Honeywell

Experion
System Administration Guide

EP-DSX124
300
11/05

Release 300

Honeywell

Document	Release	Issue	Date
EP-DSX124	300	0	November 2005

Notice

Honeywell trademarks

Other trademarks

Support and other contacts

United States and Canada

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

Europe

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

Pacific

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

India

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

Korea

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

People's Republic of China

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

Singapore

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

Taiwan

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

Japan

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

Elsewhere

Call your nearest Honeywell office.

World Wide Web

To access Honeywell Solution Support Online, do the following:

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

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

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

Training classes

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

Related documentation

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

Contents

About this guide

1

This guide is intended primarily for system administrators who are responsible for the administration and maintenance of Release 300 of the Experion Server software and operating system.

This guide includes basic information on Windows system administration features and discusses how to:

Task	Go to
Administer users	page 12
Prevent unauthorized access to the operating system and to non-Station software.	page 17
Change the system time and time zone.	page 25

For information on:

- Installing the system, see the *Software Installation and Upgrade Guide*
- Configuring Experion after installation, see the *Server and Client Configuration Guide*
- Starting up and shutting down Experion, see the *Experion Startup and Shutdown Guide*.

Before reading this guide

Before using this guide for administration and maintenance of your Experion server, you need to:

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

Prerequisite skills

This guide assumes that you have a basic knowledge of the hardware you are using: that is, the computers, printers, network components.

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

System administration

2

This chapter discusses system administration tasks you might be required to perform.

To perform administration tasks you must belong to the Administrators Group and have full access to the computer or domain controller.

Troubleshooting tips and procedures are described in the *Server and Client Troubleshooting Guide*.

Administering users

The tasks you need to perform to administer users might include:

- Creating Windows user accounts
- Adding user accounts to groups
- Deleting Windows user accounts
- Creating Experion operator accounts
- Changing passwords

Creating windows user accounts

To enable your users to have access to Experion they must be able to log on to the computers running the Experion software. To enable this you create Windows user accounts.

The way you create Windows user accounts depends on your environment.

If your site is set up in a domain environment, you create user accounts using the Active Directory Users and Computers tool.

If your site is set up in a workgroup environment, you create user accounts locally using the Computer Management tool on each computer that a user needs to log on to.

See the Microsoft Windows documentation for specific procedures on how to create user accounts.

Adding users to groups

Users inherit the rights of the groups to which they belong. For example, every member of the Honeywell Administrators group inherits all the rights assigned to the Honeywell Administrators group.

There are several groups that are created when you install Experion. You can use Computer Management to see a description of each local group.

If you have a domain environment, you add users to global groups.

The particular group to which you add a user depends on the type of rights the user needs.

If the type of user is an operator, add this user to the Users group. Users belonging to this group can run certified applications, for example, Station. They cannot perform any administrative functions.

If you want to further restrict the access of an operator, you can set up the computer so that the operator only has access to Station. See “Restricting access to operating systems and non-Station software” on page 17.

If the type of user requires Windows administrator privileges, add this user to the Windows Administrators group. Users belonging to this group can use all installed applications and carry out Windows administrative functions.

If the type of user requires Experion administrator privileges, add this user to the Honeywell Administrators group. Users belonging to this group can use all installed applications and carry out Experion administrative functions.

For information about adding a user to a group, see the Windows online help.

Changing passwords

If you have administrator privileges you can change any user’s password. For example, you might need to reset the password for a user who has forgotten their password.

If you have domain accounts, you use the Active Directory Users and Computers tool to change a user’s password.

If you have local accounts, you use Computer Management to change a user’s password.

If your site uses integrated Experion accounts, see the section on changing passwords for integrated accounts in the security section of the *Configuration Guide*.

Changing the password for the **mngr** account has implications for other Experion services that also use the **mngr** account. If you change the password for the **mngr** account, you must change the password for the **mngr** account on all computers that contain the **mngr** account. For more information see “Windows mngr account and Experion services and processes” on page 15.

Deleting a user

Caution

Do not delete the **mngr** user account. If you delete a Windows account (or group) which has been granted access to certain resources (for example, files), then access to those resources through the deleted account is lost, even if you recreate another Windows account with the same name.

If you have administrator privileges, you can delete user accounts.

If you have domain accounts you use the Active Directory Users and Computers tool to delete an account.

If you have local accounts you use Computer Management to delete an account.

Creating Experion operator accounts

After you create the required Windows user accounts, if your system uses operator-based security, you need to create operator accounts. For details on creating operator accounts see the section on configuring security in the *Configuration Guide*.

Windows mngr account and Experion services and processes

The Windows mngr account is created with User privileges during the Experion installation process. The Experion services and some other Experion processes run under this account.

Changing the Windows mngr account password

This section describes how to change Experion Windows account passwords across the Experion system using the Password utility.

Prerequisites

If you have redundant Experion servers, the passwords must the same on server A and server B.

Considerations

Passwords must be eight to 14 characters in length and must contain at least one numeric character and at least one alpha character.

The Password utility, `pwdutil.exe`, can be found in the following locations:

- `Utilities\Password Utility` folder on the Experion R300 Knowledge Builder CD.
- `C:\Program Files\Honeywell\Experion PKS\Utilities\PwdUtil` folder on an Experion server.

To change the Windows mngr account password:

1. Double-click the `pwdutil.exe` file.
2. Click the `mngr` account.
3. Type the new password and then click **OK**.
4. If an error message is displayed one or more times, click **OK** on each message.
5. When finished changing Windows account passwords, click **Done**.
6. Click **OK**.
7. Restart the computer.

Changing the mngr password for OPC Interface configuration

When the Experion OPC Interface connects to a third-party OPC server over the network, it uses the Windows mngr account and password on the Experion server to connect to the computer running the OPC server. If this login fails, the OPC connection is refused.

To ensure that security does not become an issue for OPC Connections, ensure that a guest account exists on the third-party OPC server computer with the same name and password as the Windows mngr account on the Experion server computer.

Changing the mngr password for OPC Integrator

When the Experion OPC Integrator connects to a third-party OPC server over the network, it uses the Windows mngr account and password on the Experion server to connect to the computer running the OPC server. If this login fails, the OPC connection is refused. To ensure that security does not become an issue for OPC Integrator connections, ensure that a guest account exists on the third-party OPC server computer with the same name and password as the Windows mngr account on the Experion server computer.

Changing the mngr password for ODBC Data Exchange security settings

When the Experion ODBC Data Exchange report connects to an ODBC compliant database over the network, it uses the Windows mngr account and password on the Experion server to connect to the computer running the database. If this login fails, the ODBC connection is refused.

To ensure that security does not become an issue for ODBC connections, ensure that the guest account on the computer exists with the same name and password as the Windows mngr account on the Experion server computer.

Changing the mngr password Alarm/Event and report printing settings

When the Experion server attempts to print Experion alarms, events, or reports to a printer that is connected to a remote computer, the server uses the Windows mngr account and password to make a connection to the remote computer. If the login fails, the print job is rejected.

The account and password on the computer where the network printer resides must match the server account.

For further details, see the *Software Installation and Upgrade Guide*.

Restricting access to operating systems and non-Station software

The procedures in this section can be used in conjunction with the High Security Policy.

To prevent an operator from accessing the operating system and software other than Station software, you can configure the computer as a "secure" Station.

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

Considerations

- If you want an operator to print, you need to set up access to the printers for the operator before you complete the tasks in this section.
- If you set up automatic logon, to log on as Administrator you need to press the Shift key to prevent automatic logon.
- For information on configuring full screen lock for Station and restricting access to certain Station menu choices, see "Locking Station in full screen and disabling menus" on page 23.
- For information on limiting access to Intranet and Internet sites via Station, see the chapter "Configuring Stations and Printers" in the Configuration Guide.
- You should also remove the link from the System Menu display to Knowledge Builder as Knowledge Builder uses Internet Explorer. When Internet Explorer is open operators can gain access to other files.

Setting up a secure Station

This section describes how to set up a secure Station with Windows XP.

Prerequisites

To complete these tasks, you must be logged on to the local machine as a Windows Administrator.

Tasks

Complete the following tasks:

Task	Go to:	Done?
Create a batch file which starts Station automatically.	page 18	

Task	Go to:	Done?
Specify the batch file as a logon script to the user account.	page 19	
Prevent operators from shutting down their computer.	page 20	
Remove access to applications via Task Manager and Windows Explorer.	page 20	
Set up automatic logon (optional).	page 21	
Prevent users from locking the computer.	page 21	

Creating a batch file to start Station

In order for operators to access Station on a secure computer, you need to create a batch file that enables Station to start automatically when the operator logs on to the computer.

Considerations

- If you use Signon Manager and Electronic Signatures, you should use the `-sl` option so that Station is in full-screen mode but always on the bottom so that the Signon Manager and Electronic Signatures dialog boxes appear on top of Station.

