Honeywell

Experion PKS
Administration and Startup Guide

EP-DSX123
210
10/04

Release 210

Honeywell

Document	Release	Issue	Date
EP-DSX123	210	0	October 2004

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
Facsimile	+91-20-2687-8369
Mail	TATA Honeywell Ltd. 55 A8 & 9, Hadapsar Industrial 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

Honeywell Solution Support Online:

`http://www.ssol.acs.honeywell.com`

Training classes

Honeywell holds technical training classes on Experion PKS. 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 PKS, see the *Experion PKS Overview*.

Contents

About this guide

1

This guide is intended primarily for system administrators who are responsible for the administration and maintenance of Release 210 of the Experion PKS 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
Perform a backup and restore of a system.	page 64
Start and stop Experion PKS.	page 27

For information on installing the system, see the *Software Installation and Upgrade Guide*.

For details on configuring Experion PKS after installation, see the *Configuration Guide*.

Before reading this guide

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

- Understand basic Experion PKS concepts such as “channel,” “controller,” “point,” and “Station,” as explained in the *Overview.*
- Install the Experion PKS 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 PKS operator accounts
- Changing passwords

Creating windows user accounts

To enable your users to have access to Experion PKS they must be able to log on to the computers running the Experion PKS 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 PKS. 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 PKS administrator privileges, add this user to the Honeywell Administrators group. Users belonging to this group can use all installed applications and carry out Experion PKS 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 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 PKS 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 PKS services and processes” on page 15.

Deleting a user

Caution

Do not delete the **mngr** user account. If you delete a user 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 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 PKS operator accounts

After you create the required Windows user accounts, if you 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 PKS services and processes

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

Changing the Windows mngr account password

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

Prerequisites

If you have redundant Experion PKS 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:

- In the `Utilities\Password Utility` folder on the Experion PKS R210 Knowledge Builder CD.
- In the `C:\Program Files\Honeywell\Experion PKS\Utilities\PwdUtil` folder on an Experion PKS 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 PKS OPC Interface connects to a third-party OPC server over the network, it uses the Windows mngr account and password on the Experion PKS 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 PKS server computer.

Changing the mngr Password for OPC Integrator

When the Experion PKS OPC Integrator connects to a third-party OPC server over the network, it uses the Windows mngr account and password on the Experion PKS 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 PKS server computer.

Changing the mngr password for ODBC Data Exchange security settings

When the Experion PKS ODBC Data Exchange report connects to an ODBC compliant database over the network, it uses the Windows **mngr** account and password on the Experion PKS 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 PKS server computer.

Changing the mngr password Alarm/Event and report printing settings

When the Experion PKS server attempts to print Experion PKS 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 2000.

Prerequisites

To complete these tasks, you must be logged on as a Windows Administrator.

Tasks

Complete the following tasks:

Task	Go to:	Done?
Create a batch file which starts Station automatically.	page 18	
Specify the batch file as a logon script to the user account.	page 19	

Task	Go to:	Done?
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 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 `\Winnt\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 `\winnt\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 operators 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 `\Winnt\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 is displayed.

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 is displayed.

4 Deselect **Local Policy Setting** for the Users group and the Honeywell Experion PKS Users group 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 `winnt\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 `\winnt\explorer.exe`.
9. Repeat steps 1 through 7 of this task for the file `\winnt\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 **Experion PKS** icon.
5. Right-click the **Station** icon and select **Properties**.
6. In the **Station Properties** dialog box, modify the **Target** field 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 PKS 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.

C200 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 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.

Re-synchronizing the system time

If you are running a redundant system or you have Console Stations you must synchronize the time and date on your servers and Console Stations. However it may also be desirable to synchronize the time if you have a DSA system or point servers. For information on setting up time and date synchronization, see the *Software Installation and Upgrade Guide*.

If you change the time on the computer that is acting as the time source, you need to stop and restart the Time Service on the other computers that synchronize with the time source. For example, If you change the time on the primary server in a redundant server system, (or the primary server is down for some period of time), you need to re-synchronize the time on the backup server with the primary server.

To re-synchronize the time:

1. On the computer that is to be re-synchronized with the time source, select **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Stop and start the **Windows Time** service.

Stopping and starting the server and Console Station

3

Experion PKS software usually runs continuously on the server or Console Station in the background, whether or not a user is logged on.

The Experion PKS software can be stopped and started without shutting down and re-booting the server or Console Station.

Stopping Experion PKS Server or Console Station

You can stop Experion PKS server or Console Station in one of the following ways:

- Use the **Start-Stop Experion PKS** utility in the Experion PKS program group.
- Right-click the **Status** icon in the Windows Taskbar (if applicable) and select **Stop Server** or **Database Unloaded**.
- From a Command Prompt, type:

  ```
  hscserver /stop
  ```

Starting Experion PKS Server or Console Station

You can start Experion PKS server or Console Station in two ways:

- Use the **Start-Stop Experion PKS** utility in the Experion PKS program group.
- From a Command Prompt, type:

  ```
  hscserver /start
  ```

Using the Start-Stop Experion PKS Utility

To stop or start the Experion PKS server:

1 Select **Start > Programs > Honeywell Experion PKS > Server > Start-Stop Experion PKS Server**. The **Start-stop** dialog box displays in either Simple or Full mode.

2 Stop the server using either of the following methods:

- For Simple mode, click **Stop**.
- For Full Mode, select **Database Unloaded**.

3 Start the server using either of the following methods:

- For Simple mode, click **Start**.
- For Full Mode, select **System Running**.

To stop or start the Experion PKS Console Station:

1 Select **Start > Programs > Honeywell Experion PKS > Console Station > Start-Stop Experion PKS Console Station**. The **Start-stop** dialog box displays in either Simple or Full mode.

2 Stop the Console Station using either of the following methods:

- For Simple mode, click **Stop**.
- For Full Mode, select **Database Unloaded**.

3 Start the Console Station using either of the following methods:

- For Simple mode, click **Start**.
- For Full Mode, select **System Running**.

Shutting down the system

To prevent data loss, corruption, or operating system errors, you need to stop the Experion PKS server before you shut down the server computer. Stop the server as described in “Using the Start-Stop Experion PKS Utility” on page 28. When the server is stopped you can shut down the computer in the normal manner.

Tuning a server's performance

4

This section describes how to tune a server's performance. (For a description of specialized terms, see "Specialized terms" on page 30.)

Notes

- These topics are also generally applicable to Console Stations.

Specialized terms

This section describes the specialized terminology applicable to tuning the performance of Experion PKS servers.

