settings in a domain environment:

- 1 On the Domain Controller choose **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 Right-click the domain name and choose **Properties**.
- 3 Click the **Group Policy** tab.
- 4 Select the Group Policy you want to view and click **Edit**.

Workgroup environment

Considerations

- The `wksta_1o.inf` template cannot be copied from one computer to another. If you make changes, you must make these changes to every template on every computer.

To view security templates in a workgroup environment:

- 1 Choose **Start > Run**, type `mmc` and click **OK**. The MMC opens.
- 2 Choose on **File > Add/Remove Snap-in**.
The **Add/Remove Snap-in** dialog box opens.
- 3 Click **Add**.
The **Add Standalone Snap-in** dialog box opens.
- 4 Select **Security Templates** and click **Add**.
- 5 Click **OK**.
The Security Templates snap-in is added to the console.
- 6 Navigate to the `wksta_1o.inf` template and review the settings.

Apply Group Policy objects to a global Windows group

You only need to perform this procedure if you use domains.

To apply Group Policy objects to a global Windows group:

- 1 On the Domain Controller choose **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 Right-click the domain name and choose **Properties**.
- 3 Click the **Global Policy** tab.
- 4 Right-click the policy and choose **Properties**.
- 5 Click the **Security** tab.
- 6 Add the Windows groups and/or users to the policy.
- 7 Select the **Read** and **Apply group policy** check boxes.
- 8 Click **OK**.
- 9 Click **OK**.

Considerations for adding user accounts to Windows groups

User accounts inherit the permissions of the Windows group to which they belong. When adding user accounts to Windows groups, you need to consider the permissions of the Windows group and choose the appropriate Windows group for the type of user. For example, operators should be added to operator Windows groups; administrators should be added to administrator Windows groups.

There are certain accounts used by Experion processes that need to be added to specific groups. If you have the System Event Server and the System Performance Server, the DCSCComServer account must be added to the LocalServers local Windows group on the computer where the System Event Server is installed. If you have the Engineering Repository database, the administrator account must be added to the Engineering Repository Administrators Windows group.

If you add an account to more than one Windows group, you need to be aware of how permissions in one Windows group may override permissions in other Windows groups to which the user belongs.

Linking the domain Windows groups to local Windows groups

You only need to perform this procedure if you use domains.

Considerations

- Perform this procedure on every computer in the domain where you want to implement the High Security Policy.

Prerequisites

- The computer must already be added to the domain.

To link the domain Windows groups to the local Windows groups:

- 1 Open a Command Prompt.
- 2 Change the directory to `c:\Program Files\Honeywell\wkstaSecurity`.
- 3 Type the command `Linkdomaingroups.vbs`.

Results

After you have run `Linkdomaingroups.ubs`, the domain Windows groups are linked to the local Windows groups as follows.

Domain Windows group	Linked to local Windows group
Ack View Only Users	Local Ack View Only Users
Continuous Ctrls	Local Continuous Controls
DCS Administrators	Honeywell Administrators, Administrators
DCS Domain Servers	Local Servers
Engineering Repository Administrators	Engineering Repository Administrators
Engineers	Local Engineers, Engineering Repository Users
Intimate Users	Local Intimate Users
Operators	Local Operators, Engineering Repository Users
Point Builders	Local Point Builders
Programs	Local Programs
Supervisors	Local Supervisors, Engineering Repository Users
View Only Users	Local View Only Users

Enabling the Local Security Policy in a workgroup environment

If you are implementing the High Security Policy in a workgroup environment, you need to enable the local security policy on each computer.

If you use domains, you do not need to perform this procedure.

Considerations

- The `Lockdownlocalusers.bat` file enables the local security policy as well as changing the access security permissions to the `\system32\GroupPolicy` folder. The security permissions are changed such that local Administrator account does not have access to the GroupPolicy folder so that the policy is not applied when the Administrator logs on to the computer. This is necessary to enable the Administrator account to perform administrative tasks on the computer.

To enable the local security policy:

- 1 Open a command prompt.
- 2 Change the directory to `c:\Program Files\Honeywell\wkstaSecurity`.
- 3 Type the command `Lockdownlocalusers.bat`.

Configuring profiles for scope of responsibility

A profile consists of an asset list, containing one or more assets, and a time period. If you are using operator-based security, profiles provide:

- Additional security, through the ability to assign assets only for specified times
- A method of giving an operator additional access at specified times. For example, after hours monitoring from a central location.
- A quick way of assigning assets to operators

If you make any changes to a profile, these changes are not available to any operator using that profile until the next time the operator logs on.

To use profiles, you need to:

- 1 Configure the assets in the system (see “About assets and the asset model” on page 40)
- 2 Configure asset lists (see “Configuring asset lists” on page 333)
- 3 Configure time periods (see “Configuring time periods” on page 334)
- 4 Configure profiles (see “Configuring profiles” on page 335)

Configuring asset lists

To configure an asset list, first ensure that all the assets you want to use have been defined.



Attention

The first list in the summary is a predefined list for which all configured assets are selected. This list is supplied with the name All Assets. You can change the name, description, and asset name of the All Areas list, but you cannot change the assets selected.

To create an asset list:

- 1 In the Configuration Explorer of Configuration Studio click, click **Security**.
- 2 In the Profiles list, click the **Configure asset lists** task.
- 3 Click an empty row in the summary. The Asset Lists Configuration display opens.

- 4 Under Definition, type:
 - The name you want to give the asset list.
 - A description of the list.
- 5 Select the assets that you want to include in this list. If you want to include all assets in the list, click **Select All**.
- 6 If you want to include subordinate assets, select **Apply changes to subordinate items**.
- 7 Type the name of the asset that must be assigned to operators to allow them to change this list.

Configuring time periods



Attention

The first time period in the summary is a predefined time period that includes all hours of all days. This time period is defined with the name All Hours. If you do not need to limit the hours that assets are assigned to operators, you can use this time period for all your Profiles.

You can change the name, description, and asset name of the All Hours Time Period, but you cannot change its time period details.

To configure a time period:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 In the Profiles list, click the **Configure time periods** task.
- 3 Click an empty row in the summary. The Time Periods configuration display opens.
- 4 Under Definition, type:
 - The name you want to give the asset time period.
 - A description of the time period.
- 5 Select the days and type the start time and stop time for the segments you need.
- 6 Type the name of the asset that must be assigned to operators to allow them to change this time period.

Configuring profiles



Attention

The Full Access profile in the summary is a system-defined profile that consists of the All Assets / All Hours pair only. An operator with this profile has access to all assets at any time.

This profile is supplied with the name Full Access. You can change the name, description, and asset name of the full access profile, but you cannot change its asset list / time period details.

To configure a profile:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 In the Profiles list, click the **Configure profiles** task.
- 3 Click an empty row in the summary. The Profiles configuration display opens.
- 4 Under Definition, type:
 - The name you want to give the profile.
 - A description of the profile.
- 5 The lower half of the screen provides for 16 Asset List / Asset Time Period pairs. Specify the pairs that you require for this profile.
- 6 Type the name of the asset that must be assigned to operators to allow them to change this profile.

Assigning scope of responsibility

You define an operator's or Station's scope of responsibility by assigning access to assets, nodes in the Network tree and components in the System Components tree. Assigning access enables you to restrict or allow access to parts of the plant, process, or equipment for your operators or Stations.

For example, if you have an asset called, `Precipitator`, that asset and all child assets and points associated with the `Precipitator` asset are viewable by Stations or operators that have had the `Precipitator` asset assigned to them with an access level of at least "View". If a Station or operator does not have the `Precipitator` asset assigned, they cannot view child assets or points associated with the `Precipitator` asset.



Attention

- Asset number 1 is reserved for system item alarms and alarms for unassigned points.
- If assets are associated with points or processes that are currently in alarm, these existing alarms will not observe asset restrictions. It is therefore recommended that assets be configured before points are defined or otherwise configured when there are no alarms affecting points and processes associated with the assets you are creating.
- Alarms for an asset can be temporarily disabled using the Status Change Alarm Area Inhibit algorithm. See "Configuring algorithms" on page 235 for details.

Assignment restrictions

You can specify the level of access that an operator or Station has. The following table lists the levels of access and the actions permitted.

Access level	Description
Full access	The operator or Station can perform all actions with this level of access on all items that have been assigned to the operator or Station.
View and acknowledge	The operator or Station can only view the assigned items and can only acknowledge alarms associated with those items.
View only	The operator or Station can only view the assigned items and can view alarms associated with the assigned items. No other actions are permitted.

Scope of responsibility and Station-based security

If you use Station-based security, you assign assets, Network tree nodes, and System Components to Stations (Flex and Console Stations) to define the scope of responsibility of each Station. When an action is performed, the assignment of the Station is checked to ensure the action is within the scope of responsibility of the Station. If you use Console Extension Stations, the assignment of the Console Station to which they are connected is used to determine access.

If a Console Station belongs to a console and is using the console settings, the asset assignment of the console is used to determine access. If the Console Station is not using the console settings, the asset assignment of the Station is used to determine access. For information about Console Stations and consoles, see “Configuring Console Stations and consoles” on page 521.

Scope of responsibility and operator-based security

If you use operator-based security, you assign assets, Network tree nodes, and System Components to operators (or Experion Windows groups) to define scope of responsibility. When an operator performs an action, the assignment of that operator (or the Experion Windows group to which the operator belongs) is checked to ensure the action is within the defined scope of responsibility.

By default for operator-based security, only the assignment of the individual operator (or Experion Window group) is used to define the scope of responsibility. You can, however, choose to combine operator (or group) assignment with Station assignment, as described below.

Combining operator assignment and Station assignment

If you are using operator-based security, you can configure the assignment of both Stations and operators (or Experion Windows groups) and configure your server so that the assignment of both the Station and the operator (or the Experion Windows group to which the operator belongs) are checked before access is granted.

If you are using Station-based security, configuring your server to check the assignment of both the Station and the operator has no impact: only the assignment of the Station is used to determine the access rights.

To configure the server to check the assignment for both the operator and the Station:

- 1 In the Configuration Explorer in Configuration Studio, click **Security**.
- 2 Click the **Configure server wide security settings** task.
The Server wide settings display appears in the System Display tab in Configuration studio.
- 3 Select the **Check both the Operators AND the Stations asset assignment for access to a given asset** check box.

Assigning scope of responsibility to Flex Stations

To configure the assignment of individual Flex Stations:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Flex Stations** task.
The Flex Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Station to which you want to assign access.
- 4 Click the **Assignment** tab.
- 5 Select the level of access for each asset, Network node and System component you want to assign to the Flex Station.



Tip

To change the assignment for different Flex Stations, use the list of Flex Stations available above the Assignment tab.

Assigning scope of responsibility to Console Stations

Considerations

- The assets you assign to a Console Station also apply to any Console Extension Stations connected to the Console Station.

To assign scope of responsibility to a Console Station:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Console Station to which you want to assign assets.
- 4 Click the **Assignment** tab.
- 5 Select the level of access for each asset, Network node and System component you want to assign to the Console Station.

Assigning scope of responsibility to consoles

To assign scope of responsibility to a console:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure consoles** task.
The Console Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Console Station to which you want to assign assets.
- 4 Click the **Assignment** tab.
- 5 Select the level of access for each asset, Network node and System component you want to assign to the Console Station.

Assigning scope of responsibility to operators or Windows group accounts

To assign scope of responsibility to individual operators or Windows groups accounts:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 Click the **Configure operators and Windows group accounts** task.
The Operators display appears in the System Display tab in Configuration Studio.
- 3 Click the operator or Windows Group account to which you want to assign assets.
- 4 Click the **Assignment** tab.
- 5 For each operator or Windows group account, you can select a profile from the list (see “Configuring profiles for scope of responsibility” on page 333) or you can select level of access for each asset, Network node and System component the operator needs to be assigned.



Tip

To change the assignment for different operators or Windows Groups, use the list available above the Assignment tab.

Assigning displays to assets

Access to custom displays can also be restricted using assets. An area code (asset tagname) can be assigned to a custom display when it is built. For details on how to build custom displays, see the *Display Building Guide*.

Actions permitted at each security level

The tables in this section show the actions permitted at each security level in Experion. Most of these actions correspond to options available from Station.

General

Table 11 Permissions for general Experion actions

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View startup display	Yes	Yes	Yes	Yes	Yes	Yes
Call up displays	Yes	Yes	Yes	Yes	Yes	Yes
View message pad	Yes	Yes	Yes	Yes	Yes	Yes
Edit message pad			Yes	Yes	Yes	Yes
View system acronyms	Yes	Yes	Yes	Yes	Yes	Yes
Configure system acronyms						Yes
View user acronyms	Yes	Yes	Yes	Yes	Yes	Yes
Configure user acronyms						Yes
View redundant server status	Yes	Yes	Yes	Yes	Yes	Yes
Configure server redundancy				Yes	Yes	Yes
Failover/synchronize redundant servers				Yes	Yes	Yes
View History Assignment	Yes	Yes	Yes	Yes	Yes	Yes
Configure History Assignment				Yes	Yes	Yes
View connections	Yes	Yes	Yes	Yes	Yes	Yes
View server wide Station settings	Yes	Yes	Yes	Yes	Yes	Yes
Configure server wide Station settings						Yes
View application summary	Yes	Yes	Yes	Yes	Yes	Yes
Configure application summary				Yes	Yes	Yes
View application point list summary	Yes	Yes	Yes	Yes	Yes	Yes
Configure application point list summary				Yes	Yes	Yes
Edit server scripts					Yes	Yes
View system sinewave	Yes	Yes	Yes	Yes	Yes	Yes

Table 11 Permissions for general Experion actions (*continued*)

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
Configure system sinewave						Yes
View Task Timers	Yes	Yes	Yes	Yes	Yes	Yes
View Watchdog Timers	Yes	Yes	Yes	Yes	Yes	Yes
View file replication	Yes	Yes	Yes	Yes	Yes	Yes
Configure file replication						Yes
Start file replication						Yes
View DSA configuration	Yes	Yes	Yes	Yes	Yes	Yes
Configure DSA					Yes	Yes
View DSA tuning settings	Yes	Yes	Yes	Yes	Yes	Yes
DSA tuning						Yes
Print page	Yes	Yes	Yes	Yes	Yes	Yes
Change SUPV level display object				Yes	Yes	Yes
Change ENGR level display object					Yes	Yes
Change MNGR level display object						Yes
Edit displays					Yes	Yes
Edit SCADA control strategy					Yes	Yes
Edit Process control strategy						Yes
Edit assets						Yes
Edit alarm groups						Yes
Edit servers						Yes

System security and assets

Table 12 Permissions for system security and assets

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View profiles	Yes	Yes	Yes	Yes	Yes	Yes
Configure and assign profiles						Yes
View Operator's ID and name	Yes	Yes	Yes	Yes	Yes	Yes
View Operator's full details				Yes	Yes	Yes
Configure Operators, excluding security level, command segregation and asset assignment						Yes

Table 12 Permissions for system security and assets *(continued)*

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
Assign assets to operators, Flex Stations, Console Stations and consoles						Yes
View sign on administration	Yes	Yes	Yes	Yes	Yes	Yes
Configure sign on administration						Yes

Points

Table 13 Permissions for points

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View point information	Yes	Yes	Yes	Yes	Yes	Yes
Configure point information excluding descriptor and asset				Yes	Yes	Yes
Configure point information descriptor and asset						Yes
Control points			Yes	Yes	Yes	Yes
View point algo information	Yes	Yes	Yes	Yes	Yes	Yes
Configure point algo information				Yes	Yes	Yes
View point schedules	Yes	Yes	Yes	Yes	Yes	Yes
Configure point schedules					Yes	Yes
View shifts	Yes	Yes	Yes	Yes	Yes	Yes
Configure shifts				Yes	Yes	Yes
Configure shift management				Yes	Yes	Yes
Initialize shift management					Yes	Yes
View point processing limits	Yes	Yes	Yes	Yes	Yes	Yes
Configure point processing limits				Yes	Yes	Yes

System hardware

Table 14 Permissions for system hardware

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View Station, printer, channel, point server, system interfaces, controller, DSA and redundant server status	Yes	Yes	Yes	Yes	Yes	Yes
Modify Station, printer, channel and controller status				Yes	Yes	Yes
View Channel maintenance	Yes	Yes	Yes	Yes	Yes	Yes
Configure Channel maintenance						Yes
View Flex Station settings	Yes	Yes	Yes	Yes	Yes	Yes
Configure Flex Station settings				Yes	Yes	Yes
View Console Station configuration	Yes	Yes	Yes	Yes	Yes	Yes
Configure Console Station					Yes	Yes
View Console Station settings	Yes	Yes	Yes	Yes	Yes	Yes
Configure Console Station settings					Yes	Yes
Delete Console Station					Yes	Yes
View Console configuration	Yes	Yes	Yes	Yes	Yes	Yes
Configure Consoles					Yes	Yes
View Console settings	Yes	Yes	Yes	Yes	Yes	Yes
Configure Console settings					Yes	Yes
Delete Consoles					Yes	Yes
Configure LEDs for specialized keyboards						Yes

Alarms and alarm management



Attention

eServer users do not have access to alarms and cannot perform any of the actions listed in this table.

Table 15 Permissions for alarms and alarm management

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View alarms	Yes	Yes	Yes	Yes	Yes	Yes
Acknowledge alarms		Yes	Yes	Yes	Yes	Yes
Enable and disable alarms server wide						Yes
Configure server-wide setting for Alarm return-to-normal only non-alarm states						Yes
Configure external alarm notification				Yes	Yes	Yes
Configure unanswered alarms				Yes	Yes	Yes
View system alarm priorities	Yes	Yes	Yes	Yes	Yes	Yes
Configure system alarm priorities						Yes
Configure server redundancy alarm priority						Yes
View alarm pager	Yes	Yes	Yes	Yes	Yes	Yes
Configure alarm pager				Yes	Yes	Yes
View alarm message text	Yes	Yes	Yes	Yes	Yes	Yes
Configure alarm message text				Yes	Yes	Yes
View server wide alarm color settings	Yes	Yes	Yes	Yes	Yes	Yes
Configure server wide alarm color settings						Yes
View Alarm, Event and Message Summary permission	Yes	Yes	Yes	Yes	Yes	Yes
Configure Alarm, Event and Message Summary permission						Yes
View alarm priority elevation settings	Yes	Yes	Yes	Yes	Yes	
Configure alarm priority elevation settings			Yes	Yes	Yes	Yes

Events and event archiving

Table 16 Permissions for events and event archiving

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View events	Yes	Yes	Yes	Yes	Yes	Yes
Archive/Restore events			Yes	Yes	Yes	Yes
Configure event archive parameters						Yes
View event tamper detection settings	Yes	Yes	Yes	Yes	Yes	Yes
Configure event tamper detection settings						Yes

Groups and trends

Table 17 Permissions for groups and trends

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View groups	Yes	Yes	Yes	Yes	Yes	Yes
Configure groups				Yes	Yes	Yes
View trends	Yes	Yes	Yes	Yes	Yes	Yes
Configure trends			Yes	Yes	Yes	Yes

Reports

Table 18 Permissions for report functions

Action	View Only	Ack Only	OPER	SUPV	ENGR	MNGR
View report definitions	Yes	Yes	Yes	Yes	Yes	Yes
Configure report definitions, excluding security requirement				Yes	Yes	Yes
Configure security on report definitions						Yes
Request reports	Yes	Yes	Yes	Yes	Yes	Yes

Setting security levels for enabling/disabling channels and hardware

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

To set the minimum security level required for enabling or disabling:

- 1 In the Configuration Explorer in Configuration Studio, click **Security**.
- 2 Click the **Server wide security settings** task.
The Server wide Station settings display appears in the System Display tab in Configuration Studio.
- 3 Under **Enable and disabling hardware**, select the security level you want to set for this operator function.

When you call up the Channel Status Summary and the Controller Status Summary display you will not be able to use the **Enable** check boxes on these displays unless you are currently logged on at the security level specified.



Attention

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

Changing the names of security levels

You can change the default names (OPER, MNGR, and so on) that are used to identify each security level, and which are displayed in Station's Status Line. The default name for security levels are Experion acronyms that can be changed via the System Acronym Configuration display.

Considerations

- Any changes you make to default security level names will be overwritten when you upgrade Experion. If you do not use the default names for security levels, you need to repeat the above process every time you upgrade Experion.
- Acronyms are more commonly used in building custom displays. For information about how acronyms are used in custom displays, see the *Display Building Guide*.
- Changing the name of the security level does not change the password for the security level. See “Setting and changing passwords for Station-based security” on page 317.

To change the security level acronyms:

- 1 In the Configuration Explorer of Configuration Studio, expand **Advanced Options** and click **Acronyms**.
- 2 Click the **Configure system acronyms** task.
The Acronyms display appears in the System Display tab in Configuration Studio.
Acronym numbers 265 through 270 are used for the default security levels.
- 3 Click the acronym that you want to change and type in a new 4-character acronym.

Signon Manager

15

This chapter describes how to configure and use Signon Manager.

About 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 for applications that are “Signon aware”.

Signon Manager can be used with Station if the Station security type you are using is operator-based security.

You install Signon Manager on each computer on which you want to use Signon Manager.

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 and scope of responsibility for the current signed on user.

For example, an operator is logged on to Signon Manager and is running multiple Stations. 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.

The current signed-on user is displayed in the Current User window. By default the Current User window is always visible above any applications that are running. You can position the Current User window anywhere along the top or bottom of the screen or you can hide the Current User window. You can also customize the color of the Current User window.

In addition to the Current User window, the Current User taskbar icon appears in the taskbar. When you move the mouse over the taskbar icon, the current signed on user is displayed.

If no user is signed on to Signon Manager, both the Current User window and taskbar icon shows the user currently signed on to the Windows desktop.

**Attention**

Single sign-on must be enabled on the Experion server to enable the default Windows desktop user to sign into Station.

Configuring Signon Manager

After you have installed Signon Manager you can configure the appearance of Signon Manager

To customize the appearance of Signon Manager:

- 1** Choose **Start > Programs > Honeywell Experion PKS > System Management > Configuration Utility**. The Configuration Utility appears.
- 2** Choose **Configure > Signon Manager**.
- 3** To hide the Current User window, deselect **Keep Signon display on-screen at all times**.
- 4** To change the color of the text in the Current User window click **Text**. The Color palette appears.
- 5** Select the required color and click **OK**.
- 6** To change the color of the background of the of Current User window, click **Background**. The Color palette appears.
- 7** Select the required color and click **OK**.
- 8** Click **OK** to apply the changes and close the Signon Manager Configuration.

Using Signon Manager

To sign on to Signon Manager:

- 1 Click the Current User window. (If the Current User window is hidden, press CTRL+ALT+S or click the Current User taskbar icon.)
The **Signon** dialog box opens.
- 2 Type your user name.
- 3 Type your password.
- 4 Select the appropriate domain if your user account is a domain account or leave blank for a traditional operator account.
- 5 Click **Sign On**.
The Current User window displays the current signed-on user.

To sign off use one of the following methods:

- In the Current User window, click **Signoff**.
- Right-click the Signon Manager taskbar icon and select **Signoff**.

To override the current user:

- 1 Click the Current User window. (If the Current User window is hidden, press CTRL+ALT+S.)
The **Signon** dialog box opens.
- 2 Type your user name.
- 3 Type your password.
- 4 Select the appropriate domain if your user account is a domain account or leave blank for a traditional operator account.
- 5 Click **Override**.

To end the user override use one of the following methods:

- In the Current User window, click **End Override**.
- Right-click the Signon Manager taskbar icon and select **End Override**.

Configuring Electronic Signatures

16

This chapter describes how to configure Electronic Signatures.

About Electronic Signatures

Electronic signatures are the legally binding equivalent of an operator's handwritten signature. Depending on your site requirements, you can configure operator actions, such as acknowledging a message or controlling a point, to request one or more electronic signatures to complete the action.

Electronic Signatures requires you to use integrated accounts for operators. Traditional operator accounts cannot be used with Electronic Signatures. For more information about integrated accounts see “Using integrated security” on page 287.

You can configure an action to require single or double signatures as well as a reason for the action. You can configure a set of reasons the operator can select at the time of signing.



Attention

The IKB and the OEP keyboard are not compatible with Electronic Signatures. You cannot use either of these keyboards with Electronic Signatures.

Operator actions are not complete if:

- The user name or password provided by the operator is invalid.
- The operator cancels the **Electronic Signature** dialog box.
- The operator does not have the appropriate security level required for the action.

The steps required to configure electronic signatures are:

- 1 Configure points that require electronic signature (see *Quick Builder Reference*).
- 2 Configure messages that require electronic signature (see the *Control Builder Components Reference*).
- 3 Customize legal text (see “Customizing legal text” on page 358).
- 4 Configure reason sets (see “Configuring Electronic Signature reason sets” on page 359).

Considerations for Electronic Signatures and DSA

If you want to use Electronic Signatures in your Distributed System Architecture, consider the following:

- All servers in the DSA must be licensed for Electronic Signatures.
- Reason sets must be consistent across servers in the DSA. Reason sets are not automatically synchronized across the servers.
- Legal text must be consistent across servers in the DSA.
- All servers in the DSA must use integrated accounts for operators.

Customizing legal text

The legal text displayed in the **Electronic Signatures** dialog box can be customized to your site requirements. The legal text informs the operator that their electronic signature is the legally binding equivalent of their handwritten signature.

To customize legal text:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 Click the **Configure Electronic Signatures** task.
The Electronic Signatures display appears in the System Display tab in Configuration Studio.
- 3 Type the legal text you require for your site.

Configuring Electronic Signature reason sets

You can associate a set of reasons with a particular action so that when the operator performs an action and provides a signature, the operator can select from a list of preconfigured reasons. A reason set can contain up to 32 reasons.

A reason indicates why a control action is required.

For example, when you build a point in Quick Builder that requires electronic signatures, you also need to associate a reason set with that point.

To configure a reason set:

- 1 In the Configuration Explorer of Configuration Studio, click **Security**.
- 2 Click the **Configure Electronic Signatures** task.
The Electronic Signatures display appears in the System Display tab in Configuration Studio.
- 3 Click the **Reason Sets** tab.
- 4 Click a blank row. The **Electronic Signature Reason Set definition** display appears.
- 5 Type a title for the Reason Set.
- 6 Type the reasons you require.

Configuring group and trend displays

17

This chapter describes how you configure two types of standard displays that can be used for grouping information and showing trends:

- Group displays
- Trend displays

These displays require only minimal configuration and provide a convenient way for operators and other users to view information about a group of related points on a single display.

These displays are standard displays available with every Experion installation, but it is not mandatory to use them. You might prefer to use custom displays instead of (or as well as) standard displays.

For more information, see “Configuring Station displays for points” on page 222. For information on defining displays for points on Experion Process Controllers, see the *Experion Control Building User’s Guide*.

Configuring groups

You can only configure groups after you have configured points for your site.

To configure groups, you need to be using Station with a security level of SUPV (or higher). Security levels and the procedures for changing security levels are described in “Configuring security and access” on page 281.

About groups and displays

When you configure groups, information for up to eight points can be viewed on a single Station display.

Each group can contain a mixture of point types: analog, status, accumulator, process and flexible points.

The total number of groups you can create depends on the size of your database. See the *Installation Guide* for information about the relationship between database size and the number of available groups.

By configuring groups for your site, you can access the following standard Group display types:

Display	Description
Group Detail	Shows the important data such as PV, SP for each point in the group.
Group Trend	Shows trend information for each point in the group.
Group Numeric History	Shows numeric history information for each point in the group.

These displays are described in detail in the *Operators Guide*.

Figure 25 on page 363 shows an example of a typical Group display.

Figure 25 Group Detail display



Creating groups

This section describes creating a new group.

To add a new group:

- 1 In the Configuration Explorer of Configuration Studio, click **Trends and Groups**.
- 2 Click the **Configure groups** task.
The Group Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click an empty title. This calls up the Group Configuration display for that group.
- 4 In the **Title** box, type a title for the group you are creating.
- 5 Enter the point IDs for the points you want to include in the group. Point descriptions appear automatically as each point is entered.
- 6 Select the parameter that you want shown in the group trend and group numeric history for each point.

This parameter would normally be PV for standard points, or the equivalent for flexible points.

The choice of parameter does not change the parameters shown on the faceplates in the group displays.

- 7 Click **View Group** to call up the Group Detail display for this group.

Modifying groups and points

To change the name of an existing group:

- 1 Call up the Group Configuration display for the group you want to rename.
- 2 Under **Definition**, edit the **Title** and press **ENTER**.
- 3 Change the points assigned to the group using the **Point IDs** boxes.

Deleting groups and points

To delete a group

- 1 In the Group Configuration Summary display, click the name of the group you want to delete.
This calls up the Group Configuration display for that group.
- 2 Under **Definition**, place your cursor in the **Title** box and press **DELETE** then **ENTER** to remove the group from the active list of groups.
- 3 To delete any point currently assigned to a group, select the point you want to delete in the relevant **Point IDs** box, and press **DELETE**, then press **ENTER**.

Navigating to group displays

When calling up a group display in Station, you can use:

- Standard navigation methods
- Custom navigation methods

Standard navigation methods

Standard navigation methods require no configuration. They are listed below because you might want to use them when checking a group configuration or display.

The following standard methods can be used to call up a group display:

- Go to the Group Summary display click the name of a specific group to call up. When the Group Configuration display for a specific group is displayed, click the **View Group** link to view the group.
- Click the Group icon on the Station toolbar and type a group number in the Station command zone and press **ENTER**.
- Press **F6** to call up a group by number.

- In Station's Command Zone, type the GRP command and the number of the group you want to display then press ENTER.
- In any Group display, change the current number in the **Group** box to the number of the another group to display. Alternatively, choose another group from the list of titles at the top of the display.

These standard methods are described in detail in the *Operators Guide*.

Custom navigation methods

Alternatively, you might want to configure one of the following custom call-up methods to provide a quick and easy way of calling up a display:

- User-defined Station function keys
- Push-button objects on a custom display

Details on user-defined function keys are stored in the Station setup file. For details on configuring user-defined function keys, see “Customizing toolbars, menus and keyboard shortcuts” on page 74.

For details on configuring push buttons on custom displays, see the push button section in the *HMIDisplay Building Guide*.

Configuring trend displays

Trend displays are standard Station displays that provide a way of viewing historical data for points.

Trend displays complement other types of displays that can be used to view historical data such as point detail trends, group trends, and custom display trends.

About trend displays

Trend displays show historical information for point parameters that have been selected to be historized. If a parameter that is not being historized is allocated to a trend, the trend will update in real-time. In order to configure and use the Trend displays effectively, it helps if you understand how Experion collects point history. Point history collection is described in “History collection and archiving” on page 215.

When configuring a Trend, you need to specify the required history interval to be viewed. (History intervals are the periods between snapshots and the periods over which averages are calculated. These periods are then used for collecting history.)

The number of trends available in your system depends on the server database sizing. For details about database sizing, see the *Software Installation and Upgrade Guide*.

About interpolation

If the history interval you specify when you configure your trends differs from the history collection for any point parameters in your trend, values for these point parameters are interpolated for the trend.

For example, if you had a point parameter that was assigned to standard history and the trend was configured to show fast history, the trend would display an x every minute for historical data, and then a continuous plot line in real time.

Data can also be interpolated in instances where a point parameter is assigned to more than one history type but gating has been configured for the point parameter for one of the history types.

Trends and history archiving

The history archive files are automatically searched to display archived history data for specified times and dates on a Trend display.

For details on archiving point history, see “History archiving” on page 218.

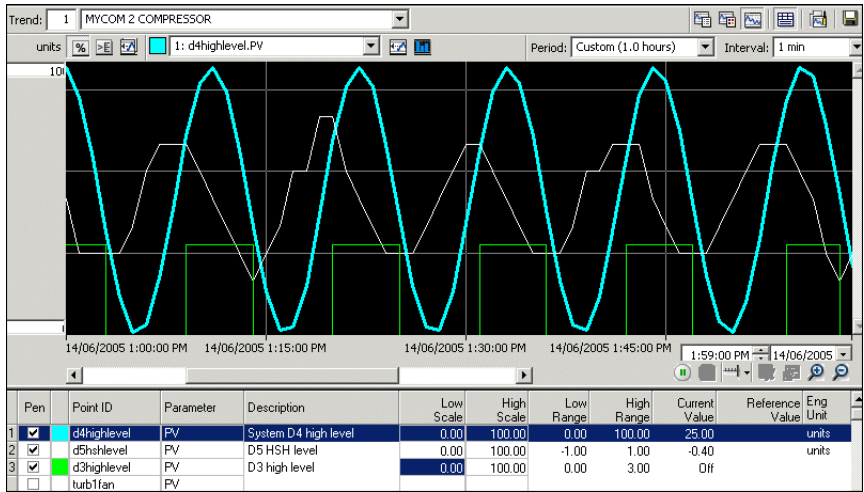
Trend types

The following types of trends can be configured:

Trend type	Description
Standard Trend	Displays historical data for up to 32 points as line graphs.
Dual Trend	Displays bar graphs of historical data for two points on separate charts.
Triple Trend	Displays bar graphs of historical data for up to three points on separate charts.
X-Y Plot	Used to display an X-Y plot of the historical data for two analog points with one point's values plotted against the others.

After the trend has been configured, there are several changes that can be made when you are viewing the trend. For more information on how you can change the trend, see “Changing trends” on page 370.

Figure 26 Trend display



Related display types

The Trend displays complement other types of displays that are used to view historical data:

Detail Trend display Accessible directly from a Point Detail display. It requires no configuration and shows a bar graph display of historical information for a single point.

Group Trend display	Accessible from a Group Detail display. Once the group itself is configured, no configuration of the Group Trend display is required. It gives a multi-plot trend of the points in the group. The points can be trended and controlled from the same display. This enables the downstream effect of point controls on cascaded functions to be observed on a single display.
Custom Trend display	Trends can be added to custom displays. For details, see the <i>HMIWeb Display Building Guide</i> .

Configuring a trend

Considerations

- You use a Trend Definition display to create a new trend, but trends can be modified directly from a Trend display. This makes it easy for operators to change the trend configuration interactively in order to analyze process history.
- By default, an operator can change the configuration of a trend while it is being displayed. To restrict the ability to change the points or parameters in a trend display, select the **MNGR or ENGR security level required to change traces** check box.
- To add a PHD tag to a trend, set the point ID to PHD and the parameter to the required PHD tag name. For more information about PHD, see “Integrating PHD” on page 801.
- PHD tag names are not listed in the Parameter list. Change the parameter to display as an alphanumeric so that you can type the PHD tag name in the parameter box.

To configure a new trend:

- 1 In the Configuration Explorer of Configuration Studio, click **Trends and Groups**.
- 2 Click the **Configure trends** task.
The Trend Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 In the Trend Summary display, click an empty title. This opens the Trend Configuration display.
- 4 In the **Title** box, type the name of the trend.
- 5 From the **Trend Type** list, select the type of trend you want to configure.
- 6 In the **Sample Interval** box, select the desired history interval from the list (for example, 1-minute snapshots, 6-minute averages, and so on).

- 7 In the **Duration** box, select the period for which you want to see data.
- 8 Select the **Multi-Range** check box if you want to set the range for each point individually.
- 9 Select the **Percent** check box if you want the scale to be shown as a percent. Clear the check box if you want the scale to be shown in engineering units.
- 10 In the **Trend Range** box, type the range you want to display. Note that this is for display only and does not affect the actual range of the point.
- 11 If you want to prevent operators from changing the configuration of the trend, select the **MNGR or ENGR security level required to change traces** check box.
- 12 Enter the point ID of each point you want to add to the trend.
- 13 From the **Parameter** list, select the point parameter to be trended for each point.
If you the parameter is not available in the list, select the **Alphanumeric** check box and type the parameter.
- 14 To show or hide the trend for a particular point, select or clear the check box for that point.
This can reduce the complexity if a particular trend is obscured.
- 15 In the **History offset** box, type the date and time if a history offset is required. Otherwise, you can leave the box blank.
- 16 Click **View Trend** to call up the Trend display in which you can change details interactively for this trend.

Figure 27 Trend Definition display

 Trends
2295
Tutorial Trend

Definition

Title:

Trend Type:

Sample Interval:

Duration:

Samples:

Trend range:

☐ Multi-Range
☒ Percent

☒ MINR or ENGR security level required to change traces

Point ID	Parameter	Description	Trend Range
☐	0001		0.00 100.00
☐	0002		0.00 100.00
☐	0003		0.00 100.00
☐	0004		0.00 100.00
☐	0005		0.00 100.00
☐	0006		0.00 100.00
☐	0007		0.00 100.00
☐	0008		0.00 100.00
☐	0009		0.00 100.00
☐	0010		0.00 100.00
☐	0011		0.00 100.00
☐	0012		0.00 100.00
☐	0013		0.00 100.00
☐	0014		0.00 100.00
☐	0015		0.00 100.00
☐	0016		0.00 100.00
☐	0017		0.00 100.00
☐	0018		0.00 100.00
☐	0019		0.00 100.00
☐	0020		0.00 100.00
☐	0021		0.00 100.00
☐	0022		0.00 100.00
☐	0023		0.00 100.00
☐	0024		0.00 100.00
☐	0025		0.00 100.00
☐	0026		0.00 100.00
☐	0027		0.00 100.00
☐	0028		0.00 100.00
☐	0029		0.00 100.00
☐	0030		0.00 100.00

Display Parameter: ☒ Comboxbox ☐ Alphanumeric

History

History offset:

[View Trend](#)

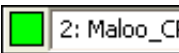
**Tip**

You can use the list in the Trend description box at the top of the Trend display to choose a different trend to view.

Changing trends

Trends are designed so an operator can change the way information is displayed directly in the Trend display.

When viewing trends in Station, use the various buttons on the display to change the trend. The following table describes the buttons that are available on the default trend:

Button	Description
	Individual scales in EU Scaling used in the trend is separate for each point and is in engineering units. Click the arrow to change the scale. For more information about scaling trends, see “Changing the scale on a trend” on page 372.
	Individual scales in % Scaling used in the trend is separate for each point and is shown as a percent. Click the arrow to change the scale. For more information about scaling trends, see “Changing the scale on a trend” on page 372.
	Single scale for all plots The range displayed on the Y-axis is the same for all plots. For more information about scaling trends, see “Changing the scale on a trend” on page 372.
	Selected Point Indicates the point that is currently selected. If you are not using a single scale for all plots, the Y-axis displays the scale for the selected point.
	Display as bar graph The selected point is displayed as a bar graph. Data for the remaining points is obscured by the bar graph. Click the arrow to change from a bar graph to a line graph.

Button	Description
	Display as line graph The plots are displays as line graphs. Click the arrow to change from a line graph to a bar graph.
	View single trend only Indicates the current view is a single trend without the event pane or the tabular history pane. Click the arrow to change the view to Trend with Events or Trend with Tabular History.
	View Trend with Tabular History Indicates the current view is the trend with the tabular history pane. Click the arrow to change the view to Single Trend Only or Trend with Events.
	View trend with events Indicates the current view is the trend with the event pane. Click the arrow to change the view to Single Trend Only or Trend with Tabular History.
	Show legend Shows or hides the legend for this trend.
	Configure trend Calls up the Trend Configuration display.
	Save trend Saves any changes you have made to the trend. After you save, the changes are made available to any other operators viewing the trend.
	Pause live updates Pauses the trend so that data is not updated. A trend is automatically paused when you zoom in and out.
	Resume live updates Restores the trend so that it is updated with live data.
	Remove reference line Removes the reference line.
	Reset zoom level Resets the zoom level.
	Zoom in Zooms in by 25% of the visible range. If a reference line is visible, the zooming is centered around the reference line.

Button	Description
	Zoom out Zooms out by 25% of the visible range. If a reference line is visible, the zooming is centered around the reference line.
	Show time selector Shows the time selector and provides options for the position of the time selector which is used to set a history offset.

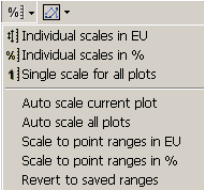
The changes you can make to a dual, triple, and X-Y trends are different to the changes available on the standard trend. The following list summarizes the changes you can make to a specialized trend:

- Switch between displaying units as engineering units or percentage
- Change the period
- Change the sample interval

Changing the scale on a trend

When viewing a standard trend, you can change the scale that is used for the trend. For example, you can switch from having a single scale for all plots as a percent to individual scales, in engineering units, for each plot. The following figure, Scale options for a standard trend, shows the scale options available in a list which you can access from the trend toolbar.

Figure 28 Scale options for a standard trend



The following table describes all the scale options available for a standard trend.

Scale option	Description
Individual scales in EU	You specify the maximum and minimum value that will be shown on the trend for each plot individually. Values that fall outside this scale are not visible in the trend. The scale is represented in engineering units.

Scale option	Description
Individual scales in %	You specify the maximum and minimum value that will be shown on the trend for each plot individually. Values that fall outside this scale are not visible in the trend. The scale represents the point parameter range in percentage terms. For example, if you specify the scale as 0% to 100%, the minimum value for the point parameter is expressed as 0% and the maximum value for the point parameter is expressed as 100%.
Single scale for all plots	One scale is used for all points in the trend. You specify the maximum and minimum value that will be shown on the trend. Values that fall outside this scale are not visible in the trend.
Auto scale current plot	Adjusts the selected plot so that it is centered vertically in the chart and scaled such that the plot uses most of the vertical chart space.
Auto scale all plots	Adjusts all plots that are currently visible so that they are centered vertically in the chart and scaled such that each plot uses most of the vertical chart space.
Scale to point ranges in EU	The scale is set so that it correlates with the maximum and minimum point parameter range of all points in the trend and is shown in engineering units.
Scale to point ranges in %	The scale is set so that it correlates with the maximum and minimum point parameter range of all points in the trend and is shown in percentage terms. The minimum point parameter value is always 0% and the maximum point parameter value is always 100%.
Revert to saved ranges	The scale options is restored to what was last saved for the trend. Any changes to the scale that were not saved are removed.

To specify an individual scale:

- 1 Call up the trend.
- 2 Click arrow on the scale toolbar button at the top of the trend.
The button shown depends on the type of scale currently in use for the trend.
- 3 Select the required individual scale.
- 4 In the **Low Scale** box on the legend, type the low scale value for each plot.
- 5 In the **High Scale** box on the legend, type the high scale value for each plot.

To specify a single scale:

- 1 Call up the trend.
- 2 Click arrow on the scale toolbar button at the top of the trend and select **Single scale for all plots**.
The button shown depends on the type of scale currently in use for the trend.
- 3 On the y-axis, type the low and high scale value.

Changing the period on a trend

When you are viewing a trend, you can change the period for the data you want to see. You specify the length of time for which you want to see data, then you specify the start and end time for the period in which you are interested.

You specify a period that either:

- Starts at a specific date and time by showing the time selector on the left.
- Ends at a specific date and time, by showing the time selector on the right.
- Starts and ends at a specific date and time by showing the time selector on the left and right.
- Is centered around a specific date and time by showing the time selector at the center.

To change the period for the trend you are viewing:

- 1 In the **Period** box, select the period you want to see on your trend.
- 2 Click the Time selector and choose the required position of the selector.
- 3 In the **Date** box, type or select the required date.
- 4 In the **Time** box, type the required time and press ENTER.

Example scenario

An incident occurred in your plant at around 11.00 A.M today. You want to see the values for a particular set of points for the hour preceding the incident and the hour following the incident.

Solution

- 1 Call up a Trend Configuration display and add the required points to the trend.
- 2 Click **View Trend**.
- 3 In the **Period** box, select 2 hours.
- 4 Click **Show Selector** and choose **Show Selector at center**.
- 5 In the **Date** box, type today's date.

- 6 In the **Time** box, type 11.00.00 AM and press Enter.



Tip

Click the **View trend with events** button to see events that occurred during this time.

Adding a reference line to a trend

By adding a reference line to your trend you can obtain values for a point at a specific point in time. If the Legend is visible, when you add a reference line, the legend contains the reference values for each point in the trend. You can also mouse over the plot when the reference line intersects the plot to obtain the reference value.

To add a reference line to a trend you are viewing:

- Click on the chart area of the trend.



Tip:

To move a reference line, drag the line to the required point. To remove the reference line, click the Remove reference line button.

Viewing events with a trend

You can add an Event Summary to your trend so that you can see events that occurred within the time range of your trend. This is useful for historical analysis and for real-time monitoring.

For historical analysis, viewing events with your trend can help you to investigate the cause of abnormal process events and analyze and improve the alarm system performance.

For real-time monitoring, viewing events with your trend can help you analyze the relationship between alarms and events and changes in point values in your trend.

After you add the events to your trend, you can filter events in the same manner as the standard Event Summary.

You should be aware of the following considerations when viewing events with your trend:

- If you have DSA, events from remote servers are not included.

- Events are not automatically filtered by the points that are included in the trend.
- For performance reasons, there is a maximum of 200 events displayed in the event bar.
- The trend save function does not save changes you make to the Event Summary, however, if you navigate away from the trend, any filtering, with the exception of date and time filters, is saved.

Example scenario

An area of your plant is generating an unusually high number of alarms. You want to understand what is causing this area of your plant to be unstable.

Solution

- 1 Call up a trend display for the area of your plant that is generating the alarms.
- 2 Click the **View trend with events** button.
The event summary is added underneath the trend.
- 3 The event summary shows several alarms occurred at the same time as values in the trend declined. To see this in more detail, zoom in on this area of the trend.
The trend is paused enabling you to analyze the data and the number of events in the summary is filtered.
- 4 To investigate variations in other parts of the plant, add the related points to the trend and filter the event summary to see events for assets related to this part of the plant.
- 5 If necessary, reduce the number of events in the summary by:
 - Filtering the events using the column filters.
 - Hide the pen for plots you do not want to view.
- 6 Save the trend.

Zooming in on a trend

If you want to focus on a particular part of your trend, you can use the zoom function to zoom in on the area of interest.

To zoom in on a trend:

- Using the mouse, drag over the area of interest.
As you drag, a rectangle shows the area you are selecting.



Tip

Alternatively, click the Zoom in button to zoom in at increments of 25%.

To zoom out on a trend:

- Click Reset Zoom to return to the original zoom level.



Tip

Alternatively, click the Zoom out button to zoom out at increments of 25%.

Saving your changes

If you make changes to the trend you are viewing, these changes are only visible to you. If other operators are viewing the same trend simultaneously, the changes you make are not visible to them.

You can save the changes you make to a trend. If you save the changes, these changes are then available to other operators who are viewing the trend simultaneously.

To save the changes to a trend:

- Click the Save button.

Calling up trend displays

In addition to the standard methods available to call up trends, it is also possible to configure other methods to call them up.

The following custom methods can be configured:

- A user-defined Station function key
- A push-button object on a custom display

For details on configuring user-defined function keys, see “Customizing toolbars, menus and keyboard shortcuts” on page 74. For details on configuring push buttons on custom displays, see the *Display Building Guide*.

Template displays and container points

18

A template display is a custom display that is used to represent a unit of equipment containing several points of one or more fixed types. A template display is functionally equivalent to the supplied Point Detail displays for status, analog, and accumulator points.

To use a template display, you first define a container point for the unit of equipment. The container point operates as a custom point type for a unit of equipment, such as a compressor or a door, that contains several points of one or more fixed types. For example, you might have a number of compressors that all contain:

- An analog point to monitor the pressure
- A status point to control the motor
- An accumulator point to monitor hours run

“Compressor” container points tie these sets of points together so that each set can be managed as a single point.

For information about how to define container points, see Quick Builder’s help. For information about building custom displays, see the *Display Building Guide*.



Attention

Template displays are different to generic displays. Generic displays are displays that can be reused across your plant where you have implemented an asset model that has a repeated asset structure. For more information about generic displays, see the topic, About generic displays, in the section, Creating displays, in the HMIWeb Display Building Guide.

Engineering guidelines for container points

Container points behave like fixed type points, with the following exceptions:

- Alarms raised on a contained point are not promoted to its container point. This means that a container point never goes into alarm, and therefore never appears on the Station Alarms display.
To ensure that operators can quickly recognize an alarm on a container point, you might:
 - Include the point ID of the container point in the description of all the points it contains.
 - Configure the Associated Display for all contained points as the template display specified for the container point.
- You cannot attach an algorithm to a container point.

Customizing alarm, alert, event and message summaries

19

This chapter describes how you can customize the Alarm, Event and Message summaries to suit your requirements.

About the summary displays

The default summary displays provide a scrollable list of all alarms, alerts, events and messages. The System Status display provides a scrollable list of system alarms. This can often be a large amount of information for an operator to view at one time.

Customizing the summaries enables you to organize the information to provide more useful summaries for operators. For example, you can customize the Alarm Summary to show only the urgent priority alarms for a particular asset.

You can customize a summary by:

- Filtering and sorting entries shown on the summary
- Changing the layout of the summary
- Showing or hiding the Location pane
- Showing or hiding the Details pane

You can save these settings as a view so that operators can reapply the customization when required.

You can apply security to the customization functions so that only operators with the appropriate security level are able to customize the summaries.

To learn about	Go to:
Filtering the summary displays	page 383
Sorting the summary displays	page 392
Customizing the layout of the summary displays	page 393
Creating views	page 394
Applying security to the customization functions	page 398

Filtering the summaries

Filtering the summary displays allows you to show or hide information according to filter criteria. Each of the summary displays have a set of filters available for some of the columns in the summary.

In addition to these column filters, you can create and apply custom filters to meet your specific criteria. You can also filter by selection.

The table below summarizes the filtering actions you can perform on the summary displays.

To	Do This
Filter by asset	Select the asset from the Location pane.
Filter by system component or node	Select the component or node from the Location pane. (Applicable to the System Status display only.)
Apply a filter saved in a predefined view	Select the view from the list of views.
Filter by column filter	Click the appropriate column heading and select the appropriate filter. For example, click the Date & Time column and select Yesterday to show entries for yesterday only.
Apply a custom filter	Click the column heading you want to filter by and select (custom filter). For more information see “Creating a custom filter” on page 390.
Filter by selection	Select the appropriate entry, click the column heading you want to filter by and select (like currently selected).

Filtering the Alarm Summary

You are provided with several filters that are saved in predefined views. These are:

- (unacknowledged alarms)—shows only unacknowledged alarms
- (urgent and high priority alarms)—shows only urgent and high alarms
- (urgent priority alarms)—shows only urgent alarms

The Alarm Summary contains column filters for the following columns:

- Alarm state
- Date & Time
- Priority

These filters are listed in the table below.

Alarm State	Date & Time	Priority
• Urgent • High • Low • Acknowledged • Unacknowledged • Active • Returned to normal	• Today • Yesterday • Current Shift • Previous Shift • Last 24 hours • This week • Last week	• Urgent • High • Low

The Category, Comments added, and the Video Link columns can be added to the Alarm Summary (using the column organizer) and contain the following filters:

Category	Comments Added	Video Link
• System Alarms • Process Alarms	• With Comments Added • Without Comments Added	• With Video Link • Without Video Link

Filtering system alarms from the Alarm Summary

The default Alarm Summary contains all alarms, including system alarms, which are also included on the System Status display. You can change the Alarm Summary so that system alarms are not included in the Alarm Summary.

To filter system alarms from the Alarm Summary:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm and event options** task.
The Server-wide Stations Settings display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm/Event** tab.
- 4 Clear the Show system alarms on process alarm summary check box.

Filtering the System Status display

The System Status display can be used to view system alarms as well as viewing the general status of items in the System components tree and items you have added to the Network tree.

By default, the System Status display lists all system alarms in the same manner as the Alarm Summary. The System Status display can be easily filtered using the Location pane to show the status of items in the Network tree and the System components tree.

If you choose not to use the Location pane, or there are many alarms for a particular item, you can use the filters that are saved in predefined views. These are:

- (unacknowledged alarms)—shows only unacknowledged system alarms
- (urgent and high priority alarms)—shows only urgent and high system alarms
- (urgent priority alarms)—shows only urgent system alarms

The System Status display contains column filters for the following columns:

- Alarm state
- Date & Time
- Priority

These filters are listed in the table below.

Alarm State	Date & Time	Priority
• Urgent • High • Low • Acknowledged • Unacknowledged • Active • Returned to normal	• Today • Yesterday • Current Shift • Previous Shift • Last 24 hours • This week • Last week	• Urgent • High • Low

The Category, Comments added, and the Video Link columns can be added to the System Status display (using the column organizer) and contain the following filters:

Category	Comments Added	Video Link
• System Alarms • Process Alarms	• With Comments Added • Without Comments Added	• With Video Link • Without Video Link

Filtering the Alert Summary

To filter the Alert Summary, you are provided with several filters that are saved in predefined views. These are:

- (all alerts)—shows all alerts
- (my private alerts)—shows alerts for which the current operator is the author
- (my private and public alerts)—shows alerts for which the current operator is the author, as well as any alerts marked as public

The Alert Summary contains filters for the following columns:

- Alert state
- Date & Time
- Author

These filters are listed in the following table.

Alert State	Date & Time	Author
• Acknowledged • Unacknowledged • Active • Returned to normal	• Today • Yesterday • Current Shift • Previous Shift • Last 24 hours • This week • Last week	• My Private and Public Alerts • My Private alerts

The Comments added column can be added to the System Status display (using the column organizer) and contains the following filters:

Comments Added
• With Comments Added • Without Comments Added

Filtering the Event Summary

Events are initially collected into a circular event file called the online event file. This file forms part of the real-time server database and is independent of the SQL Server event database. Every 30 seconds, events are copied from the online event file to the SQL event database, where events are stored permanently. As the online event file becomes full, the oldest events from the file are deleted to make room for new events. For performance reasons there is no sorting capability and only limited filtering capabilities when viewing events from the online event file. However, you can perform all filtering and sorting of events when viewing events that are stored in the SQL Server event database.

When viewing events from the online event file, you can only filter on the Location, Priority and Category columns. All other filter menus are disabled and you cannot sort on any columns. If you want to filter or sort on the other columns, you need to view events from the SQL Server event database by changing the Date and Time filter to something other than (all recent events - live).



Attention

The filtering and sorting restrictions are applicable to events viewed from the online event file only.

You are provided with two filters that are saved in predefined views. These are:

- (all recent events with live updates)—shows events as they are occurring with the newest event at the top of the summary. This is the default view and shows events from the online event file.
- (today's events snapshot)—shows all events that occurred today, up until the view was applied.

The Event Summary contains column filters for the following columns:

- Date & Time
- Priority

These filters are listed in the following table.

Date & Time	Priority
• (all recent events - live) • (custom filters) • Today (snapshot) • Yesterday • Last... • Last... • Last... • Last... • Last... • Last 7 days	• Urgent • High • Low • Journal

The (all recent events - live) Date and Time filter views events from the online event file and it provides live events update, which means it shows events as they are occurring. Apart from the (all recent events - live) Date & Time filter, all the other Date & Time filters view events from the SQL Server event database and they provide only a snapshot view of the events that occurred up until the view was applied.

The five Last... filters in the Date and Time column change depending on what day it is today. For example, if today is Wednesday, the Last... filters are:

- Last Monday
- Last Sunday
- Last Saturday
- Last Friday
- Last Thursday

The Category and the Video Link columns can be added to the Event Summary (using the column organizer) and contain the following filters:

Category	Video Link
• System Alarms • System Events • Process Alarms • Process Events • System Change Events • Operator Change Events • Batch Events • Process Alerts • Simple Alerts • Informational Messages • Confirmable messages	• With Video Link • Without Video Link

Filtering the Message Summary

You are provided with several filters that are saved in predefined views. These are:

- (all messages)—shows all messages
- (confirmable messages)—shows confirmable messages only
- (informational messages)—shows unacknowledged informational messages only

The Message Summary contains column filters for the following columns:

- Message State
- Date & Time
- Priority
- Category

The filters are listed in the following table.

Message State	Date & Time	Priority	Category
• Urgent • High • Low • Single Signature • Double Signature • Confirmable • Informational • Acknowledged • Unacknowledged	• Today • Yesterday • Current shift • Previous shift • Last 24 hours • This week • Last week	• Urgent • High • Low	• Information Messages • Confirmable Messages

Creating a custom filter

Creating a custom filter enables you to perform more advanced filtering.

Considerations

- You can filter on more than one column at a time.
- Filters are not case-sensitive.
- You can use wildcard characters in the filter criteria.

To create a custom filter:

- 1 Click the column heading you want to filter.
- 2 Select **(custom filter)**.
The **Custom filter** dialog box opens.
- 3 Specify the appropriate criteria for the column by which you are filtering.
- 4 Click **OK**.

Example Scenario

You want to filter the Alarm Summary so that it shows alarms only for the point called FLOW1.

Solution

- 1 Call up the Alarm Summary display
- 2 Click the Source column heading and select **(custom filter)**.
The **Custom filter** dialog box opens.

- 3 Select **Equals**.
- 4 Type in `FLOW1`.
- 5 Click **OK**.

The Alarm Summary shows any alarms for the point `FLOW1`.

About Time Stamps

The time stamp applied to an alarm or event depends on where it came from:

- If it came from a scan task, or is a system event, the time stamp is set when the alarm/event is generated on the server.
- If it came from a point server, then the time stamp is the time at which the point server received notification of the alarm/event from the controller.

If a controller supports the concept of field time, then the field time will more closely relate to the time of the actual event.

Sorting the summary displays

Sorting the summaries is another way of organizing the information. You can sort by any of the columns that are displayed in the summary. You can sort in ascending (0-9, A-Z) or descending order (9-0, Z-A).



Attention

You can only sort the by the Date & Time and Source columns on the Event Summary and only if you are not viewing the live events.

To sort by any column:

- 1 Click the column heading by which you want to sort.
- 2 Select the appropriate sort order. The column heading is highlighted to signify that the summary is sorted by that particular column.

Example Scenario

You want to sort the Event Summary so that the oldest events are shown at the top of the summary.

Solution

- 1 Call up the Event Summary display.
- 2 Click the **Date & Time** column.
- 3 Select **Ascending**.

The Event Summary is sorted by the Date & Time column, with the oldest events shown at the top of the summary.

Customizing the layout of the summary displays

Customizing the layout enables you to specify which items of information appear, and how they appear on the summary displays. You can then save the layout as a view, combined with any filtering and sorting, and reapply the view at a later time.

When you define the layout you can:

- Show or hide columns on the summary
- Resize columns
- Change the order in which columns appear from left to right

To	Do This
Hide columns	Open the Column Organizer and deselect the columns you want hide.
Change the order of the columns	Select the column and click Move Up or Move Down until the column is in the required position.
Resize columns	On the summary display place the mouse pointer on the right side of the column heading, click and drag until the column is the width you require.

Other settings, such as the date/time format and number of decimal places, are controlled by the computer’s regional settings. (To see or change the regional settings, select **Start Settings Control Panel** and then double-click **Regional and Language Options**.)

Creating a view

If you have customized the summary display and want to retain the customization, you can save the customized summary as a view. A view can contain information relating to:

- Filtering and sorting
- Column order
- Column width

Creating views enables operators to easily switch between the default summary and a customized summary without having to redo the customization each time.

Considerations

- Give your views a descriptive name so that operators have an idea of what is displayed in the summary. For example, Cooling Tower Urgent Alarms to indicate the view shows urgent alarms for the asset called Cooling Tower.
- You can restrict the access to view by assigning an asset to the view.

To create a view:

- 1 Click **Show Configuration Pane** .
- 2 If you have not already done so, customize the summary.
- 3 Type a name for the view in **Save current view as**.
- 4 If you want to assign an asset, select the **Asset** check box and type the asset name.
- 5 If you want to save the location filter as part of the view select the **Include location filter in view definition** check box.
- 6 Click **Save**.

Example Scenario

You want to customize the alarm summary as follows:

- Filtered to show alarms for the asset Pump_Station only
- Filtered to show urgent alarms only
- The Location tag column is not in the summary
- The Priority column is next to the alarm priority icons
- The Description column is widened

Solution

- 1 Click **Show Configuration Pane**.
- 2 Click **Show Location Pane**.
- 3 Select asset Pump_Station and hide the Location Pane.
- 4 Click **Show Column Organizer**.
- 5 Deselect the Location Tag column.
- 6 Select the Priority column and click **Move Up** until Priority is below the Alarm State Indication column.
- 7 Click **OK** to apply the changes and close the Column Organizer.
- 8 Place your mouse over the right side of the Description column heading. Click and drag until the column is the required width.
- 9 Type the name Pump Station Urgent Alarms in Save current view as.
- 10 Select the **Include location filter in view definition** check box.
- 11 Click **Save**.

The customization is now saved as a view called Pump Station Urgent Alarms. This view can be selected from the list of views at the top of the Alarm Summary.

When you have created your views, you can make them read-only to prevent others from saving changes to the view.

To make a view read-only:

- 1 Open Windows Explorer.
- 2 Navigate to Program Files\Honeywell\Experion PKS\server\data\views. The views for each of the summary displays are in separate subfolders. For example, views for the Event Summary are located in the events subfolder.
- 3 Open the appropriate subfolder. The views are saved as xml files.
- 4 Right-click the view you want to make read-only and select **Properties**.
- 5 On the General tab, select Read-only.
- 6 Click **OK**.

Changing the font size for the summary displays

Station supports the following resolutions for the summary displays:

- 1024 by 768
- 1280 by 1024
- 1600 by 1200

If you are using a high resolution, the text in the alarm summary may not appear large enough for operators to clearly read. To correct this, you can change the Windows font size. By default, Windows XP and Windows Server 2003 use the normal size font. The summary displays in Station can support the Windows large font.

Considerations

- You may need your Windows installation CD to copy fonts if you do not have the correct fonts on your computer.

To change the Windows font for Windows XP and Windows Server 2003:

- 1 Choose **Start > Control Panel**.
- 2 Double-click **Display**.
- 3 Click the **Settings** tab.
- 4 Click the **Advanced** button.
- 5 Select **Large size (120dpi)** from the **DPI setting** list.
- 6 Click **OK**.

Printing a summary as a report

As an alternative to requesting the preformatted alarm and event reports you can print a report directly from the Alarm, Alert, Event and Message Summary displays.

Printing a report directly from the summary provides you with the same data that is contained in the Summary retaining any filters and layout changes you have applied. If column widths are not wide enough to show text on one line, the text is continued on the next line. The icons that appear in the Alarm and Message Summaries are converted to text when the Summary is printed.

In addition to the data from the summary, the report contains other information such as:

- The date and time the report was requested.
- If you are using operator-based security, the operator ID of the operator requesting the report.
- If you are using Station-based security, the Station number where the report was requested.
- The filter and sort criteria.
- The name of the server where the data originates.
- A key to interpret the type of alarms and messages.

To enable printing the summary displays as reports, you need to configure a printer on each Station computer where the summary displays are printed. If there is more than one printer configured, the report is printed using the Windows default printer and using the settings for that printer.

Preventing operators from customizing the summary

If you do not want your operators to be able to customize or print the summary, you can set security levels to prevent operators from accessing these functions on the summary displays.

The Server Wide Settings display allows you to set the minimum security level required by an operator or Station to access the following functions:

- Full page acknowledgment
- Filtering and sorting
- Organize columns
- Save views
- Pause summaries
- Printing

To set the minimum security level:

- 1 Call up the **Server Wide Settings** display.
- 2 Click the Alarm/Event Options tab
- 3 Under Alarm, Event and Message Summary Restrictions, select the appropriate security level for each of the functions for which you want to restrict access.

Configuring reports

20

Experion reports provide a simple and flexible way to extract information from the server database.

This chapter begins with an introduction to the various types of reports used in Experion. It then describes how you call up a summary on reports and how you configure the reports (“Configuring reports” on page 403).

The reports that are available as part of Experion are pre-formatted reports that can be configured via Station displays (see “Report types” on page 400). You can also configure custom reports. Microsoft Excel and Free-format custom reports are available in Experion. This chapter also includes information on how to configure these report types.

Report types

Pre-formatted

You can choose from the following types of pre-formatted reports for retrieving information from the Experion server database.

Report type	Description
Alarm and Event	Alarm and event details from the event file. This report enables you to analyze alarms, alerts, and events that occurred during a specified time span on specific points. Excludes remote points. See “Alarm and Event reports” on page 409.
Alarm and Event DSA	Alarm and event details from other servers in the DSA. This report enables you to analyze alarms, alerts, and events that occurred during a specified time span on remote points. See “Alarm and Event DSA reports” on page 411.
Alarm Duration	The duration of alarms and events on nominated points during a nominated time span. Excludes remote points. See “Alarm Duration reports” on page 413.
Cross Reference	Where points are referenced in the server database. The report lists a range of references for the nominated points, including trends, algorithms and reports. Excludes remote points. See “Cross Reference reports” on page 415.
Point Attribute	Points that are in a specified state; for example, you can generate a report on all points that are off-scan, have alarms inhibited, have a bad PV, or are in manual mode. Excludes remote and flexible points. See “Point Attribute reports” on page 417.
Sequence of Events	Some types of controllers, such as the TDC 3000 PIU, have the capability to time-stamp events to millisecond resolution. When this capability is used, the server stores the high resolution event information in the server “sequence of events” file. The Sequence of Events Report is based on data extracted from this server file. Excludes remote points. See “Sequence of Events reports” on page 418.
Batch Reports	Batch reports are used to collect history for a set of points and events for an asset for the duration of a production run. See “Batch reports” on page 419.

Additional custom reports

Report type	Description
Microsoft Excel	This report type enables you to run a customized report created using Microsoft Excel. The server database can be accessed through the ODBC driver or Microsoft Excel Data Exchange. See “Microsoft Excel reports” on page 426.
Free Format	Free Format reports are only available with the Free Format Report Writer Option. This option enables you to design customized reports that can read and write from the server database.
ODBC Data Exchange	This option is only available if you are licensed for ODBC Data Exchange. This report enables the two-way exchange of data with local or remote SQL databases. Point value, point history and user file data can be exchanged.

How reports are used

After you have configured reports for your site, operators and other users can request these reports. Reports can be printed, viewed on a Station display, or saved in a file.

You can request a report from a configuration display by selecting the report you want from the Reports display then clicking the **Request** button on the Definition or Content tab. (If you want to know more about how operators can call up and request reports, see the *Operators Guide*.)

You can also configure reports to be requested:

- By selecting a button on a custom display. See the *Display Building Guide* for details.
- By pressing a function key. See “Customizing toolbars, menus and keyboard shortcuts” on page 74 for details.
- As a result of a process event. For more details, see the description of the Status Change Report Request algorithm in “Configuring algorithms” on page 235.

Configuring reports

Considerations

- The options on the Definition tab are the same for all report types; they are described in the section “Configuring definition details” on page 403.
- The options on the Content tab depend on the report type, and are discussed under a separate heading for each type. However the section, “Entering report content configuration details” on page 406 describes some data entry features that apply to content configuration for all report types.
- The fields sizes for reports that output event information can be configured on a server wide basis. See “Configuring field sizes” on page 408.
- The Scripting tab allows you to create scripts for reports. For more information on scripts see the *Server Scripting Reference*.

To add a report to your system:

- 1 In the Configuration Explorer of Configuration Studio, click **Reports**.
- 2 Click the **Define reports** task.
The Reports display appears in the System Display tab in Configuration Studio.
- 3 From the Reports display, click an empty report row in the display.
This Report configuration display opens.

Configuring definition details

The options in the Definition tab specify the general characteristics of the report. The following list shows all options that can appear in a definition. Not all options apply to all types of report.

Property	Description
Type	Select the report type you want from the drop down list. For a description of the report types see “Report types” on page 400.
Name	The name to be used when the report is requested by name. For example, you might want to use a more specific description such as “Shift1” for the report name. You can use a maximum of 10 characters. The name must be unique to this report and must not contain any spaces.

Property	Description
Title	The report title to be shown on the report output and the summary display. The title can be up to 70 characters. For example, you might want to use a general description such as “Alarm and Events Report for Asset AB” for the report title.
Request Program LRN	The LRN of an application program to be requested after the report is completed. LRNs are briefly described in “Server Display Program” on page 103. For more detailed information about LRNs and application programs, see the <i>Application Development Guide</i> .
Reporting on Request	
Enable Reporting on Request	Reporting on request means that operators and other users can run the report at any time they need it. To configure a report to be run on demand, select Enable reporting on request and complete the remaining options in that area of the display. When users request a report, they can view the report on screen at the Station they are using, and they can also request that the report be printed.
Destination	If you want to print the report to: • The report printer, select Station Default Printer. (To learn how to define the report printer, see “Printer Assignment” on page 114.) • A printer other than report printer, select it from the list. • Screen, select either: the first (empty) line in the list if a report printer has been defined, or Station Default Printer if a report printer has not been defined. • File, select a file type. The supported file types are text, MS Word, RTF, HTML, MS Excel 5, CSV and TSV. (Note that some file types may not support all the character sets and formatting options that are available if the report is printed or viewed on-line.)
Periodic Reporting	
Enable Periodic Reporting	Select this check box if you want the report to be run automatically at specified intervals.
Destination	Choose a printer for the periodic reports from the Destination list.
Next Report	The time and date that the report should run next.

Property	Description
Interval	To specify the frequency of periodic reporting, click the Interval list and select the desired interval. The interval can be: none, hour, shift, day, week, month, quarter or year. If you specify an interval, the server will calculate the next run time automatically. Every time the report runs, the next run time is recalculated. If this calculation gives a date that does not exist, the run time is set to the beginning (not necessarily the 1st) of the next month. For example, the next run time for a monthly report scheduled for 31-Feb is calculated as 3-March, because 31-Feb does not exist.
Security	If you want to ensure that only operators or Stations with a particular asset assigned can view or request the report, type the asset name. (For information about controlling system access, see “Configuring security and access” on page 281.)
Operator ID	To limit the assets from which data is reported, specify the ID of an operator who is assigned the assets you want to include. Operator ID does not apply to all reports, but when the option is visible you must specify an ID.

Report output

Even if they are sent to a printer, reports are also always written to a file. The file names used are:

\Program Files\Honeywell\Experion PKS\server\report\rpt nnn .htm

or for Crystal reports:

\Program Files\Honeywell\Experion PKS\server\report\rpt nnn .asp

where nnn is the report number

For example:

\Program Files\Honeywell\Experion PKS\server\report\rpt001.htm

Each time the report runs, it overwrites this output file using current data.