To create the batch file:

1. Log on as a Windows Administrator.
2. Create the following folder path under `\Windows\System 32\Repl\Import\Scripts`.
3. Use a text editor, such as Notepad, to create the following batch file:

```
rem ********************************************
rem change to station directory
rem ********************************************
cd Program Files\Honeywell\Experion PKS\client\station
rem ********************************************
rem the following line need only be included
rem if you are on the Server PC
rem and also using automatic logon.
rem It delays Station startup to let the
rem Server start completely first.
rem ********************************************
sleep 70
rem ********************************************
rem start station with "full screen lock" and always on top
rem and all “Station" menu options inactive.
rem stnsetup.stn is optional, delete if not
rem required.
rem ********************************************
```

```
start station.exe [stnsetup.stn] -sslxc
cd \Program Files\Honeywell\TPS\Base
start signon
```

4 Save the file as `\windows\system32\repl\import\scripts\start_station.bat`

Specifying the batch file as a logon script

Once you have created the batch file, you need to associate the batch file with the operator's user account so that the batch file runs when the user logs on.

Prerequisites

- The batch file must be stored locally on each computer in the `\Windows\System 32\Repl\Import\Scripts` folder.

To specify the batch file as a logon script for domain accounts:

1 Select **Start > Settings > Control Panel >Administrative Tools > Active Directory Users and Computers**.

2 In the tree view select **Users** to display the list of users in the domain.

3 Right-click the account name to which the Logon Script is to be assigned and and select **Properties**.

4 On the Profile tab type `start_station.bat`.

5 Click **Close**.

6 Close Active Directory Users and Computers.

To specify the batch file as a logon script for local accounts:

1 Select **Start > Settings > Control Panel > Administrative Tools > Computer Management**.

2 Select **Local Users and Groups**.

3 Select **Users**.

4 Double-click the user account you want to modify.

The **Properties** dialog box opens.

5 Select **Password never expires**.

6 Click **Apply**.

7 Click **Profile**, and in **Logon Script Name** type `start_station.bat`.

8 Click **Apply**.

9 Click **Close** to close the **Properties** dialog box.

10 Close Computer Management.

Preventing operator shut down

Operators can shut down a computer in several ways:

- From the Start menu
- Pressing CTRL + ALT + DEL
- At the logon screen

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

To change the local policies to prevent shut down:

1. Select **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**.
2. Select **Local Policies > User Rights Assignment**.
3. Double-click **Shutdown the system**.

   The **Local Security Policy Setting** dialog box opens.
4. Deselect **Local Policy Setting** for the Users group and the Honeywell group that you are modifying and click **OK**. This modifies all users that belong to this group.
5. Close **Local Security Settings**.

To edit the registry to prevent operator shut down:

1. Select **Start > Run,** type `regedit` and click **OK**. The Registry Editor opens.
2. Locate the key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\ShutdownWithoutLogon`

   Set its value to `0`.
3. Exit Regedit.

Removing access to Task Manager, Windows Explorer and Internet Explorer

You can prevent operators from accessing applications through Task Manager and Windows Explorer by removing access to Task Manager and Windows Explorer.

To remove access to Task Manager and Windows Explorer:

1. In Windows Explorer, right-click the file `windows\system32\taskmgr.exe`.
2. Select **Properties > Security**.
3. Click **Add**.
4. Select the user you want to modify, click **Add** and **OK**.

5 Select the user you added, click **Deny for full control**.

6 Click **OK**.

7 Select **Yes** in response to the "Do you wish to continue?" prompt.

8 Repeat steps 1 through 7 of this task for the file `\windows\explorer.exe`.

9 Repeat steps 1 through 7 of this task for the file `\windows\iexplore.exe`.

If you do not need to set up automatic logon, restart the computer and log on as the user you have modified to run the secure Station. If you need to complete any administration tasks, log off and log on again as Windows administrator.

Setting up automatic logon

If you want Windows to start automatically without the operator entering a Windows password, you can set up automatic logon. If you set up automatic logon, the computer always logs on with the same user name and password.

To set up an automatic logon:

1 Start Regedit.

2 Locate the key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\ DefaultUserName`

Set the value to the user name of the operator you are modifying.

3 Select **Edit > New > String Value**, and type `DefaultPassword`. Set the value to the password of user you are modifying.

4 Select **Edit > New > String Value**, and type `AutoAdminLogon`. Set the value to `1`.

5 Close the Registry Editor.

Disabling the lock computer option

If you have set up an account with automatic logon without requiring a password, you should disable the Lock Computer option so that an operator cannot lock themselves out of the computer.

To disable the Lock Computer option:

1 Select **Start > Run**, type `mmc` and click **OK**. The MMC opens.

2 Select **Console > 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 **Group Policy** from the list and click **Add**.
5. Accept the defaults and click **Finish**.
6. Click **Close** to close the **Add Standalone Snap-in** dialog box.
7. Click **OK** to close the **Add/Remove Snap-in** dialog box.
8. In the Console Window, navigate to **Console Root > Local Computer Policy > User Configuration > Administrative Templates > System > Logon/ Logoff**.
9. In right-hand pane double-click **Disable Lock Computer**.

   The **Disable Lock Computer Properties** dialog box opens.
10. Select **Enabled** and click **Apply**.
11. Press **CTRL** + **ALT** + **DEL** to verify that Lock Computer option is disabled. Click **Cancel**.
12. Click **OK** to close the **Disable Lock Computer Properties** dialog box.
13. Close MMC, you do not need to save the save console settings.

Locking Station in full screen and disabling menus

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

If you want to completely restrict access to the Station computer, use the procedure in the section “Restricting access to operating systems and non-Station software” on page 17 and use the High Security Policy.

Changing the Station command line allows you to:

- Lock the Station window in full screen so that users cannot resize the window or access operating system functions and non-Station applications.
- Disable the **Exit** menu choice so users cannot close down this Station.
- Disable the **Setup** menu choice so that users cannot change the connection or display settings for this Station.
- Disable the **Connect** menu choice so that users cannot attempt to connect to a different server and disconnect from the current server.

Access to Intranet and Internet sites is disabled by default on Station. For information on enabling full or restricted access via Station’s SafeBrowse feature, see the chapter on configuring Stations in the *Configuration Guide*.

Note

If you have already set up a secure computer using the procedures in Restricting access to operating systems and non-Station software, you can skip this procedure.

Changing the Station command line

To lock the Station window in full screen and to disable menu choices, you need to use various switches to change a Station’s command line.

Some of the syntax options for a Station command line are as follows:

```
Station [-s[f][l][x][s][c]]
```

where:

Parameter	Description
`-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
`-sx`	Disables the Exit menu choice
`-ss`	Disables the Setup menu choice

Parameter	Description
`-sc`	Disables the Connect menu choice

For example, to use `opsetup.stn` as the default setup file for this Station, and to disable the **Exit** and **Setup** menu choices, type:

```
station.exe opsetup.stn -sxs
```

There are a number of other command line options, such as specifying the name of the setup file that you want Station to start up with (see the chapter on configuring Stations in the *Configuration Guide*.) For details of other command line options, see the station command in the Command Reference chapter in the *Configuration Guide*.

To change a Station's command line:

1. Right-click the **Start** button.
2. Select **Open All Users**.
3. Double-click the **Programs** icon.
4. Double-click the **Honeywell Experion PKS** icon.
5. Double-click the **Client Software** icon.
6. Right-click the **Station** icon and select **Properties**.
7. In the **Station Properties** dialog box, modify the **Target** option to include any of the parameters required for Station.

Changing the system time and time zone

When you install the Windows operating system, the time is set to automatically adjust for daylight saving time. It is recommended that you retain this automatic adjustment.

The Experion server uses coordinated universal time (UTC) to determine how alarms and events are presented in summary displays and reports. As a result:

- In summary displays, the newest alarms and events appear at the top. The time displayed is the local time as set on the computer.
- In reports alarms and events are sorted by UTC. The time displayed is the local time as set on the computer.
- Sequence of events reports lists events in their order they occurred.

For example, an Alarm Summary contains entries for alarms raised and 01.30 and 02.30. At 03.00 the time changes from daylight saving to standard time and the time on the server computer is reset to 02.00. Another alarm is raised at 02.15, after the time change from daylight saving. The alarm raised at 02.15 appears above the alarm raised at 02.30 daylight saving time. This ordering of alarms is correct since the alarm raised at 02.15 standard time is newer than the alarm raised at 02.30.

Process controller nodes and ACE nodes are continually updated with the correct (UTC) time from the server. The TIMEZONE and DAYLIGHTTIME parameters must be manually adjusted.

Any trends that are open during the time change to or from daylight saving time stop updating until the display is refreshed.

If you do not want the time automatically adjusted for daylight savings, contact your Honeywell Technical Assistance Center (TAC) for information on how to manually adjust for daylight saving time.

Tuning system performance

3

This section describes how to tune system performance. For a description of specialized terms, see “Specialized terms” on page 28.

Notes

- These topics are also generally applicable to Console Stations.

Specialized terms

This section describes the components of the supervisory network and the features in Experion that affect reliability, system availability, and performance.

