Honeywell

Experion PKS
Diagnostic Studio User's Guide

ESDOC-XX28-en-2301A
July 2014

Release 230.1

Honeywell

Document	Release	Issue	Date
ESDOC-XX28-en-2301A	230.1	0	July 2014

Disclaimer

Contents

1 About this guide

This guide provides the instructions to use Diagnostic Studio.

Revision history

Revision	Date	Description
A	January 2014	Initial version

References

Refer to the following documents for more information.

- Installation Builder User's Guide
- Experion Support and Maintenance Software Change Notice

Security consideration

It is important to understand the security considerations before proceeding. For security-related information, ensure to refer to the *Experion Network and Security Planning Guide*.

2 Introduction

Related topics

“About Diagnostic Studio” on page 8

2.1 About Diagnostic Studio

The Diagnostic Studio provides system diagnostics and configuration analysis for Experion. The Diagnostic Studio supports detection and troubleshooting, thus providing the ability to quickly correct Experion software, node configuration and network related problems.

Diagnostic Studio provides an intuitive and easy-to-use user interface that enables you to perform troubleshooting and analytical tests on the Experion PKS system.

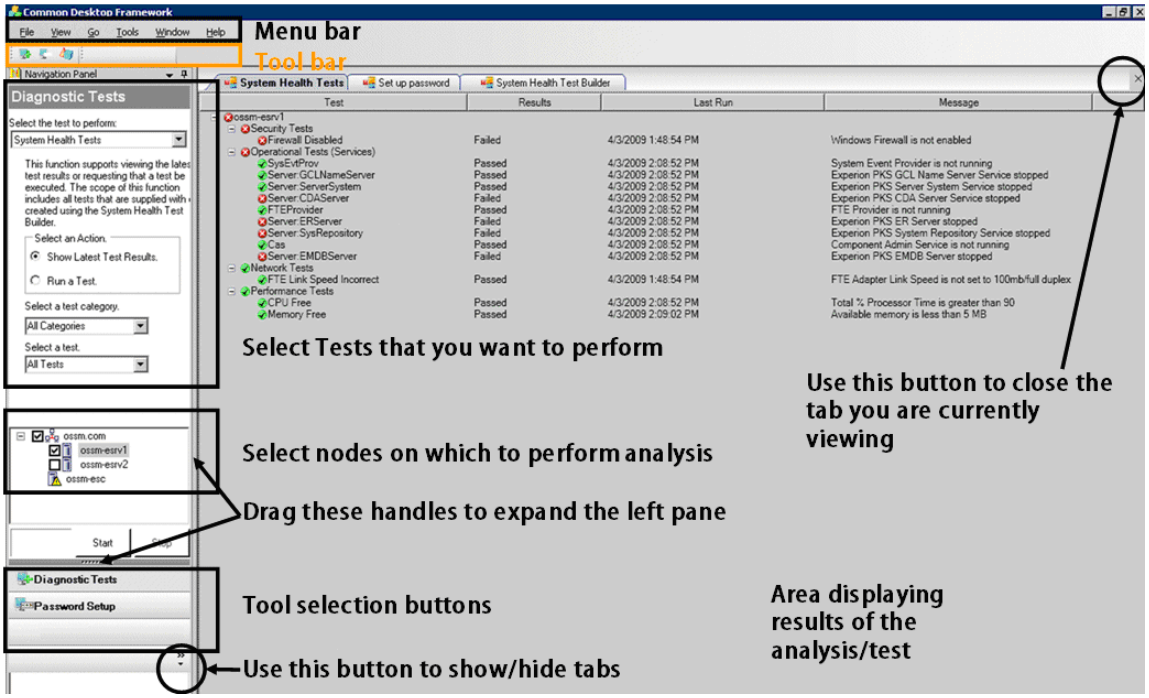


Figure 1: Common Desktop Framework

Use the Diagnostic Studio to analyze one or more similar devices. For example, you can select a group of computers and verify if their “Hosts” files are configured correctly. You will receive a verification status for each node selected and analyzed. When the analysis tool detects a system incompatibility, the tool presents recommended options to fix the incompatibility.

Diagnostic Studio tasks

Use Diagnostic Studio to enable the following capabilities:

- Node configuration analysis using Diagnostic Tests
- Domain and local account synchronization Password Setup

You can perform initial analysis on nodes within the network tree using the following Diagnostic Tests tools:

- Network analysis tools
- Security analysis tools

Diagnostic Studio log files

Detailed information about any analysis you perform is recorded in a system analysis log file.

Before using Diagnostic Studio

Node definition in the IDB

Before you can use the Diagnostic Studio on any node, the node’s configuration settings must be defined in the Installation Database (IDB). This is accomplished by using the Installation Builder. If the node is not defined in the Installation Builder, it will not appear in the Diagnostic Studio network tree. If the node is defined but does

not have valid configuration data, it will show in the tree with a special icon and a pop up help message indicates that the condition needs to be corrected.

Access privileges for the Diagnostic Studio

All analysis tools require you to be have specific privileges in order to access and modify network devices.

- With ESM 200 for the Experion R400 release, if the system is in a domain, you must log on with Domain Administrator privilege. If the system is in a Workgroup, you must still log on with Administrator privilege. There are certain tests, for example, the Com Server Setting Verification test, which can only be run on the local node in order to execute the fix action successfully.