Operators can use the “pr” command to view and print an existing report through Station (for details, see the *Operators Guide*). Anyone who has access to Windows can view and print the file through Microsoft Internet Explorer.

Entering report content configuration details

This section describes some data entry features that apply to content configuration for all report types. See “Report types” on page 400 for a description of the report types.

Using wildcard characters to specify report data

A number of the Content tabs allow you to search for specific information. Since the general conditions for conducting a search are essentially the same for all these reports, the search procedure is described below.

Wildcard characters allow multiple items to be selected in a single field. Where indicated on reports, the ? and * wildcard characters can be used. In addition, most text entry fields support the use of wildcard characters, even though this may not be indicated on the report configuration display.

Wildcard Character	Description
?	Matches any single character.
*	Matches any sequence of zero or more characters.



Attention

- The ? character must match exactly one character.
- The character “?????????????” (16 question mark characters) matches only those points whose names are exactly sixteen characters long. To match all points in your database, use “*”. Some fields are blank for some records. A search on “*” will include these blank entries.
- To find only non-blank entries use “?*”.

For Example, LC?? would only match point ID LC34 but would not match LC, LC2 or LC123. (Note that you can also use the * wildcard character to match any string of characters.)

Specifying time periods for reporting

The Alarm/Event and Alarm Duration Reports and other similar reports all search the event file for required events during a specified time. For some of these reports, you must specify the start and end times for the report period. For others, you choose either a specific or a relative time period, and then type the time span in the appropriate format. This section explains how to define these time spans.

To define a specific time period:

- 1 Call up the Report Configuration Content tab.
- 2 Under Occurring, select the Between option.
- 3 In the Start time box type the start time in the format HH:MM and the start date in the format DD-MMM-YY. For example, 10:24 for 10:24 am and 14-Nov-02 for 14 November 2002. To specify the current date, leave the date blank.
- 4 In the End time box type the end time and end date.

To define a relative time period:

- 1 Call up the Report Configuration Content tab.
- 2 Under Occurring, select the In the last option.
- 3 Type the required number of days, hours or minutes prior to the current time. For example specifying 1 in the hours box and 30 in the minutes box means “from 1 hour and 30 minutes before the present time up to the present time”.

If you specify more than 24 hours, the number of days and hours is automatically calculated.

Changing the date format for reports

The reports use the default Windows date format. If you change the Windows date format, the you need to follow this procedure to ensure the reports are using the correct date format.

To change the date format:

- 1 Change the Windows date format as described in the Windows Online Help.
- 2 Open a Command Prompt window.
- 3 Type `\Program Files\Honeywell\Experion PKS\server\run\defaultdateutil.exe` and press ENTER.
- 4 Stop the Experion Server.
- 5 Restart the Experion Server.

Modifying report configuration details

If necessary, you can change report configuration details. For example, you can change the name of a report by typing in a new name in the **Title** box.



Attention

If you change the report type by making a new **Type** selection from the Definition tab, the report configuration details for the old report are erased.

Configuring field sizes

For reports that output event information, you can set the field sizes for certain fields in the report, on a server wide basis. The field sizes you can configure are:

- Source
- Description
- Value
- Operator
- Condition

Considerations

- If the data does not fit the field size, the data is truncated however a tilde (~) is *not* added to the field to indicate that it is truncated.

To configure field sizes:

- 1 Call up the **Report Configuration Summary** display.
- 2 Click the **Server Wide Report Configuration** link.
- 3 Type in values for each field size you want to configure.

Alarm and Event reports

Every alarm and event that occurs is saved in the SQL Server online event database for a configurable period, after which they are removed. The Alarm and Event report retrieves data from the SQL Server online event database.

If you have configured Event Archiving, events in the SQL Server online event database are archived according to a schedule you specify. Archived events can be restored to a playback area and are available for reporting.

You can also print the Alarm Summary and the Event Summary as a report directly from the summary displays. See “Printing a summary as a report” on page 397.

To configure an Alarm and Event report:

- 1 Click the **Definition** tab (see “Configuring definition details” on page 403), select **Alarm and Event** from the **Type** selection list, and specify the report definition details.
- 2 Click the **Content** tab.
- 3 Specify the types of alarms and events you want included in the report:

Property	Description
Alarm or Event type	Select the code for the alarm or event type you want included in the report. The types available are: • All—All alarms and events • Journal—Journal events only • Low—Low priority alarms only • High—High priority alarms only • Urgent—Urgent priority alarms only • Operator—Operator-initiated events For information about alarm priorities, see “Customizing alarm behavior” on page 249.
Assignable Asset	Type the tagname of the asset to include alarms and events for a specific asset only.
Source	Type a specific point ID or use wildcard characters to search for a number of points. For details of wildcard characters, see “Using wildcard characters to specify report data” on page 406.
Description	You can either type a specific event description or use wildcards to specify a number of event descriptions. For details of wildcard characters, see “Using wildcard characters to specify report data” on page 406.

Property	Description
Operator	For operator generated alarms and events, type the name of the operator or part of the name with wildcard characters.
Location	Select the location of the events to be searched for the report. The options are: • Online, to search the SQL Server online event database. • Playback, to search the SQL Server online event database and any archives that have been restored to the playback area.

- 4 Under **Occurring**, set your time period as described in “Specifying time periods for reporting” on page 406.
- 5 Under **Options**, select or clear the **Print field time** check box as required.
Print field time is not supported on all controllers. Where supported, it is used to include in the report printout, the time that the event took place in the controller.
- 6 Select **Check for tampering of event data returned from archives** to enable events to be checked for modifications or deletions.

Alarm and Event DSA reports

To configure a DSA Alarm and Event report:

- 1 Click the Definition tab (see “Configuring definition details” on page 403), select **Alarm and Event DSA** from the **Type** selection list, and specify the report definition details.
- 2 Click the **Content** tab.
- 3 Specify the types of alarms and events you want included in the report:

Property	Description
Source	Type a specific point ID or use wildcard characters to search for a number of points. For details of wildcard characters, see “Using wildcard characters to specify report data” on page 406.
Condition	Type the code for a specific alarm or event type you want included in the report. For example: ALARM ALARM OK
Operator	For operator generated alarms and events, type the name of the operator or part of the name with wildcard characters.
Priority	Select the alarm priority: • J—Journal • L—Low • H—High • U—Urgent Leave blank to specify alarms of every priority.
Sub-Priority	Select the alarm sub-priority, 0 - 15.
Description	You can either type a specific event description or use wildcards to specify a number of event descriptions. For details of wildcard characters, see “Using wildcard characters to specify report data” on page 406.
Location	Select the location of the events to be searched for the report. The options are: • Online, to search the SQL Server online event database. • Playback, to search the SQL Server online event database and any archives that have been restored to the playback area.

Property	Description
Check for tampering of event data returned from archives	If selected checks events for modifications or deletions.
Show user comments on alarms and events	If selected includes any user comments associated with an alarm or event.

- 4 Under **Occurring**, set your time period as described in “Specifying time periods for reporting” on page 406
- 5 Select the servers from which to report.

Alarm Duration reports

Alarm Duration reports show the duration of alarms that occurred during a particular time period.

To configure an Alarm Duration report:

- 1 Click the **Definition** tab (see “Configuring definition details” on page 403), select **Alarm Duration** from the **Type** selection list, and specify the report definition details.
- 2 Click the **Content** tab.
- 3 Specify the types of alarms and events you want included in the report.

Property	Description
Alarm/Event type	Use the Event type list to select the code for the event type you want included in the report. The options are: • All—All alarms and events • Journal—Journal events only • Low—Low priority alarms only • High—High priority alarms only • Urgent—Urgent priority alarms only
Assignable	Type the tagname of an asset to include alarms and events for a specific asset only.
Source	Type a specific point ID or use wildcard characters to search for a number of points. (See “Using wildcard characters to specify report data” on page 406.)
Description	Type a specific event description or use wildcards to specify a number of event descriptions. (See “Using wildcard characters to specify report data” on page 406.)
Location	Select the location of the events to be searched for the report. The options are: • Online, to search the SQL Server online event database. • Playback, to search the SQL Server online event database and any archives that have been restored to the playback area.

- 4 Specify the time span for the report, as described in “Specifying time periods for reporting” on page 406.
- 5 Select **Check for tampering of event data returned from archives** to enable events to be checked for modifications or deletions.

Cross Reference reports

The Cross Reference Report can be used to find where points have been referenced in the server database. It can be used to list the following types of references for the nominated points:

- Custom displays (numbered displays, but not named displays)
- Trends
- Algorithms
- Reports
- Source address for another point
- Application program point lists
- Schedules
- Group detail displays
- Remote subscribers
- History gating parameter of another point

To configure a Cross Reference report:

- 1 Click the **Definition** tab (see “Configuring definition details” on page 403), select **Cross Reference** from the **Type** selection list, and specify the report definition details.
- 2 Click the **Content** tab.
- 3 In the **Point ID(s)** box type the point ID you want to report on, or use wildcard characters to report on a number of points. (See “Using wildcard characters to specify report data” on page 406.)
- 4 If you want the report to include points that are not implemented in the database, select the **Report on unimplemented points** check box. For example, you might report on unimplemented points if you need to check whether any displays are still referencing a point that you have deleted.
- 5 Select the **Use Previous Cross Reference file** check box to use the cross reference file generated the last time the Cross Reference Report was run. If there have been no changes to the database since the last time you ran this report, you can save time by selecting this option.
If this option is not selected, the report examines the database and produces cross reference files which are then searched for the specified points.
- 6 Select the **Show all subscribed parameters on the specified points** check box if you want the report to list the parameters that are being subscribed to by remote subscribers.

Viewing used algorithm blocks

Running the Cross Reference Report produces a file that lists used algorithm blocks. The file is called `almap.rpt` and is located in the `Program Files\Honeywell\Experion PKS\server\report` folder. For example:

`Program Files\Honeywell\Experion PKS\server\report\almap.rpt`

Viewing cross reference errors

Any inconsistencies found in the database are recorded in the following file when the report is run. An error log is also generated at the end of the actual report file (`rptxxx.htm`):

`Program Files\Honeywell\Experion PKS\server\report\xrferror`

Point Attribute reports

Reports can be made of points with various attributes.

To configure a Point Attribute report:

- 1 Click the **Definition** tab (see “Configuring definition details” on page 403), select **Point Attribute** from the **Type** selection list, and enter the report definition details.
- 2 Click the **Content** tab.
- 3 In the **Point ID(s)** box, enter the point ID you want to report on or use wildcard characters to search for a number of points. (See “Using wildcard characters to specify report data” on page 406.)
- 4 Use the **Attribute** list to enter the appropriate code for the point attribute to be reported on. The available attributes are described in the next table.

Property	Description
Off-Scan	Reports on points that are “off-scan,” that is, points for which scanning is disabled
Alarm Inh	Reports on points for which alarming is inhibited
Bad PV	Reports on points whose PV value is bad
Manual MD	Reports on points in manual mode
State	Reports on status points in a particular state
Value	Reports on current point values, including PV, current alarm(s), OP, and MD
Alarm Attr	Reports on alarm configuration settings

- 5 If you are configuring this report for the first time you must enter your descriptor choices such as **Open**, **Alarm**, **Close** and **Normal** and so on in the **State Descriptor Choices** boxes.
A descriptor can be up to eight characters. If you enter a longer descriptor, it is truncated.
- 6 After descriptors have been configured in the **State Descriptor Choices** boxes, you can choose one of these descriptors from the **State List** on which to build a report.

Sequence of Events reports

Some types of controllers, such as the TDC 3000 PIU, have the capability to time-stamp events to millisecond resolution. When this capability is used, the server stores the high resolution event information in the server “sequence of events” file. You can configure the Sequence of Events report to list events from this server file for selected points during a selected time span.

To configure a Sequence of Events (SOE) report:

- 1 Click the Definition tab (see “Configuring definition details” on page 403), select **Sequence of Events** from the **Type** selection list, and specify the report definition details.
- 2 Click the **Content** tab.
- 3 In the **Point ID(s)** box, type the point ID you want to report on or use the wildcard characters to specify multiples points to be included in the report. (See “Using wildcard characters to specify report data” on page 406.)
- 4 Specify a time period as described in “Specifying time periods for reporting” on page 406.

Batch reports

Batch reports are used to collect history for a set of points and events for an asset for the duration of a production run.

A batch report can collect:

- One type of history sample (such as 5-second samples or 1-hour averages) for up to 50 points
- Events for one asset

Notes

- Each point included in a batch report must be configured to collect the type of history required by the report. For example, if the report requires 1-hour averages, each point must be configured to collect Standard history, which includes 1-hour averages.
- A batch report can collect up to 65000 history samples.
- Once started, a batch report continues to run until it is stopped. See “Starting and stopping a batch report” on page 424.
- A batch report generates a set of four files:
 - A text file that contains the history and event data
 - A Microsoft Excel file that contains the history and event data
 - A comma-delimited (csv) file that contains the history data
 - A comma-delimited (csv) file that contains the event data
- Batch reports are started/stopped by using LRN 178. See “Starting and stopping a batch report” on page 424.
- Batch report files are stored in Program Files\Honeywell\Experion PKS\server\report\batch, with their read-only attribute set. The filenames are as specified in “Batch report filenames” on page 423.

To configure a batch report:

- 1 Click the Definition tab (see “Configuring definition details” on page 403), select **Batch Report** from the **Type** selection list, and specify the report definition details.
- 2 Click the **Content** tab and configure the details as appropriate.

Property/Button	Description
Batch identifier	A user-defined property (such as a batch) that forms part of the report filenames each time the report is run. 20 characters maximum. (Because it forms part of a filename, it must not contain characters such as *, ?, \, and /.) “Batch report filenames” on page 423 describes how report filenames are generated.
Lot identifier	A user-defined property (such as a lot) that forms part of the report filenames each time the report is run. 20 characters maximum. (Because it forms part of a filename, it must not contain characters such as *, ?, \, and /.)
Size of production run	An information-only property that is included in the report’s header. An integer.
Number of pieces in run	An information-only property that is included in the report’s header. An integer.
Employee identifier	An information-only property that is included in the report’s header. 20 characters maximum.
Batch description	An information-only property that is included in the report’s header. 80 characters per line.
Product re-run	Specifies whether the last batch run needs to be re-run. If set to Yes, the Last sequence num value is re-used, and a re-run counter is used (which is incremented each time the Lot is run). The Re-run number forms part of the report filenames each time the report is run. If set to No, the re-run number is set to 0.
Historical point list	The name of the points list used by this report. (The list specifies the points/parameters whose history is included in the report.) To define the list, click Define Point Lists. See “Creating a points list” on page 422.
History type	The type of point history that is included in the report.
Events assignable asset	The asset for which events are recorded by the report.
Generate Excel file	When checked (the default), a Microsoft Excel Batch report (xls file) is generated. If you deselect the option the text and comma-delimited files are still generated.

Property/Button	Description
Status	Shows the current status of the report, which can be: • Ready - the report is not running. • working - the report is running. • Finishing - a complete batch report is being generated. • Error - the report has stopped because of an error.
Start time	The time/date when the report started.
End time	The time/date when the report competed. If Status is set to working , End time is replaced by Duration .
Duration	Only visible if the report is running. The length of time in days, hours, minutes and seconds that the current report has been running.
Current sequence num, or Last sequence num	Current sequence number is only displayed if the report is running. Indicates the sequence number that is currently being used. Last sequence number is only displayed if the report is not running. Indicates the sequence number that was used the last time the report was run.
Request	Calls up the report. If the report is running, the data available from the time the report started to the time of the request is displayed. If the report is not running, the last report that was run is displayed. If you want to start the report, see “Starting and stopping a batch report” on page 424.
Reset sequence num	Sets the value of Last/Current sequence num to 0.
Batch Report Filename	The report’s filename. If Product Re-run is set to Yes , the incremental re-run number is used. If the report is being run, the next partial report number is used.

Creating a points list

You use the Application Point List to define the set of points used in a batch report.

Note that every point on the list must be configured to collect the type of history required by the report. For example, if the report requires 1-hour averages, each point must configured to collect Standard history, which includes 1-hour averages.

To create a point list:

- 1 Choose **Configure > Application Development > Application Point Lists** to call up the Applications display.
- 2 Click an empty row to call up the Application Point List display.
- 3 Give the list an appropriate name, and add each point/parameter that you want to include in the batch report.

Figure 29 Typical application point list

System Configuration

General

System Hardware

Areas

Alarm & Event Management

Operator Security

History

Reports

Schedules

Trend & Group Displays

Acronyms

Applications

Application Development

- Applications (User Developed)
- Application Point Lists
- System Sinewave
- Task Timers
- Watchdog Timers
- Used Defined Data Formats

Server Scripting

Application Point List 1

Application Point List Description

	Point ID	Point Description	Parameter	History Offset
1	01COMP1LVL	GAS COMP 1 LEVEL	PV	0
2	01COMP2LVL	GAS COMP 2 LEVEL	PV	0
3	01COMP1PRES	GAS COMP 1 PRESS	PV	0
4	01COMP2PRES	GAS COMP 2 PRESS	PV	0
5				0
6				0
7				0
8				0
9				0
10				0
11				0
12				0
13				0
14				0
15				0
16				0
17				0
18				0
19				0
20				0

Batch report filenames

The filename of batch reports are defined as follow:

`Rptnnn-bBatchId-lLotId-sSeqNo-rReRun-pPartial.ext`

Part	Description
<i>nnn</i>	The report number, as shown in the Reports display.
<i>BatchId</i>	The Batch identifier specified for the report.
<i>LotId</i>	The Lot identifier specified for the report.
<i>SeqNo</i>	The report's sequence number, which contains three digits with leading zeros. (Corresponds to the Last/Current sequence num on the Definition tab for the report.)
<i>ReRun</i>	The report's re-run number, which contains 2 digits with leading zero.
<i>Partial</i>	The report's partial report number, which is incremented each time a report is requested while it is being run. Two digits with leading zeros. After the report has finished running, the number reverts to 00, and all partial reports from the same run are removed.
<i>ext</i>	Each report generates four files, which have the following extensions and contents: • <code>txt</code> - plain text • <code>hst.csv</code> - CSV file containing history data • <code>evt.csv</code> - CSV file containing event data • <code>xls</code> - Excel file containing the history and event data

Example

This example shows the four files that are created in Program Files\Honeywell\Experion PKS\server\report\batch after a report has been run.

```
rpt001-bA1N0458-1105-s005-r00-p00.txt
rpt001-bA1N0458-1105-s005-r00-p00.hst.csv
rpt001-bA1N0458-1105-s005-r00-p00.evt.csv
rpt001-bA1N0458-1105-s005-r00-p00.xls
```

The Program Files\Honeywell\Experion PKS\server\report folder also contains a copy of the text version (txt) of the report.

Starting and stopping a batch report

You use LRN 178 to start and stop the collection of data for a batch report. You can invoke LRN 178 in a number of ways, for example by requesting it via push button to a custom display, or by invoking it in a script or via action algorithm 71 (Queued Task Request).

This LRN uses the following parameters.

Parameter	
1	The number of the batch report for which you want to start/stop collecting data.
2	Specifies the required action, depending on its value: 1 = Starts the collection of data for the report. 2 = Stops the collection of data for the report and outputs the report. 3 = Stops the collection of data for the report, but doesn't output the report.

For the various methods of invoking LRN 178, the parameters are entered in differing fields. The table below lists the methods and the corresponding fields in which the parameters need to be entered.

Method	Enter Parameter 1 in:	Enter Parameter 2 in:
Pushbutton	Parameter 1	Parameter 1
Algo 69	Word 2	Word 3
Algo 71	Word 1	Word 2
Server script	Param1	Param2
Rqstsk	First word in buffer	Second word in buffer
Rqstkb	Param1	Param2

ODBC Data Exchange reports

The ODBC Data Exchange option enables you to configure the two-way exchange of data between the server database and an ODBC-compliant third-party database, using standard Structured Query Language (SQL) commands. This feature is available if your server license includes ODBC Data Exchange.

After the system is configured to include the ODBC Exchange option, you can use Station to configure report details in the same way as you configure pre-formatted reports. For complete information on how to configure an ODBC Exchange prior to reporting, see “Configuring the Experion ODBC driver” on page 639.

To configure an ODBC Data Exchange report on Station:

- 1 Configure the report definition, with Report type set to **ODBC Data Exchange** (see “Configuring definition details” on page 403).
- 2 When definition details are complete, click the **Content** tab. For information on what you can specify, see “Configuring ODBC Data Exchange Reports” on page 673.

Microsoft Excel reports

With Microsoft Excel Reports you can:

- Get values from point parameters
- Perform calculations on those points
- Retrieve historical data to determine summations, maximums, minimums, and standard deviations
- Retrieve alarms and events
- Generate graphs and tables
- Store new values or calculations in the server database, provided you installed Microsoft Excel Data Exchange with the “write” option enabled.

Microsoft Excel reports enable you to design a custom report in Microsoft Excel, which is configured and run from Station like other Experion reports. You can use Microsoft Excel Data Exchange or the Experion ODBC Driver to access data in the server database from Microsoft Excel. See “Using Experion data in other applications” on page 33 for further information on these. When the report runs this data is refreshed and a copy of the data is saved.



Attention

If you create a new spreadsheet for Integrated Microsoft Excel Reports prompts and error messages are not visible in Station. You need to open the new spreadsheet in Microsoft Excel using the **mng**r account before running the report in Station.

Choosing between Microsoft Excel Data Exchange and ODBC

Microsoft Excel Data Exchange is a licensable option for Experion, and the Experion ODBC driver is standard. Points to consider when choosing between Microsoft Excel Data Exchange and the ODBC Driver are:

- Microsoft Excel Data Exchange can access all information in the server database, the ODBC Driver can only access point, history, event, and some access control data.
- Microsoft Excel Data Exchange can write to the server database.
- The ODBC Driver follows the same security conventions as other reports, while Microsoft Excel Data Exchange has no security.

They have different installation requirements (for details, see the *Software Installation and Upgrade Guide*).

Creating custom reports with Microsoft Excel

To create a Microsoft Excel report you need to:

- Create a report definition file to define the data that the report will contain.
- Configure the report on Station to specify when and how your report will be run.

Creating the report definition file

A report definition file is an Microsoft Excel file that is set up to access and process data from the server database. There are two ways to access data in the server database—through Microsoft Excel Data Exchange or the Experion ODBC Driver.

Inserting server data into your report

Data you can access using Microsoft Excel Reports includes:

- Point parameter values and history data
- Alarms and events
- Other data in any server or system files

To insert server data into your report, set up either Microsoft Excel Data Exchange functions or ODBC queries that access the server database. You can then set up calculations and graphs that use the data in your report file.

When the report is run:

- All functions and queries contained within the report definition file are executed, updating the data in the report.
- Any calculations or graphs in the report are refreshed.
- The data in the report definition file is saved as a Microsoft Excel file in the Experion report folder. All links, formulas, and ODBC queries are removed in the report output—it becomes a snapshot of the data in the file at the time the report was requested. This prevents report data from being subsequently refreshed. The report file is named `rptnnn.xls`, where `nnn` is the number of the report. A `rptnnn.htm` file is also generated, to enable viewing of the report from Station.
- The report can be printed. Printing uses the printer settings configured on Microsoft Excel and sent to the printer configured on Station.

See “Using Experion data in other applications” on page 33 for details of the data you can access via Microsoft Excel Data Exchange or the ODBC Driver and how to access it.



Attention

Do not create a report that will require users to respond to a prompt. Microsoft Excel is not visible when the report is run. If the report requires a response it will either hang or fail.

Before you make a spreadsheet available as an integrated Microsoft Excel report, open it at least once with **mng**r level security. As **mng**r you can see Microsoft Excel messages and prompts that are not visible at other security levels.

Saving the report definition file

Save the report definition file in a folder which is visible from the server. This may be over a network.

On redundant server systems the report definition file must be saved in the same folder on both servers (For example, Program Files\Honeywell\Experion PKS\server\user). To automatically back up the definition, add the folder containing the files to the file f1kbup.def, located in the data folder. See “Synchronizing other files” on page 489 for details on using f1kbup.def to transfer non-database files to the backup.

Security issues

There are two ways for an Microsoft Excel Report to access data from the database: via Microsoft Excel Data Exchange, or via the Experion ODBC driver.

The security of data fetched via the ODBC driver will depend on the type of report.

- For reports requested on Stations with operator-based security, the ODBC Driver uses the access capacity of the requesting operator.
- For reports requested on Stations without operator-based security on the ODBC Driver uses Station security.
- For Periodic reports there is no security.

If a report requests data that is not accessible to the requesting operator or Station then the ODBC Driver will not return the data.

Microsoft Excel Data Exchange, in conjunction with a Microsoft Excel Reporting, provides no operator authentication or other security measure. It is recommended that Microsoft Excel Data Exchange be installed with read-only capacity.

Configuring the Microsoft Excel report details

Microsoft Excel reports, like other Experion reports, need to be configured on Station. This is done on the Microsoft Excel Report Configuration display.

To configure an Microsoft Excel report:

- 1 Click the Definition tab (see “Configuring definition details” on page 403) and specify the report definition details.
- 2 Select Microsoft Excel from the **Type** selection list.
- 3 Click the **Content** tab.
- 4 In the **Definition File** box, type the full path name of the report definition file.

Example

Using Microsoft Excel reports with Microsoft Excel Data Exchange.

This example leads you through the steps involved in producing an Microsoft Excel report which uses Microsoft Excel Data Exchange to access the server database. It assumes that you have already completed the installation of your Experion system. In particular that you have:

- Installed Microsoft Excel and Microsoft Query on the server.
- Enabled Microsoft Excel Data Exchange on the server using the Windows `mng` account (see “Enabling Microsoft Excel Data Exchange under different user accounts” on page 776).
- Disabled the **Ask to update automatic links** prompt on Microsoft Excel.

This report retrieves the last 20 history values of a system sinewave point. Before continuing, configure a system sinewave point, called *sinewave*, and assign it to fast history. For details on how to do this see “Using Experion ODBC driver and Microsoft Access” on page 661.

Creating the Microsoft Excel report definition file

To create a report definition file which retrieves the last 20 fast history values of the point ID “sinewave”:

- 1 Log on using the `mng` user account.
- 2 Start Microsoft Excel.
- 3 Choose **Tools > Microsoft Excel Data Exchange > Wizard**.
- 4 Select **Get history values from server(s)** and click **Next**.

- 5 Set the options as follows:
 - **Server:** localhost
 - **Point ID:** sinewave
 - **Point parameter:** pv
- 6 Click **Add**, then **Next** to display the next step.
- 7 Set the options as follows:
 - **history type:** Fast History Snapshots
 - **number of values:** 20
 - **offset:** 1
 - **Arrange data:** vertically
 - for all other options accept the default.
- 8 Click **Finish** to display the result.
- 9 To include the date-time at the which the report is run, select an empty cell and type **Now()**.

Saving the report definition file

To save the report definition file:

- 1 In Microsoft Excel choose **File > Save As**.
- 2 Browse to the Program Files\Honeywell\Experion PKS\server\user folder and type **sinewave** as the filename.
- 3 Click **OK** and Exit Microsoft Excel.

Configuring the Microsoft Excel report in Station

Considerations

- If you have a report definition file that was created by a user account other than mngr, you need to:
 - a. Ensure you are logged on to Windows as **mngr**.
 - b. Open the workbook in Microsoft Excel.
 - c. Choose **Tools > Microsoft Excel Data Exchange > Update Formulas in Workbook**.
 - d. Save the workbook.

To configure the report in Station:

- 1 Start Station and log on at mngr security level.
 - 2 Choose **Configure > Reports**. This opens the Reports display (see “Configuring reports” on page 403).
 - 3 Go to an unassigned report row and click the **Configure** button.
 - 4 In the Definition tab, complete the following:
 - add a title and a name
 - select Microsoft Excel from the **Report type** list.
 - enable reporting on request
 - 5 Click the **Content** tab.
 - 6 Type the full path to the file, sinewave.xls, saved above. For example, *c:\Program Files\Honeywell\Experion PKS\server\user\sinewave.xls* where *c* is the drive where you saved the file (see Saving the report definition file).
-

Configuring Free Format Reports

This section provides overview information about the Free Format Report. It shows how you use Station to configure a custom report and describes the components of a Report Definition file.

For detailed information about the structure of a Report Definition file and the variables used, see “Free Format report reference” on page 434.

Free format reports

Free format reports are only available with the Free Format Report Writer option.

You can use the Free Format Report Writer option to create and format customized reports. These custom reports can include information from calculated values as well as data extracted from the server database.

Free Format reports can also be used to write information back to the server database, and can be used instead of application software for simple applications.

If you are using the Free Format Report Writer option, you can create custom reports that:

- Get values from point parameters
- Perform calculations on those values (for example, addition, subtraction, multiplication, division, and exponentiation)
- Retrieve historical data to determine summations, maximums, minimums, and standard deviations
- Generate an X-Y plot of the historical values for two points
- Store new values or calculations in the server database or in operating system files

Creating a report definition file

To create a report definition file, you can use any text editor supported by Windows.

When a Free Format report is run, the report definition file is read and a report based on the contents and format defined in this file is generated.

For details of the structure, contents and variables of Free Format Report definition files, see “Free Format report reference” on page 434.

Saving report definition files

Report definition files can be given any name, and should be saved in the following path:

Program Files\Honeywell\Experion PKS\server\user

Configuring the report details

After creating the definition for the Free Format Report, you need to configure it via the Reports display on a Station just like any other Experion report.

To configure a Free Format report:

- 1 Click the **Definition** tab (see “Configuring definition details” on page 403) and specify the report definition details.
- 2 Select **Free Format** from the **Type** selection list.
- 3 Click the **Content** tab.
- 4 In the **Definition File Path** box, type the path and file name.
For detail on creating a Definition File, see “Structure of a report definition file” on page 434.

If the data in your report does not fit within the width of a portrait page, change the page orientation to landscape. Log on to Windows using the Windows mngr account and change the orientation in the Windows Printing Preferences to landscape.

Free Format report reference

This section gives details about the structure and contents of a Free Format Report. It contains:

- Information about the structure of a Free Format Report definition file and how it should be stored
- A description of report variables by function
- An alphabetical listing and detailed description of variables
- An example of a Free Format Report definition file and its output

Structure of a report definition file

To create a report definition file, you can use any text editor supported by Windows.

A report definition file is a text file that is made up of two sections:

Variable definition	This section defines the variables and gives them values that will be used in the report.
Formatting	This section defines how the data that is generated via the variable definition section is to be presented in the report output.

When a Free Format report is run, it reads the report definition file and produces a report based on the entries in this file.

Variable definition section

There are 14 different types of entries you can use in creating variable definitions. Entries consist of one line starting with either:

- An alphabetic character representing a variable definition (instruction), or
- An asterisk representing a comment line.

The different types of variable definition entries and their parameters are listed in “Variable definitions by functions” on page 435.

Within a variable definition line:

- The fields must be space or tab-separated.
- Index numbers can be used to identify variables.

A variable is one item of information (such as a temperature) stored in a point parameter. A variable can contain:

- Point values (including historical data)
- Values from server database files and regular operating system files
- Calculated values

You can include up to 999 variables in a definition file. Of these variables, a maximum of 400 can be character variables (ASCII).

Example

The following lines are an excerpt from a variable definition file, showing a comment line and a variable definition entry:

```
*   Get the Point ID
F   1 01IT1LEVEL NAME   A10
```

In this example, the variable definition line represents an instruction to:

“F(etch) the value of the point whose point ID is 01IT1LEVEL and whose parameter is NAME and store the value in index 1, using an ASCII 10-character format.”

Formatting section

The formatting section follows the variable definition section. This section refers to the variables you defined in the variable definition section.

The layout for the report output is specified in a WYSIWYG (what-you-see-is-what-you-get) format. This includes headings, outlines and spacing.

Free format reports can be a maximum of 132 columns wide.

Detailed information about formatting options is given in “Formatting the report output” on page 438 and in “B (Start of Report Body)” on page 441.

Saving report definition files

Report definition files should be saved in the Program Files\Honeywell\Experion PKS\server\user folder or a folder under it. The file can be given any name.

Variable definitions by functions

This section groups Free Format Report variables according to the type of function they perform. For a detailed description of each variable and some examples, see “Free Format variables reference” on page 439.

Using point values

The most common values used in custom reports are point values.

Reading a point parameter from the server database

Three report definition file entries are provided for reading and writing points values:

Entry	Description
F = Fetch from point	Reads a specified point parameter into a Free Format variable. The format to be used when the variable is printed in the report can be specified. When reading history parameters, it is also possible to read multiple history values into successive Free Format variables at once by specifying an offset into the history file and the number of history samples.
A = Acquire field value	Is identical to “fetch from point” except that the point parameter is scanned from the field before reading the value. This entry is used to obtain an up-to-date field value if required.
X = Demand point processing	Is identical to “acquire field value” except that processing of the point is forced regardless of whether or not the point value has changed. This entry is used to force any algorithms attached to the point to be executed.

Storing values in point parameters

There is one entry for storing values in the point parameters:

Entry	Description
G=“Give to Point”	Stores a value in a Free Format variable in the specified point parameter.

Performing calculations

Two entries are provided so that calculations can be performed with Free Format variables:

Entry	Description
C = Calculated Variable Definition	Used to specify the print format to be used for the Free Format variable that is the result of the calculation.

Entry	Description
P = Perform Calculation	Used to specify the expression for a calculation on several Free Format variables. Addition, subtraction, multiplication, division and exponentiation operations can be performed.

Working with historical data

In addition to the entries provided for reading history data for points (see “Using point values” on page 436), Free Format entries are provided for history data calculations:

Entry	Description
T = Totalize history	Enables history values for a point to be read from the database and totalized. The total is stored in the specified Free Format variable. The format used when the variable is printed in the report can be specified.
L = History maximum/minimum	Enables the maximum and minimum history values for a point to be determined and stored into two successive Free Format variables.
D = History standard deviation	Enables the standard deviation to be determined for history values for a point and then stored in a Free Format variable.

Using server database and operating system file values

The server database consists of a number of files including “user files” that are provided for use by application programs. (For details about the server database and user files, see the *Application Development Guide*.)

Free Format report entries are provided to read values from and write values to server database files. Values can also be read from operating system files.

Entry	Description
M = Operating system file definition	Provided to specify the details about an operating system file to be accessed. It enables the record size and path name of the file to be specified.
R = Read from file	Provided to read a value from a server database file or operating system file into a Free Format report variable. To read from an operating system file the file must first be defined with the entry, M, Operating system file definition.
W = Write to file	Provided to write a value from a Free Format report variable into a server database file.

Formatting the report output

Entry	Description
B = Start of report body	Used at the end of the variable definition section to indicate the start of the formatting section of the report. Any lines following this entry will be included in the report output. They are used to specify the layout of the report including headings and spacing.

Specify any sections of the report output that are to contain values from Free Format report variables by enclosing the variable index number in single quotation marks.

Special characters can be added for spacing lines and forcing page breaks.

Lines can be repeated. Free Format variable index numbers can be incremented within repeated lines.

An operating system text file can be copied directly into the report. To include an operating system file, first define the file with the 'Operating System File Definition' entry in the variable definition section.

An X-Y plot of history samples for a point can be plotted. The history samples need to have been previously read from the database using the 'F = Fetch from point' entry in the variable definition section.

Free Format variables reference

This section contains details about each of the Free Format Report Definition file entries.

- A (Acquired Field Value)
- B (Start of Report Body)
- C (Calculated Variable Definition)
- D (History Standard Deviation)
- F (Fetch From Point)
- G (Give to Point)
- L (History Maximum and Minimum)
- M (Operating System File Definition)
- P (Perform Calculation)
- R (Read From File)
- T (Totalize History)
- W (Write to File)
- X (Demand Point Processing)

A (Acquired Field Value)

Purpose

Scans a point parameter value before storing it in a Free Format variable. Otherwise this entry is identical to the F (Fetch from point) entry.

Format

A Index *Point_ID* *Parameter* *Print_Format*

Description

Index	Number (1-999) identifying report variable to store value acquired from field.
<i>Point_ID</i>	Point name
<i>Parameter</i>	As described for entry type F. History parameters are not enabled.
<i>Print_Format</i>	As described for entry type F.

See Also:

Entries F, G, and X

B (Start of Report Body)

Format

B

Description

This entry is the last in the variable definition section. Lines that follow this entry specify report layout, including: headings, outlines and spacing.

Areas to contain variable information are identified by single quotation marks enclosing the index number of the Free Format variable. The width of the field that will print equals the number of characters entered between (and including) the quotation marks. It is not dependent on the format specified in the 'Print_Format' entry. For example, if the value 13645.23 is stored at index 7 and you type '_7____' (only four additional spaces for a total 7 character width) for the variable, an error will result. The field will be filled with "*"s.

Errors in a field (for example, "bad" values; "Point does not exist" and so on), will cause a single asterisk (*) to be printed immediately after the field, ".."*. For this reason, it is recommended to leave a space following each field to accommodate possible error conditions.

Lines are single-spaced unless spacing characters are found in column 1.

- : leave 1 blank line
- / skip to head of next page

Lines can be repeated in the following way, starting in column 1.

\$RRII...

where:

\$	Shows repeat requested
RR	Is the number of times a line must be repeated. Can be an index I\$RRII.
II	Is the index increment for each line
...	Is the layout of the line

An operating system file can be copied into the body of the report using the following command, starting in column 1.

\$Cnnn

where:

nnn	Is the index number (501-599) of a user defined sequential file previously defined using the M entry

An X-Y plot of two arrays of values can be output in the body of the report using the following command, starting in column 1.

```
$XY Xindex Yindex Num Xmin Xmax Ymin Ymax
```

where:

Xindex	The first element in array for x-axis variable.
Yindex	The first element in array for y-axis variable
Num	The number of samples to plot
Xmin	x-axis minimum
Xmax	x-axis maximum
Ymin	y-axis minimum
Ymax	y-axis maximum



Attention

Points with co-ordinates equal to the x-axis minimum or maximum will not be plotted.

C (Calculated Variable Definition)

Purpose

Specifies the print format for the Free Format variable containing the result of a calculation. This entry is always used together with the P (Perform calculation) entry and may come before or after it.

Format

C Index Print_Format

Description

<i>Index</i>	Number (1-999) identifying report variable to store result of calculation.
<i>Print_Format</i>	As described for entry type F.

See Also:

Entry P.

D (History Standard Deviation)

Purpose

Used to calculate the standard deviation of history values of a point and to store the standard deviation in a Free Format variable.

Format

D *Index Point_ID Parameter Print_Format [History Type(Offset)
Repeat]*

Description

<i>Index</i>	The number (1-999) identifying report variable to store standard deviation.
<i>Point_ID</i>	Point name of the analog point.
<i>Parameter</i>	As described for entry type F. Only history parameters are permitted.
<i>Print_Format</i>	As described for entry type F.
<i>[History Type],[Offset], [Repeat]</i>	As described for entry type F.

Example

D 2 SINEWAVE PV F8.2 H6M(10) 5

In the above example, five values of “6 minute history” for Point SINEWAVE (offset 14 to offset 10) are retrieved. The standard deviation of these values is stored in Index 2 and printed as a floating point number.

See Also:

Entries L and T.

F (Fetch From Point)

Purpose

Reads a point parameter value and stores it in a Free Format variable. Multiple point history values can be read into successive free format variables.

Format

*F Index Point_ID Parameter Print_Format [History Type (Offset)
Repeat]*

Description

Index

The number (1-999) identifying the start of the report variable in which to store the history value fetched. The first value fetched is the most recent history value.

Point_ID

The point name.

Parameter

Any valid parameter name can be entered. Experion Process Controller parameters can be entered in the form <block>.<parameter>. For example, PIDA.PV.

The names of commonly used point parameters are:

Parameter	ANA	STA	ACC
PV Process Variable	x	x	x
MD Mode	x	x	
OP Output	x	x	
SP Set Point	x		
A1 Auxiliary 1	x		
A2 Auxiliary 2	x		
A3 Auxiliary 3	x		
A4 Auxiliary 4	x		
EULO 0% Range	x	x	
EUHI 100% Range	x	x	

(For a list of standard point parameters, see “Summary of standard point parameters and addresses” on page 174.)

Print_Format

“FORTRAN” style format descriptors:

In	Integer
Zn	Short integer in hexadecimal notation
Fn.m	Floating point
En.m	Floating point in exponential form
An	ASCII
D	Date (DD-MMM-YY) integer date is in minutes
T	Time (HH:MM:SS) real data is in seconds

where:

n Is the width of the field and m is the number of decimal places.

When accessing status points, the PV or OP can be expressed as a state descriptor by specifying the print format as:

Sn State descriptor of length n characters.

[History Type]

Can be one of:

Type	Description
H1M	History Standard 1 minute snapshot
H6M	History Standard 6 minute snapshot
H1H	History Standard 1 hour average
H8H	History Standard 8 hour average
H24H	History Standard 24 hour average
H5SF	History Fast snapshot
H1HE	History Extended 1 hour snapshot
H8HE	History Extended 8 hour snapshot
H24HE	History Extended 24 hour snapshot

[Offset]

This is the offset within the history file. It locates the required value in the history file. For example:

- (1) Start from most recent value
- (10) Start from 10th most recent value

An index number may be used as the offset, for example, “\$2”.

[Repeat]

This number of history values will be retrieved starting from the offset and going back in time. An index number may be used in the Repeat, for example, “\$3”.

Notes

- The Offset and Repeat fields are only required for history parameters (for example, H1M). They should be left blank if a non-history parameter (for example, PV) is specified.
- Entry type F assigns index numbers to the fetched history values by incrementing from the index number specified. For details, see Example 1 below.

Examples**Example 1:**

```
F    2 FIC123    PV    F8.2    H6M(10)    3
```

In this example, “6 minute history” is required. The starting index is 2. The offset is 10 and the repeat value is 3. The history values are reported in floating point format.

Therefore:

- The 10th most recent value will be index no 2.
- The 11th most recent value will be index no 3.
- The 12th most recent value will be index no 4.

Example 2:

```
F    6 FIC123    PV    D6    H6M(10)    3
```

In this example, the date of the history values retrieved in Example 1 will be obtained. They will be stored in indexes 6, 7 and 8. The format of the date will be DD-MMM.

Example 3:

```
F    5 FIC123    PV    F8.2
```

In this example, the value of the PV of point FIC123 is fetched from the database and stored in Index number 5.

Example 4:

```
F   20 FIC123    PV    F8.2    H6M($10)    3
```

In this example, the value stored in index 10 is used as the history offset.

Example 5:

```
F 20 FIC123 PIDA.PV F8.3 H1M(1) 10
```

In this example the last 10 samples of 1 minute standard history for the parameter PIDA.PV of point FIC123 are fetched.

See Also:

Entries A, G, and X.

G (Give to Point)

Purpose

Stores the value in a Free Format variable in a point parameter. A control will be performed for point parameters with destination addresses.

Format

G Index Point_ID Parameter

Description

<i>Index</i>	The variable containing the value to be stored; this variable must have previously been initialized.
<i>Point_ID</i> and <i>Parameter</i>	As described for entry type F. History parameters are not supported.

See Also:

Entries A, F, and X.

L (History Maximum and Minimum)

Purpose

The maximum and minimum history values of a point are stored in two successive free format variables.

Format

```
L Index Point_ID Parameter Print_Format [History  
Type(Offset) Repeat]
```

Description

<i>Index</i>	The number (1-999) identifying the report variable to store the total.
<i>Point_ID</i>	The point name of the analog point.
<i>Parameter</i>	As described for entry type F.
<i>Print_Format</i>	As described for entry type F.
[History Type], [Offset], [Repeat]	As described for entry type F.

Example

```
L 2 SINEWAVE PV F8.2 H6M(10) 5
```

In this example, 5 values of “6-minute history” for point SINEWAVE (offset 10 to offset 14) are retrieved. The maximum and minimum values are stored in Index 2 and 3 respectively and printed as floating point numbers.

See Also:

Entries T and D.

M (Operating System File Definition)

Purpose

Defines the details about an operating system file to be accessed by the R (Read from file) or W (Write to file) entries.

Format

M SEQ No Rec_sz Path

Description

SEQ	SEQ for sequential file.
No	Internal file number (501-599) used for file identification within the Free-Format report.
Rec_sz	Record size in bytes.
Path	File name (and path) for example, Program Files\Honeywell\Experion PKS\server\user\dlyacc.dta. If a new file is to be used, it must first be created.

Notes

- If the file is to be accessed by a FORTRAN program using standard READ/ WRITE then the first element of data is stored at word offset three (if the file is relative).
- A sequential file (xxx) is copied onto a scratch file (xxx.REL) for READ/ WRITE. Therefore a file with this name must not already exist.
- The length of the name of a sequential file should be four characters less than that of the longest file name.

See Also:

Entries R and W.

P (Perform Calculation)

Purpose

Specifies a calculation to be performed. The result of the calculation is stored in a free format variable. This entry is always used together with the C (Calculated Variable Definition) entry and may come before or after it.

Format

P Index Expression

Description

Index

The number (1-999) identifying report variable to store result of calculation.

Expression

Free-Format expression

The expression can be composed of index numbers, (denoted by a “\$” meta-character), constants, and any combination of the operators:

+ add
- subtract
/ divide
* multiply
^ exponentiate
= equate
() brackets

Example

P 22 = \$27+\$99*0.75/(\$32+5)

Where:

\$27, \$99 and \$32 are index numbers 27, 99 and 32 respectively.

Notes

- The expression is terminated with a blank (space) or a “.” character. A maximum of 10 operations may be performed on one line.
- Calculations are done to the highest precision and rounded to the desired print format. This can result in the following situation:

123.0
123.0
TOTAL 246.1

R (Read From File)

Purpose

Used to read a value from either an operating system file or a server database file. If the value is to be read from an operating system file the M entry should be used to define the details about the file.

Format

R Index No Rec_No Offset Print_Format Type [Read]

Description

Index

Number (1-999) identifying variable to store value read from file.

No

File number 1 - 500 for server file;
501 - 599 for operating system defined files.

Rec_No

Record number within file.

Offset

Word offset within record for relative files,
character offset for sequential files.

Print_Format

As described for entry type F, except S format.

Type

Data type in record

RL for Real

1 for Integer

I2 for integer*2

I4 for Integer*4

Ib.w for bit field: b=bit, w=width

DP for Double Precision

An for ASCII: n=length of string

[Read]

Optional. This specifies the format to be read from the specified sequential file. If omitted, the value read is unformatted and has the same representation as it does in memory.

In	Integer
Zn	Short integer in hexadecimal notation
Fn.m	Floating point
En.m	Floating point in exponential form
An	ASCII
D	Date (DD-MMM-YY) integer date is in minutes
T	Time (HH:MM:SS) real data is in seconds
where:	
n	Is the width of the field and m is the number of decimal places.

Examples

Example 1:

R 26 00031 \$25 00001 F8.2 RL

The value stored in Index number 25 will be used as the record number. If the file numbered 31 is sequential, the read will be assumed to be unformatted.

Example 2:

R 74 00503 00043 00027 Z4 I I5

The file numbered 503 is sequential. If line 43 of the file is:

2 2 3 3
0 5 0 5
data: 4567890012345678

Then the value of index number 74 will be 1,234 and on the report will appear as 04D2 (hex).

Example 3:

R 011 00502 00003 00005 I6 I4

File numbered 502 is sequential. If record 3 contains 0001 (hex) and 8001 (hex) in its fifth and sixth word, then the value of Index number 11 will be 98,305.



Attention

No, Rec_No, and Offset can all be indirect by using the “\$” operator (for example, Rec_No = \$123 means use the value of index number 123).

See Also:

Entries M and W.

T (Totalize History)

Purpose

Totals the history values for a point and stores the total in a free format variable.

Format

*T Index Point_ID Parameter Print_Format [History Type
(Offset) Repeat]*

Description

<i>Index</i>	Number (1-999) identifying report variable to store total.
<i>Point_ID</i>	Point name of the analog point.
<i>Parameter</i>	As described for entry type F.
<i>Print_Format</i>	As described for entry type F.
<i>[History Type],[Offset], [Repeat]</i>	As described for entry type F.

Example

T 2 SINEWAVE PV F8.2 H6M(10) 5

In this example, five values of “6 minute history” for Point SINEWAVE with offset 10 are summed and stored in Index 2. The sum is printed as a floating point number.

See Also:

Entries L and D.

W (Write to File)

Purpose

Used to write a value from a free format variable to either an operating system file or a server database file. If an operating system file is to be accessed, then the details about the file should be specified with the M entry.

Format

W Index No Rec_No Offset Type [write]

Description

Index

Number (1 - 999) identifying the database variable storing the value to be written.

No

File Number 1 - 500 for server file;
501 - 599 for operating system defined files.

Rec_No

Record number within file

Offset

Word offset within record for relative files,
character offset for sequential files.

Type

Data type in record

RL for Real

I for Integer

I2 for integer*2

I4 for Integer*4

Ib.w for bit field: b=bit, w=width

DP for Double Precision

An for ASCII: n=length of string

[*write*]

Optional. Format to write in specified sequential file. If omitted, the value written will be unformatted and has the same representation as it does in memory.

In Integer

Zn Short integer in hexadecimal notation

F_{n.m} Floating point

E_{n.m} Floating point in exponential form

An ASCII

D Date (DD-*MMM*-*YY*) integer date is in minutes

T Time (HH:MM:SS) real data is in seconds

Where:

n is the width of the field and *m* is the number of decimal places.

See Also:

Entries M and R.

X (Demand Point Processing)

Purpose

Scans a point parameter value and forces processing of the point regardless of whether or not the point value has changed. This entry is used to force any algorithms attached to the point to be executed. Otherwise this entry is identical to the F (Fetch from point) entry.

Format

X Index Point_ID Parameter Print_Format

Description

Index

Number (1-999) identifying report variable to store value acquired from field.

Point_ID

Point name

Parameter

As described for entry type F. History parameters are not enabled.

Print_Format

As described for entry type F

See Also:

Entries A, G and F.

Free Format Report Example

This section shows an example of a report definition file and the resulting report output.

Report Definition File

```

*
*This is an example free format report
*Get the Point ID
F 1 01IT1LEVEL NAME A10
*
*Get the last 10 history values and store at
*index 20..
F 20 01IT1LEVEL PV F8.3 H1M(1) 10
*Get the maximum and minimum of these values and store at 50,51
  respectively
L 50 01IT1LEVEL PV F8.3 H1M(1) 10
*Store these values in user table 254 record 3 words 1,2
W 50 254 3 1 RL
W 51 254 3 4 RL
*Calculate the standard deviation for these history values
D 52 01IT1LEVEL PV F8.3 H1M(1) 10
*Calculate the sum of these history values
T 53 01IT1LEVEL PV F8.3 H1M(1) 10
*Take an average of these values and store it at index 1
C 11 F8.3
P 11 = ($53)/10
P 70 = 1
P 71 = 2
P 72 = 3
P 73 = 4
P 74 = 5
P 75 = 6
P 76 = 7
P 77 = 8
P 78 = 9
P 79 = 10
*Store the result in the SP of a point
G 11 01OT1LEVEL SP
*
*Read some text from a file
M SEQ 501 0 c:\reports\freeformat\ffrdata.in
R 40 254 3 1 F8.3 RL F8.2
*2345678901234567890123456789012345678901234567890
B:
-----
$C501
-----

```

For point '1 ' the latest 10 history values are:
 \$\$1001 '20 '

The Sum of these values is '53 '
 The Maximum value is '50 '(saved as '40 ')
 The Minimum value is '51 '
 The Standard Deviation is '52 '
 The Average of these values is '11 '

\$XY 70 20 10 0 10 0 75

Report output

P26-FEB-96 18:14:21 RPT003: freefmt : FREE FORMAT REPORT
 :DEMANDED: PAGE 01

A
 A Example Free Format report
 A

0

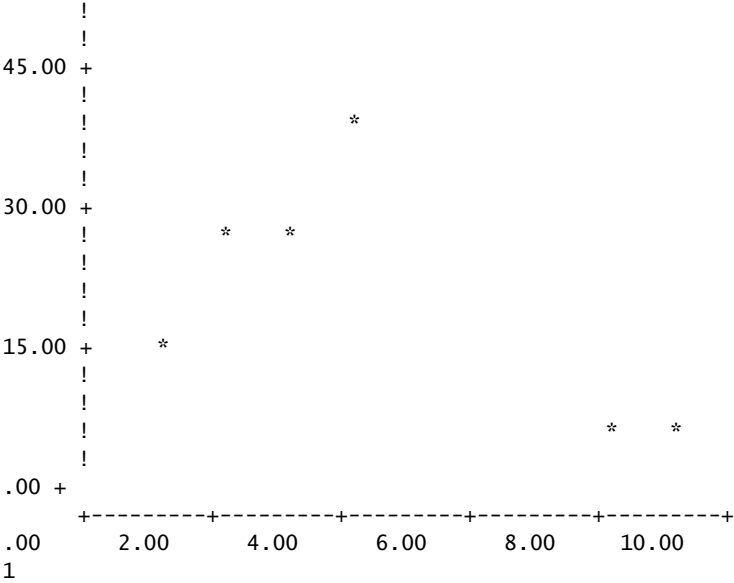
 Heading for Example report !!

For point 01IT1LEVEL the latest 10 history values are :

15.990
 27.500
 27.500
 38.950
 55.600
 55.600
 72.800
 6.900
 6.900
 6.900

The Sum of these values is 314.640
 The Maximum value is 72.800 (saved as .000)
 The Minimum value is 6.900
 The Standard Deviation is 22.385
 The Average of these values is 31.464

75.00 +
 !
 !
 !
 60.00 +
 * *
 !
 !



Configuring and monitoring a redundant server system

21

This chapter describes:

- Server redundancy
- Network redundancy, including Fault Tolerant Ethernet (FTE)
- Configuring and monitoring redundant servers
- Setting up Station for redundancy

Prerequisites

- Set up the computer names for your primary and backup servers. It is important that you follow the correct server naming convention for redundant server systems when you install Windows. See the *Software Installation and Upgrade Guide* for details.
- Installed the network cards in the primary and backup servers.
- Configured TCP/IP on the primary and backup servers and assigned a TCP/IP address to each network card.

If you have FTE, for instructions on configuring FTE, see the following topic in Knowledge Builder:

Experion R300 > Installation and Upgrades > Fault Tolerant Ethernet
Installation and Service Guide > FTE Installation and Configuration
Checklists.

- Installed Experion software on the primary and backup servers.
- Installed Station software on client computers.
- Set up time synchronization. It is important that the primary and backup servers are synchronized so that all dates and/or times associated with events in the database are consistent between servers. See the section “Setting up time synchronization” in the *Supplementary Installation Tasks Guide*.

Tasks

Task	Go to:	Done?
Complete the TCP/IP configuration by configuring the primary and backup server hosts files and testing the TCP/IP configuration of the servers	page 470	
Ensure the duplex settings on your network card match the duplex settings for your network switches	page 476	
Define the redundant connections	page 477	
Configure Station setup files for redundancy	page 481	
Synchronize the servers	page 483	
If your system has process points, synchronize the Engineering Repository database	page 484	
If your system has process points, set failover settings in the event of Process controllers communications subsystem failure	page 491	
Synchronize the enterprise model database	page 485	
If required, configure fast failover settings	page 494	

About redundancy

Redundancy is a configuration that allows a backup or second server to automatically continue the role of the primary server in the event of a hardware or software failure on the primary server.

The primary server is the server that is performing all the Experion server roles at a given time. A backup server is idle, waiting to take over the primary role if needed.

Redundant server names are always made up of two parts; the basename and an identifier letter of a or b. For example, the base name could be hsserv, therefore one server would be named hsserva and the other hsservb.

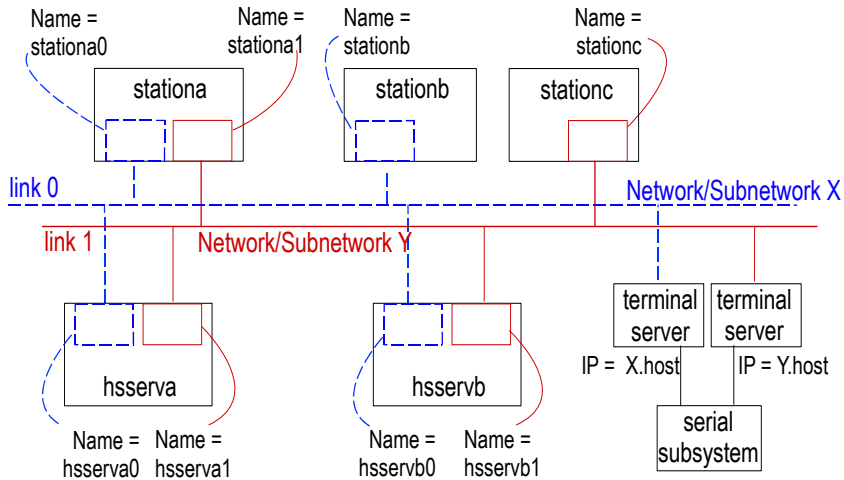
Experion supports dual networks and redundant servers, in any combination, and FTE networks. For example, you can configure:

- Station connections to redundant servers over dual networks
- Redundant connections between redundant servers (recommended)
- Stations and redundant servers connected using an FTE network

The following figure shows a sample network architecture drawing for a fully redundant non-FTE system. A diagram like this is useful for checking the validity of your configuration and for finding problems during configuration and testing. If any node or network seems to be functioning incorrectly with respect to network communications, checking its configuration against the network architecture drawing is a quicker way to find any misconfiguration than just running diagnostics.

Your diagram should show:

- All network-connected computers running Experion server or Station (generically called “nodes”)
- Single, dual and FTE network connected
- Network/subnetwork ID for each of the networks
- Name and IP address for each network interface card (NIC) connected anywhere on either network
- Hubs and switches used, including any cross over cables

Figure 30 Sample network architecture diagram

In this example, the system consists of:

- Dual networks $\times$ (link 0) and γ (link 1)
- Redundant servers, with basename hsserv and identifiers a and b. These servers are redundantly connected, which means that each has an NIC for each network. The server names are therefore hsserva0 (hsserva connected to link 0), hsservb0 (hsservb connected to link 0), hsserva1 (hsserva connected to link 1), and hsservb1 (hsservb connected to link 1).
- Stationa, which has a redundant connection to the redundant server. Stationa sees all four server names.
- Stationb, which has a single connection to the redundant server over network X. Stationb sees server names hsserva0 and hsservb0.
- Stationc, which has a single connection to the redundant server over network Y. Stationc sees server names hsserva1 and hsservb1.

The following section contains an overview of network redundancy (see “Network redundancy” on page 467).

Network redundancy

Two forms of network redundancy, both optional, are available for servers and Stations:

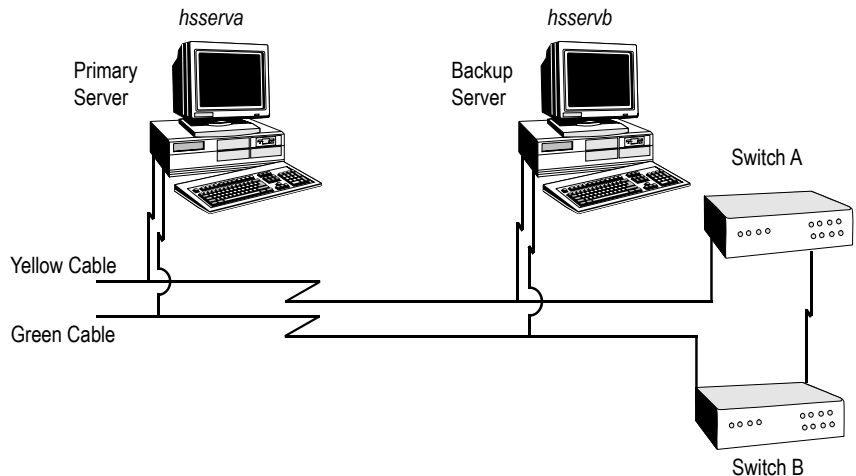
- Ability for a pair of servers to perform database synchronization and other redundancy functions over a dual or FTE network (highly recommended to avoid a single point of failure)
- Ability of Stations to connect to non-redundant and redundant servers via dual or FTE networks

These capabilities are independent of each other and are configured separately. However, they have the same requirements for network configuration, which are described in this section. For dual network configuration procedures, see the *Software Installation and Upgrade Guide*.

Network redundancy with FTE

In an FTE configuration the servers are connected to two cables on the same subnet and have two network cards. The cables are connected to two switches and the switches are connected by a cable as illustrated in the following figure.

Figure 31 FTE configuration



Network redundancy without FTE

Following is a list of network configuration requirements:

- Two networks that have distinct IP Subnet/Network IDs. The network redundancy scheme requires two NICs in the server or servers, and also in any Stations that participate in the dual network scheme. In the sample diagram and for this discussion, these networks are called X and Y.
- Two separate IP Networks (or subnets). One NIC in each participating server or Station must be connected to one cable/hub. The other NIC in each participating server or Station must be connected to the other cable/hub.
- All NICs connected to the first cable/hub have the same network/subnetwork ID, X.
- All NICs connected to the second cable/hub have the same network/subnetwork ID, Y.
- All IP addresses on either network must have the form X.host or Y.host. This is a consequence of the required NIC connections. If you are not careful to ensure this, you can create some very difficult situations to debug.

The IP address assigned to NIC A in a node has no relationship to the IP address assigned to NIC B in the same node, but both addresses must comply with these network and subnetting requirements. If you need to use certain IP addresses because of their availability, you must ensure that they are on the correct subnet.

However, the naming (or at least alias) scheme given to these nodes is important for servers (for example: hsserva, hsservb, hsserva0, hsserva1, hsservb0, hsservb1). This naming convention enables each redundant server to find the other and programs like Microsoft Excel Data Exchange and ODBC Driver to “autofind” the current primary server based on a *basename* (hsserv in the example) for the pair of servers.

It is important that the hsserva0 and hsservb0 names are both associated with the X network, and the hsserva1 and hsservb1 names are both associated with the Y network.

Station network redundancy

Station Network redundancy details are stored in the Station setup files (.stn) and in the hosts file on each Station. On each Station you define auxiliary .stn files that round robin among any number of server connections (see “Single network configuration” on page 470). The Station software works its way through the configured sequence of setup files until it finds a connection to the current primary server.

Stations connected to a single server on dual networks see two names for the server (for example, hsserv0, hsserv1) and need two Station setup files, each pointing to the other in the **Auxiliary setup file** option in the Station Connection Properties dialog box.

Stations that are connected to redundant servers on dual networks see four names for the pair of servers (for example, hsserva0, hsserva1, hsservb0, hsservb1). These Stations need four Station setup files, configured so that each auxiliary setup option points to the next Station setup file in the desired round robin sequence, with the fourth file pointing back to the first to complete the loop (see “Configuring Stations for server redundancy” on page 481).

You must determine whether each Station is on a single or a dual network. If it is on a single network, just ensure that the IP network/subnetwork ID for that Station’s NIC is consistent with other nodes attached to the network (that is, X on the X network, or Y on the Y network).

Stations connected to redundant servers on a single network see two server addresses for the pair of servers (for example, hsserva0 and hsservb0 **OR** hsserva1 and hsservb1). In this case there might still be a dual network present and being used for the servers and some Stations; it is not mandatory to connect all Stations to a dual network if one exists.

Redundant server network redundancy

Server network redundancy between redundant servers is configured through **hdwbld** (see “Defining the redundant connections” on page 477).

Completing the TCP/IP configuration of the servers

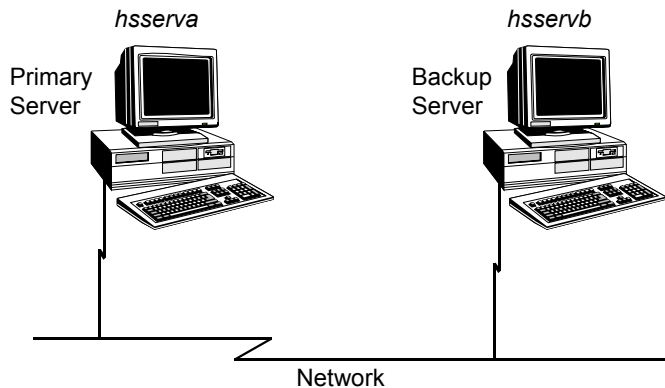
This section describes how to complete the configuration of your primary and backup servers and how to test your configuration. The section assumes that your primary server is called **hsserva** and your backup server is called **hsservb**.

For detailed information about configuring TCP/IP for servers, see the *Software Installation and Upgrade Guide* and the Microsoft Windows documentation.

Single network configuration

In a single network configuration, both servers are connected on a single network and have a single network card installed. The following figure shows an example of a single network configuration.

Figure 32 Single network configuration



Modifying the hosts File

The following procedures assume that the TCP/IP address of **hsserva** is 192.168.0.1 and the TCP/IP address of **hsservb** is 192.168.0.2.

You can also verify the host Files are consistent when you use the host Files verification tool as documented in the section on “Verifying hosts files” in the *Server and Client Troubleshooting Guide*.

To modify the hosts file:

- 1 Use a text editor to edit the hosts file. (**Note:** If you use Microsoft Notepad to edit the hosts files, you need to remove the .txt file extension after you save the files.)

The hosts file is:

%SystemRoot%\system32\drivers\etc\hosts

For example:

c:\winnt\system32\drivers\etc\hosts

- 2 Add the following lines to the hosts file:

TCP/IP address for primary

192.168.0.1 hsserva hsserva0

TCP/IP address for backup

192.168.0.2 hsservb hsservb0

Remember to use the base server name and TCP/IP addresses that are applicable to your site.

Verifying host files using analysis tools

Although using a text editor to modify the hosts file is convenient, the analysis tools in the network tree provide a hosts file verification tool to verify host files in a defined system.

To verify hosts files

- 1 In the Configuration Explorer in Configuration Studio, click **Analysis Tools**.
- 2 Click the **Host File Verification** task.
- 3 Select from the list the computers that need their hosts file verified for consistency in IP addressing and node naming.
- 4 Determine from the displayed results and recommendations whether any further hosts file actions need to be taken.

Testing the TCP/IP configuration

After you have modified the hosts file on both servers, you should test the TCP/IP configuration on both servers.

To test the TCP/IP configuration:

- 1 Open a Command Prompt window.
- 2 Ping each host name in turn; for example, type the following commands one by one:
ping hsserva
ping hsserva0

```
ping hsservb
ping hsservb0
```

- 3 If any requests time out, or if the incorrect TCP/IP address is pinged, go back and re-examine your TCP/IP configuration. See the *Installation Guide* for more information, if necessary.

FTE configuration

In an FTE configuration the servers are connected as shown in “FTE configuration” on page 467. For instructions on installing FTE, see the following topic in Knowledge Builder:

Experion R300 > Installation and Upgrades > Fault Tolerant Ethernet Installation and Service Guide > FTE Installation and Configuration Checklists.

Modifying the hosts file

The following procedures assume that the TCP/IP address of the network card connected to the yellow cable on **hsserva** is 192.168.0.1 and the TCP/IP address of the network card connected to the yellow cable on **hsservb** is 192.168.0.3. (Normally, a computer’s green address differs by 1 from its yellow address. For example, the green address of **hsserva** would be 192.168.0.2.)

Note that you do not add entries for the network cards connected to the green cable.

To modify the hosts file:

- 1 Use a text editor to edit the `hosts` file. (**Note:** If you use Microsoft Notepad to edit the `hosts` files, you need to remove the `.txt` file extension after you save the files.)

The `hosts` file is:

```
%SystemRoot%\system32\drivers\etc\hosts
```

For example:

```
c:\winnt\system32\drivers\etc\hosts
```

- 2 Add the following lines to the `hosts` file:

```
# TCP/IP address for primary
192.168.0.1 hsserva hsserva0
# TCP/IP address for backup
192.168.0.3 hsservb hsservb0
```

Remember to use the base server name and TCP/IP addresses that are applicable to your site.

Testing the TCP/IP configuration

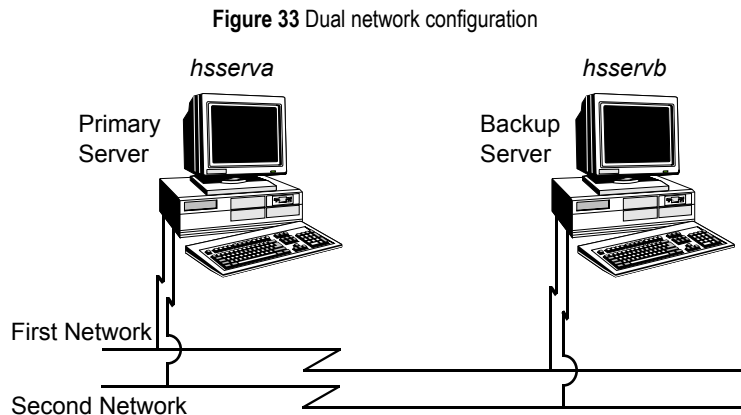
After you have modified the hosts file on both servers, you should test the TCP/IP configuration on both servers.

To test the TCP/IP configuration:

- 1 Open a Command Prompt window.
- 2 Ping each host name in turn; for example, type the following commands one by one:
ping hsserva
ping hsserva0
ping hsservb
ping hsservb0
- 3 If any requests time out, or if the incorrect TCP/IP address is pinged, go back and re-examine your TCP/IP configuration. See the *Software Installation and Upgrade Guide* for more information, if necessary.

Dual network configuration

In a dual network configuration the servers are connected on two networks and have two network cards as illustrated in the following figure.



Modifying the hosts file

The following procedures assume that:

- For **hsserva** the TCP/IP address for the first network card is 192.168.0.1 and for the second network card the TCP/IP address is 192.168.1.1.
- For **hsservb** the TCP/IP address for the first network card is 192.168.0.2 and for the second network card the TCP/IP address is 192.168.1.2.

To modify the hosts file:

- 1 Use a text editor to edit the `hosts` file on the primary and the backup server. (**Note:** If you use Microsoft Notepad to edit the `hosts` files, you need to remove the `.txt` file extension after you save the files.)