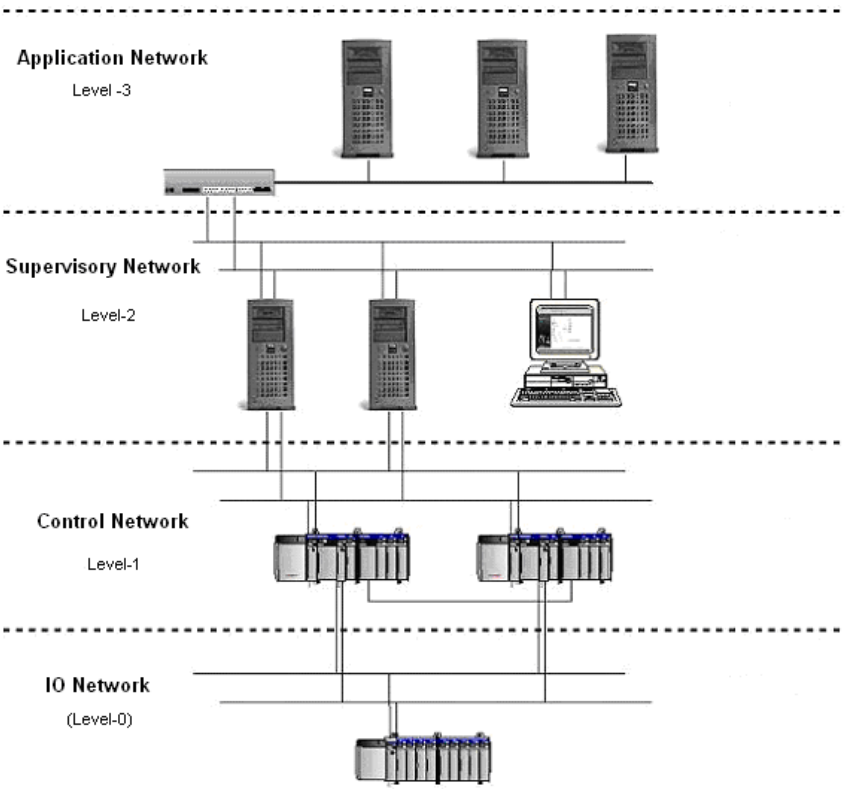
Performance describes the speediness of a system to react to a series of tasks, and the ability to perform those tasks in a reliable manner. There are two aspects of performance:

- **Overall system performance**. This type of performance is most affected by the configuration of drivers and related software that make up the system.
- **Individual application/subsystem performance**. This type of performance is typically configured through the use of software settings and hardware components.

Reliability and system availability are the primary concern of process control systems. The main goals are to make sure that the system is available to the user at any point it time, and that Experion is responsive and presents the correct data.

Network layers

The following figure shows how a process control system can contain several network layers: IO, Control, Supervisory, and Application.



Control network (level 1)

This is the network between PC devices and controller. There are various options for this network type:

- CIP over Ethernet.
- CIP over ControlNet.
- Fault Tolerant Ethernet (FTE) (see the Attention below).
- LCNP interface.

Examples of devices communicating on this network:

- Server to Series C controller (C300 or C200)
- Console Station to FIM.
- ACE to C200.

Supervisory network (level 2)

This communication network is for the distribution of data between data collection devices (typically servers) and user interfaces. Two options exist for this network:

- Ethernet
- Fault Tolerant Ethernet (FTE) (see the Attention below).

Examples of systems communicating over this network:

- Server to Console Station.
- Server to Flex Station.
- Server to ACE.
- Server to EHG.

Application network (level 3)

This communication network is for applications that manage control devices but not necessary for control process itself. Two options exist for this network:

- Ethernet.
- Fault Tolerant Ethernet (FTE) (see the Attention note below).

Examples of systems communicating over this network:

- @ssetMAX.
- ProfitMAX.

Business network (level 4, not shown)

This communication network is for applications that interface between business systems and the control system. Two options exist for this network:

- Ethernet.
- Fault Tolerant Ethernet (FTE) either a co-joined (combined level 1 control network and level 2 supervisory network) or a level 2 network. When co-joined, it is physically one network, but logically separated by the use of subnet masks.

Examples of systems communicating over this network:

- OptiVISION.

Tuning the operating system

Computers ordered from Honeywell with the installation services option (EXPPlus) already have the operating system tuned for operations. Operating system (or kernel) tuning changes the way the operating system assigns process priorities.

Prerequisites

To tune the operating system as described in this section, you need to log on to a Windows account with administrative privileges.

Tuning the Windows XP Professional kernel

To tune Windows XP Professional:

1. Choose **Start** > **My Computer**.
2. Right-click the **My Computer** icon in the menu and choose **Properties**.
3. Click the **Advanced** tab.
4. Click **Settings** in the Performance group.
   The **Performance Options** window opens.
5. Click the **Advanced** tab.
6. In the Processor scheduling group, click **Programs**.
7. In the Memory usage group, click **Programs**.
8. Click **OK.**

Tuning the Windows Server 2003 kernel

Tuning Windows Server 2003 is a two-step process that involves:

1. Setting the application response.
2. Tuning the server service.

Setting the application response

During the configuration phase, applications that run on the server are affected by the application response setting. This setting can be set to **Applications** during the configuration phase and then changed to **Background Services** for the operational phase.

Note that Honeywell recommends that you run your server as a "headless node", that is, you do not run applications (for example Control Builder, Station, Excel) on your Experion server. If, however, you do run applications on the server during the operational phase (that is, you configure your server as a "non-headless node", it is recommended that you set the application response to **Applications**.

To set the application response:

1. Right-click the **My Computer** icon on the Desktop, and choose **Properties**.
2. Click the **Advanced** tab.
3. In the Performance section, click **Settings**.
4. In the **Performance Options** window, click the **Advanced** tab.
5. In the Processor scheduling section, click
   - **Background services** for "headless nodes".
   - **Programs** for "non-headless nodes".
6. Click **OK** to close the Performance Options window.
7. Click **OK** to close the System Properties window.

Tuning the server service

Considerations

- During the configuration phase, applications that run on the server are affected by the server service setting. Follow these guidelines, based on system configuration:
  - On small systems, and medium-to-large systems with the Engineering Repository running on a separate server, the Server service can be set to **Minimize memory used** on during the configuration phase and then changed to **Maximize data throughput for network applications** for the operational phase.
  - On medium-to-large systems with the Engineering Repository running on the Experion server(s), the Server service can be set to **Balance** during the configuration phase, and then changed to **Maximize data throughput for network applications** for the operational phase.

To tune the server service:

1. Right-click the **My Network Places** icon on the Desktop, and choose **Properties**.
2. Right-click one of the network connections (it does not matter which one) and choose **Properties**.

3 Click **File and Printer Sharing for Microsoft Networks** and then click **Properties**.

4 Click the appropriate option based on the server's use:

If the server is:	Click this:
Experion server	Maximize data throughput for network applications
ACE/SCE server	Balance
Experion Highway Gateway	Balance
Remote Engineering and Station Server	Maximize data throughput for network applications

Optimizing the server's hard disk performance

Disk performance, or the capability of a computer to access and store files on the hard disk, can greatly affect its overall performance. The two main file system issues (that is, issues related to the format of storage on the hard disk) that affect a computer are:

- File system errors, which are typically caused by power outages or hardware malfunctions.
- Fragmentation, which occurs gradually over time.

Note that the following procedures also apply to Console Stations.

Fixing file system errors

About file system errors

File system errors can be caused by the following events:

- Power outages
- Improper shutdown
- Disk hardware malfunction

To check and fix file system errors, you need to start the file system scan, and then restart the computer.

Requirements

- Your process must be “off control” before scanning for file system errors.
- Check that no other applications are running as this task requires restarting the computer.

To fix file system errors:

1. On the Windows Desktop, double-click the **My Computer** icon.
2. Right-click the hard drive to check and choose **Properties**.
3. Click the **Tools** tab.
4. In the Error-checking section, click **Check Now**.

   The **Check Disk** window opens.
5. Click **Automatically fix file system errors.**

   Unless a previous check for file system errors revealed bad sectors, do not select **Scan for and attempt recovery of bad sectors**.
6. Click **Start**.

   Because the file system (NTFS) locks the hard disk, the computer cannot scan for file system errors until the computer is restarted.
7. Click **Yes** to schedule the operation to occur the next time the computer is started.
8. Restart the computer.

   The computer checks for file system errors during startup.
9. Log on to the computer.
10. Review the disk report in the Event Viewer. To display the Event Viewer:
    a. Right-click the **My Computer** icon on the Windows Desktop and choose **Manage**.
    b. Expand the **Event Viewer** item and then click the **Application** item.

If the disk report contains bad sector error, you must restart this task, and select the **Scan for and attempt recovery of bad sectors** option.

If a hard disk continuously reports bad sectors, it should be scheduled for replacement as it usually indicates that the hard disk is experiencing hardware malfunctions.