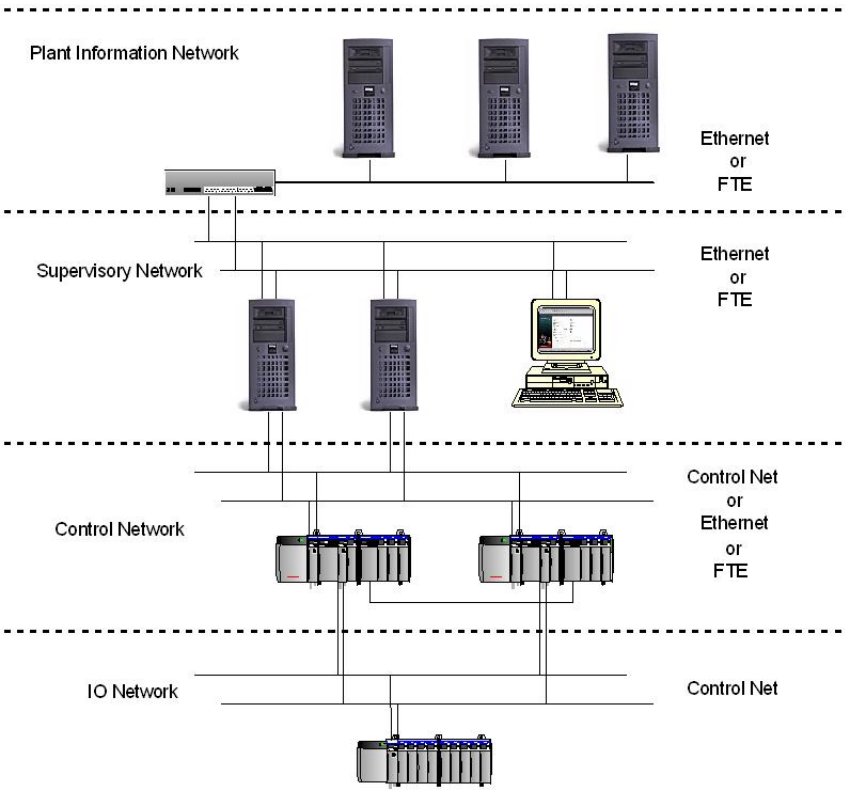
Performance describes the speediness of a system to react to series of tasks, and the ability to perform those tasks in a reliable manner. There are two aspects of performance:

- **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 PKS 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 Plant Information.



Life cycle phases

There are two life cycle phases:

- **Configuration**. During the configuration phase engineers use various tools to configure control hardware and software for processes. Hardware components are defined, strategies are implemented, system limits are calculated, and so on.
- **Operational**. During the operational phase Experion PKS runs as a standard client/server system.

Tuning the operating system

These procedures describe how to tune the Windows kernel for each of the Windows versions used by Experion PKS. (Tuning the kernel changes the way Windows assigns process priorities.)

Note

You do not need to tune the operating system if you purchased a system that was supplied with Installation Services (the NT5Plus/XPPlus operating system) because it has already been configured for optimal performance in the operational phase.

Prerequisites

- To tune the operating system, you must be logged on with Windows administrator privileges.

Tuning the Windows 2000 Server kernel

Tuning Windows 2000 Server is a two-step process that involves:

- Setting the application response
- Tuning the server service

Prerequisites

- Check whether user-applications, such as Microsoft Excel, Control Builder or Station, run on the server. (If user-applications do not run on the server, it is known as a *headless node* server.)

Considerations

- It is recommended that you do not run user-applications on the server.

Setting the application response

Considerations

- 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.
- If you run applications on the server during the operational phase, 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. Click **Performance Options**.
4. Click **Background services** if you are running a headless node server.

   The Windows operating system assigns higher priority to background services, such as Experion PKS server, than to user-applications.
5. Click **Application** if you are *not* running a headless node server.

   The Windows operating system assigns higher priority to user-applications, such as Station or Control Builder, than to background processes.
6. Click **OK**.

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 PKS 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 PKS server	Maximize data throughput for network applications
ACE	Balance
Engineering Repository server	Maximize data throughput for network applications
SCE	Balance

5 Click **OK**.

Tuning the Windows 2000 Professional kernel

To tune Windows 2000 Professional:

1. Right-click the **My Computer** icon on the Desktop, and choose **Properties**.
2. Click the **Advanced** tab.
3. Click **Performance Options**.
4. Click **Applications**.

   The Windows operating system assigns higher priority to user-applications, such as Station or Control Builder, than to background processes.
5. Click **OK**.

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 to display the **Performance Options** dialog box.
5. Click the **Advanced** tab.
6. In the Processor scheduling group, click **Programs**.
7. In the Memory usage group, click **Programs**.
8. Click **OK**.

   The Windows operating system assigns higher priority to user-applications, such as Station or Control Builder, than to background processes.

Optimizing the server's hard disk performance

The performance of a hard disk can greatly affect the performance of the computer. The two factors that affect the performance of a disk are:

- Fragmentation, which occurs gradually over time
- File system errors, which are typically caused by power outages or hardware malfunctions
- This procedure is also applicable to Console Stations.

Defragmenting the hard disk

Although the NT file system (NTFS) attempts to minimize file system fragmentation, it is typically the most frequent performance problem that occurs during normal computer operations.

"Fragmentation" means that, when a file or piece of data is written to the hard disk, it is not written contiguously. 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 fragmentation 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 effect 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 to defragment and choose **Properties**.
3. Click the **Tools** tab.
4. Click **Defragment now** in the Defragmentation group to display the **Disk Defragmentor** dialog box.

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

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

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

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

Fixing file system errors

Requirements

- Your process must be "off control" before fixing file system errors.
- Check that no other applications are running because the procedure involves restarting the computer.

To fix file system errors:

1. On the Windows Desktop, double-click the **My Computer** icon.
2. Right-click the hard disk to check and choose **Properties**.
3. Click the **Tools** tab.
4. Click **Check Now** in the Error-checking group to display the **Check Disk** dialog box.
5. Click **Automatically fix files system errors** and then click **Start**.
6. Click **Yes** to schedule the operation to occur the next time the computer is started.
7. Restart the computer.

   The computer checks for file system errors during startup.
8. Log on.
9. Review the disk report in the Event Viewer. To display the Event View:
   a. On the Desktop, right-click the **My Computer** icon 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 procedure 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 because it usually indicates that the hard disk is experiencing hardware malfunctions.

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 2000, 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).

Clients/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

To adjust the pagefile on Windows 2000 Professional and Server:

1. On the Windows Desktop, right-click the **My Computer** icon and choose **Properties**.
2. Click the **Advanced** tab.
3. Click **Performance Options**.
4. Click **Change** to display the **Virtual Memory** dialog box.
5. Click the drive containing the pagefile.
6. Type the **Initial size** and **Maximum size** values that you calculated.
7. Click **Set**, and then click **OK**.

   For these changes to take effect, you need to restart the computer. When you click **OK** to accept previous dialog boxes, you are prompted to restart the computer.

To adjust the pagefile on 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** to display the **Virtual Memory** dialog box.
7. Click **System managed size**, and then click **Set**.

   For these changes to take effect, you need to restart the computer. When you click **OK** to accept previous dialog boxes, you are prompted to restart the computer.