The `hosts` file is:

```
%SystemRoot%\system32\drivers\etc\hosts
```

For example:

```
c:\winnt\system32\drivers\etc\hosts
```

- 2 Add the following lines to the `hosts` file:
 - # First TCP/IP link of the primary
 - 192.168.0.1 hsserva hsserva0
 - # First TCP/IP link of the backup
 - 192.168.0.2 hsservb hsservb0
 - # Second TCP/IP link of the primary
 - 192.168.1.1 hsserva1
 - # Second TCP/IP link of the backup
 - 192.168.1.2 hsservb1

Remember to use the base server name and TCP/IP addresses that are applicable to your site.

Testing the TCP/IP configuration

After you have modified the `hosts` file on both computers, you should test the TCP/IP configuration on both computers.

To test the TCP/IP configuration:

- 1 Open a Command Prompt window.
- 2 Ping each host name in turn; for example, type the following commands one by one:
 - ping hsserva
 - ping hsserva0
 - ping hsserva1
 - ping hsservb

ping hsservb0

ping hsservb1

- 3 If any requests time out, or if the incorrect TCP/IP address is pinged, go back and re-examine your TCP/IP configuration. If necessary, see the *Software Installation and Upgrade Guide* and Windows documentation for more information.

Checking network card settings

Many network cards allow the duplex setting to be configured. Ensuring the duplex settings on your network card are the same as the duplex settings for your network settings can help make synchronization more robust.

Contact your system administrator to find out the duplex settings of your network switches.

To check the network card duplex settings:

- 1** Choose **Start > Settings > Control Panel > Network and Dial-up Connections**.
- 2** Select the appropriate adapter and open its properties.
- 3** Find the duplex settings and, if necessary, change them to reflect the settings of your network switches.
- 4** Close the Network and Dial-up Connections.
- 5** Reboot your computer.

Defining the redundant connections

Details about the connection between the two servers in a redundant server system are defined using entries in a hardware definition file. The following details need to be specified for the connection:

- The Redundant Arbitration method (see the description of Redundant arbitration below)
- The data links between the primary and the backup servers

To define the redundant connections in the server database, you need to create entries in a hardware definition file and then run the **hdwbld** utility to define the details in the server database.



Attention

If you are using FTE, you must use the Single Network Data Link definition.

Redundant arbitration

Redundant arbitration is the task of deciding which of the servers will run as the primary (that is, communicating with field devices and Stations) and which will run as the backup (providing a standby system in case the primary fails).

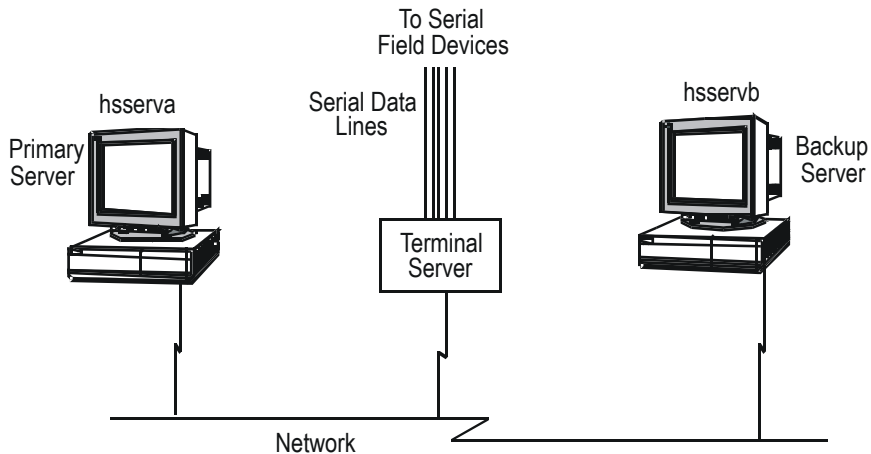
The method of arbitration is called Software arbitration.

Software arbitration

When software arbitration is used, software running on the primary and backup servers provides the arbitration. Each server polls the other (via the network) so that it knows if the other server has failed.

For example, if **hsserva** is running as the primary server and fails, the arbitration software running on **hsservb** detects this and switches from running as backup to running as primary.

“Software arbitration” on page 478 illustrates software arbitration.

Figure 34 Software arbitration

When software arbitration is used, terminal servers provide the data link between the servers and the serial field devices.

The server running as primary communicates with the field devices (via the terminal servers). If the primary server fails, the backup server becomes the primary and takes over communications with field devices.

Defining the arbitration method

The arbitration method to be used in your redundant server system must be defined for the primary and backup servers.

Prerequisites

- You must stop the Experion server before using the **hdwbld** utility.

Considerations

- An example hardware definition file (which you can modify and use) is shipped with Experion. The file is called **redun.hdw** and is located in `Program Files\Honeywell\Experion PKS\server\user`.

To define the arbitration method:

- 1 In any text editor open or create your hardware definition file.
- 2 Add the following entry to the hardware definition file:

```
DEL PSW00
ADD PSW00 NETWORK_PSW RECOVER=recover_option
```

Where `recover_option` is `ABORT` or `REBOOT`. `ABORT` means that when a failover occurs, Experion server is stopped and restarted on the failed server. `REBOOT` means that when a failover occurs, Experion server service is stopped and the database unloaded on the failed server. The Experion server service is then restarted.
- 3 Save the file and copy to the primary and backup servers.
- 4 Run the **hdwbld** utility on the primary and backup servers to store this connection definition in the Experion database.

For information about the content and syntax of hardware definition files and how to run the **hdwbld** utility, see the *Hardware and Point Build Reference*.

Example

The following hardware definition file entries is for a redundant server system with software arbitration. When a failover to the backup server occurs, Experion is stopped and restarted on the primary server.

```
DEL PSW00
ADD PSW00 NETWORK_PSW RECOVER=ABORT
```

Data links between primary and backup servers

When the primary and backup servers are running in redundant mode, all database changes on the primary server are sent to the backup server via one or more data links. (A data link is a network path between the primary server and the backup server.)

Hardware building the data links

A hardware definition file must be created defining the data links. This file must be hardware built (using the **hdwbld** utility) on both servers.

The example hardware definition file `Program Files\Honeywell\Experion PKS\server\user\redun.hdw` also includes data link definition examples.

Single network data link definition

The single network data link configuration is illustrated in “Single network configuration” on page 470.

You define the single data link as follows in a hardware definition file:

```
DEL LNK00  
ADD LNK00 NETWORK_LINK
```

Dual network data link definition

The dual network data link configuration is illustrated in “Dual network configuration” on page 473.

You define the dual data links as follows in a hardware definition file:

```
DEL LNK00  
ADD LNK00 NETWORK_LINK  
DEL LNK01  
ADD LNK01 NETWORK_LINK
```

Configuring Stations for server redundancy

Stations need to connect to whichever server is running as the primary server.

However, for local and network-connected Stations to always connect to the server running as primary requires special Station configuration. How this is done for single and dual networks is described in the following sections.

Single network and FTE configuration

In a single network and FTE configuration when a Station connection to the primary server is lost (or the primary server fails), the Station should attempt to connect to the backup server.

Similarly when the backup server stops running as primary, the Station should try to reconnect to the primary server.

You can configure Station to do this by configuring an auxiliary setup file. The auxiliary setup file contains the name of the server to connect to if the current connection is lost (or the current server fails).

In the case of a single network configuration, two Station setup files are required:

- `default.stn` which connects to **hsserva** (and has auxiliary setup file `hsservb.stn`)
- `hsservb.stn` which connects to **hsservb** (and has auxiliary setup file `default.stn`)

When Station starts, it connects to **hsserva** (as configured in `default.stn`). If **hsserva** fails (or connection to **hsserva** is lost), Station reconnects to **hsservb** (as configured in the auxiliary setup).

For details on configuring setup files see “Configuring Station connections” on page 72 and “Connection Properties” on page 95.

Dual network configuration

Dual network configuration is more complicated than single network configuration because there are two data paths (networks) which Station can use to connect to the server running as primary.

In dual network configuration when Station connection to the primary server is lost (or the primary server fails) the Station attempts to connect to the backup server via the same network.

If Station is unable to connect to the backup server using the first network Station attempts to reconnect to the primary server using the second network.

If Station is unable to connect to the primary server using the second network Station attempts to connect to the backup server using the second network.

This way both servers and both networks are tested by Station in an attempt to make a valid connection.

In this case, four Station setup files are required:

- default.stn which connects to **hsserva0** via the first network (and has auxiliary setup file hsservb.stn)
- hsservb.stn which connects to **hsservb0** via the first network (and has auxiliary setup file hsserva1.stn)
- hsserva1.stn which connects to **hsserva1** via the second network (and has auxiliary setup file hsservb1.stn)
- hsservb1.stn which connects to **hsservb1** via the second network (and has auxiliary setup file default.stn)

If connection to this server fails:	Station then tries connecting to this server:
hsserva (using default.stn)	hsservb (using hsservb.stn)
hsservb (using hsservb.stn)	hsserva (using hsserva1.stn)
hsserva (using hsserva1.stn)	hsservb (using hsservb1.stn)
hsservb (using hsservb1.stn)	hsserva (using default.stn)

In addition to specifying the auxiliary files, you need to ensure that Station can access displays by:

- Ensuring the host files include the host server names.
- Creating the network connections on the computer running Station.
- The relevant network paths are added to the Displays tab in the Connection Properties dialog box for all of the required .stn files.

For details on configuring setup files see “Configuring Station connections” on page 72 and “Connection Properties” on page 95.

Synchronizing the server databases

At this point the Experion server redundancy configuration is complete. The primary and backup servers can now be put into redundant mode.

Synchronization is the process of copying over the Experion server database from the primary server to the backup server. When the server database on the backup server is identical to the database on the primary server, the servers are said to be *synchronized*.



Attention

The process whereby database changes on the primary server are automatically sent to the backup server is known as *automatic checkpointing*. Automatic checkpointing from the primary to the backup server does not occur until the two servers have been synchronized.

To synchronize your servers:

- 1 Start Experion on the primary server and connect a Station to it.
- 2 Choose **View > System Status > Server Redundancy** to call up the **Server Redundancy Status** display.
For information about the options on this display, see “Monitoring redundant servers” on page 486.
- 3 Start Experion on the backup server.
- 4 On the **Server Redundancy Status** display on the primary server, the LEDs in the **Link Status** group should change from red to green and indicate the following:
 - **Running**
 - **Link n (LINK0n)**
- 5 On the **Server Redundancy Status** display on the primary server, click the **Synchronize** button to synchronize the two servers.

The Experion database on the primary server is automatically copied to the backup server.

The time taken to synchronize completely depends on the size of your system. Synchronization on a large system can take considerable time to complete. Synchronization on a small system can take a few minutes to complete.

The synchronization indicator (the first LED in the **Backup Server** group) should change from red to green and the text change from **Unsynchronized** to **Synchronized**.

Synchronizing the Engineering Repository database

This section describes how to set up the Engineering Repository database redundancy on the backup server.

Prerequisites

- You must log on to Configuration Studio using the mngr account.

To set up redundancy for the Engineering Repository database:

- 1 In Configuration Studio, connect to the backup server.
- 2 In the Configuration Explorer, click the backup server.
- 3 Click the **Administer the control strategy database task**. DBAdmin opens.
- 4 Choose **DBAdmin > Experion PKS Node > Admin Tasks**.
- 5 Click **Enable Replication**.
- 6 Click **Yes** when the Before proceeding to enable replication dialog box appears.
- 7 Click **OK** when the Successfully Enabled Database Replication message appears.
- 8 Close the ER Database Administration Tool.

After you have enabled replication, any changes that are made to the primary Engineering Repository database are automatically replicated to the backup Engineering Repository database.

You can check the status synchronization status of the Engineering Repository database using Control Builder.

Synchronizing the Enterprise Model database

This section describes how to set up the Enterprise Model database redundancy on the backup server.

To set up redundancy for the Enterprise Model database:

- 1 In Configuration Studio, connect to your system.
- 2 In the Configuration Explorer, click the system name.
- 3 Click the **Administer the system database task**.
- 4 Expand **DBAdmin > Experion PKS Node > EMDB Admin Tasks**.
- 5 Click **Enable Replication**.
- 6 Click **Yes** when the Before proceeding to enable replication dialog box appears.
- 7 Click **OK** when the Successfully Enabled Database Replication message appears.
- 8 Close DBAdmin.

After you have enabled replication, any changes that are made to the primary Enterprise Model database are automatically replicated to the backup Enterprise Model database.

You can check the status synchronization status of the Enterprise Model database using Enterprise Model Builder.

Monitoring redundant servers

Once the servers are running in redundant mode, you can use a number of methods to monitor the status of your system.

Using Station to monitor redundant servers

You can use the Server Redundancy Status display on Station to:

- Determine which server is currently running as the primary
- Determine whether the servers are synchronized
- Synchronize the servers
- Manually fail over to the backup server
- Monitor the redundancy queue availability and data transfer rates
- Change the checkpoint period

To call up the Server Redundancy Status display choose **View > System Status > Server Redundancy** from the Station menu.

A description of some of the options on the Server Redundancy Status display follows:

Property	Description
Queue Availability	Experion uses a queue to buffer database information to be sent from the primary to the backup server. On the Server Redundancy Status display the Availability option shows the percentage of the queue size. In the course of normal operations, this number should be close to 100. If the number is less than 100%, then there is currently data in the queue that needs to be transferred to the backup server.
Availability threshold	When you specify a value in the Availability threshold box, the system will record the amount of time that the queue availability drops below the specified percentage
Checkpoint period	The checkpoint period is the cyclic period that the contents of the memory-resident part of the database are sent to the backup server. The default value is 300 seconds (5 minutes). This value is not normally changed.
Link transfer rate	The Link Transfer Rate value gives a measure of the throughput of the redundant link.
Tracing mask	The Tracing Mask value is used for diagnostic purposes. Do not change this value unless advised to do so by Honeywell support personnel.

Using points to monitor redundant servers

When you have synchronized your servers use the point definition file, called `redun.pnt`, located in `Program Files\Honeywell\Experion PKS\server\user` to define points to monitor the redundant server queue. You define the points in Quick Builder and download the points to the primary server. The points are:

Point	Description
<code>redun_ack_no</code>	Monitors the last acknowledged message number
<code>redun_cur_q_ava</code>	Monitors the amount of free queue space as a percentage
<code>redun_msg_no</code>	Monitors the current message number
<code>redun_syncd</code>	Monitors whether the servers are synchronized
<code>redun_xfer_rate</code>	Monitors the transfer rate of the queue

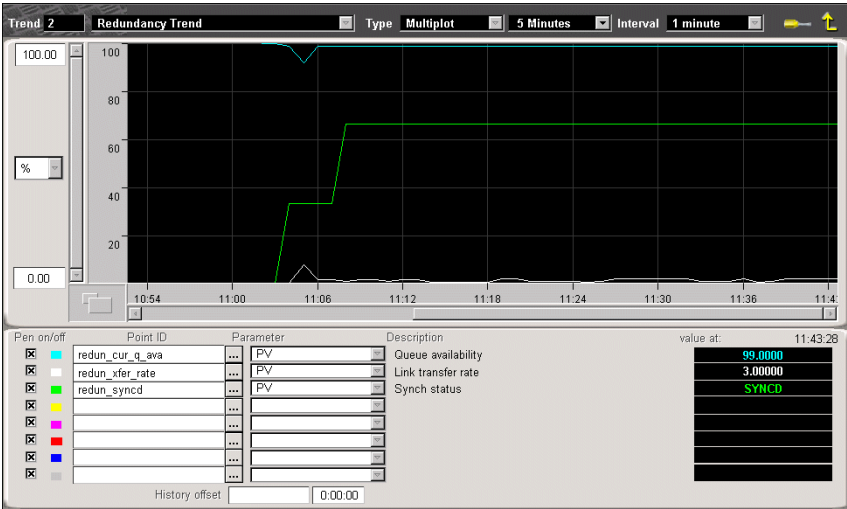


Attention

The syntax of the sample points assumes that the controller is controller one. If you need to, customize the points to suit your requirements.

Configure a multiplot trend which displays these points so that the status of the redundant server system can be monitored. The current message number and the last acknowledged message number should closely follow. If the current message continues to grow but the last acknowledge number is falling behind or flattening out, redundant synchronization can be lost.

Figure 35 Trend Display for monitoring redundant server system



For more information on configuring and using trends, see “Configuring trend displays” on page 366 in this guide, and the *Operators Guide*.

Synchronizing other files

Experion database information is automatically transferred from the primary server to the backup server. Any configuration changes to the database (such as changes to points and displays) are also transferred.

You might also want automatic copy of other files after they are modified on the primary server, such as the Quick Builder database, custom displays, application source files, and history archives.

There are two ways of synchronizing files:

- Configure a File Replication (recommended).
- Edit the configuration file flbkup.def.

It is recommended that you use the File Replication service to copy files such as custom displays, and use flbkup.def to copy history archives between the backup and primary servers. For details see “Configuring File Replication” on page 589.

Alternatively, you edit the configuration file `Program Files\Honeywell\Experion PKS\server\data\flbkup.def` on both the backup and primary servers to specify which files are to be copied.

Uncomment existing lines or add new lines. The file uses the following syntax. Lines starting with:

- * - Are comment lines
- S - Specify a folder to be copied. All subfolders are also copied unless excluded by the X entry
- X - Specify a folder not to be copied to the backup

There should be one line in the file starting with a T. This line records the date and time of the last successful transfer. This entry should not be changed.

Example

If you want your Quick Builder database, custom displays, and history archives copied to the backup server, the flbkup.def would look like this:

```
T 11/11/99 10:56:15
* Copy the Quick Builder database to the backup
S \client\qckbld
* Copy custom displays to the backup
S \client\abstract
* Copy history archives to the backup
S \server\archive
```

Files are copied periodically from the primary to the backup server. The default period is 60 minutes. For information on changing this default see “Changing the default transfer period” on page 490.

During synchronization the file transfer program attempts to transfer files from the indicated folders on the primary server to the backup server. The time and date that the file transfer program ran is recorded. During periodic transfers the file transfer program attempts to transfer any files from the indicated folders that have changed since the last time the program ran. Files are transferred if either:

- The file does not exist on the backup server
- The date and time stamp on the backup server differs by more than 60 seconds to the date and time stamp on the primary server, even if the file on the secondary server is newer.

Changing the default transfer period

You can change the default transfer period, by adding an option to the link add line in the redundancy hardware definition file. The redundancy hardware definition file is found in the Program Files\Honeywell\Experion PKS\Server\user\redun.hdw.

The following example changes the transfer period to 30 minutes for a dual network.

Example

```
DEL LNK00
ADD LNK00 NETWORK_LINK DAEMON_VALUE2=30
DEL LNK01
ADD LNK01 NETWORK_LINK DAEMON_VALUE2=30
```

Failover of a redundant server system

The backup server takes over from the primary if:

- The primary server software or hardware fails and the backup cannot communicate with it
- All network links between the primary and backup server are broken
- A user does a manual failover (see “Manually failing over a redundant server system” on page 493)

If you have Process Controllers, you can specify that failover occurs when there is a failure in the Process Controller communications subsystem. The following actions cause a failover:

- The Experion PKS Control Data Access Server service is stopped via the Windows Control Panel.
- The RSLinx service is stopped via the Windows Control Panel (this also stops the Experion PKS Control Data Access Server service).
- RSLinx terminates abnormally.
- A critical Process Controller communications failure is detected.

To specify failover when the CDA communications subsystem fails:

- 1 Synchronize the servers.
- 2 Call up the Server Redundancy Configuration display.
- 3 Select the **Failover to backup server on CDA hosts, devices or nodes Communications Subsystem failure if servers are synchronized** check box.

The following actions do not cause a failover:

- The CNet cable is disconnected.
- A C300 or C200 controller is disconnected or fails.

The primary server can be configured to restart (with the backup server becoming primary) if one of the following tasks fails:

- timer controls timing of all Experion server tasks (Task 50)
- scanx controls the SCADA scanning subsystem (Task 60)
- daqmgr controls the delivery of SCADA acquisition requests to the appropriate SCADA driver (Task 61)

By default, these tasks are set to restart if they fail.

To configure the primary server to restart if a task fails:

- 1** In Station, choose **Configure > Application Development > Watchdog Timer**.
- 2** Set the **Action** for the appropriate task to **Reboot**.

The backup server does not take over from the primary if a SCADA channel fails.

Manually failing over a redundant server system

There might be times when you want the backup server to run as the primary for a while. For instance, you may want to upgrade your primary server in some way (for example, upgrade memory, upgrade the hard disk or install a Windows Service Pack).

Experion supports manual (operator-controlled) failover from the primary server to the backup server. This failover causes the backup server to run as the primary.



Caution

- If you manually fail over your Experion system, the primary and backup servers lose synchronization. The servers need to be resynchronized if they are to run in redundant mode again. The automatic transfer of database updates from the primary server to the backup server does not occur until the two servers have been synchronized.
- When you want to fail back to your primary server after a failover, you must first resynchronize your servers. If you do not resynchronize them you lose changes to the Experion database that were made while the backup server was running as the primary.
- Stopping Experion on your primary server also causes your system to fail over to the backup server. If you do not want this to happen, you should always stop your backup server before stopping your primary server.

Considerations

- If the primary servers services are manually stopped, operator intervention is required for Station to connect to the backup server.

To manually fail over:

- 1 Open the Server Redundancy Status display
- 2 Click **Manual Failover**. This notifies the backup server that it is to run as the primary.

Server redundancy fast failover configuration

Normally Station reconnect time is approximately 30 seconds. It is possible to tune server and Station redundancy timeout parameters to achieve approximately 10 second Station reconnect time (also known as fast failover).

Configuring fast failover is only recommended for high performance servers running on high performance networks, because it increases:

- The traffic that the Stations and servers put onto the network
- The servers' susceptibility to failover from disruptions on the network

One way to improve failover time without affecting network performance is to define IP addresses in the hosts files so that IP address resolution is faster (see “Making IP address resolution faster” on page 497).

If you want to configure fast failover, you set parameters for:

- The time until the backup server becomes primary after it detects that the primary is down (see “Time until backup server becomes primary” on page 494).
- The time until the server allows a new Station connection to use a Station number after a Station connection fails (see “Time until server disconnects Station” on page 495).
- The time until a Station fails over to the backup network after a connection to the server fails (see “Time until stations fail over to backup network” on page 496).

Time until backup server becomes primary

To tune the time until the backup server becomes primary after it detects that the primary server is down, you reset the number of messages permitted to be lost before failover occurs. The following steps must be performed on both the primary and backup server:

- 1 Open a Command Prompt window and type **hscserver /database** to stop the Experion server.
- 2 Isolate the network between the servers from other network traffic.

- 3 Edit the PSW00 line in the redundancy configuration file, Program Files\Honeywell\Experion PKS\server\user\redun.hdw
 - For fast failover, add **IDLE=5 READ=10** to the **PSW00** line
 - For normal operation, delete the **IDLE** and **READ** values from the **PSW00** line, or set the default values **IDLE=10 READ=15**.

For example:

```
ADD PSW00 NETWORK_PSW RECOVER=ABORT IDLE=5 READ=10
```
- 4 From the command prompt, run the command **hdwbld redun.hdw** to make the changes effective.
- 5 Use Start/Stop Experion PKS Server to set the server state to **System Running**.

Time until server disconnects Station

Set the time that the server waits for data from a Station before disconnecting it. The fast failover setting is 5; the normal setting is 30.

Considerations

- If you adjust this setting, you must also adjust the time until Stations fail over to the backup network. If the settings are not properly synchronized, the Stations will disconnect frequently.

To change the time until the server disconnects Station:

- 1 On the primary server, and then on the backup server, open a command prompt and run (**bold** indicates your entries):

```
C:\>fileio
Database contains      400 files
File number (=0 to exit) ? 8
Use memory image [YES|NO|BOTH(default)] ? both
File   8 contains      1 records of size      4096 words
Record number (=0 to back up) ? 1
word offset (=0 to back up) ? 82
Mode = 0 to back up
      = 1 for INTEGER      (int2)
      = 2 for HEX          (int2)
      = 3 for ASCII        (int2)
      = 4 for F.P.         (real)
      = 5 for SET bit      (int2)
      = 6 for CLR bit      (int2)
      = 7 for LONG INTEGER (int4)
      = 8 for LONG F.P.    (dble) ? 1
INTEGER VALUE =      30 NEW VALUE = 5
Save value [YES|NO (default)] ? yes
```

```
word offset (=0 to back up) ? 0
Record number (=0 to back up) ? 0
File number (=0 to exit) ? 0
```

Time until stations fail over to backup network

The time until a Station fails over to the backup network depends on:

- The **KeepAliveTimeout** and **DisconnectTimeout** settings in the `station.ini` file.
- The **TcpMaxConnectRetransmissions** setting in the registry.
- If you are using Fault Tolerant Ethernet (FTE) you also need to set the interval properties for the Honeywell Fault Tolerant Ethernet Service to 500 ms.

Considerations

- If you adjust the timeout settings, you must also adjust the time until the server disconnects Station. If these times are not properly synchronized, Stations will disconnect frequently.

To change the KeepAliveTimeout and DisconnectTimeout settings for a computer:

- 1 Edit the file `%SystemRoot%\station.ini`. In the [Station] section, add or uncomment the lines:
 - For fast failover (non Fault Tolerant Ethernet network):


```
KeepAliveTimeout=30
DisconnectTimeout=30
```
 - For fast failover (Fault Tolerant Ethernet network):


```
KeepAliveTimeout=50
DisconnectTimeout=0
```
 - For default failover:


```
KeepAliveTimeout=150
DisconnectTimeout=150
```

Both timeouts are in units of 0.1 seconds.

- 2 Edit the registry entry for **TcpMaxConnectRetransmissions**:
 - a. From a command prompt, type **Regedt32**.
 - b. Open the path `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
 - c. Open **TcpMaxConnectRetransmissions**. If it does not exist, select **Edit > Add Value** to add it. The **Data Type** is **REG_DWORD**.
 - d. In the DWORD Editor, type **0** for fast failover, or **Decimal 3** for default failover. Then click **OK**.
 - e. Exit Registry Editor. You need to restart the computer to use the new setting.

To set the interval properties for the Honeywell Fault Tolerant Ethernet Service:

- 1 Choose **Start > Settings > Network and Dial-up Connections**.
- 2 Right-click the Local Area Connection you want to modify.
- 3 Select **Honeywell Fault Tolerant Ethernet Service** and click **Properties**
- 4 In the **Interval** box, type **500**.

Making IP address resolution faster

One way to achieve faster failover without necessarily increasing network traffic is to define IP addresses in the hosts files of all computers on the network.

Considerations

- Stations configured as static Stations reconnect marginally more quickly than those configured as rotary Stations.

To define IP addresses in the hosts file:

- 1 On all Station computers, ensure that there is an entry in the hosts file (`%SystemRoot%\system32\drivers\etc\hosts`) for both server computers.
- 2 On both server computers, ensure that there is an entry in the hosts file (`%SystemRoot%\system32\drivers\etc\hosts`) for every Station computer.

FTE-specific configuration

If you have FTE, you should see the *Fault Tolerant Ethernet Overview and Implementation Guide* and the *Fault Tolerant Ethernet Installation and Service Guide* for most of the configuration instructions. However, the following details are specific to Experion.

- The Honeywell Fault Tolerant Ethernet Service should be set to 500 ms.
- The Station timeout must be longer than the time FTE might take to redirect output. This is essentially the following:
$$(\textit{Disjoin multiplier} + 1) * \textit{Interval} + \textit{TCP retransmission time}$$
where *TCP retransmission time* is determined by the characteristics of your system, and can be up to about 1 second.

Configuring Distributed System Architecture

22

The Distributed System Architecture (DSA) option enables multiple Experion servers to share data, alarms, messages, and history without the need for duplicate configuration on any server. This chapter describes the architecture and functions of a DSA system and the configuration procedures that are required.

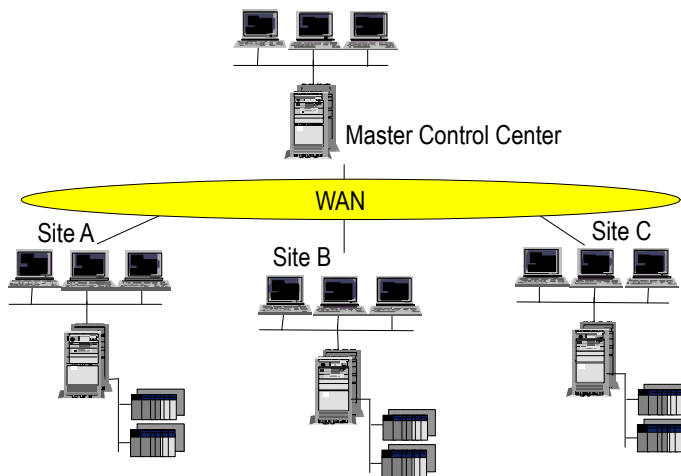
Overview

The Distributed System Architecture (DSA) option enables you to integrate multiple Experion servers into a single operational system.

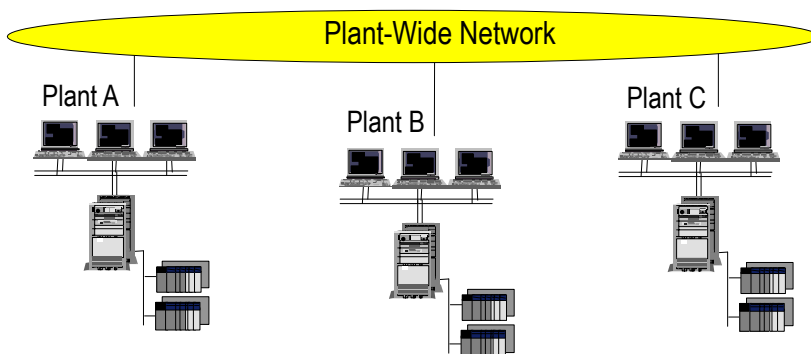
It is effective for geographically distributed systems, for logically separate Experion systems located in different parts of a plant, and for combinations of the two.

Geographically distributed systems collect data from a wide area and can be controlled locally and remotely. Common configurations include a master control center accessing data from several remote sites, which might each contain several servers and which can also exchange information. Communication bandwidth of the network between the servers is typically less than that available within an individual plant.

Figure 36 Geographically distributed system



In a plant-wide system, data is typically shared between servers over a high-bandwidth network, such as a 100 MB or higher Ethernet. In this case each server is assumed to be responsible for controlling a different part of the plant. Typically there are multiple control rooms, or multiple Stations in the same control room, each associated with a specific server.

Figure 37 Plant-wide distributed system

Requirements for implementing a DSA system

The requirements for implementing a DSA system are:

- The password for the Windows mngr account (created when you install the Experion server) must be the same on all servers connected via DSA.
- Within a given system (as defined in Configuration Studio), you can have only one Enterprise Model Database (EMDB). Note that where there is more than one system, and therefore more than one Enterprise Model database, it is possible to share an Enterprise Model (or parts thereof) across those systems, provided that the parts of the Enterprise Model that you want to share between systems are identical; that is, the asset tag names (asset point ID's) and full item names must be the same.
- The date and time must be synchronized on distributed servers to ensure that all dates and times associated with events in the database are consistent. Servers can be in different time zones but still have their coordinated universal time (UTC) synchronized.
- To access points on another server with the same point ID, the point ID must be prefixed with a server alias
- Every point that will be accessed from more than one server must be assigned to an asset (see "Point IDs" on page 503).
- All displays that a Station needs to access must be accessible through the Displays Path defined for the Station.
- Message indexes and text should be the same on all servers (see "Configuring messages" on page 243).
- If you are using Electronic Signatures, all servers must be licensed for Electronic Signatures.

- Electronic Signature reason sets and legal text must be the same on all servers.
- Each server database must contain all acronyms used on any displays it needs to access, including those copied from remote servers.

For information about the asset model, see “Configuring your Enterprise Model” on page 37. For information about alarms in a DSA system, see “Notifications” on page 507.

Data access

DSA provides global access to point parameter data on all servers in the system. Each server provides automatic dynamic caching of remote data for all of its clients, so that clients access their local server for all data. Clients do not access remote servers directly.

For example:

- Station accesses its local server to display alarms or data for points on local and remote servers.
- An OPC client application can access a local OPC server on an Experion server to obtain point data from that or any other Experion server.
- A Microsoft Excel spreadsheet connected only to its local server can display data through Microsoft Excel Data Exchange from multiple servers.
- An application, or a network application, connected only to its local server can access point data from multiple servers.

A server establishes a local cache point (see How remote points are located) and subscribes to a remote server when one of its clients requests data for a point that is not already in the database. While the subscription is in effect the data owner uses report by exception, only sending data to the caching server on change. When the data is no longer referenced by any of its client Stations or applications, the subscribing server cancels the subscription to the data owner. This subscription mechanism ensures maximum efficiency both on the servers and over the network.

How remote points are located

The first time a remote point is accessed, the local server asks the servers in the system for the data owner of the point. When the data owner is determined, the local server automatically creates a cache reference in the local database. This cache reference is known as a “cache point”.

Point IDs

Duplicate point IDs can exist in a DSA system, however points with duplicate IDs must not belong to the same server in the DSA. To distinguish between points with duplicate point IDs, you must prefix the point ID with the server name, for example, `ExperionServerNorth:FIC123`.

Internal point numbers

Point data for a remote point is ultimately accessed by its internal point number on its local server. If a point is deleted and then recreated, its internal point number might change, which means that remote group, trend, and custom displays can no longer access the point. You need to re-enter the point into the remote group, trend, and custom displays that access it. For more information, see “Understanding internal point numbers” on page 234.

The cache points are automatically deleted from all remote servers when the point is deleted at the data owner.

In a distributed system architecture, the internal numbering of points and the ordering of points cannot be assumed. The internal point number for a cache point is usually different from the internal point number on the local server, and cache points are created in the order that points are accessed.

Applications that run on a remote server should never use hardcoded point numbers, and custom displays that are called from a remote server should never be created with point repeats.

Point count licensing

Cache points do not count against the licensed point count on a server. However, the total of cache points and licensed points on any server cannot exceed 65000.

Displays in a DSA system

Operators interact with local and remote data on displays in the same way. From an operator's perspective, there is no difference between a local and a remote point.

Displays locations

You can configure the Displays Path in the Station setup files to access displays from any server. This means that you can set Stations in the distributed system to use displays from one central file server or from several local servers, depending on your network and other environmental conditions. For example, in a geographically distributed system, custom displays should be loaded on individual servers.

If displays are on more than one server, you need to ensure that all the appropriate paths are configured in the Station setup files.

Custom displays

Custom displays engineered on one server can be used on any Station in the system without change, provided they do not use internal database references (for example, user files).

Consolidated Alarm Summary

The Alarm Summary shows a consolidated list of local and remote alarms. The remote alarms displayed to an operator are those from the assets for which alarms are enabled on the local server, and which have been assigned to the Station or operator. Local and remote alarms can be filtered in the same way.

The Station Alarm Zone shows the highest priority unacknowledged alarm, regardless of whether it is a local or remote alarm.

An operator can navigate directly to the Associated or Point Detail display for a remote alarm, just as for a local alarms.

The “in-alarm” and acknowledgment status of remote points is indicated on custom displays in the same way as local points.

Associated displays

Each Station displays the Associated Display defined on its local server. To ensure that the appropriate Associated Display is displayed for remote points, the numbers and contents of Associated Displays should be consistent across all servers.

Notifications

Notifications include process alarms, system alarms, messages and journaled events. In a DSA system, alarms, alerts and messages are distributed as needed by the processes running on each server in the system.

Alarms

On each server, you must set the server to subscribe to alarms from other servers in the DSA.

To identify the server from which an alarm originates, you can show the following columns on the Alarm Summary:

- DSA Connection Name
- DSA Server Name

See “Customizing the layout of the summary displays” on page 393 for information on how to show extra columns in the Alarm Summary.

An alarm is also displayed if a remote server cannot be accessed.

For information about the different effects of disabling alarms for local and remote areas, see “Disabling alarms in a DSA system” on page 507.

Disabling alarms in a DSA system

In a DSA system, the effect of disabling alarms depends on whether they are disabled by:

- Individual points
- Asset
- Server

If alarms for an individual point are disabled, then no alarms for that point are shown on any server in the DSA system.

If alarms are disabled for an asset on a local server, then no alarms are generated locally and no alarms are distributed for that asset to remote servers. Alarms generated on a remote server for that asset are not displayed locally. For example, `ServerEast` and `ServerWest` have an asset called `ConveyorBelt`. You disable alarms for asset `ConveyorBelt` on `ServerEast`. Alarms generated for the asset `ConveyorBelt` on `ServerEast` are not displayed on `ServerEast` or `ServerWest`. An alarm is raised on `ServerWest` indicating that alarms are disabled for asset `ConveyorBelt` on `ServerEast`. Alarms generated for the asset `ConveyorBelt` on `ServerWest` are *not* displayed on `ServerEast` but are displayed on `ServerWest`.

If alarms are disabled server-wide on a local server, then no alarms are generated locally and no alarms are distributed to remote servers. An alarm is raised on the remote servers indicating alarms have been disabled server-wide on the local server.

For information on how to disable alarms, see “Disabling alarming” on page 250.

Alarm and message acknowledgement policy

By default, alarm acknowledgements are distributed to all servers. This means that the alarm only needs to be acknowledged once, at any server that displays it. Remote alarms can be acknowledged in the same way as local alarms, from custom displays, the Alarm Summary display, and the Station Alarm Zone.

You can configure the **Alarm Acknowledgement Policy** setting so that alarms must be acknowledged at each server. This setting must be the same on all servers.

Message acknowledgements are always distributed to all servers.

Message index

Each Station displays the message text defined on its local server. To ensure that appropriate messages are displayed for remote points, the message indexes and text should be the same on all servers.

Journalized events

Because distributing all journaled events would need significant bandwidth, most events are recorded only on the server where the point is defined. The exceptions are Acknowledgement events and Point Value Change events, which are recorded both on the server where they occurred and on the data owner.

This means that the event archive on each server includes all events for its local points, and Acknowledgement events and Point Value Change events that occurred on the local server and affect remote points.

To view events for a remote server:

- Configure an **Alarm and Event DSA** report that includes events from the remote server. (For more information about configuring this report, see “Alarm and Event DSA reports” on page 411.)
- Use Station to log on to the remote server and view the Event Summary display.
- If sufficient bandwidth is available an ODBC-based report, using the Experion ODBC Driver, can be constructed to generate a consolidated event

report from multiple servers. The ODBC Driver is included with the Experion Open Data Access option.

Journalled operator changes

Operator changes to a remote point are journaled on both the local server and the data owner.

Trends

When a trend includes a remote point, historical data for that point is retrieved from the remote server in real time. If the history intervals on local and remote servers are configured differently, trend data is interpolated. For example, a local server is configured to collect fast history at 1 second intervals and a remote server is configured to collect fast history at 5 second intervals. If you create a trend on the local server requesting data from the remote server at 1 second intervals, data from the remote server is interpolated.

It is possible, but not advisable, to collect history locally for a remote point. Therefore a remote point should not be assigned to history.

Security

Assignable assets are used to restrict access to both local and remote Server data.

If you are using Station-based security, you assign assets to the Stations. See “Assigning scope of responsibility to Flex Stations” on page 338.

If you are using operator-based security, you configure the operators on all servers where they need to log on. You then assign assets to the operators. See “Assigning scope of responsibility to operators or Windows group accounts” on page 340.

If you are using point control levels, the control level is passed to the remote server and checked at the remote Server.

Working with DSA

For normal operation, a DSA system works in the same way as a single server system.

This section discusses the characteristics of a DSA system for engineering tasks.

Working with algorithms

Point Algorithm displays use internal database references. This means that you need to log on to the remote server, using standard Station networking facilities, to view point algorithm configuration from Station.

Configuring hardware items

The configuration summaries for hardware items only show items configured on the local server. However, the System Status display allows you to view alarms or work with the configuration of the following items on remote servers:

- Connections
- Channels
- Controllers
- Printers
- Redundant Servers
- Stations

Performance considerations

The accuracy of information and timeliness of control for remote servers depends on the capacity and reliability of the networks and data links.

A local server issues an alarm if the response from a remote server takes longer than the time specified in its configuration. Operators can also monitor the status of links and remote servers from the System Configuration - Distributed Systems summary. Clicking a server in the summary list displays more detailed status information.

Accessing history data for remote points in real time might impact the overall performance of a low bandwidth network, such as a WAN. For example, history data trend displays is requested and returned in real time.

Multicasting

For any server in the distributed architecture, you can choose multicasting to remote servers that are connected over a network that supports it. The performance effects of multicasting depend on the network and the number of servers. Contact your local Honeywell representative for information about the network devices that support multicasting, and its appropriateness for your system.

When multicasting is used, a server sends a single copy of its data over the network to other servers. The other servers on the network need to know the network address and port number the multicast packets use so that the networking software can listen for data on that address. The benefit of multicasting is to conserve bandwidth and reduce network traffic.

Some routers are not configured with multicasting enabled. In this situation multicasting must be manually enabled on the router.

Experion uses multicasting to provide the status of both the server and the links between servers in a DSA system. Each server has a link daemon which multicasts its status to the network. Daemons on the other servers listen for these multicasts to obtain the status of other servers.

The multicast address used by DSA is 225.7.4.103. The multicast port is 2911.

Synchronization considerations

To share alarms and historical data, the servers need to be time synchronized. However, the servers can be in different time zones, each showing its own local time.

For information about how to synchronize servers, see section “Setting up time synchronization” in the *Supplementary Installation Tasks Guide*.

Server redundancy and networks

If you are using Fault Tolerant Ethernet (FTE), your DSA system should be configured as a single link between servers.

No special configuration is required for DSA systems. The Distributed System status summary and status tabs show the redundancy architecture of each server.

Operator keyboard support

Specialized operator keyboard functions, such as AUTO/MANUAL and raise/lower, are supported in the same way for local and remote points.

The fast raise/lower step is specified in the system wide Station configuration for the server that the Station is connected to (see “Configuring alarm settings” on page 86). This step applies to local and remote points.

Internationalization

All servers in the DSA system must be in the same language.

Configuration for Distributed System Architecture

Prerequisites

- Experion server software is installed on all servers that are participating in the DSA.
- The Enterprise Model Builder database is installed on one of the Experion servers.
- Configuration Studio is installed.
- If there is a firewall in your DSA system, make sure that the necessary ports are opened in the firewall to enable DSA communications between the DSA client and server nodes. For information on configuring firewalls in a DSA system, see the topic “Firewall configuration” in the chapter on “Network security” in the *Network and Security Planning Guide*.

Considerations

- On any server, remote points only appear in the Display Builder properties point list after the server has accessed them and identified their host servers. The remote point references are resolved at runtime.

Tasks

Task	Go to	Done?
In Enterprise Model Builder define all servers that are to be connected via DSA.	<i>Enterprise Model Builder User's Guide</i>	
In Configuration Studio, configure each server connected via DSA to subscribe to data and alarms.	page 516	
In Configuration Studio configure alarm tuning settings.	page 517	
Ensure the paths of any custom display files and numbered display files are added to the Connections Properties for Stations connected to the server.	page 96	
Copy all user-defined acronyms used by the custom display files to the server, using fildmp .	<i>Application Development Guide</i>	
If Station-based security is being used, assign the assets that each Station needs to access.	page 338	
If operator-based security is being used, assign the assets that each operator needs to access.	page 340	

Configuring servers to subscribe to data and alarms

You configure each server in your system to subscribe to alarms and data from other servers in the system. A server can subscribe to:

- both alarms and data
- data only

When you first define a server and download this server definition to other servers in the system, the default subscription for the server is disabled and it does not participate in the DSA.

In addition to subscriptions, on each server you can configure:

- Overload alarms
- Multicasting
- Updates to the Point Browser

Considerations

- When you configure a server to subscribe to Alarms and Data, or only Data, a DSA license check is completed. If the configuration exceeds your DSA license, the changes to the configuration are cancelled.

To configure data subscriptions:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure distributed servers** task.
The Distributed Servers Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the name of the server you want to configure.
- 4 Click the **Configuration** tab.
- 5 Enter the following information:

Property	Description
Alarms and Data Subscriptions	
Enable both Alarms and Data	Select this value if the server is to receive both alarms and data from the remote server.
Enable only Data	Select this value if the server is to receive only data from the remote server.
Overload Alarms	
Enable Data Connection Overload Alarm	Enables an alarm to be raised in the event of data connection overload.

Property	Description
Enable Notification Connection Overload Alarm	Enables an alarm to be raised in the event of notification connection overload.
Multicasting	
Link Supports Multicast Traffic	Specifies whether the network connection to the remote server supports multicast traffic.
Point Browser List	
Enable automatic update of list	If selected, any changes made to areas or points on any server connected via DSA is reflected in the Point Browser. Do not select this option if the connection between servers is slow, for example over a WAN.
Last update time	Shows the time of the most recent update to the Point Browser list.
Manual Update	Enables the Point Browser list to be manually updated.

Tuning your distributed system

The Tuning tab contains Cache and Communications Settings for the remote server. These settings should only be changed by experienced technical personnel in consultation with your local Technical Assistance Center.

To set tuning settings:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure distributed servers** task.
The Distributed Servers Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the server alias name.
- 4 Click the **Tuning** tab.
You can tune the following settings for individual connections to publishing servers:

Property	Description
Cache flush time	The intervals (in milliseconds) that the subscription list is checked for references to old data. The default value is 15 seconds.
Cache age time	The amount of time (in milliseconds) old data remains in the dynamic cache. The default value is 1 minute.

Property	Description
Maximum subscription time	The slowest subscription time (in milliseconds). The default value is 10 seconds. If the subscription time is slower than that specified, the subscribing server switches from subscription to synchronous read (polls). Maintaining a slow subscription is not efficient.
List fragment size	The size of data packets sent over the network. The default is 500 parameter values. This is tuned for optimal performance on low bandwidth links.
Connection timeout	The amount of time (in seconds) a packet of data can remain on the network without being acknowledged. When the timeout period expires, the connection is broken and communication is initiated again.
Notification buffer interval	(Applicable to remote server) The maximum amount of time (in seconds) a notification can be delayed on the publishing server before being sent to the subscribing server. The default value is 2 seconds
Notification keep alive interval	(Applicable to remote server) The maximum amount of time (in seconds) the publishing server does not send packets to the subscribing server. If there are no notifications within this time, an empty keepalive packet is sent to the subscribing server. The default value is 15 seconds.

The maximum tuning settings for each remote server are set by the global cache age time. The cache flush time is calculated first. The cache flush time is then used to calculate the cache age time. The cache age time is then used to calculate the maximum subscription time. These calculations are as follows:

Tuning Setting	Minimum Value	Maximum Value
Cache Flush Time	10000ms.	(Global Cache Age Time)/4
Cache Age Time	Cache flush time	Global Cache Age Time - (2 * Cache Flush Time)
Maximum Subscription Time	100ms	Cache Age Time

Prerequisites

- In Configuration Studio, you must be connected to the server you are tuning.

To tune the global cache settings:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure distributed servers** task.
The Distributed Servers Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the link flagged as **This Server**.
The **Distributed System Local Configuration** display opens.
- 4 Click the **Tuning** tab.
You can tune the following global cache settings to apply to all distributed architecture connections on the subscribing server.

Property	Description
Cache Age Time	Sets the maximum limits (in milliseconds) for the tuning settings for each remote server this server will access. The default is 1 hour. (Also referred to as global cache age time.)
Read Data Valid Time	The amount of time (in milliseconds) that data remains valid. When this time expires, the values are read again from the publishing server. This value is independent of the subscription time. The default value is 10 seconds.

Configuring Console Stations and consoles

23

This chapter describes the tasks required to configure:

- Consoles
- Console Stations
- Console Extension Stations

About Console Station

The Console Station provides direct access to process data and alarms and messages from CDA sources such as Process Controllers, FIM, IOLIM, and ACE nodes. This direct access provides a continuous view of your process, even if the Experion server is unavailable.

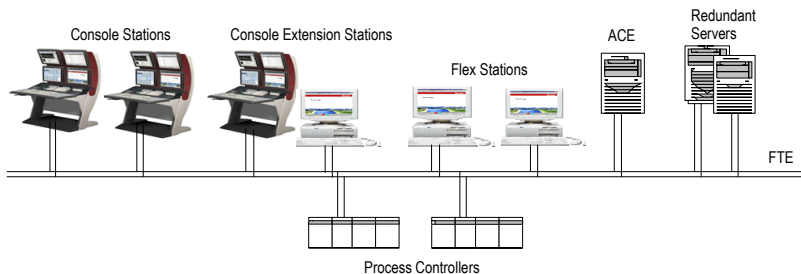
A Console Station is also connected to an Experion server. After you configure the connection to the Experion server, the server database files are replicated to the Console Station. This means that configuration of items such as process points is only done once. However, some functions such as reporting, history and events collection, are still provided by the Experion server. Therefore if the Experion server is unavailable, these functions are not available on the Console Station.

A Console Station can also have clients connected to it. These clients are called Console Extension Stations. A Console Extension Station connects to a Console Station in the same way a Flex Station connects to an Experion server. A Console Extension Station has the same functionality as a Console Station.

A Console Station and Console Extension Station can operate in the following environments:

- Distributed system architecture
- Icon Series Console environment
- Multi-window environment

The following figure shows an example architecture including Console Stations.



Functions available on the Console Station

The following functions are always available on the Console Station regardless of the availability of the Experion server:

- Data access from direct data sources such as Process Controllers and ACE nodes
- Notifications from direct sources
- Security restrictions, for example security levels and asset assignments
- Real-time trending of data from direct data sources such as Process Controllers
- Event journaling of Console Station events such as operator actions, for example, acknowledging alarms and logging on
- Display printing
- Backup and restore of the Console Station database

What happens when the Experion server is unavailable

When the Experion server becomes unavailable, for example during a server failover, an alarm is raised on the Console Station to indicate that the Console Station is operating in a server unavailable mode. During this time, the following functions on the Console Station are unavailable:

- History collection, assignment, retrieval and display
- Trend configuration
- Group configuration
- Chart visualization (Embedded CB Charts/Forms)
- Event and SOE Summary display
- Alarm and event printing
- Adding comments to alarms and events
- Report requests or report printing
- View or control of points and alarms from server connected controllers or other servers in a DSA configuration
- External alarm notification from server connected controllers
- Configuration changes, for example server wide settings and asset assignment
- Engineering Tools configuration load/upload and snapshot save/restore

How server wide settings relate to Console Station

The server wide settings that you can configure using the Server Wide Settings Station displays are applicable to Flex Stations, Console Stations, and Console Extension Stations. When you add a Console Station to your system, the server wide settings that have been defined on the server to which the Console Station is connected are automatically applied to the Console Station and any connected Console Extension Station clients. Server wide settings include:

- Startup displays
- Timeouts
- Alarm colors
- Alarm and event options

For information on the server wide settings see “Server wide settings” on page 107.

About Database and File Replication

To minimize the amount of configuration required for a system that includes Console Stations, files are replicated from the Experion server to the Console Stations. After you configure the connection between the Experion server and the Console Station, the server database is replicated to the Console Station. The data that is replicated includes:

- Process points
- TPS points
- Assets
- Alarm groups
- Asset assignment configuration
- Profiles
- Lists
- Time Periods
- Connection configuration
- Operator configuration
- Trend assignment configuration
- Group assignment configuration
- System configuration
- Acronyms
- Printer configuration

- Holiday configuration
- Console Station configuration
- Console configuration

Other files that need to be replicated to the Console Station include:

- Custom displays
- Summary views
- Category and attribute mappings

You use the File Replication utility to replicate these types of files and any other custom files you want replicated to the Console Station.

For information on configuring File Replication, see “Configuring File Replication” on page 589.

Security

As with a Flex Station, you can use either Station-based or operator-based security with a Console Station and Console Extension Station. You also use assignable assets to further restrict access to your Experion system. For information on assignable assets see “About assignable assets” on page 44.

The type of security you choose for the Console Station applies to any connected Console Extension Stations. Likewise, the asset assignment you apply to the Console Station also applies to any connected Console Extension Stations.

If you are using operator-based security:

- You need to define operators on the server as well as selecting the Operator signon required option when you configure the Console Station.
- You assign assets to operators. See “Assigning scope of responsibility to operators or Windows group accounts” on page 340.
- You can assign assets to operators as well as Console Stations and consoles and configure your system so that the asset assignment for both the operator and the Console Station or the console are checked before access is granted to an asset. (For the procedure on how to configure this, see the section “To configure the server to check the assignment for both the operator and the Station.” on page 338.)
- You can also use integrated security. Integrated security allows you to combine Windows user accounts with Experion operator accounts. For more information on integrated security see “Using integrated security” on page 287.

If you are using Station-based security, you assign assets to the Console Station. See “Assigning scope of responsibility to Console Stations” on page 339.

If you have domain controllers you can use high security policy. High security policy enables you to use Windows group policy to apply restrictions to particular groups of users. For more information see “Using High Security Policy” on page 324.

Configuring a Console Station

To configure a Console Station you need to complete tasks on both the Experion server and the Console Station.

Prerequisites

- You have completed all of the tasks for installing Experion Console Station. See the *Software Installation and Upgrade Guide*.
- You have updated the hosts file on the Console Station and the server, as documented in the section, “Updating the computer’s hosts file” in the *Software Installation and Upgrade Guide*.
- You can verify hosts files are consistent among Stations and server when you use the hosts file verification tool as documented in the section “Completing the TCP/IP configuration of the servers” on page 470.
- You have synchronized the date and time on the Console Station with the date and time on the server, as documented in the section, “Setting up date and time synchronization” in the *Supplementary Installation Tasks Guide*.

The tasks you need to complete on the server are:

Task	Go to	Done
Configure Console Station details.	page 529	
Configure Console Station options	page 530	
Assign scope of responsibility to the Console Station	page 532	
Configure File Replication so that any custom displays, summary display views and mapping files (used for notification and category attribute mapping) are replicated to the Console Station.	page 592	
If you have an OEP or IKB keyboard, configure LEDs.	page 533	
If you are using operator-based security, define operators on the Experion server.	page 306	
Optionally add Console Extension Stations to the Console Station	page 536	
Optionally configure consoles and add Console Stations to consoles	page 543	
If you have redundant servers, synchronize the servers so that the Console Station configuration is replicated to the backup server.	page 483	

The tasks you need to complete on the Console Station are:

Task	Go to	Done
Configure the Station connection properties.	page 534	
Create a file replication share.	page 599	

Results

- Configuration of the Console Station is successful when:
 - The server name appears in the Status Line and there is no red LED. (A yellow LED indicates that the Console Station is synchronizing with the server.)
 - The Node Status and the Station Status are set to OK on the Console Station Status Summary display.

If the configuration is not successful, see the *Server and Client Troubleshooting Guide*.

Configuring Console Station details

Considerations

- This task can be done using any Station that is already connected to the same server to which the Console Station is to be connected.
- If you try to configure more Console Stations than you are licensed for, you receive an error message.

To configure Console Station details:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click a blank row to call up the **Console Station Configuration** display.
- 4 In the **Network Name** box type the computer name of the Console Station.
- 5 If you want to specify operator-based security for this Console Station or for the Console Extension Stations that connect to this Console Station, select **Operator sign-on required**.
- 6 Type the remaining required information as described in the following table:

Property	Description
Normal Update rate	The rate, in seconds, at which dynamic values on displays at this Console Station are updated from the server database.
Fast update rate	An optional fast update rate, in seconds, that can be set by function key for displays at this Console Station.
Station Alias	Applicable only if you are adding this Console Station to a console. An alternative name for this Console Station that can be used to specify the destination of a display when invoked from another Station within the console. For more information about aliases see “Sending displays using aliases” on page 559.

Configuring Console Station options

There are several options that you can configure for a Console Station:

- The startup page that is displayed when a Console Station starts
- The Action taken when the idle timeout period is exceeded.
- The alarms that are audible alarms
- The printers used for printing reports and alarms and events.

These options are the same as the options that can be configured for a Flex Station. For a description of these options see “Flex Station Configuration Display” on page 113.

To configure Console Station options:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Console Station you want to configure.
- 4 Click the **Options** tab. Specify the appropriate options as described in the following table.

Property	Description
Start up page	Specifies the display called up on startup.
Change to start up page on idle timeout	If selected, when the idle timeout timer for the Station expires the display specified as the startup display is called up.
Activate for LOW Alarms	Controls whether an audible alarm is sounded for low priority alarms.
Activate for HIGH Alarms	Controls whether an audible alarm is sounded for high priority alarms.
Activate for URGENT Alarms	Controls whether an audible alarm is sounded for urgent priority alarms.
Also activate when Operator is signed off	Controls whether an audible alarm is sounded when, under alarm conditions, no operator is signed on to a Station configured for operator-based security.
Station failure Alarm	Controls whether an alarm is generated if communication to the Station is lost.
Alarm/Event Printer	Specifies the printer designated to print alarms and events.

Property	Description
Report Printer	Specifies the printer designated to print reports.
Print LOW alarms	Enables printing of alarms for points going in and out of low priority alarm conditions.
Print HIGH alarms	Enables printing of alarms for points going in and out of high priority alarm conditions.
Print URGENT alarms	Enables printing of alarms for points going in and out of urgent priority alarm conditions.
Print EVENTS	Enables printing of alarms for points going in and out of journal priority alarm conditions and other events.
Print Operator changes	Enables printing of all changes to points an operator has made from the Station.

Assigning scope of responsibility to a Console Station

To assign scope of responsibility to a Console Station:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Console Station to which you want to assign assets.
- 4 Click the **Assignment** tab.
- 5 Select the check boxes for each asset, Network item and System Component you want to assign to this Console Station.

Configuring LEDs on operator keyboards for Console Stations

Each LED on the IKB or OEP keyboards can be associated with a point. When the point goes into alarm, the associated operator keyboard LED shows the highest priority alarm.

Prerequisites

- You have installed the appropriate drivers and connected the keyboard. For these instructions, see the following topic in Knowledge Builder:
Experion R300 > Installation and Upgrades > Supplementary Installation Tasks Guide > Installing specialized hardware on a computer.

Considerations

- You only need to do this task if you are using either the IKB or the OEP keyboard.

To configure LEDs:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click Console Station for which you want to configure LEDs to call up the **Console Station Configuration** display.
- 4 Click the **Operator Keyboard** tab.
- 5 For every LED you want to associate with a point, type the point ID in the corresponding LED key number box.

Configuring the Station connection properties on the Console Station

Considerations

- The Station on a Console Station can operate in single mode or multi-window mode. If you are using multi-window mode, there are special configuration tasks you need to complete. See “Configuration tasks for multi-window Station” on page 125.
- This procedure covers settings required specifically for a Station on a Console Station. There are other settings you can set that are applicable to any type of Station. For information on these settings see “Configuring Stations and printers” on page 63.

To configure Station connection properties on a Console Station:

- 1 Start the Console Station.
- 2 Choose **Start > Programs > Honeywell Experion PKS > Console Station > Station**.
- 3 Choose **Station > Connect**.
The **Connect** dialog box opens.
- 4 Select default.stn and click **Edit**.
The **Connection Properties** dialog box opens.
- 5 Click the **Console Station** connection type.
- 6 In the **Console Station** list leave the default setting as localhost.
- 7 In the **Station Number** box, leave the default setting as 1.
- 8 Click the required window mode.
- 9 Click **Save**.

Deleting a Console Station

If required, you can delete the connection between the Experion server and the Console Station. For example, if you wanted to move the Console Station and connect it to a different Experion server, you would need to delete the connection from the original Experion server.

If the Console Station you are deleting has any Console Extension Stations, these are deleted when you delete the Console Station.

Considerations

- You can delete a Console Station from any Flex Station or any Console Station other than the Console Station you are deleting.
- You require a security level of ENGR to delete a Console Station.

Prerequisites

- The Console Station you are deleting is disconnected from the server.
- Any Console Extension Stations are disconnected from the Console Station.

To delete a Console Station:

- 1 In Station call up the **Console Station Configuration Summary** display.
- 2 Click the Console Station you want to delete.
- 3 Click **Delete**.
- 4 Click **Yes** to confirm the deletion.

Adding Console Extension Stations

For each Console Station, you can connect up to three Console Extension Stations. Console Extension Stations connect to a Console Station in the same way a Flex Station connects to an Experion server.

A Console Extension Station uses the configuration settings from the Console Station to which it is connected. The configuration settings obtained from the Console Station are:

- The type of security
- Asset assignment
- Startup page, idle timeout, alarm settings, printer settings
- LED configuration for operator keyboards (IKB or OEP keyboards)

The Console Extension Station needs to have access to custom displays. There are two options for providing access to custom displays:

- Configure the Console Extension Station to access the custom displays on the Console Station
- Replicate the custom displays to the Console Extension Station

The tasks you need to complete to add a Console Extension Station are:

Task	Go to	Done
Add Console Extension Stations to the Console Station	page 537	
Configure connection properties	page 538	
Provide access to custom displays by doing one of the following: • Configure File Replication so that any custom displays are replicated to the Console Extension Station. • Configure the Console Extension Station to directly access custom displays on the Console Station.	page 594 page 538	

Considerations

- If you try to add more Console Extension Stations than you are licensed for, you receive an error message.

To add Console Extension Stations:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
The Console Station Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the name of the Console Station to which you want to add Console Extension Stations.
This calls up the **Console Station Configuration** display.
- 4 In the **Console Extension Stations** box, select the required number of Console Extension Stations to be connected to the Console Station.
You can specify a maximum of 3 per Console Station.
- 5 Type the remaining required information for each Console Extension Station as described in the following table:

Property	Description
Normal Update rate	The rate, in seconds, at which dynamic values on displays at this Console Extension Station are updated from the server database.
Fast update rate	An optional fast update rate, in seconds, that can be set by function key for displays at this Console Extension Station.
Station Alias	Applicable only if you are adding the associated Console Station to a console. An alternative name for this Console Extension Station that can be used to specify the destination of a display when invoked from another Station within the console. For more information about aliases, see “Sending displays using aliases” on page 559.

Configuring the connection properties on a Console Extension Station

To configure connection properties on a Console Extension Station:

- 1 Start the Console Extension Station.
- 2 Choose **Start > Programs > Honeywell Experion PKS > Console Station > Station**.
- 3 Choose **Station > Connect**.
The **Connect** dialog box opens.
- 4 Select default.stn and click **Edit**.
The **Connection Properties** dialog box opens.
- 5 Click the **Console Station** connection type.
- 6 In the **Console Station** list type the name of the Console Station to which this Console Extension Station is connecting.
- 7 In the **Station Number** box, type the connection number.
The connection number can be 2, 3, or 4.
- 8 Click the required window mode.
- 9 Click **Save**.

Configuring a Console Extension Station to access custom displays on the Console Station

You can map a network drive to the custom displays folder on the Console Station computer or you can use a UNC path to specify the location of the custom displays folder on the Console Station.

Considerations

- You only need to perform this procedure if you are not configuring File Replication to replicate custom displays to Console Extension Stations. (For information on configuring File Replication see “File Replication for client computers” on page 594.)

To configure the Console Extension Station to access custom displays:

- 1 Start the Console Extension Station.
- 2 Choose **Start > Programs > Honeywell Experion PKS > Console Station > Station**.
- 3 Choose **Station > Connect**.
The **Connect** dialog box opens.

- 4 Select default.stn and click **Edit**.
The **Connection Properties** dialog box opens.
- 5 Click the **Displays** tab.
- 6 Modify the path to the custom displays as appropriate:

If:	Do this
You are using a UNC path	Change C:\Program Files\Honeywell\Experion PKS\Client\Abstract to \\ <i>ConsoleStation</i> \c\$\Program Files\Honeywell\Experion PKS\Client\Abstract where ConsoleStation is the computer name of the Console Station.
You are using a mapped drive	Change the drive letter in C:\Program Files\Honeywell\Experion PKS\Client\Abstract to the drive letter to which you mapped the Abstract folder.
Custom displays are stored in a folder other than the Abstract folder	Add your custom displays path to the to the Search for displays in box.

- 7 Click **Save**.

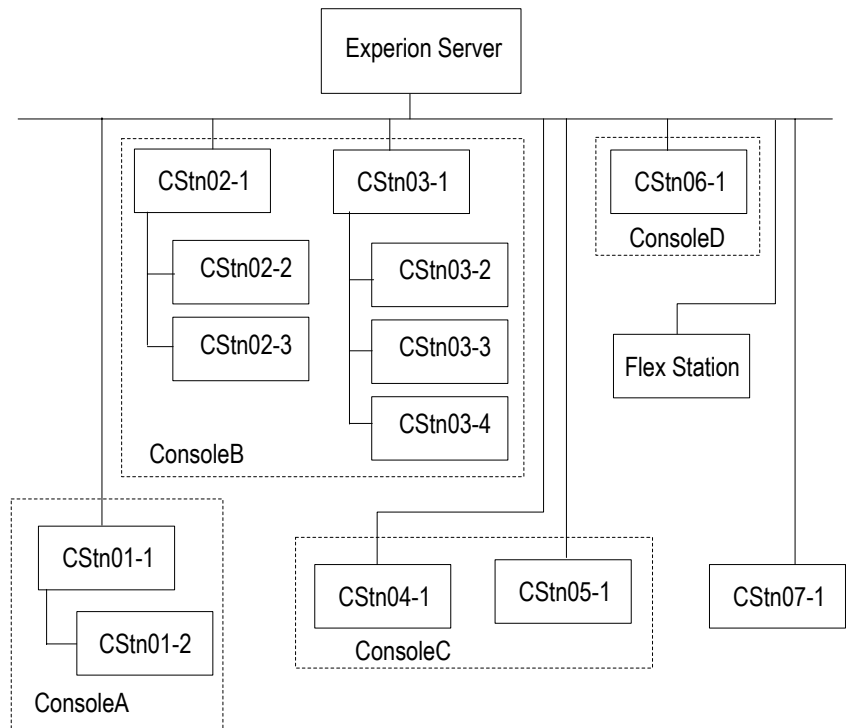
About consoles

A console is a logical grouping of Console Stations and Console Extension Stations which is associated with an Experion server. In general, the Console Stations and the Console Extension Stations will also be grouped together physically. A console can include the following combinations:

- A single Console Station
- A Console Station with a Console Extension Station
- Multiple Console Stations
- Multiple Console Stations with Console Extension Stations

The following diagram shows several different combinations of Stations:

- `consoleA` includes a Console Station, `cstn01-1` and a Console Extension Station, `cstn01-2`.
- `consoleB` includes two Console Stations, `cstn02-1` and `cstn03-1` and Console Extension Stations `cstn02-2`, `cstn02-3`, `cstn03-2`, `cstn03-3`, `cstn03-4`.
- `consoleC` includes two Console Stations, `cstn04-1` and `cstn05-1`.
- `consoleD` includes a single Console Station, `cstn03-1`.



A console enables you to prevent alarm acknowledgement within a console when the alarm is acknowledged outside of the console. This ensures that operators are seeing and responding to alarms for which they are responsible. For more information about alarm acknowledgement within a console, see “About alarm and message acknowledgement/silence synchronization” on page 552.

You can configure your console so that Operators can send displays from one Station for viewing on another Station within the same console.

A console provides ease of configuration by allowing you to configure settings at the console level and apply these settings to all Stations within the console. The settings you can configure for the console are:

- LEDs for IKB and OEP keyboards
- Asset assignment
- Startup pages
- Alarm settings
- Printer settings

If you want the console settings to apply to Stations within the console, you must configure each Station to use the console settings. See the procedure for adding a Console Station to a console on page 549.

Configuring consoles

To configure a console, complete the following tasks:

Task	Go to	Done
Configure the console	page 544	
If the Console Stations are using console settings, configure:		
• Console options	page 545	
• Assign scope of responsibility to consoles	page 547	
• LEDs on the operator keyboards for the console	page 548	
Add Console Stations to the console	page 549	

Results

- You have successfully configured a console and added Console Stations to the console when the console name appears in the Status Line of the Console Stations and Console Extension Stations that belong to the console.

Configuring a console

Considerations

- This task can be done using any Station (Console or Flex) that is already connected to the same server to which the console is to be connected.
- Consoles connected to the same server must have unique names.
- The settings you configure for the console apply to any Stations within the console that are configured with the option **Use console settings for Station configuration**. If the Station is configured to use its own settings, the settings you configure for the console do not apply.

To configure a console:

- 1 In the Configuration Explorer of Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure consoles** task.
The Console Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click a blank row to call up the **Console Configuration** display.
- 4 In the **Name** box, type the name of this console.
- 5 Type the remaining required information as described in the following table:

Property	Description
Normal Update rate	The rate, in seconds, at which dynamic values on displays at Stations in this console are updated from the server database.
Fast update rate	An optional fast update rate, in seconds, that can be set by function key for displays at Stations in this console.
Operator signon required	If selected indicates that operator-based security is used for Stations in this console and therefore operators are required to sign on.

Configuring console options

Considerations

- The options you configure for the console apply to any Stations within the console that are configured with the option **Use console settings for Station configuration**. If the Station is configured to use its own settings, the options you configure for the console do not apply.

To configure console options:

- In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- Click the **Configure Consoles** task.
The Console Configuration Summary display appears in the System Display tab in Configuration Studio.
- Click the Console you want to configure.
- Click the **Options** tab. Specify the appropriate options as described in the following table.

Property	Description
Start up page	Specifies the display called up on startup.
Change to start up page on idle timeout	If selected, when the idle timeout timer for the Station expires the display specified as the startup display is called up.
Activate for LOW Alarms	Controls whether an audible alarm is sounded for low priority alarms.
Activate for HIGH Alarms	Controls whether an audible alarm is sounded for high priority alarms.
Activate for URGENT Alarms	Controls whether an audible alarm is sounded for urgent priority alarms.
Also activate when Operator is signed off	Controls whether an audible alarm is sounded when, under alarm conditions, no operator is signed on to a Station configured for operator-based security.
Station failure Alarm	Controls whether an alarm is generated if communication to the Station is lost.
Alarm/Event Printer	Specifies the printer designated to print alarms and events.
Report Printer	Specifies the printer designated to print reports.
Print LOW alarms	Enables printing of alarms for points going in and out of low priority alarm conditions.

Property	Description
Print HIGH alarms	Enables printing of alarms for points going in and out of high priority alarm conditions.
Print URGENT alarms	Enables printing of alarms for points going in and out of urgent priority alarm conditions.
Print EVENTS	Enables printing of alarms for points going in and out of journal priority alarm conditions and other events.
Print Operator changes	Enables printing of all changes to points an operator has made from the Station.