Defragmenting the hard disk

Although the Windows file system (NTFS) attempts to minimize file system fragmentation, it is the most frequent performance issue related to normal computer operations.

Fragmentation occurs when files or pieces of data are not written to the hard disk contiguously (that is, they are not written in order and in the same part of the disk). Consequently, the computer must perform multiple read and lookups every time that file/data is accessed.

The process of defragmentation optimizes the file system so that each file is written contiguously on the disk. In addition, certain files, such as the operating system or frequently accessed files, are moved to the first sectors on the hard disk, so that they can be found and accessed faster.

Requirements

- Your process must be "off control" before defragmenting the hard disk because the performance of the computer is severely degraded during the defragmentation process.
- Check that no other applications are running because the procedure involves restarting the computer.

Considerations

- It is recommended that you add this task to your system's maintenance schedule, so that it is performed during control shutdowns.
- Fragmentation occurs during the configuration phase of the system. Consequently, you should defragment the hard disk immediately after the configuration phase (but before starting the operation phase).
- You can upgrade the default defragmentation utility included with Windows to the full version. Executive Software's Diskeeper includes a scheduler, and can defragment folders and pagefiles when a computer restarts. Defragmentation tasks affect the control system if they are set to run automatically with the scheduler. Care must be taken when scheduling defragmentation tasks.

To defragment the hard disk:

1. On the Windows Desktop, double-click the **My Computer** icon.
2. Right-click the hard disk that needs defragmenting and choose **Properties**.
3. Click the **Tools** tab.
4. Click **Defragment Now** in the Defragmentation group.
   The **Disk Defragmenter** window opens.

5 Click the hard disk to defragment, and then click **Analyze**.

This analyzes the fragmentation level of the hard drive. Large areas of red indicate that the hard disk is fragmented. Large areas of blue indicate that the hard drive is mostly contiguous.

6 Click **Defragment** in the **Analysis Complete** window to start defragmenting the hard disk, even if this window recommends that no defragmentation is required.

Depending on the level of fragmentation and usage, the task may take some time to complete.

Optimizing the server's memory usage

Computers have two types of memory: physical and virtual. Multi-tasking operating systems, such as Windows, can move data from the RAM (physical memory) and swap it to a file on the hard disk (virtual memory). This technique frees up the RAM for other processes. If a process requires data which has been swapped to a file, the data is first swapped back from the file to RAM so that the process can continue. This technique is called *paging*, and the file is called the *pagefile*.

Viewing memory usage

In the Windows Task Manager dialog box you can view memory usage. Click the **Performance** tab to view the Commit Charge (K) group, which displays the total memory available in physical and virtual memory combined (the Limit value), and Physical Memory (K) group, which displays the amount of physical memory available for use.

Checking the pagefile settings

The pagefile settings include a lower and upper limit. The lower limit is typically the amount of physical RAM plus management space. This is almost always 1.5 times the amount of physical RAM.

It is recommended that the upper limit be set to around three times the amount of physical RAM.

Windows Server 2003 and Windows XP, in normal operation, will only use the lower limit size, and therefore only the value of the lower limit (Initial Size) is pre-allocated. If the usage exceeds this limit, the computer will then continue to allocate additional space until the upper limit (Maximum Size) is reached or the computer runs out of hard disk space. If this occurs, it usually means that an application/process is leaking memory.

Adding more memory to reduce paging

Some paging is normal. However, excessive paging affects computer performance during the swapping and allocation phases.

If a computer pages frequently during normal operation, you can significantly improve its performance by adding more physical RAM. However, if you do add more RAM, you must make the appropriate adjustments to the virtual memory configuration.

Servers/Console Stations

Based on the operating system and application usage, the server/Console Station is not affected by paging as long as the memory specifications are followed for the computer size and usage. If adjustments are needed, you must follow the default rules of the Operating System suggestion (approximate example for a 1024 MB computer):

- Initial Size: 1.5 times physical or default operating system suggestion (for example, 1536 MB).
- Maximum Size: 3 times physical or default operating system suggestion. (for example, 3072 MB).

Console Extension Stations/Flex Stations

Based on the operating system and application usage, the client/Flex Station is not affected by paging operations as long as the memory is at the specified amount of 512 MB. If adjustments are needed, you must follow the default rules of the operating system suggestion (approximate example for a 512 MB computer):

- Initial Size: 1.5 times physical or default operating system suggestion (for example, 768 MB).
- Maximum Size: 3 times physical or default operating system suggestion (for example, 1536 MB).

Adjusting the size of the pagefile

Requirements

- Check that no other applications are running as this task requires restarting the computer.

To adjust the pagefile on Windows Server 2003 and Windows XP Professional:

1. Choose **Start** > **My Computer**.
2. Right-click the **My Computer** icon and choose **Properties**.
3. Click the **Advanced** tab.
4. Click **Settings** in the Performance group.
5. Click the **Advanced** tab.
6. Click **Change** in the Virtual memory section.

   The **Virtual Memory** window opens.
7. Click **System managed size**, and then click **Set**.

   You are prompted to restart the computer. Click **Yes** to restart the computer so these changes can take effect.

Optimizing the network's performance

A network is the communication media between servers, clients, and devices. If this network is not tuned properly, the following problems may occur:

- The performance of the client application may be poor
- There may be intermittent or complete device communication failures
- Redundant servers may lose synchronization
- There may be intermittent or complete loss of communication between clients and servers

In Windows, there are several settings to optimize the network. It is recommended that these settings be combined with an overall plan to monitor and adjust to the traffic on the network. Consult your networking equipment vendor for tools and management applications that work best with your hardware.

Operating system tuning also affects the ability of the computer to respond to network traffic. See "Tuning the operating system" on page 31.

The order in which the system accesses the network is also important—this is known as the *binding order*. It is recommended that the binding order be adjusted so that each computer accesses the network in the same order. If your computer has more than one network card, you must verify that the bindings for each computer are in the correct order.

Managing network traffic

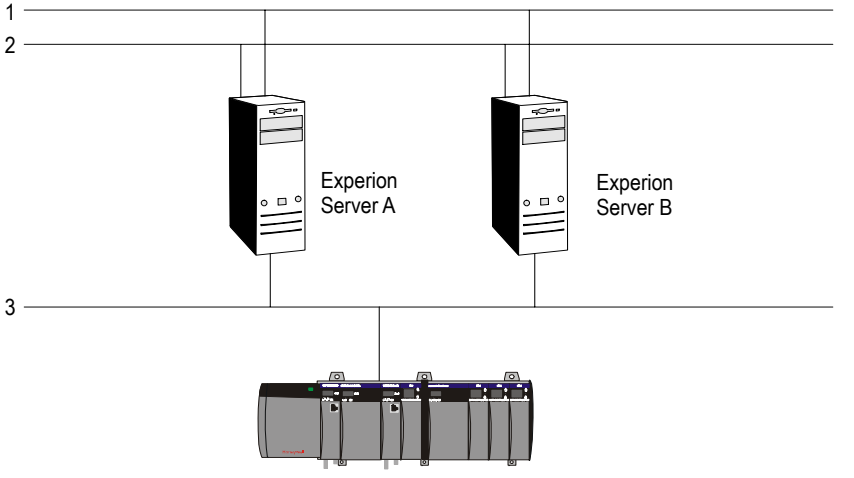
If your control system uses Ethernet as the control network, you can achieve network performance benefits by restricting the type of traffic over this network.

Windows, by default, uses all network cards defined in a computer for communication with other systems as long as the networks are common between the initiator and target.

The following figure shows a configuration in which all three Ethernet networks are common between the two servers. Effective server-to-server communication management would direct all server-to-server traffic across networks 1 and 2, and reserve network 3 for control traffic.

Server-to-server communication (Windows networking traffic), mostly uses the NetBIOS transport protocol. You can restrict this type of communication on network 3 by disabling this protocol.

Note that special handling/restrictions placed on NetBIOS are required if networks 1 and 2 use a Fault Tolerant Ethernet (FTE) topology.



Adjusting bindings and disabling protocols on standard networks

If you have the Installation Services option, the network connection names *Primary Supervisory Network*, *Backup Supervisory Network*, and *Supervisory Control Network* are created. You must use these names in the following instructions. If you do not have the Installation Services option, you need to determine the names of the network connections that handle each task before using this procedure.

To adjust bindings or disable protocols on standard networks:

1. On the Windows desktop, right-click the **My Network Places** icon and choose **Properties**.
2. Choose **Advanced** > **Advanced Settings**.

   The **Advanced Settings** dialog box opens.
3. In the **Connections** list, the order of items must be:
   - Primary Supervisory Network.
   - Backup Supervisory Network, if you have redundant networks.
   - Supervisory Control Network, if you are doing control over Ethernet.

   Use the Up and Down arrow buttons to the right of the **Connections** list to correctly order these items.
4. If the system has a Supervisory Control Network:
   a. Click the **Supervisory Control Network** item in the **Connections** list.
   b. Clear the **File and Printer Sharing for Microsoft Networks** check box in the **Bindings** list.
5. Click **OK**.