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 works 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 32.

The order in which the system accesses the network is also important—this is known as the *binding order*. It is recommended the binding order is 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

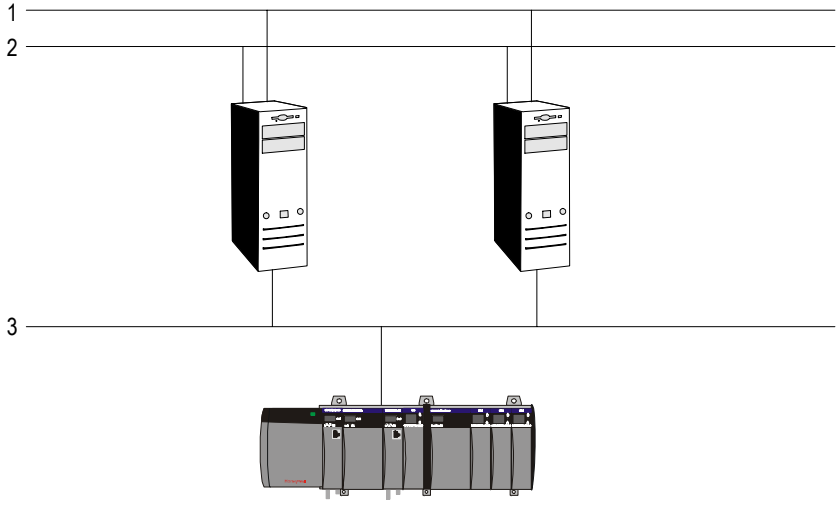
If your control system uses Ethernet as the control network, you can achieve network performance benefits by restricting the type of traffic over this network.

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** to display the **Advanced Settings** dialog box.
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

Setting connection names

If your cards are unnamed, you need to set the connection names.

To set the connection names:

1. On the Windows desktop, right-click the **My Network Places** icon and choose **Properties**.
2. Right-click on the connection name for the "A" or "Yellow" network, and click **Rename**.
3. Type in the new connection name based on the following convention:
   `FTE <Community Name> Yellow`

   For example, **`FTE SID Yellow`**
4. Right-click on the connection name for the "B" or "Green" network, and click **Rename**.
5. Type in the new connection name based on the following convention:
   `FTE <Community Name> Green`

   For example, **`FTE SID Green`**
6. Choose **Start** > **Run**.
7. Type **`cmd`** and then click **OK** to display a Command Prompt window.
8. If the computer is running:
   - Windows 2000, type **`nbtstat -n`** to verify the new connection names.
   - Windows XP, type **`netdiag /test:Bindings`** to verify the new connection names.

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.

To identify network interface card ports and connecting network cables:

1. Connect the yellow network cable to the switch in the yellow tree.
2. Connect the green network cable to the switch in the green tree.
3. Connect the yellow network cable (yellow boot) to one of the network interface card ports.

4 On the Windows desktop, right-click the **My Network Places** icon and choose **Properties** to display the **Network and Dial-up Connections** dialog box.

5 If the status of the FTE Yellow connection is **Network cable unplugged**, connect the Yellow network cable to the other network interface card port.

The connection status must be **Enabled**.

6 Connect the green network cable (green boot) to the other network interface card port.

The connection status of both connections must be **Enabled**.

Adjusting TCP/IP binding order

To adjust the TCP/IP binding order:

1 On the Windows desktop, right-click the **My Network Places** icon and choose **Properties** to display the **Network and Dial-up Connections** dialog box.

2 Choose **Advanced** > **Advanced Settings** to display the Advanced Settings dialog box.

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.

4 Click **OK**.

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

6 Click **Internet Protocol (TCP/IP)** and then click **Properties** to display the Internet Protocol (TCP/IP) Properties dialog box.

7 Click **Advanced** to display the **Advanced TCP/IP Settings** dialog box.

8 In **Interface Metrics**, type `1`.

9 Click the **WINS** tab.

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

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

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

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

14 Click **Internet Protocol (TCP/IP)** and then click **Properties** to display the **Internet Protocol (TCP/IP) Properties** dialog box.

15 Click **Advanced** to display the **Advanced TCP/IP Settings** dialog box.

16 In **Interface Metrics**, type **5**.

17 Click the **WINS** tab.

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

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

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

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`. 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. See the *Advanced Online Documentation and the Network Planning Guide* for further details.

Optimizing other server settings

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 that this may produce anomalies in some displays.

In order to receive the best performance, the video card should use the AGP bus and contain at least 32 MB of VRAM. 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 type 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 21.

Optimizing topology-related settings

Physical location of systems

The location and distance between each node becomes a factor in the performance. Experion PKS 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.

Station 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 "Checking the server's performance" on page 21.

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 PKS server have an impact on the server's CPU and memory usage. This must be taken into consideration when planning the hardware purchase for your server. See the Advanced Documentation set for more information.

Network integration

Integrating the Plant Networks with the Companies 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. If considering this type of integration, you must plan this into your hardware purchase for your server. See the *Experion PKS Network Planning Guide* for more information.

Optimizing the scanning load

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

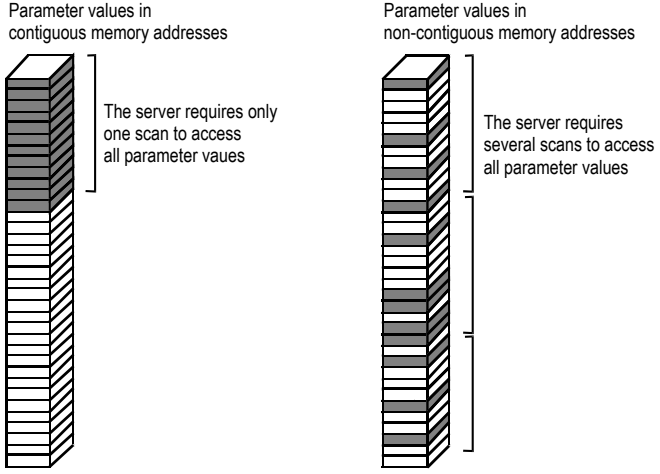
Controllers with badly configured scanning can place a significant load on the system and result in data not being accurately represented in the server database.

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 system and 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 58.
- 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 13	
Use **trace** utility to record the communications activity for heavily loaded channels.	page 830	
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.

Backups and recovery

5

This chapter discusses backup and recovery strategies and procedures for the server, the Engineering Repository Database (ERDB), and Console Station.

Performing backups and recovery

This section provides some general advice on backup strategies.

The procedures in this section assume that you are using Microsoft Windows Backup. If you want to use other third-party backup software, contact your local Honeywell Technical Assistance Center for the latest information about qualified backup software.

Deciding on a backup strategy

Performing backups is the most important of system administration tasks. If backups of important data such as the server database and configuration files are not made, the data will be lost if a hardware failure (such as a hard disk crash) occurs, or if files are accidentally deleted.