Assigning scope of responsibility to a console

Considerations

- The assets you assign to the console apply to any Stations within the console that are configured with the option **Use console settings for Station configuration**. If the Station is configured to use its own settings, the assets you assign to the console do not apply.

To assign assets to a Console:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Consoles** task.
The Console Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the Console to which you want to assign assets.
- 4 Click the **Assignment** tab.
- 5 Select the check boxes for each asset you want to assign to this Console Station.

Configuring LEDs on operator keyboards for a console

Each LED on the IKB or OEP keyboards can be associated with a point. When the point goes into alarm, the associated operator keyboard LED shows the highest priority alarm.

Prerequisites

- You have installed the appropriate drivers and connected the keyboard as described in the *Software Installation and Upgrade Guide*.

Considerations

- You only need to do this task if you are using either the IKB or the OEP keyboard.
- The LEDs you configure for the console apply to any Stations within the console that are configured with the option **Use console settings for Station configuration**. If the Station is configured to use its own settings, the LEDs you configure for the console do not apply.

To configure LEDs:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Consoles** task.
The Console Configuration Summary display appears in the System Display tab in Configuration Studio.
- 3 Click the console for which you want to configure LEDs to call up the **Console Configuration** display.
- 4 Click the **Operator Keyboard** tab.
- 5 For every LED you want to associate with a point, type the point ID in the corresponding LED key number box.

Adding Console Stations to a console

Considerations

- Selecting the option **Use console settings for Station configuration** applies all of the console settings, including operator-based security, asset assignment, and LED configuration, to the Console Station and the Console Extension Stations. When you select **Use console settings for Station configuration**, any options that are no longer required are removed or disabled.

To add Console Stations to a console:

- 1 In the Configuration Explorer in Configuration Studio, click **Stations and Consoles**.
- 2 Click the **Configure Console Stations** task.
- 3 Click the name of the Console Station you want to add to the console.
- 4 From the **Console** list, select the name of the console to which this Console Station is to be added.
- 5 If you want this Console Station to use the settings configured for the console, select the **Use Console settings for Station configuration** check box.

Deleting Console Stations from a console

To delete a Console Station from a console:

- 1** In Station choose **Configure > System Hardware > Stations > Console Stations**.
The Console Station Configuration Summary display opens.
- 2** Click the Console Station you want to delete from the console.
- 3** From the Console list, click the blank space at the top of the list of consoles.

Deleting a console

Prerequisites

- Any Console Stations within the console must be disconnected from the server.

To delete a console:

- 1 In Station choose **Configure > System Hardware > Consoles**.
The Console Configuration Summary display opens.
- 2 Click the console you want to delete.
- 3 Click **Delete**.
- 4 Click **Yes** to confirm the deletion.

About alarm and message acknowledgement/silence synchronization

The Alarm and Message Summaries on a Console Station are independent of the Alarm and Message Summaries on the Experion server and any other Console Stations. This allows the Alarm Summary and Message Summary on a Console Station to receive alarms and messages (from all points and controllers connected directly to the Console Station node) when the Experion server is unavailable. In addition, the alarms and messages can be acknowledged, confirmed and silenced when the Experion server is unavailable. This ensures continuous availability regardless of the operational state of the server.

In the event that an action such as alarm or message acknowledgment occurs when the Experion server is unavailable, synchronization of that action is maintained between available Console Stations. Synchronization with the server occurs when the Experion server becomes available.

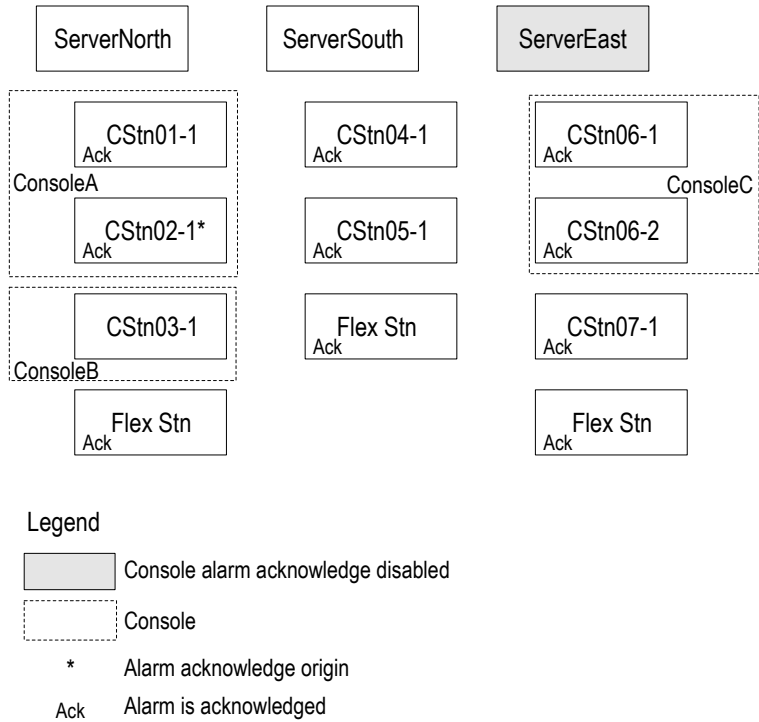
Alarm acknowledgement and consoles

In a system without consoles, the default alarm acknowledgement behavior is such that when an alarm is acknowledged on a Station, either a Console Station, Console Extension Station, or a Flex Station, the alarm is acknowledged on all Stations. However, if you configure consoles, by default, all alarms must also be acknowledged in every console. You can change the alarm acknowledgement behavior for consoles so that when an alarm is acknowledged, it is acknowledged on all Stations within the console.

Figure 38 on page 553 shows a DSA system using the default system wide alarm acknowledgement policy for DSA. `ServerNorth` and `ServerSouth` are using the default console alarm acknowledgement behavior. `ServerNorth` has two consoles, `ConsoleA` and `ConsoleB`. `ServerEast` has `ConsoleC`. If an alarm is acknowledged on `Cstn02-1`, connected to `ServerNorth`, the alarm is acknowledged elsewhere as follows:

- The alarm is acknowledged on `Cstn01-1`, `Cstn02-1` (where the acknowledge action occurred), and `Flex Stn` but must be acknowledged separately in `consoleB` because the server is using the default console alarm acknowledgement setting.
- Alarms are acknowledged on all Stations connected to `ServerSouth` because there are no consoles.
- Alarms are acknowledged on all Stations connected to `ServerEast` because the server has been configured so that when an alarm is acknowledged on one Station, it is acknowledged on all Stations, including Console Stations within a console.

Figure 38 Alarm acknowledgement behavior



To enable or disable console alarm acknowledgement:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm and event options** task.
- 3 On the **Alarm/Event Options** tab under **Alarm/messages must be acknowledged**, select the required option as described in the following table.

Property	Description
At each console	If selected, if the alarm is acknowledged on a Station in a console, the alarm is acknowledged on all Stations in the same console and all Stations not in another console. If the alarm is acknowledged on a Station not in a console the alarm is acknowledged on all Stations not in a console.
Once (applies to all Stations)	If selected, acknowledges the alarm on all Stations including Flex Stations, Console Stations, and Console Extension Stations.

Alarm silence and consoles

In a system that does not have consoles, the default alarm silence behavior is such that when you silence an alarm it is silenced on the Station where the silence action was implemented only. If you have consoles, the default alarm silence behavior is such that when an alarm is silenced on a Station within a console, the alarm is silenced on all Stations within the console, but is not silenced on Stations external to the console. You can change the silence behavior such that when an alarm is silenced on a Station, it is silenced on all Stations, regardless of whether or not the original silence action was performed on a Station in a console.

Figure 39 on page 555 shows how the alarm silence is handled for each silence option.

When the Silence single Station or single console option is enabled, if the alarm is silenced on `csn02-1`, it is also silenced on `csn01-1` because these two Stations form a console. The alarm is not silenced on other Stations connected to the server.

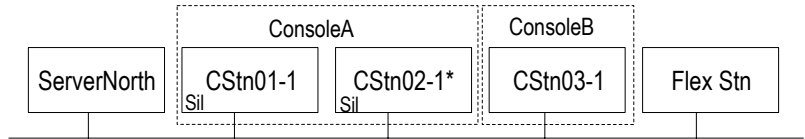
When the Silence all Stations option is enabled, if the alarm is silenced on `csn02-1`, the alarm is silenced on all Stations connected to the server.

When the Silence single Station only option is enabled, if the alarm is silenced on `csn02-1`, it is silenced on this Station only.

Figure 39 Alarm silence behavior

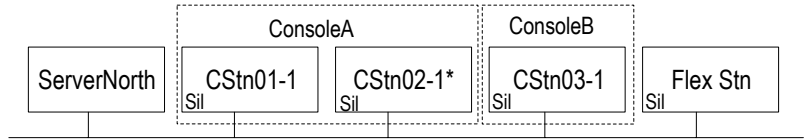
Scenario 1

Silence single Station or single console enabled



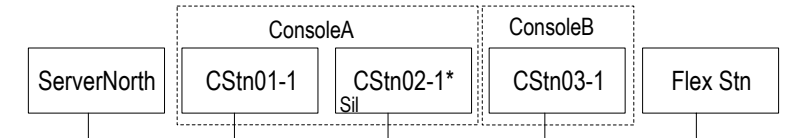
Scenario 2

Silence all Stations enabled



Scenario 3

Silence single Station only enabled



Legend

- Console
- * Alarm silence origin
- Sil Alarm is silenced

To configure the alarm silence behavior:

- 1 In the Configuration Explorer in Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm and event options** task.
- 3 On the **Alarm/Event Options** tab under **Silence action applies to**, select the required option as described in the following table.

Property	Description
Single Station only	If selected, silences the alarm on the Station where it is silenced. The alarm is not silenced on other Stations
Single Station or single Console (all Stations in console)	If selected, if the alarm is silenced on a Station within a console, the alarm is silenced on all Stations in the console but not on any Stations outside the console. If the alarm is silenced on a Station not in a console, the alarm is silenced on the Station where the silence action occurred but the alarm is not silenced on any other Stations.
All Stations	If selected, silences the alarm on all Stations, including Flex Stations, Console Stations, and Console Extension Stations, that are connected to the same server.

Sending displays to another Console Station

In a console, you can configure keyboard shortcuts, toolbar buttons or display scripts that enable an operator to send the current display or the next display to another Station within the console.

For information about creating display scripts to send displays to other Stations within the console, see the section “Example Scenarios” in the *HMIWeb Display Building Guide*.

Considerations



Attention

You can send system displays or custom displays created with HMIWeb Display Builder or Display Builder. You cannot send web pages or other documents.

Example scenario—sending the current display to another Station

You have a console called `consoleA`. Within `consoleA` you have Console Stations and Console Extension Stations, `cstn01-1`, `cstn02-1`, `cstn02-2`. You want operators to use the keyboard shortcut CTRL+K to send the current display to `cstn02-2`.

Solution

The solution involves the following steps:

- Creating a new command to send the current display.
- Applying the keyboard shortcut to the new command.
- Saving these customizations in an `stb` file. For the purpose of this example, `console.stb` is used.
- Copying the `console.stb` file to all Stations within the console.

This solution assumes:

- The `default.stb` file has not been customized and is used as the basis for creating `console.stb`.

To implement the solution:

- 1 In Station choose **File > Connection Properties**.
The **Connection Properties** dialog box opens.
- 2 Click the **Toolbars** tab.
- 3 In the **Menu, toolbar & keyboard shortcuts** box, specify `default.stb`.

- 4 Click **Customize**.
The **Customize** dialog box opens.
- 5 Click **New Command**.
The **Command Properties** dialog box opens.
- 6 In the **Name** box, type **Current display to cstn02-2**.
- 7 Place the cursor in the **Enter keyboard shortcut** box and press CTRL+K.
- 8 From the **Action** list, select **Current Display to**.
- 9 In the **Location** box, type **cstn02-2**.
- 10 Click **OK**.
- 11 Click **Save As**.
- 12 In the **File Name** box, type **console.stb**.
- 13 Click **Save**. **console.stb** is now listed in the **Menu, toolbar & keyboard shortcuts** box.
- 14 Click **Save** to save **console.stb** in the connection properties.

Example scenario—sending the next display to another Station

You have a console called **consoleA**. Within **consoleA** you have Console Stations and Console Extension Stations, **cstn01-1**, **cstn02-1**, **cstn02-2**. You want operators to use the keyboard shortcut CTRL+N to send the next display called up to **cstn02-2**.

Solution

The solution involves the following steps:

- Creating a new command to send the next display.
- Applying the keyboard shortcut to the new command.
- Saving these customizations in an stb file. For the purpose of this example, **console.stb** is used.
- Copying the **console.stb** file to all Stations within the console.

This solution assumes:

- The **default.stb** file has not been customized and is used as the basis for creating **console.stb**.

To implement the solution:

- 1 In Station choose **File > Connection Properties**.
The **Connection Properties** dialog box opens.
- 2 Click the **Toolbars** tab.

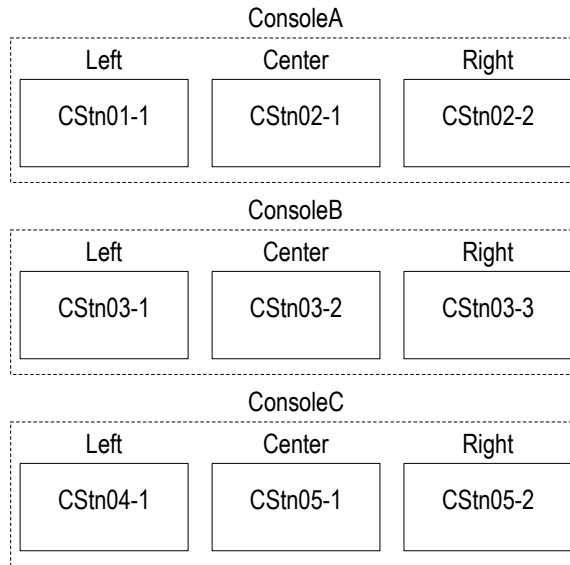
- 3 In the **Menu, toolbar & keyboard shortcuts** box, specify `default.stb`.
- 4 Click **Customize**.
The **Customize** dialog box opens.
- 5 Click **New Command**.
The **Command Properties** dialog box opens.
- 6 In the **Name** box, type **Next display to cStn02-2**.
- 7 Place the cursor in the **Enter keyboard shortcut** box and press CTRL+N.
- 8 From the **Action** list, select **Next Display to**.
- 9 In the **Location** box, type **cStn02-2**.
- 10 Click **OK**.
- 11 Click **Save As**.
- 12 In the **File Name** box, type **Console.stb**.
- 13 Click **Save**. `console.stb` is now listed in the **Menu, toolbar & keyboard shortcuts** box.
- 14 Click **Save** to save `console.stb` in the connection properties.

Sending displays using aliases

If you specified a Station alias when you configured your Console Station you can use the alias to specify the destination when you configure shortcuts or menus to send displays to other Stations within the console.

Using the alias as the destination enables you to reuse customized shortcut keys menus or display scripts for other consoles, assuming that the aliases are the same in all your consoles.

The following figure shows three separate consoles using the Station aliases `Left`, `Center`, `Right`. In this situation you could reuse your customized `.stb` file in all consoles if you configure your keyboard shortcuts or toolbar buttons using the Alias as the destination rather than the Station name.



Example scenario—sending the current display to another Station using an alias

You have a console called `consoleA`. Within `consoleA` you have Console Stations and Console Extension Stations, `cstn01-1`, `cstn02-1`, `cstn02-2`. You want operators to use the keyboard shortcut `CTRL+U` to send the current display to `cstn02-2` using the alias.

Solution

The solution involves the following steps:

- Creating a new command to send the current display.
- Applying the keyboard shortcut to the new command.
- Saving these customizations in an `stb` file. For the purpose of this example, `console.stb` is used.
- Copying the `console.stb` file to all Stations within the console.

This solution assumes:

- The `default.stb` file has not been customized and is used as the basis for creating `console.stb`.
- The alias for `CStn02-2` is `right`.

To implement the solution:

- 1 In Station choose **File > Connection Properties**.
The **Connection Properties** dialog box opens.
- 2 Click the **Toolbars** tab.
- 3 In the **Menu, toolbar & keyboard shortcuts** box, specify default.stb.
- 4 Click **Customize**.
The **Customize** dialog box opens.
- 5 Click **New Command**.
The **Command Properties** dialog box opens.
- 6 In the **Name** box, type **Current display to Right**.
- 7 Place the cursor in the **Enter keyboard shortcut** box and press CTRL+U.
- 8 From the **Action** list, select **Current Display to**.
- 9 In the **Location** box, type **Right**.
- 10 Click **OK**.
- 11 Click **Save As**.
- 12 In the **File Name** box, type **console.stb**.
- 13 Click **Save**. console.stb is now listed in the **Menu, toolbar & keyboard shortcuts** box.
- 14 Click **Save** to save console.stb in the connection properties.

Configuring eServer

24

This chapter provides an overview of eServer and describes the steps required to configure eServer.

About eServer

The eServer combines Experion server and Web server technology, enabling you to provide secure read-only access to casual users. For example, your production manager requires access to the latest production figures, but does not need control of the process. eServer can provide your production manager with read-only access to your process graphic displays without providing any control.

The eServer enables you to provide users with read-only access to your plant data using a standard Web browser. Users are isolated from control of the plant and therefore do not have access to process alarms, that is, users cannot view or acknowledge alarms. The level of access provided is similar to the view only security level, excluding alarm management. For a list of the actions permitted at the view only security level, see “Actions permitted at each security level” on page 341.

The eServer calls up your process graphic displays and serves them as a read-only version to your casual users on request. Casual users can navigate to your process schematics and other displays in the same way as navigating to any Web site or Web page.

There are two types of access to the eServer:

- standard access
- premium access

With standard access, users are provided with a “snapshot” of your plant displays with data current at the time of navigating to the display using any Web browser. Users are limited to using the navigation controls on the pages. Standard access users only require a Web browser, and do not need to download or install additional software.

With premium access, users are provided with “live” plant displays with updating data, using Internet Explorer. Their interaction is limited to navigation controls and copying trend and report data to other applications such as Microsoft Excel and Microsoft Word. Premium access users need to download a small self-installing package before connecting to eServer.

eServer configuration procedures

Prerequisites

- You have installed the eServer software and Internet Information Services (IIS) as described in the topics “Installing an eServer” and “Installing Internet Information Services” in the *Software Installation and Upgrade Guide*.

After installing eServer and IIS, you need to complete the following configuration tasks:

- Set up eServer to access the other Experion servers in your system. See “Setting up eServer access to Experion servers” on page 566.
- Secure your eServer. See “eServer security” on page 569.
- Set up “home” pages so that users can navigate to the required displays and provide details of the links/URLs to users. See “Setting up a home page for eServer” on page 574.

Setting up eServer access to Experion servers

The eServer accesses other Experion servers in your system using Distributed System Architecture technology.

The tasks required to set up the eServer are similar to setting up a server in a DSA system.

Note that an eServer requires a DSA license for each Experion server that it subscribes to. For information on DSA licensing, see the topic “DSA” in the chapter “Servers” in the *Server and Client Planning Guide*.

You need to complete the following tasks to enable eServer to access the other Experion servers:

Task	Go to	Done
Define your eServer using Enterprise Model Builder. Ensure that you check the Non-Publishing Server check box.	Knowledge Builder > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Add servers	
Load the system model to your eServer using Enterprise Model Builder.	Knowledge Builder > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Load system configuration	
Load the asset model to your eServer using Enterprise Model Builder.	Knowledge Builder > Enterprise Model Builder User's Guide > Accessing Enterprise Model Builder > Load asset model and alarm groups	
Assign scope of responsibility to the eServer Stations.	“Assigning scope of responsibility to Flex Stations” on page 338	
Ensure that all custom displays (including those specifically developed for eServer) are stored locally in the eServer display folder. (The default folder for custom displays is Program Files\Honeywell\Experion PKS\Client\Abstract.) Note also that Trends need to be configured locally on each eServer.	See the <i>HMIWeb Display Building Guide</i> . “Configuring trend displays” on page 366	
If user-defined acronyms are used on custom displays files, copy these user-defined acronyms to the server using fildmp.	<i>Application Development Guide</i>	

Tuning eServer for standard access

The eServer configuration tool enables you to specify:

- The size of pages served by the eServer
- Cache time

To set the size of pages served by the eServer, you specify the image height and width in pixels. If both are set to zero (the default) pages appear in the client browser at the resolution of the eServer. If you specify a width and height, pages appear at the specified dimensions, regardless of the eServer resolution.



Attention

Correct aspect ratio is not enforced. Ensure that the height and width you specify delivers a valid aspect ratio.

If displays are required to support non-standard aspect ratios, such as PDA displays, custom displays should be designed for this purpose.

The cache time is the time, in seconds, that the snapshot of display pages is kept and served to users. When a page older than the cache time is requested, an updated page is served. Often the pages will not update very frequently (for example monthly production records) therefore you do not require a new snapshot of the page for each client that requests the page.

The cache time you specify will significantly affect the performance and scalability of eServer standard access. Setting longer cache times allows the eServer to function mainly as a Web server, rather than forcing regular requests to the eServer process database. As a Web server with few requests to the process database, standard access can serve thousands of users. However, if used to provide a frequently updating view of process data, as few as 10-20 users may be served.

The table below describes other settings you can change using the configuration tool. Information for these settings is supplied during installation. We recommend that you do not change these settings.

Property	Description
Configuration file	The stn file that defines the standard access connection to the eServer database. This is preconfigured to point to the local database and to retrieve display files only from the eServer display folder. You should not need to change this file.
Username	The name of the operator that is used when connecting to Station. The default is oper.
Password	This allows a password to be supplied for the current user. This will not be used with Experion systems.

Property	Description
URL of eServer machine	This is the URL that is used to access the eServer machine. This is set during installation.
Standard access Web root directory	This is the folder that standard access uses to serve files out to clients. This is set during installation.

If you change any of these settings, you need to restart your eServer computer.

eServer security

There are several security considerations you need to be aware of when setting up your eServer.

- Securing access to the eServer by using IIS to restrict access for casual users and blocking access to your connected Experion systems using firewalls.
- The Station connections that occur when users access eServer (Station-based security for the eServer administration Station and operator-based security for Premium Access users)
- Restricting the data that can be viewed via eServer by assigning assets for all eServer Standard Access clients and each Premium Access client.

Securing access to the eServer

By default, all users on the same network as your eServer have standard access privileges to the eServer. If you want to restrict the access of certain users, you can use Internet Information Services (IIS) to secure the eServer. For information about using IIS to restrict access, see the topic “Internet Information Services” in the chapter “Securing access to the Windows operating system” in the *Network and Security Planning Guide*.

You should also consider securing access to your connected Experion systems via the eServer. For example, you could use a firewall between the eServer and your Experion system. For information about firewall settings for eServers, see the topic “Firewall configuration” in the chapter “Network Security” in the *Network and Security Planning Guide*.

eServer Stations and operators

To facilitate the eServer serving pages to casual users, Station connections are required. During installation, several Stations are defined. Two static Stations using Station-based security are created, one for administration tasks that need to be done on the eServer, the other required for standard access. The remaining Stations are rotary connections using operator-based security. These Station connections are required for premium access.

In addition to the Stations, an operator definition is created. The operator definition is locked with a security level of `view onlyLVL1`, which is a view-only security level.

Restricting access to assets

You assign assets to the eServer Stations and operators to control access to your Experion system. For example, you may have sensitive data contained in a report to which casual users should not have access. Assign this report to an asset which is only assigned to the appropriate operators.

For information on assigning assets, see “Assigning scope of responsibility” on page 336.

Considerations for Standard Access displays

You can make your existing Experion process graphic displays available on eServer or optionally create displays specifically for eServer. Displays can be DSP or HMIWeb. When providing or creating displays for your eServer you should consider:

- Because eServer users do not have access to the standard Station navigation aids, you need to create a home page that provides adequate navigation to the displays that users can access via eServer. When creating eServer displays, you therefore need to add navigation aids such as push buttons with display callup actions or task requests that call up displays or hyperlink objects.
- Controls that require interaction with the host system, such as combo boxes, do not work.
- Do not use animation because standard access users will only see a static snapshot.
- Not every kind of display can be viewed via eServer. For example, Alarm, Event, Message, and Alert Summary displays use scripts and other interactive controls that are not available under “view only” access.
- Ensure that the information you put on a page can be displayed without scrolling. Scroll bars that appear in displays are not active using standard access.
- Alphanumeric data objects are used to display dynamic data. If you use alphanumerics, consider that the data display will not update with standard access.
- If you want to provide access to reports, consider the difference between calling up a report and requesting a report. Users will only be able to call up a report.
- There are various restrictions associated with the use of eServer: some are a consequence of eServer’s “view only” access; some are associated with the use of the Web browser interface (as opposed to the Station interface). For more information, see “Actions permitted at each security level” on page 341.

Considerations for Premium Access displays

With premium access, the displays are delivered to connected clients by different methods. By default, HMIWeb displays are served by IIS and DSP displays are shared through Microsoft Windows file sharing.

For premium access clients to view DSP displays, the client computer must be able to access file shares on the eServer. This means that the client and eServer computers must be on the same network. If the eServer computer is behind a firewall, you need to either have the DSP displays available locally on the client or else ensure that specific ports are opened in the firewall to enable file sharing, otherwise DSP displays cannot be viewed. For information on enabling file sharing and on eServer and firewalls, see the topic *Configuring the DMZ firewall in the Network and Security Planning Guide*.

HMIWeb displays can be viewed regardless of the network configuration.

Accessing DSP displays where the eServer computer is behind a firewall

To allow client computers to access DSP displays where the eServer is behind a firewall, the required DSP displays must be copied from the eServer to a directory on the client computer. Then the `default.stn` file must be modified to point to the location of the local DSP display files.

To modify the `default.stn` file to access DSP displays:

- 1 Using Windows Explorer, clear the read-only attribute of the `default.stn` file located with the eServer display files. The default path to this file on the eServer is:
`C:\Program Files\Honeywell\Experion PKS\Client\System\R300`
- 2 Open the `default.stn` file in a text editor.
- 3 Locate the [PATHS] section. Add a new PATH entry with a value set to the name of the local folder on the client computers containing the DSP display files.

For example:

```
PATH3=C:\Program Files\Honeywell\Experion PKS\Client\
MyLocalDisplays\
```

This is the path to the DSP displays on the client computer. This folder does not need to exist on the eServer, however, it must exist on each client computer that is required to view the DSP displays.

- 4 Save the file.

About eServer Trend displays

Note that eServer's "view-only access" has a number of implications for Trend displays. The following table shows what can and what cannot be done with Trend displays accessed via an eServer:

Action	Permitted?
View	Yes
Zoom	Yes
Scroll	Yes
Modify	No
Configure	No

Setting up a home page for eServer

eServer provides a default home page. The URL is `http://MyServer/eServer` where *MyServer* is the name of the eServer computer. This page provides access to:

- The standard access home page. This HMIWeb page is located in the `Program Files\Honeywell\Experion PKS\client\R300\eServer` folder and can be modified to provide links to your commonly used standard access pages.
- The download links for premium access. Premium access users need to download self-installing packages for the premium access client to be able to access eServer pages.
- The premium access home page. This is a HMIWeb page located in the `Program Files\Honeywell\Experion PKS\client\R300` folder and can be modified to provide links to commonly used premium access pages.

After you have set up your eServer and created your displays, distribute the URL of the eServer home page to your users. For example, you could send the URL as a link in an email. Users can then bookmark the URL.

Configuring Mobile Station

25

Mobile Station comprises a series of solutions that enable access from remote devices to Station.

A remote device can be:

- A handheld or similar mobile device on a wireless network.
- A computer on a remote network.
- A computer that is not on your Experion network (for example, a computer that is connected to your business network).
- A computer that is not running Microsoft Windows.

This chapter describes the range of Mobile Station solutions and the configuration procedures required to enable mobile access to Station from remote devices.

About Mobile Station

Mobile Station is a series of solutions that enable you to access your Experion system from remote devices. If you have a wireless network, for example, you can use Mobile Station to provide mobile access to your plant data, wherever it is needed.

The following solutions are available under Mobile Station:

- **Mobile Access for Station** provides you with remote access to full Station capabilities. Users have the same level of control of the plant from their remote device as they would from Station on a desktop computer.
The Remote Engineering and Station Server that enables remote access to Station can also be used to enable remote access to Configuration Studio, the Experion configuration tool.
- **Mobile Access for eServer Premium** provides “live” plant displays with updating data, using Internet Explorer. Users do not have any control of the plant and do not have access to process alarms. Their interaction is limited to navigation controls.
- **Mobile Access for eServer Standard** provides a “snapshot” of your plant displays with data current at the time of navigating to the display using any Web browser. Users do not have any control of the plant and therefore do not have access to process alarms. They are also limited to using the navigation controls on the pages.

For more information about:	See:
Mobile Access for Station	“Configuring and connecting to Mobile Access for Station” on page 582. For information about remote access to Configuration Studio, see “About Remote Engineering and Station Server” on page 580.
Mobile Access for eServer Premium	“Configuring and connecting to Mobile Access for eServer Premium” on page 585.
Mobile Access for eServer Standard	“Using Mobile Access for eServer Standard” on page 577

Using Mobile Access for eServer Standard

Mobile Access for eServer Standard does not require any special software or any installation or configuration procedures.

Prerequisites

The prerequisites for using Mobile Access for eServer Standard are:

- You have set up and configured an eServer (see “Configuring eServer” on page 563)
- A Web browser is installed on the remote device.

All Honeywell-recommended remote devices have a built-in web browser and do not require any installation. For other remote devices, refer to the manufacturer’s instructions to find out if there is a web browser available and how it can be installed.

To connect to eServer Standard from your remote device:

- 1 Start the web browser on the remote device.
- 2 Type the address of the eServer into the address bar:
`http://computer name/eserver`
where *computer name* is the name of the eServer (see “Setting up a home page for eServer” on page 574).
- 3 Click the hyperlink for the eServer Standard home page.

Configuring Remote Engineering and Station Server

26

A Remote Engineering and Station Server is a computer that supports remote access to Station and the Experion configuration tool, Configuration Studio.

This chapter describes the procedures for configuring, and connecting to, a Remote Engineering and Station Server.

About Remote Engineering and Station Server

A Remote Engineering and Station Server enables you to provide remote access to Station and Experion configuration tools on remote devices that have not had Experion Station or other Experion components installed.

This gives you the flexibility to provide Station and engineering access to those who need to use:

- Handheld and similar mobile devices on a wireless network.
- Remote networking.
- Computers that are not on your Experion network (for example, computers that are connected to your business network).
- Computers that are not running Microsoft Windows.

You can set up a Remote Engineering and Station Server to enable remote access to either full Flex Station functionality (Mobile Access for Station) or to eServer Premium displays (Mobile Access for eServer Premium). For an explanation of the difference between these two types of remote access to Station, see “About Mobile Station” on page 576.

Configuration and connection guidelines

When setting up and connecting to a Remote Engineering and Station Server you need to bear in mind the following:

- A Remote Engineering and Station Server can only be configured to support:
 - Either Mobile Access for eServer Premium
 - Or Mobile Access for Station.

That is, you need to set up separate Remote Engineering and Station Servers for each type of access.

A Remote Engineering and Station Server that provides remote access to Station can, however, also be used to provide remote access to Configuration Studio.

- The maximum number of concurrent remote access sessions that a Remote Engineering and Station Server supports is 5.

Notes

- Within this maximum number of 5 concurrent sessions you can have a maximum of 5 concurrent connections to Station or 4 concurrent connections to Configuration Studio (or a mix of both types of connections provided that you do not exceed the individual limits for each type of connection).

Note that you cannot run separate instances of Station and Configuration Studio within the one session. This means that if you launch Station on the remote device, you cannot then start up Configuration Studio. However, because Station is one of the suite of configuration tools available under Configuration Studio, you can access Station via Configuration Studio even though you cannot launch a separate instance of Station during that session.

- Although you can run 4 concurrent connections to Configuration Studio, only one of those connections can run the Quick Builder component of Configuration Studio at any one time.

Configuring and connecting to Mobile Access for Station

Before a remote device can access Station or Configuration Studio, you need to configure:

- The Remote Engineering and Station Server
- The remote device

Considerations

Check that your Experion server has enough licensed Stations to allow for concurrent direct Station connections as well as remote connections to Station via a Remote Engineering and Station Server.

Remote Engineering and Station Server

Prerequisites

- You have installed a Remote Engineering and Station Server for Mobile Access for Station as described in “Installing Remote Engineering and Station Server” in the *Software Installation and Upgrade Guide*.

This includes completing the following procedures on the Remote Engineering and Station Server node:

- Installing Terminal Services Server.
- Installing Experion Flex Station.
- Creating the required Windows accounts for the users who require access to the Experion server.
- Configuring the Windows user accounts.

The following procedures need to have been completed on the Experion server:

- Building the required number of rotary stations with operator-based security on the Experion server.
- Creating the required number of operators on the Experion server (see “Adding an operator” on page 306).
- The Remote Engineering and Station Server is connected to the Experion server via the Experion network. For information on configuring firewall access for an Engineering Station, see the topic “Enterprise Model Update” in the chapter “Network Security” in the *Network and Security Planning Guide*.

Configuring the Station connection

- 1 On the Remote Engineering and Station Server node, create a separate .stn file for each Experion server that needs to be accessed remotely (see “Configuring Station connections” on page 72).

The .stn files that you create must:

- Connect to the appropriate Experion server.
- Use rotary connections.
- Specify a fully qualified path to your custom displays folder on the Experion server. For example, \\servername\Program Files\Honeywell\Experion PKS\client\abstract where *servername* is the name of the Experion server.

Remote devices

Prerequisites

- If necessary, install (or locate) terminal services client software on the remote device.

Remote devices connect to a Remote Engineering and Station Server by means of terminal services client software. If you are using:

- Microsoft Windows XP or Windows Server 2003, this software is known as Remote Desktop Connection.
- Microsoft Windows Mobile Software for Pocket PC, it is known as Terminal Services Client.

All Honeywell recommended remote devices have a built-in terminal services client software and do not require any installation. For other remote devices, refer to the manufacturer’s instructions to find out if there is a terminal services client available and how it can be installed.

Connecting to Station or to Configuration Studio

To connect to Station or to Configuration Studio from a remote device:

- 1 Open the **Remote Desktop Connection** or **Terminal Services Client** dialog box. See “Starting Microsoft Terminal Services Client or Remote Desktop Connection” on page 588.
- 2 In the **Server** box type the name of the Remote Engineering and Station Server. This is the computer name (as specified in the `hosts` file).
- 3 If you are using Terminal Services Client, make a selection from the **Screen area** list. It is recommended that you choose a high resolution to ensure that Station (or Configuration Studio) display correctly.
- 4 Click **Connect**.

To access Station:

- 1 Choose **Start > Programs > Honeywell Experion PKS > Station**.
- 2 If required (that is, if operator-based security is being used for Station), type the appropriate operator ID and password to log on to Station.

To access Configuration Studio:

- 1 Choose **Start > Programs > Honeywell Experion PKS > Configuration Studio**.

The **Configuration Studio Connect** dialog box opens.

- 2 Select the system to which you want to connect and click **Connect**.
The **Login to Server** dialog box opens.
- 3 Type your logon details and click **OK**.

Configuring and connecting to Mobile Access for eServer Premium

Before a remote device can access eServer Premium, you need to configure:

- The Remote Engineering and Station Server
- The remote device

Considerations

With eServer Premium, you are licensed for a certain number of users. Mobile Access for eServer Premium makes use of these existing eServer Premium user licenses. Ensure that the number of eServer Premium users is adequate to support concurrent eServer Premium users and Mobile Access for eServer Premium users.

Remote Engineering and Station Server

Prerequisites

- You have installed a Remote Engineering and Station Server for Mobile Access for eServer Premium as described in “Installing Remote Engineering and Station Server” in the *Supplementary Installation Tasks Guide*.

This includes completing the following procedures on the Remote Engineering and Station Server node:

- Installing Terminal Services Server.
- Installing Experion eServer client.
- Creating the required Windows accounts for the users who require access to the Experion server.
- Configuring the Windows user accounts.

The following procedures need to have been completed on the Experion server:

- Building the required number of rotary stations with operator-based security on the Experion server.
 - Creating the required number of operators on the Experion server (see “Adding an operator” on page 306).
- The Remote Engineering and Station Server can connect to the eServer.

Remote devices

Prerequisites

- If necessary, install (or locate) terminal services client software on the remote device.

Remote devices connect to a Remote Engineering and Station Server by means of terminal services client software. If you are using:

- Microsoft Windows XP and Windows Server 2003, this software is known as Remote Desktop Connection.
- Microsoft Windows Mobile Software for Pocket PC, it is known as Terminal Services Client.

All Honeywell recommended remote devices have a built-in terminal services client software and do not require any installation. For other remote devices, refer to the manufacturer's instructions to find out if there is a terminal services client available and how it can be installed.

Connecting to eServer Premium

To connect to eServer Premium from a remote device:

- 1 Open the **Remote Desktop Connection** or **Terminal Services Client** dialog box. See “Starting Microsoft Terminal Services Client or Remote Desktop Connection” on page 588.
- 2 In the **Server** box type the name of the Remote Engineering and Station Server. This is the computer name (as specified in the `hosts` file).
- 3 If you are using Terminal Services Client, make a selection from the **Screen area** list. It is recommended that you choose a high resolution to ensure that Station (or Configuration Studio) display correctly.

- 4 Click **Connect**.

Internet Explorer starts up and displays the eServer home page as set up during the installation procedures (see “Mobile Access for eServer Premium checklist” in the section on “Installing a Remote Engineering and Station Server” in the *Supplementary Installation Tasks Guide*).

- 5 If you are connecting to eServer Premium Access for the first time, the eServer home page will be displayed with instructions for installing eServer for Premium Access.

Follow the procedures for installing the components for eServer for Premium Access.

- 6 Once eServer for Premium Access is installed on the remote device, you can access Station from your Web browser (see “Setting up a home page for eServer” on page 574).
- 7 Type the required operator ID and password to log on to the eServer.

Starting Microsoft Terminal Services Client or Remote Desktop Connection

To start Remote Desktop Connection (Windows XP):

- Choose **Start > Programs > Accessories > Communication > Remote Desktop Connection**.

The **Remote Desktop Connection** dialog box opens.

To start Terminal Services Client (Windows Mobile Software for Pocket PC):

- Consult the documentation for your device.

Configuring File Replication

27

The File Replication Service is a network file copying tool which is integrated with Experion. The File Replication Service:

- Copies user files between servers in a DSA system on schedule.
- Copies user files between a server and client on schedule.
- Keeps folders synchronized between servers in a DSA system.
- Synchronizes a folder between a server and client.
- Keeps an entire folder sub-tree synchronized between servers and between a server and client.
- Copies files from an Experion server to Console Stations.
- Copies files from Experion server to Console Extension Stations

This chapter describes:

- How to configure the File Replication Service
- How to use the File Replication Service

Understanding File Replication

If you have Console Stations, you must use File Replication so that alarm, message, alert, and event summary views, category and attribute mapping files, and custom displays and shapes are replicated to Console Stations from the Experion server.

The File Replication Service can also be used in large DSA systems to provide a reliable way to keep important files, such as custom displays and reports, synchronized between servers. For servers with large numbers of client computers, it can improve client access by allowing displays and other files to be replicated to client computers.

The File Replication Service does not copy any databases. If you have a redundant system, database synchronization is configured when you configure your redundant system.

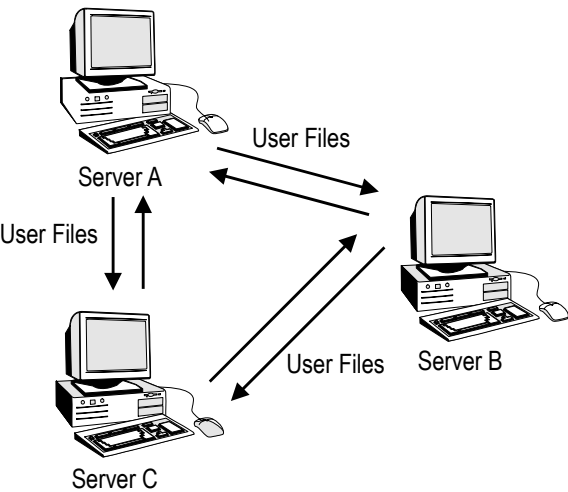
About replications

A *replication* is an object that represents a set of files to be copied from computer to computer. A replication:

- Has a unique name (up to 16 characters) to differentiate it from all other replications.
- Name must be common across all computers participating in the replication.
- Is configured separately at both the source and the destination server and destination client.
- Is mapped to a local share path on each server. Any files sent or received in this replication are stored in this path.
- The name of the share will match the name of the replication object.
- On each server has its own schedule and set of options for copying files.
- Cannot copy files that are locked by the Windows operating system.

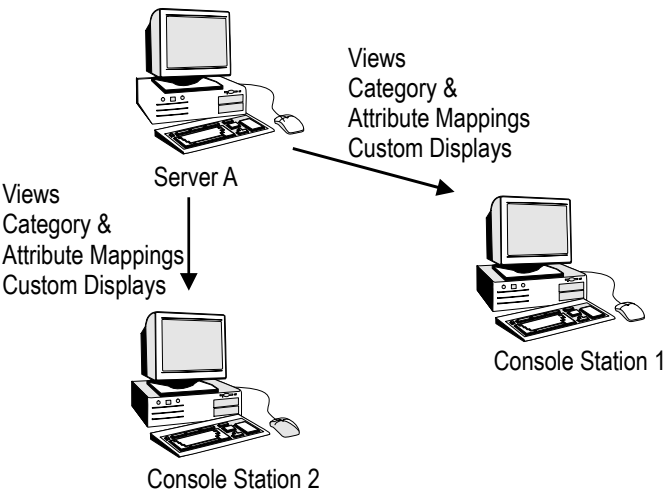
Servers can be both sources and destinations for files in a replication. The following figure shows three servers in a distributed network. All three servers are both sources and destinations for the replication of user files.

Figure 40 Source and destination servers in a DSA



A Console Station is a client and therefore only ever receives files. The following figures shows a server and two Console Stations. Server A is the source of all view files, category and attribute mapping files, and custom displays.

Figure 41 Source server and Console Stations



Configuring File Replication

The steps for configuring File Replication vary depending on where File Replication is required.

You configure File Replications using:

- The File Replication Summary display.
- The File Replication Settings display.
- Windows Explorer.

File Replication for DSA

To configure File Replication Services for use in DSA, complete the tasks in the following order.

Task	Go to	Done?
Configure replications on each source and destination Experion server.	page 595	
If you have redundant servers, prepare the backup server.	page 598	

File Replication for redundant servers

If you have redundant servers you need to be aware of how files are replicated.

If you have redundant servers in a DSA environment and you select the **All distributed servers** option when you configure the source server in the replication, the backup server automatically receives files, however you need to prepare the backup server as described in the section “Preparing the backup server” on page 598.

If you have redundant servers that are the only destination in a replication, you need to specify both the primary and the backup server to receive files when you configure the replication on the source server. You also need to configure the replication on the primary and prepare the backup server as described in the section “Preparing the backup server” on page 598.

File Replication for Console Stations

Considerations

- When you install Experion on your server, several replications are created automatically. These replications are configured to replicate files for the following folders to all Console Stations connected to the server:
 - Program Files\Honeywell\Experion PKS\server\data\views.
Contains view files for the Alarm, System Alarm, Alert, Message, Events, and SOE Summary displays.
 - Program Files\Honeywell\Experion PKS\server\data\mapping.
Contains notification, category and attribute mapping files.
 - The folder where custom displays and shapes are stored. The default folder is Program Files\Honeywell\Experion PKS\client\abstract, however, you can choose another folder.

If you store custom displays and shapes in a folder other than the abstract folder, you need to use a unique name for the replication of the folder where you store your custom displays and shapes, for example, customDisplays.

- When you install Console Station, the network shares views, mapping, and abstract are automatically created to receive files from the replications that are automatically created on the Experion server during installation. If you choose to store custom displays and shapes in a folder other than the default, you must configure this folder on the Console Station as a network share with the same name you have given to the replication on the server.

Tasks

Complete the tasks in the following order.

Task	Go to	Done?
Configure replications on the Experion server.	page 595	
If you have redundant servers, prepare the backup server.	page 598	
If you store custom displays and shapes in a different location to Program Files\Honeywell\Experion PKS\client\abstract, configure the folder where the custom displays and shapes are stored as a network share on the Console Station computer.	page 599	

File Replication for client computers

You can configure File Replication Services to copy files any client computer, even if Experion client applications are not installed on that computer.

To configure File Replication Services for client computers, complete the tasks in the following order.

Task	Go to	Done?
Configure replications on the Experion server.	page 595	
If you have redundant servers, prepare the backup server.	page 598	
Configure replications on each client computer.	page 599	

File Replication for a Console Extension Station

You can use File Replication to copy custom displays from the Experion server so that custom displays are available on the Console Extension Station if the server is unavailable.

To configure File Replication for a Console Extension Station, complete the tasks in the following order.

Task	Go to	Done?
Modify the abstract replication (or appropriate replication if you store your custom displays in a folder other than abstract) on the Experion server to replicate files to the Console Extension Station by selecting the Specific PCs check box and adding the name of the Console Extension Station.	page 595	
If you have redundant servers, prepare the backup server.	page 598	
Create the Windows mngr account and the abstract share on the Console Extension Station as described in the section, “Configuring replications on a client computer” on page 599.	page 599	

Configuring replications on an Experion server

The following procedure describes how to configure replications on an Experion server.

If you are configuring File Replication for DSA, you need to configure replications on both the source server and the destination server in the DSA. If you want to configure a destination server only, you do *not* need to specify all the options on the File Replication Settings display.

To configure replications on the server:

- 1 On the **System Configuration Menu** display, click **File Replication**.
- 2 To create a new replication, click a blank row. To edit an existing replication click the replication name. The File Replication Settings display opens.
- 3 Complete the options as described in the following table. If you are configuring a replication to send files to Console Stations, skip this step and go to step 4.

Property	Description
Name	A unique name for this replication, up to 16 characters. This name uniquely identifies this replication across all servers and clients on your system. It must be entered identically on all servers and clients participating in this replication. This is used as the share name when setting up File Replication on a backup server or client.
Path	A local path used as the source and destination folder for files in this replication. The share path is local to your server and is independent of share paths on other servers and clients. The share path is created by Experion with a network share and the required permission.
Allow files to be replicated to this path	Specifies whether this server receives files in this replication. If selected, any servers sending files to this server under this replication name have permission to copy and overwrite files into the share path. Do not select this option if you are configuring a replication for a Console Station.
Replicate files from this path	Specifies whether this server sends files in this replication. If selected, the server can send files to destination servers and clients. The remaining options are only applicable if this option is selected.

Property	Description
Network bandwidth limit	Specify a limit to the rate at which files are replicated across the network. It is used to stop a replication from consuming too much of the network bandwidth. If set to None, files are transferred at maximum speed.
File Mask	Use a file mask to specify files in the share path as part of this replication. Files not matching the file mask are ignored on both the source and the destination computers. Leave blank to include all files in the replication.
Include subdirectories	If selected, copies all subfolders (subdirectories) of the share path. This is useful in replicating an entire folder subtree.
Overwrite existing files (even if newer)	If selected, overwrites the files at a destination server. If cleared, files are still overwritten at the destination but <i>only if they are older</i> .
Auto Purge/Mirror files (file mask will be cleared)	If selected, deletes files at the destination that do not exist at the source. Any file mask you have specified is cleared if you select this option.
All Console Stations	Applicable only if you have Console Stations. Sends files in this replication to all Console Stations connected to this server.
All distributed servers	If selected, sends files in this replication to all servers in the system. If you don't have a DSA system, this option has no effect. Note, if the DSA nodes are not on the same release and you are replicating directories holding specific data (e.g. an application compiled to work on a particular release), you should not use this option.
Specific PCs	If selected, sends files in this replication to client computers. Type the names of all client computers and Console Extension Stations.
Replicate every day at	If selected, this replication runs on a daily schedule at the time you specify. The time must be in 24 hour format.
Replicate automatically whenever files change	If selected, the replication runs automatically whenever there is a change on the share path. This option can cause the system to slow if changes occur often or the folder in which changes occur have many files.
Failed replication raises alarm of priority:	Sets the priority of alarms raised when replications fail. A journal level alarm does not appear in the alarm summary but in the event log only.

- 4 Complete this step only if you are configuring a replication to send files to Console Stations. Complete the options as described in the following table:

Property	Description
Name	A unique name for this replication, up to 16 characters. This is used as the share name on the Console Stations. When you set up replications for the folders described in the “Considerations” section, you must use the replication names identified in that section.
Path	The path of the source folder containing the files to be replicated. For example, C:\Program Files\Honeywell\Experion PKS\client\abstract.
Replicate files from this path	Select this check box to send files to destination Console Stations.
Include subdirectories	Select this check box to copy all subfolders (subdirectories) of the source folder defined in the Path box. This is useful in replicating an entire folder subtree.
Overwrite existing files (even if newer)	Select this check box to overwrite existing files on the Console Station.
Auto Purge/Mirror files (File mask will be cleared)	Select this check box to delete files on the Console Station if they do not exist in the source folder.
All Console Stations	Select this check box to send files to Console Stations connected to this server.
Replicate automatically whenever files change	Select this check box so that replication runs automatically whenever there is a change in the source folder. This option may cause the system speed to slow if changes occur often, or if the source folder has many files.

- 5 Click **Save** to save the settings.
- 6 Click **Replicate now** to complete an initial replication to each Console Station connected to the server.
- Replications with the **All Console Stations** check box selected, automatically replicate to Console Stations configured on this server.

Preparing the backup server

The backup server in redundant Experion servers is an automatic destination for all replications. However, the share folders on a backup server need to be manually created. For each replication, you must create a *network share* on the backup server.

To create a network share:

- 1 On the backup server, open **Windows Explorer**.
- 2 Select the folder that you want to use as the share path for receiving files.
- 3 Right-click and select **Properties**.
- 4 Click the **Sharing** tab.
- 5 Select **Share this folder**.
- 6 Type the name of the share. You must use the same name as the replication name on the server.
- 7 In the **Comment** box type **FILEREP**.
- 8 Click **Permissions** and add the **mngr** account, or the group containing the **mngr** account.
- 9 Click **OK** to apply the changes and close the **Permissions** dialog box.
- 10 Click **OK** to apply the changes and close the **Properties** dialog box.

Configuring replications on a client computer

Client computers are destinations for replicated files, however, they do not send files to the server.

A client computer does *not* need to have any Experion client software installed to receive replicated files. If a client computer does not have Experion client software installed, the client computer must be accessible on your network.

The steps for configuring replications on a client computer include:

- Creating the Windows mngr account. If you have Console Station installed, the Windows mngr account already exists.
- Creating a network share for each replication defined on the server. The network share must be the same source path as replication on the server, and the network share name must be identical to the replication name on the server. If you have Console Station installed, the default shares views, mapping, and abstract already exist.

To create the Windows mngr account:

- 1 On the Windows desktop, right-click on the **My Computer** icon and choose **Manage**.
- 2 Expand the **System Tools** item and then expand the **Local Users and Groups** item.
- 3 Click **Users**.
- 4 Choose **Action > New User**.
The **New User** dialog box opens.
- 5 In the **User Name** box, type **mngr**.
- 6 In the **Full Name** box, type **Experion PKS Server Manager**.
- 7 In the Password and Confirm Password boxes, type the password for this user.
The Windows mngr account password must be the same on all computers.
- 8 Clear the **User must change password at next logon** check box and then select the **Password never expires** check box.
- 9 Click **Create** to add the account.
- 10 Close the **Computer Management** dialog box.

To create a network share:

- 1 Open **Windows Explorer**.
- 2 Select the folder that you want to use as the share path for receiving files.
- 3 Right-click and select **Properties**.
- 4 Click the **Sharing** tab.

- 5 Select **Share this folder**.
- 6 Type the name of the share. You must use the same name as the replication name on the server.
- 7 In the **Comment** box type **FILEREP**.
- 8 Click **Permissions** and add the **mng**r account, or the group containing the **mng**r account.
- 9 Click **OK** to apply the changes and close the **Permissions** dialog box.
- 10 Click **OK** to apply the changes and close the **Properties** dialog box.

Using File Replication

A replication can be configured to run:

- Manually
- Automatically according to a schedule you set
- Automatically when any changes are made

You can check the status of a replication and view a report detailing information of the last replication.

Running a replication manually



Caution

The **Purge** button should be used with caution. It has the ability to delete data from destination servers and clients. It should only be used when you want to mirror the share path to all destinations.

To run a replication manually you can:

- Click **Replicate Now** on the File Replication Settings display. This runs the replication, as configured, immediately.
- Click **Replicate All Now** on the File Replication Summary display. This runs all configured replications immediately.
- Click **Purge** on the File Replication Details display. This runs the replication with the “purge” option selected. This means that all files on destinations that are not on the source are deleted at the destination. This is useful if you want to *mirror* the source share path to destinations, that is, make the share paths at the source and destination contain exactly the same files.

If you specify a file mask, using the Purge option does not delete any files on the destination server. You need to manually delete any files on the destination that are not on the server.

Running a replication automatically

Replications configured to run automatically copy any additions or modifications to the share path of the replication to destination servers without any user input. A background process runs which monitors the share path constantly for changes in the file system. If a file is added or modified, the change is replicated to all destinations immediately.

Automatic replications are useful for keeping folders synchronized with the same data across a distributed system.

Checking the status of a replication

The File Replication Details and Configuration displays show the status of a replication. The status of a replication can be:

Status	Description
Yellow (Running)	The replication is running and sending files.
Red (Failed)	Errors occurred the last time the replication ran.
Green (OK)	The replication ran without errors.
Black (Not configured)	The replication is not configured or is not configured correctly.

A report is created every time a replication runs. Click the **View Report** link on the File Replication Settings display to see a report of the last replication. The report includes:

- The time the replication ran
- The duration of the replication
- The number and names of files copied
- The names of destination servers
- Any errors encountered during the replication

The report file is overwritten every time a replication runs.

Report files are stored as text files in \Program Files\Honeywell\Experion PKS\report under the name filrep xx .rpt where xx is the replication number.

Example scenarios

Scenario

You have a DSA system set up as follows:

- Three servers, `server1`, `Server2` and `Server3`.
- One Console Station, `ConsoleStation1`.
- One Console Extension Station `consoleExtnStn`.
- Two client computers, `Client1` and `Client2`, connected to `ServerA`.

You want user files in `c:\Program Files\Honeywell\Experion PKS\user` on `server1` to be replicated to `Server2` and `Server3`, `ConsoleStation1`, `consoleExtnStn` and `Client1` and `Client2`.

The files on `server1` must be replicated once every day, automatically.

Solution

The solution involves the following steps:

- Configure `server1` as the source server
- Configure `server2` and `Server3` as destination servers
- Configure `ConsoleStation1` as a destination Console Station
- Configure `consoleExtnStn` as a destination Console Extension Station
- Configure `Client1` and `Client2` as destination clients

Configuring Server1 as the source server

Configure `Server1`, the source server to send files to all the destination computers. For details on configuring a server see “Configuring replications on an Experion server” on page 595.

For this particular scenario, configure `server1` with the following settings:

Property	Value
Name	UserFiles
Share Path	C:\Program Files\Honeywell\Experion PKS\server\user
Send files from this share path to:	Select this option. Sets <code>Server1</code> as the source server.
All Console Stations	Select this option. Sets <code>ConsoleStation1</code> as a destination Console Station.

Property	Value
All distributed servers	Select this option. Sets other servers in the DSA system as destination servers.
Client PCs named	Select this option. Type client1 , client2 , and consoleExtnStn in the boxes provided. Sets the named clients as destination clients.
Replicate every day at	Select this option. Type 23:30 in the box provided. Schedules the file replication to take place automatically once every day at the specified time.

Configuring Server2 and Server3 as destination servers

Configure Server2 and Server3, the destination servers, to receive files from Server1. For details on configuring destination servers see “Configuring replications on an Experion server” on page 595.

For this particular scenario, configure Server B and C with the following settings:

Property	Value
Name	UserFiles Ensure the name is exactly the same as the name you specified as the replication name on Server1.
Share Path	c:\Program Files\Honeywell\Experion PKS\server\user
Receive files	Select this option. Sets this server as the destination server.

Configure ConsoleStation1 as a destination Console Station

Configure ConsoleStation1 to receive files from Server1. You configure a Console Station to receive files in the same way you configure other client computers. For details on configuring destination clients see “Configuring replications on a client computer” on page 599.

For this particular scenario, configure consolestation1 with the following network share settings:

Property	Value
Shared name	UserFiles Ensure the name is exactly the same as the name you specified as the replication name on Server1.

Property	Value
Share Permissions	mng Assign permission to the mng account.

Configuring ConsoleExtStn as a destination Console Extension Station

Configure ConsoleExtStn to receive files from Server1. You configure a Console Extension Station to receive files in the same way you configure other client computers. For details on configuring destination clients see “Configuring replications on a client computer” on page 599.

For this particular scenario, configure ConsoleExtStn with the following network share settings:

Property	Value
Shared name	UserFiles Ensure the name is exactly the same as the name you specified as the replication name on Server1.
Share Permissions	mng Assign permission to the mng account.

Configuring Client1 and Client2 as destination clients

Configure Client1 and Client2, the destination clients, to receive files from server1. For details on configuring destination clients see “Configuring replications on a client computer” on page 599.

For this particular scenario, configure Client1 and Client2 with the following network share settings:

Property	Value
Shared name	UserFiles Ensure the name is exactly the same as the name you specified as the replication name on Server1.
Share Permissions	mng Assign permission to the mng account.

The system is now ready to replicate user files.

To run a replication on demand, click **Replicate now** on the File Replication details page on Server A. Any changes made to the user files folder on Server A are automatically sent to Servers B and C and the Clients 1 and 2.

Scenario

You have a DSA system set up as follows:

- Three servers HSCMyServer, HSCServerA and HSCServerB (a redundant pair) and HSCYourServer.

You want files your custom displays and shapes, stored in Program Files\Honeywell\Experion PKS\client\abstract, to be replicated only to your redundant pair, HSCServerA and HSCServerB.

The files on HSCMyServer must be replicated whenever the files change.

Solution

The solution involves the following steps:

- Configure HSCMyServer as the source server.
- Configure HSCServerA as the destination server.
- Prepare HSCServerB as the backup server.

Configuring HSCMyServer as the source server

Configure HSCMyServer, the source server to send files to HSCServerA and HSCServerB. For details on configuring the source server see “Configuring replications on an Experion server” on page 595.

For this particular scenario, configure HSCMyServer with the following settings:

Property	Value
Name	Abstract
Share Path	C:\Program Files\Honeywell\Experion PKS\client\abstract
Send files from this share path to:	Select this option. Sets HSCMyServer as the source server.
Client PCs named	Select this option. Type HSCServerA and HSCServerB in the boxes provided. Sets the named redundant servers as destination clients.
Replicate automatically whenever files change	Select this option so that files are replicated whenever they are updated.

Configure HSCServerA as the destination server

Configure HSCServerA as the destination server to receive files from HSCMyServer. For details on configuring the destination server see “Configuring replications on an Experion server” on page 595.

For this particular scenario, configure HSCServerA with the following settings:

Property	Value
Name	Abstract Ensure the name is exactly the same as the name you specified as the replication name on HSCMyServer.
Share Path	C:\Program Files\Honeywell\Experion PKS\client\abstract
Receive files	Select this option. Sets this server as the destination server.

Prepare HSCServerB

Prepare HSCServerB to receive files so that if failover occurs, HSCServerB has the most up-to-date display files.

Configuring schedules

28

This chapter describes how you configure:

- Holidays
- Shifts
- Point control schedules

About schedules

Schedules enable the control of points to be scheduled on both a one-off and periodic basis. For example, a pump could be scheduled to be switched on at 4 pm and off at 6 pm each day.

Point control schedules

Point Control Schedules are configured using Station displays. The following attributes can be configured for each schedule:

- The time and date of the point control
- The point and point parameter to be controlled
- The value to control the point parameter to
- The schedule action

The schedule action can be one-shot, daily, work day, weekend, holiday, or a day of the week.

The number of schedules that can be configured is based on database sizing (see the *Installation Guide* for details).

Configuration information that is related to the scheduling option is the configuration of holidays and shifts. Holiday and Shift configuration displays are part of a standard Experion system and are described in the following topics.

Considerations when adding a Point Control Schedule

The Point Control Scheduler runs once per minute to check if any scheduled controls should be performed. Controls are performed sequentially. Therefore, if a large number of schedules are configured for the same time, the last control requests might be delayed. Depending on the channel capacity and the load from routine scanning, it is possible that a number of Point Control Schedules at the same time may cause channel overload or adversely impact communications performance. These factors should be assessed prior to implementing Schedules.

Only one-shot and holiday schedules run on the holiday dates; all other schedule types are ignored. If you want a point control to occur on a daily basis, you must also create separate schedules for holidays.

Configuring holiday and shift details

Holiday information is used by:

- Point Control Scheduler
- Global Schedules
- Controllers associated with access control

Shift information is used in:

- Point Control Schedules
- Periodic Reports (see “How reports are used” on page 402 for details)
- Algorithms (see “Configuring algorithms” on page 235 for details)

You use Station displays to configure holidays and shifts. To configure holidays or shifts you need to be using a security level of SUPV or higher.

Configuring holidays

You can use the Holiday Configuration display to configure the dates of up to 30 holidays.

To configure holidays:

- 1 In the Configuration Explorer of Configuration Studio, click **Schedules**.
- 2 Click the **Configure holidays** task.
The Holiday Configuration display appears in the System Display tab in Configuration Studio.
- 3 For each holiday you want to configure, type the date in the format DD-
MMM-YY.

To delete a holiday:

- 1 In the date box, type **NOW** or press DELETE so that the date is blank.

Configuring shifts

Use the Shift Configuration display to configure the start time and length of shifts at your site.

To configure a shift:

- 1 In the Configuration Explorer of Configuration Studio, click **Schedules**.
- 2 Click the **Configure shifts** task.
The Shift Configuration display appears in the System Display tab in Configuration Studio.
- 3 Type a time in the **Start of Day** box in the format HH:MM. (Start of day is the time since midnight on a 24 hour clock.)
- 4 Type a period in the **Length of Shift** box in the format HH:MM.

Configuring Point Control Schedules

The Point Control Schedule display allows you to:

- Create a point control schedule
- Modify a point control schedule
- Filter schedules to see schedules for a particular point
- Delete schedules

The Point Control Schedule display is divided into three sections. The top part of the display shows a list of currently configured schedules. The **Schedule Maintenance** options in the middle of the display are used for adding, deleting, or updating schedules. The filter at the bottom of the display is used to display point control schedules for a particular point.

Adding a schedule

Considerations

- You must have a security level of ENGR or higher.
- If the point you want to control requires an electronic signature, you are required to provide a valid user name and password to add the point to a schedule.
- You cannot add more than one schedule with the same point, date, and time. If you need to control more than one parameter, for example to set a point to manual before setting its value, add the schedules for each parameter in sequence, a minute apart.
- If you want a point control to occur each day, you need to configure both a daily schedule and a holiday schedule for the point. Daily schedules do not occur on those days defined as holidays.

To add a schedule:

- 1 In the Configuration Explorer of Configuration Studio, click **Schedules**.
- 2 Click the **Configure Point Control Schedules** task.
The Point Control Schedules display appears in the System Display tab in Configuration Studio.
- 3 Under **Schedule Maintenance**, set the properties as described in the table below.
- 4 When you have added all the schedule details, click **Insert** to add the schedule.

- 5 If the point you want to control requires an electronic signature, the Electronic Signature dialog box opens.
- 6 Select a reason from the Reason list.
- 7 Type your user name.
- 8 Type your password
- 9 Type the domain, if required.
- 10 Type any additional information in Comments.
- 11 Click **OK** (or click Sign if a double signature is required).
- 12 If a second signer is required, click the Secondary signature tab.
The secondary signer must have a different user name from the primary signer and must have a security level equal to or higher than level displayed in the Secondary signature tab.
- 13 The secondary signer enters their user name, password and domain.
- 14 If required, the secondary signer enters any addition information in Comments.
- 15 Click **OK**.

The following table describes the properties on the Point Control Schedule display:

Property	Description
Date	The date that the schedule is performed.
Time	The time that the schedule is performed.
Point ID	The point ID of the point that is controlled by the schedule. If your system is configured to use electronic signatures, you are required to provide a valid user ID and password in order to add a point to a schedule.
Parameter	The point parameter of the point that is controlled by the schedule, usually the OP (output). For analog points, the SP, OP, MD, A1 - A4 parameters can be controlled. For status points, the OP and MD parameters can be controlled. You cannot schedule the control of a PV point parameter. For flexible points, any writable numeric parameter can be controlled.

Property	Description
Target	The value that the point parameter is controlled to. For analog points: The target value of the SP and OP parameters can be set to any value between the SP and OP control limits respectively. For more information about analog point parameters, see “Analog point parameters” on page 178. For more information about status point parameters, see “Status point parameters” on page 175. For more information about flexible points, see “Point types” on page 166 and the documentation for the device.
Type	The type of schedule action. For a description of the types see the table below.

The following table describes the types of schedule action.



Attention

- Only One-shot and Holiday schedule actions run on the holiday dates. All other schedule types are ignored.
- Exception type indicates only One-shot, Holiday or Exception schedule for a specified point parameter runs on the exception date. All other schedule types are ignored.

Type	Description
One-shot	The control is performed when the scheduled date and time becomes equal to the current date and time, then the schedule is deleted.
Daily	The control is performed when the scheduled date and time becomes equal to the current date and time and the day has not been defined as a holiday. It is then re-scheduled for the following day at the same time.
Work day	The control is performed when the scheduled date and time becomes equal to the current date and time, if that is between Monday and Friday inclusive and the day has not been defined as a holiday. The control is then re-scheduled for the following day at the same time to check for a work day condition.
Weekend	The control is performed when the scheduled date and time becomes equal to the current date and time, if that is a Saturday or a Sunday and the day has not been defined as a holiday. The control is then re-scheduled for the following day at the same time to check for a weekend condition.

Type	Description
Holiday	The control is performed when the scheduled date and time becomes equal to the current date and time, if the day has been defined as a holiday (see “Configuring holiday and shift details” on page 611). The control is then re-scheduled for the following day at the same time to check for a holiday condition.
Monday Tuesday Wednesday (and so on through to) Sunday	The control is performed when the scheduled date and time become equal to the current date and time if it is the configured day of the week and the day has not been defined as a holiday. The control is then re-scheduled for the following day at the same time to check for the specified day.
Exception	The control is performed when the scheduled date and time become equal to the current date and time. The schedule is deleted at the end of the day that it has been scheduled for. The exception type is only configured by Global Schedules.

Deleting a schedule

To delete a schedule:

- 1 Specify the schedule you want to delete by clicking it in the display.
- 2 When the schedule you want to delete is displayed in the **Schedule Maintenance** boxes, click **Delete**.

Updating or copying a schedule

To update a schedule:

- 1 Specify the schedule you want to update by clicking it.
- 2 In the **Schedule Maintenance** boxes, make your modifications.
- 3 Click **Update**.
- 4 If electronic signatures are required, specify the required information as described in “Adding a schedule” on page 613.

When updating a schedule, click the schedule you want to update (rather than manually typing in the information in the Schedule Maintenance boxes).

To copy a schedule:

- 1 Specify the schedule you want to copy by clicking it.
- 2 In the **Schedule Maintenance** boxes, make your modifications.
- 3 Click **Insert**.
- 4 If electronic signatures are required, specify the required information as described in “Adding a schedule” on page 613.

Event log entries for schedules

Experion logs an event for every:

- Insertion, deletion, and update of a point control schedule
- Command executed by a point control schedule

Filtering the Point Control Scheduler

You can filter the Point Control Scheduler to show schedules for a particular point ID.

To filter the Point Control Scheduler:

- 1 Call up the Point Control Schedule display.
- 2 Select **Only show point ID**.
- 3 Specify the point ID you want to display schedules for.

The Point Control Schedule display shows schedules for the specified point only.

To remove the filter, select **Show all**.

Configuring recipes

29

This chapter describes how you configure recipes.

A “recipe” is a set of pre-configured values that can be loaded into one or more sets of point parameters. A set of point parameters generally controls a “unit”, which is a set of equipment used to produce the recipe. A recipe can be loaded into any units that share similar sets of points.

Recipes can consist of up to 30 ingredients. If more than 30 ingredients are required, you can chain individual recipes together to form a larger recipe.

The Recipe Manager feature in Experion is designed as a simple way of downloading values to multiple point parameters. If a full batching system is required, Total Plant Batch should be used.

About recipe configuration

The total number of recipes that can be configured depends on the size of your database. For more information about database sizing, see the following topic in Knowledge Builder:

Experion R300 > Installation and Upgrades > Supplementary Installation Tasks Guide > Changing license and server configuration details > Configuring the database setup > Adjusting sizing for non-licensed items.

For each recipe, the following attributes can be configured:

- Recipe title
- Scale factor for recipe ingredients (This can be specified by an operator.)
- Descriptors of the units to be loaded with the recipe (This can be specified by an operator.)
- Up to 30 ingredients (If more than 30 ingredients are required, you can chain recipes together.)

For each ingredient, the following attributes can be configured:

- Partial ID of the point to be loaded (leaving out the 2-character unit prefix)
- Parameter into which the value is to be loaded (usually a set point)
- Description of the ingredient of action that it represents
- Master value - the usual value that is loaded
- Maximum value - the maximum allowable working value
- Minimum value - the minimum allowable working value
- Working value - the actual value to be loaded (can be specified by an operator)
- Whether or not the value is scaled

After a recipe has been configured, operators can start the process by “loading” the recipe. For details, see the Operators Guide.

You can use custom displays to monitor the progress of a loaded recipe. Custom displays can show the point parameter values that are used to control the production. For details on how to build custom displays, see the Display Building Guide.