Adjusting bindings and disabling protocols on FTE networks

Included with FTE is the NDISUIO layer. Due to the inclusion of this layer, traditional commands such as “nbstat -n” will no longer show the correct NetBios binding order. For Windows XP, use the “netdiag /test:Bindings” command.

For Windows Server 2003 and XP, adjustments to the TCP/IP binding order also change the NetBIOS binding order.

Setting the network interface card (NIC) names

If your network interface cards are unnamed, you need to set the connection names. The NIC labeled “Local Area Connection” should be named as the Yellow NIC and the card labeled “Local Area Connection 2” should be named as the Green NIC.

To set the connection names:

1. On the Windows desktop, right-click the **My Network Places** icon and choose **Properties**.
2. Right-click on **Local Area Connection**, and choose **Rename**.
3. Type in the new NIC name based on the following convention:
   `FTE <Community Name> Yellow`

   In the following example, the community name is “SID”.

   `FTE SID Yellow`
4. Right-click on **Local Area Connection 2**, and choose **Rename**.
5. Type in the new NIC name based on the following convention:
   `FTE <Community Name> Green`

   For example, **`FTE SID Green`**

Identifying network interface card ports and connecting network cables

Use the following instructions to identify which adapter port the Yellow network cable must be attached to and which adapter port the Green network cable must be attached to.

1. Connect the yellow network cable (yellow boot) to one of the network interface card cards.
2. On the Windows Desktop or Start menu, right-click the **My Network Places** icon and choose **Properties**.

   The **Network and Dial-up Connections** dialog box opens.
3. If the status of the FTE Yellow connection is **Network cable unplugged**, connect the Yellow network cable to the other network interface card port, and

then connect the FTE Green connection to the remaining network interface card port.

If the status of the FTE Yellow connection is **Enabled**, connect the FTE Green connection to the remaining network interface card port.

4 Connect the Yellow network cable to the switch in the Yellow Tree.

5 Connect the Green network cable to the switch in the Green Tree.

Adjusting TCP/IP and NetBIOS binding order

To adjust the TCP/IP and NetBios binding order:

1 On the Windows desktop, right-click the **My Network Places** icon and choose **Properties**.

2 Choose **Advanced** > **Advanced Settings**.

3 In the **Connections** list, the order of items must be:

- FTE Yellow
- FTE Green

Use the Up and Down arrow buttons to the right of the **Connections** list to correctly order these items.

Adjusting the NetBIOS protocol settings

To adjust the NetBIOS protocol settings:

1 On the Windows Desktop, right-click the **My Network Places** icon and choose **Properties.**

2 Right-click on the **FTE Yellow** connection and choose **Properties**.

3 Click **Internet Protocol (TCP/IP)** and click **Properties**.

4 Click **Advanced**.

5 Click the **WINS** tab.

6 Click **Enable NetBIOS over TCP/IP** and then click **OK**.

7 Click **OK** on the **Internet Protocol (TCP/IP) Properties** dialog box.

8 Click **OK** on the **FTE Yellow Properties** dialog box.

9 Right-click on the **FTE Green** connection and choose **Properties**.

10 Click **Internet Protocol (TCP/IP)** and click **Properties**.

11 Click **Advanced**.

12 Type **5** in the **Interface metrics** box.

13 Click the **DNS** tab.

14 Clear the **Register this connection's address in DNS** check box.

15 Click the **WINS** tab.

16 Click **Disable NetBIOS over TCP/IP** and then click **OK**.

17 Click **OK** on the **Internet Protocol (TCP/IP) Properties** dialog box.

18 Click **OK** on the **FTE Green Properties** dialog box.

Setting the link speed

To set the link speed:

1 Right-click the **My Network Places** icon on the Windows Desktop and choose **Properties**.

2 Right-click on the **FTE Yellow** connection and choose **Properties**.

3 Click **Configure**.

4 Click the **Advanced** tab.

5 Click **Link Speed & Duplex** in the **Property** list.

6 Click **100Mbps/Full Duplex** in the **Property** list.

7 Click **OK**.

8 Right-click on the **FTE Green** connection and choose **Properties**.

9 Click **Configure**.

10 Click the **Advanced** tab.

11 Click **Link Speed & Duplex** in the **Property** list.

12 Click **100Mbps/Full Duplex** in the **Value** list.

13 Click **OK**.

Special considerations for Fault Tolerant Ethernet/EHG networks

EHG systems combine a FTE network with an additional network connection to the Data Highway. Honeywell suggests that you identify the NIC as the DHEB Network to differentiate it from participation in the FTE network.

Prerequisites

If you have not done so yet, assign FTE Yellow to the first port on the dual port NIC, FTE Green to the second port on the dual port NIC and DHEB Network to the remaining NIC.

To adjust the TCP/IP and NetBIOS binding order

1. Right-click on the **My Network Places** icon on the Windows Desktop and then choose **Properties**.
2. Choose **Advanced > Advanced Settings**.
3. In the **Connections** list, the order of the items must be:
   - FTE Yellow
   - FTE Green
   - DHEB Network

   Use the Up and Down arrow buttons to the right of the **Connections** list to correctly order these items.

To adjust the NetBios protocol settings

1. Right-click on the **My Network Places** icon on the Windows Desktop and then choose **Properties**.
2. Right-click on the **DHEB Network** connection and choose **Properties**.
3. Click **Internet Protocol (TCP/IP)** and click **Properties**.
4. Click the **Advanced** button on the Internet Protocol (TCP/IP) Properties window.
5. In the **Interface Metric** box, type **10.**
6. Click the **DNS** tab.
7. Clear the **Register this connection's address in DNS** checkbox.
8. Click the **WINS** tab.
9. Click **Disable NetBIOS over TCP/IP** and then click **OK**.
10. Click **OK** on the **Internet Protocol (TCP/IP) Properties** dialog box.
11. Click **OK** on the **DHEB Network Properties** dialog box.

To set the link speed

1. Right-click the **My Network Places** icon on the Windows Desktop and then choose **Properties**.
2. Right-click on the **DHEB Network** connection and choose **Properties**.
3. Click **Configure**.
4. Click the **Advanced** tab.
5. Click **Link Speed & Duplex** in the **Property** list.
6. Click **10 Mbps/Full Duplex** in the **Value** list.
7. Click **OK**.

Optimizing other network services

By optimizing the use of Network Browsing services, you can reduce the number of broadcasts a computer performs while communicating and maintaining itself on the network.

If you use a Workgroup model, you must rename the computer's Workgroup Name to a name other than `default WORKGROUP`. When integrating other systems and networks, you must create independent workgroups by naming all of the systems that communicate together with the same workgroup name, but different from other workgroup names.

If you use other services to provide directory and resolution information, you can also optimize networking while minimizing management tasks, for example, Active Directory, WINS, DNS, Domains, and so on. However, this can make some functions of the control system dependent on these services for operation. In order to integrate these types of services into the computer, you need to carefully plan and take care when implementing the plan.

Optimizing other computer settings

Optimizing file sharing

For easier management, it is possible to share custom displays and other files from servers with Flex Stations and other computers.

Considerations

- Due to the performance settings for the servers, you are limited in the amount of information that can be shared.
- The movement of such files can cause additional network activity. This will degrade the performance of the server to perform other tasks.

Optimizing video settings

There are no great performance gains to be made by adjusting the video settings. The system applications and displays have been optimized for resolutions of 1024 by 768 and 1280 by 1024 with 65k (High Color 16 bit) colors. Using any other setting than this may produce anomalies in some displays.

For best performance, the video card should:

- Use a specialized video bus (AGP or PCI Express)
- Have a dedicated RAMDAC capable of 300 MHz (or better), and
- Contain at least 32 MB of VRAM per video display port.

This frees up the computer bus and gives the video processor a more direct line to the CPU and memory resources.

Optimizing system usage

The system usage itself will have an impact on the performance of the system. Most memory and CPU recommendations are based on “average” use of the system, which means that your system may require servers with, for example, more memory, higher CPU speed or larger disks.

These types of adjustments can only occur over time as you gain experience with your system. The following will affect the performance of your system:

- Number of Stations, and:
  - The display update rate
  - Shared versus local displays
  - Chart visualization
  - The number of parameters viewed (across all Stations) and their frequency of change
- Frequency of report generation
- Frequency of performed maintenance, for example, defragmentation level of the disk
- If you have a DSA system, the number of servers and the number of shared parameters
- The amount of history being collected
- The frequency at which events are archived and the duration for which events are kept online
- Server synchronization with file backup
- Size of the system, including the size of the Engineering Repository database for Process systems

As your system is adjusted over time and customized to your control environment, you should regularly evaluate how your systems are performing and make the appropriate adjustments. See “Checking the server’s performance” on page 27.

Optimizing topology-related settings

Physical location of computers

The location and distance between each node becomes a factor in the performance. Experion servers are designed to be within the same network. Consequently, if "hops" are introduced, then timing parameters need to be adjusted due to the increased time to perform such things as synchronization. As tasks take longer to complete, they affect the other running tasks on the system.