Choosing an appropriate backup strategy allows you to minimize the downtime due to various situations that cause loss of data. When choosing your backup strategy, consider the types of situations that can occur:

- Media failure—if one or more disk drives fails, there is a potential for a complete loss of data unless the system was properly backed up.
- User error—if a user makes invalid modifications to data, for example, changing the control strategy or modifying displays, an effective way to undo these changes is to restore the data from backup.
- Permanent loss of a server—if a server becomes permanently unusable, for example due to natural disaster, unless you have a backup the system and data have to be reconstructed.

It is important to decide on a backup strategy for the system. The backup strategy should include:

- What will be backed up
- Who will be responsible for backups
- How often it will be backed up
- The verification of backups
- The storage of backups
- The testing of backups
- Procedures for recovering from a system crash

Ideally, the backup strategy for your system should be documented and a copy kept with the system.

Deciding what to back up

To recover from the various situations in which you can lose data, consider the types of information you need to include in a backup. For example:

- Operating system and Windows specific data including:
  - System state data such as boot files
  - System registry data
  - User account information
  - Microsoft system files such as operating system files and patches
- Experion PKS data on the server and Console Station
- Engineering repository database
- Enterprise Model database
- Event archives
- History archives

The following table lists the items to back up and where they are located on your server.

Table 1 Backup Items and Folders on a Server

Item	Folder to Back Up
Experion PKS server database	`c:\Program Files\Honeywell\Experion PKS\server\data`
Enterprise Model database (EMDB)	`c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\er`
Engineering Repository (ERDB)	`c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\er`
Quick Builder database	`c:\Program Files\Honeywell\Experion PKS\server\data\qdb`
Events database	`c:\Program Files\Honeywell\Experion PKS\server\evtarch`
History archive files (default folder)	`c:\Program Files\Honeywell\Experion PKS\server\archive`
Custom files	`c:\Program Files\Honeywell\Experion PKS\server\user`
Custom applications	`c:\Program Files\Honeywell\Experion PKS\server\user\applic\src`

Table 1 Backup Items and Folders on a Server

Item	Folder to Back Up
Report output files	`c:\Program Files\Honeywell\Experion PKS\server\report`
Custom displays	`c:\Program Files\Honeywell\Experion PKS\client\abstract`
BOOTPDATA.TXT	`c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\bin`
RSLinx configuration information	Use the RSLinx backup utility. See “RSLinx configuration file” on page 74.

The following table lists items to back up and where they are located on the Console Station.

Table 2 Backup Items and Folders on a Console Station

Item	Folder to Back Up
Experion PKS Console Station database	`c:\Program Files\Honeywell\Experion PKS\server\data`
Custom files	`c:\Program Files\Honeywell\Experion PKS\server\user`
Station.ini file	`c:\winnt` for Windows 2000 Professional or `c:\windows` for Windows XP
Menu files, startup scripts, alarm.wav files	`c:\Program Files\Honeywell\Experion PKS\client\station`
Custom displays	`c:\Program Files\Honeywell\Experion PKS\client\abstract`
BOOTPDATA.TXT	`c:\Program Files\Honeywell\Experion PKS\Engineering Tools\system\bin`

You might want to back up other files or folders on your server. Examples include:

- Microsoft Excel Spreadsheets
- The Experion PKS server run folder (if you have installed custom applications or updates)
- Additional history archive folders

You should also ensure that you have a backup of the configuration for each Flex Station or Console Extension Station:

Table 3 Backup Items and Folders on a Flex Station

Item	Folder to Back Up
Station.ini file	`c:\winnt` for Windows 2000 Professional or `c:\windows` for Windows XP
Menu files, startup scripts, alarm.wav files	`c:\Program Files\Honeywell\Experion PKS\client\station`
Custom displays	`c:\Program Files\Honeywell\Experion PKS\client\abstract`

Deciding how often to back up

Deciding how often to back up depends on how much data your site can tolerate to lose. Ideally, the Experion PKS database should be backed up every day, and other items should be backed up whenever they change.

For example, during system configuration, backups should be made daily, as configuration data is constantly changing. After system configuration is complete, configuration data only needs to be backed up when the configuration changes.

If history archiving is done weekly, then the history archive folder should be backed up every week.

Suggested backup strategy

Note

You can also use this strategy to back up a Console Station, however a Console Station does not have the events database or history archive files.

Use this strategy to ensure that the entire contents of an Experion PKS server computer is backed up. This strategy enables you to recover from most situations.

1. Create an image of the hard drive after installing the operating system, service packs, security patches, and the Experion PKS software. Use disk-imaging software to create an image. See the documentation for your disk-imaging software.

   Restoring an image restores the computer name and the IP address. For this reason you should create an image for each computer.

   If you change the computer name or the IP address, you should create a new image.

2. Create an emergency repair disk (ERD) using the Backup utility included with Windows 2000 System Tools. The ERD will allow the system to be recovered if your system becomes unbootable.

3. Create a backup of the Experion PKS data after you have configured your system so that you have a backup of your configuration. You might consider doing this sort of backup on a daily basis while you are configuring your system. See “Backing up Experion PKS using fullbkup” on page 70.

4. Create a backup of your system state data if you make changes to your registry settings. See “Backing up Windows system state data” on page 73.

5. Create regular backups of your events database and history archive folders. See “Backing up the events database” on page 72 and “Back up considerations for history archive files” on page 69.

6. Create regular backups of other files and folders that are important to your system. Use the Windows Backup utility. See “Backing up specific folders” on page 69.

Creating an emergency repair disk

The emergency repair disk (ERD) allows the system to be repaired in situations where you have an unbootable system. An ERD can help you to repair your system without having to restore the entire disk image.

To create an emergency repair disk:

1. Insert a blank, formatted 1.44 Mb floppy disk into the computer's floppy disk drive.
2. Choose **Start > Programs > Accessories > System Tools > Backup**.
3. On the **Welcome** tab, click **Emergency Repair Disk**.
4. Follow the instructions that appear on your screen.

Back up considerations for history archive files

If your system uses history archiving, free space on the archiving disk must be checked regularly.

When the disk becomes full you can either:

- Save the history archives to a backup tape and then delete them (if you are saving archives to the server hard disk), or
- Remove the removable disk and replace it with a new one.

To back up and restore history archives to and from tape, you can either use the Windows backup and restore function, or use your own backup system of choice.

Caution

If you delete an archive folder, it cannot be recovered unless it has been previously saved to off-line media.

Backing up specific folders

Considerations

- This procedure uses the Microsoft Windows Backup program. Event Archiving uses the same program to save/restore events to tape. You should not use Backup at the same time that Event Archiving is saving/restoring events to/from tape.
- The server database and the EMS database cannot be backed up directly. If you want to back up the entire server you use **fullbkup**. See “Backing up Experion PKS using fullbkup” on page 70.
- It is advisable to enable the **Verify After Backup** and **Backup Registry** options during backup.
- If your drive supports hardware compression you might also want to enable **Hardware Compression**, which will allow more data to be stored on the tape.