To configure recipes, you need to be using Station at a security level of SUPV or higher. (Security levels are described in “Configuring security and access” on page 281.)

Depending on the channel capacity and the load from routine scanning, it is possible that recipes with large numbers of steps may cause channel overload or adversely impact communications performance. These factors should be assessed prior to implementing recipes.

Configuring points for recipes

If a point will be in a recipe, the first two characters of the point ID must be the unit descriptor. The unit descriptor is a 2-character identifier (for example 01, L7).

You need to configure a point for every combination of unit descriptor and ingredient that you want to use. For example, if two units (“01” and “02”) are to be used with a recipe that contains the ingredient WATER, the points 01WATER and 02WATER need to be configured.

You can also configure an analog point with the name *uu*RECIPE, where *uu* is the unit descriptor. Whenever a recipe is run, *uu*RECIPE’s SP and description are updated to reflect the recipe’s number and name respectively.

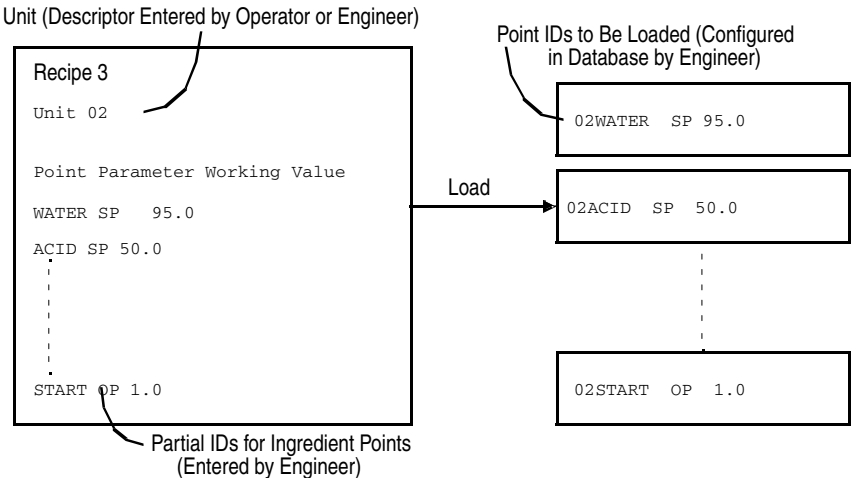


Attention

For some controllers, you need to set the mode of points in the controller to allow control by programs such as recipes. For example, the mode attribute (MODEATTR) for PID blocks in the Experion Process Controller must be set to Program to allow control by recipes.

When the operator loads a recipe, Experion determines the point ID to be loaded by combining the unit descriptor defined for the recipe with the partial point IDs defined for each ingredient. The following figure shows how the unit descriptor and points in the recipe are used.

Figure 42 How points are used with recipes



Configuring recipes

To configure a recipe:

- 1 In the Configuration Explorer of Configuration Studio, expand **Advanced Options** and click **Applications**.
- 2 Click the **Configure Recipes** task.
The Recipe Summary display appears in the System Display tab in Configuration Studio.
- 3 To work with an existing recipe, click its number or title. This calls up the Recipe Detail display.
- 4 To create a new recipe, click an unassigned row. When the blank Recipe Detail display opens, type the appropriate information. (See “Defining a recipe” on page 623.)

Defining a recipe

To configure a recipe, you define the recipe itself in the boxes at the top of the Recipe Detail display, and define up to 30 ingredients in the boxes in the bottom part of the screen (see “Defining the ingredients of the recipe” on page 624).

Figure 43 Recipe Detail display

System Configuration Recipe 1

Title: Load

Description:

Scale (%):

Unit:

Recipe last loaded: 00:00 with Scale (%) 0 to Unit

Begin

Point	Parameter	Description	Master	Min	Max	Working	Scaled
1	01Temp	SP	100	0	200	95	No
2	01Amonia	SP	10	0	20	15	No
3			0	0	0	0	No
4			0	0	0	0	No
5			0	0	0	0	No
6			0	0	0	0	No
7			0	0	0	0	No
8			0	0	0	0	No
9			0	0	0	0	No
10			0	0	0	0	No

End

The options that define the recipe are:

Property	Description
Title	The title that appears on the Recipe Summary display.
Description	A fuller description of the recipe than can be displayed in the title.
Scale	The scale factor for the recipe. Ingredients in a recipe can be scaled to less than 100% so that a partial recipe quantity can be produced. When the recipe is loaded, all ingredients with Scaled set to “Yes” are scaled by the percentage specified. This percentage can be changed by anyone using the OPER security level or higher.
Unit	The descriptor of a unit to which the recipe can be loaded.

Defining the ingredients of the recipe

You can define up to 30 ingredients in a recipe. If there are more than 30 ingredients, you need to divide the process into 2 or more recipes and chain them together (see “Chaining recipes” on page 625).

The options that define the recipe are:

Property	Description
Point	The last 38 characters of the point ID to be loaded (the first two characters are taken from the unit descriptor).
Parameter	The point parameter to be loaded.
Description	A description of the ingredient. This description will be used in custom reports.
Master	The usual value for the ingredient. This value is for operator information.
Minimum	The minimum value for the ingredient. If an operator enters a value that is less than the minimum value, then the minimum value is used.
Maximum	The maximum value for the ingredient. If an operator enters a value that is greater than the maximum value, the maximum value is used.
Working	The value to be loaded. If Scaled is set to “Yes” for this ingredient, this value will be scaled by the percentage specified for the Scale option for the recipe. This option can be changed by anyone using the OPER security level.

Property	Description
Scaled	Type Yes if the working value should be scaled by the Scale percentage. Otherwise type No .
Begin/Continue/End Comboboxes	If the recipe consists of 30 ingredients or less, set the box above the list of ingredients to BEGIN and the box at the bottom of the display to END. See Chaining recipes for details on using the Continue option.

Chaining recipes

If more than 30 ingredients are required in a recipe, you need to divide the process into 2 or more recipes, which you enter in sequence and chain together.

For example, if you need to chain two recipes:

- In Recipe 1, select BEGIN in the top combobox, and select CONTINUED in the bottom combobox.
- In Recipe 2, select CONTINUED in the top combobox, and select END in the bottom combobox.

Only an individual with a security level of SUPV or higher can chain recipes.

Configuring custom reports

You can set up free format custom reports to show the results of completed processes.

The following sections describe how you set up custom reports to run automatically, and how you configure a free format report for recipes.

Running custom reports automatically

To configure a report to run automatically at the end of a process, you define a digital value in a controller that changes state at the end of the process:

- Configure a status point to scan the digital value from the controller that indicates the end of the process. For details about configuring points, see “Understanding and configuring points” on page 163.
- Configure the Status Change Report Request Algorithm with this point so that the required report will be run when the digital value changes to a nominated state. For details about how to configure algorithms, see “Configuring algorithms” on page 235.

Configuring a free format report

Free Format reports can include point values, calculated values, point history and values from server database files. This section describes how to include information from the server database file that is used to hold recipe configuration. The procedures for configuring Free Format reports are described in “Configuring Free Format Reports” on page 432.

All recipe configurations are stored in one server database file called the Recipe table. Each record in this file contains the configuration for a single recipe. For example, record number 3 holds the configuration for recipe number 3.

Each record in the Recipe table is divided into fields. Each field holds an item of recipe configuration. For example, one field is used to hold the scale factor. “Recipe table field details” on page 627 shows details about the fields in each Recipe table record.

To read data from a field in the Recipe table, you specify:

- The file number of the Recipe table file. This number is 146.
- The Recipe number
- The starting location of the field, as specified in the Word Offset column
- The data type of the field, as specified in the Data Type column

For a Free Format report, you use the Read from File statement (see “R (Read From File)” on page 453) with the following parameters:

- No = 146 (the file number of the Recipe table file)
- Rec_No = recipe number
- Offset = word offset of field
- Print_Format = a format descriptor (for details of the available descriptors, see “F (Fetch From Point)” on page 445)
- Type = data type of the field

Example

To read the scale field (word offset 117) from recipe no. 3 into Free Format variable no 999, the Free Format report entry would be:

```
R 999 146 3 117 I3 I2
```

Table 19 Recipe table field details

Word Offset	Field Description	Data Type
1	Recipe title	A70
106 Bit 15	Chained to previous recipe (1=chained)	I15.1
106 Bit 14	Chained to next recipe (1=chained)	I14.1
107	Scale (0-100)	I2
108	Unit	A2
114	Day of last load	I2
115	Time of last load	RL
117	Scale of last load	I2
118	Unit of last load	A2
125	Ingredient 1 point ID (repeated for the 30 ingredients at an increment of 19, that is, word 143 for ingredient 2)	A14
695	Ingredient 1 description (repeated for the 30 ingredients at an increment of 20, that is, word 715 for ingredient 2)	A20
1295 Bit 0	Ingredient 1 scaled (1=scaled) (repeated for the 30 ingredients, that is, word 1295 bit 1 for ingredient 2)	I0.1
1297	Ingredient 1 master value (repeated for the 30 ingredients, that is, word 1299 for ingredient 2)	RL
1357	Ingredient 1 minimum value (repeated for the 30 ingredients, that is, word 1359 for ingredient 2)	RL

Table 19 Recipe table field details *(continued)*

Word Offset	Field Description	Data Type
1417	Ingredient 1 maximum value (repeated for the 30 ingredients, that is, word 1419 for ingredient 2)	RL
1477	Ingredient 1 working value (repeated for the 30 ingredients, that is, word 1479 for ingredient 2)	RL
1537	Ingredient 1 parameter (repeated for the 30 ingredients, that is, word 1573 for ingredient 2)	A72

Configuring Event Archiving

30

Every event, such as a point status change or an operator action, is stored in an event database. The event database stores events for a specified period of time. Using Event Archiving, you can archive these events to a network fileserver or to a disk where they can be stored for future retrieval and reporting.

This chapter describes:

- What Event Archiving is, and how it works
- How to configure Event Archiving

For information on archiving events or restoring events from archive, see the *Operators Guide*.

About Event Archiving

Events are collected in an Experion system database file. Periodically events are copied from the Experion system database to the Microsoft SQL Server event database for queries and reporting. Events are archived from the SQL Server database according to a schedule you specify. You can set up automatic archiving or you can set an alarm to alert an operator to archive events. Events are kept in the SQL Server event database for a period of time you specify. When the time period expires, the oldest events are progressively deleted.

The contents of an archive are verified automatically when the archive process is complete. The status (success or failure) of the archive is logged in the Event Summary, and the operator is notified with a message.

If necessary, you can also perform an early archive (that is, before the scheduled archive or the low disk space limit is reached). You can restore an archive of events at any time and use standard Experion reports to access this information.

Methods of archiving

Event Archiving allows you to archive events to a local disk or a network file server. Honeywell recommends that you use your offline backup or archive strategy to backup the generated event archive files on the local disk or network file server. For example, you can copy the generated event archive files to other media, such as CD or tape, or include them in your system backup. For more information about system backup see the *Backup and Restore Guide*.

For details about configuring a suitable tape device, see the Microsoft Windows documentation.

Performance considerations

There is a relationship between the number of events retained in the SQL Server event database and the performance of the Experion system. The more events retained, the greater the negative impact on CPU performance of the server. While Honeywell recommends that you keep no more than 1.2 million events online, you should always keep them to a minimum. When considering the number of days to retain events online, you should identify the minimum number of events to meet the business requirements for reporting. You can always restore event archives to meet your ad-hoc reporting requirements.

Estimating space requirements

You require a base value of 10 MB of disk space for events online, plus additional disk space for each event. You also require a base value of 10 MB of disk space for each event archive, plus additional disk space for each event.

To estimate the disk space requirements, you need to know the following:

- An estimate of the events generated per day.
- The duration that events are to be kept online.
- An average event size (approximately 1200 bytes per event).

Use the following formula to calculate the estimated disk space requirements both for events online and for each event archive:

$$((\text{number\_of\_events} * \text{duration}) * \text{average\_event\_size}) + 10 \text{ MB}$$

Example

You estimate your system generates 3000 events per day. You want to keep events online for 31 days. This is the formula to estimate the disk space requirements for events online:

$$((3000 \text{ events} * 31 \text{ days}) * 1200 \text{ bytes}) + 10 \text{ MB} = 120 \text{ MB}$$

In this example, you require 120 MB of disk space for events online.

In addition to events online, you also need to calculate the disk space requirements for each event archive. You use the same formula to calculate the disk space for each event archive. For example, if you schedule automatic archiving once every week, this is the formula to estimate the disk space requirements for each event archive:

$$((3000 \text{ events} * 7 \text{ days}) * 1200 \text{ bytes}) + 10 \text{ MB} = 34.6 \text{ MB}$$

In this example, you require 34.6 MB of disk space per event archive.



Attention

These calculations are only a guide.

Restoring events

You can restore archived events so that they are available for reporting. Events archives are restored to a playback database and are available for reporting and can be viewed on the Event Summary. The Event Archiving Operations display lists restored archives.

For instructions on restoring events, see the *Operators Guide*.

Event tamper detection

You can enable your system to detect if event data has been added, modified or deleted by anything other than the normal Experion processes. Event tamper detection occurs when you run reports and query events in the SQL Server online events or playback database.

If tampering is detected, an alarm is raised and reports show a list of tampered events.

Considerations

- Enabling Event Tamper Detection on a server-wide basis significantly decreases the rate at which events are retrieved.

To enable tamper detection system-wide:

- 1 In the Configuration Explorer of Configuration Studio, click **Alarms and Event Management**.
- 2 Click the **Server wide alarm and event options** task.
The Server-wide Station Settings display appears in the System Display tab in Configuration Studio.
- 3 Select **Check for tampering of all event data returned from archives**.

Event Archiving system configuration

To configure Event Archiving you need to do the following:

- 1 Install Internet Information Services (IIS) as described in “Installing Internet Information Services 6.0” in the *Software Installation and Upgrade Guide*.
- 2 Configure IIS for Event Archiving (see below).
- 3 Use Configuration Studio to complete the configuration of Event Archiving (see below).

Prerequisites

You have installed IIS on your Experion server and selected World Wide Web service, as described in the *Software Installation and Upgrade Guide*

To configure IIS for Event Archiving:

- 1 On the server, choose **Start > Administrative Tools**.
- 2 In the **Administrative Tools** window, double-click the **Internet Information Services (IIS) Manager** icon.
- 3 In the **Internet Information Services (IIS) Manager** window, expand the tree displaying the computer name.
- 4 Expand **Web Sites**.
- 5 Select **Default Web Site** and then choose **Action > New > Virtual Directory** from the Window's menu.
- 6 In the **Welcome** window, click **Next**.
- 7 In the **Virtual Directory Creation Wizard** window, type **eventmanagement** in the **Alias** box and then click **Next**.
- 8 In the **Web Site Content Directory** window, set the directory to *drive*\Program Files\Honeywell\Experion PKS\server\evtarch\eventmanagement, where *drive* corresponds to the drive on which Experion PKS is installed.and then click **Next**.
- 9 In the **Virtual Directory Access Permissions** window, ensure the **Read** option is selected and clear the remaining options, and then click **Next**.
- 10 Click **Finish**.
- 11 Close the **Internet Information Services (IIS) Manager** window.

To configure Event Archiving:

- 1 In the Configuration Explorer of Configuration Studio, click **Alarm and Event Management**.

2 Click the **Configure Event Archiving task.**

The Event Archiving Configuration display appears in the System Display tab in Configuration Studio.

3 You use the options on the Event Archiving Configuration display as follows:

Property	Description
Online Events	
Keep events online for	The period of time events are kept online before being deleted. You can specify the time period in days, weeks or months. The maximum value is six weeks.
Disk space required at current event rate	The estimated disk space required based on the current event rate and the time period events are kept.
Raise alarm if disk space falls below	The minimum disk space allowed before an alarm is raised.
Event Archiving	
Create an archive	Enables archiving at the time you specify. You specify the time of day on a daily, weekly or monthly basis. The maximum value is six weeks.
When archive is due	Sets the action taken when archiving is due. You can set up automatic archiving or to raise an alarm when archiving is due.
Archive using	Sets the method of archiving. You can archive using Windows Backup or FileSystem. FileSystem archives to a network file server. Use a UNC path rather than mapping a drive to your local computer. For example, use \\myserver\archive instead of f:\archive.
Create archive in directory	Applicable if you use the FileSystem method of archiving. Specifies the folder to archive events to. The default is blank. You must type a valid path to enable event archiving to function correctly.
Append	Applicable if you use the Windows Backup method of archiving. Specifies the next archive will be added to tape.
Overwrite	Applicable if you use the Windows Backup method of archiving. Specifies the next archive will overwrite all existing contents on the tape.
Alarm Priorities	
Time to archive	Applicable if you are raising an alarm when archiving is due. Sets the priority of the alarm raised.
Event archiving error	Sets the priority of the alarm if archiving is in error.

Event Archiving status

The status of event collection and archiving is shown on the Event Archiving Operations display. The status can be:

Status	Description
OK	Event collection and archiving is operating as required.
Overload	Events collection is overloaded. If this state continues for extended periods of time contact Honeywell support.
Failed	Events collection has failed.
Full Disk	There is not enough disk space to continue events collection. Events collection is stopped until there is sufficient disk space available.
Synchronizing	Events collections is temporarily stopped while servers are synchronizing.

About Windows backup

Event Archiving uses the Windows Backup program to archive events to tape. Windows Backup is installed with Windows XP and Windows Server 2003. It can be started independently by typing **ntbackup** in a Command Prompt window.

Windows Backup utilizes the Removable Storage Manager (RSM) Service to manage tape information. Tapes are automatically allocated to Media Pools by RSM when they are loaded and subsequently used. You can view and manipulate the information maintained by the RSM Service by selecting **Start > Control Panel > Administrative Tools > Computer Management > Storage > Removable Storage**.

For more information about using Microsoft Backup, see “Using Microsoft Backup” in the chapter “Planning backups using Microsoft Backup” in the *Experion Backup and Restore Guide*.

Known Problem

There is a known problem with the RSM service that may prevent Windows Backup recognizing the tape currently loaded in the tape drive. RSM occasionally determines that the media type of a particular tape is unknown. The tape is marked as being of “Unknown” media type and subsequently Windows Backup cannot use the tape. Windows Backup requires all tapes to be of the type associated with the installed tape drive. It is unclear why the RSM Service behaves in this way.

In the event of this happening during archiving events to tape, Windows Backup will start and immediately exit. The error message indicates that the tape archive has failed. To confirm that the above problem is occurring, start Windows Backup, and attempt to manually archive any file to the tape currently loaded. If you cannot configure Windows backup to select the currently loaded tape, then you are experiencing the above problem.

If the tape holds data that must be retrieved, the tape can be read using software that bypasses the Windows RSM Service, such as ArcserveIT. If you want to re-use the tape then it must be reformatted by one of these applications.

Configuring Experion ODBC

31

ODBC is a standard interface for accessing data in a database. This interface enables you to perform Structured Query Language (SQL) queries on the database.

ODBC may be used as the underlying technology for ADO, OLEDB, or .NET based clients. It can be used in any client/server architecture, regardless of whether the database and client application are resident on the same computer, separated by a network, or even if they are on different computers using different operating systems.

Experion ODBC support enables the transfer of data between the Experion server database and other third-party databases. The supported databases are any application that provides support for ODBC function calls (for example, Microsoft Access) or has an ODBC driver.

Experion ODBC driver is fully compliant with ODBC 1.0 and partially compliant with ODBC 2.0. For a list of supported keywords, see “ODBC Standard compliance” on page 670.

ODBC support is provided through two separate Experion options:

- ODBC Driver, which enables retrieval of:
 - Point data
 - History data
 - Event data
- ODBC Data Exchange Report, which enables two-way transfer of:
 - All server data



Attention

ODBC Driver is intended for ad hoc queries. For repetitive or high-speed data retrieval you should consider Microsoft Excel Data Exchange, Network API, or OPC server.

About the Experion ODBC driver

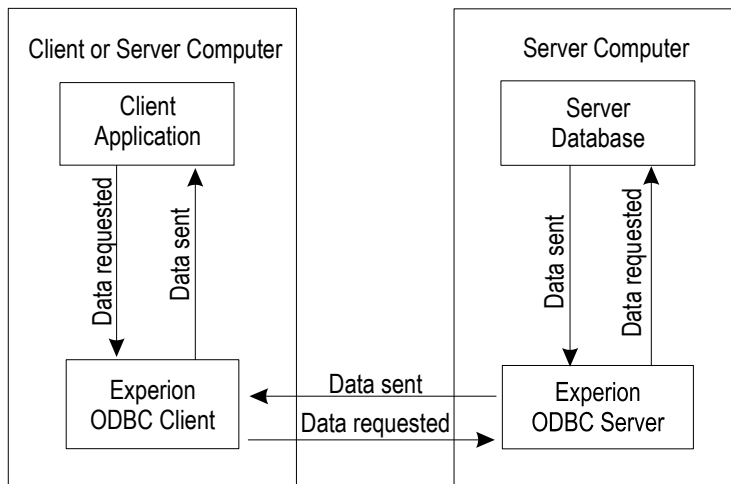
The Experion ODBC driver enables you to access Experion server data (such as history, event, and point data) directly from any application that provides ODBC support; for example, Microsoft Access, Microsoft Excel, or Crystal Reports.

The Experion ODBC driver has two parts: the ODBC Server and the ODBC Client.

- The Experion ODBC Client handles the ODBC calls made by a client application and passes them to the Experion ODBC Server.
- The ODBC Server processes the ODBC calls, queries the Experion server database and returns the information to the client application.

The Experion ODBC Server always runs on the Experion server. The Experion ODBC Client can run on the server or on any other computer on the network. The following diagram shows a basic Experion ODBC driver configuration.

Figure 44 Accessing data via the ODBC driver



For more information about ODBC, see the documentation for the third-party software that you are using to query the Experion database (for example, Microsoft Access).

Configuring the Experion ODBC driver

The following procedures assume that you have already completed the installation of the Experion server software as described in the *Software Installation and Upgrade Guide*. Specifically, the procedures assume that:

- You have installed the Experion ODBC Client software on the client computer (that is, the computer that will be used to query the Experion server database).
- You have also installed the client application (for example, Microsoft Access) and its ODBC components, on the client computer.

The configuration procedures may vary according to the client application that you will use to query the Experion server database. Application-specific help is usually provided with the client application.

In general, the steps are as follows:

- 1 Configure a data source on the client computer, as described in “Configuring a data source” on page 640). This only needs to be done once per computer, not every time you want to set up a query.
- 2 Start up the client application and use the ODBC support provided to connect to the Experion server database, as described in “Connecting to the Experion server database” on page 642).
- 3 Set up a query to query the Experion server database.

Configuring a data source

To query the Experion server database you need a configured data source on the client computer from which you are making the query.

Configuring a data source sets up an association between a data source name (DSN) and an ODBC driver. Your client application will prompt you for a DSN to connect to before sending queries to the Experion server database.

Considerations

- You can set up a system DSN or a user DSN. If you set up a user DSN it is available to the current user only. A system DSN is available to all users and services.
- You can set up a file DSN instead of a system DSN. However, a file DSN cannot be built for the Experion ODBC driver using the ODBC Administrator. You can create a file DSN using any text editor.
- ODBC connections using a file DSN will not work with Microsoft Access 2000-SR1. Use a system DSN instead.
- If you know the required strings you can edit the registry to contain details of your data source without using the ODBC Administrator. The registry location is HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\<DSN>.

To configure a data source:

- 1 Choose **Start > Settings > Control Panel > Administrative Tools**.
- 2 Double-click **Data Sources (ODBC)**. The ODBC Data Source Administrator opens.
- 3 Select either the User DSN or the System DSN tab.
- 4 Click **Add** to start the Create New Data Source wizard.
- 5 Select **Experion PKS ODBC Driver** from the list of installed ODBC drivers, and click **Finish**

The **Setup** dialog box for the selected source opens.

- 6 Complete the options as follows:

For this option:	Type:
Data Source Name	The name of the data source. It is advisable to name the data source after the Experion server that you will be querying, for example hsserv.
Description	A description of the data source, for example Data source for Experion database on hsserv.

For this option:	Type:
Host	The name of the computer on which the Experion server software is running. This can either be local or remote. If the DSN is being set up locally on an Experion server that is not in a redundant system, type <code>localhost</code>. If you are running a redundant system, type only the server's basename. For example, if your two servers are called <code>hsserva</code> and <code>hsservb</code> type only <code>hsserv</code> as the server name. The ODBC driver will connect automatically to the computer currently running as primary.
Redundant Server	Select this box if you are running a system with redundant servers.
Dual LAN	Select this box if you have 2 physical networks. Do not select this box if FTE is being used.

- 7 Click **OK** to close the **Setup** dialog box.
- 8 Click **OK** to close the **ODBC Data Source Administrator** dialog box.

Considerations

- If you intend to query multiple Experion servers from a single client, you need to set up a data source for each server.

To configure a file DSN:

- 1 Build a system data source.
- 2 Using any text editor, create a file containing:


```
[ODBC]
DRIVER=Experion PKS ODBC Driver
DSN=<data source name>
REMOTEHOST=<remotehost name>
UID=<userid>
DBQ=Experion PKS
```

Where:

 - `<data source name>` is the same as built in Step 1 above
 - `<remotehost name>` is the computer name of the remote Experion server if you are connecting to a remote host
 - `<userid>` is the operator-based security mngr user id on the remote Experion server
- 3 Save the file to `C:\Program Files\Common Files\odbc\Data Sources`. The DSN is the name of the saved file.

Connecting to the Experion server database

Connection to the Experion server database via ODBC is different in each Client application. Consult the documentation accompanying the application for details. For a step-by-step guide for Microsoft Access see “Using Experion ODBC driver and Microsoft Access” on page 661. For information for Microsoft SQL Server see “Establishing a connection between the Experion Database and Microsoft SQL Server” on page 643. For information for Visual Basic and C++ see “Using the Experion ODBC driver with Visual Basic and C++” on page 668.

Considerations

- When querying the Experion database, you must connect to it as an operator already configured in the Experion server database.
- The operator ID you use to connect to the server determines the data you can access as the Experion ODBC driver honors any asset assignment restrictions that apply to that operator. If you require access to all data on the server you should use an operator ID with the same security level as the mngr operator account.
- Any changes to asset configuration are not available to the client application until the next time the application connects to the Experion server database.

In general:

- 1 When prompted by the client application, select the data source you configured (as described in the previous section).
The **Connection Details** dialog box opens, which enables you to connect to your Experion database.
- 2 Complete the options as follows:

For this option:	Type:
Operator ID	The user ID of an operator already configured on your Experion system.
Password	The corresponding password.
Host	The name of the computer on which the Experion server software is running. If you are running a redundant system, type only the server's basename. This information is inherited from the DSN you set up in “Configuring a data source” on page 640.
Domain	Applicable only if you are using integrated security and domain accounts. The name of the domain to which the operator ID belongs.

For this option:	Type:
Redundant Server	Select this box if you are running a system with redundant servers. This information is inherited from the DSN you set up in “Configuring a data source” on page 640.
Dual LAN	Select this box if you have 2 physical networks. Do not select this box if FTE is being used. This information is inherited from the DSN you set up in “Configuring a data source” on page 640.

Establishing a connection between the Experion Database and Microsoft SQL Server

To configure Microsoft SQL Server you use the DTS Wizard and includes the following steps:

- Configuring the data source in SQL Server
- Configure the destination SQL Server database
- Selecting the tables you want to link to
- Select when data is copied

To configure Microsoft SQL Server:

- 1 Choose **Start > Run**, type **C:\Program Files\Microsoft SQL Server\80\Tools\Binn\dtswiz.exe**
where, C is the drive where Microsoft SQL Server is installed.
- 2 Press **ENTER**. The DTS Wizard starts.
- 3 Click **Next**.
- 4 Select **Experion PKS Server ODBC Driver** from the **Source** list.
- 5 Select the previously configured data source:

Select	If
User/System DSN list	You are using a user or system DSN.
File DSN list.	You are using a file DSN.

- 6 Type the Experion operator-based security operator ID and password. Click **Next**.
- 7 Select **Microsoft OLE DB Provider for SQL Server** from the **Destination** list.
- 8 Specify the computer name on which the SQL server is running.
- 9 Select the appropriate authentication.

- 10 Select the SQL database name. Click **Next**.
- 11 Select **Copy table(s) and view(s) from the source Database**. Click **Next**.
- 12 Select the Experion tables you want to copy. Click **Next**.
- 13 Select **Run immediately** to ensure Experion data is copied when queried.
- 14 Select **Save DTS Package** to save these settings.
- 15 Click **Next**.
- 16 Type a name for this DTS package. Click **Next**.
- 17 Click **Finish**.

What data can you access with the Experion ODBC driver?

The data that can be queried in the Experion database is presented to the client application in the form of tables. The following sections describe those tables and how to use them.

Considerations

- In some cases, the use of OR conditions in the WHERE clause of a query may result in slow performance or unexpected results.
- The ODBC driver does not support the BETWEEN operator for dates in the Event tables.

Point tables

You can query the following Experion point tables with the ODBC driver:

- AccumulatorPoint
- AnalogPoint
- StatusPoint
- FlexiblePoint (point server points)
- ControlModulePoint (process points on Experion Process Controllers)

The point fields (which are visible as columns in each of the point tables) are shown in the following graphic.

Figure 45 Point data that you can access

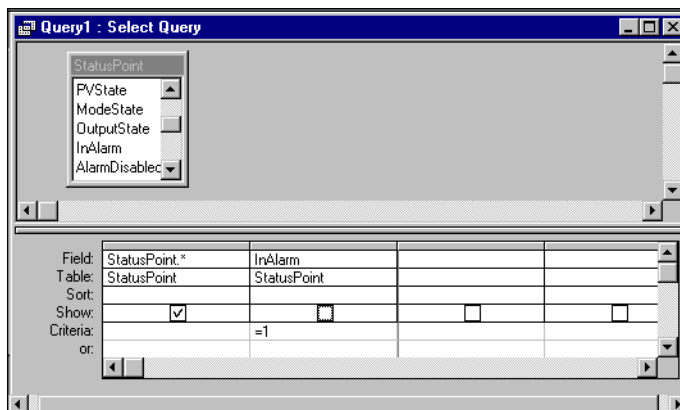
Relationships			
Accumulator Point	Analog Point	Status Point	Control Module Point
PointID	PointID	PointID	PointID
Description	Description	Description	Description
Area	Area	Area	Area
OnScan	OnScan	OnScan	ControlLevel
PVValue	PVValue	PVState	InAlarm
PVInError	PVInError	ModeState	AlarmUnacknowledged
RollOver	ModeState	OutputState	PointDetailDisplay
MeterFactor	ModeValue	InAlarm	GroupDetailDisplay
ScaleFactor	ModelnError	AlarmDisabled	Parameter001
RawPVValue	OutputValue	PVValue	TextValue001
AlarmDisabled	OutputInError	PVInError	NumericValue001
AlarmState	SetPointValue	ModeValue	Type001
AlarmValue	SetPointInError	ModelnError	Quality001
HundredPercentRange	A1Value	OutputValue	Parameter002
Units	A1InError	OutputInError	TextValue002
ControlLevel	A2Value	ControlLevel	NumericValue002
AlarmUnacknowledged	A2InError	AlarmUnacknowledged	Type002
	A3Value		Quality002
	A3InError		Parameter003
	A4Value		TextValue003
	A4InError		
	AlarmDisabled		
	AlarmState		
	AlarmValue		
	ZeroPercentRange		
	HundredPercentRange		
	Units		
	ControlLevel		
	AlarmUnacknowledged		

Status, analog, and accumulator point tables can be opened and viewed directly from most client applications that have ODBC support (for example, Microsoft Access).

A table opened in this way displays every point field for every point of that type in the Experion server database. This might be more information than is needed.

To select particular data out of the table, you need to build a query. A query can be used to reduce the number of columns (point fields) or rows (points) which are retrieved from the database. In some client applications a wizard will assist you to build a query; the application converts this query to SQL before sending it to the ODBC driver. A query built using a Microsoft Access wizard is shown below. It selects all point fields for all status points currently in alarm.

Figure 46 Microsoft Access query



The SQL equivalent of the above query is:

```
SELECT StatusPoint.*
FROM StatusPoint
WHERE StatusPoint.InAlarm=1;
```

Because flexible and process points have user defined parameters, their associated tables cannot be directly opened. You must define queries that nominate the parameters to be returned. For information about setting up queries on process points, see “SQL query on ControlModulePoint table” on page 648.

The first 8 columns in the CDA (Control Module) table (see “Point data that you can access” on page 646) are common to all points and can be accessed by name. The other columns are parameters of the particular kind of point.

To access a flexible point parameter, in the WHERE clause of a query you set ParameterXXX to equal the parameter name that you need. Experion then sets the QualityXXX, TypeXXX, and TextValueXXX parameters to the corresponding values. For example, if you set Parameter001, then Quality001, Type001, TextValue001 and NumericValue001 will contain values corresponding to this parameter for every point.

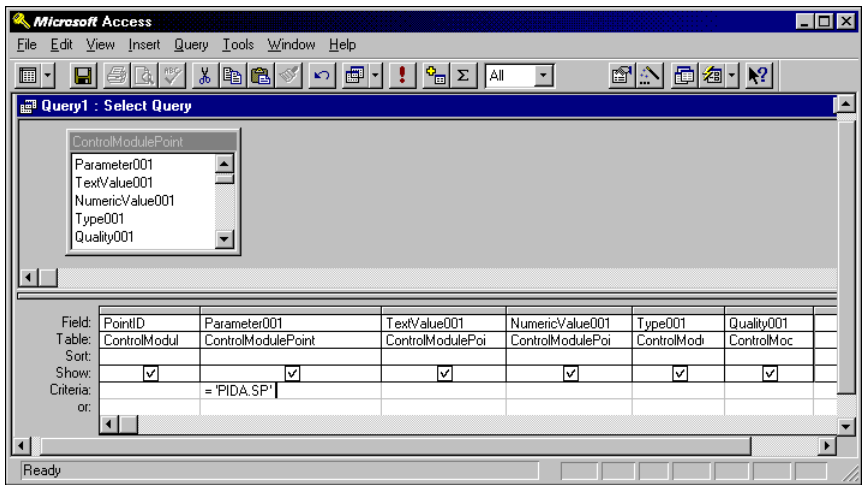
For information about parameter names, see the relevant point server documentation supplied with the point server software.

SQL query on ControlModulePoint table

The first eight columns in the ControlModulePoint table (see “Point data that you can access” on page 646) are common to all process points. The other columns are user-designated parameters. To access a user-designated parameter, set ParameterXXX to equal the parameter name. For example, Parameter001 = PIDA.SPTVNORMRATE.

Quality001, Type001, TextValue001 and NumericValue001 will then contain values corresponding to this parameter for every point. Below is an example query retrieving these fields for the parameter PIDA.SP for every point on the system.

Figure 47 Control module point query



The SQL equivalent of the above query is:

```
SELECT PointID, Parameter001, TextValue001, NumericValue001,
Type001, Quality001
FROM ControlModulePoint
WHERE Parameter001 = 'PIDA.SP'
```

The result set is shown in the following figure.

Figure 48 Result for example query for control module point

PointID	Parameter001	TextValue001	NumericValue001	Type001	Quality001
AIMOD1	PIDA.SP		0	INVALI	UNIM
AOMOD1	PIDA.SP		0	INVALI	UNIM
CEE_NT	PIDA.SP		0	INVALI	UNIM
CPM_NT	PIDA.SP		0	INVALI	UNIM
DIMOD1	PIDA.SP		0	INVALI	UNIM
DOMOD1	PIDA.SP		0	INVALI	UNIM
PIDLOOP	PIDA.SP		66	NUMBER	GOOD

Record: 1 of 7

The **Quality** field indicates the point parameter status when the data was retrieved. It can take the following values:

UNIM

The parameter has not been implemented for the point.

UNSPECIFIED

No parameter has been specified in the parameter field.

NaN

The numeric value is not a floating point number (NaN).

BAD

The parameter status is bad and not NaN.

GOOD

There are no errors for the value.

The **Type** field indicates one of four parameter types: ENUM, NUMBER, TEXT, or INVALI.

The relationship between the **Quality** and **Type** field is as follows:

- If the quality is shown as BAD, then the type is shown as INVALI.
- If the quality is shown as NaN, then the type will be set and the corresponding value will be the last good value of the parameter.

The relationship between the **Type** field and the **TextValue** and **NumericValue** fields is as follows:

- If the parameter type is TEXT, then the value is shown in the **TextValue** field.
- If the parameter type is NUMBER, the value is shown in the **NumericValue** field.
- If the parameter type is ENUM, the value is shown in both the **TextValue** and the **NumericValue** field.
- If the parameter type is INVALI, no data is shown in either field.

The following table summarizes this relationship.

Table 20 Parameter types and value fields

Type	Applicable Value Field	
	TextValue	NumericValue
ENUM	4	4
TEXT	4	7
NUMBER	7	4
INVALI	7	7

You can retrieve more than one parameter in a query by setting subsequent ParameterXXX fields to other parameter names; for example, Parameter002 = PIDA.pv, Parameter003 = PIDA.op.

The number of parameters that you can retrieve in one query might be restricted by the application you are using. For example, Microsoft Access limits this number to about 40. The total size of the record being retrieved may also be limited. If you are retrieving every field for every parameter, the number of parameters able to be viewed in Microsoft Access will be reduced to 14. This number can be increased by not requesting fields which you don't require, for example the **TextValue** field for numeric parameters.

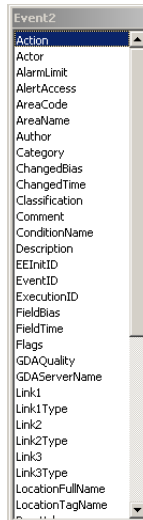
The following restrictions apply to queries involving process points:

- Wild cards are not permitted in the parameter names of process points.
- 'Or' conditions cannot be used in the query.

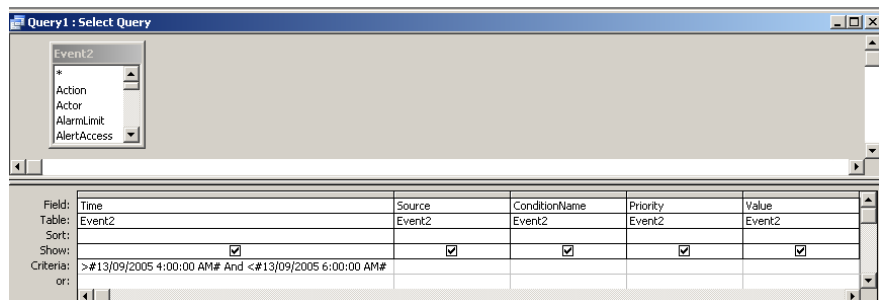
Event tables

All Experion events displayed in the Event Summary can be viewed through the Event2 table. Like the point tables, the event table can be opened and viewed directly from most client applications.

For maximum performance it is recommended that event queries filter on date/time range only and do no sorting. Further filtering and sorting can be done on the returned record set.

Figure 49 Event2 table data

The follow query, created in Microsoft Access, returns all events for a two hour period and display the time of each event, the event type and level, the source of each event and the value of the point at the time of the event.

Figure 50 Select query dialog box

The same query in SQL is:

```
SELECT Time, Source, ConditionName, Priority, Value
FROM Event2
WHERE (Time > {ts '2005-09-13 04:00:00'} and < {ts '2005-09-13
06:00:00'})
```

If you want to specify a value for Time in Microsoft Access use the format:

```
Time > #yyyy-mm-dd hh:mm:ss#
```

If you want to specify a value for Time in standard SQL use the format:

Time > {ts 'yyyy-mm-dd hh:mm:ss'}



Attention

- If no value is specified for Time, then, by default, only events generated within the last 24 hour period are returned.

If you want to manipulate the data, for example you may have written a custom application, you need to be aware of the field lengths of the following fields in the Event2 table:

Field	Description	Data type	Length
Action	The action performed by the operator.	Text	8
Actor	The identifier of the client that initiated the action. This can be a user ID or a full name. The user ID can be a Windows account or an Experion operator account.	Text	50
AlarmLimit	The limit that was exceeded to cause the alarm.	Text	8
AlertAccess	Accessibility of an alert source. It indicates the level of access other users have to the alert sources you create. It can either be public or private.	Text	1
AreaCode	Reserved.		
AreaName	Asset name of the event. The value is a user defined asset name containing the source causing the event.	Text	40
Author	The author of an alert source, the user who creates the alert source.	Text	50

Field	Description	Data type	Length
Category	A grouping of similar notifications. They have a correspondence to OPC categories. 1 = Process Alarm 2 = Point Alarm 3 = System Alarm 4 = Informational Message 7 = Operator Change 8 = System Change 9 = Sequence of Events 11 = Confirmation Message 12 = Process Event 13 = Point Event 14 = System Event	Text	4
ChangedBias	Offset, in minutes, from GMT of the ChangedTime.	Text	4
ChangedTime	The time that a condition changed state in the field.	Date/Time	
Classification	The classification to which an alert belongs. A classification is a user-defined name that can be used to logically group conditions that are related.	Text	20
Comment	The comment string passed in by the client who last acknowledged this condition	Text	50
ConditionName	The state this notification is annunciating. For example, OK, PVHI, PVLO.	Text	30
Description	A description associated with the event. The length is truncated to the first 128 characters.	Text	128

Field	Description	Data type	Length
EEInitID	Initialization ID of the execution environment. EEInitID shall record the time of the execution environment's most recent controller reload or the time when the sequence ID wrapped-around. It is used to identify the sequence ID cycle at which the recipe events are generated.	Text	20
EventID	The ID of the event. Each journaled event is assigned a unique ID. Event IDs are assigned in ascending order	Text	20
ExecutionID	Execution ID of the control recipe execution. Each run of a control recipe will have a discrete execution ID, and each recipe event will carry this execution ID to identify the control recipe execution that it is generated from.	Text	20
FieldBias	Offset, in minutes, from GMT of the FieldTime	Text	4
FieldTime	The time the event occurred in the field	Date/Time	
Flags	The flags of the alarm/event/message. A value with 0x2000 bit set indicates the event is journal only.	Text	4
GDAQuality	Reserved.		
GDAServerName	Reserved.		20
Link1	Navigation link (URL). Used to navigate to displays and documents that are relevant to the alarm or event.	Text	128
Link1Type	The type of link for Link1, for example, point detail display, digital video captured with the event, default display, instructions.	Text	4

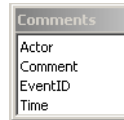
Field	Description	Data type	Length
Link2	Navigation link (URL). Used to navigate to displays and documents that are relevant to the alarm or event.	Text	128
Link2Type	The type of link for Link2, for example, point detail display, digital video captured with the event, default display, instructions.	Text	4
Link3	Navigation link (URL). Used to navigate to displays and documents that are relevant to the alarm or event.	Text	128
Link3Type	The type of link for Link3, for example, point detail display, digital video captured with the event, default display, instructions.	Text	4
LocationFullName	The full item name of the event source's location in the enterprise model.	Text	200
LocationTagName	The tag name of the event source's location in the enterprise model.	Text	40
PrevValue	The value of the source before alarm/event/message was generated.	Text	24
PrevValueType	The type of PrevValue. See ValueType.	Text	4
Reason	The reason the operator performing the action and providing a signature	Text	60
SequenceID	Sequence ID of the recipe event. Each recipe event has a unique 8-byte increasing sequence ID, assigned in the order of when they are generated. It is used to support Guaranteed Event Delivery.	Text	20
Severity	OPC severity. The urgency of the event.	Text	4
SignatureMeaning	Describes the meaning of entering the signature	Text	24

Field	Description	Data type	Length
Source	A reference to the entity that the notification is associated with.	Text	40
SourceEntityName	The item name of the event source	Text	40
Station	The Station where the client initiated the action.	Text	30
SubConditionName	Required only for OPC events with multistate conditions. The substate this notification is annunciating.	Text	30
Time	The time the event occurred.	Date/Time	
TimeBias	Offset, in minutes from GMT of Time.	Text	4
TransactionID	The Transaction ID associates comments with events. When an alarm is added to the alarm list, the Transaction ID is set to the Event ID. While this alarm remains in the alarm list all journaled events pertaining to this alarm are given the same transaction ID. As a result, comments made against any event with the same Transaction ID are shown against all events with the same Transaction ID.	Text	20
Units	Engineering units of the value.	Text	24
Value	The value associated with the event.	Text	24
ValueType	The type of Value. 1 = text 2 = 16 bit integer 3 = 32 bit integer 4 = short float 5 = long float 15 = 64 bit integer	Text	4

Comments tables

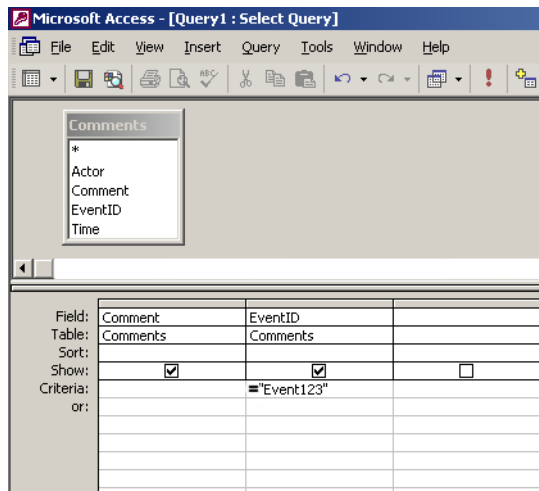
The Comments table is related to the Event2 table. Each event can have multiple comments, which are stored in the Comments table. To return all comments for a particular event, you query the Comments table.

Figure 51 Comments table



The following query, created in Microsoft Access, selects all comments for the event EventID=123.

Figure 52 Design view of a Comments table query in Access



The same query in SQL is:

```
SELECT Comments.Comment, Comments.EventID
FROM Comments
WHERE (((Comments.EventID)=123));
```

History tables

Nine history tables from the Experion database are visible via the ODBC driver. These are:

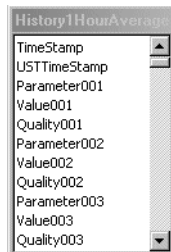
- History1HourAverage

- History1HourSnapshot
- History1MinSnapshot
- History24HourAverage
- History24HourSnapshot
- History n SecondSnapshot
Where n is the configured collection rate, for example,
History5SecondSnapshot
- History6MinAverage
- History8HourAverage
- History8HourSnapshot

Unlike most other tables, history tables cannot be opened and viewed directly. You need to build a query that specifies the point (or points) whose history you are interested in. When you query the history table, include the USTTimeStamp column in the query so that history appears in the correct order even over daylight savings changes.

The first columns in a history table are shown below. All history tables have the same columns.

Figure 53 History table list



History1HourAverage	
TimeStamp	
USTTimeStamp	
Parameter001	
Value001	
Quality001	
Parameter002	
Value002	
Quality002	
Parameter003	
Value003	
Quality003	

To specify the point whose history you are trying to retrieve, you must set ParameterXXX to equal the point ID and parameter.

For example, Parameter001 = 'TankLevel.pv'. This sets Value001 to be the value of the TankLevel's PV, and Quality001 to be the quality of the corresponding history value. The quality indicates the state of the point at the time the sample was taken. Possible qualities are:

GOOD

There are no errors.

BAD

The point was not scanning at time sample taken.

NOT HISTORIZED

The specified parameter has not been assigned to history, but the point has been implemented.

POINT UNSPECIFIED

One of the parameters in the query does not have the corresponding point specified.

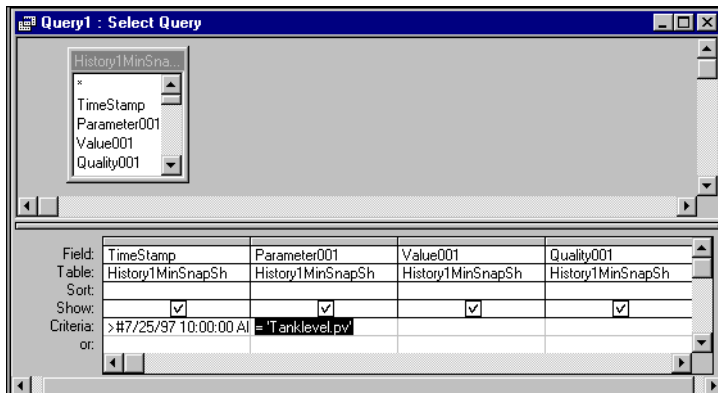
UNIMPLEMENTED

The point specified does not exist in the database, or the user does not have access to that point.

If the parameter name is not specified, it defaults to the point's PV.

As an example, a query set up in Microsoft Access is shown below. This query returns snapshot history values of the PV parameter of the point TankLevel for every minute between 10 am and 4 pm on the 25/7/97.

Figure 54 Design view of a history table query in Access



The equivalent SQL query is:

```
SELECT "TimeStamp", "Value001", Quality001
FROM "History1MinSnapshot"
WHERE ( ( ("Parameter001" = 'TankLevel.pv' ) AND
("TimeStamp" > {ts '1997-07-25 10:00:00'} ) ) AND
("TimeStamp" < {ts '1997-07-25 16:00:00'} ) )
```

Case-sensitive searches

By default all queries made by the Experion ODBC driver are case insensitive. For some queries it might be useful to perform a case-sensitive search. If you want to make searches case-sensitive for a particular data source, you need to add a string to the registry.

To do this:

- 1 Open a Command Prompt window and type the command:
regedt32
- 2 Go to the registry key
HKEY_LOCAL_MACHINE->Software->ODBC->ODBC.INI-> *<Experion data source>*
where:
<Experion data source>
Is the data source you configured (as described in “Configuring a data source” on page 640) and want to use to do case-sensitive searches.
- 3 Add the following new string value for that registry key.
CaseSensitive
- 4 Set the Data value to:
1

Searches Containing Special Characters

If the values you are searching contain special characters, such as - and %, in your query, you need to precede the special character with a backslash (\).

For example, to search for the point sine-1 the query would be:

```
SELECT *
FROM AnalogPoint
WHERE PointID LIKE 'sine\-1'
```

Using Experion ODBC driver and Microsoft Access

The following example assumes that you have already completed the installation and configuration of your Experion system with the ODBC driver.

It assumes that you have:

- Installed the Experion server software
- Installed the ODBC Client software on a client computer
- Configured a data source on the client computer
- Installed Microsoft Access on the client computer
- Started Experion on the server computer
- A license for user scan tasks

The example is based on the following architecture, where the ODBC Client software and Microsoft Access are installed on a network computer.

Step 1. linking tables

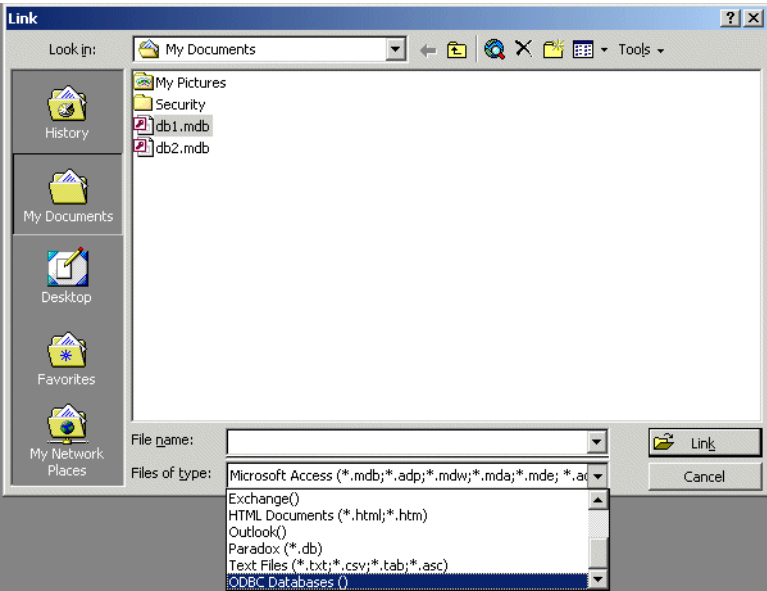
The first step is to link tables so that you can view Experion server data.

To link tables:

- 1 Start up Microsoft Access on your client computer and open a new (blank) database.
- 2 Click the right mouse button in the database window to display the pop-up menu, and select **Link Tables**.

The **Link** dialog box opens.

Figure 55 Link dialog box



- 3 From the Files of Type combobox, select ODBC Databases.
The **Select Data Source** dialog box opens.
- 4 Select **Experion PKS Data Source**, or the data source you configured with the Experion ODBC driver and click **OK**.
The **Connection Details** dialog box opens.
- 5 Use the **Connection Details** dialog box to connect to your Experion database as follows:

For this option:	Type:
Operator ID	The user ID of an operator already configured on your Experion system.
Password	The corresponding password.
Domain	Applicable only if you are using integrated security and domain accounts. The name of the domain to which the operator ID belongs.
Server Name	The name of the computer on which the Experion server software is running. This information is inherited from the DSN you set up in “Configuring a data source” on page 640.

For this option:	Type:
Redundant Server	Check this box if you are running a system with redundant servers. This information is inherited from the DSN you set up in “Configuring a data source” on page 640.
Dual LAN	Check this box if you have a dual network. This information is inherited from the DSN you set up in “Configuring a data source” on page 640.

6 Click OK.

The **Link Tables** dialog box opens.

7 Click Select All, and then OK to produce links to all the visible tables from the Experion database.

8 A number of dialog boxes titled Select Unique Identifier appear. Click OK in each dialog box without selecting any items.

These dialog boxes refer to a feature that is not supported by the Experion server. Changing anything in any of these boxes can lead to unpredictable results.

You have now created links to all the tables in the database. The table names and icons should be visible when the Tables tab is selected.

Step 2. viewing tables

Most tables can be viewed without writing a specific query. For example, you can click the Event2 table to retrieve and display events from the last 24 hours.



Attention

You cannot view the History tables and the Flexible Point table in datasheet view. Use a query to view these tables.

Figure 56 Event2 table viewed in Access

	Time	Source	ConditionName	Priority	Description	Action
	12/11/2002 9:00:32 AM	azgallons	PVLO	L 00		OK
	12/11/2002 9:02:54 AM	azgallons	PVHI	U 00		
▶	12/11/2002 9:04:40 AM	azgallons	PVHI	U 00		OK
	12/11/2002 9:04:51 AM	STATION 1	LEVEL		Security level	
	12/11/2002 9:07:02 AM	azgallons	PVLO	L 00		
	12/11/2002 9:08:52 AM	azgallons	PVLO	L 00		OK
	12/11/2002 9:11:14 AM	azgallons	PVHI	U 00		
	12/11/2002 9:13:00 AM	azgallons	PVHI	U 00		OK
	12/11/2002 9:15:22 AM	sinewave	PVLO	L 00		

Record: 53 of 192

Step 3. designing a simple query

The following queries assume you have built a system sinewave point (called sinewave) on your Experion system that:

- Generates high and low alarms
- Is configured to collect fast history

To do this:

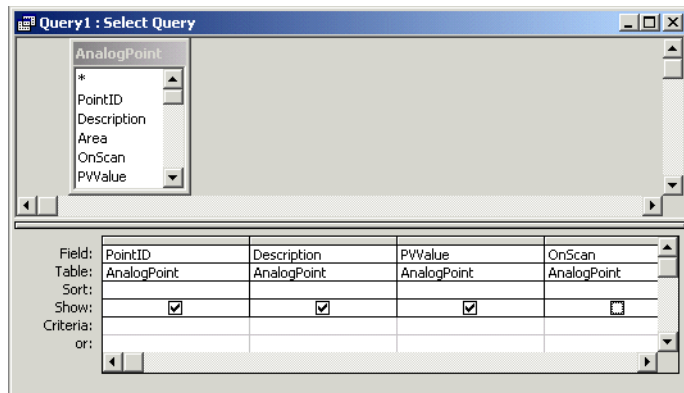
- 1 In the Configuration Explorer of Configuration Studio, click **Control Strategy**.
- 2 In the SCADA Control list, click the **Build channels** task.
- 3 Add a channel, select the channel type **UserScanTask**.
- 4 Add a controller, choosing the controller type **UserScanTask**, and set:
 - The channel name to that of the channel you just created
 - The file number to 8
 - The record number to 1
 - The LRN number to 0
- 5 Add an analog point and set:
 - The PointID to **sinewave**
 - The PV Scan Period to **2** seconds
 - The PV Source address to the controller just built, with a location of **114**.
- 6 Select the Alarm tab and set:
 - The PV High with urgent priority and limit 90
 - The PV Low with urgent priority and limit 10
- 7 Select the History tab and assign the PV to fast history.
- 8 Start Station and log on at MNGR level.
- 9 Choose **Configure > Application Development > System Sinewave**.
- 10 Set the maximum sinewave value to 100, the minimum sinewave value to 0, and the period to a non-zero value (say, 500).

Building a point query

To build a query that selects all the analog points which are currently scanning:

- 1 In your Microsoft Access database, select the **Queries** tab.
- 2 Click **New**.
The **New Query** dialog box opens.
- 3 Select **Design View** and click **OK**.
The **Show Table** dialog box opens.
- 4 Select **AnalogPoint**, click **Add**, and then close the dialog box to bring up the design view.

Figure 57 Design view of an analog point query in Access



- 5 In the first row/first column select **PointID** from the list.
- 6 In the second column select **Description** from the list.
- 7 In the third column select **PVValue**.
- 8 In the fourth column select **OnScan**. In the **Criteria** row, type:
=1
(to select all the points which are currently scanning)
Unmark the check-box to prevent this column from being displayed.
- 9 Choose **View > Datasheet** to send the query to your Experion database.
You should see a table like the one below.

Figure 58 Results of query on analog point table in Access

PointID	Description	PVValue
azgallons		81
sinewave		81

Record: 1 of 2

Building an event query

To build a query that retrieves all events in the last 24 hours:

- 1 In the New Query dialog box, select **Design View**.
- 2 Select **Event2**, click **Add**, and then close the dialog box.
- 3 In the first row/first column select **Event2.*** from the list.
- 4 Choose **View > Datasheet** to send the query to your Experion database.

By default, the ODBC driver retrieves events over the last 24 hours. If you want to retrieve events over a specific period of time you need to specify time criteria.

To retrieve events for a specific time period:

- 1 Open the query in Design View
- 2 Select **LogTimeStamp** from the next available column.
- 3 In the Criteria row, type:
 > #2005-05-24 08:30:00# AND < #2005-05-24 15:30:00#
 (using the actual timespan of your choice)
- 4 Choose **View > Datasheet** to send the query to your Experion database.

Building a history query

The format for history queries is slightly different from other queries because the names of points are system-configurable.

To build a query which retrieves the 5-second snapshot values of your sinewave point over a 10 minute period:

- 1 Select the Queries tab.
- 2 Click **New**, select **Design View** and click **OK**.
The **Show Table** dialog box opens.
- 3 Select **History5SecSnapshot**, click **Add**, then close the dialog box.

- 4 In the first row/first column click the left mouse button and select **TimeStamp** from the list.
In the **Criteria** row type:
> #2005-05-24 08:30:00# AND < #2005-05-24 08:40:00#
(using the actual timespan of your choice)
- 5 In the second column select **Parameter001**.
In the Criteria row type:
= 'sinewave.PV'
- 6 In the third column select **Value001**.
- 7 In the fourth column select **Quality001**.
- 8 Choose **View > Datasheet** to send the query to your Experion database.

Using the Experion ODBC driver with Visual Basic and C++

You can access the server database using Visual Basic or C++ and the Experion ODBC driver.

For information on the data that is accessed see “What data can you access with the Experion ODBC driver?” on page 645.

Prerequisites

- Installed the Experion server software
- Installed the ODBC Client software on a client computer
- Configured a data source on a client computer (see “Configuring the Experion ODBC driver” on page 639)
- Started Experion on the server computer
- Visual Basic Version 6 SP5
- Microsoft Visual C++ 2003

Considerations

- The Experion ODBC driver does not support OR conditions in the WHERE clause of a query.

Visual Basic Example

The following example shows how to access the server database through ODBC Driver using VB. It assumes that there is a Server ODBC Driver Data source called "SRVODBC" set up as described in “Configuring the Experion ODBC driver” on page 639.

- 1 In Visual Basic start a new Standard EXE VB Project.
- 2 Add a Project Reference to Microsoft ActiveX Data Objects Library. (Menu Projects -> References.) This allows communication with the ODBC Driver.
- 3 Add a Project Component: Microsoft Hierarchical FlexGrid Control 6.0 (SP4). (Menu Project -> Components, Controls Tab.) This allows the results of the query to be displayed graphically. A different method can be used to display the returned data if you require.
- 4 Add a command button and an MSHFlexGrid to the form.
- 5 Add the following code:


```
Option Explicit
Private ServerConnection As New ADODB.Connection
' variable for holding
' the connection to the ODBC Driver
Private result As New ADODB.Recordset
' variable for holding the results
```

```

' of the query
Private Sub Command1_Click()
On Error Resume Next
' The following command attempts to open
' a connection to the ODBC Driver
' Replace "userid" with the name of the operator ID you
' are using to connect
' Replace "passwd" with password for the operator ID you are
' using
' Replace "domainname" with the name of the domain to which
' the operator account belongs if you are using integrated
' security and domain accounts
' Replace "hostname" with the name of the Server
ServerConnection.Open "DSN=SRVODBC;UID=userid;" & _
"PWD=passwd;DOMAIN=domainname;RemoteHost=hostname;" & _
"RedundantLAN=0;RedundantCPU=0"
If Err Then
MsgBox "Could not connect", vbCritical
Else
' The following command executes an example query
result.Open ("SELECT AnalogPoint.PointID,
AnalogPoint.Description, AnalogPoint.Area " & _
"FROM AnalogPoint AnalogPoint " & _
"WHERE AnalogPoint.Description Like '%""), ServerConnection
' Display the results in the grid
Set MSHFlexGrid1.DataSource = result
End If
End Sub

```

Where *hostname* is the name of the computer on which the Experion server is running, *userid* is the user ID of an operator already configured on your Experion system and *password* is the correct password for the specified user ID.

6 Run the project and click the command button.

C++ Example

A sample file, `odbcExample.cpp`, containing an example for C++ can be found in Program Files\Honeywell\Experion PKS\server\user\examples\src.

ODBC Standard compliance

The Experion ODBC driver is fully compliant with ODBC 1.0, and partially compliant with ODBC 2.0, and includes ODBC Cursor Library support.

The following table contains the supported keywords. Many of the data manipulation macros supported by SQLServer are not available with the Experion ODBC driver.

Table 21 Supported keywords

Keywords	Keywords
All	IS
AND	LIKE
AS	MAX
ASC	MIN
AVG	NOT
BY	NULL
COUNT	OR
CREATE	ORDER
DELETE	SELECT
DESC	SET
DISTINCT	SQL
DROP	SUM
FROM	TABLE
GROUP	UPDATE
HAVING	USER
IN	VALUES
INSERT	WHERE
INTO	

About Experion ODBC Data Exchange

The ODBC Data Exchange option enables you to configure the two-way exchange of data between the Experion server database and an ODBC-compliant local or network third-party database, using standard Structured Query Language (SQL) commands.

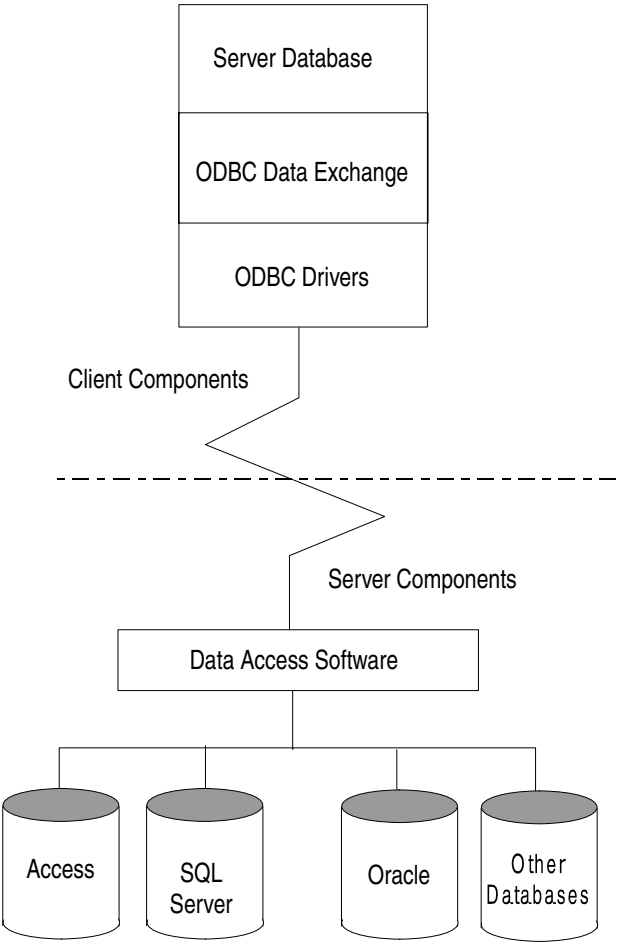
When you configure the Experion ODBC Data Exchange option, the Experion server acts as a *client* application. (Contrast this with the Experion ODBC Driver option where the Experion server acts a *server* application.)

Data from a local Experion server database can be transferred to a third-party database, and data from a third-party database can be transferred into the Experion server database. The information that can be exchanged includes point values, point history, and user file data.

The ODBC Data Exchange option transfers data to and from a third-party database using the ODBC interface. An ODBC driver must be installed for the third-party database. Databases that include ODBC drivers include Microsoft SQL Server, Oracle 7, Microsoft Access, and Sybase 10.

The following diagram shows how the Experion ODBC Data Exchange option interacts with ODBC drivers and third-party databases.

Figure 59 ODBC data exchange architecture



Configuring ODBC Data Exchange Reports

The following procedures assume that you have already completed the Experion ODBC Data Exchange installation as described in the *Installation Guide*.

Specifically, the procedures assume that:

- Your Experion Server license includes ODBC Data Exchange
- You have installed the third-party ODBC driver on the Experion server for the database that you will be transferring data to and from. (For information on installing and configuring the ODBC driver, consult the documentation supplied with the third-party database.)

The configuration procedures depend to a certain extent upon the third-party databases you intend to use in conjunction with the Experion ODBC Data Exchange option.

In general, however, the procedures are as follows:

- 1 Configure a data source on the Experion server, as described in “Configuring the ODBC Data Source” on page 674).
- 2 Configure the ODBC Data Exchange Report, as described in “Configuring the ODBC Data Exchange report” on page 675.
- 3 Create the Input Reference file as described in “Specifying the report definition file details” on page 675.
- 4 Run the report you configured in Step 2.

Configuring the ODBC Data Source

The procedures for configuring the ODBC data source vary according to the third-party database software you will be using. The following procedures show you how to configure the data source for Microsoft SQL Server 7.0. The set up for each driver will differ slightly.

To configure the data source:

- 1 Choose **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.
The **ODBC Data Source Administrator** dialog box opens.
- 2 Click the System DSN tab to display the available data sources.
- 3 Click **Add** to display the Create New Data Source wizard.
- 4 Select **SQL Server** from the list of installed ODBC drivers and click **Finish**.
The **ODBC driver setup** dialog box opens.
- 5 In the ODBC driver setup dialog box, type the data source name, description and Server name and click **Next**.
- 6 Click **Next** and follow the prompts to complete the SQL Server configuration.

Notes

If you intend to use multiple databases, you need to set up a data source for each database.

Configuring the ODBC Data Exchange report

The next step is to use the ODBC Data Exchange Report Configuration display on Station to configure details about the report such as:

- The input reference file name
- Data source name
- Scheduling information for the report

Two displays are used to configure a report:

- Definition Display

This display is common to all reports. Details on using this display are described in “Configuring definition details” on page 403.

- Content Display

Each type of report has a contents display that is specific to the type of report you want to create. For details on configuring the contents of a report on Station, see the following sections.

Specifying the report definition file details

Input Reference File

The Input Reference file defines the actions carried out in the ODBC Data Exchange Report. To create this file, see “Creating the input reference file” on page 679.

Type the full path to the Input Reference file for running the report, or the relative path from the server run folder.

Record Number Offset

Specify a record number offset to be added to the absolute value of any negative record numbers used in references to Experion server database files in the input file. This is optional and the default is zero.

Specifying the SQL database login details

Data Source Name

Type the name of the data source for the database to which the report is to connect. This name should match the Data Source Name entered when you configured the ODBC System Data Source (see “Configuring the ODBC Data Source” on page 674).

User Name

Type the user login name that has permission to access the required database. This is optional.

Store User Password

Click this button to store the password for the user login name that you have specified.

Using the report status information

The **Report status** field of the Configuration display shows one of the following status messages:

WORKING

The report is running

GOOD

The last report completed without errors

ERROR

The last report completed with errors

Notes

- If there are any syntax errors in the Experion server database references, the report is halted, the errors recorded and no data is transferred between the databases.
- If an error occurs while transferring SQL commands to the ODBC driver, the report is halted and errors recorded.
- All syntax error messages are written to both the report output file and the Experion server error log file.
- All Experion server error messages are written to the Experion server log file.

Making a report secure**Report Security Level**

Use the combobox to select a report security level that will be required for a user to demand a report.

Configuring the report setup options**Restricting Data Upload**

Data read from the ODBC database into the Experion server database can be restricted in two ways by stopping:

- Point PV values from being written to
- Point history values from being written to

If you do not want to allow operators to overwrite PV or history value data on the Experion server database, make sure that the **Enable PV Upload** and **Enable History Data Upload** options are not enabled.

Storing failed commands

If you want, you can store commands that have produced database errors by enabling the **Enable Failed Commands Backup** option. If this option is enabled, a backup file is created or appended to whenever an error occurs as a result of a failed SQL command. There is one backup file per report. The reports use the naming convention rptnnn.bak where nnn is the report number.

Any command that results in an error from the SQL database server, as well as those remaining commands which were not executed as a result of the error, will be copied to this backup file, and a message is sent to the log file giving details of the error.

The backup file, if it exists, is run before the Input Reference file each time the report is requested. Execution of the backup file will halt if any SQL command results in an error. Any commands successfully completed from the backup file will be removed from that file. The backup file can be edited or deleted to stop the same erroneous commands being processed.

If any errors are detected, the report status will be set to ERROR and an alarm (priority determined by the “Alarm priority error” combobox) is raised.