A Station's performance will also be affected if it is running remotely.

See the documentation for setting up the server to support these types of architectures. Monitor the server performance—see the topic "Checking the server's performance" in the chapter "Isolating Problems" in the *Server and Client Troubleshooting Guide*.

Physical location of components

During the operational phase of the system, client response will be better when applications are not run on the server itself.

If you have Process Controllers and the server is being overwhelmed, you may want to change the configuration and move the Engineering Repository database to its own dedicated node. Depending on system usage, this can have a dramatic impact on system performance.

Service integration

Adding services, such as Active Directory, to the Experion server has an impact on the server's CPU and memory usage. This must be taken into consideration when planning the hardware purchase for your server.

Network integration

Integrating the process control network with the company's business network can also impact the system's performance. If Active Directories are going to be integrated, you must plan to be able to support the whole business network infrastructure. Depending on the size of the company, this can have a large impact on the server's CPU and memory usage.

Optimizing the scanning load

This section is only applicable if you have controllers other than Process Controllers.

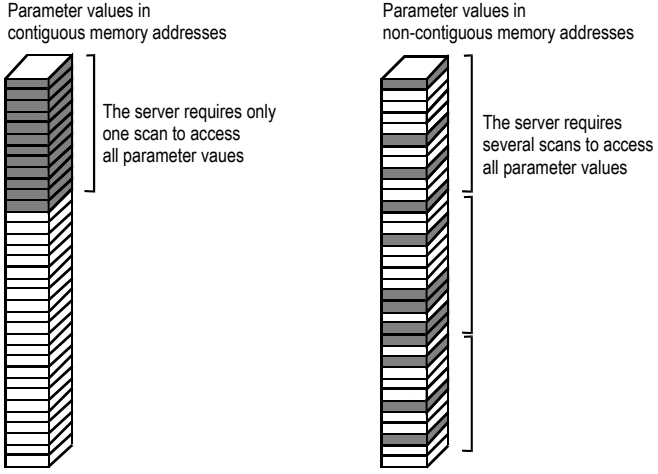
Controllers with badly configured scanning can place a significant load on the system and result in data not being accurately represented in the server database.

It is also important to remember that making even seemingly minor changes to a controller's configuration—such as adding a few new points—can have a significant impact on a system and can result in unstable performance.

Checking the health of the scanning subsystem.

Guidelines for scan optimization

- Use unsolicited messaging if the controller supports this feature and values change infrequently.
- Use periodic scanning if values change frequently.
- Choose a scanning period appropriate to the values being scanned. For example, you do not need to scan a temperature every 5 seconds if it changes only slightly over an hour. For guidelines, see “Choosing an appropriate periodic scanning periods” on page 57.
- Minimize the number of scan packets as follows:
  - Specify the minimum number of scan periods for a given controller because the server requires a separate scan for each scan period. For example, you may only need two scan periods for a particular controller: a short one for a few critical values, and a long one for all other values.
  - For each scan period you use, specify the longest period that is acceptable to your needs.
  - Arrange parameter value addresses so that they occupy contiguous addresses in the controller’s memory, as shown in the following figure. If parameters occupy contiguous addresses, the server can access many parameters in a single scan—the exact number is controller-specific.



Choosing an appropriate periodic scanning periods

Periodic scanning involves reading parameter values at specified time intervals. This means that you need to select an appropriate scan period, ranging from seconds to minutes, for each input/output parameter. For example, if you assign a

scan period of 15 seconds to the PV, the server scans the value in the controller every 15 seconds.

When choosing a scan period, consider the following factors:

- 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 you need to collect history for the point (in the case of the PV parameter). A point requiring one minute snapshots needs a scan period greater than 60 seconds.
- How quickly field changes need to appear in Station displays. 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 from a controller connected to server via a serial line operating at 1200 baud.
- Whether periodic scanning is available—some controllers do not respond to scanning polls and rely on reporting by exception.

Checking the health of the scanning subsystem

Task	Go to:	Done?
Call up the Channel Scanning Statistics display and check the scanning load of each channel. There is a loading problem on a channel if the **Ovld** column is not clear, or if the **Daq** and **Cnt** columns contain high values (ideally, they should be close to zero).	page 19	
Use **trace** utility to record the communications activity for heavily loaded channels.	page 836	
Run the communications test utility for heavily loaded controllers. There is a separate test utility for each type of controller—for example, **abrtst** for an Allen-Bradley controller.	Associated interface reference	
Use **shheap** to diagnose Shared Heap corruption.		
If there are any overloaded controllers, optimize their scanning packets.	page 60	

Optimizing a controller's scanning packets

The basic steps involved in optimizing scanning packets are:

1. Monitor/capture the existing communication statistics, so that you can use them later as a reference point.
2. Identify a controller that needs to be optimized.
3. Use **lisscn** to generate a scan list for that the controller. Use the `-out` option to save the report to a file.
4. Import the scan list into a Microsoft Excel spreadsheet. See "Importing the scan list into a spreadsheet" on page 60.
5. Manipulate the spreadsheet and analyze the current scanning efficiency. See "Manipulating and analyzing the spreadsheet" on page 61.
6. Change the scanning settings in accordance with your analysis.
7. Monitor/capture the new communication statistics, and compare them with the original statistics.
8. Use **lisscn** to generate a new scan list and check that your changes have had the desired effect.

Importing the scan list into a spreadsheet

To import the scan list into a spreadsheet:

1. Open a new spreadsheet.
2. Choose **Data > Import External Data > Import Data**.
3. Select the scan list file and click **Open**.
4. In the Text Import Wizard, select **Fixed width** and click **Next**.
5. Adjust the lines so that the data is imported into the correct columns, such as Index, Scan type and Point/Parameter.
6. Click **Next** and then click **Finish**.
7. Select **Existing worksheet** and click **OK**. The result should look similar to the following figure.

	1.0 SEC	OND SCAN LIST (I	NTERVAL 02)		
INDEX	SCAN TYPE	RTU	FIRST POINT/PARAMETER	FIRST	ADDRESS
1	Hardware acquisition	1 SCU COIL 1	592-HSL-1303.PV S 43	43	for 1
2	Hardware acquisition	1 SCU COIL 1	592-LSLL-2030.PV S 95	95	for 1
3	Hardware acquisition	1 SCU COIL 1	592-LY-3905A_1.PV S 112	112	for 1
4	Hardware acquisition	1 SCU COIL 1	592-UI-EE110A.PV S 122	122	for 3
5	Hardware acquisition	1 SCU COIL 1	599-XZSC-9910.PV S 173	173	for 1
6	Hardware acquisition	1 SCU COIL 1	599-XZSO-9910.PV S 177	177	for 1
7	Hardware acquisition	1 SCU COIL 1	598-VSHH-9102.PV S 179	179	for 5
8	Hardware acquisition	1 SCU COIL 1	592-KY-3251A.PV S 229	229	for 2
9	Hardware acquisition	1 SCU COIL 1	592-LIC-2008.PV S 232	232	for 14
10	Hardware acquisition	1 SCU COIL 1	592-UA-1502.PV S 291	291	for 23
11	Hardware acquisition	1 SCU COIL 1	592-LY-3905B2_1.PV S 336	336	for 1
12	Hardware acquisition	1 SCU COIL 1	598-UI-PC9101A.PV S 347	347	for 2
13	Hardware acquisition	1 SCU COIL 1	598-XY-FA9101A.PV S 351	351	for 27
14	Hardware acquisition	1 SCU COIL 1	592-IALL-2070.PV S 469	469	for 1
15	Hardware acquisition	1 SCU COIL 1	592-PDAHH-2067.PV S 539	539	for 5
16	Hardware acquisition	1 SCU COIL 1	592-UA-3700.PV S 626	626	for 1
17	Hardware acquisition	1 SCU COIL 1	592-UA-EE110.PV S 628	628	for 4
18	Hardware acquisition	1 SCU COIL 1	592-UA-3899_1.PV S 664	664	for 1
19	Hardware acquisition	1 SCU COIL 1	598-LALL-9101A.PV S 687	687	for 8

Manipulating and analyzing the spreadsheet

After importing the scan list into Excel, you manipulate the list so that you can analyze the current scanning efficiency.

To manipulate the spreadsheet:

1. Add a column on the right, label it “Period” and fill in the scan period for each row.
2. Sort the spreadsheet by index.
3. Clean up the spreadsheet by removing unnecessary rows and, for example, removing “for” after the addresses.
4. Sort the spreadsheet by Address. The result should look similar to the following figure.