Prerequisites

- You must be logged on with an account that belongs to the Administrators group or the Backup Operators group.

To back up specific folders:

1. Insert a tape in the tape drive.
2. Choose **Start > Programs > Accessories > System Tools > Backup** to start the Windows backup program.
3. Select the folders that you want to back up.
4. Click **Backup**, and then click **OK**.
5. Make sure that the backup tape is labelled correctly with the time, date, and details about options used when making the backup.

For more details, see your Microsoft Windows documentation or online help.

Backing up Experion PKS using fullbkup

Using **fullbkup** enables you to back up your Honeywell folder and its subfolders, the Engineering Repository database (ERDB), and the Enterprise Model database (EMDB) to tape or other media such as CD.

You can use the **fullbkup** utility on an Experion PKS server or Console Station.

The **fullbkup** command automatically creates copies of the databases that cannot be backed up directly. If you are backing up to tape, these copies are then included in the backup of the Honeywell folder. If you are backing up to other media, backing up the Honeywell folder will include the copies of the databases.

Syntax

```
fullbkup [FILE] [TAPE "tapedrive"]
```

Considerations

- The tape drive name is found in Windows Backup. Click the Backup tab and look in the Backup destination field for your tape drive name.
- If you back up to CD, the CD recording software may not complete the backup because of the “live” database files.
- If you back up to CD, when backup is complete you must delete the backup copies of the server database and the events database.

- An entry for the tapedrive you are backing up to must exist in the Backup media pool before you use **fullbkup**. To ensure this entry exists, run Windows backup.
- If you have the Engineering Repository you must be logged on with a Windows account that belongs to the Engineering Repository Administrator Group.

To create a tape backup using fullbkup:

1. If the server to be backed up is a member of a redundant server pair, synchronize the Experion PKS server and the ER databases:
   a. From the system menu in Station, select **View > System Status > Server Redundancy**.
   b. On the Server Redundancy display, select **Synchronize**.
   c. (For systems with the Engineering Repository only.) From Control Builder, use **Tools** > **Synchronize Engineering database now**.
2. Check that all Experion PKS client applications are closed on the computer to be backed up, such as Station, Display Builder, and Quick Builder.
3. Insert a tape in the computer's tape drive.
4. Open a command prompt window (**Start** > **Programs > Accessories** > **Command Prompt**).
5. Type the command:

   `fullbkup TAPE "`*`tapedrive`*`"`

   where ***`tapedrive`*** is the name of the tape drive you want to use for this backup. For example, **`fullbkup TAPE "4mm DDS"`**.

   The **fullbkup** command copies files, then displays the Windows Backup program. No further action is needed until the procedure completes.
6. Make sure that the backup tape is labelled correctly with the time, date, and details about options used when making the backup.
7. To review the success of the backup, start Windows backup program and select **Tools > Report**.

For more details about the Windows Backup program, see your Windows documentation or online help.

To create a backup to other media using fullbkup:

1. Check that all Experion PKS client applications are closed on the computer to be backed up, such as Station, Display Builder, and Quick Builder.
2. Open a command prompt window (**Start** > **Programs > Accessories** > **Command Prompt**).

3 Type the command:

fullbkup FILE

4 When **fullbkup** is complete make a backup of the `Program Files\Honeywell\Experion PKS` folder and its subfolders to your preferred media.

Backing up the events database

You can create a local copy of the events database to include in a backup to tape or other media. Experion PKS can continue to run during the copy.

The copy of the events database is created in the folder `c:\Program Files\Honeywell\Experion PKS\server\evtarch\backup`.

The events database is backed up when you use **fullbkup**. You might want to use this procedure if you want to back up the events database more frequently than you than you create a backup using **fullbkup**.

To back up the database:

1 Start Microsoft SQL Server Enterprise Manager (select **Start** > **Programs** > **SQL Server**)

2 Expand the left tree down the path **Microsoft SQL Servers > SQL Server Group > <Computer Name> > Management > SQL Server Agent > Jobs**

3 Start the job named `EMS Maintenance` (right-click the Backup job and select **Start job**)

Backing up the Enterprise Model database

Use this procedure if you want to back up the enterprise model database only.

Prerequisites

- You must be logged on with an account that belongs to either the Administrators group or the Backup Operators group.

To back up the enterprise model database:

1 Start Configuration Studio and connect to the system that contains the EMDB you want to back up.

2 In the Configuration Explorer, click the system item.

3 Click the **Administer the system database** task.

The Db Admin console opens.

4 Expand the tree and click **EMDB Admin Tasks**.

5 Click the **Backup database** task.

6 Browse to the folder where you want to back up the database, type the name of the backup file, and then click **Save**.

7 Click **OK** to confirm the backup.

8 Close the Db Admin application.

Backing up Windows system state data

Backing up the Windows System State Data ensures you have a backup of the following components:

- Registry
- COM+ Class Registration database
- Boot files such as Ntdr and Ndetect.com and system files

For more information about backup up Windows System State Data, see the Microsoft Windows online help.

Prerequisites:

- You must be logged on with an account that belongs to either the Administrators group or the Backup Operators group.

To back up the system state data:

1 If backing up to tape, insert a tape into the tape drive.

2 Choose **Start > Programs > Accessories > System Tools > Backup** to start the Windows backup program.

3 Click the **Backup** tab.

4 Select the **System State** check box.

5 Click **Start Backup**.

Additional files

If your system also has RSLinx, you need to consider the following files:

- RSLinx Activation file
- RSLinx Configuration file
- bootpdata.txt file

RSLinx activation file

RSLinx is a third party windows-based communication software component provided by Rockwell Automation to interface to various Honeywell and Rockwell automation hardware, including CNI cards, Control Net, PCI-C card.

RSLinx is installed with software copy protection. This protection is not backed up using either the **fullbkup** utility or the Microsoft Windows Backup utility and therefore the copy protection cannot be restored. The software protection is physically encoded into sectors on a hard disk. In the case of a hard disk replacement the copy protection needs to be re-activated.

As an alternative to backing up you can move the RSLinx Activation file to either the RSLinx floppy diskette that it was distributed on or the root directory of a server share.

If a hard drive fails, with the RSLinx activation on the drive, you need to contact Rockwell to restore the activation, see `http://support.rockwellautomation.com/`. Rockwell offers one free activation restoration per year.

If you have to replace a hard disk but you do not have the activation file on disk, you must go to Rockwell's site or contact your local Honeywell Technical Assistance Center to restore it. If the activation file can be removed before the disk is replaced, then moving the disk off the hard drive and back onto the replacement drive ensures the copy protection can then be applied to the new disk.

RSLinx activation is independent of the PCIC and Ethernet modules. The PCIC or Ethernet modules can be replaced without affecting the RSLinx activation file.