Enabling auto-commit for SQL code

If you enable the **Auto-Commit SQL Code** option, Experion will automatically **commit** each command in the Input Reference file as it is executed. This means that any **rollback** commands issued will not be effective, and if a command fails, all previous commands will already have been carried out.

If this option is not enabled, the commands will be committed after successful completion of the report, or rolled back in the event of an error in the report. If you would like to perform **commit** or **rollback** operations at any other time during the report, these must be included in the Input Reference file.

Selecting an alarm priority in the event of a failed SQL report

If the SQL report fails, an alarm is generated with a message describing the type of error. Configure the priority of this alarm by selecting an alarm type from the **Alarm priority on error** list.

Specifying how bad values are handled

You can configure how bad or Not a Number (NaN) numeric and string values are stored in the ODBC database. You use the **Replace Bad/NaN numeric values with** list to specify either a NULL or a zero. You use the **Replace Bad string values with** list to select either a NULL value or an empty string.

Creating the input reference file

The tasks performed by an ODBC Data Exchange report are defined in a free format ASCII file called the Input Reference file. You create this file with a text editor. The file is restricted to 80 characters per line.

Creating SQL transactions

The Input Reference file consists of any number of SQL transactions. Each transaction is made up of:

- Commands

Any SQL command supported by the Open Client interface can be used. Note that any variables declared in these commands will apply only until the end of the current transaction and that each transaction may be up to 1000 lines long.

Each SQL command must begin on a new line and must end with an end-of-command marker (“;”).

- Experion Server references

References to the Experion server database need to be enclosed in “at” symbols (that is, in the format “@. . .@”), and can be embedded anywhere inside the SQL transaction.

Data is extracted from the Experion server database using Experion server references embedded in the SQL command before the end-of-command marker (“;”). Data can be inserted into the Experion server database using Experion server references immediately after the “;”.

Adding comments to the reference file

You can add comments to the Input Reference file to aid readability. Comments are enclosed in /*...*/ and may be nested. There must not be any comments between the end-of-command marker (“;”) and an embedded reference.

Adding Experion server database references

There are three ways to reference the Experion server database:

Point references

Access Experion server point parameters and send or receive data from the ODBC-compliant database.

History references

Access Experion server point history data or receive data from the ODBC-compliant database.

Table references

Access Experion server file data and send or receive data from the ODBC-compliant database.

The following table shows the types of embedded reference which can be used to access or write data to the Experion server.

Action	Experion Server
Read point parameter data	Yes
Write point parameter (excluding point ID, and PV and history parameters)	Yes
Write to PV parameter	Yes ⁱ
Write to history point parameter	Yes ⁱⁱ
Read history	Yes
Write to history	No
Read system and user tables	Yes
Write to system files	No
Write to user tables	Yes
Key: Yes = allowed No = not allowed	

- i To write to the PV parameter of a point, the report must be configured with the “Enable PV Data Upload” option enabled.
- ii To write to a point history parameter, the report must be configured with the “Enable History Data Upload” option enabled.

Understanding the report output

The report output file contains the transactions with data substituted from the Experion server application database. Any syntax errors are flagged with error messages. The report file becomes a record of the data sent to the ODBC-compliant database and the errors found in the reference file.

Troubleshooting ODBC Data Exchange Reports

If an ODBC Data Exchange report fails check the Experion log file for the cause of the problem.

Checking commands

SQLCHK Utility

The Input Reference file can be checked for Experion server database reference syntax errors by using a command-line utility, **SQLCHK**. Each command is read and if there is an embedded Experion server database reference before the end-of-command marker (“;”) it is resolved and data substituted. Embedded references occurring after the “;” are checked for consistency but data is not substituted. Any errors are flagged and a total error count is given after all commands have been read. The commands plus substitutions and error messages are printed to the workstation display and to an output file if one is specified.

Format

```
SQLCHK reference_file [-OUT output_file] [-OFFSET record_offset]
```

Where:

reference_file

Path of input SQL file

output_file

Optional path name of the file to receive checked data and error messages. If this is not specified, the output is printed to the display only.

record_offset

Optional offset added to a negative record number in a reference to a Experion server database file. This is optional and the default is zero.

Example

```
sqlchk command.sql -out command.out -offset 3
```

ODBC Data Exchange report reference

The following sections provide details of how each type of database reference is formatted.

Point reference type

Format

"@ POINTREF POINTNAME *pointname* PARAMETER *parameter* [Numeric] @"

Description

This reference type is used to access point parameters in the Experion server application database.

pointname

Point ID

parameter

Source/destination of data. process point parameters may be used here in the format <block>.<parameter>. For example, PIDA.PV. The names of commonly used point parameters are:

Parameter	Description
PV ³	Process variable
MD	Mode
OP	Output
SP	Setpoint
A1	Auxiliary 1
A2	Auxiliary 2
A3	Auxiliary 3
A4	Auxiliary 4
NAME	Name
DESC	Description
H1M ⁴	1 min history
H6M ⁴	6 min history
H1H ⁴	1 hour history
H8H ⁴	8 hour history
H24H ⁴	24 hour history
H5SF ⁴	Fast history
H1HE ⁴	1 hour extended history
H8HE ⁴	8 hour extended history
H24HE ⁴	24 hour extended history

Notes

1. All SQL keywords may be abbreviated to the first 2 letters
2. Each line must be no more than 80 characters long
3. Data can only be uploaded to the PV of a point if the option “Enable PV Data Upload” is enabled.
4. Data can only be uploaded to the history parameters of a point if the option “Enable History Data Upload” is enabled.
5. If you include the keyword NUMERIC, the PV is transferred as a numeric value.

Example

The following example will extract the PV of the SQLSINE point on the server so that it can be stored in the ODBC-compliant database.

```
update rwb
set realnum=("@ POINTREF POINTNAME sqlsine PARAMETER PV @")
where name_id='Fred Smith';
```

The following example will extract a value from the SQL database, and store it in the PV of the SQLSINE point on the local Experion server.

```
select small from rwb where name_id='Fred Smith';
"@ POINTREF POINTNAME sqlpnt PARAMETER PV @"
```

History reference type report

Format

```
"@ HISTORYREF POINTNAME pointname TYPE histype HOSTNAME hostname
DATE date TIME time | OFFSET offset [ITEMS numitems] [PARAMETER
paramname] [DTSTAMP] [EXTDATA]@"
```

Description

This reference type is used to access point history data on the Experion server. You cannot use this reference type to upload history values. Individual history parameters can be uploaded using the Pointref reference type.

pointname

Point ID

type

Source of data. The names of possible history types are:

History Type	Description
H1M	1 min history
H6M	6 min history
H1H	1 hour history
H8H	8 hour history
H24H	24 hour history
H5SF	Fast history
H1HE	1 hour extended history
H8HE	8 hour extended history
H24HE	24 hour extended history

hostname

The name of the server you are accessing the data from

date

Date of history to access given as DD-MMM-YY format

time

Time of history to access given in HH:MM:SS format

offset

The offset within the history file. Use an offset of **1** to specify the most recent history data.

numitems

Optional number of history items to read.

Parameter

The name of a parameter. For the names of standard point parameters, see “Summary of internal parameters” on page 186.

DTSTAMP

Returns the date and time stamp of when the data was read and stored, as a string. The point value is stored for later retrieval. If DTSTAMP is not specified, the point value is returned and the date and time stamp information is stored for later retrieval.

You use EXTDATA in a separate report without any other arguments to retrieve the stored information.

EXTDATA

Returns the date and time stamp and the point value separated by a comma.

Notes

- All SQL keywords may be abbreviated to the first 2 letters.
- Specify either the date and time, or an offset, but not both.

Example

The following example will extract five SQLSINE values in 6 minute history starting from 10 samples ago, and store values in the ODBC-compliant database.

```
insert into historytable
values
("@HISTORYREF POINTNAME sqlsine TYPE H6M OFFSET 5
ITEMS 10 @")
;
```

Table reference type report

Format

```
"@ TABLEREF TABLENUM table RECORDNUM record WORDNUM word
  NUMRECORDS numrecords datatype @"
```

Description

This reference type is used to access file data in the Experion server database.

table

The server file number to read from or write to

record

First record number to use

word

First word number to use

numrecords

The number of records to read/write

datatype

A data type for each column in the ODBC-compliant database must be entered. The following data type SQL keywords are available.

Data Type Keyword	Data Type Description	Data Item Following Keyword	Stored in database as
FLOAT	32 bit floating point	[Optional number of items]	2 words
2INT	16 bit signed integer	[Optional number of items]	1 word
4INT	32 bit signed integer	[Optional number of items]	2 words
CHAR	Character string enclosed in '...'	Number of characters + [Optional number of items]	(Number of chars/2) words byte swapped
RAWCHAR	Character string not enclosed in '...'	Number of characters + [Optional number of items]	(Number of chars/2) words byte swapped
BITNUMBER	The number of the bit to retrieve from, starting at 0	Bit number	Part of word

Data Type Keyword	Data Type Description	Data Item Following Keyword	Stored in database as
SIZE	For use with BITNUMBER. The number of bits to retrieve, starting at BITNUMBER. The number of bits specified cannot extend over a word boundary.	Number of bits + [RPTBIT keyword to denote bit repeat] + [Optional number of items]	
RPTBIT	Denotes that successive BITNUMBER items should be taken from the same word instead of successive words (the default).		
JULDATE	16 bit integer describing the number of days since 1 January 1981.	[Optional number of items]	1 word
TIME	32 bit floating point describing the number of seconds since midnight.	[Optional number of items]	2 words
DATETIME	JULDATE followed by a time field.	[Optional number of items]	3 words first word is JULDATE, second and third words are time

Notes

- All SQL keywords may be abbreviated to the first two letters.
- For table data being extracted from the Experion server, any database file can be accessed.
- For table data being inserted into the Experion server database, only user files can be accessed.
- If the BITNUMBER keyword is used, then the SIZE keyword must appear after the bit number (that is, BITNUMBER *bitnumber* SIZE *num-of-bits*).
- The RPTBIT keyword must appear after the BITNUMBER/SIZE reference and will denote that successive BITNUMBER items will be read/written from the same word rather than successive words, which is the default.

In addition, the number of bits specified cannot extend over a word boundary. For example, if BITNUMBER = 2, then the data can only extend from bits 2 to 15 for that word. Bit counting starts from 0. Thus, the number of bits must

be limited to a value 14. Otherwise, an error will occur during validation. In general, the BITNUMBER must be £ 16.

- If a number of items appear without one of the data type SQL keywords, then the data type will default to 2INT.

Example

The following example will extract a floating point number, a 2-byte integer and 3 strings 10 characters long from an ODBC-compliant database, and store the values in record 5 of the file 256 starting at word 1.

```
select floatnum,intnum,string1,string2,string3 from rwb
where name_id='Fred Smith';
"@ TABLEREF TABLENUM 256 RECORDNUM 5 WORDNUM 1 NUMRECORDS 1
  FLOAT 2INT CHAR 10 3 @"
```

The following example will extract a floating point number, a 2-byte integer and 3 strings 10 characters long from record 5 of the file 256 starting at word 1, and store this data in the SQL database.

```
insert into rwb
values(
where name_id='Fred Smith';
"@ TABLEREF TABLENUM 256 RECORDNUM 5 WORDNUM 1 NUMRECORDS 1
  FLOAT 2INT CHAR 10 3 @"
```

SQL report example

The following example is written for Microsoft SQL Server. Some of the SQL syntax is specific to Microsoft SQL Server, for example, `getdate()`.

SQL input data reference file

```

/* insert values from Points "01SQLANA","01SQLSTA" to ODBC-
   compliant database "testtable"*/
insert into testtable
values(
"@ Pointref Pointname 01SQLANA parameter name @",
getdate(),
"@ Pointref Pointname 01SQLANA parameter PV @",
"@ Pointref Pointname 01SQLSTA parameter PV @",
"@ Pointref Pointname 01SQLANA parameter A1 @",
"@ Pointref Pointname 01SQLSTA parameter H1H @",
"@ Pointref Pointname 01SQLANA parameter OP @");

/* read from ODBC-compliant database "testtable" to Points
   "01SQLANA","01SQLSTA"*/
select distinct testint from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter PV @"

select distinct testsmall from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLANA parameter A1 @"

select distinct smallfloat from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter H1M @"

select distinct testint from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter OP @"

select distinct smallfloat from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLANA parameter SP @"

select distinct name from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter DESC @"

/* read from a user table 4 (file 254) to ODBC-compliant
   database "testtable"*/
insert into testtable
values(
'New Record',
"@ tableref tablenum 254 record 1 word 1 datetime @",
"@ tableref tablenum 254 record 1 word 2 float double 4int 2int
   bit 0 size 8@"
);

```

```

/* read from user table 4 to ODBC-compliant database "testtable"
   with record offset */
insert into testtable
values(
'Offset Record',
"@ tableref tablenum 254 record -1 word 1 datetime @",
"@ tableref tablenum 254 record -1 word 2 float
   double 4int 2int bit 0 size 8@");

/* read from ODBC-compliant "testtable" to user table 4*/
select distinct name,name,testdate,smallfloat,testint,
testsmall,testtiny,testtiny
from testtable where name='01SQLANA';
"@ tableref tablenum 254 rec 3 word 1 char 10 2 datetime float 2
2int bit 1 size 5 rptbit 2 @"

/* read from ODBC-compliant with record offset to user table */
select distinct name,name,testdate,smallfloat,testint,
testsmall,testtiny,testtiny
from testtable where name='01SQLANA';
"@ tableref tablenum 254 rec -3 word 1 char 10 2 datetime float
2
2int bit 1 size 5 rptbit 2 @"

/* read history values into ODBC-compliant */
update testtable set
testint=
"@ history Pointname 01SQLANA type H24H offset 3 @",
smallfloat =
"@history Pointname 01SQLANA type H6M date 15-FEB-94 time
13:48:00 @"
where name='01SQLANA'

```

Contents of report file and output from SQLCHK

```

/* insert values from Points "01SQLANA","01SQLSTA" to ODBC-
   compliant "testtable"*/
insert into testtable
values(
'01SQLANA',
getdate(),
1.200000e+01,
0.000000e+00,
0.000000e+00,
0.000000e+00,
0.000000e+00
);

/* read from ODBC-compliant "testtable" to Points "01SQLANA",
   "01SQLSTA"*****/

```

```

select distinct testint from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter PV @"

select distinct testsmall from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLANA parameter A1 @"

select distinct smallfloat from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter H1M @"

select distinct testint from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter OP @"

select distinct smallfloat from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLANA parameter SP @"

select distinct name from testtable where name='01SQLANA';
"@ Pointref Pointname 01SQLSTA parameter DESC @"

/* read from a user table 4 (file 254) to ODBC-compliant
"testtable"*/
insert into testtable
values(
'New Record',
'01-JAN-81 00:00',
0.000000e+00,
0.000000e+00,
0,
0,
0
);

/* read from user table 4 to ODBC-compliant "testtable" with
record offset */
insert into testtable
values(
'Offset Record',
'01-JAN-81 00:00',
0.000000e+00,
0.000000e+00,
0,
0,
0
);

/* read from ODBC-compliant "testtable" to user table 4*/
select distinct name,name,testdate,smallfloat,testint,
testsmall,testtiny,testtiny
from testtable where name='01SQLANA';
"@ tableref tablenum 254 rec 3 word 1 char 10 2 datetime float 2
2int bit 1 size 5 rptbit 2 @"

```

```

/* read from ODBC-compliant with record offset to user table */
select distinct name,name,testdate,smallfloat,testint,
testsmall,testtiny,testtiny
from testtable where name='01SQLANA';
"@ tableref tablenum 254 rec -3 word 1 char 10 2 datetime float
2
2int bit 1 size 5 rptbit 2 @"

/* read history values into ODBC-compliant */
update testtable set
testint = 0.000000e+00,
smallfloat = 0.000000e+00

where name='01SQLANA'

```


Configuring OPC

32

This chapter describes how to configure Experion OPC options.

To:	Go to:
Learn about Experion OPC options	page 696
Learn about OPC's background and basic terminology	page 704
Learn how Experion communicates with third-party OPC servers and clients	page 706
Configure the Experion OPC Advanced Client	page 709
Configure the Experion OPC Display Data Client	page 718
Configure the Experion OPC Data Access Server	page 720
Configure the Experion OPC Historical Data Access Server	page 738
Configure the Experion OPC Alarm and Event Server	page 741
Configure the Experion OPC Integrator	page 743

Experion OPC Options

Experion provides the following OPC options, each of which has been optimized for a particular purpose:

- Experion OPC Client Interface
- Experion OPC Advanced Client
- Experion OPC Display Data Client
- Experion OPC Data Access Server
- Experion OPC Alarm and Event Server
- Experion OPC Historical Data Access Server
- Experion OPC Integrator

Experion OPC Client Interface

The Experion OPC Client Interface is primarily designed for integrating low-complexity subsystems, such as controllers. Configuration involves individually mapping OPC items to standard Experion points (analog, status and so on). If you require alarming for an item, you must configure the associated point's alarm properties.

There are two options for supporting redundant third-party OPC servers:

- The OPC Client interface native supports the concept of preferred and secondary servers.
- Redirection Manager can be used with redundant third-party OPC servers, which can give better performance during OPC server failover due to the fact that it builds OPC groups on both OPC servers.

Experion OPC Advanced Client

The Experion OPC Advanced Client includes a data client, and an alarm and event client for connection to third-party OPC servers.

Redirection Manager should be used when communicating to redundant third-party OPC servers. It is preferable for the third-party OPC servers to run in a dual active mode rather than an active-passive mode.

Experion OPC Advanced Data Client

The Experion OPC Advanced Data Client is primarily designed for integrating complex subsystems, such as distributed control systems. Such systems typically have point-like structures, that is, complex data structures. It is based on the OPC Foundation Data Access Specification Version 2.0.

OPC items are mapped to OPC advanced points. You build OPC advanced points in Quick Builder. The OPC advanced point allows you to create arbitrary point parameter names to reference OPC items. The OPC advanced point also allows you to have more than 8 scanned parameters. The scanned parameters can also have user-defined names.

After you have built your OPC advanced points, you can add these points to trends, custom displays, group displays, just as you can with other point types in Experion.

If you want alarms, you need to use the OPC Advanced Data Client in conjunction with the OPC Advanced Alarm And Event Client.

Experion OPC Advanced Alarm and Event Client

The Experion OPC Advanced Alarm and Event Client enables Experion to receive alarms and events from third-party OPC alarm and event servers. It is based on the OPC Foundation Alarm and Events Specification Version 1.0.

OPC alarms are displayed and acknowledged in the same way as Experion alarms, giving operators a uniform user interface. For example, when an OPC alarm is received, it appears in the Alarm Summary; and when an operator acknowledges the alarm, confirmation of the acknowledgement is sent to the OPC alarm and event server.

To learn how to configure an Experion OPC Advanced Alarm and Event Client, see “Configuring the Experion OPC Advanced Client” on page 709.

Experion OPC Display Data Client

The Experion Display Data Client is designed to be used when you want to add OPC data to custom displays and you have no requirement for other information such as history or alarms. It supports the OPC Foundation 2.0 Data Access Specification Version 2.0.

Redirection Manager should be used when communicating to redundant third-party OPC servers. It is preferable for the third-party OPC servers to run in a dual active mode rather than an active-passive mode.

You can add OPC data items directly to custom displays without having to build points in Quick Builder.

To learn how to configure an Experion OPC Display Data Client see “Configuring the Experion OPC Display Data Client” on page 718.



Attention

The Experion Display Data Client does not support:

- Alarming
 - History
 - Server Scripting
 - Microsoft Excel Data Exchange
 - ODBC driver
 - Reports
-

Experion OPC Data Access Server

The Experion OPC Data Access Server gives an OPC client read/write access to Experion point parameters. It is based on the OPC Foundation Data Access Specification Version 2.0, and can accept connections from either OPC Version 1.0 or Version 2.0 clients.

The Experion OPC Data Access Server supports all mandatory OPC interfaces, including an automation interface for application development in Visual Basic, as well as the IOPCBrowseServerAddressSpace interface. For more information on the automation interface, see the *OLE for Process Control Standard Version 1.0a* or the *OLE for Process Control Standard Version 2.0*.

To learn how to configure the Experion OPC Data Access Server, see “Configuring the Experion OPC Data Access Server” on page 720.

Experion OPC Historical Data Access Server

The Experion OPC Historical Data Access Server gives an OPC client access to Experion point parameter history. It supports the OPC Historical Data Access Specification Version 1.2.

For more information about the Experion OPC History Data Access Server, see “Configuring the Experion OPC Historical Data Access Server” on page 738.

Experion OPC Alarm and Event Server

The Experion OPC Alarm and Event Server allows an OPC alarm and event client to receive alarm and event information from Experion. It supports the OPC Version 1.02 Foundation Alarm and Event Specification.

To learn how to configure an Experion OPC Alarm and Event Server, see “Configuring the Experion OPC Alarm and Event Server” on page 741.

Experion OPC Integrator

The Experion OPC Integrator is designed to allow data to be transferred bi-directionally between two or more OPC servers. The following scenarios illustrate typical uses of the Experion OPC Integrator:

- You have a system that provides an OPC data access server, but not an OPC client. However, the system needs to retrieve data from Experion.
- Experion data needs to be transferred to a third-party OPC server whenever it changes, irrespective of the reason for the change (including when the data is changed by an operator).
- You have Experion Process controllers and need to transfer data efficiently between the controllers at the supervisory control layer.

**Caution**

Do not use OPC Integrator to transfer safety or mission critical information between controllers. For this type of information, use a method to transfer information directly between controllers.

OPC Integrator supports redundant Experion servers, and is therefore itself redundant; it also supports redundant third-party OPC servers.

To learn how to configure an Experion OPC Integrator, see “Configuring Experion OPC Integrator” on page 743.

About OPC

OPC (OLE for Process Control) consists of a set of standards that define COM interfaces to be observed by OPC clients and servers. (The COM interfaces are based on Microsoft's COM/OLE technology.)

These standards were established by the OPC Foundation to foster greater interoperability between automation and control applications, field systems and devices, and business and office applications. (For detailed information about OPC, visit the OPC Foundation's Web site, <http://www.opcfoundation.org>.)

OPC provides data from a data source (server) and communicates the data to any client application in a standard way, thereby eliminating the requirement for an application to have specific knowledge about a particular data source, such as its internal structure and communications protocols.

About the OPC Data Access Standard

The OPC Data Access Standard does not have a concept of hardware or points—there are just *items* (units of data in the data source).

Transferring data

To receive items from the OPC server, the OPC client must gather one or more items into a *group*. The OPC client requests the OPC server to create a group with a client-specified maximum update rate and a *deadband*. The OPC client then requests the OPC server to add items to the group. The update rate and the deadband of a group apply to all items in that group. (Although the OPC client can specify any update rate for a group, the OPC server decides whether the request is honored.)

Callback

Generally, the OPC server sends data to OPC clients using a *callback* technique.

After a group has been created, the OPC server creates a cache for the group, which is updated according to the group's update rate. The OPC server only sends updated values to the OPC client for items in the group if there has been significant change since the last cache update. (What constitutes "significant" is based on the group's deadband.)

The callback technique significantly reduces traffic between the OPC client and the OPC server because there is no need for periodic read requests to the OPC server. An OPC client gets data whenever there is a significant change (which is defined by the OPC client).

Synchronous read request

The OPC client can obtain data from the OPC server by sending *synchronous read requests* to the OPC server, independent of the server callbacks. The OPC client specifies whether the data should come from the OPC server's internal cache or from the field/hardware device.

About Experion-to-OPC Server/Client communications

This section provides an overview of the way in which Experion OPC servers and clients communicate with third-party OPC clients and servers.

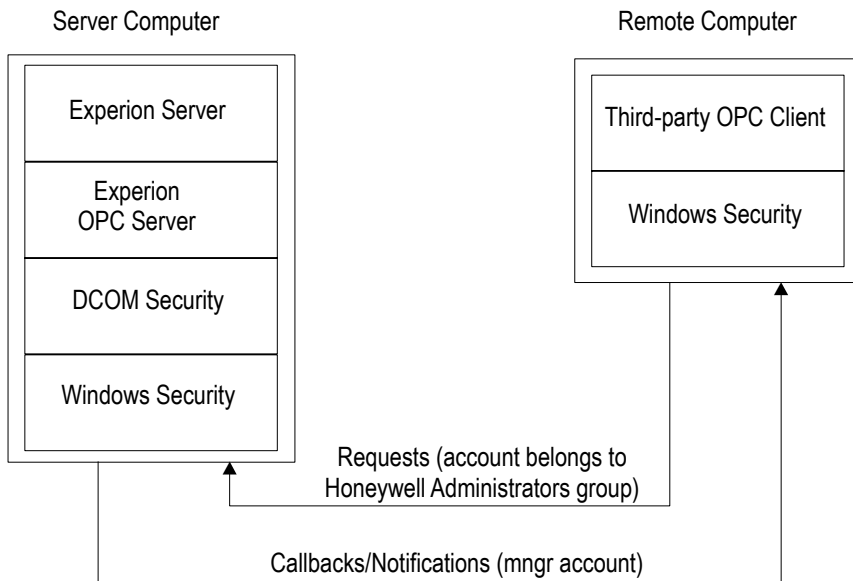
The accounts used to communicate with third-party OPC clients and servers were set up when installing Experion.

Communicating with third-party OPC clients

The following figure shows a typical setup where you have an Experion OPC server.

When the OPC client wants to communicate with the Experion OPC server, it connects to the server computer using an account on the server computer that belongs to the Honeywell Administrators group. (This group has the DCOM security permissions required to access the OPC server.)

Conversely, when the Experion OPC server wants to communicate with the OPC client, it connects to the remote computer using the `mngr` account on that computer.

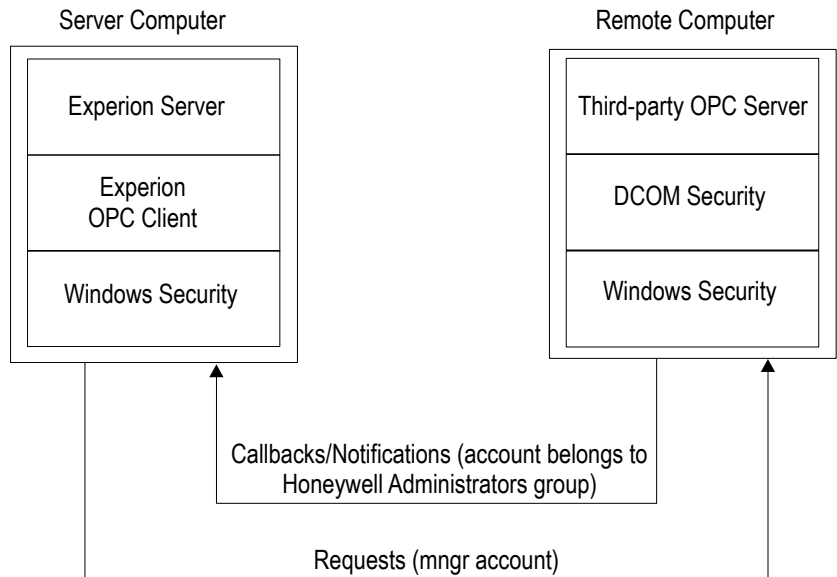


Communicating with third-party OPC servers

The following figure shows a typical setup where you have an Experion OPC client (data or alarm/event).

When the Experion OPC client wants to communicate with the third-party OPC server, it connects to the remote computer using the `mngtr` account on that computer, and accesses the OPC server via DCOM security.

Conversely, when the third-party OPC server wants to communicate with the Experion OPC client, it connects to the server computer using an account on the server computer that belongs to the Honeywell Administrators group.



Firewall security

Microsoft Windows XP SP2 and Windows Server 2003 SP1 add significant security enhancements to the operating system which includes changes to host firewall. By default, the host-based firewall rejects any incoming connections such as OPC connections.

During Experion installation some of the default Windows security settings to allow connections to the Experion OPC servers.

If you are connecting to third-party OPC servers, you need to modify the default Windows security settings to allow these connections. For more information, see the document, *Using OPC via DCOM with Microsoft Windows XP Service Pack 2*, available from the OPC Foundation.

Redirection Manager

Redirection Manager (RDM) provides transparent connection between a third-party OPC client and redundant Experion servers. RDM should also be used when Experion OPC clients connect to redundant third-party OPC servers. For information about the tasks required to install and configure Redirection Manager, see the following topic in Knowledge Builder: Experion R300 > Installation and Upgrades > Supplementary Installation Tasks Guide > Installing Redirection Manager.

Configuring the Experion OPC Advanced Client

To use the Experion OPC Advanced Client, you must first configure a connection to the third-party OPC server.



Attention:

There are different interpretations of the OPC AE standard by third-party OPC AE server vendors. Integration issues have been seen with OPC condition events in areas such as alarm acknowledgement and duplicate alarm identification. If you want to integrate a third-party OPC AE server that utilizes OPC condition events with Experion, you should contact Honeywell.

The risks with OPC simple and tracking events are lower than for OPC condition events, however, due to different interpretations of the OPC AE standard, integration issues may still be found. Thorough testing between the Experion OPC client and third-party server should be performed to ensure correct operation.

Considerations

- For an introduction to OPC and its terminology, see “About OPC” on page 704.
- For details about how standard OPC event attributes are mapped to their Experion equivalents, see “Experion support for OPC event attributes” on page 716.

Tasks

Complete the tasks in the following order.

Task	Go to:	Done?
Configure the OPC server connection (data and alarm/event).	page 710	
Map OPC alarms/events to Experion alarms/events.	page 714	
If you are configuring the client for alarms/events, select the Notifications check box on the Status tab to start processing OPC alarms/events.		
If you are configuring the client for data only, build OPC advanced points in Quick Builder.	<i>Quick Builder Guide</i>	
If Stations are set up to monitor specific assets, set up the appropriate Stations to monitor the assets you have assigned to the OPC server.	page 338	

Configuring the OPC server connection

This procedure is applicable to both data and alarm/event servers.

Prerequisites

- You must be logged on to Station with ENGR or MNGR security level to perform this task.
- When you configure asset mapping, you must disable notifications.

Considerations

- OPC AE server source names must obey Experion point naming conventions for legal characters.

To configure the OPC server connection:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure system interfaces** task.
The System Interfaces display appears in the System Display tab in Configuration Studio.
- 3 In an empty row select OPCADVNC from **Type** and click **OPCADVNC** in the **Alias** column to call up the System Interface configuration displays.
- 4 Click the following tabs and configure the properties as appropriate:
 - Configuration tab
 - Attribute Mapping tab
 - Asset Mapping tab

(The Tuning tab properties are automatically adjusted to be compatible with the Experion server's global cache settings. The Status tab provides status information about the connection.)

Configuration tab

The Configuration tab specifies the connection details for an OPC data server (**Data Source** properties) and an OPC alarm/event server (**Notification Source** properties).

Property	Description
Server Identity	

Property	Description
Server Alias	The name of the connection. This name is used in alarms and events generated for this connection and also appears in the Location pane of the System Status display.
Data Source	
Network Name	The name of the network on which the OPC data server resides.
Server ProgID	The ProgID of the OPC data server.
Notification Source	
Network Name	The name of the network on which the OPC alarm/event server resides.
Server ProgID	The ProgID of the OPC alarm/event server.

Attribute Mapping tab

The Attribute Mapping tab specifies how the OPC server attributes (alarm/event) are mapped to Experion attributes.

Property	Description
Notification Category and Attribute Mapping	
Mapping File	The name of the XML file that defines the mapping of OPC alarm/events to Experion alarms/events. See “Mapping OPC alarms/events to Experion alarms/events” on page 714.

Asset Mapping tab

The Asset Mapping tab specifies how areas defined on the OPC server (alarm/event) are mapped to Experion assets. (When Experion receives alarm/event from the OPC server, it is automatically assigned to the appropriate Experion asset.)

Considerations

- Before you can map OPC areas to Experion assets, you must first define the Experion assets.

Property	Description
Map all OPC areas to this default assignable asset	Maps all OPC areas to the default Experion asset. Select this if areas have not been defined on the OPC server.

Property	Description
Use assignable assets as defined on the OPC server (direct mapping)	Automatically maps OPC areas to Experion assets with the same name. Note: The tag names of the Experion asset must exactly match the OPC areas. If there is no matching Experion asset for an OPC area, Experion will not correctly process data or alarms/events from that area. The Experion asset must be an assignable asset.
Map OPC areas as follows	Individually map OPC areas to Experion assets.

Tuning tab

The Tuning tab specifies the communication-related properties of the connection.



Attention

The tuning properties are automatically adjusted to be compatible with the Experion server's global cache settings. You should only change them if you have been instructed to do so by Honeywell support personnel, or you have extensive experience with system interfaces.

Property	Description
Data Settings	
Cache flush time	The intervals (in milliseconds) that the subscription list is checked for references to old data. The default value is 15 seconds (15,000 ms).
Cache age time	The amount of time (in milliseconds) old data remains in the dynamic cache. The default value is 1 minutes (600,000 ms).
Maximum subscription time	The slowest subscription time (in milliseconds). The default value is 10 seconds (10,000 ms). If the subscription time is slower than that specified, the subscribing server switches from subscription to synchronous read (polls). Maintaining a slow subscription is not efficient.
Connection Timeout	The maximum time (in seconds) the Experion server allows for a data request to complete. If the connection times out, a connection failure is recorded and a new connection is attempted. The default value is 30 seconds .
List fragment size	The size of data packets sent over the network. The default is 500 parameter values. This is tuned for optimal performance on low bandwidth links.

Property	Description
Drift Deadband	The OPC server only sends an updated value to the Experion server if the value has changed by the deadband percentage since the last update.
Notification Settings	
Connection timeout	The amount of time (in seconds) a packet of data can remain on the network without being acknowledged. When the timeout period expires, the connection is broken and communication is initiated again. The default value is 10 seconds.
Notification buffer interval	The maximum amount of time (in seconds) a notification can be delayed on the publishing server before being sent to the subscribing server. The default value is 2 seconds
Notification keep alive interval	The maximum amount of time (in seconds) the publishing server does not send packets to the subscribing server. If there are no notifications within this time, an empty keepalive packet is sent to the subscribing server. The default value is 15 seconds.
List fragment size	The size of data packets sent over the network. The default is 100 notifications. This is tuned for optimal performance on low bandwidth links.

Status tab

The Status tab provides status information about the connection. It also contains the following controls:

- **Notifications** check box which enables/disables notifications (alarm/events) from the OPC alarm/event server
- **Reset Statistics** button

Mapping OPC alarms/events to Experion alarms/events

When you create the OPC server connection, Experion defines the name for a mapping file, the name of which is based on the server alias. Experion creates this file only when you first connect to the OPC server. This mapping file, which is an XML file, defines the event types on both the Experion server and the OPC server.

To see the name of this mapping file, click on the **Attribute Mapping** tab of the OPC server configuration. The XML file is located in Program Files\Honeywell\Experion PKS\server\data\mapping.

The mapping file includes two parts:

- **Experion event type definitions** (delineated by the <!-- and --> element pair)
- **OPC server event type definitions** (delineated by the <configuration> and </configuration> element pair)

Editing the mapping file

In order to map OPC alarms/events to Experion alarms/events, you must open the mapping file (in a text editor such as Notepad) and specify appropriate values for the “mapto” attributes of the OPC event types. (When Experion creates the file, it does not specify any values for these attributes.)

Notes

- Before editing the mapping file, you must clear the **Notifications** check box on the Status tab to block incoming alarms/events from the OPC server. Conversely, after editing the mapping file, you must select the **Notifications** check box.

Example

The following extract from an XML file contains an Experion alarm called “Process Alarm” and an OPC alarm called “Level”.

```
<!--
.
.
Category:   'Process Alarm'
Attributes: ... 'Comment' 'Asset name'...
.
.
-->

<configuration>
<category name="Level" type="Condition" mapto="">
  <attribute name="AckComment" mapto="" />
  <attribute name="Areas" mapto="" />
```

```

      .
      .
    </category>
  </configuration>

```

In order to map the “Level” alarm to the “Process Alarm”, you would edit the definition of “Level” as follows:

```

    <category name="Level" type="Condition" mapto="Process Alarm">
      <attribute name="AckComment" mapto="Comment" />
      <attribute name="Areas" mapto="Asset name" />
      .
      .
    </category>

```

Experion support for OPC event attributes

The following table describes how standard OPC event attributes are mapped to their Experion equivalents.

OPC Attribute	Experion Attribute(s)	Experion Data Type	Notes
ActiveTime	Date, Time		Experion converts to its system date/time.
AREAS	Asset Name	40 chars	Recommended vendor-specific attribute.
Source	Source	40 chars	
SubConditionName	Alarm	7 chars	
Severity	Priority, Level		Experion converts to its priority and level. See “OPC severity mapping” on page 716.
Message	Description	30 chars	
NEW VALUE	Value	18 chars	Recommended vendor-specific attribute.

OPC severity mapping

OPC (1-1000)	Experion Scale	
	Priority	Sub Pr (0-15)
950	Urgent	12
900	Urgent	8
850	Urgent	4
800	Urgent	0
750	High	12
700	High	8
650	High	4
600	High	0
550	Low	12
500	Low	8
450	Low	4
400	Low	0
350	Journal	12

OPC (1-1000)	Experion Scale	
	Priority	Sub Pr (0-15)
300	Journal	8
250	Journal	4
200	Journal	0
100		
1	Event	

Configuring the Experion OPC Display Data Client

This section describes how to set up the Experion OPC Display Data Client.

Prerequisites

- You must be logged on to Station with ENGR or MNGR security level to perform this task.

To configure the OPC server connection:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure system interfaces** task.
The System Interfaces display appears in the System Display tab in Configuration Studio.
- 3 In an empty row, select **OPCDISPLAY** from the **Type** list and click the blue dash (-) in the **Alias** column to call up the System Interface configuration displays.
- 4 In the **Server Alias** box, type the alias to use for this connection.
Experion creates a point with the same name to hold the OPC data item.
- 5 In the **Network Name** box, type the name of the OPC server you are connecting to.
- 6 In the **Server ProgID** list, select the program ID of the OPC server you are connecting to.

After you have configured the OPC Display Data Client you can add OPC data to custom displays.

To add OPC data to a custom display:

- 1 Start HMIWeb Display Builder:
 - If you are on the Experion server, choose **Start > Programs > Honeywell Experion PKS > Server > HMIWeb Display Builder**
 - If you are on a client computer, choose **Start > Programs > Honeywell Experion PKS > Client Software > HMIWeb Display Builder**
- 2 Choose **File > New > Display**.
A blank display appears.
- 3 Click the  (Alphanumeric) icon on the Toolbox toolbar and then drag the pointer on the display to define the size, shape and position of an alphanumeric.

- 4 Double-click the alphanumeric to open the Properties Window, which shows the alphanumeric's current properties.
- 5 Click the Data tab and make sure that Point/Parameter is selected in **Type of database link**.
- 6 In the **Point** box, type the OPC server alias.
- 7 In the **Parameter** box, type the OPC item you want to display.
- 8 Configure the other properties as appropriate.
- 9 Repeat steps 3 to 8 for other items you want to include in the display.

Mapping OPC data types to Experion data types

OPC data from the OPC server is sent inside a variant. The following table shows how the variant data types map to Experion data types.

Variant	Experion Data Type
VT_UI1	16 bit signed integer (INT2)
VT_I1	16 bit signed integer (INT2)
VT_I2	16 bit signed integer (INT2)
VT_UI2	32 bit signed integer (INT4)
VT_INT	32 bit signed integer (INT4)
VT_UINT	64 bit floating point (DBLE)
VT_I4	32 bit signed integer (INT4)
VT_UI4	64 bit floating point (DBLE)
VT_I8	64 bit floating point (DBLE)
VT_UI8	64 bit floating point (DBLE)
VT_R4	32 bit floating point (REAL)
VT_R8	64 bit floating point (DBLE)
VT_BSTR	String
VT_DATE	Date/Time

Other variant types are stored as a variant in the Experion database. Their value can be accessed through the API but not displayed in Station.

If the data type is numeric and has enumerated data attached, the Experion data type will be an enumeration. In this case it is possible to access either the numeric index or the associated string value.

Configuring the Experion OPC Data Access Server

This section describes how to set up the Experion OPC Data Access Server so that it can service requests from an OPC data client.

Prerequisites

- You have installed and set up the third-party OPC client components as described in the *Supplementary Installation Tasks Guide*.

Considerations

- The ProgId of the Experion OPC Data Access Server is `HWHsc.OPCServer`.
- For an introduction to OPC and its terminology, see “About OPC” on page 704.



Tip

For instructions on how to change the read/write permissions for the Experion OPC data access server, see the *Supplementary Installation Tasks Guide*.

See also

“OPC-accessible point parameters” on page 724

“Error codes and qualities” on page 737

Accessing Experion data

In order to access Experion data, you need to build OPC items using the following formats:

- For all point types, except process
FullItemName.parameter [/enum]
- For process points
FullItemName.block.parameter [/enum]

For details about building items, see the documentation supplied with your OPC client.

Item	Description
<i>FullItemName</i>	The full item name of the point. For example, /Assets/Plant/Filtration/Tank/FlowMeter.
<i>block</i>	The control module parameter.
<i>parameter</i>	The point's parameter. See "OPC-accessible point parameters" on page 724.
<i>enum</i>	Indicates that the parameter is enumerated. See "Interpreting enumerated parameters" on page 721.

Examples

```
/Asset/Plant/Filtration/Tank/FlowMeter.PV
/Asset/Asset1/TestPoint.PIDA.MD
/Asset/Plant/Filtration/Tank/FlowController.PV /enum
```



Attention

The formats *point.parameter* [/enum] and *point.block.parameter* [/enum] are supported for backward compatibility.

Interpreting enumerated parameters

An enumerated parameter is one that contains an integer value and a string. The Experion OPC Data Access Server supports two methods of accessing enumerated parameters:

- The parameter is written and/or read as text. (For this method to work, the parameter must be configured with its **enum** property selected.)
- The parameter is written and/or read as an integer. The server reads/writes the integer value, and it is the responsibility of the client to convert the integer value into text if required.

Notes

- If you build an item for which enumeration makes no sense, an empty string is returned.

Update rates and deadbands for items

An update rate and a deadband can be associated with each item or group.

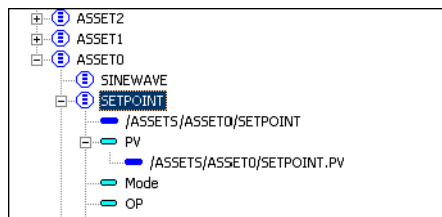
The update rate is the fastest rate at which the Experion OPC Data Access Server will notify the OPC client of changes in data. In the case of deadband, the server will only notify the client of changes if the data has changed by more than the deadband.

The client may automatically determine the update rate and deadband, or you may need to configure it. You can normally specify any update rate and deadband in the client; however, specifying high rates or low deadband values will increase the load on the server and the connecting network. If the load is too high, the server will not return data at the requested rate.

Specifying the model used in the browse address space

You can specify how the Experion OPC Data Access Server presents the browse address space. The alternatives are presenting the enterprise model or the asset-point model.

The enterprise model provides a hierarchical model of the assets and points on your Experion server. The first level consists of alarm groups, assets and system components. The first level assets then expand to show assets as defined in your asset model. If you use the enterprise model, the name format used is the full item name, for example, /Asset/Asset0/Setpoint. The following figure shows an example of how points and parameters are shown in the browse address space.



The asset-point model provides a list of all assets. The assets then expand to show points associated with each asset. If you use the asset-point model, CPM, CEE, and IOM hardware points are not shown in the browse address space. To access these points you need to build OPC items using the format:

Point.block.parameter [/enum]

To specify which model is used in the browse address space:

- 1 From the **System Configuration Menu** display, click **Server Wide Settings**.
The Server Wide Settings display opens.
- 2 On the **General** tab select the **Use Enterprise Model hierarchy when OPC clients browse into EPKS address space** check box.
Clear the check box to use the asset-point model.

OPC-accessible point parameters

The following tables list the parameters for each type of point that can be accessed via the Experion OPC Data Access Server. The tables also specify each parameter's OPC type, access type and whether it is enumerated.

Status point parameters

Parameter	OPC type	OPC access	Enumerated?
PV	VT_I4		Yes
Mode	VT_I4		Yes
EUHI	VT_I2		
EULO	VT_I2		
OP	VT_I4		Yes
Area	VT_I2	Read-only	Yes
Point ID	VT_BSTR	Read-only	
Description	VT_BSTR		
LastProcessedDate	VT_I2		
LastProcessedTime	VT_I2		
OnScan	VT_BOOL		
AlarmValue	VT_I4	Read-only	Yes
ControlLevel	VT_I2		
AlarmDisabled	VT_BOOL		
PVInError	VT_BOOL	Read-only	
ModeInError	VT_BOOL	Read-only	
OutputInError	VT_BOOL	Read-only	
State0Descriptor	VT_BSTR		
State1Descriptor	VT_BSTR		
State2Descriptor	VT_BSTR		
State3Descriptor	VT_BSTR		
State4Descriptor	VT_BSTR		
State5Descriptor	VT_BSTR		
State6Descriptor	VT_BSTR		
State7Descriptor	VT_BSTR		
TargetPVforOPState0	VT_I4	Read-only	Yes
TargetPVforOPState1	VT_I4	Read-only	Yes

Parameter	OPC type	OPC access	Enumerated?
TargetPVforOPState2	VT_I4	Read-only	Yes
TargetPVforOPState3	VT_I4	Read-only	Yes
EnterToZone	VT_I2		
InputStateforOutputState3	VT_I4	Read-only	Yes
PVAlgoNumber	VT_I2	Read-only	
PVAlgoBlock	VT_I2	Read-only	
ActionAlgoNumber	VT_I2	Read-only	
ActionAlgoBlock	VT_I2	Read-only	
UnackAlarmExists	VT_BOOL		
AlarmPriority	VT_I4		Yes
ControlFailAlarmPriority	VT_I4		Yes
State0AlarmPriority	VT_I4		Yes
State1AlarmPriority	VT_I4		Yes
State2AlarmPriority	VT_I4		Yes
State3AlarmPriority	VT_I4		Yes
State4AlarmPriority	VT_I4		Yes
State5AlarmPriority	VT_I4		Yes
State6AlarmPriority	VT_I4		Yes
State7AlarmPriority	VT_I4		Yes
DefaultAlarmSubPriority	VT_I2		
ControlFailAlarmSubPriority	VT_I2		
State0AlarmSubPriority	VT_I2		
State1AlarmSubPriority	VT_I2		
State2AlarmSubPriority	VT_I2		
State3AlarmSubPriority	VT_I2		
State4AlarmSubPriority	VT_I2		
State5AlarmSubPriority	VT_I2		
State6AlarmSubPriority	VT_I2		
State7AlarmSubPriority	VT_I2		
AssociatedDisplay	VT_BSTR		
AssociatedDisplayDefault	VT_BSTR		
InstructionDisplay	VT_BSTR		
InstructionDisplayDefault	VT_BSTR		
AlarmMessageIndex	VT_I2		

Parameter	OPC type	OPC access	Enumerated?
REALARM	VT_I2		
PVExternalChangeAlarmEnable	VT_BOOL		
MDEternalChangeAlarmEnable	VT_BOOL		
OPEternalChangeAlarmEnable	VT_BOOL		
SPEternalChangeAlarmEnable	VT_I2		
State0AlarmEnabled	VT_BOOL		
State1AlarmEnabled	VT_BOOL		
State2AlarmEnabled	VT_BOOL		
State3AlarmEnabled	VT_BOOL		
State4AlarmEnabled	VT_BOOL		
State5AlarmEnabled	VT_BOOL		
State6AlarmEnabled	VT_BOOL		
State7AlarmEnabled	VT_BOOL		
NumberOfInputStates	VT_I2	Read-only	
NumberOfOutputStates	VT_I2	Read-only	
NORMALMODE	VT_I4		
PulseWidthSecs	VT_I4		Yes
OPREVERSE	VT_BOOL		
ControlConfirmRequired	VT_BOOL		
ControlTimeout	VT_I4		Yes
AlarmDeadbandPercent	VT_I4		Yes
PvSource	VT_BSTR		
MdSource	VT_BSTR		
OpSource	VT_BSTR		
AckDestination	VT_BSTR		
MdDestination	VT_BSTR		
OpDestination	VT_BSTR		
PvPeriod	VT_I2		
MdPeriod	VT_I2		
OpPeriod	VT_I2		
PvController	VT_I2		
MdController	VT_I2		
OpController	VT_I2		
CreateTime	VT_R4		

Parameter	OPC type	OPC access	Enumerated?
AlarmPriority	VT_I4		
AlarmSubPriority	VT_I2		
PointDetailDisplayDefault	VT_BSTR		
GroupDetailDisplayDefault	VT_BSTR		
PVAlgoExists	VT_BOOL	Read-only	
ActionAlgoExists	VT_BOOL	Read-only	
PointInAlarm	VT_BOOL	Read-only	
State0InAlarm	VT_BOOL	Read-only	
State1InAlarm	VT_BOOL	Read-only	
State2InAlarm	VT_BOOL	Read-only	
State3InAlarm	VT_BOOL	Read-only	
State4InAlarm	VT_BOOL	Read-only	
State5InAlarm	VT_BOOL	Read-only	
State6InAlarm	VT_BOOL	Read-only	
State7InAlarm	VT_BOOL	Read-only	
ModeCheckDisabled	VT_BOOL		

Analog point parameters

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
PV	VT_R8		
Mode	VT_R8		Yes
OP	VT_R4		
SP	VT_R4		
A1	VT_R4		
A2	VT_R4		
A3	VT_R4		
A4	VT_R4		
EULO	VT_R8	Read-only	
EUHI	VT_R8	Read-only	
AlarmLimit1	VT_R4		
AlarmLimit2	VT_R4		
AlarmLimit3	VT_R4		
AlarmLimit4	VT_R4		

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
AlarmType1	VT_I4		Yes
AlarmType2	VT_I4		Yes
AlarmType3	VT_I4		Yes
AlarmType4	VT_I4		Yes
Area	VT_I2	Read-only	Yes
SetPointLowLimit	VT_R4		
SetPointHighLimit	VT_R4		
OutputLowLimit	VT_R4		
OutputHighLimit	VT_R4		
Point ID	VT_BSTR	Read-only	
Description	VT_BSTR	Read-only	
LastProcessedDate	VT_I2		
LastProcessedTime	VT_R2		
OnScan	VT_BOOL		
AlarmValue	VT_I4	Read-only	Yes
ControlLevel	VT_I2		
AlarmDisabled	VT_BOOL		
PVInError	VT_BOOL	Read-only	
ModeInError	VT_BOOL	Read-only	
OutputInError	VT_BOOL	Read-only	
SetPointInError	VT_BOOL	Read-only	
A1InError	VT_BOOL	Read-only	
A2InError	VT_BOOL	Read-only	
A3InError	VT_BOOL	Read-only	
A4InError	VT_BOOL	Read-only	
Units	VT_BSTR		
Units1	VT_BSTR		
Units2	VT_BSTR		
Units3	VT_BSTR		
Units4	VT_BSTR		
Units5	VT_BSTR		
Units6	VT_BSTR		
Units7	VT_BSTR		
PVAlgoNumber	VT_I2	Read-only	

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
PVAlgoBlock	VT_I2	Read-only	
ActionAlgoNumber	VT_I2	Read-only	
ActionAlgoBlock	VT_I2	Read-only	
UnackAlarmExists	VT_BOOL		
UnreasonableAlarmPriority	VT_I4		
ControlFailAlarmPriority	VT_I4		
Alarm1Priority	VT_I4		Yes
Alarm2Priority	VT_I4		Yes
Alarm3Priority	VT_I4		Yes
Alarm4Priority	VT_I4		Yes
Alarm5Priority	VT_I4		
Alarm6Priority	VT_I4		
Alarm7Priority	VT_I4		
Alarm8Priority	VT_I4		
UnreasonableAlarmSubPriority	VT_I2		
ControlFailAlarmSubPriority	VT_I2		
Alarm1SubPriority	VT_I4		
Alarm2SubPriority	VT_I4		
Alarm3SubPriority	VT_I4		
Alarm4SubPriority	VT_I4		
Alarm5SubPriority	VT_I4		
Alarm6SubPriority	VT_I4		
Alarm7SubPriority	VT_I4		
Alarm8SubPriority	VT_I4		
AssociatedDisplay	VT_BSTR		
AssociatedDisplayDefault	VT_BSTR		
InstructionDisplay	VT_BSTR		
InstructionDisplayDefault	VT_BSTR		
AlarmMessageIndex	VT_I2		
PVExternalChangeAlarmEnable	VT_BOOL		
MDEternalChangeAlarmEnable	VT_BOOL		
OPEternalChangeAlarmEnable	VT_BOOL		
SPEternalChangeAlarmEnable	VT_BOOL		
NormalMode	VT_I4		Yes

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
OPReverse	VT_BOOL		
ControlConfirmRequired	VT_BOOL		
ControlTimeout	VT_I4		Yes
DriftDeadbandPercent	VT_I4		Yes
AlarmDeadbandPercent	VT_I4		Yes
ControlDeadbandPercent	VT_I4		Yes
PVClampingEnabled	VT_BOOL		
PvSource	VT_BSTR		
MdSource	VT_BSTR		
OpSource	VT_BSTR		
SpSource	VT_BSTR		
A1Source	VT_BSTR		
A2Source	VT_BSTR		
A3Source	VT_BSTR		
A4Source	VT_BSTR		
AckDestination	VT_BSTR		
MdDestination	VT_BSTR		
OpDestination	VT_BSTR		
SpDestination	VT_BSTR		
A1Destination	VT_BSTR		
A2Destination	VT_BSTR		
A3Destination	VT_BSTR		
A4Destination	VT_BSTR		
PvPeriod	VT_I2		
MdPeriod	VT_I2		
OpPeriod	VT_I2		
SpPeriod	VT_I2		
A1Period	VT_I2		
A2Period	VT_I2		
A3Period	VT_I2		
A4Period	VT_I2		
PvController	VT_I2		
MdController	VT_I2		
OpController	VT_I2		

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
SpController	VT_I2		
A1Controller	VT_I2		
A2Controller	VT_I2		
A3Controller	VT_I2		
A4Controller	VT_I2		
CreateTime	VT_R4		
AlarmLimit5	VT_R4		
AlarmLimit6	VT_R4		
AlarmLimit7	VT_R4		
AlarmLimit8	VT_R4		
AlarmType5	VT_I4		
AlarmType6	VT_I4		
AlarmType7	VT_I4		
AlarmType8	VT_I4		
AlarmPriority	VT_I4		
AlarmSubPriority	VT_I2		
PointDetailDisplayDefault	VT_BSTR	Read-only	
GroupDetailDisplayDefault	VT_BSTR	Read-only	
PVAlgoExists	VT_BOOL	Read-only	
ActionAlgoExists	VT_BOOL	Read-only	
PointInAlarm	VT_BOOL	Read-only	
InRateOfChangeAlarm	VT_BOOL	Read-only	
InDeviationLowAlarm	VT_BOOL	Read-only	
InDeviationHighAlarm	VT_BOOL	Read-only	
InTransmitterLowAlarm	VT_BOOL	Read-only	
InTransmitterHighAlarm	VT_BOOL	Read-only	
InLowAlarm	VT_BOOL	Read-only	
InHighAlarm	VT_BOOL	Read-only	
InLowLowAlarm	VT_BOOL	Read-only	
InHighHighAlarm	VT_BOOL	Read-only	
InUnreasonablyLowAlarm	VT_BOOL	Read-only	
InUnreasonablyHighAlarm	VT_BOOL	Read-only	
A1ExternalChangeAlarmEnable	VT_BOOL		
A2ExternalChangeAlarmEnable	VT_BOOL		

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
A3ExternalChangeAlarmEnable	VT_BOOL		
A4ExternalChangeAlarmEnable	VT_BOOL		
ModeCheckingDisabled	VT_BOOL		
A1AssociatedParameter	VT_I4	Read-only	Yes
A2AssociatedParameter	VT_I4	Read-only	Yes
A3AssociatedParameter	VT_I4	Read-only	Yes
A4AssociatedParameter	VT_I4	Read-only	Yes

Accumulator point parameters

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
PV	VT_R8		
Mode	VT_I4		
EUHI	VT_R8	Read-only	
EULO	VT_R8		
AlarmLimit1	VT_R4		
AlarmLimit2	VT_R4		
AlarmLimit3	VT_R4		
AlarmLimit4	VT_R4		
AlarmType1	VT_I4		Yes
AlarmType2	VT_I4		Yes
AlarmType3	VT_I4		Yes
AlarmType4	VT_I4		Yes
RollOver	VT_I4		
MeterFactor	VT_R4		
ScaleFactor	VT_R4		
RawPV	VT_I4		
Area	VT_I2	Read-only	Yes
PointID	VT_BSTR	Read-only	
Description	VT_BSTR		
LastProcessedDate	VT_I2		
LastProcessedTime	VT_R2		
OnScan	VT_BOOL		
AlarmValue	VT_I4	Read-only	Yes

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
AlarmDisabled	VT_BOOL		
PVInError	VT_BOOL	Read-only	
ModeInError	VT_I2		
Units	VT_BSTR		
PVAlgoNumber	VT_I2	Read-only	
PVAlgoBlock	VT_I2	Read-only	
ActionAlgoNumber	VT_I2	Read-only	
ActionAlgoBlock	VT_I2	Read-only	
UnackAlarmExists	VT_BOOL		
DefaultAlarmSubPriority	VT_I4		
ControlFailAlarmPriority	VT_I4		
Alarm1Priority	VT_I4		Yes
Alarm2Priority	VT_I4		Yes
Alarm3Priority	VT_I4		Yes
Alarm4Priority	VT_I4		Yes
Alarm5Priority	VT_I4		
Alarm6Priority	VT_I4		
Alarm7Priority	VT_I4		
Alarm8Priority	VT_I4		
DefaultAlarmSubPriority	VT_I2		
DefaultControlAlarmSubPriority	VT_I2		
Alarm1SubPriority	VT_I2		
Alarm2SubPriority	VT_I2		
Alarm3SubPriority	VT_I2		
Alarm4SubPriority	VT_I2		
Alarm5SubPriority	VT_I2		
Alarm6SubPriority	VT_I2		
Alarm7SubPriority	VT_I2		
Alarm8SubPriority	VT_I2		
AssociatedDisplay	VT_BSTR		
AssociatedDisplayDefault	VT_BSTR		
InstructionDisplay	VT_BSTR		
InstructionDisplayDefault	VT_BSTR		
AlarmMessageIndex	VT_I2		

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
ControlConfirmRequired	VT_BOOL		
AlarmDeadbandPercent	VT_I4		Yes
PvSource	VT_BSTR		
MdSource	VT_BSTR		
OpSource	VT_BSTR		
SpSource	VT_BSTR		
A1Source	VT_BSTR		
A2Source	VT_BSTR		
A3Source	VT_BSTR		
A4Source	VT_BSTR		
AckDestination	VT_BSTR		
MdDestination	VT_BSTR		
OpDestination	VT_BSTR		
SpDestination	VT_BSTR		
A1Destination	VT_BSTR		
A2Destination	VT_BSTR		
A3Destination	VT_BSTR		
A4Destination	VT_BSTR		
PvPeriod	VT_I2		
MdPeriod	VT_I2		
OpPeriod	VT_I2		
SpPeriod	VT_I2		
A1Period	VT_I2		
A2Period	VT_I2		
A3Period	VT_I2		
A4Period	VT_I2		
PvController	VT_I2		
MdController	VT_I2		
OpController	VT_I2		
SpController	VT_I2		
A1Controller	VT_I2		
A2Controller	VT_I2		
A3Controller	VT_I2		
A4Controller	VT_I2		

OPC Data Access Param Name	OPC Type	OPC Access	Enumerated?
CreateTime	VT_R4		
AlarmLimit4	VT_R4		
AlarmLimit6	VT_R4		
AlarmLimit7	VT_R4		
AlarmLimit7	VT_R4		
AlarmLimit8	VT_R4		
AlarmType5	VT_I4		
AlarmType6	VT_I4		
AlarmType7	VT_I4		
AlarmType8	VT_I4		
AlarmPriority	VT_I4		
AlarmSubPriority	VT_I2		
PointDetailDisplayDefault	VT_BSTR		
GroupDetailDisplayDefault	VT_BSTR		
PVAlgoExists	VT_BOOL	Read-only	
ActionAlgoExists	VT_BOOL	Read-only	
PointInAlarm	VT_BOOL	Read-only	
InRateOfChangeAlarm	VT_BOOL	Read-only	
InHighAlarm	VT_BOOL	Read-only	
InHighHighAlarm	VT_BOOL		

Flexible point parameters

The following parameters are mandatory for flexible points.

OPC Data Access Param Name	OPC type	OPC access	Enumerated?
Name	VT-BSTR	Read-only	
Area	VT_I2	Read-only	Yes
Description	VT-BSTR	Read-only	
PointDetailDisplay	VT-BSTR		
GroupDetailDisplay	VT-BSTR		
AssociatedDisplay	VT-BSTR		
Control Level	VT-I2		
InstructionDisplay	VT-BSTR		

Process parameters

The following parameters apply to all process points.

OPC Data Access Param Name	OPC type	OPC access	Enumerated?
Area	VT_I2	Read-only	Yes
PointID	VT_BSTR	Read-only	
Description	VT_BSTR		
AlarmValue	VT_I4	Read-only	Yes
ControlLevel	VT_I2		
UnackAlarmExists	VT_BOOL	Read-only	
AssociatedDisplay	VT_BSTR		
AssociatedDisplayDefault	VT_BSTR		
InstructionDisplay	VT_BSTR		
InstructionDisplayDefault	VT_BSTR		
AlarmMessageIndex	VT_I2		
PointDetailDisplay	VT_BSTR		
PointDetailDisplayDisplay	VT_BSTR		
GroupDetailDisplayDefault	VT_BSTR		
GroupDetailDisplay	VT_BSTR		

Error codes and qualities

The following error codes and qualities can be returned by the Experion OPC Data Access Server.

Read function error codes and qualities

Function HRESULT	Item HRESULT	Quality value	Condition
S_FALSE	0xE00483FD (for all items)	OPC_QUALITY_BAD OPC_QUALITY_OUT_OF_SERVICE	Host backup
S_FALSE	0xE00483FC (for all items)	OPC_QUALITY_BAD OPC_QUALITY_LAST_KNOWN	Host not running (but not backup)
S_FALSE	0xE0048231	OPC_QUALITY_BAD OPC_QUALITY_CONFIG_ERROR	Invalid point number
S_FALSE	0xE0048232	OPC_QUALITY_BAD OPC_QUALITY_CONFIG_ERROR	Invalid parameter number
S_FALSE	0xE004xxxx xxxx = status	0x0000 (non-specific)	Any other error status

Write function error codes and qualities

Function HRESULT	Item HRESULT	Condition
S_FALSE	0xE00483FD (for all items)	Host backup.
S_FALSE	0xE00483FC (for all items)	Host not running (but not backup).
S_FALSE	0xE0048222	Point not active.
S_FALSE	0xE0048223	Parameter error
S_FALSE	0xE0048224	Control inhibited
S_FALSE	0xE0048227	RTU disabled.
S_FALSE	0xE0048228	Channel disabled.
S_FALSE	0xE0048229	Illegal mode for control.
S_FALSE	0xE004822A	Value error.
S_FALSE	0xE0048212	Point on scan.
S_FALSE	0xE004xxxx xxxx = status	Any other error status.

Configuring the Experion OPC Historical Data Access Server

This section describes the interfaces and related methods supported by the Experion OPC Historical Data Access server.

Prerequisites

- You have installed and set up the third-party OPC client components as described in the *Supplementary Installation Tasks Guide*

Notes

- For point parameters assigned to multiple history types, fast, standard and extended, the Experion OPC Historical Data Access server returns historical data from the fastest history collection interval.
- For point parameters assigned to both fast and standard history and when no history archiving is configured for fast history, the Experion OPC Historical Data Access server returns historical data from the history collection interval that best satisfies the request from the OPC client. For example, a fast history file covers three days and a standard history file covers ten days. For a request from an OPC client with a start time of now minus eight days, the Experion OPC Historical Data Access server returns data from the standard history file. When history archiving is configured for fast history, the Experion OPC Historical Data Access server returns data from the fast history only.
- If the fast history rate has been set to one second and fast history archiving has not been configured then most queries to the OPC HDA server will return standard history by default. This is because by default the fast history file holds only 12 minutes of one second history data online. To rectify this, enable fast history archiving and configure it to retain the period of one second history online that is needed by OPC HDA clients.

Supported interfaces and methods

The following table lists the interfaces and methods supported by the Experion OPC Historical Data Access server.

Interface	Methods
IOPCHDA_Server	GetItemAttributes GetAggregates GetHistorianStatus GetItemHandles ReleaseItemHandles ValidateItemIDs CreateBrowse
IOPCHDS_Browser	GetEnum ChangeBrowsePosition GetItemID GetBranchPosition
IOPCHDA_SyncRead	ReadRaw ReadAttribute ReadProcessed
IOPCHDA_AsyncRead	ReadRaw AdviseRaw ReadAttribute ReadProcessed AdviseProcessed Cancel
IOPCHDA_Playback	ReadRawWithUpdate ReadProcessedWithUpdate Cancel
IOPCHDA_SyncUpdate	QueryCapabilities Insert

Supported aggregates

The following aggregates are supported by the Experion OPC Historical Data Access server:

- OPCHDA_INTERPOLATIVE
- OPCHDA_AVERAGE
- OPCHDA_MAXIMUM
- OPCHDA_MINIMUM

Configuring the Experion OPC Alarm and Event Server

This section describes the mapping of Experion alarm/event properties to appropriate OPC notification properties so that they are correctly processed by an OPC notification client.

The Experion OPC Alarm and Event Server supports the OPC Alarm and Events Specification Version 1.02, and the OPC Common Definitions and Interfaces specification Version 1.0.

Notes

- When an OPC client calls the `IOPCEventServer::QueryEventAttributes` method, it will get the relevant attribute details for each category. However, for individual event instances, if some attributes for the category are not applicable, those attributes are set to `VT_NULL`, as described by the OPC AE Standard.
- The ProgId of the Experion OPC Data Access Server is `HWHsc.OPCServer`.
- On your OPC client, you can create subscription filters to receive alarms for specific assets. If you create a filter for a top level asset which contains lower level assets, you only receive alarms for the specified asset, you do not receive alarms for any lower level assets. For example, if you have an asset hierarchy, `Assets/Precipitation1/Train1` and you create a filter for `Precipitation1`, you receive alarms only for `Precipitation1`, not alarms for `Train1`. To receive alarms for `Train1`, you must create a separate filter.

Categories

Category	OPC Event Type
Process Alarm	Conditional
System Alarm	Conditional
Info Message	Conditional
Operator Change	Tracking
System Change	Tracking
SOE	Simple
Confirmable Message	Conditional
Process Event	Simple
Batch Event	Simple
Process Alert	Conditional
Simple Alert	Simple

Attributes

The following table lists Experion alarm and event attributes in alphabetical order.

Attribute	Attribute Type
AckComment	VT_BSTR
Action	VT_BSTR
Alert accessibility	VT_I2
Areas	VT_ARRAY VT_BSTR
Author	VT_BSTR
Classification	VT_BSTR
Comment	VT_BSTR
Condition	VT_BSTR
Data access item	VT_BSTR
Field Time	VT_DATE
Limit	VT_R8
Link 1 Type	VT_I2
Link 2 Type	VT_I2
Link 3 Type	VT_I2
Link1	VT_BSTR
Link2	VT_BSTR
Link3	VT_BSTR
Location full name	VT_BSTR
Location tag name	VT_BSTR
Parameter	VT_BSTR
Previous value	VT_BYREF VT_VARIANT
Reason	VT_BSTR
Signature 2 Level	VT_I2
Signature Meaning	VT_BSTR
Signature 2 Meaning	VT_BSTR
SourceEntityName	VT_BSTR
Station	VT_BSTR
Units	VT_BSTR
Value	VT_BYREF VT_VARIANT

Configuring Experion OPC Integrator

This section describes recommended practices for configuring how to set up the Experion OPC Integrator so that it can exchange data with a third-party OPC server.

Recommended practices for configuring Experion OPC Integrator

The Experion OPC Integrator option offers considerable flexibility. Therefore care is needed when configuring Experion OPC Integrator in order to avoid placing undesirable load on the communications subsystems of target controllers. This section describes recommended practices for configuration of an Experion OPC Integrator solution.

Perform writes to local points rather than remote points via DSA

Experion OPC Integrator groups should be configured on the server where the writes will occur. If one or more items in a destination group are part of a controller that is connected to a different Experion server, the writes to that controller will use the DSA subsystem to transfer the data between servers; this may place an unnecessary load on the DSA subsystem. It is recommended that items in OPC Integrator destination groups are part of the same server as OPC Integrator itself.

Configure Transfer Rate that do not exceed communication throughput limits

Experion OPC Integrator data transfers are asynchronous using OPC callbacks such that items are only transferred when they change at the source location. Experion OPC Integrator uses the group transfer rate to check what items have changed inside the transfer rate period. The changed items are then transferred to the destination items. The asynchronous nature of the transfers means that the load that the Experion OPC Integrator transfers put on the system depends on the rate of change of the source items. This needs to be taken into consideration when trying to determine the load that Experion OPC Integrator puts on the system. Analog parameters usually change more frequently than digital parameters but digital parameters may have bursts of many parameter changes at once.

It is important to determine the sustained load that is put on the system plus being able to cope with small bursts of increased load. The following sections provide some help and guidance on how this can be determined.

Using bidirectional groups when there is a need for two way data transfer

Bidirectional groups are specifically designed for scenarios where value changes are likely to occur in both the source item and destination item, for example, in a supervisory system migration project where operator changes may occur from both systems. To avoid creating two different OPC Integrator groups to transfer data in both directions and losing changes or overwriting changes, there is a special group called bi-directional group. In bi-directional groups, changes are transferred in both directions, initiated by a value change in the source and destination. One of the groups (source or destination) is nominated master to

prevent continuous writes in case changes occur in both source and destination at the same time or within a very short time period.