Index	Scan type	RTU	First point/parameter	Address	No	Scan period
75	Hardware acquisition	1 SCU COIL 1	592-HS-KC101.PV S 467	467	2	5
14	Hardware acquisition	1 SCU COIL 1	592-IALL-2070.PV S 469	469	1	1
76	Hardware acquisition	1 SCU COIL 1	592-LAHHH-3905.PV S 470	470	16	5
111	Hardware acquisition	1 SCU COIL 1	592-XL-PC203.PV S 486	486	1	10
77	Hardware acquisition	1 SCU COIL 1	592-LALL-4130.PV S 487	487	52	5
15	Hardware acquisition	1 SCU COIL 1	592-PDAHH-2067.PV S 539	539	5	1
42	Hardware acquisition	1 SCU COIL 1	592-TAHH-1416.PV S 544	544	82	2
16	Hardware acquisition	1 SCU COIL 1	592-UA-3700.PV S 626	626	1	1
43	Hardware acquisition	1 SCU COIL 1	592-UA-3899.PV S 627	627	1	2
17	Hardware acquisition	1 SCU COIL 1	592-UA-EE110.PV S 628	628	4	1
44	Hardware acquisition	1 SCU COIL 1	592-VAHH-1411.PV S 632	632	14	2
112	Hardware acquisition	1 SCU COIL 1	592-XA-1499.PV S 646	646	14	10
45	Hardware acquisition	1 SCU COIL 1	592_Heart2.PV	660	2	2
18	Hardware acquisition	1 SCU COIL 1	592-UA-3899_1.PV S 664	664	1	1

You can now see how efficient your current scanning strategy is, and where you can make improvements.

Ideally contiguous addresses should have the same scanning period—unlike the above figure, where almost every subsequent address has a different period.

Having analyzed the problem, you can make appropriate adjustments to the scanning periods. In the above figure, for example, if it is not possible to slow all points down to 5 seconds or to speed them up to 1 second, you may find it acceptable to change the scan rate of all points to 2 seconds.

Monitoring the system

Assessing the need for hardware upgrades

Most monitoring of the system should be done during the operational phase of the system.

The Windows Event Viewer

The Windows Event Manager (System and Application Logs) should be checked immediately after installation and major configuration changes. Errors in configuration and problems with components in the system are reported in these logs. If you locate any, you should contact your Honeywell Technical Assistance Center (TAC) for assistance in getting them resolved.

After initial configuration, you should periodically check for any new errors in the log. This should be part of your normal maintenance routines.

Using Dell OpenManage

If your computer is ordered with the installation services (EXPPlus), the Dell OpenManage tools are pre-installed and configured on the computer. These tools monitor the performance and operation of the internal hardware components that make up the system. If any type of hardware event occurs, the system will notify the user and, if necessary, perform critical actions to prevent more major problems from occurring.

These tools are also available on computers without the installation services, but you need to download, install, and configure the software.

There are two types of Dell OpenManage client software:

- Dell OpenManage Server Administrator (OMSA) for server operating systems.
- Dell OpenManage Client Interface (OMCI) for client operating systems.

OMSA provides a view application to look at hardware events and internal sensor readings. OMCI requires a central application (Dell's IT Administrator) to view the hardware events and internal sensor readings. (This does not stop the software from reporting events local on the system.)

Dell's IT Administrator application must not be installed on any Experion node. It must be on a dedicated computer if used with an Experion system. Dell IT Administrator application is not required, as both client applications are SMTP and CIM compliant. They can interoperate with any central system monitoring

utilities such as HP OpenView, Tivoli, or other systems that support these standards.

Monitoring performance

You use the Windows Performance Monitor to monitor a server's performance.

Considerations

- This procedure is also applicable to Console Stations.
- If your computer is ordered with the installation services (EXPPlus), a performance monitoring tool is configured and installed.
- If your computer was *not* ordered with Installation Services, you first need to configure the Performance Monitor. See "Configuring Performance Monitor" on page 65.

To start monitoring performance:

1 Choose **Start > Programs > Honeywell Experion PKS > PC Performance Tools.**

2 Double-click the **PC Performance Tools** icon.

3 Double-click the **System Performance** icon.

Configuring Performance Monitor

You only need to perform this task if your computer was not ordered with the installation services.

To configure Performance Monitor

1 Choose **Start > Programs > Administrative Tools > Performance**.

2 Click the + button on the toolbar.

3 Add each counter specified in the following table:

   a. Select the performance object from the **Performance Object** list.

   b. Select the counter in the **Select counters from list**.

   c. If required, select the instance in the **Select instance from list**.

   d. Click **Add**.

#	Performance Object	Counter	Instance
1	Paging File	% Usage	<\\??\C:\Pagefile.sys>
2	System	Processor Queue Length	
3	System	Context Switches/Sec	

#	Performance Object	Counter	Instance
4	Processor	% Processor Time	_Total
5	Processor	% Interrupt Time	_Total
6	Server Work Queues	Queue Length	0
7	Server Work Queues	Bytes Transferred/Sec	0
8	TCP	Segments/Sec	

Interpreting the performance counter values

Paging file usage

Evaluating the Paging File Usage counter tells you whether or not your computer has enough physical RAM. The counter itself tells you how often the computer is using the Paging File. Average values approaching 40% or higher are a strong indication that the computer is running without enough memory.

Processor speed and quantity

In order to evaluate whether or not you computer has adequate processing power, you must look at several counters:

- System/Processor Queue Length
- System/Context Switches/Sec
- Processor/% Processor Time
- Processor/% Interrupt Time
- Server Work Queues/Queue Length

The **Processor Queue Length** indicates how many threads are waiting for CPU time. Evaluating the Average gives you an idea of how well the system is supporting the configuration. Generally, numbers averaging from 2 to 15 indicate the system could benefit by moving to a faster CPU. Numbers averaging above 15 indicate the system could benefit by moving to a multiple CPU system. (Microsoft states that systems with average queue lengths above 2 indicate processor congestion.)

Evaluating the **Context Switches/Sec** gives you an idea of how busy the system is. The counter measures the number of times a thread:

- Voluntarily relinquishes the processor
- Is preempted by a higher priority thread
- Switches between user-mode and privileged (kernel) mode to use an Executive or subsystem service.

The **Percent Processor Time** indicates the utilization of the processor measured in a percentage. Average percentages higher than 25% usually indicate that the system could benefit from an upgrade to a faster processor or multiple CPU system.

The **Percent Interrupt Time** indicates how often the system is handling hardware-related tasks, and where CPU congestion might exist. Evaluating this counter may assist you in customizing your system configuration and usage to gain the best performance.

The **Server Work Queue Length** indicates the workload the server is performing. A sustained queue length greater than four might indicate processor congestion.

It is recommended that you evaluate all these counters before considering an upgrade for the CPU. Faster speed processors will not always solve CPU performance problems. Some systems will require the use of multiple CPUs. If you are unsure of the CPU requirements of your system, it is recommended you purchase a system capable of supporting multiple CPUs. This leaves you with the option of going to higher speed CPUs as well as the ability to add a second.

Networking

Network utilization is best measured using third-party tools to evaluate the network hardware itself. However, you can gain knowledge by how a particular server node is performing by looking at the following counters:

- Server Work Queues/Bytes Transferred/Sec
- TCP/Segments/Sec

With these counters, you can also evaluate the network using the pre-installed network diagnostic tools provided with the network drivers. Two exist depending on platform and configuration:

- 3Com Diagnostic Tool: For use with 3Com Cards on Precision 340.

  To access, Choose **Start > Programs > 3Com NIC Utilities > 3Com NIC Doctor**.

- Intel Pro Set: For use with Intel Pro Cards on Precision 340 with FTE, and all PowerEdge Servers.

  To access, choose **Start > Settings > Control Panel** and the double-click the **Intel ProSet** icon.

Experion clients utilize two methods to communicate with the server. To adequately evaluate the performance of this mechanism, it requires viewing both counters at the server to determine how busy the network/server is performing these tasks:

- **Bytes Transferred/Sec** shows how busy the server is servicing network clients. This is the rate at which the server is sending and receiving bytes with the clients.
- **TCP/Segments/Sec** shows the amount of TCP traffic sent or received by the server.

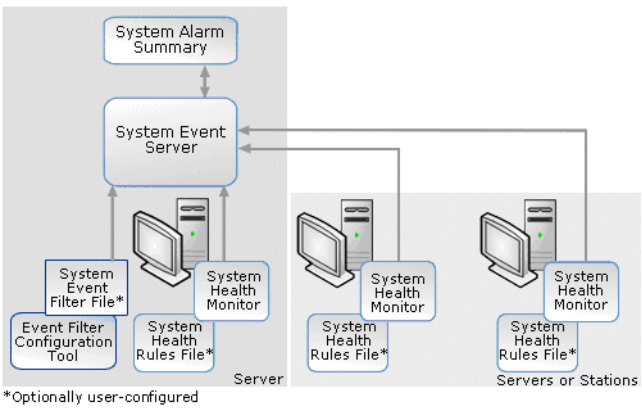
Monitoring System Health

About System Health Monitoring

The System Health Monitor ties together local node health events with the Experion System Alarm Summary. Monitoring examples include:

- computer specific resources
- node specific hardware

The System Health Monitor is a local node service that monitors the computer, compares it against a System Health Rules File and logs events when a fault has occurred. In order to send the event to the Experion System Alarm display, the System Event Server uses a corresponding event filter file that handles the events raised from the System Health Monitor. Users can modify the filter file or rules files to include additional fault rules.