RSLinx configuration file

A Microsoft Windows full system backup will back up configuration information for the RSLinx communication software component, however, the Experion PKS **fullbkup** utility will not. If the RSLinx configuration information has changed since the last Microsoft Windows full backup, you must use the supplied RSLinx Driver Configuration utility to backup the driver configuration.

The RSLinx Driver Configuration contains information required for the RSLinx communication software to communicate to the plant devices. For example:

- The user defined name of the driver, such as PCIC-1, ETH-1
- MAC addresses of the PCIC cards
- The Ethernet drivers of the configured Ethernet devices

The RSLinx backup utility can be used to copy driver configuration information onto several servers.

To use the RSLinx backup utility:

1 Choose **Start** > **Programs** > **Rockwell Software** > **RSLinx** > **Backup Restore Utility**.

2 Specify a filename and location to store the configuration information.

This configuration file can now be copied to a safe backup location or backed up using the Microsoft Windows backup utility. See “Backing up specific folders” on page 69.

bootpdata

The Bootpdata.txt is an Experion PKS file that contains IP address information of 10 Mbps and 10/100 MBps Ethernet Communication devices on the Supervisory Network (that is, TC-CEN011 and TC-CEN021). These devices are configured using the Remove Devices via Linx Gateway drivers in RSLinx.

The Experion PKS server contains a built-in BOOTP Data Server that allows Ethernet devices to discover their IP addresses in topologies where a domain controller is separated from the Ethernet communication devices. The BOOTP Data Server (which resides on both the Primary and Secondary Experion PKS servers) needs its configuration information backed up.

The BOOTPDATA file is backed up using the Microsoft Windows full backup utility, however, the Experion PKS **fullbkup** utility does not backup BOOTP Data configuration information.

The configuration information resides in `\Program Files\Honeywell\Experion PKS\Engineering Tools\SYSTEM\BIN\BOOTPDATA.TXT`. This file can be copied to a network share, backup medium, or use Microsoft Windows backup utility to back it up.

Recovery scenarios

This section describes various scenarios from which you might have to recover. The scenarios assume that the suggested backup strategy is used.

Note

Recovering a Console Station is similar to recovering an Experion PKS server however you do not need to recover the Engineering Repository, the events database, or history archives.

Repairing your Windows system

If you encounter problems starting your computer, use the Windows 2000 emergency repair feature to fix problems that may be preventing you from starting your computer.

To repair your Windows system:

1. Start your computer from the Windows 2000 Setup disks or CD.
2. The Setup program will ask whether you want to continue installing the Windows 2000 operating system. Press **ENTER** to continue.
3. The installation process asks whether you want to install a fresh version of Windows 2000, or to repair an existing installation. Press **R** to repair.
4. Press **R** again to use the emergency repair process.
5. Select the fast repair option.
6. Have your ERD ready to start the repair process.

Recovering from hard disk failure

If you encounter a hard disk failure, you can quickly recover your system as follows:

1. Replace the hard disk.
2. Restore the disk image. See the documentation supplied with your disk-imaging software.
3. Restore Experion PKS data. See “Restoring Experion PKS data from a backup made using fullbkup” on page 79.
4. If you have a more recent backup of the events database, restore the events database. See “Restoring the events database” on page 82.

5 Restore system state data if you made changes such as registry changes after you created the disk image.

6 Restore any other files that were backed up since you created the disk image.

If you have a backup of your system state data that is more recent than your emergency repair disk, restore your system state data after repairing your system.

Recovering from a virus attack

Any computers that are compromised by a virus or unauthorized access is in an unknown state. As a result, the computer could contain hidden programs that allow unauthorized access to the computer, programs could be embedded into other programs, exist in hidden sectors or be disguised.

To recover from a virus attack:

1 Remove the computer from the network.

2 Reformat the hard disk.

3 Restore the disk image. See the documentation supplied with your disk-imaging software.

4 Restore Experion PKS data. See “Restoring Experion PKS data from a backup made using fullbkup” on page 79.

5 If you have a more recent backup of the events database, restore the events database. See “Restoring the events database” on page 82.

6 Restore system state data if you made changes such as registry changes after you created the disk image.

7 Restore any other files that were backed up since you created the disk image.

Replacing a computer

If you have to replace a computer for any reason, regardless of whether you have a disk image and a backup of the Experion PKS data, you should not restore the image. Instead, you should set up the computer as though it is a new computer.

To replace a computer:

1 Install the operating system and Experion PKS software as described in the *Software Installation and Upgrade Guide*.

2 Restore the Experion PKS data. See “Restoring Experion PKS data from a backup made using fullbkup” on page 79.

3 If you have a more recent backup of the events database, restore the events database. See “Restoring the events database” on page 82.

Restoring a redundant Experion PKS Server

If your system has the Engineering Repository, use the procedure documented in the section Restoring redundant Experion PKS Servers and the Engineering Repository.

If the computer you are restoring is part of a redundant server system, then it is likely that the data on the running server is more up-to-date than the backed up data.

To restore a redundant server:

1 Restore the disk image. See the documentation supplied with your disk-imaging software.

2 Synchronize the restored server with the running server.

Restoring redundant Experion PKS Servers and the Engineering Repository

In situations where you are restoring one server of a redundant server pair, you need to consider whether the most recent and most reliable copy of the data is on the backup set or in the redundant partner's database.

This section refers to the primary and secondary servers as SERVERA and SERVERB respectively.

For example, if restoring a backup that was made some time ago, the data on that tape will most likely be out of date. After the restore, the Experion PKS databases should be updated from the other server using the procedures outlined below.

If however the Engineering Repository database was corrupted on SERVERB, it is possible that the SERVERA backup copy is also corrupted as a result of replication of the corrupted data. In this case the data at SERVERB should be restored from a backup made using **fullbkup** utility. Then the database replica at SERVERA can be restored from SERVERB using the DbAdmin utility.

To restore SERVERB:

1 Restore the disk image. See the documentation supplied with your disk-imaging software.

2 Restore Experion PKS data. See "Restoring Experion PKS data from a backup made using fullbkup" on page 79

3 Restore SERVERB databases.

If you are:	See:
Restoring from a backup made using fullbkup	Restoring the Engineering Repository database
Recovering the primary database	"Restoring SERVERB Engineering Repository databases" on page 83

To restore SERVERA:

1. Restore the disk image. See the documentation supplied with your disk-imaging software.
2. Restore Experion PKS data. See “Restoring Experion PKS data from a backup made using fullbkup” on page 79.
3. Restore SERVERA databases. See “Restoring SERVERA Engineering Repository databases” on page 84.

Restoring the EMDB databases

In situations where you are restoring one server of a redundant server pair, you need to consider whether the most recent and most reliable copy of the data is on a backup file or in the redundant partner’s database.

This section refers to the primary and secondary servers as SERVERA and SERVERB respectively.