Use Redirection Manager when transferring large number of items between redundant third-party OPC servers

In cases where there are redundant remote OPC Servers, Experion OPC Integrator can manage the redundancy itself or it can use the Honeywell Redirection Manager (RDM) to manage the redundancy. If Experion OPC Integrator manages the redundancy additional time is taken by re-adding the OPC transfer groups at approximately 100 items per second. This additional time needs to be included in the total failover time.

It is therefore recommended to use RDM when transferring large numbers of items, for example, more than 500 items.

Performance considerations

OPC Integrator uses asynchronous data transfer, which means that it is very efficient in transferring data. However, Experion OPC Integrator has the potential of putting undesirable load onto the system if used inappropriately. This section describes factors to be aware of when configuring OPC Integrator.

When using the Experion OPC server as the destination

Data is written to standard points as single items. However, data is written to process points (Process Controller points) using lists, which is a more efficient technique and allows a higher data transfer rate.

The following table specifies the recommended maximum transfer rates. (Note that only changed data is written.)

Point type	Recommended maximum transfer rate
Process points	100 parameters per second across all groups. For example, 5 groups with a maximum of 20 changes per group per second.
Standard points	2 parameters per second per controller.
Database points	Several thousand parameters per second.

Write retry items and diagnostic interval

Diagnostic interval is used to periodically check the status of the group, including performing diagnostic checks on the configured OPC servers.

During each diagnostic interval, OPC Integrator attempts to write the values of any items that previously failed to write. OPC Integrator stops subsequent write attempts for the item when its value changes on the source OPC server or the write retry succeeds or when the group is disabled. Poorly configured groups or groups that experience a large number of write failures occur, combined with a low value for the diagnostic interval, for example, five seconds, can degrade the performance of the OPC Integrator. It is recommended to use diagnostic intervals that are as slow as possible while maintaining an acceptable frequency for the diagnostic checks.

When using a third-party OPC server as the destination

The limitation will depend on the implementation of the third-party OPC Server. Honeywell recommends that you consult the third-party documentation to find out what the limits are.

Safety or process critical data

Although Experion OPC Integrator is designed for robust data transfers and support of redundancy, Experion OPC Integrator is not recommended for transfer of safety or process critical data. Transfer of critical data should be achieved by direct peer to peer communication between controllers and not through a server based process.

Performance and system load dependent on underlying transport mechanism

Experion OPC Integrator is typically used as a transfer mechanism between controllers. The primary limiting factor for Experion OPC Integrator transfers is dependant on the underlying communications subsystem of the controller or third-party OPC Server. In many cases throughput limitations are determined by the available bandwidth of the physical connection to the controller. This bandwidth is also consumed by other clients that may also be communicating with the controller or third-party OPC server. When considering loading and transfer limitations, the sum of the transfers from the Experion OPC Integrator and other clients should be kept within the communication specification limits of the controller or third-party OPC server. For throughput limits, see Recommended Throughput Limits.

Consider the total items in all groups

When determining the load that Experion OPC Integrator adds to the system, and in particular to the controller interfaces, all items that write to a single controller from each Experion OPC Integrator transfer group should be considered. For instance when calculating the additional load on a channel, add up all items from each Experion OPC Integrator group that write to that controller, taking into account the groups transfer rate and rate of change of the source parameter.

Experion OPC Integrator redundancy and failover considerations

Experion OPC Integrator group configuration is stored in SQL Server. This configuration is duplicated in a series of text files stored on the server. Every time a change is made to the database, the content of the database is exported to these text files. These files are then sent across to the backup server as part of the Experion redundancy.

When the server fails over, the Experion OPC Integrator service on the backup server is restarted, the database is populated from the text files, any currently enabled groups are recreated on the OPC servers and transfers are subsequently activated. This process results in a temporary interruption of data transfers. The length of the interruption is dependant on the size of the database, the number of enabled groups, and the number of items within each of those groups.

Recommended read throughput limits

For Process Controllers (C300 and C200), ACE, FIM and TPS, OPC Integrator uses subscription mechanism to acquire data from controllers. The total from OPC-Integrator load and other clients, such as displays, should not exceed the communications capacity of the subsystem. For example, if the limit for a C300 controller is 1500 parameters/second, then the total load from OPC Integrator and other clients should not exceed this limit. Note that subscriptions to the same parameter by multiple clients result in only a single request to the subsystem.

For SCADA interfaces, such as FSC, OPC Integrator acquires data from the Experion server database. The Experion server database supports very high throughput and would typically not be a limiting factor.

Recommended write throughput limits

Write throughput is more limited than read throughput. The following guidelines indicate recommended maximums. Note that the total OPCIntegrator writes plus writes from other clients and applications should not exceed the write throughput specification for the controller.

Controller	Limit
Process controller (C300 or C200)	Up to a maximum of 100 parameters per second across all OPC Integrator groups, for example, 5 groups with a maximum of 20 changes per group per second.
FSC Ethernet connected controller	20 writes per second per controller
FSC Serial connected controller	2 writes per second per controller

Tuning parameters

You tune the deadband, transfer rate, and refresh interval parameters to influence the rate that data transfers take place and therefore the load that Experion OPC Integrator imposes on the system.

Deadband

You can set the deadband on a group-by-group basis to tune the amount of data that is transferred. The deadband represents the percent change in item values configured for a group that will cause the item value to be updated on the OPC server. That is, the lower the deadband, the more data that will be transferred.

Valid values for deadband are 0 through 100. A deadband outside this range will generate an error (Invalid Argument). A deadband value of 0 (default) will cause

all data changes to be written. Non-zero deadband values will cause item writes when:

$$(\text{Current Item Value} - \text{Cached Value}) > ((\text{Deadband}/100) * (\text{EU High} - \text{EU Low}))$$



Attention

- Deadband only applies to analog data items (as it uses configured EU High and EU Low values).
 - Deadband functionality has not been implemented for the Experion OPC server. Configuring a deadband value for a group will have no bearing on the data being transferred for that group.
-

Transfer rate

OPC Integrator data transfers are asynchronous using OPC callbacks so that items are only transferred when they change at the source location. OPC Integrator uses the group transfer rate to check what items have changed inside the transfer rate period - the changed items are then transferred to the destination items. The transfer rate will be the fastest possible rate at which an item will be transferred. The transfer rate is configured on a group by group basis. The higher the transfer rate the more items will be transferred in one cycle but with a larger interval between cycles. A low transfer rate (for example, less than 2 seconds) will detect changes in the source items more frequently but will increase the load on the overall system.

Valid transfer rates depend on the OPC Server. It is recommended to use transfer rates that are as slow as possible while meeting the needs of the application in order to minimize load on the system. Use different groups with different transfer rates where some data needs to be transferred at a faster rate.

Refresh interval

Refresh interval is used to update all destination items in a group on a regular, low frequency interval to ensure transfers take place at least at this interval, regardless of source item changes. At each refresh interval, all data within a group is transferred from the source to the destination.

Because every item is transferred at this interval the additional load can be much higher than the asynchronous OPC callback transfers. The refresh interval should therefore be set to a high value, for example, 600 seconds. Refresh interval and transfer rate should be used in such a way to ensure no data loss while still maintaining a reasonable load on the system.



Attention

Some remote OPC Servers use a deadband to determine when a source item is considered changed. This can also be used to tune the overall system load. See the vendor's OPC Server documentation for details.

Start delay

You can configure a start delay so that there is a delay before groups are created on the OPC servers. The start delay reduces the load on the OPC server on startup. For example, if there are a number of OPC clients configured whose data is considered more critical than that configured in OPC Integrator, group startup can be delayed to give priority to the OPC clients.

In general, you only need to change this setting if you experience performance issues. For more information see the *Troubleshooting Guide*.

Timeout

You can configure a timeout for all local and remote OPC COM calls to prevent OPC Integrator becoming unresponsive when an OPC server is not responding. This includes OPC server connections, group and item load and unload, read and write operations, status checks, and refresh operations.

In general, you only need to change this setting if you experience performance issues. For more information see the *Troubleshooting Guide*.

Example scenario

OPC Integrator facilitates data transfer between a C300 controller and an ethernet connected FSC controller, both connected to the same Experion server.

Maximum writes to FSC controller is 20 parameters per second and maximum writes to C300 controllers is 100 parameters per second. Items are transferred between C300 and FSC in both directions.

The OPC Integrator group configuration is as follows:

Group 1		Group 2	
Transfer rate: 5 seconds		Transfer rate: 5 seconds	
Refresh interval: 600 seconds		Refresh interval: 600 seconds	
Source	Destination	Source	Destination
C300-item1	FSC-item1	FSC-item101	C300-item101
C300-item2	FSC-item2	FSC-item102	C300-item102
C300-item3	FSC-item3	FSC-item103	C300-item103
C300-item4	FSC-item4	FSC-item104	C300-item104
C300-item5	FSC-item5	FSC-item105	C300-item105
...	...	...	...
C300-item50	FSC-item50	FSC-item150	C300-item150
Total 50 items		Total 50 items	

OPC Integrator transfers only occur when the source value changes. This means the additional load that OPC Integrator puts on the interface channel depends on how often the value of the source parameter changes.

Depending on the average rate of change the additional load would be:

- 1 20% of source parameters in 5 second interval (group transfer rate)
Additional load on C300 channel: 2 items written per second / 2% of max throughput
Additional load on FSC channel: 2 items written per second / 10% of max throughput
- 2 50% of source parameters in 5 second interval (group transfer rate)
Additional load on C300 channel: 5 items written per second / 5% of max throughput
Additional load on FSC channel: 5 items written per second / 25% of max throughput
- 3 100% of source parameters in 5 second interval (group transfer rate)
Additional load on C300 channel: 10 item written per second / 10% of max throughput
Additional load on FSC channel: 10 item written per second / 50% of max throughput

Bidirectional data transfer

Default OPC Integrator group behavior is to transfer item data from the source server to the destination server. When a group is configured as bidirectional, data is transferred in both directions.

Bidirectional groups have a “publish-subscribe” relationship between the two servers configured for data transfer. When data changes occur on the publishing OPC server, data is written from the publishing OPC server to the subscribing OPC server. When data changes occur on the subscribing OPC server, data is written from the subscribing OPC server to the publishing OPC server except under the following conditions:

- Value being written is equal to the current value on the publishing OPC server
- The publishing OPC server has not yet successfully written a value to the subscribing OPC server
- Data transfer is a result of a periodic group refresh.

Data on the publishing OPC server is considered more critical than the data on the subscribing OPC server. This is to prevent:

- Data from the subscribing server overwriting data on the publishing server before the publishing server has finished writing to the subscribing server.
- Data changes bouncing back and forth between the publishing and subscribing servers.

Configuration tasks

Prerequisites

- You have installed and set up the third-party OPC server components as described in the *Supplementary Installation Tasks Guide*.

Considerations

- For an introduction to OPC and its terminology, see “About OPC” on page 704.
- For details about building items that access Experion data, see “Accessing Experion data” on page 721.

Task	Go to	Done
Configure alarms	page 754	
Configure groups	page 755	
Enable groups	page 761	

Configuring OPC Integrator alarms

To configure OPC Integrator alarms:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure OPC** task.
The list of OPC Integrator Groups display appears in the System Display tab in Configuration Studio.
- 3 Click the **Alarm Settings** tab.
- 4 Configure alarm priorities as required.
- 5 Click **Commit** when you are satisfied with your configuration.

Alarm settings tab

Property	Description
Alarm	System alarm raised by OPC Integrator. For details on the types of alarms raised by OPC Integrator, see “OPC Integrator alarms and events” on page 764
Priority	The priority of the selected alarm. Alarm priority can be Urgent, High, Low, or Journal.
Commit	Commits changes to the database.
Cancel	Cancels any changes since the last successful commit action.

Configuring OPC groups

To configure a group:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure OPC** task.
The OPC Integrator Group configuration display appears in the System Display tab in Configuration Studio. Any previously configured groups are displayed in the group list.
- 3 Click **Add New Group** to create a new group.
- 4 Click the newly created group in the group list to call up the **Group Details** tab.
- 5 Configure the group as required.
For a description of the properties you can configure, see “Group Details tab” on page 755.
- 6 To configure the items in the group, click the Item List tab.
For a description of the item list properties, see “Item List tab” on page 758.
- 7 Click **Validate Group** to check your configuration.
If an error occurs which is applicable to the whole group, it is displayed in red text at the bottom of the display. If an error occurs for an item, an error message appears in the table opposite the item. Resolve any reported errors, and validate again.
- 8 Click **Commit Group** when you are satisfied with your configuration.

Results

When the group configuration is successfully committed, the group status display at the top right of the display is set to Disabled. To enable the group see “Enabling OPC Integrator groups” on page 761.

Group Details tab

Property/Button	Description
General	
Group ID	The group’s ID, which is used to identify the group in error/alarm messages. The number of items in this group is displayed next to the group ID.
Group Name	The group’s name. You must specify a name.

Property/Button	Description
Deadband	The deadband expressed as a percentage of full range. Item values that change by less than this deadband amount are not transferred. Note that this is an optional OPC server feature and has not been implemented on the Experion OPC Server.
Transfer Period	The source OPC server attempts to look for changed data at a rate faster than this interval. This interval defines the fastest rate at which data is written to the OPC destination server. You must specify a period.
Refresh Interval	All data in the group is transferred from the source OPC server to the destination OPC server at this interval (approximately) regardless of whether data has changed. Set to 0 (default) to disable this functionality.
Diagnostic Interval	The transfer group diagnostic interval (seconds), which is used as follows: • The time between checks for source and destination OPC server status. • The interval between group re-start attempts when a group fails. • The time between checks for data refresh. • The interval between write retries of values for items that failed to write.
Bidirectional	Transfer the data for configured items in this group in both directions. For more information, see “Bidirectional data transfer” on page 752.
Source	
This Experion PKS server Other OPC server	If the source of data for this group is the local Experion server, select This Experion PKS server . If it is another OPC server, select Other OPC server and complete the following details.
Server	This is either: • The name or IP address of the OPC server that is used as the source of data for this group. • The name or IP address of the preferred server of a redundant OPC server pair that is used as the source of data for this group. The OPC server must be registered on the OPC Integrator server.

Property/Button	Description
ProgID	The ProgID of this OPC server. This defaults to <code>HWHsc.OPCServer</code>, which is the ProgID of the Experion OPC Server. Click  to select an OPC server from the list of OPC servers that are registered on the computer.
Redundant	Select this if the source of data for this group is a redundant OPC Server pair.
Redundant Server Redundant ProgID	Only applicable if you have redundant OPC servers. The name or IP address, and the ProgID, of the backup server. The OPC Server must be registered on the OPC Integrator server.
Status Item	This is an item that is used to show the status of this group on the source server. Click  to browse the address space of the source server. For more information on the use of status items, see “Using status items” on page 766. For more information on using the browser, see “Browsing the source or destination” on page 759.
Destination	
All settings	The details of the destination of data for this group. (These are equivalent to the source settings described above).
Validate Group	Requests the OPC Integrator to validate the current working configuration for the group. The result of the validation is displayed in a message box. Any group-wide errors appear in the Group Details tab. Any item-specific errors appear in the Item List tab. After the group has been committed, the group must be enabled using the System Status display before any data transfer begins.
Commit Group	If the group is currently enabled, it is temporarily disabled, the new configuration is loaded and the group re-enabled. This function is only available if you have made changes to the group since the last commit, or if the group is new.
Delete Group	Deletes (after confirmation) and then disables and deletes the online copy of the group.

Property/Button	Description
Cancel Changes	If the group is new and has not been committed, this acts as if you clicked Delete Group. If the group has been committed and you have made changes since the last commit, this cancels (after confirmation) those changes and restores the configuration to the current online settings.

Item List tab

Items can be entered manually into the item list by clicking the required position in the list and typing the item name. Alternatively, the item browser can be used to add items to the list. For information on using the browser, see “Browsing the source or destination” on page 759.

Items can be removed from the list by selecting one or more rows and clicking Delete Items.

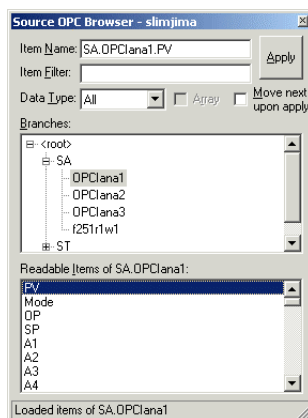
For details about the syntax used by an item that accesses Experion data, see “Accessing Experion data” on page 721. For details about accessing data on a third-party server, see the manufacturer’s documentation.

Property/Button	Description
Item ID	Unique number, supplied by the OPC Integrator, that represents the item pair. This property is read-only.
Source Item	The description of the source OPC item.
Destination Item	The description of the destination OPC item.
Source Type	The data type of the source OPC item, which is supplied by the OPC Integrator following validation. This property is read-only.
Destination Type	The data type of the destination OPC item, which is supplied by the OPC Integrator following validation. This property is read-only.
Error	Blank if the item was successfully validated. A description as to why the source or destination OPC item is invalid. This is supplied by the OPC Integrator when attempting to validate the item. This property is read-only. When viewing this tab from the System Status display, any transfer errors for individual items are displayed as well as trace data if tracing is enabled.

Property/Button	Description
Validate Group Commit Group Cancel Changes	Same as for the Group Details tab, except for the Delete Group button. You can only delete a group from the Group Details tab.
Delete Items	Deletes the selected items in the item grid.
Browse Source Browse Destination	These buttons open a dialog box that allows you browse for items on the source/destination OPC server. See “Browsing the source or destination” on page 759.
Import Items	Allows you to import item pair configurations from a text file. See “Importing items” on page 760.
Export Items	Allows you to export item pair configurations to a text file. See “Exporting items” on page 760.

Browsing the source or destination

If the source or destination OPC servers support browsing, you can click **Browse Source** or **Browse Destination** to open a Browse dialog box and browse the OPC source/destination server for OPC items.



Property	Description
Item Name	Fully qualified server item name. This property is populated when the required parameter is selected from the list of parameters.
Item Filter	Filter string for the parameters listed for the selected item. Filter only matches those parameters identical to the filter string

Property	Description
Data Type	Filters the list of parameters by data type
Array	Filters the list of parameters by array data types
Move next upon apply	When Apply is clicked, the focus of the item grid moves to the next row. A new row is created if required.
Branches	A hierarchical structure of items available on the selected server.
Items	List of available parameters for the selected item. When browsing the source server, the list shows all readable parameters. When browsing the destination server, the list shows all writable parameters.
Apply	Adds the selected item to the list.
Cancel	Closes the item browser.

Importing items

You can import item pair configurations from a text file. (Note that you should only perform this on the OPC Integrator server, not on a remote client.)

Imported items are appended to the existing item list.

The following example shows the required format (a tab separates the two columns).

```
SourceItem1  DestinationItem1
SourceItem2  DestinationItem2
.
.
SourceItemN  DestinationItemN
```

Exporting items

You can export item pair configurations to a text file. (Note that you should only perform this on the OPC Integrator server, not on a remote client.)

The format of the text file is the same as the import file.

Enabling OPC Integrator groups

Considerations

- When tracing is enabled, transferred values are written to the log file and also are shown on the Item Details tab.
- Data transfers occur only when a group is enabled.

To enable OPC Integrator groups:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure OPC** task.
- 3 Select the Enable check box for each group that you want to enabled.
- 4 Select the Trace check box for each group you want to trace.



Tip

To disable a group, clear the Enable check box for the group you want to disable.

Checking the status of OPC Integrator groups

To check the status of groups:

- 1 In the Configuration Explorer of Configuration Studio, click **System Interfaces**.
- 2 Click the **Configure OPC** task.
Each line shows a group's ID, enabled state, name, status and trace flag.
- 3 Click a group name to call up the group's configuration details (in read-only mode).

Group states

The following table describes a group's possible states. The value and alarm level refer to the value that is written to status points (if they are configured) and the suggested alarm level.



Caution

If the Experion service is not running, these status items will not correctly reflect the state of the group. Honeywell therefore recommends that you use an external watchdog.

State (value)	Alarm level	Description
Disabled (0)	(none)	The group is not transferring data.
Starting (1)	(none)	Groups are being created. Data is not yet being transferred.
Ok (2)	(none)	Data is being transferred and no problems have been detected.
Overload (3)	High	The Destination OPC Server is unable to write item values at the required rate.
Marginal (4)	High	Some data is being transferred but some problems have been detected.
Failed (5)	Urgent	A problem has occurred resulting in no data being transferred for this group. Attempts are made to recover the group while the group remains enabled.

Location of OPC Integrator files

OPC Integrator data files are stored in Program Files\Honeywell\Experion PKS\server\data\OPCIntegrator.

These files store all OPC Integrator configuration information, including group states and alarm priorities. When a configuration change is made, the OPC Integrator database is exported to these data files.

If you have redundant servers, these files are automatically replicated to the backup server.

It is strongly recommended that you do not modify these files manually.



Attention

You should back up these files in the same way as you back up the other data files.

OPC Integrator alarms and events

Alarms

All alarms are raised with a source of OPC Integrator.



Tip

If you double-click an OPC Integrator alarm in the Alarm Summary, the OPC Integrator System Status display is called up.

OPC Integrator can generate the following alarms.

Group [*GroupName*] write failure

Write failed for group name *GroupName*.

Group [*GroupName*] partial write failure

One or more writes failed for group *GroupName*. To find out which items within the group failed, check the event log. Note that the *GroupName* may be truncated.

Group [*GroupName*] failed

Group *GroupName* is reporting a failed status, transfers are not taking place. To find out why the group has failed, check the Experion server log. This alarm is latched.

Source OPC server failed [*GroupName:ServerName*]

The source OPC server *ServerName* configured for group *GroupName* has failed. This alarm is latched.

Destination OPC server failed [*GroupName:ServerName*]

The destination OPC server *ServerName* configured for group *GroupName* has failed. This alarm is latched.

Events

OPC Integrator can generate the following events.

OPC Integrator started

The OPC Integrator service has started.

OPC Integrator stopped

The OPC Integrator service has stopped.

Source Error writing to item [*GroupName:ItemName*]

An error was reported by the destination OPC server while writing to Item *ItemName* in group *GroupName*. This would be reported, for example, if the value was outside the range configured for the item.

Invalid data from item [*GroupName:ItemName*]

The item *ItemName* in group *GroupName* returned invalid data from the source OPC server.

Invalid data for group [*GroupName*]

The data for group *GroupName* is corrupt. The group may need to be restarted.

OPC server not primary for group [*GroupName:ServerName*]

OPC Integrator has detected that the OPC server with which it is communicating is running as the backup in a redundant pair, and cannot therefore be read from or written to. OPC Integrator will failover to the other server in the redundant pair.

Group status returned to normal [*GroupName*]

Group *GroupName* that has previously failed, has returned to normal.

Group validated [*GroupName*]

Group *GroupName* has been successfully validated.

Group committed [*GroupName*]

Group *GroupName* has been successfully committed.

Group Deleted [*GroupName*]

Group *GroupName* has been successfully deleted.

Group Enabled [*GroupName*]

Transfers on group *GroupName* have been enabled.

Group Disabled [*GroupName*]

Transfers on group *GroupName* have been disabled.

Group Trace On [*GroupName*]

Tracing on group *GroupName* has been turned on.

Group Trace Off [*GroupName*]

Tracing on group *GroupName* has been turned off.

All groups enabled

All enabled groups have successfully started. This event occurs when a backup server becomes primary.

All groups disabled

All enabled groups have successfully stopped. This event occurs when a primary server becomes backup.

Monitoring the status of the Experion OPC Integrator

You can view the status of the Experion OPC Integrator using the Experion client. However under normal operation this client is not monitored on a continuous basis. For this reason Honeywell recommends that you use status items and an external watchdog.

Using status items

Experion may be transferring critical data around a system. It may detect problems in the transfer of data. For example reading an item with a bad quality, or attempting to write a value beyond its configured range. These problems should be monitored using *status items*.

Status items are OPC items built on the source and destination servers to monitor the state of the transfer. One item should be configured on the source server and one item configured on the destination server for every group configured in the Experion server.

The value of these items is set by the Experion server to reflect the state of each of the configured groups. The values representing warning or errors should be configured to generate alarms, thereby bringing them to the operator’s attention.



Caution

If the Experion service is not running, these status items will not correctly reflect the state of the group. Honeywell therefore recommends that you use an external watchdog.

Example

This is an example of a status item.

Item: OPCI_Group_1_Status

Description: The status of Experion transfer group 1

Values:

Value	Text	Suggested Alarm level
0	Stopped	(none)
1	Starting	(none)
2	Ok	(none)
3	Overload	High
4	Marginal	Urgent
5	Failed	Urgent

Using an external watchdog

The state of the service itself should be monitored using an external watchdog. This guards against hardware faults, such as a power failure or network failure.

Configuring Microsoft Excel Data Exchange

33

The Microsoft Excel Data Exchange option allows you to capture real-time point value and history information from Experion and display the data in an Excel spreadsheet.

Data can be retrieved from Experion by using either the Microsoft Excel Data Exchange Wizard, or through cell formulas. The captured data can be static or dynamically updating, and can consist of either point parameter or historical data from any Experion server database on the network.

After the data has been captured you can create charts to display and analyze data with Microsoft Excel's toolset. You can also link the values into other OLE-enabled applications.

Microsoft Excel Data Exchange gives:

- Read/write access to point parameter values (for example, read the PV of point ID=T1C123)
- Read access to history data
- Read/write access to Experion database files (user files)

Changing the read/write permissions for Microsoft Excel Data Exchange

During installation, you specify whether Microsoft Excel Data Exchange has permission to write to the Experion server database. You can change the permission that you set during installation.

To change the permissions for Microsoft Excel Data Exchange:

- 1 Choose **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 Click the appropriate product as described in the following table:

If you are changing permission on:	Click:
The Experion PKS server	Experion PKS Server R300
A Console Station	Experion PKS Console Station R300
A Flex Station	Experion PKS Client Software R300

- 4 Click **Change**.
- 5 Click **Next**.
- 6 Click **Modify** and click **Next**.
- 7 If Microsoft Excel Data Exchange is not installed, click the Microsoft Excel Data Exchange icon and select **This feature will be installed on local hard drive**.
- 8 Click **Next**.
- 9 If you want to grant Microsoft Excel permission to write to the Experion server database, click **Yes**, otherwise click **No**.
- 10 Click **Next**.
- 11 Click **Modify** to confirm the change.
- 12 Click **Finish**.

Using the Microsoft Excel Data Exchange wizard

The following procedures explain how to capture point or history values and display them in Microsoft Excel using the Microsoft Excel Data Exchange Wizard.

Before beginning any of these procedures:

- 1 Start Microsoft Excel.
- 2 Open the worksheet in which you want your data displayed.
- 3 Highlight the cell that is to be the starting point for the data.

Retrieving point parameters

A cell in a Microsoft Excel worksheet can display the value of a parameter of a point configured on a particular Experion server, for example, the PV of point 01T1LEVEL from the server **hsserv**.

To display a particular point parameter:

- 1 Choose **Tools > Microsoft Excel Data Exchange > Wizard**.
- 2 Select **Get point values from server(s)**.
Specify the target point parameters:
 - a. Type the name of the Experion server, for example **hsserv**.
 - b. Type the desired point ID into the **Point ID** box, for example, **01T1LEVEL**.
 - c. Select the point parameter from the **Point Parameter** list (or type the parameter name into the box), for example, **PV**. You can add or remove point parameters as required.
The **Point Parameter** list does not display all available parameters for the entered point, if the required parameter is not shown in the list, simply type the parameter in. You must enter a parameter that is valid for your point.
 - d. Click **Add** to add the point parameter specification to the list.
- 3 Specify to arrange the data either **Horizontally** or **Vertically**.
- 4 Specify how the data is to be displayed on the worksheet.

Display Server Name

Inserts the name of the Experion server into a cell on your Excel worksheet.

Display Point ID

Inserts the point ID into a cell on your Excel worksheet.

Display Parameter

Inserts the parameter name into a cell on your Excel Worksheet.

Paste Values

When unchecked, it inserts updateable values in your Microsoft Excel Worksheet. When checked, it inserts fixed values into your Microsoft Excel Worksheet. Fixed values cannot be updated.

Minimize number of server calls

This option is only available when you choose to get history values from the Experion server. When it is unchecked, Microsoft Excel queries the Experion server separately for every cell that it fills with data on your Microsoft Excel worksheet. When checked, Microsoft Excel uses as few queries as possible; in general, this means just one query per server. It is important to check **Minimize number of server calls** when the values in the Microsoft Excel worksheet automatically update.

- 5 When you are satisfied with your selection of **Display Options**, click **Finish**. The data is displayed on your worksheet.

Retrieving historical information

You can insert a sequence of historical data into your Microsoft Excel worksheet. In a sequence, each cell contains a single sample from history, for example, five-second snapshots of the PV for point 01T1LEVEL from server **hsserv**.

Considerations

- Ensure that your selection matches the history collection for the points on the server. If you select a history collection that is not configured for that point, Microsoft Excel displays an error code instead of the data.
- **Offset** is the number of samples relative to “now.” You can select this option to see a continuously updating sequence of values. You use the **Date/Time** option to specify a sequence of values from a fixed period of time.
- To view continuously updating data, ensure **Paste values** check box is cleared.

To display a sequence of historical values:

- 1 Choose **Tools > Microsoft Excel Data Exchange > Wizard** to start the wizard.
- 2 Select **Get history values from server(s)**.
- 3 You can specify the target point parameters you want retrieved.
- 4 Specify the desired historical values to be retrieved for the selected points.
- 5 Specify how the data is to be displayed on the worksheet.

Using cell formulas

In addition to using the Microsoft Excel Data Exchange Wizard, you can use cell formulas to capture point or history values. Microsoft Excel Data Exchange includes a number of functions to allow data exchange with Experion. In fact, by using the Microsoft Excel Data Exchange Wizard to retrieve point parameters and historical data, you are actually using several of these functions.



Caution

Do not use the Function Wizard for any **PUT** functions because this may write undesired values to the server. See the Caution in “Microsoft Excel Data Exchange functions” on page 779 for more details.

To use the Microsoft Excel Data Exchange functions:

- 1 Select a cell, or a range of cells, where you want the data to appear.
- 2 Click in Excel’s formula bar, then click the **fx** button to start the Microsoft Excel Function Wizard.



- 3 Select the function you want, as described below.
To select a function:
 - a. From the **Function Category** list, click **User Defined**.
 - b. Select a function from the **Function Name** list.
 - c. Type any required details for the function.

For a more detailed explanation of each Microsoft Excel Data Exchange function, see “Microsoft Excel Data Exchange functions” on page 779.

Changing the data updating rate

Dynamic data on the worksheet is data retrieved by formulas. It includes data retrieved using the Microsoft Excel Data Exchange Wizard when the Paste values check box is cleared (see “Using the Microsoft Excel Data Exchange wizard” on page 771).

To check or to change the data update rate, choose **Tools > Microsoft Excel Data Exchange**. The current setting for the active user account is selected. To change it, select the setting you want.

For best performance, the update rate should be greater than 5 seconds. The more formulas used in a worksheet, the more work has to be performed every time the worksheet is updated. With a large number of formulas, the time taken to update a worksheet might exceed the specified update rate.

Enabling Microsoft Excel Data Exchange under different user accounts

Microsoft Excel Data Exchange is installed for the `mng` account. If you log on under a different account, you cannot see Microsoft Excel Data Exchange in Excel.

The following instructions show you how to enable Microsoft Excel to recognize a range of different user accounts. They assume that Microsoft Excel has been installed and Microsoft Excel Data Exchange has been installed to `\CLIENT\XLDATAEX`.

To enable Microsoft Excel to recognize different user accounts:

- 1 Start Microsoft Excel.
- 2 Check to see if the **Microsoft Excel Data Exchange** choice is in the **Tools** menu.
 - If it is not there, close Microsoft Excel and continue with the following steps.
 - If it is there, Microsoft Excel Data Exchange has been successfully installed for the current account. You do *not* need to continue with the following steps.
- 3 In Windows Explorer, navigate to the Microsoft Excel Data Exchange folder (in this case `C:\CLIENT\XLDATAEX`).
- 4 Double-click **activatemedex.vbs**.
- 5 Start Microsoft Excel.
- 6 The **Microsoft Excel Data Exchange** choice should now be available in the **Tools** menu.

You need to install Microsoft Excel Data Exchange for all user accounts that need to use it.

If you want to use `.xls` files that have been created by other users, you need to:

- 1 Open the workbook
- 2 Choose **Tools > Microsoft Excel Data Exchange > Update Formulas in Workbook**.
- 3 Save the workbook.

Interpreting Microsoft Excel Data Exchange errors

When reading and writing data from/to an Experion server an error may be encountered when a formula is executed in a cell such as:

An unknown Parameter error was encountered (-32215) with server
"matchbox" and point "29471" : matchbox : 29471 : 3

To determine the cause of the error:

1 Choose **Start > Programs > Honeywell Experion PKS > Server > Diagnostic Tools > Error Viewer.**

2 Type the error number and then press **ENTER.**

An error message, such as the following is displayed.

Enter argument(s) for display.exe (<ENTER> for none): **-32215**
08229 CONTROL - illegal mode for control of parameter

Using Experion parameters with Microsoft Excel Data Exchange functions

The following Microsoft Excel Data Exchange functions take the parameter argument as a string (for example, "PV", "SP"):

```
GetPointVal
GetPointValArray(actually a list eg "PV,MD,OP")
GetHistVal_Offset
GetHistValArray_Offset(actually a list e.g. "PV,MD,OP")
GetHistVal_Date
GetHistValArray_Date(actually a list e.g. "PV,MD,OP")
PutPointVal_Number
```

The following Microsoft Excel Data Exchange functions take the parameter argument as an integer (for example, 0 for PV, 3 for SP). For a list of integers, see “Summary of internal parameters” on page 186:

```
NAPI_rGetVal_Number
NAPI_rGetVal_Ascii
NAPI_rGetVal_History
NAPI_rPutVal_Number
NAPI_rGetHstPar_Ofst
NAPI_rGetHstPar_Date
```

The following functions do not have a parameter as an argument:

```
NAPI_rGetPnt_Num
NAPI_rGetPnt_Status
NAPI_rgetdat_int
NAPI_rgetdat_long
NAPI_rgetdat_float
NAPI_rgetdat_double
NAPI_rgetdat_str
NAPI_rputdat_int
NAPI_rputdat_long
NAPI_rputdat_float
NAPI_rputdat_double
NAPI_rputdat_str
```

Microsoft Excel Data Exchange functions

This section describes the Microsoft Excel Data Exchange functions and parameters.

**Caution**

- Functions that are prefixed by NAPI_ should only be used by advanced or experienced users who are familiar with the Network API.
 - Do not use the Microsoft Function Wizard to write NAPI routines into cells. When you type the formula in the Wizard, it displays a value in the top of the Wizard to indicate what you will see in the cell, given the currently entered formula. To determine this value, Microsoft Excel actually runs the function, and this means that if you are setting up a PUTVAL, it will write down to the server as you enter your intermediate values. For example, if you write the PUTVAL (POINT,SP,123.4) it will write the values, 1, 12, 123 and 123.4 to the setpoint of POINT.
-

Formula arrays

When using formulas in worksheet cells in Microsoft Excel, some formulas may return an array as a result. By default Microsoft Excel will only show the first element of the array in the cell the formula is in. To see the complete array, you need to spread the formula across a few cells.

To insert a formula array:

- 1 Select the cells in which you would like to insert the output.
- 2 Type in the function (or use the Microsoft Excel Function Wizard to build the function).
- 3 After completing the formula, press CTRL+SHIFT+ENTER (instead of ENTER) to put the formula into all the cells.

This formula will only be executed once for the whole selection of cells and the output array will be placed in these cells.

**Tip**

If you click one of the cells in the formula array you will notice that the formula appears in parentheses { } instead of by itself.

To edit a formula array:

- 1 Select all the cells which form the formula array.
- 2 Click the formula in the formula entry line near the top of the window.
- 3 Edit the formula as necessary.
- 4 Press CTRL+SHIFT+ENTER to place the formula back into the formula array cells.

To change the number of cells in a formula array:

- 1 Follow Steps 1 and 2 of the editing instructions.
- 2 Copy the formula to the clipboard (press CTRL+C).
- 3 Delete the cells.
- 4 Select the required cells for the new formula array.
- 5 Paste the formula from the clipboard (CTRL+V).
- 6 Press CTRL+SHIFT+ENTER to place the formula back into the formula array cells.

For more information on these topics see Microsoft Excel's help.

GetHistVal_Date

For a single point parameter, retrieves multiple consecutive history values by date and time. GetHistVal_Date inserts each history sample into an individual cell in your Microsoft Excel worksheet. Before using the function, you must highlight the cells that will contain history values (that is, you must highlight the number of rows and columns necessary for displaying the data).

Server	Name of the Experion server from which data is retrieved.
PointID	Name of the point on the Experion server from which data is retrieved.
PointParameter	The point parameter of interest, for example, "PV" . See "Summary of point parameter types" on page 174 for a list of parameter types.
HistoryType	The history type to be retrieved, for example, "H5SF" for fast history snapshots. See "Types of history collection" on page 215 for a list of history types.
HistoryDate	The start date of the historical data. The date can be in any string format that Microsoft Excel can interpret as a date or time, for example "02/08/04" or "02-Aug-04" . Enclose the date with double quotes.
HistoryTime	The starting time of the historical data to retrieve in 24 hour format. For example, "17:30:15" for 5:30:15pm. Enclose the time with double quotes.
ArchivePath	Set this to " "

Example	To retrieve 10 fast history values at 8:00am on 2 August 2004 for the PV parameter of point PNTANA1 on server HSSERVA. <code>=GetHistVal_Date("hsserva","pntana1","pv","h5sf","2 August 2004","8:00am",10,"")</code>

GetHistVal_Offset

For a single point parameter, retrieves multiple consecutive history values by offset. GetHistVal_Date inserts each history sample into an individual cell in your Microsoft Excel worksheet. Before using the function, you must highlight the number of cells that will contain history values (that is, you must highlight the number of rows and columns necessary for displaying the data). Offset sets the function to retrieve samples relative to now. So, for example, setting an offset of 5, means the first sample is 5 samples ago.

For example, when you want to return five history samples with an offset of 5, you must select five consecutive cells horizontally across your spreadsheet, and the function returns the values from 5 samples ago until the current sample, inclusive.

Server	Name of the Experion server from which data is retrieved.
PointID	Name of the point on the Experion server from which data is retrieved.
PointParameter	The point parameter of interest, for example, "PV" . See "Summary of point parameter types" on page 174 for a list of parameter types.
HistoryType	History type of the point to retrieve. For example, "H5SF" for fast history snapshots. See "Types of history collection" on page 215 for a list of history types.
HistoryOffset	Starting history interval from now.
ArchivePath	Set this to " "

Example	To retrieve the last 10 fast history values for the PV parameter of point PNTANA1 on server HSSERVA. <code>=GetHistVal_Offset("hsserva","pntana1","pv","h5sf",1,10,"")</code>

GetHistValArray_Date

For multiple point parameters, retrieves multiple consecutive history values by date and time. Before using the function, you must highlight the number of cells that will contain history values (that is, you must highlight the number of rows and columns necessary for displaying the data). This function can display data horizontally (history values by point parameters) or vertically (point parameters by history values).

NumPoints	Number of points.
Server	Name of the Experion server from which data is retrieved.
PointIDList	A list of point IDs on the Experion server from which data is retrieved. The names in the list must be separated by commas, for example "sinewave,tank1temp" . The number of names in the list must match the number specified in NumPoints.
PointParamList	A list of point parameters separated by commas, for example "pv,sp" . The number of parameters in the list must match the number specified in NumPoints. See "Summary of point parameter types" on page 174 for a list of parameter types.
HistoryType	History type of the point to retrieve. For example, "H5SF" for fast history snapshots. See "Types of history collection" on page 215 for a list of history types.
HistoryDate	Starting date of historical data to retrieve. The date can be in different formats, for example "02/08/04" and "02-Aug-04" . Enclose the date with double quotes.
HistoryTime	Starting time of historical data to retrieve. The data is formatted in 24 hour format. For example, "17:30:15" for 5:30:15pm. Enclose the time with double quotes.
NumHistValues	Number of history values to retrieve.
Orientation	Type "h" for horizontal and "v" for vertical.
ArchivePath	Set this to ""

Example	To retrieve 10 fast history values at 8:00 am on 2 August 2004 for the PV and OP parameters of point PNTANA1 on server HSSERVA, and format the output to display the history values for each parameter horizontally: <pre>=GetHistValArray_Date(2,"hsserva","pntana1,pntana1", "pv,op","h5sf","2 August 2004","8:00am",10,"h","")</pre>

GetHistValArray_Offset

For multiple point parameters, retrieves multiple consecutive history values by offset. Before using the function, you must highlight the number of cells that will contain history values (that is, you must highlight the number of rows and columns necessary for displaying the data). The function can display data horizontally (history values by point parameters) or vertically (point parameters by history values).

NumPoints	Number of points.
Server	Name of the Experion server from which data is retrieved.
PointIDList	A list of point IDs on the Experion server from which data is retrieved. These names must be separated by commas, for example "sinewave,tank1temp" . The number of names in the list must match the number specified by NumPoints.
PointParamList	A list of point parameters separated by commas, for example "pv, sp". The number of parameters in the list must match the number specified in NumPoints. See "Summary of point parameter types" on page 174 for a list of parameter types.
HistoryType	History type of the point to retrieve. For example, "H5SF" for fast history snapshots. See "Types of history collection" on page 215 for a list of history types.
HistoryOffset	Starting history interval from now.
NumHistValues	Number of history values to retrieve.
Orientation	Type "h" for horizontal and "v" for vertical.
ArchivePath	Set this to " "

Example	To retrieve the last 10 fast history values for the PV and OP parameters of point PNTANA1 on server HSSERVA, and format the output to display the history values for each parameter horizontally: <pre>=GetHistValArray_Offset(2,"hsserva","pntana1,pntana1","pv,op", "h5sf",1,10,"h","")</pre>

GetPointVal

Retrieves a single point parameter value from the server.

Server	Name of the Experion server from which data is retrieved.
PointID	Name of the point on the Experion server from which data is retrieved.
PointParameter	The point parameter of interest, for example, "PV" . See "Summary of point parameter types" on page 174 for a list of parameter types.

Example	To retrieve the current value for the PV of point PNTANA1 on server HSSERVA: <code>=GetPointVal("hsserva","pntana1","pv")</code>

GetPointValArray

Retrieves the value of multiple point parameters from the server. Before using the function, you must highlight the number of cells that will contain history values (that is, you must highlight the number of rows and columns necessary for displaying the data). Can display data horizontally or vertically.

NumPoints	Number of points.
Server	Name of the Experion server from which data is retrieved.
PointIDList	A list of point IDs on the Experion server from which data is retrieved. These names must be separated by commas, for example "sinewave,tank1temp" . The number of names in the list must match the number specified in NumPoints
PointParamList	A list of point parameters separated by commas, for example "pv,sp". The number of parameters in the list must match the number specified in NumPoints. See "Summary of point parameter types" on page 174 for a list of parameter types.
Orientation	Type "h" for horizontal and "v" for vertical.

Example	To retrieve the current values for the PV and OP of point PNTANA1 on server HSSERVA, and arrange the parameter output values vertically: <code>=GetPointValArray(2,"hsserva","pntana1,pntana1","pv,op","v")</code>

PutPointVal_Number

Changes a single point parameter value from the server.

Server	Name of the Experion server on which data is changed.
PointID	Name of the point on the Experion server on which data is changed.
PointParameter	The point parameter of interest, for example, “OP” . See “Summary of point parameter types” on page 174 for a list of parameter types.

Example	To change the current value for the OP of point PNTANA1 on server HSSERVA: =PutPointVal_Number("hsserva","pntana1","op",45)

NAPI_rGetdat_int, NAPI_rGetdat_double, NAPI_rGetdat_float and NAPI_rGetdat_long

Retrieves a single field from a user file in the following formats:

double	double precision (8 bytes) I.E.E.E. floating point
float	single precision (4 byte) I.E.E.E. floating point
int	two bytes signed integer
long	four bytes signed integer

Server	Name of the Experion server from which data is retrieved.
File	Experion database file number. User files start from file 251 so that user file 1 is file 251, user file 2 is file 252 and so on.
Record	The record number in the user file.
Word	The word number in the record.
Flags	For a circular file, specifies the direction to read. Type newest for the newest record or oldest for the oldest record. Type 0 for non-circular files.

Example	To retrieve the current system sinewave value (int) from file 8, record 1, word 114 from server hsserva: <code>=NAPI_rGetdat_int("hsserva",8,1,114,0)</code>

NAPI_rGetdat_str

Retrieves a single field from a user file in string format

Server	Name of the Experion server from which data is retrieved.
File	Experion database file number. User files start from file 251 so that user file 1 is file 251, user file 2 is file 252 and so on.
Record	The record number in the user file.
Word	The word number in the record.
Flags	For a circular file, specifies the direction to read. Type newest for the newest record or oldest for the oldest record. Type 0 for non-circular files.
Length	The length of the string to retrieve.

NAPI_rGethstpar_date

Retrieves history parameter value for a single point by date and time.

Server	Name of the Experion server from which data is retrieved.
HistoryType	History type of the point to retrieve. For example, 6 for fast history. The history types and the parameter values are: • 1—H1M (one minute history) • 2—H6M (six minute history) • 3—H1H (1 hour history) • 4—H8H (8 hour history) • 5—H24H (24 hour history) • 6—H5SF (fast history snapshots) • 7—H1HE (1 hour extended history) • 8—H8HE (8 hour extended history) • 9—H24HE (24 hour extended history)
HistoryDate	Starting date of historical data to retrieve, specified as the number of days since 1 January 1981.
HistoryTime	Starting time of historical data to retrieve, specified as the number of seconds since midnight.
NumHistValues	Number of history values to retrieve.
ArchivePath	Set this to “ ”
PointNumber	Point number of the point. See “NAPI_rGetPnt_Num” on page 792 for details of how to obtain the point number for a point ID.
ParamNumber	The point parameter of interest, for example, PV. See “Summary of point parameter types” on page 174 for a list of parameter types.

Example	To retrieve the 10 values of fast history at 8:00am on 2 August 04 for the PV of point PNTANA1 from server HSSERVA: <pre>=NAPI_rGethstpar_date("hsserva",6,date(2004,08,2)- date(1981,1,1),8*60*60,10,"",NAPI_rGetPnt_Num("hsserva", "pntana1"),0)</pre>

NAPI_rGethstpar_ofst

Retrieves history parameter value for a single point by offset.

Server	Name of the Experion server from which data is retrieved.
HistoryType	History type of the point to retrieve. For example, 6 for fast history. The history types and the parameter values are: • 1—H1M (one minute history) • 2—H6M (six minute history) • 3—H1H (1 hour history) • 4—H8H (8 hour history) • 5—H24H (24 hour history) • 6—H5SF (fast history snapshots) • 7—H1HE (1 hour extended history) • 8—H8HE (8 hour extended history) • 9—H24HE (24 hour extended history)
HistoryOffset	Starting history interval from now.
NumHistValues	Number of history values to retrieve.
ArchivePath	Set this to “ ”
PointNumber	Point number of the point. See “NAPI_rGetPnt_Num” on page 792 for details of how to obtain the point number for a point ID.
ParamNumber	The point parameter of interest, for example, PV. See “Summary of point parameter types” on page 174 for a list of parameter types.

Example	To retrieve the last 10 values of fast history for the PV of point PNTANA1 from server HSSERVA: <pre>=NAPI_rGethstpar_ofst("hsserva",6,1,10,"",NAPI_rGetPnt_Num("hsserva","pntana1"),0)</pre>

NAPI_rGetPnt_Num

Retrieves the point number for a point.

Server	Name of the Experion server from which data is retrieved.
PointID	Name of the point on the Experion server from which data is retrieved.

Example	To retrieve the point number of point PNTANA1 from server HSSERVA: =NAPI_rGetPnt_Num("hsserva","pntana1")

NAPI_rGetPnt_Status

Retrieves a point status information.

Server	Name of the Experion server from which data is retrieved.
PointID	Name of the point on the Experion server from which data is retrieved.

Example	To retrieve the point status of point PNTANA1 from server HSSERVA: =NAPI_rGetPnt_Num("hsserva","pntana1")

NAPI_rGetVal_Ascii

Retrieves a string parameter of a point.

Server	Name of the Experion server from which data is retrieved.
PointNumber	Point number of the point. See “NAPI_rGetPnt_Num” on page 792 for details of how to obtain the point number for a point ID.
ParamNumber	The point parameter of interest, for example, DESC. See “Summary of point parameter types” on page 174 for a list of parameter types.

Example	To retrieve the ASCII value of parameter DESC of point PNTANA1 from server HSSERVA: <code>=NAPI_rGetVal_Ascii("hsserva",NAPI_rGetPntNum("hsserva", "pntana1"),37)</code>

NAPI_rGetVal_History

Retrieves the value of the PV history type of a point.

Server	Name of the Experion server from which data is retrieved.
PointNumber	Point number of the point. See “NAPI_rGetPnt_Num” on page 792 for details of how to obtain the point number for a point ID.
ParamNumber	The point parameter of interest, for example, PV. See “Summary of point parameter types” on page 174 for a list of parameter types.
HistoryOffset	Starting history interval from now.

Example	To retrieve the history value at history offset 5 of parameter H5SF (Fast History) of point PNTANA1 from server HSSERVA: <code>=NAPI_rGetVal_History("hsserva",NAPI_rGetPntNum("hsserva", "pntana1"),46,5)</code>

NAPI_rGetVal_Number

Retrieves a numeric parameter of a point.

Server	Name of the Experion server from which data is retrieved.
PointNumber	Point number of the point. See “NAPI_rGetPnt_Num” on page 792 for details of how to obtain the point number for a point ID.
ParamNumber	The point parameter of interest, for example, PV. See “Summary of point parameter types” on page 174 for a list of parameter types.

Example	To retrieve the numeric value of parameter PV of point PNTANA1 from server HSSERVA: <code>=NAPI_rGetVal_Number("hsserva",NAPI_rGetPntNum("hsserva", "pntana1"),0)</code>

NAPI_rPutdat_int, NAPI_rPutdat_double, NAPI_rPutdat_float, NAPI_rPutdat_long and NAPI_rPutdat_str



Caution

Do not use this function through Microsoft Excel’s Function wizard, as multiple controls may be performed for the given address. See the Caution at the beginning of “Microsoft Excel Data Exchange functions” on page 779 for more details.

Writes a single value to a field in a user file in the following formats:

double	double precision (8 bytes) I.E.E.E. floating point
float	single precision (4 byte) I.E.E.E. floating point
int	two bytes signed integer
long	four bytes signed integer
str	character string

Server	Name of the Experion server to which the value is written.
File	Experion database file number. User files start from file 251 so that user file 1 is file 251, user file 2 is file 252 and so on.
Record	Record number in the user file.
Word	Word number in the record.
Flags	For a circular file, specifies the direction to read. Type newest for the newest record or oldest for the oldest record. Type 0 for non-circular files.
Value	Value to write.

Example	To store an integer value of 42 into user table 1, record 1, word 15 for server HSSERVA. <code>=NAPI_rPutdat_int("hsserva",251,1,15,0,42)</code>

NAPI_rPutVal_Number



Caution

Do not use this function through Excel’s Function wizard, as multiple controls to undesired values may be performed for the given point’s parameter. See the Caution at the beginning of “Microsoft Excel Data Exchange functions” on page 779 for more details.

Set a numeric parameter of a point.

Server	Name of the Experion server from which data is retrieved.
PointNumber	Point number of the point. See “NAPI_rGetPnt_Num” on page 792 for details of how to obtain the point number for a point ID.
ParamNumber	The point parameter of interest, for example, PV. See “Summary of point parameter types” on page 174 for a list of parameter types.
ParamValue	Value to set.

Example

To store the numeric value of parameter SP of point PNTANA1 from server HSSERVA:

```
=NAPI_rPutVal_Number("hsserva",NAPI_rGetPntNum("hsserva",  
"pntana1"),3,42)
```

Developing custom applications

34

You can use the API (Application Programming Interface), the Network API or the Server Automation Object model to develop your own custom applications that work in conjunction with Experion. For example, you can configure an Experion report to request a custom application when it has completed running.

You use the API for applications that run on the server computer. The types of applications you can create are utilities, user scan tasks and tasks. You can use the following languages:

- C
- C++

You use the Network API for applications that run on another computer. The type of applications you can create are utilities. You can use the following languages:

- C
- C++
- Visual Basic

You use the Server Automation Object model for applications that run on the server computer. The type of applications you can create are utilities and tasks. You can use the following languages:

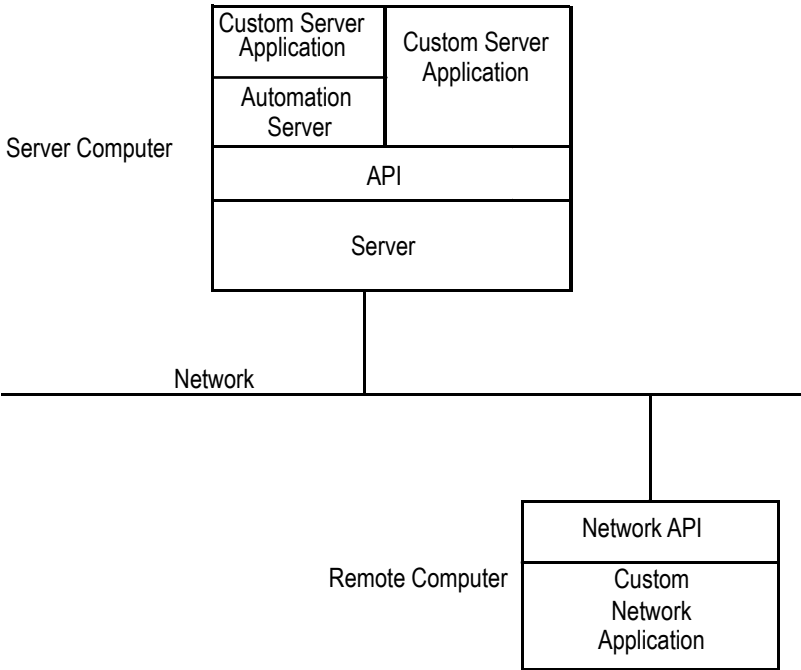
- C++
- Visual Basic

Network API gives:

- Read/write access to point parameter values (for example, read the PV of point ID= T1C123)
- Read access to history data
- Read/write access to Experion database files (user files)

The following figure gives a simplified view of the relationship between the Experion server, the API, the Network API, the Automation server and custom applications.

Figure 60 How custom applications work with Experion



For details about the API and Network API, see the *Application Development Guide*. For an overview of the Server Automation Object Model, see the chapter on Automation Objects in the *Application Development Guide*.

This chapter provides an overview of how to integrate PHD with Experion using the Experion-PHD Link.

Using the Experion-PHD Link:

- Data collected by Experion can be transferred to PHD for long-term storage and management.
- You can display PHD data on Experion trends.

After integrating PHD with Experion, each point parameter that is historized in Experion is automatically added to PHD as a tag. This is referred to as *tag synchronization*.

Tag synchronization features include:

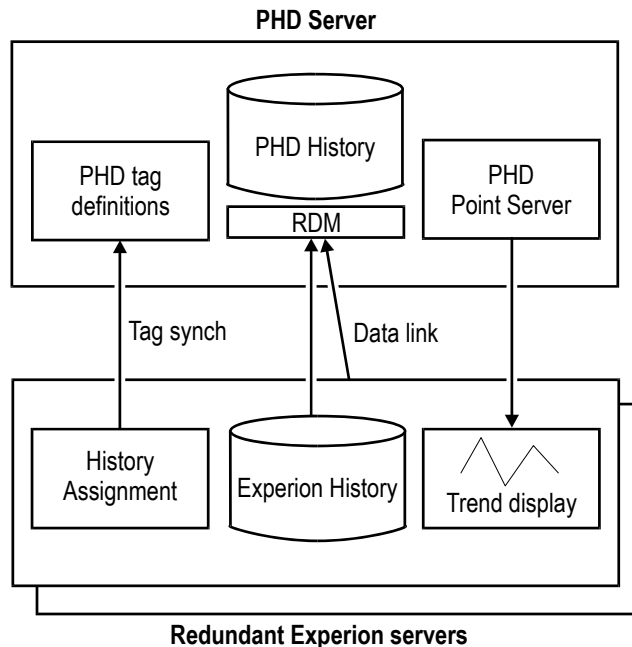
- When you delete a point parameter in Experion, the PHD tag stops collecting history, although the tag and history are not deleted from PHD.
- Changes to key configuration parameters, such as range and engineering units, are automatically synchronized with PHD.
- You can choose to override the default behavior of PHD and Experion on a tag-by-tag basis. For example, you can stop PHD synchronizing a tag with an Experion point parameter, or you can stop PHD collecting history values for a particular Experion point parameter.
- If the connection between Experion and PHD is lost, after the connection is restored, tag synchronization and data collection automatically resume, with any past tag updates and data values automatically transferred to PHD.

You can install a PHD Point Server on the PHD server to return history data for non-synchronized tags to Experion.

PHD integration architecture overview

Experion and PHD are integrated through three functions:

- Tag synchronization for synchronizing Experion point parameters with PHD tag definitions.
- The data link that enables PHD to request history data from Experion.
- The PHD point server for requesting data from PHD for use in Experion trends.



PHD and Experion tag synchronization components

The PHD tag synchronization component is installed as part of the PHD installation. No Experion configuration is required for tag synchronization. For more information about configuring PHD for tag synchronization, see the *PHD User's Guide*.

Point parameter and history assignment changes are queued in the Experion tag synchronization component for exchange with the PHD tag synchronization component every few minutes.

Data link and history

PHD tags can be configured to collect data from Experion using the Experion-PHD Link. For more information about how to configure the Experion-PHD Link, see the *PHD User's Guide*.

Synchronized tags are automatically configured to be collected by PHD. PHD requests the history data from Experion. For redundant Experion servers, it communicates this request through Redirection Manager (RDM). RDM determines the redundant Experion server that is active prior to forwarding requests. When RDM detects a failover, it stores requests until the failover process is completed, then forwards them to the newly active Experion server.

Experion stores only numeric history. Enumerations are stored as ordinals, and the enumerated state obtained from the underlying data owner when providing history data. When enumerated values are collected by PHD, the corresponding states must be added to PHD. For more information about adding these states, see the *PHD User's Guide*.

PHD point server

If you want PHD history data for display on trends, you need to install a PHD Point Server on the PHD server. Only one Experion server can receive data from the PHD Point Server. If you want to access this data from other Experion servers, you will need to configure these servers to subscribe to this server using DSA.

To access PHD tags, you use the PHD Point Server alias as the point name and the PHD tag name as the parameter. You define the PHD Point Server alias when you configure the Experion connection to the PHD Point Server.

Configuring the Experion-PHD Link

The following checklist identifies the high-level tasks to configure the Experion-PHD Link. After completing these tasks, point parameters assigned to history in Experion are synchronized with tags in PHD and the history data is replicated to PHD.

Task	Go to	Done
If you have redundant Experion servers, install Redirection Manager (RDM) on the PHD server node. You can also install the System Management display when you install RDM.	<i>RDM User Guide</i>	
If you installed the System Management Display during the RDM install, configure the System Management display.	<i>System Management Configuration Guide</i>	
Configure the RDM.	<i>RDM User Guide</i>	
Configure the PHD/Experion link.	<i>PHD/Experion Link Configuration Guide</i>	
Evaluate the standard tag synchronization rule. If necessary, customize the rule or add more rules to meet your requirements. The default rule covers most scenarios when there is no existing PHD database.	<i>PHD User Guide</i>	
For LCN-connected Experion servers, assign TPS points to history for tag synchronization with PHD.	page 811	
If you want to bring PHD-only data back into Experion for display on a trend, do the following: • Install the PHD point server on the PHD node. • Configure the point server client to communicate with the PHD point server.	<i>Supplementary Installation Tasks Guide</i>	

Tuning the PHD point server

Configuration settings for the PHD point server are stored in the registry and default values are set during installation. You may want to change some of these settings to suit your site requirements.



Caution

Incorrectly editing the registry can cause severe damage to your system. Before you make any changes to the registry, you should back up your system state data.

Changing PHD retrieval attributes

The Experion trend currently supports two types of data aggregation, snapshots and averages. For example, the fast history (5 second), 1 minute, 1 hour, 8 hour and 24 hour intervals use snapshots. The 6 minute average, 1 hour average, 8 hour average and 24 hour average intervals use average.

The PHD Point Server maps these types of requests to PHD data request properties. This mapping can be changed using the `AverageRetrievalSettings` and `SnapshotRetrievalSettings` registry keys.

To change the PHD average retrieval attributes:

- 1 On the PHD point server computer choose **Start > Run**.
- 2 Type **regedit** and click **OK**.
- 3 Locate the key:
**HKEY_LOCAL_MACHINE\SOFTWARE\Honeywell\PHDPointServer/
AverageRetrievalSettings**
- 4 Change the values of the key as appropriate for your site.
For information about the values see Table 22 on page 806.
- 5 Click **OK**.
- 6 Restart the PHD point server service to apply the new settings.

To change the PHD snapshot retrieval attributes:

- 1 On the PHD point server computer choose **Start > Run**.
- 2 Type **regedit** and click **OK**.
- 3 Locate the key:
**HKEY_LOCAL_MACHINE\SOFTWARE\Honeywell\PHDPointServer/
SnapshotRetrievalSettings**

- 4 Change the values of the key as appropriate for your site.
For information about the values see Table 22 on page 806.
- 5 Click **OK**.
- 6 Restart the PHD point server service to apply the new settings.

Table 22 PHD retrieval attributes

Value	Description
ResampleType	The type of resampling. Valid values are: • AVERAGE • INTERPOLATEDRAW • RAW • RESAMPLED • SNAPSHOT The default value for AverageRetrievalSettings is InterpolatedRaw. The default value for SnapshotRetrievalSettings is Resampled.
ResampleFrequency	The value stored here is currently ignored. If UseResampleFrequency is 1 (TRUE), then the ResampleFrequency is set to the interval period of the trend. For example, a 1 minute trend uses a 1 minute (60 second) resample frequency for the PHD data request. The default value for AverageRetrievalSettings is 60.
UseResampleRequency	Whether to set the resample frequency or the reduction frequency. If set to 1 (TRUE), then the interval period of the trend is used as the PHD resample frequency. If set to 0 (FALSE), then the interval period of the trend is used as the PHD reduction frequency. For example, if calling up a 1 hour interval, and UseResampleFrequency is set to 1 (True), then the PHD data request uses a resample frequency of 1 hour (3600 seconds) and a reduction frequency of 0. If UseResampleFrequency is set to 0 (False), then the PHD data request uses a resample frequency of 0 and a reduction frequency of 1 hour (3600 seconds). The default value for AverageRetrievalSettings is 0. The default value for SnapshotRetrievalSettings is 1.

Table 22 PHD retrieval attributes

Value	Description
ReductionType	The type of reduction. Valid values are: • AVERAGE • DELTA • FIRST • LAST • MAXIMUM • MINIMUM • NONE • REGRESSIONCONSTANT • REGRESSIONDEVIATION • REGRESSIONSLOPE • STANDARDDEVIATION The default value for AverageRetrievalSettings is Average. The default value for SnapshotRetrievalSettings is None.
ReductionOffset	The reduction offset. Valid values are: • AFTER • BEFORE • AROUND The default value for AverageRetrievalSettings is Before. The default value for SnapshotRetrievalSettings is Before.
ReductionFrequency	The value stored here is currently ignored. If UseResampleFrequency is 0 (FALSE), then the ReductionFrequency is set to the interval period of the trend. For example, a 1 minute trend uses a 1 minute (60 second) reduction frequency for the PHD data request. The default value for SnapshotRetrievalSettings is 60.

Changing history timeout

The PHD point server measures the time it takes to read a single PHD tag and then estimates the time required to read the number of PHD tags included in a trend. If the estimated time exceeds the HistoryTimeout registry value, then the request is canceled and no data is plotted on the trend for the requested time range.

To change the history timeout

- 1 On the PHD point server computer choose **Start > Run**.
- 2 Type **regedit** and click **OK**.
- 3 Locate the key:
**HKEY_LOCAL_MACHINE/SOFTWARE/Honeywell/PHDPointServer/
HistoryTimeout**
- 4 Change the value as appropriate for your site requirements.
The HistoryTimeout value is in milliseconds.
- 5 Click **OK**.
- 6 Restart the PHD point server service to apply the new settings.

Changing the confidence value

The PHD point server checks all the data returned from the PHD server to determine if values are below the minimum confidence configured. If a returned value is below the minimum confidence, then it is not plotted on the Experion trend.

To change the confidence value

- 1 On the PHD point server computer choose **Start > Run**.
- 2 Type **regedit** and click **OK**.
- 3 Locate the key:
**HKEY_LOCAL_MACHINE/SOFTWARE/Honeywell/PHDPointServer/
MinConfidence**
- 4 Change the value as appropriate for your site requirements.
The value must be an integer between -1 and 100.
- 5 Click **OK**.
- 6 Restart the PHD point server service to apply the new settings.

Guidelines for optimizing performance

The PHD point server sends history data requests from the Experion server (for trends) to the PHD server. The amount of time required to retrieve the data and the amount of CPU usage by the PHD server and the PHD point server is dependent on several factors. The following topics provide guidelines on minimizing CPU usage and data requests.

Trend data types

Calling up a trend with average interval types, for example, 1 hour average, causes the PHD point server to request average reductions from PHD. This can cause:

- Increased CPU usage because PHD has to average all the raw data before retuning it to the PHD point server. Larger intervals relative to the PHD tag scanning rate causes more CPU usage. For example, a trend with a 24 hour average with PHD tags that have a 5 second scanning rate causes increased CPU usage by the PHD software.
- Increased call-up time due to the calculations that PHD has to perform to average the data.

It is recommended that you avoid calling up trends that include PHD tags with averages of PHD tags at fast scanning rates.

Number of traces

Calling up a trend with a large number of PHD tags causes the PHD point server to request the tags from PHD. This can cause:

- Increased CPU usage because more data and values have to be retrieved from PHD.
- Increase call-up time because of the amount of values that PHD has to process and the number of values that have to be transferred from PHD to the PHD point server and then to the Experion server. There is a reasonably linear relationship between the number of traces and the call-up time.

It is recommended that you avoid including too many PHD tags on a single Experion trend.

Call-up time and live updates

The initial call-up of a trend causes the PHD point server to request data for all traces for the entire time period of the trend. This leads to significant CPU usage and call-up time. For example, a 1 minute interval trend of 1 day for ten PHD tags

means that the PHD point server needs to retrieve 14400 values (60 minutes * 24 hours * 10 tags) immediately on call-up.

If an Experion trend is put into live update mode (by clicking Resume live updates) the trend updates at the interval rate. In this situation, only the newest values are retrieved which means the amount of CPU usage is minimal. For example, if viewing a 1 minute interval trend with ten PHD tags, the PHD point server only has to retrieve 10 values (1 value * 10 tags) every minute.

Assigning TPS point parameters to history

For LCN-connected Experion systems, you can assign TPS point parameters to history so that they are added to PHD as a tag using one of the following methods:

- Import HM history assignment into Experion. For instructions, see “Importing HM history assignment into Experion” on page 812.
- Create and execute an LCN-connected server point build file to assign TPS point parameters to history, and to cause the TPS points and parameters to be discovered. For instructions, see “Creating an LCN-connected server point build file” on page 814.

Importing HM history assignment into Experion

You can import HM history using the TPN History Configuration Import tool.

Considerations

- You should prime the TPN Server cache before running the TPN History Configuration Import tool.
- It may take several hours to upload the history assignment from the LCN, and then several hours more to export the history assignment to the LCN-connected server.
- TPN history collection rates are mapped to the following Experion rates:
 - 5, 10, 20 second rates are mapped to Experion FAST.
 - 60 second rates are mapped to Experion STANDARD (60 secs).
- You can change collection rates, assignment to Experion history groups, or delete items, by exporting the upload as a .csv file, editing the .csv file, reading the edited file into TPN History Configuration Import tool, and then exporting it to the LCN-connected server.
- You can edit the .csv using a text editor or Microsoft Excel.
- The format of the exported .csv file is:

point.parameter, TPN_unit_name, Experion_rate

For example:

```
AHEAPF35.PV,01,FAST
AHEAPF36.PV,01,FAST
AHEAPF35.PV,01,STANDARD
AHEAPF36.PV,01,STANDARD
AHEAPF37.PV,01,STANDARD
AHEAPF38.PV,01,STANDARD
AHEAPF35.PV,01,EXTENDED
AHEAPF36.PV,01,EXTENDED
AHEAPF37.PV,01,EXTENDED
AHEAPF38.PV,01,EXTENDED
```

To import the HM history assignment:

- 1 Start the TPN History Configuration Import tool on the primary LCN-connected server.
The **TPN History Configuration Import** window appears.
- 2 Click **Get HM Groups**.
The history groups are uploaded from the LCN. This may take several hours.
- 3 In the **TPN Units/History Groups** list, select the history groups you want to export to the LCN-connect server.

- 4 If you want to change the collection rates, assignment to Experion history groups, or to delete points, click **Save .CSV**. Save this file, and then edit the values. When you have finished editing the .csv file, click **Read .CSV** and select the edited file.
- 5 Click **Export**.
The selected history groups are exported to the LCN-connected server. This may take several hours.
- 6 Close the TPN History Configuration Import tool.

Creating an LCN-connected server point build file

To create an LCN-connected server point build file:

- 1 Create a text file with one of the following commands on each line.
- 2 To assign a point parameter to 1 or 5 second history (depending on what was selected at install time), use the following syntax:
HISTFAST Point_ID parameter
- 3 To assign a point parameter to 60 second history, use the following syntax:
HISTSLOW Point_ID parameter
- 4 Assign a point to 60 minute history, use the following syntax:
HISTEXTD Point_ID parameter
- 5 Execute the commands in the file by entering at the command prompt, e.g.:
pntbld file.pnt

Note that you must run pntbld on the LCN-connected Server. It cannot be run on an LCN-connected ES-C.