System Health Monitoring Considerations

The System Health Monitoring service is installed during an Experion install with the system management runtime package. You do not need to perform any service installation as the default installation enables system health monitoring. The System Health Monitoring service runs locally and can monitor the local node without the system definition residing in the Enterprise Model Database (EMDB).

You can configure the System Event Server to access a System Health Monitoring event filter file that allows System Health Monitoring faults to appear as system events in the Experion System Alarm summary. You can also view the logged

System Health Monitored events from the nodes' Windows event log, whether or not the System Event Server is available to support System Health Monitoring.

Modifying System Health Rules files

In most cases you should not have to modify the rules files because the default rules files should meet most of your needs. You will need some knowledge of Windows system administration and/or OPC concepts if you modify a rule (fault model). You modify the default System Health Rules files using an Expression Builder from the Configuration Explorer in Configuration Studio. The rules are stored to System Health Rules files that are read by the local System Health Monitoring service.

Attention

The Expression Builder tool supports updating the rules for the system health monitoring service. Honeywell recommends that the rules only be updated using Expression Builder because the tool provides rule validation.

To modify System Health Rules files

1. In the Configuration Explorer in Configuration Studio, click **Analysis Tools**.
2. Click **Expression Builder** from the **System Health Monitoring** task.
3. From the System Health Monitor Expression Builder, select or enter the following:
   - Rule - Select the name of the System Health Rule or fault model, or enter a new rule name if making a new rule.
   - Rate - Select how often you want the system to evaluate the rule.
   - Node type - Select the node types this rule monitors.
   - Description - Enter text describing the rule.
   - Message - Enter a text message that is associated with the event.
   - Priority - Select an event priority (low, high, urgent) to support the Experion summary display indications.
4. In the **Expression** field, enter or modify the fault expression. If you are building a new fault model and need to create a new expression, see "Entering an expression for system health monitoring" on page 73.
5. Save the modified system health rule.

   The saved result is stored locally in a `Honeywell.FaultModels.xml` file.
6. Synchronize the system health rule, if the rule needs to be available on other nodes in the system in addition to the local node.

About System Health Monitoring expressions

System Health Monitoring expressions can consist of two data sources:

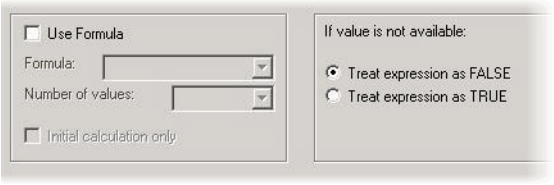
- Performance counters - Any performance object that is accessible from the perfmon application.
- OPC - Any OPC point.paramters.

Note

Building expressions with OPC values requires knowledge of the point.paramter names and also requires some knowledge of the OPC server of interest. The System HEalth Monitoring service runs as localsystem by default, so it would not be able to access remote OPC server as that account. To avoid DCOM calls, OPC rules should only communicate with a local OPC server. This can be controlled by only enabling OPC rules on the machine on which they are to execute.

Formulas and values in expressions

Regardless of the data source, the data can be used in formulas, or missing values can be handled. The formula will be applied once the number of values has been collected (one value gathered each time the rule runs). If the **Initial calculation only** option is selected, the formula only runs once, otherwise it is continually recalculated with the latest values. When a value is not available, the expression can be set as well.



Custom functions in expressions

In addition to using the data sources, custom Visual Basic (VB) functions can also be used in expressions. The System Health Monitoring service will load the file `user_defined_fault.vb`. You can write custom functions and add them to this file. The functions need to return a Boolean and must be valid VB.net syntax.

Example VB function for an expression

One of the faults, “Link Speed Incorrect” only contains a call to the “LinkSpeedNotFull()” function. This function is shown below, and makes WMI calls. VB functions like this can be combined with perfmon and OPC values as wee for more complex fault models. The whole expressions needs to be a valid VB.net expression.

```
'Test() is a sample function
'Function Test() as boolean
'      Test = true
'End Function

Function LinkSpeedNotFull() As Boolean
   Dim strComputer As String
   Dim objWMIService As Object
   Dim objShare As Object
   Dim objInParam2 As Object
   Dim objOutParams1, objOutParams2 As Object
   Dim arrayOfAdapter As Object
   Dim strAdapter As String
   Dim strSpeed As String
   Dim returnValue As Boolean

   returnValue = False
   strComputer = "."
   objWMIService = GetObject("winmgmts:\\" & strComputer & "\
   root\Honeywell")
   objShare = objWMIService.Get("TPS_Config")
   objOutParams1 = objWMIService.ExecMethod("TPS_Config",
   "GetIPAdapterOrder")
   arrayOfAdapter = objOutParams1.sAdapterName
   For Each strAdapter In arrayOfAdapter
      objInParam2 = objShare.Methods_
   ("GetIPAdapterInfoByName").inParameters.SpawnInstance_()
      objInParam2.Properties_.Item("sAdapterName") = strAdapter
      objOutParams2 = objWMIService.ExecMethod("TPS_Config",
   "GetIPAdapterInfoByName", objInParam2)
      strSpeed = objOutParams2.sSpeedDuplexDescription.ToLower()
      If ((strSpeed.Length() > 0) And
   (strSpeed.CompareTo("unknown") <> 0) And
   (strSpeed.IndexOf("100 mb") < 0) And
   (strSpeed.IndexOf("100mb") < 0) And (strSpeed.IndexOf("full")
   < 0)) Then
      returnValue = True
      Exit For
      End If
   Next
   LinkSpeedNotFull = returnValue
End Function
```

Entering an expression for system health monitoring

If you are building a new fault model, you create an expression for system health monitoring using Windows performance counters or objects similar to those available from Perfmon. Building the expression for your own fault model is in addition to the steps for defining its system health rule, rate, description, node type, event message, and priority.

Expression Builder supports data read from two sources - Perfmon counters and OPC. You can use the data for comparisons or in calculations. Each rule can be configured to run on a particular node type and at a specified interval. You can use data in a formula that will return a value once a specified number of values are collected. You can set the formulas to calculate only once (for example, you need to baseline a value) or to continuously calculate.

To enter an expression for a system health rule

1 In the System Health Monitor Expression Builder, click **Points**.

The Expression Builder display appears.

2 Determine whether you want to monitor a performance counter and/or OPC item in your expression.

- Choose the **Performance Counter** tab for monitoring counters similar to those found in Perfmon.
- Choose the **OPC** tab for monitoring OPC item.

3 Configure the following for monitoring Performance Counters

a. Choose either local computer counters or from a list of counters on another computer.

b. Select the Performance Object and its property value.

Tip

Click **Explain** if you need a brief explanation of the selected value.

c. Skip the following step if you do not need an OPC item in your expression.

4 Configure the following for monitoring OPC items.

a. Choose the server machine containing the OPC item.

b. Select the Server ProgID from the drop-down menu.

c. Select the OPC item name.

5 Decide whether to enable a formula. If enabled, determine the following:

- Formula - select from MAX, MIN, AVG, and standard deviation formulas.
- Numbers of values - Enter the number of values you plan to use in the formula.
- Initial calculation only - Enable the checkbox if you want to calculate the formula only once. You would enable this, for example, when you want to baseline a value and compare it to a recalculated value.

6 Decide what to do if a value from a monitored process is not available. You can then enable treat (evaluate) the expression as false or true.

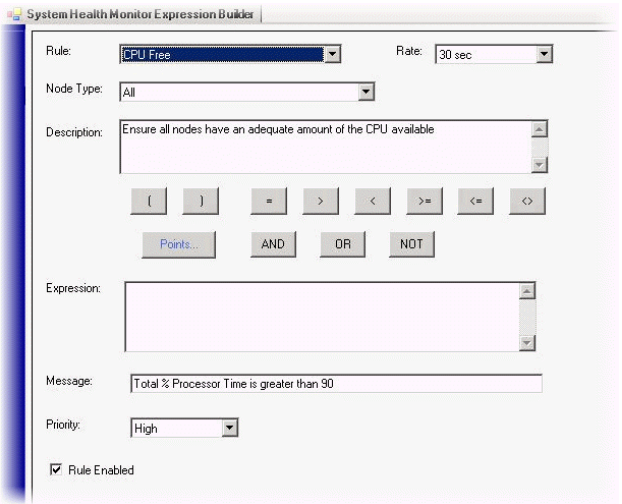
7 Click **Add**.

The expression appears in the System Health Monitor Expression Builder.

System Health Monitor fault models

Fault models evaluate an expression. All System Health Monitoring expressions share the following common settings:

- Rule - name of the rule.
- Rate - frequency at which the rule is executed.
- Node Type - node types on which the rule is run.
- Expression - the rule itself in expression form.
- Message - message associated with this rule.
- Priority - importance of the rule.
- Rule enabled - if the rule is being monitored.
- Save - saves the rule to a local file.
- Synchronize - allows for rules to be saved to other computers.



Index

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

EP-DSX124
11/05