For example, if restoring a backup that was made some time ago, the data on that backup will likely be out of date. After the restore the EMDB should be updated from the other server.

If however the EMDB on SERVERB was corrupted it is possible that the SERVERA backup copy is also corrupted as a result of replication of the corrupted data. In this case the data on SERVERB should be restored from a backup. Then the backup copy on SERVERA can be restored from SERVERB using the DBAdmin utility.

If you are:	See:
Restoring from a backup	“Restoring the Enterprise Model database” on page 87
Recovering the primary database	“Restoring the SERVERB Enterprise Model database” on page 87
Recovering the secondary database	“Restoring the SERVERA Enterprise Model database” on page 88

Restoring Experion PKS data from a backup made using fullbkup

There are two parts to restoring Experion PKS server data:

- Restoring the files from the backup media
- Restoring the data

If you are:	Do this:
Restoring from tape	1. Restore the files from tape, see page 80. 2. Restore the data, see page 81.
Recovering from other media	1. Copy the `Honeywell\Experion PKS` folder and subfolders from the backup media to the server replacing the existing `Honeywell\Experion PKS` folder. 2. Restore the data, see page 81.

Considerations

- This procedure can only be used to restore to the identical hardware platform as the tape backup was made from. In particular, the adapters must be compatible with the drivers that were backed up on the original system.
- If you are restoring an Experion PKS system that includes the Engineering Repository, see "Restoring redundant Experion PKS Servers and the Engineering Repository" on page 78.
- If any of the following Windows user accounts or groups have been deleted, you need to re-install the Experion PKS software before attempting to restore data.
  - mngr
  - Honeywell Administrators group
  - Engineers group
  - Engineering Repository Users group
  - Engineering Repository Administrators group
- Although this procedure restores event archives, they are not reattached as SQL databases. You need to follow the procedure to restore event archives as documented in the *Operators Guide*.

To restore the backup files from tape:

1 Log on as Administrator. Insert the backup tape that was made previously into the computer's tape drive.

2 Select **Start** > **Program** > **Accessories > System Tools** > **Backup**, to run the Windows Backup program to restore the tape.

3 Click the Restore tab.

4 Select the check boxes for the folders and files you want to restore.

5 Click the System State check box to restore system state data.

6 Select **Tools > Options** and click the General tab.

7 Ensure the Verify data after backup completes is checked, and click **OK**.

8 Click **Start Restore** to start the restore operation.

9 If you are restoring SERVERB and your system contains the Engineering Repository, skip this step and go to steps 10 and 11. After the restore completes, reboot the computer and start the procedure to restore the backup server data.

10 If your system contains the Engineering Repository you need to disable replication. On SERVERB select **Start > Programs > Experion PKS Engineering Tools > DBADMIN**.

11 Select the **Admin Tasks** in the tree view then select **Disable Replication**.

12 Restore the data using postrestore.

Restore the data using postrestore:

1 Open a command prompt window (**Start** > **Programs** > **Accessories > Command Prompt**).

2 Run the program **postrestore**. This copies the backed up server data into the correct folder then starts the services. Reply **yes** when asked if you want to start Server.

3 Verify that the following were restored correctly:

- **Machine name**: Use Network Neighborhood to verify that the computer is configured with the correct name.
- **User accounts**: Use **Start** > **Programs** > **Administrative Tools** > **User Manager**.
- **ODBC data source**: Use **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Data Sources (ODBC)** to verify your ODBC data source.

4 Use **Start** > **Settings** > **Control Panel** > **Services** and verify that all Experion PKS services have started correctly.

5 Use **Start** > **Programs** > **Honeywell Experion PKS** > **Server** > **Start-Stop Experion PKS**, and verify that Server is running.

If the server being restored is a member of a redundant pair, you need to synchronize the databases:

1 Fail over if necessary so that the recovered computer is Secondary.

2 Synchronize the Server databases (**View > System Status > Server Redundancy**).

Restoring Windows system state data

To restore Windows System State Date:

1. If restoring from tape, insert the tape into the tape drive.
2. Choose **Start > Programs > Accessories > System Tools > Backup**.
3. Click the **Restore** tab.
4. Select the **System State** check box.
5. Click **Start Restore**.

Restoring the events database

To restore the database:

1. Check in `c:\Program Files\Honeywell\Experion PKS\server\evtarch\backup` to determine which Backup file you want to restore. This is usually the file with the most recent date and time, but it depends on your circumstances. Note the name of this file.
2. Start Microsoft SQL Server Enterprise Manager (select **Start > Programs > SQL Server**).
3. Expand the left tree down the path:

   Microsoft SQL Servers > SQL Server Group > *`PC Name`* > Databases > EMS Events
4. Right-click the EMS Events Database and select **All Tasks > Restore Database...**
5. In the Restore Database dialog box, ensure that:
   - **Restore as database** is set to `EMS Events`
   - **Restore** is set to `From Device`

   Press the **Select Devices** command button and add a new device

   `c:\Program Files\Honeywell\Experion PKS\server\evtarch\backup\EMSDailyBackup.dat`

   Click **OK** until you return to the Restore Database dialog box.
6. Leave the default values for the other settings:

   Backup number = `1`

   Restore backup = `set`

   Database = `Complete`
7. In the **Restore Database** dialog box, select the **Options** tab.
8. Select the **Force restore over existing database** check box.

9 Select **OK** to run the restore.

If you have any errors, stop SQL Server and then restart it, to ensure that no one else is connected to the database.

Restoring the Engineering Repository database

Use the following procedure to restore a backup copy of the Engineering Repository database.

To restore the ERDB from a backup:

1 Start Configuration Studio and connect to the Experion PKS server.

2 In the Configuration Explorer, click **Control Strategy**.

3 Click the **Administer the control strategy database task**.

4 Expand the DBAdmin and Server Node tree.

5 Click **ERDB Admin tasks**.

6 If you have redundant servers, click **Disable Replication** to ensure that database replication is stopped.

7 Click **Restore Database**.

8 At the prompt to disable replication, click **OK**.

9 Locate the backup of the ERDB and click **Open**.

10 When restoration is complete click **OK**.

11 Click **Enable Replication**.

Restoring SERVERB Engineering Repository databases

This procedure is applicable only if you have the Engineering Repository and you are restoring a server that is part of a redundant pair.

Use this procedure after a restoration of a backup of SERVERB to update it with the latest copy of the databases from SERVERA. This procedure may also be used if SERVERB databases are corrupt and the SERVERA databases are known to be good.

To restore the databases:

1 On SERVERB**,** open Windows Explorer and delete any snapshot files that were restored. These will be in the same directory, with the filename <controllername>.snapshot. Note that they are hidden files so ensure that the option **View All Files** is enabled.