Example

Here is an example history file:

```
HISTFAST FIC123 PV
HISTFAST FIC201 PV
HISTSLOW FIC123 SP
HISTSLOW FIC201 SP
HISTEXTD FIC123 OP
HISTEXTD FIC201 OP
```

Specialized pntbld functionality

To learn how to construct more specialized pntbld statements, see entries, such as HISTFAST, HISTSLOW, HISTEXTD, HISGATE, see the *Experion Hardware and Point Build Reference*.

This chapter describes the commands and utilities used to configure Experion. They are grouped as follows:

- Installation/migration commands
- Configuration commands
- Controller configuration commands
- Diagnostic commands
- Administration commands
- Database initialization commands
- Application development commands

To run a command/utility, see [Running Experion commands/utilities](#).

Running Experion commands/utilities

To use the commands and utilities described in this chapter you need to log on to the server using an account that belongs to the Honeywell Administrator group.

To run a command/utility:

- 1 Choose **Start > Programs > Accessories > Command Prompt** to open a Command Prompt window.
Alternatively, choose **Start > Programs > Honeywell Experion PKS > Server > Diagnostic Tools** and then select the relevant tool.
- 2 Type the command and press ENTER.

Installation/migration commands

The following commands and utilities are used for installation and migration tasks:

- sysbld
- utbconv

sysbld

Description

sysbld is used to adjust the number of configurable database items within the maximum number of items permitted by your license. **sysbld** allows you to adjust:

- History retention periods, including duration and number of samples
- Number of points you can collect history for each history type
- Maximum number of:
 - Printer connections
 - Channels
 - Controllers
 - Algorithm blocks
 - Assets
 - Trends
 - Groups
 - Reports
 - Point control schedules
 - Operators
 - Concurrent alarms
 - Concurrent messages
 - Stored events
 - User files
 - Application tasks
 - Point lists



Caution

If you initialize the database, all your configuration and process data will be deleted.

Syntax

```
sysbld mode [options]
```

Part	Description
<i>mode</i>	One of the following: -initialise Initializes the database, and deletes all configuration and process data. -preserve Preserves data in the database. See “Disk space considerations” on page 819.
<i>options</i>	-default Builds the database using default sizes. -diag Prints diagnostic messages. -full Resizes all database items. -y Answers yes to all questions.

Notes

- You cannot use **sysbld** to increase the point count for which you are currently licensed. To increase the point count, you need to upgrade your Experion software license to provide for a larger database size. You use the Experion PKS Server Configuration Panel to change your license details.
- You must stop the Experion server before running **sysbld**.

Disk space considerations

If you preserve the contents of the database, the contents of the existing database are retained. However, some additional temporary disk space is required.

When **sysbld** preserves the database, it copies the data from each database file in the Program Files\Honeywell\Experion PKS\server\data folder to a new re-sized file, one database file at a time. To calculate the amount of temporary disk space required, determine the size of the largest file in the Program Files\Honeywell\Experion PKS\server\data folder, and make sure that you have at least this amount of temporary disk space available before running **sysbld**.

utbconv

Description

utbconv is provided to migrate point and parameter reference numbers embedded in user files from an old release of Experion to the current release. (When you upgrade to the current release, all parameter and point numbers except those in user files are automatically translated (if necessary) by the Experion installation process.)

Syntax

```
utbconv release_number input_file
```

Part	Description
<i>release_number</i>	The old release that is being migrated.
<i>input_file</i>	The relative path name of the input file specifying which user table words are to be migrated. See “UTBCONV definition file format” on page 820 for the input file format.

Notes

- Before migrating user files using **utbconv**, you must make a backup of the existing user files data using the **filemp** utility—see “Backing up user files before using utbconv” on page 821.

Example

This example converts files from Release 100 and use the input file `utable.def`.

```
utbconv 100 utable.def
```

UTBCONV definition file format

The definition file contains a line for each set of words to be migrated in each user file. The format of the lines is:

```
parameter file=file_num, rec=record_num, words=word_list
```

or

```
point file=file_num, rec=record_num, words=word_list
```

Part	Description
<i>file_num</i>	The number of the file where the point or parameter number is located.
<i>record_num</i>	The records to be converted, either all or a specific record number.

Part	Description
<i>word_list</i>	The words to be converted, which can include: • Specific words, for example: 5 or 5, 9. • Range A range of words, for example: 5-9.

Notes

- Comments can be inserted by placing a # at the start of the line.

Example

The following example migrates:

- Parameter numbers at words 2, 5, 6, 7, 8, 9, and 12 of record 5 of user table 3 (file 253)
 - Parameter numbers at word 2 or all records of user table 4 (file 254)
 - Point number at word 7 of record 6 of user table 5 (file 255)
- ```
example utbconv input file
#
parameter file = 253, rec=5, words=2, 5-9, 12
parameter file = 254, rec=all, words=2
point file = 255, rec=6, words=7
```

Note the free-format of input files and the ability to specify ranges of words and all records for specific files.

### Backing up user files before using utbconv

Before migrating user files using **utbconv**, you need to make a backup of the existing user files data using **fildmp**. For information on fildmp see the *Application Development Guide*.

**To back up, for example, records 1 to 10 of user file 1 to a file user\_file.dmp:**

- 1 Open a Command Prompt window, and type **fildmp**  
The system responds as follows:  
System status is ON-LINE  
Reading from memory. Writing to memory,disc,link.  
Enter FUNCTION: 1-dump, 2-restore, 3-compare
- 2 Type **1**  
The system responds with:  
Enter DEVICE/FILE name
- 3 Type **user\_file.dmp**  
The system responds with:  
Enter FILE number

**4 Type 251**

The system responds with:

Enter START,END record number

**5 Type 1,10**

The system responds with:

Enter FORMAT: "INT","HEX","ASC","FP"

**6 Type hex**

The system responds with:

File 251 record 1 dumped

File 251 record 2 dumped

File 251 record 3 dumped

File 251 record 4 dumped

File 251 record 5 dumped

File 251 record 6 dumped

File 251 record 7 dumped

File 251 record 8 dumped

File 251 record 9 dumped

File 251 record 10 dumped

Enter FILE number

**7 Press ENTER twice to exit from **fildmp**.**

---

## Configuration commands

The following commands and utilities can be used for a range of configuration purposes.

- `alglst`
- `bckbld`
- `dspbld`
- `hdwbckbld`
- `hdwbld`
- `hscconfig`
- `paswrđ`
- `pntbld`
- `qckbld`
- `rtusum`
- `station`
- Experion PKS Server Configuration Panel

## alglst

### Description

**alglst** lists the free algorithm blocks in the database.

### Syntax

`alglst`

### To run alglst:

- 1 Type **alglst**.  
The system responds with:  
Enter first algo block number
- 2 Type the lower limit of the range of algorithm block numbers in your system (usually 1).  
The system responds with:  
Enter the last algo block number
- 3 Type the upper limit of the range of block numbers.  
The system reports:
  - Any invalid algo block number
  - The numbers of free algo blocks

### Notes

- To run **alglst**, the database must be loaded, but the server software can be running or not running.
- If you want help, type **alglst -?**



## bckbld

### Description

**bckbld** is used to create a point definition file that reflects the current point configuration details in the server database. It is used, for example, when you have made changes to point configuration data via Station, rather than via Quick Builder or **pntbld**.

After creating a point definition file, you can upload it into a Quick Builder project. For details, see the Quick Builder help.

### Syntax

```
bckbld [-out file_name] [options]
```

| Part             | Description                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------|
| <i>file_name</i> | The name of the file to which the point definitions are written. By default the output goes to the screen. |

| Part           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>options</i> | <p>The options are:</p> <ul style="list-style-type: none"> <li>-fd Generates full dynamic parameter definitions.</li> <li>-gp Groups the output by points (but does not alphabetically sort the point IDs).</li> <li>-id <i>point_id</i> Only backbuilds the specified point.</li> <li>-nd Suppresses dynamic parameters.</li> <li>-ng Suppresses group definitions.</li> <li>-nh Suppresses history definitions.</li> <li>-np Suppresses point record definitions.</li> <li>-ns Suppresses output file sorting.</li> <li>-nt Suppresses trend definitions.</li> <li>-nu Suppresses point definitions for points not supported in Quick Builder.</li> <li>-rtu <i>rtu_number</i> Only backbuilds points on the specified controller. The default is to backbuild all points.</li> <li>-st Specifies output files sorting.</li> <li>-tag <i>tag_type</i> Only backbuilds points of the type specified by <i>tag-type</i>, which is: <ul style="list-style-type: none"> <li>• STA for status</li> <li>• ANA for analog</li> <li>• ACC for accumulator</li> <li>• CON for container</li> <li>• CDA for process</li> <li>• RDA for remote</li> <li>• PSA for flexible</li> </ul> </li> </ul> |

### Notes

- To run **bckbld**, the database must be loaded, but the server software does not need to be running.
- Quick Builder cannot upload a file created with the -ns option because it has history, trend, and group point build lines at the bottom of the file. Quick Builder requires all point build lines related to a point to be grouped together. If you want to upload the file, do not specify an option, or specify the -gp option.

- If more than 500 points are being built at the same time, **bckbld** may take a long time to sort the file. You can use the **-ns** (no-sort) or **-gp** (partial-sort) option to speed up the process.
- If you did not specify a PVSOURCE, the point will not be backbuilt in an rtu when using: **bckbld -rtu -out tmp.pnt**. To pick up the point use: **bckbld -out tmp.pnt**.

### Example

This example saves the point definitions for all points in a file called `point.txt`.

```
bckbld -out point.txt
```

### See Also

- “hdwbckbld” on page 829

## **dspbld**

### **Description**

**dspbld** starts Display Builder and opens a display or exports a display (system or custom).

For details, see the *Display Building Guide*.

## hdwbckbld

### Description

**hdwbckbld** is used to create a hardware definition file that reflects the current hardware configuration details in the server database. It is used, for example, when you have made changes to hardware and hardware connections via Station, rather than via Quick Builder or **hdwbld**.

After creating a hardware definition file, you can upload it into a Quick Builder project. For details, see the Quick Builder help.

### Syntax

```
hdwbckbld [-out file_name] [options]
```

| Part             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>file_name</i> | The name of the file to which the hardware definitions are written. By default the output goes to the screen.                                                                                                                                                                                                                                                                                                                                            |
| <i>options</i>   | -chn <i>chn_num</i> Backbuilds the specified channel.<br>-cnt <i>cnt_num</i> Backbuilds the specified controller.<br>-prt <i>ptr_num</i> Backbuilds the specified printer<br>-stn <i>stn_num</i> Backbuilds the specified Station<br>-chncnt <i>chn_num</i> Backbuilds the specified channel and controllers associated with that channel.<br>-cntchn <i>cnt_num</i> Backbuilds the specified controller and the channel to which the controller belongs |

### Notes

- To run **hdwbckbld**, the database must be loaded, but the server software does not need to be running.

### See Also

- “bckbld” on page 825

## hdwbld

### Description

**hdwbld** defines hardware and hardware connections in your system.

For most configuration tasks, the preferred engineering tool is Quick Builder, which generates the **hdwbld** input file and runs the utility.

For details about **hdwbld**, see the *Hardware and Point Build Reference*.

### Notes

- To run **hdwbld**, the database must be loaded, but the server software does not need to be running.
- Quick Builder does not fully support configuration for redundancy, and for redundant systems you need to use **hdwbld** directly. See “Configuring and monitoring a redundant server system” on page 463 for details.

## hscconfig

### Description

**hscconfig** is used to configure Windows-related features used by Experion, such as specialized accounts and permissions.

### Syntax

```
hscconfig [options]
```

| Option               | Description                                                 |
|----------------------|-------------------------------------------------------------|
| /addrights           | Sets the permissions of folders and files used by Experion. |
| /allpermissions      | Equivalent to /setpassword /addrights /dcom /services.      |
| /dcom                | Sets DCOM permissions.                                      |
| /displayshares       | Creates file shares for the display paths.                  |
| /removedcom          | Removes DCOM permissions                                    |
| /removedisplayshares | Removes the display path shares created by this command.    |
| /services            | Sets permissions for services.                              |

### Notes

- If you remove the display shares, Configuration Studio will not be able to alter some settings for the server, for example, operator records.

## paswrđ

### Description

**paswrđ** is used to change the passwords for Station security levels if you use Station-based security.

For details, see “Configuring Station-based security” on page 303.

### Notes

- To run **paswrđ**, the database must be loaded, but the server software does not need to be running.



## pntbld

### Description

**pntbld** is used to define points for the system.

### Notes

- You should use Quick Builder in preference to **pntbld** to define points.
- For details of creating or updating point definition files and running **pntbld**, see the *Hardware and Point Build Reference*.
- To run **pntbld**, the database must be loaded, but the server software does not need to be running.

# qckbld

## Description

**qckbld** starts Quick Builder and, if specified, opens a project.

## Syntax

qckbld [*filename*]

| Part            | Description                      |
|-----------------|----------------------------------|
| <i>filename</i> | The project file that is opened. |

## Notes

- This command should only be used when working with Quick Builder in offline mode.
- The folder in which Quick Builder is located must be specified. If you want to run the utility from the Command prompt, you must first change to the Quick Builder folder before running the command.

## rtusum

### Description

**rtusum** lists all points assigned to a particular controller. Control information for each point is also displayed.

### Syntax

```
rtusum controller_number [-v]
```

| Part                     | Description                              |
|--------------------------|------------------------------------------|
| <i>controller_number</i> | The number of the controller.            |
| -v                       | Shows the bit, width, format and imgsiz. |

### Notes

- To run **rtusum**, the database must be loaded, but the server software does not need to be running.

## station

### Description

**station** starts Station.

### Syntax

```
station [setupfile] [-d[n]] [-s[c][f][l][s][x]] [-t tracefile] [-z[1|2|3|f]]
```

| Part                | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>setupfile</i>    | The default Station setup file. If no file is specified, <code>default.stn</code> is used.                                                                                                                                                                                                                                                                                                                            |
| -d[n]               | The monitor number in which this instance of Station is visible.                                                                                                                                                                                                                                                                                                                                                      |
| -sc                 | Disables the <b>Connect</b> menu item.                                                                                                                                                                                                                                                                                                                                                                                |
| -sf                 | Disables window resizing so that Station can only operate in full screen mode and is always on top.                                                                                                                                                                                                                                                                                                                   |
| -sl                 | Disables window resizing so that Station can only operate in full screen mode and is always on the bottom.                                                                                                                                                                                                                                                                                                            |
| -ss                 | Disables the <b>Setup</b> menu item.                                                                                                                                                                                                                                                                                                                                                                                  |
| -sx                 | Disables the <b>Exit</b> menu item.                                                                                                                                                                                                                                                                                                                                                                                   |
| -t <i>tracefile</i> | The file to which trace data is copied.                                                                                                                                                                                                                                                                                                                                                                               |
| -z[n/f]             | The zoom level used when Station is started:<br>-z1 Starts Station at the largest window size for the current resolution.<br>-z2 Starts Station at the second largest window size for the current resolution.<br>-z3 Starts Station at the third largest window size for the current resolution<br>-zf Starts Station at Zoom to Fit zoom level.<br>If not specified, Station starts up with the Zoom to Fit setting. |

### Notes

- The folder in which Station is located must be specified. If you want to run the utility from the Command prompt, that you must first change to the Station folder before running the command.
- If you use Signon Manager or Electronic Signatures, you should use the -sl option so that the Signon Manager and Electronic Signatures dialog boxes appear on top of the Station Window.

**Example**

This example uses `opsetup.stn` as the setup file, `trace.txt` as the file for trace data, and disables window sizing and the **Exit** and **Setup** menu items.

```
station.exe opsetup.stn -sfxs -t trace.txt
```

## Experion PKS Server Configuration Panel

**Experion PKS Server Configuration Panel** is used to update the server settings for:

- The paths for system displays and custom displays (so that the server can get data from displays into the run-time database)
- The default path for event archives
- The default path for history archives
- The default path for restoring history archives
- The fast history setting
- The paper size used for reports
- The font used in reports
- Viewing the Experion license
- Making a license change



### Attention

Do not change the path for system displays.

---

### To run the Experion PKS Server Configuration Panel:

- 1 Choose **Start > Programs > Honeywell Experion PKS > Server > Experion PKS Server Configuration Panel**.
- 2 Click **Edit**.
- 3 Update the settings as required and click **OK**.

---

## Controller configuration commands

The following commands and utilities can be used for various controller configuration purposes:

- `hdwconfig`
- `tdc_cl`

For information about controller-specific utilities, including test utilities, see the associated Controller Reference. These references are available from Quick Builder's Help menu.

# hdwconfig

## Description

**hdwconfig** is used with TDC and UDC controllers. It enables the server’s configuration image for controllers and channels to be saved and restored to files.

## Syntax

To save channel or controller configuration data to a file:

```
HDWCONFIG SAVE file {-CHN cc| -RTU rr} [-RENEW]
```

To restore channel or controller configuration data from a file to the specified channel or controller with the same channel and controller:

```
HDWCONFIG RESTORE file {-CHN cc| cc-RTU rr} [-FROM nn]
```

To list channel and controllers whose configuration data is contained in the file:

```
HDWCONFIG LIST file
```

| Part        | Description                                                                        |
|-------------|------------------------------------------------------------------------------------|
| <i>file</i> | The file to which the data is saved/restored.                                      |
| <i>cc</i>   | The channel whose data is being saved/restored.                                    |
| <i>rr</i>   | The controller whose data is being saved/restored.                                 |
| -RENEW      | Saves data to an existing file.                                                    |
| -FROM       | Allows you to restore controller <i>nn</i> from the file to controller <i>rr</i> . |

## Notes

- To use the RESTORE option, the system must be running and the controllers must be disabled. See “Enabling and disabling channels and controllers” on page 156 for information on disabling controllers.

## Example

This example saves the configuration data for controller 21 to a file called box21.

```
hdwconfig save box21 -rtu 21
```



## tdc\_cl

### Description

**tdc\_cl** is used to compile CL programs ready for loading into an MC/AMC. (TDC 3000 Multifunction & Advanced Multifunction Controllers (MC/AMCs) can be programmed using CL to execute user-defined control strategies or custom functions.)

### Syntax

```
tdc_cl file [-d] [-x]
```

| Part        | Description                                            |
|-------------|--------------------------------------------------------|
| <i>file</i> | The name of the CL source file (with a .cl extension). |
| -d          | Compiles source lines beginning with %DEBUG            |
| -x          | Generates reference data during compilation.           |

## Diagnostic commands

The following commands and utilities can be used for server diagnostics:

- display
- lisscn
- listag
- tail
- trace

For controller diagnostics, see to the associated Controller Reference. These references are available from Quick Builder's Help menu.

As an alternative to using these diagnostic commands, you can use the Diagnostic Capture Tool. For more information see the *Server and Client Troubleshooting Guide*.

# chkem

**chkem** checks the integrity of the enterprise model on your system and fixes any identified problems.

## Syntax

chkem [options]

| Part | Description                                                   |
|------|---------------------------------------------------------------|
| /?   | Displays help for this command.                               |
| /all | Applies all available integrity checks to the running system. |

## Notes

- This command should be run only if you notice inconsistencies in the enterprise model, for example, if the alarm counts are incorrect.
- To run this command, the database must be loaded, but the server software does not need to be running.

# display

**display** gives a description of the specified error code.

## Syntax

`display error_code`

| Part              | Description                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <i>error_code</i> | The number of the server error code for which you want more information.<br><br>If the error code is hexadecimal, prefix it with 0x. |

## Notes

- To run this command, the database must be loaded, but the server software does not need to be running.

## Example

This example displays the description for hexadecimal error code 0106.

`display 0x0106`

# lisscn

## Description

**lisscn** lists the following configuration details:

- The scan packets in each scan period (interval)
- The number of scan packets per scan period
- The scan packets per period per second

## Syntax

`lisscn [options]`

| Part                    | Description                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------|
| -ALL                    | Lists all scan packets (default).                                                                 |
| -FM <i>n</i>            | Specifies the first point number in the list.                                                     |
| -OUT <i>file_name</i>   | The file to which the results are written.<br>The default is to display the output on the screen. |
| -INT <i>interval_no</i> | Lists scan packets by scan period number.                                                         |
| -RTU <i>rtu_number</i>  | Lists scan packets by controller number.                                                          |
| -TO <i>n</i>            | Specifies the last point number in the list.                                                      |
| -CHN <i>channel_no</i>  | Lists scan packets by channel number.                                                             |
| -all_add                | Lists all addresses in the scan packet.                                                           |
| -all_ref                | Lists all references to an address.                                                               |

## Notes

- To run **lisscn**, the database must be loaded, but the server software does not need to be running.

## listag

### Description

**listag** lists the points currently configured in the database.

### Syntax

**listag** [*options*]

| Part                  | Description                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------|
| -OUT <i>file_name</i> | The file to which the results are written.<br>The default is to display the output on the screen. |
| -ALL                  | Lists all point types (default).                                                                  |
| -FM <i>n</i>          | Specifies the first point number in the list.                                                     |
| -ND <i>n</i>          | Specifies the width of the point description column. The default is 30 characters.                |
| -NW <i>n</i>          | Specifies the width of the point name column. The default is 16 characters.                       |
| -TO <i>n</i>          | Specifies the last point number in the list.                                                      |

### Notes

- To run this command, the database must be loaded, but the server software does not need to be running.
- If you just type **listag**, you are prompted to specify the point type and a range of point numbers.

# tail

## Description

**tail** displays the last few lines of a log file (typically, the server log file, log.txt.)

## Syntax

```
tail [-f] file
```

| Part | Description                                                                                      |
|------|--------------------------------------------------------------------------------------------------|
| -f   | Runs <b>tail</b> indefinitely.<br>To stop the utility, press CTRL+C.                             |
| file | The name of the log file, for example, Program Files\Honeywell\Experion PKS\server\data\log.txt. |

## Note

The most recent messages are stored in Program Files\Honeywell\Experion PKS\server\data\log.txt. When this file reaches its maximum size (2 MB), a new file is created and the old one is:

- Moved to Program Files\Honeywell\Experion PKS\server\data\logfiles
- Renamed with a date/time extension (For example, the log moved on 23 October 2001, at 8:38am, would be renamed logY2001M10D23H08M38.txt.)

## trace

### Description

**trace** is used to record communications activity for Stations and channels.

### Syntax

```
trace [-c] | [-q] | [lrn1 [-L lrn2] [-Mmem_size]]
```

| Part            | Description                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------|
| -c              | Continuously output trace information. To stop press CTRL+BREAK.                                                                  |
| -q              | Queries the current trace status. Lists the LRNs being traced and the <i>mem_size</i> .                                           |
| <i>lrn1</i>     | First LRN that is traced.                                                                                                         |
| <i>lrn2</i>     | Second LRN that is traced.                                                                                                        |
| <i>mem_size</i> | The amount of trace captured, in KB (default 100 KB). When the size limit is reached the oldest trace information is overwritten. |

### Notes

- To start a trace, the database must be loaded and the server must be running.
- To stop a trace, type **trace 0**.
- To dump captured information, type **trace**.
- To calculate the LRN to trace a channel, use the formula **49 + 2 \* channel number**.
- To calculate the LRN to trace a Station, use the formula **300 + Station number**.

### Example

This example start a trace for LRN 69 with 512 KB buffer.

```
trace 69 -M512
```

This example starts a trace for both communications links for an FS90 channel on channel 2 with 1M memory usage.

```
trace 53 -L54 -M1024
```

This example starts a trace for Station number 1.

```
trace 301
```



### Viewing the trace buffer contents

If you want to view the contents of a trace buffer after you have stopped a trace, you can redirect the output of the trace command to a file. For example, to save it to a file called “trace.dmp”, type **trace > trace.dmp**.

You can then use a text editor to view the contents of the file.

## Administration commands

The following commands and utilities can be used for administrative tasks:

- `hscserver /start`
- `hscserver /stop`
- `dspclr`
- `hisint`
- `usrlrn`
- `tagflb`

## **hscserver /start**

### **Description**

**hscserver /start** starts Experion.

For more information, see the *Experion Startup and Shutdown Guide*.

## **hscserver /stop**

### **Description**

**hscserver /stop** stops Experion.

For more information, see the *Experion Startup and Shutdown Guide*.

## dspclr

### Description

#### dspclr:

- Removes displays from the Display Summary
- Clears specified displays

### Syntax

```
dspclr [first_display] [last_display] [-y]
```

| Part                 | Description                                           |
|----------------------|-------------------------------------------------------|
| <i>first_display</i> | The number of the first display that is removed.      |
| <i>last_display</i>  | The number of the last display that is removed.       |
| -y                   | Removes the displays without requesting confirmation. |

### Notes

- **dspclr** only applies to numbered displays.

### Example

This example clears displays numbered between 400 and 450 without confirmation.

```
dspclr 400 450 -y
```

## hisint

### Description

**hisint** deletes all history and event data from the server database.

### Syntax

**hisint** [*options*]

| Part              | Description                                                              |
|-------------------|--------------------------------------------------------------------------|
| -SILENT           | Executes without prompting.                                              |
| -PRESERVE         | Preserves the file's contents.                                           |
| <i>database</i>   | Restores history/events from the specified database.                     |
| -R <i>nnn</i>     | Experion's release number. Required if you are restoring history/events. |
| -DIAG             | Displays diagnostic messages.                                            |
| -HISTORY <i>n</i> | Initialize only History file <i>n</i> .                                  |
| -EVENT            | Initialize only the Event file.                                          |
| -DELAY            | Initialize only the Delay file.                                          |
| -SOE              | Initialize only the SOE file.                                            |

### Notes

- To run **hisint**, ensure that:
  - All history that you want to keep has been archived
  - The server is stopped
  - The database is loaded
- To see a list of options, type **hisint -?**.

## usrln

### Description

**usrln** displays logical resource numbers (LRNs) that are available between 111 and 150.

### Syntax

**usrln** [*options*]

| Part     | Description                                                                                       |
|----------|---------------------------------------------------------------------------------------------------|
| -a       | Lists all unassigned LRNs.                                                                        |
| -h or -? | Lists the options and their usage.                                                                |
| -p       | Lists LRN, process ID, task name and any associated device for assigned LRNs between 111 and 150. |
| -u       | Lists all used LRNs between 111 and 150.                                                          |

### Notes

- To find out which LRNs are available for a new application, type **usrln**.
- To find out the process IDs for all assigned LRNs, type **usrln -p -a**.

## tagflb

### Description

**tagflb** builds the index that Experion uses look up named objects such as points, channels, controllers, and so on.

### Syntax

tagflb

### Notes

- To run **tagflb**, ensure that:
  - The server is stopped
  - The database is loaded
- Any errors in creating the index are displayed. They must be rectified for correct operation of the server.



---

## Database initialization commands

These commands and utilities are used to initialize the database:

- pntdel
- almint



### Caution

Do not run these commands/utilities unless you are absolutely sure that you want to remove the information from your Experion database.

---

For other database initialization commands, see the technical notes that come with Experion.

## pntdel

### Description

**pntdel** deletes all channel, controller, and point configuration from the server database.



### Caution

If you delete the configuration data, it cannot be recovered without completely rebuilding the data. History data will also be lost.

---

### Syntax

```
pntdel
```

### Notes

- To run **pntdel**, ensure that:
  - The server is stopped
  - The database is loaded
- When you run **pntdel**, you are prompted to initialize:
  - Point configuration
  - Hardware (channel and controller) configuration
  - User-defined data formats
- Depending on the database size and hardware platform, deleting all points might take some time.

# almint

## Description

**almint** initializes the Alarm Summary queue.



### Caution

Running **almint** will delete the contents of the alarm summary queue from the Experion database.

It does not, however, remove the alarms from the event file.

---

## Syntax

`almint [-point] [-nopoint] [-force]`

| Part     | Description                               |
|----------|-------------------------------------------|
| -point   | Clears the alarm state of all points.     |
| -nopoint | Does not clear the alarm state of points. |
| -force   | Forces execution on a running system.     |

---

## Application development commands

The following commands and utilities are primarily used for application development purposes. However, they are also useful for some configuration and administration tasks:

- fildmp
- fileio
- taglog

For information on these commands see the *Application Development Guide*.

# Glossary

## **accumulator point**

A *point* type used to represent counters. Information contained in the accumulator point can include: the raw value, a process value, a rollover value, a scale factor, and a meter factor.

## **acronym**

A text string used on a display to represent a state or a value in a form that is convenient for operators. For example, a value of “0” for a point parameter in the database might be represented on a system status display by the acronym “Stopped”.

## **action algorithm**

One of two types of algorithm you can assign to a point in order to perform additional processing to change point parameter values. An action algorithm performs an action when the value of the PV changes. Contrast with *PV algorithm*.

## **ActiveX component**

An ActiveX component is a type of program designed to be called up from other applications, rather than being executed independently. An example of an ActiveX component is a custom dialog box, which works in conjunction with *scripts*, to facilitate operator input into *Station*.

## **alarm**

An indication (visual and/or audible) that alerts an operator at a Station of an abnormal or critical condition. Each alarm has a type and a *priority*. Alarms can be assigned either to individual points or for system-wide conditions, such as a controller communications failure. Alarms can be viewed on a Station display and included in reports. Experion classifies alarms into the following types:

- PV Limit
- Unreasonable High and Unreasonable Low
- Control Failure
- External Change

**alarm group**

A group of assets and points that are otherwise unrelated to one another in the asset model, grouped together for the purpose of alarm monitoring and management.

**alarm/event journal**

A file that records all alarms and events. It is accessed to generate reports and can also be archived to off-line media.

**alarm priority**

One of four levels of severity specified for the alarm. The alarm priorities from least to most severe are:

- Journal
- Low
- High
- Urgent

**algorithm**

See *point algorithm*.

**analog point**

A point type that is used to represent continuous values that are either real or integer. Continuous values in a process could be: pressure, flow, fill levels, or temperature.

**ANSI**

American National Standards Institute

**API**

Application Programming Interface.

**application program**

A user-written program integrated into Experion using the Application Programming Interface (API).

**asset**

(Previously called area.) A representation of entities such as plant equipment, facilities, buildings. Operators or Stations can be assigned access to particular assets only.

**automatic checkpointing**

In a redundant server system, the automatic transfer of database updates from the primary server to the backup server.

**auxiliary parameter**

An analog point parameter in addition to PV, SP, OP, and MD. Up to four auxiliary parameters can be used to read and write four related values without having to build extra points.

**bad value**

A parameter value, (for example, PV), that is indeterminate, and is the result of conditions such as unavailable input.

**client software**

An umbrella term covering Quick Builder, Station, and Display Builder software.

**channel**

The communications port used by the server to connect to as controller. Channels are defined using the Quick Builder tool.

**CIM**

Communications Interface Module

**collection**

A collection is a set of named values or *display objects* that are used in *scripts*.

**Control Builder**

The control building software for the Honeywell Experion Process Controller.

**control failure alarm**

For *analog* and *status* points, an *alarm* configured to trigger if a *demand scan* on the source address of an OP, SP, MD, or other parameter finds that the value after a control is issued does not match the controlled value.

**control level**

A security designation assigned to a *point* that has a destination address configured (for analog or status points only). A control level can be any number from 0 to 255. An operator will be able to control the point only if they have been assigned a control level equal to, or higher than, the point control level.

**control parameter**

A point parameter defined to be used as a control. A control parameter has both a source and a destination address. The destination for the parameter value is usually an address within the controller. Control parameters can be defined as automatic (server can change) or manual (operator can change).

**controller**

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.

Controllers can be defined using the Quick Builder tool. Some controllers can be configured using Station displays.

**database controller**

See *User Scan Task controller*.

**database point**

Any *point* that has one or more parameters with database addresses.

**DCD**

Data Carry Detect.

**DCS**

Digital Control System.

**DDE**

Dynamic Data Exchange.

**default**

The value that an application automatically selects if the user does not explicitly select another value.

**deleted item**

In Quick Builder, an item that has been flagged for deletion from the server database and appears in the Recycle Bin grouping. When a download is performed, the item is deleted from both the server database and the Quick Builder project database.

**demand scan**

A one-time-only scan of a point parameter that can be requested either by an operator, a report, or an application.

**DHCP**

Dynamic Host Configuration Protocol.

**display**

Station uses displays to present Experion information to operators in a manner that they can understand. The style and complexity of displays varies according to the type of information being presented.



Displays are created in *Display Builder*.

**Display Builder**

The Honeywell tool for building customized graphical displays representing process data.

**display object**

A display object is a graphic element, such as an alphanumeric, a push button or a rectangle, in a *display*.

Display objects that represent point information (such as an alphanumeric) or issue commands (such as a push button) are called “dynamic” display objects.

**Distributed System Architecture (DSA)**

An option that enables multiple Experion servers to share data, alarms, and history without the need for duplicate configuration on any server. This is the preferred method for transferring data between servers in large systems.

**DNS**

Domain Name System.

**DSR**

Data Signal Ready.

**DTE**

Data Terminal Equipment.

**DTR**

Data Terminal Ready.

**dual-bit status point**

A status point that reads two bits. Status points can read one, two or three bits.

**EIM**

Ethernet Interface Module.

**ELPM**

Ethernet Loop Processor Module.

**electronic signature**

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

**EMI**

Electromagnetic Interference.

**event**

A significant change in the status of an element of the system such as a point or piece of hardware. Some events have a low, high, or urgent priority, in which case they are further classified as alarms. Events can be viewed on an operator Station display and included in reports.

Within the context of *scripts*, an event is a change in system status or an operator-initiated action that causes a *script* to run.

**Event Archiving**

Every event, such as point status change or an operator action, is stored in an event journal. The online event journal is only capable of storing a certain number of events. With Extended Event Archiving you can archive these events to disk and tape, where they may be stored for future retrieval.

**exception scan**

A scan that takes place only when a change occurs at a controller address configured for a point parameter. Some controllers can notify the server when a change occurs within the controller. The server uses exception polling to interrogate the controller for these changes. This type of scan can be used to reduce the scanning load when a fast periodic scan is not required.

**export**

In relation to Station displays, the process of registering a *display* with the *server* so that it can be called up in *Station*.

In relation to Quick Builder, the process of converting the configuration data in a project file into text files for use with other applications.

**extended history**

A type of history collection that provides snapshots of a point at a designated time interval that can be:

- 1-hour snapshots
- 8-hour snapshots
- 24-hour snapshots

**fast history**

A type of history collection that records 1-30-second snapshot history for points.

**field address**

The address within the controller that contains stored information from a field device being monitored by the controller.

**flexible point**

A point on a point server. The database structure of a flexible point is determined by the point server, rather than by Experion.

**free format report**

An optional report type that enables users to generate their own report.

**FTP**

File Transfer Protocol.

**history**

Point values stored to enable tracking and observation of long-term trends. Analog, status, and accumulator point PVs can be defined to have history collected for them. Three types of history collection are available:

- Standard
- Extended
- Fast

**history gate**

A status point parameter that is used to control the collection of history for an analog or status point. The history is only collected if the gate state value of the nominated parameter is in the nominated state.

**host server**

In a DSA system, the server on which a remote point's definition is stored and from which alarms for the point originate.

**HTTP**

Hypertext Transfer Protocol.

**HVAC**

Heating, Ventilation, and Air Conditioning.

**IEEE**

Institute of Electrical and Electronic Engineers.

**input value**

Values that are usually scanned from the *controller* registers but can be from other server addresses. Input values can represent eight discrete states. Up to three values can be read from an address in order to determine a state.

**IRQ**

Interrupt Request.

**item**

In Quick Builder, the elements necessary for data acquisition and control that comprise the Experion server data and are defined in the project file. These are:

- Channels
- Controllers
- Stations
- Points
- Printers

**item grouping**

A collection of items grouped by a common property.

**item list**

In Quick Builder, a listing of the items defined in the project file that displays in every Project View. The item list can be used to find an item and then display its properties.

**item number**

Item numbers are used in the server database to identify items. In Quick Builder, the number is assigned to an item internally. The item numbers for channels, controllers, Stations and printers can be overwritten in Quick Builder to match an existing system database.

**LCS 620**

Logical Control System 620. Honeywell's programmable logic controller.

**local display object**

A dynamic *display object* that displays information or issues a command, but which is not linked to the *server*. Such display objects are used in conjunction with *scripts*.

**local server**

The server to which the operator's station is connected.

**MCI**

Media Control Interface.

**MD**

Experion abbreviation for *mode*.

**Microsoft Excel Data Exchange**

A network option that can be used to capture the most recent point and history information in the server and display it in Microsoft Excel spreadsheets, mainly for reporting.

**Mode**

A point parameter which determines whether or not the operator can control the point value. For example, in a status point, the mode determines whether the operator can control the output value, and in an analog point the mode determines the control of the setpoint. If the mode is set to manual, the operator can change the value.

**Network Node controller**

A server running the system software defined as a controller to another server running the system software. The local server can scan and control points that have been defined in the remote Network Node controller.

**notification**

An event or alarm.

**ODBC**

See *Open Database Connectivity*.

**ODBC driver**

A driver that processes ODBC (Open Database Connectivity) calls, queries the database, and returns the results. See also *Open Database Connectivity*.

**OP**

Experion abbreviation for *output*.

**Open Database Connectivity**

A standard set of function calls for accessing data in a database. These calls include the facility to make SQL (Structured Query Language) queries on the database. To use ODBC you must have support from the client application (for example, Microsoft Access) which will generate the ODBC calls and from some database-specific software called an *ODBC driver*.

**Operating Group**

A group of up to eight arbitrarily chosen points that can be viewed by an operator on a standard Station display. An Operating Group can be defined in Quick Builder or in Station.

**operator ID**

A unique identification assigned to each operator. If Operator-Based security is enabled, the operator must use this ID and a password to sign on to a Station.

**operator password**

A character string (not echoed on screen) used with the operator ID to sign on to an operator Station.

**operator security level**

See *security level*.

**Operator-Based security**

Operator-Based security comprises an operator ID and password, which must be entered at an operator Station in order to access Experion functions.

**output**

A *point* parameter used to issue control values. The output (OP) is often related to the mode (MD) parameter and can be changed by an operator only if the mode is manual.

**parameter**

The different types of values accessed by *points* are known in Experion as “point parameters.”

The main point parameters are process variable (PV), output (OP), set point (SP), and mode (MD).

Experion can store and manage multiple values in the one point. You can therefore use a single point to monitor and control a complete loop. In many cases, however, the only parameters of a point that need to be configured are:

- The PV which shows the current value of a given location within a controller, and
- An OP used to reset or control a point

The names of the parameters reflect their most common usage. They can, however, be used to hold any controller values.

Point servers can have descriptive parameter names, depending on the type of data.

**periodic scan**

A defined regular interval in which the server acquires information from the controller and processes the value as a point parameter. The scan period must be defined in Quick Builder for each point source parameter value.

**PIN**

Plant Information Network

**PLC**

See *Programmable logic controller*.

**point**

A data structure in the server database, usually containing information about a field entity. A point can contain one or more *parameters*. A point is classified by type: status, analog, accumulator or flexible (point server points).

Experion uses different point types to represent a range of different field values. The point types themselves can be of either a flexible or fixed structure depending on the type of controller they are associated with. Flexible structure points are used for the Experion Process Controller and fixed structure points are used with all other controllers.

The fixed point types are:

- Status
- Analog
- Accumulator

**point algorithm**

A prescribed set of well-defined rules used to enhance a point's functionality. The point algorithm accomplishes this by operating on the point data either before or after normal point processing.

There are two types of point algorithms, PV (processed every time the point parameter is scanned) and Action (processed only when a point parameter value changes).

**Point Detail display**

A display that shows the current point information. Each point has a Point Detail display.

**point server**

A point server is a high-level interface that allows Experion to exchange data with another application or sub-system without the need for separately defining points in Experion.

The database structure of a point on a point server (flexible point) is determined by the application/sub-system, rather than by Experion.

**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 software**

An umbrella term for Control Builder and other process software.

**process variable**

An actual value in a process: a temperature, flow, pressure, and so on. Process variables may be sourced from another parameter and may also be calculated from two or more measured or calculated variables using algorithms. Status points have a PV of the current state (0 to 7) (eight possible states).

**programmable logic controller (PLC)**

A control and monitoring unit that connects to a field device and controls low-level plant processes with very high-speed responses. A PLC usually has an internal program that scans the PLC input registers and sets the output registers to the values determined by the program. When connected to the server, the input and output values stored in the PLC registers can be referenced, and the server can read and write to these memory addresses.

**project**

In Quick Builder, a working database file that enables you to make changes to the server database without affecting the configuration data that is currently being used to run the system.

**project view**

In Quick Builder, a window in which you can view, add, and modify any items in the current project file.

**PV**

Experion abbreviation for *process variable*.

**PV algorithm**

One of two types of algorithm you can assign to a point in order to perform additional processing to change point parameter values. A PV algorithm changes the value of the point process value (PV) input only. Contrast with *Action algorithm*.



**PV clamp**

For an analog point, a configuration that will immobilize the process value (PV) at 0% if it falls below the entry low limit value or at 100% if it goes above the entry high limit value.

**PV period**

An amount of time specified for the scanning of the point process value (PV) parameter. The PV period determines the frequency with which the scan will be performed by the server. The server groups point addresses into scan packets by PV period and controller.

**Quick Builder**

Quick Builder is a graphical tool that is used to define the hardware items and some point types in an Experion system. Quick Builder can run either on an Experion server, on another computer in your system, or on a laptop.

After defining hardware and points with Quick Builder, you download these definitions from Quick Builder to the Experion server database.

**recipe**

A set of points used in a process. The Recipe Manager option enables point parameters for sets of points to be downloaded with pre-configured working values. The individual point parameters are the recipe “ingredients.”

**redundant server**

A second server actively linked to the primary server and used as a backup system. Active linking ensures that data in the second server is constantly updated to mirror the primary server.

**remote server**

A server that supplies data to a local server over either a local area network (LAN) or a wide area network (WAN).

**report**

Information collected by the server database that is formatted for viewing. There are several pre-formatted reports, or the user can customize a report. Reports may be generated on demand or at scheduled intervals. Reports can be printed or displayed on an operator Station.

**REX**

Request to exit.

**RFI**

Radio Frequency Interference.

**RLSD**

Receive Line Signal Detect.

**RTS/CTS**

‘Request to send’/‘clear to send’.

**RTU**

See *controller*.

**S9000**

Series 9000 controller.

**SafeBrowse object**

A SafeBrowse object is a Web browser specifically designed for use with *Station*. SafeBrowse includes appropriate security features that prevent users from displaying unauthorized Web pages or other documents in Station.

**scan**

The technique used to read data from a controller. Scans are conducted for point parameters with source addresses (for example, PV, SP, OP, MD, An). Experion uses demand, exception, and periodic scanning techniques.

**scan packet**

A group of point parameter source addresses assembled by the server and used as the basic unit of server data acquisition. The server groups points into scan packets based on the controller address that they reference and the scan period defined.

**scan period**

The time interval that specifies the frequency at which the Experion server reads input values from the memory addresses of controllers. Scan periods are measured in seconds; a scan period of 120 seconds means that the server scans the controller once every 120 seconds.

**scheduler**

A facility used to schedule the control of a point on either a periodic or once-only basis.

**script**

A script is a mini-program that performs a specific task. In displays, for example, scripts are often used to produce animations.

**security level**

Access to Experion functions is limited by the security level that has been assigned to each operator. Experion has six security levels. An operator is assigned a security level and may perform functions at or below the security level that has been assigned to that operator.

**server**

The computer on which the Experion database software runs.

**Server software**

An umbrella term used to refer to the database software and server utilities installed on the Experion server computer.

**server Station**

A computer running both the Experion database (server) software and the Station software.

**setpoint**

The desired value of a process variable. Setpoint is a point parameter, whose value may be entered by the operator. The setpoint can be changed any number of times during a single process. The setpoint is represented in engineering units.

**shape**

A shape is a special type of *display object* that can be used in numerous *displays*. Shapes can be used as “clip-art” or as *shape sequences*.

**shapelink**

A shapelink is, in effect, a “window” which always displays one *shape* of a *shape sequence*. For example, a shapelink representing a point’s status displays the shape that corresponds to the current status.

**shape sequence**

A shape sequence is a set of related shapes that are used in conjunction with *shapelinks*. A shape sequences can be used to:

- Represent the status of a point (Each shape represents a particular status)
- Create an animation (Each shape is one “frame” in the animation)

**SOE**

Sequence of events.

**softkey**

A softkey is a function key which, when pressed, performs an action specified in the configuration details for the current *display*.

**SP**

Experion abbreviation for *set point*.

**Standard history**

A type of history collection for a point that provides one-minute snapshots and the following averages based on the one-minute snapshots:

- 6-minute averages
- 1-hour averages
- 8-hour averages
- 24-hour averages

**Station**

The main operator interface to Experion. Station can run on either a remote computer through a serial or LAN link, or the server computer.

When Station is running on the server computer, it is often referred to as a *server Station*. When it is running on a machine other than the server, it is often referred to as an operator Station.

**Station Automation object model**

The Station Automation object model provides the programming interface through which *scripts* control *Station* and its *displays*.

**status point**

A point type used to represent discrete or digital field values. The point can have input, output, and mode values. Input values can represent eight discrete states and cannot be changed by an operator. Up to three values can be read from up to three consecutive, discrete locations in the controller and thus can represent up to 8 states.

Output values can be used to control up to two consecutive discrete locations in a controller. Output values can be automatic or operator-defined.

Mode values apply to output values and determine whether or not the output value is operator-defined or automatic.

**supervisory control**

The action of writing information to a controller. Experion enables both automatic and manual supervisory control. See *Mode*.

**tagname**

A unique name for a point or an asset. A tagname is also referred to as a point ID or asset name.

**task**

A task is any of the standard server programs or an application program that can be invoked from a *display*.

**TCP/IP**

‘Transmission Control Protocol’/‘Internet Protocol’. A standard network protocol.

**TDC 3000**

Total Distributed Control 3000 (Honeywell’s Digital Control System.)

**terminal server**

A device on the local area network (LAN) that connects to a controller by way of a serial connection and enables the controller to “talk to” the Experion server on the LAN.

**timer**

A timer is a programming mechanism for running *scripts* at regular intervals in *Station*.

**Trend Set**

A set of point parameter historical data, usually shown as a graph on a standard Station display. Trend sets can be defined using Quick Builder or a Station display.

**UDC**

Universal Digital Controller.

**Unreasonable High and Unreasonable Low alarms**

Alarms configured for an unreasonably high value and an unreasonably low value for the PV of an analog point.

**URL**

Uniform Resource Locator. For example, a Web address.

**User Scan Task controller**

A server software option used to configure a server database table (called a “user file”) to act as a controller. The server interfaces with the user file rather than the actual device.

In this way you can write software to interface with the server and to communicate with devices that are connected to, but not supported by, the Experion server. The Experion server can then scan data from the user files into points configured on the User Scan Task controller and, for control, the Experion server can write point control data to the user file or a control queue.

**utility**

Experiion programs run from a command line to perform configuration and maintenance functions; for example, the **lisscn** utility.

**virtual controller**

See *User Scan Task controller*.

**WINS**

Windows Internet Name Service.

**WWW**

World Wide Web.

# Index

## A

- accumulator point
  - described 166
  - meter factor 185
  - parameters 178
  - PV 183
  - range high value 185
  - rollover value 184
  - scale factor 185
- acronyms, for security levels 348
- action algorithms 236
- addresses, defining for points 195
- aggregate alarming, about 256
- Alarm and Event reports 400, 409
- Alarm Duration reports 400, 413
- alarm groups, about 256
- alarm pager
  - holiday schedule 275
  - nominating alarms 276
    - by asset 277, 278
    - individual point alarms 276
  - nominating alerts 278
    - individual alert conditions 278
  - paging service providers 269
  - system alarms 276
- alarm paging 265
- Alarm Summary
  - customizing 393
  - filtering 383
  - overflow 251
  - printing 397
  - sorting 392
- alarms
  - about 207
  - accumulator point alarm types 214
  - acknowledgement synchronization 552
  - acknowledgements, addresses 210
  - aggregate alarming 256
  - alarm groups 256
  - analog point alarm types 211
  - colors, customizing 253
  - communications failures 147
  - container points 380
  - control fail alarms
    - analog points 206
    - status points 204
  - controller alarm limits, tracking 228
  - customizing colors 253
  - deadbands, defining 212
  - deviation alarms 206
  - distributed system architecture 507
  - enabling and disabling 250
  - enabling and disabling in a distributed system
    - architecture 507
  - external 247
  - external change
    - analog points 212
    - description 210
    - status points 210
  - filtering the Alarm Summary display 383
  - from remote servers 507
  - journal 208
  - limits, configuring 214
  - message text, configuring 243
  - precedence of 249
  - priorities 208
  - PV fail alarms
    - analog points 206
    - status points 204
  - PV limit alarms, analog points 211
  - server-wide configuration 250
  - sub-priorities 208
  - suppressing deviation 206
  - time stamps 391
  - types for points 209
  - unanswered alarms 248
  - unreasonable highs and lows 212
- alerts
  - about 245
  - configuring 245
- alglst command 238, 824
- algorithm

- analog point notification request 236
- cyclic task request 236
- maximum/minimum 236
- piecewise linearization 236
- run hours 235
- status point notification 236
- value transportation 236
- algorithms 235
  - action 236
  - blocks
    - listing free blocks 238
    - listing used blocks 416
  - classes 235
  - container points 380
  - defining with Quick Builder 237
  - distributed system architecture 512
  - listing free blocks 824
  - PV 235
  - remote points 512
  - sources of information on 237
  - used to disable and enable alarms 250
  - using Station to view details 237
- All Areas list 333
- All Hours area time period 334
- almint 859
- analog point
  - auxiliary value 182
  - described 166
  - external change alarms 212
  - mode value 181
  - OP 181
  - output value 181
  - process variable 179
  - PV 179
  - setpoint value 182
  - SP 182
- analog point notification request algorithm 236
- API (Application Programming Interface) 799
- Application Program Request, configuring report for 404
- Application Programming Interface (API) 799
- arbitration for redundant servers 477
- archive directories, history 219
- archiving
  - event *See* Event Archiving
  - history configuring 218
- asset
  - lists 333
  - profiles

- configuring 335
  - system-defined 335
  - time periods 334
- assets
  - about 40
  - assigning to operators 340
  - assigning to Stations 338
  - associating points 171
  - controlling access 336
  - hierarchies 41
  - naming rules 42
  - scope of responsibility 336
  - time periods
    - system-defined 334
- assignable assets 44
- associated display
  - configuring with Quick Builder 222
  - configuring with Station 87
- associated Stations 87
- auxiliary parameters
  - configuring 228
  - tracking controller alarm limits 228

## B

- barometer 147
- batch reports, configuring 419
- batch reports, running automatically 626
- bckbld command 825

## C

- cache point 503
- calculations, using free format reports 432, 436
- channels 146
  - configuration displays 159
  - enabling and disabling 156
  - Stallion EasyConnection Adapter 150
  - status and error statistics 158
- checkpoints, in redundant server systems 486
- clamp point 180
- command reference 815
- commands
  - SQL checking 681
- commands and utilities
  - alglst 824
  - almint 859
  - bckbld 825



- config 840
- Configuration Panel 838
- display 844
- dspblid 828
- dspclr 853
- hdwbckbld 829
- hdwbld 830
- hscint 854
- hscserver/start 851
- hscserver/stop 852
- lissen 845
- list of 815
- listag 846
- paswrld 832
- pntbld 833
- pntdel 858
- qckbld 834
- rtusum 835
- running 816
- station 836
- sysbld 818
- tagflb 856
- tail 847
- tdc\_cl 841
- trace 848
- usrln 855
- utbconv 820
- communications
  - activity 848
  - error statistics 158
  - failure alarms 147
  - monitoring status 147, 158
  - redundancy 148
  - statistics barometer 147
- composite alarm algorithm 236
- config 840
- configuration
  - procedures checklist 34
- Configuration Panel 838
- Configuration Studio 30
  - remote access 579
- configuration tools 30
  - remote access 580
- Console Extension Stations, adding 536
- Console Stations
  - about 522
  - alarm acknowledgement
    - synchronization 552
  - configuring 527

- configuring LEDs 533
- configuring operator-based security 525
- connection properties 534
- database replication 524
- deleting 535
- file replication 524
- security 525
- consoles
  - about 540
  - configuring LEDs 548
- consoles, configuring 543
- container points 379
  - algorithms 380
  - described 166
  - template display 379
- control
  - configuring point control 200
  - confirmation 195
  - control limits explained 205
  - deadbands 205
  - fail alarms
    - analog points 206
    - status points 204
  - levels 202
  - modes 199, 201
  - scheduling 610
  - specifying reverse output 200
  - timeout 203
- control fail alarms
  - status points 204
- controller configuration displays 159
- controllers 146
  - alarms for 147
  - connection types 146
  - enabling and disabling 156
  - viewing points configured for 160
- copying user files. See file replication
- create input reference file 679
- Cross Reference reports 400, 415
- custom applications, developing 799
- custom displays 234
- Custom Trend display 368
- cyclic task request algorithm 236

## D

- data formats
  - user-defined 229
- data links for redundant servers 479

- data source name, ODBC Data Exchange reports 675
- database
  - configuring items 818
- database points
  - addresses 226
  - described 166
- database reference 679
- deadbands
  - alarm 212
  - control 205
  - drift 179
- defmodes.src file, restoring to enable default modes 137
- demand scanning 197
- derived points, building 168
- destination address for points 195
- Detail Trend display 367
- disabling channels and controllers 156
  - security level required 347
- Display Builder
  - remote points in 515
- display command 844
- displays
  - adding aggregate alarming information 258
  - adding system performance data 61
  - custom 234
  - redundant configuration 486
  - reloading 234
  - removing from the Display Summary 853
- distributed system architecture
  - alarm message indexes 508
  - alarms 507
  - algorithms 512
  - cache points 503
  - configuration requirements 501
  - data location 503
  - disabling alarms 507
  - point IDs 503
  - remote areas 503
  - remote points 503
  - remote points in Display Builder 515
  - security 511
  - subscription 503
  - system overview 499
  - trend sets 510
- drift deadbands 179
- DSA (Distributed System Architecture) 500
- dspbl 828

- dspclr 853
- Dual Trend 367

## E

- electronic signatures 356
  - legal text 358
  - reason sets 359
- enabling
  - channels and controllers 156
  - required security 347
- engineering tools 30
  - remote access 580
- engineering tools, remote access 579
- Enterprise Model Builder 30
- enterprise model, about 38
- environment variables 120
- escalation, alarm pager 275
- eServer
  - Mobile Station 580
- eServer Premium
  - remote access 585
- Event Archiving
  - configuring 633
  - event tamper detection 632
- Event Summary
  - customizing 393
  - filtering 387
  - printing 397
  - sorting 392
- event tamper detection 632
- events
  - about 207
  - defining for points 208
  - deleting 854
  - time stamps 391
- Excel Data Exchange, Microsoft 769
- Excel reports *See* Microsoft Excel reports
- exception scanning 197
- Extended Event Archiving. *See* Event Archiving
- extended history 216
- external alarm
  - specifying point for 247
- external change 210
- external change alarms 210
  - for analog points 212
  - for status points 210
- external watchdog 767

## F

- failover 491, 493, 494
- fast history 216
- fast raise/fast lower function key 108
- file replication 590
  - configuring 592
  - configuring for Console Stations 593
  - configuring for DSA 592
  - using 601
- files
  - copying user files. See file replication
  - synchronizing on redundant servers 489
- flexible point 140
- flow control
  - explained 150
  - hardware flow control port configuration 151
  - software flow control port configuration 151
- free format report reference 434
- Free Format reports 401
  - configuring 432
  - configuring for recipes 626
  - creating report definition file 432
  - output 438
  - point values used in 436
  - running automatically 626
  - storing values in point parameters 436
  - used to perform calculations 436
  - used to read history data 437
- FTE communities, adding to the Network tree 53
- Full Access profile 335
- function keys
  - fast raise/fast lower 108
  - slow raise/lower 108

## G

- gating points, for history collection 217
- general arithmetic algorithm 235
- general logic algorithm 235
- generic displays, about 48
- group control of points algorithm 236
- Group Detail display 362
- Group Numeric History display 362
- group policy, about 324
- Group Trend display 362

## H

- hardware definition files
  - creating 829
- hdwbckbld 829
- hdwbld 830
- High Security Policy
  - about 324
  - applying 330
  - installing 327
- historical information, retrieving via Microsoft Excel Data Exchange 769
- history
  - archive directories 219
  - archiving 215, 218
  - batch reports 419
  - data for points in Trend displays 366
  - data in Free Format reports 437
  - deleting 854
  - extended history 216
  - fast history 216
  - gating points 217
  - intervals for Trends 366
  - offset, defining for Trends 369
  - retrieving data with free format reports 432
  - standard history 216
  - using Station displays to configure 218
- History Collection displays 218
- history reference type, database reference 685
- hiway switching, enabling 159
- holiday schedule
  - alarm pager 275
- holidays, configuring 611, 612
- hosts file
  - dual network redundant servers 474
  - FTE network redundant servers 472
  - single network redundant servers 470
  - station 497
- hscint 854
- hscserver/start command 851
- hscserver/stop command 852

## I

- Icon Series Console
  - about 122
  - adding manual input modules 138
  - master Station 124
  - setting up Station 125

- starting multiple static Stations 134
- starting multi-window Station 133
- individual point alarms
  - alarm pager 276
- Input Reference file
  - ODBC Data Exchange report 675, 679
- integration algorithm 236
- IP addresses for redundant networks 468

## J

- journal alarms 208

## K

- keyboard
  - support for modes 137

## L

- latched pulse width 203
- LEDs configuring for a console 548
- LEDs configuring for a Console Station 533
- legal text, customizing 358
- license
  - changing 818
- lissen 845
  - utility 198
- listag 846
  - utility 234
- LRN
  - specifying in report for application program request 404
- LRNs
  - listing 855

## M

- manual input modules, adding 138
- master Station, about 124
- maximum/minimum algorithm 236
- menus
  - customizing 76
- Message Summary
  - customizing 393
  - filtering 389
  - printing 397
  - sorting 392

- messages, configuring 243
- meter factor, for accumulator point 185
- Microsoft Excel Data Exchange 769
  - capabilities of 769
  - continuously updating data, viewing 772
  - data updating rate, changing 775
  - function parameters 779
  - output display options 771
  - point parameters, retrieving 771
  - using functions 774
  - using to capture server data 771
  - wizard, starting 771
- Microsoft Excel reports 401
  - creating 427
  - saving on redundant systems 428
  - security issues 428
  - using for custom reports 427
- migrating user files 820
- mngr account (Windows)
  - OPC server/client communications 706
- Mobile Access for eServer Premium 585
- Mobile Access for Station 582
- Mobile Station 580
- modem and radio link
  - configuring connection detect 152
- modes
  - requirements for keyboard support 137
  - set by defmodes.src file 137
- modes, for point control 199, 201
- monitoring
  - communications status 158
  - recipes 620
  - redundant servers 486
- multicast settings, changing 53
- multicasting 513, 517
- multiple static Stations, starting 134
- multi-window Station
  - about 123
  - SafeView 129
  - starting 133

## N

- naming conventions, servers 468
- Network API 799
- network card duplex settings 476
- Network tree
  - about 50

- adding computers 52
- adding FTE communities 53
- adding switches 54
- loading to your server 54
- removing items 55
- scope of responsibility 56
- nominate individual point alarms
  - alarm pager 276
- nominate individual point alerts
  - alert pager 278
- notifications
  - external alarm 247
- notifications, about 240

## O

- ODBC Data Exchange 671
- ODBC Data Exchange reports 401
  - configuring 425
  - data source name 675
  - Input Reference file 675, 679
- ODBC driver 638
  - asset assignment 642
  - case sensitive data 660
  - connecting to server database 642
  - data accessible 645
  - example 661
- offscan 228
- OPC
  - Advanced Data Client
    - configuring 709
    - overview 698
  - Alarm and Event Client
    - overview 698
  - Alarm and Event Server
    - configuring 741
    - overview 702
  - callback 704
  - Client Interface (OPC controller),
    - overview 697
  - communications setup 706
  - configuring 695
  - Data Access Server
    - configuring 720
    - enumerated parameters 721
    - error codes and qualities 737
    - overview 700
    - point parameters 724
    - update rates and deadbands 722

- data, accessing 721
- DCOM security 706
- Integrator
  - configuring 743
  - overview 703
- mngmr account 706
- options 696
- overview 704
- Redirection Manager 708
- server data, accessing 721
- synchronous read request 705
- terms
  - callback 704
  - deadband 704
  - group 704
  - item 704
  - synchronous read request 705
- transferring data 704
- Operating Group displays 362
- Operating Group Trend display 368
- operating groups
  - configuring with Quick Builder 222
  - configuring with Station 361
  - deleting 364
  - modifying 364
- operator startup display 309, 315
- operator-based security
  - configuring 304
  - configuring for Console Stations 525
  - distributed system architecture 511
  - Signon Manager 350
- operators
  - defining (adding) 306
  - idle timeout 309, 315
  - password administration 322
  - passwords 318
  - sign-on restrictions 320
  - startup display 309, 315
- output states for point control 203

## P

- parameters
  - accumulator point 183
  - addresses 174
  - aggregate alarm counts 260
  - aggregate alert counts 260
  - analog point 178
  - demand scanning 197

- exception scanning 197
- flexible point 172
- internal 186
- periodic scanning 196
- status point 175
- passwords
  - changing in Station-based security 832
  - Operator-based security 308
  - operator-based security
    - administration 322
    - Station-based security 317
- paswrd 832
- piecewise linearization algorithm 236
- pntbld 833
- pntdel 858
- Point Attribute reports 400, 417
  - configuring 417
- Point Cross Reference reports
  - configuring 433
- point definition files
  - creating 825
- Point Detail displays 225
- point ID
  - defining 169
  - in distributed system architecture 503
- point reference type
  - database reference 682, 683
- point servers
  - about 140
  - defining 142
  - tuning 143
- points
  - accumulator 166
  - addresses 195
  - alarms, configuring for 207
  - algorithms, configuring 235
  - analog 166
  - assigned to a particular controller 835
  - associated display, configuring 222
  - building offscan 228
  - cache point description 503
  - changing configuration via Station 225
  - configuration overview 164
  - configuring for recipes 622
  - configuring with Point Detail display 225
  - container 166, 379
  - control confirmation 195
  - control levels 285
  - control modes 199, 201
  - control properties 200
  - database 166
  - extended history 216
  - fast history 216
  - flexible 140
  - history collection 366
  - internal parameters, using 227
  - listing 846
  - listing points defined for each controller 160
  - modes 199, 201
  - modifying group configuration 364
  - obtaining parameter values 432
  - operating groups configuration 222
  - parameter types 174
  - process 166
  - recipes configuration 622
  - remote *See* distributed system architecture
  - specifying for inclusion in reports 409, 411, 413
  - standard history 216
  - status 166
  - trend sets configuration 222
  - types of 166
  - used to monitor redundant servers 487
  - values included in Free Format reports 436
  - values stored in parameters with Free Format reports 436
- printers, configuring 70
- printing reports 70
- process point, described 166
- production algorithm 235
- profiles
  - about 333
  - asset lists 333
  - configuring 335
  - system-defined 335
  - time periods 334
- pulse width, in point control 203
- PV
  - algorithms 235
  - clamp value, configuring 181
  - fail alarms
    - analog point 206
    - status points 204
  - limit alarms, analog points 211
  - states of a point 176

## Q

- qckbld command 834
- queue, in redundant server system 486
- Quick Builder 834
  - alarms configuration 207
  - algorithms, configuration 235
  - defining controllers 155

## R

- range
  - accumulator point 185
  - analog point 179
- reason sets, configuring 359
- Recipe Detail display 623
- recipes
  - chaining 625
  - configuring 619
  - configuring free format reports for 626, 628
  - configuring points for 622
  - defining 623
  - loading 620
  - monitoring via custom displays 620
- Redirection Manager 708
- redundant networks
  - configuration requirements 468
  - NICs 468
  - sample architecture 466
  - server names 468
- redundant OPC servers 708
- redundant servers
  - arbitration 477
  - checkpoint 486
  - configuring Stations for a single network 481
  - configuring Stations for dual networks 481
  - data links 479
  - dual network 473
  - failover 491, 493, 494
  - hosts file 470, 472, 474
  - monitoring 486
  - queue 486
  - single network 470
  - Station configuration 481
  - synchronizing
    - server database 483
    - synchronizing files 489
  - TCP/IP configuration 470
- redundant system *See*

- redundant networks
- redundant servers
- remote access
  - configuring 579
- remote alarms
  - See* distributed system architecture
- Remote Desktop Connection 582, 585, 588
- Remote Engineering and Station Server 579, 580
- remote points
  - See* distributed system architecture
- remote server *See* distributed system architecture
- removing displays 853
- report
  - commands, checking 681
  - database reference 682
  - details, configuring SQL 675
  - example SQL report 690
  - input reference file, create 679
  - output, understanding SQL 680
- report definition file 429
- report definition file, free format reports 432
- report printers 70
- reports
  - Alarm and Event 409
  - Alarm Duration 413
  - batch 419
  - configuring 399
  - cross reference 415
  - customizing requests 402
  - definition details 403
  - Free Format 401
  - Microsoft Excel 401, 427
  - ODBC Exchange 401, 425
  - on request 404
  - output options 404
  - Point Attribute 417
  - running 402
  - running automatically 626
  - search criteria 406
  - time spans 406
  - types 400
- reverse output 200, 203
- rollover value, accumulator point 184
- RSHI alarms 212
- RSLO alarms 212
- rtusum 835
- run hours algorithm 235
- running commands and utilities 816

**S**

- SafeView, configuration overview 129
- scale factor, accumulator point 185
- scan packets 198
  - lisscn command 845
  - listing details 198
- scan point special 197
- scanning 196
  - analyzing load 198
  - demand 197
  - enabling and disabling 228
  - exception scanning 197
  - periodic 196
  - scan packets 198
- scanning load
  - analyzing with lisscn 198
- schedules
  - action types 615
  - adding 613
  - copying 616
  - deleting 616
  - updating 616
- scheduling
  - considerations 610
  - point control 610
- scope of responsibility 336
- search wildcards 406
- security
  - accessing higher levels 303
  - acronyms 348
  - configuring for Station 281
  - distributed system architecture 511
  - levels 285
  - method 283
  - operator-based 304
  - point control 200, 285
  - Station-based 283
    - configuring 303
  - types 283
- Sequence of Events reports
  - configuring 418
  - described 400
- server
  - error codes 844
  - naming conventions 468
  - redundancy *See* redundant servers
  - remote *See* distributed system architecture
- server database
  - points, listing 846
  - server log file, displaying 847
  - service providers, alarm paging 269
  - shifts, configuring 611, 612
  - Signon Manager 350
    - configuring 352
  - size of data 788
  - slow raise/lower function key 108
  - snapshots
    - in history collection 216
    - using fast history 216
  - source address, defining for points 195
- SQL
  - checking commands 681
  - database reference 682
  - databases and ODBC Data Exchange 671
  - report example 690
  - report, configuring details 675
- SQL report, example 690
- SQLCHK utility 681
- Stallion EasyConnection
  - 2-wire port configuration 154
  - 4-wire port configuration 154
  - Adapter 150
  - RS-232 wiring 152
  - RS-422 wiring 153
  - RS-485 wiring 153
- standard history 216
- standard trend 367
- Start of Day 612
- starting the server 851
- state alarms, about 209
- Station
  - associated displays, configuring 222
  - associated Station, specifying 87
  - displays, configuring with Quick Builder 222
  - fast raise/fast lower function key,
    - defining 108
  - redundant servers 481
  - redundant servers, dual networks 481
  - redundant servers, single network 481
  - remote access 579
  - rotary connections 66
  - setup files 481
  - setup settings 72
  - starting 72
- station command 836
- station.ini



- SafeBrowse right mouse button menu 116
- station page appearance 68
- timeout settings for fast failover 496
- Station-based security
  - changing passwords 832
- Stations
  - mobile 580
- status change alarm area inhibit algorithm 236
- status change alarm group inhibit algorithm 236
- status change display request algorithm 236
- status change report request algorithm 236
- status change task request algorithm 236
- status items, described 766
- status line colors, customizing 253
- status point
  - alarms, about 209
  - described 166
  - OP 176
  - PV 175
- status point notification algorithm 236
- stopping the server 852
- synchronizing
  - redundant servers 483
- sysbld 818
- system alarm priorities, configuring 242
- system custom properties 48
- System Event Server, about 58
- system model, about 39
- system performance
  - adding data to displays 61
  - monitoring 58
- System Performance Server, about 58

## T

- table reference type, database reference 687
- tagflb 856
- tail 847
- TCP/IP configuration for redundant servers 470
- TDC 3000 controllers
  - config utility 840
  - tdc\_cl utility 841
- TDC 3000 Data Hiway PIU, sequence of events reports 418
- tdc\_cl 841
- template displays 379
- Terminal Services Client 582, 585, 588

- thumbwheels, adding 138
- time stamps, described 391
- timeout
  - for fast failover 496
  - operator idle 309, 315
- toolbar
  - creating 78
  - customizing 76
- trace utility 848
- trackballs, adding 138
- Trend displays 366
  - accessing history archives 366
  - calling up 378
- trends
  - adding PHD tags 368
  - configuring with Quick Builder 222
  - configuring with Station 366
  - interpolation 366
  - with distributed system architecture 510
- Triple Trend 367

## U

- UDC controllers
  - config command 840
- unanswered alarms 248
- unassigned items 45
- unreasonable highs and lows, configuring alarms 212
- user-defined data formats 229
- usrln 855
- utbconv 820
- utilities 31
- utilities and commands
  - list of 815
  - running 816

## V

- value transportation algorithm 236

## W

- watchdog 767
- wildcard searches 406
- wireless network
  - Station access 580
- wizard

*See* Microsoft Excel Data Exchange

## **X**

X-Y Plot Trend 367

X-Y plots, using free format reports to  
generate 432



**Honeywell Process Solutions**

2500 West Union Hills Drive

Phoenix AZ 85027

USA

[www.honeywell.com](http://www.honeywell.com)

EP-DSXX24

06/06

© 2006 Honeywell International Inc

**Honeywell**