2. On SERVERB, use Windows Explorer to locate the files on the SERVERA computer and copy them to SERVERB. They can be located in the folder `\\<servera>\hybrid\system\er` and will be named according to the CPM name with the extension `.snapshot`. Copy the files to `C:\Program Files\Honeywell\Experion PKS\tps50\system\er`, overwriting any files there.
3. On SERVERB, select **Start > Programs > Experion PKS Engineering Tools > DbAdmin** to start the DbAdmin tool.
4. Click **Disable Replication** to ensure that database replication is stopped.
5. Click **Recover Primary Database**.
6. Click **Enable Replication** to start ER database replication.
7. Bring the real time System Repository database on SERVERA in sync with SERVERB as follows.
   a. Select **Start > Settings > Control Panel > Administrative Tools > Services**.
   b. Select **Experion PKS System Repository** and select **Stop**.
   c. Select **Yes** to stop the Control Data Access service also. After services have stopped, select the **Control Data Access** service and select **Start**. Close the services applet.
8. Use the Station Server Redundancy display to verify SERVERA is running as primary.
9. At the SERVERA Station Server Redundancy display, initiate server synchronization to make the SERVERB runtime database concurrent with SERVERA.

Restoring SERVERA Engineering Repository databases

This procedure is applicable only if you have the Engineering Repository and you are restoring a server that is part of a redundant pair.

Use this procedure after a restoration of a backup to SERVERA to update SERVERA with the latest copy of the database from SERVERB.

Prerequisites

- You have restored SERVERA using the procedure in “Restoring Experion PKS data from a backup made using fullbkup” on page 79.

To restore databases:

1. On SERVERB Station Server Redundancy display, initiate server synchronization to make the SERVERA runtime database concurrent with SERVERB.
2. At SERVERB, select **Start > Programs > Experion PKS Engineering Tools > DbAdmin**.
3. Select **Disable Replication** to ensure that database replication is stopped.
4. Select **Recover Secondary Database**.
5. Select **Enable Replication** to start ER database replication.
6. Go to the SERVERA machine. Delete any snapshot files in `C:\Program Files\Honeywell\Experion PKS\tps50\system\er` folder. These files will be named according to the CPM name with the extension .snapshot. Note that they are hidden files so ensure that the explorer option to View All Files is enabled.
7. Bring the real time System Repository database on SERVERA in sync with SERVERB as follows:
   a. Select **Start > Settings > Control Panel** and double-click **Services**.
   b. Select **Experion PKS System Repository** and click **Stop**. Click **Yes** to stop the Control Data Access service also.
   c. After the services have stopped, select the **Control Data Access** service and click **Start**.
   d. Close Services.

Synchronizing Engineering Repository server database

Use this procedure after either an Engineering Repository database restoration of SERVERB or a corruption of the SERVERA Engineering Repository database to bring SERVERA back in sync with SERVERB:

1. On SERVERB, select S**tart > Programs > Experion PKS Engineering Tools > DbAdmin** and select **Disable Replication** to disable database synchronization.
2. If SERVERA is running as primary, use the Station Server Redundancy display to fail over to SERVERB.
3. Select **Disable Replication** to ensure that database replication is stopped.
4. Select **Recover Primary Database**.
5. Select **Enable Replication** to start ER database replication between the redundant servers.

Controller database issues

Caution

Be sure your process is “Off Control” as these procedures require that the controller be idled and/or a new database loaded.

After a restore of the Experion PKS database, the database and controllers may be out of sync if there were changes made to the control strategy or controller parameter values since the backup was made.

If there were no changes to control strategy since the backup, the current parameter values can be updated by uploading the controller to the ER database, then updating the project from loaded. In addition, the snapshot files should be re-saved from the controller.

If there were control strategy changes, the changes would need to be re-entered to the ERDB project database after it has been restored. Once this is done, the controller can be updated by loading the missing blocks as follows:

1. Add the new blocks to the project side of the ER database. Do not load the new blocks yet.
2. For each controller that had changed since the backup, load the controller snapshot that was restored with the database to delete the controller copies of the new blocks. This must be done as these new blocks are now “ghost” points and cannot be deleted directly.
3. Note that if the added blocks were IOM’s, the snapshot load may fail. In this case you will have to bring the controller to the NODB state either by using NTOOLS or by pulling the batteries and power cycling the controller, then load the snapshot.
4. Load the newly added blocks.
5. If there were external connections to the added blocks, any blocks referencing them in other Control Modules or controllers (if peer-to-peer) will also have to be reloaded to update the references to these blocks.
6. When complete, re-save the controller snapshot and create a new backup of the updated database.

After SERVERB has been restored on a system containing redundant servers, you need to be careful concerning the snapshot files. If older snapshot files are restored to SERVERB, the synchronization will attempt to update them from SERVERA, causing them to now be out of sync with the database. The solution is to delete the snapshot files from SERVERA after the database has been replicated and before ER synchronization has been enabled.

Restoring the Enterprise Model database

Use this procedure to restore a backup copy of the Enterprise Model database.

Prerequisites

- You must be logged on with an account that belongs to either the Administrators group or the Backup Operators group.

To restore the enterprise model database:

1. Start Configuration Studio and connect to the system that contains the EMDB you want to back up.
2. In the Configuration Explorer, click the system item.
3. Click the **Administer the system database** task.
   The Db Admin console opens.
4. Expand the DBAdmin and Server Node tree.
5. Click **EMDB Admin Tasks**.
6. Click **Disable Replication**.
7. Click **Restore database**.
8. Browse to location of the backup file and click **OK**.
9. Click **Enable Replication**.
10. Close DbAdmin.

Restoring the SERVERB Enterprise Model database

Use this procedure to make a backup of the SERVERA EMDB and use it to restore the SERVERB EMDB for example if the SERVERB EMDB is corrupt and the SERVERA EMDB is known to be good.

To restore the SERVERB EMDB:

1. Start Configuration Studio and connect to the system that contains the EMDB you want to back up.
2. In the Configuration Explorer, click the system item.
3. Click the **Administer the system database** task.
   The Db Admin console opens.
4. Expand the DBAdmin and Server Node tree.
5. Click **EMDB Admin Tasks**.
6. Click **Disable Replication**.

7 Click **Recover Primary database**.

8 Follow the on-screen instructions to complete the procedure.

9 Click **Enable Replication**.

10 Close DbAdmin.

Restoring the SERVERA Enterprise Model database

Use this procedure to make a backup of the SERVERB EMDB and use it to restore the SERVERA EMDB.

To restore the SERVERA EMDB:

1 Start Configuration Studio and connect to the system that contains the EMDB you want to back up.

2 In the Configuration Explorer, click the system item.

3 Click the **Administer the system database** task.

The Db Admin console opens.

4 Expand the DBAdmin and Server Node tree.

5 Click **EMDB Admin Tasks**.

6 Click **Disable Replication**.

7 Click **Recover Secondary database**.

8 Follow the on-screen instructions to complete the procedure.

9 Click **Enable Replication**.

10 Close DbAdmin.

Index

Honeywell

Honeywell Process Solutions
2500 West Union Hills
Phoenix AZ 85027
USA