3 Analyzing Network Configuration

Use Network Analysis Tools to evaluate the network configuration settings on each node within the network tree. You can use Network Analysis Tools to verify host files, LCN settings, and NTP settings.

Related topics

“Verifying hosts files” on page 12
“Verifying LCN settings” on page 13
“Verifying NTP settings” on page 14

3.1 Verifying hosts files

Use this tool to retrieve the IP addresses of computers in the Network Tree's database and determine if the hosts files on selected computers are consistent with the hosts file in the system definition. After reviewing the hosts files, the tool sends a verification status for each node indicating if the files are correct. If there is a discrepancy, you are given the option of updating the hosts file on selected nodes. This tool performs the following checks:

1. Hosts file is present
2. Format of hosts file is correct (no badly formed lines)
3. Hosts file has all of the hosts identified in the IDB
4. No discrepancies with IDB
5. No conflicting lines for computers not in IDB

To verify hosts files consistency

1 From the Diagnostics Studio, click the **Diagnostic tests** at the bottom on the left pane.

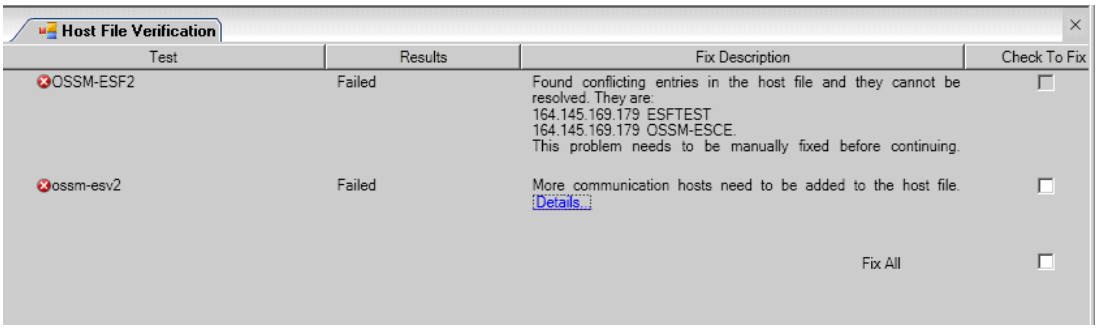
2 From the Select a test to perform list, select **Network Analysis**.
The list of network analysis tests is displayed.

3 Select the **Hosts File Verification** option.

4 Select each computer that needs the hosts file verified for consistency in IP addressing and node naming.

5 Click **Start**.

6 Review the results displayed on the right pane and determine if any further actions are needed.



7 Click **Stop** when done.

3.2 Verifying LCN settings

Use this tool to verify if the LCN configuration for the selected nodes is correct. The tool queries each selected node and verifies if the following LCN configurations are consistent with the values defined in the IDB:

1. Computer is a T-Node
2. LCN Address matches IDB
3. LCN Communication Status is good (registry key)
4. LCN Personality File is installed

With this tool, you can fix errors in the LCN settings found on a given node and save the results of the LCN configuration analysis to a file.

To verify LCN settings

1 From the Diagnostics Studio, click the **Diagnostic tests** button at the bottom on the left pane.

2 From the **Select a test to perform** list, select Network Analysis.
The list of network analysis tests is displayed.

3 Select the **LCN Settings Verification** option.

4 Select each computer that needs its LCN settings verified.

5 Click **Start**.

6 Review the results displayed on the right pane and determine if any further actions are needed.

7 Click **Stop** when done.

3.3 Verifying NTP settings

Use this tool to verify that the NTP (Network Time Protocol) settings for selected nodes are configured properly. The IDB is the source for the NTP configuration information. This tool compares the NTP configuration information retrieved from IDB and verifies the following settings:

1. NTP is enabled.
2. NTP Settings in Registry match Honeywell defaults

Example

NTP Client Settings	Honeywell Default Value
FrequencyCorrectRate	4
HoldPeriod	5
LargePhaseOffset	50000000
MaxAllowedPhaseOffset	1
MaxNegPhaseCorrection	54000
MaxPosPhaseCorrection	54000
PhaseCorrectRate	1
PollAdjustFactor	5
SpikeWatchPeriod	900
UpdateInterval	100
AnnounceFlags	10
EventLogFlags	2
LocalClockDispersion	10
MaxPollInterval	15
MinPollInterval	10

To verify NTP settings

1 From the Diagnostics Studio, click the **Diagnostic tests** button at the bottom on the left pane.

2 From the **Select a test to perform** list, select **Network Analysis**. The list of network analysis tests is displayed.

3 Select the **NTP Settings Verification** option.

4 Select each computer that needs the correct link speed verified and click **Start**.

5 Review the results displayed on the right pane and determine if any further actions are needed.

6 Click **Stop** when done.

4 Verify Security Settings

Use Security Analysis Tools to evaluate the configuration options related to security on each node within the network tree. Security Analysis Tools includes COM server settings verification and Link domain settings verification.

4.1 Verifying COM Server Settings

Use this tool to verify the DCOM configuration settings for the Honeywell OPC server: Experion OPC Server, TPN Server, System Event Server, and System Performance Server. For each selected computer, the tool looks for a server and for those found, it verifies the following settings to check if they are consistent as per Honeywell recommendations:

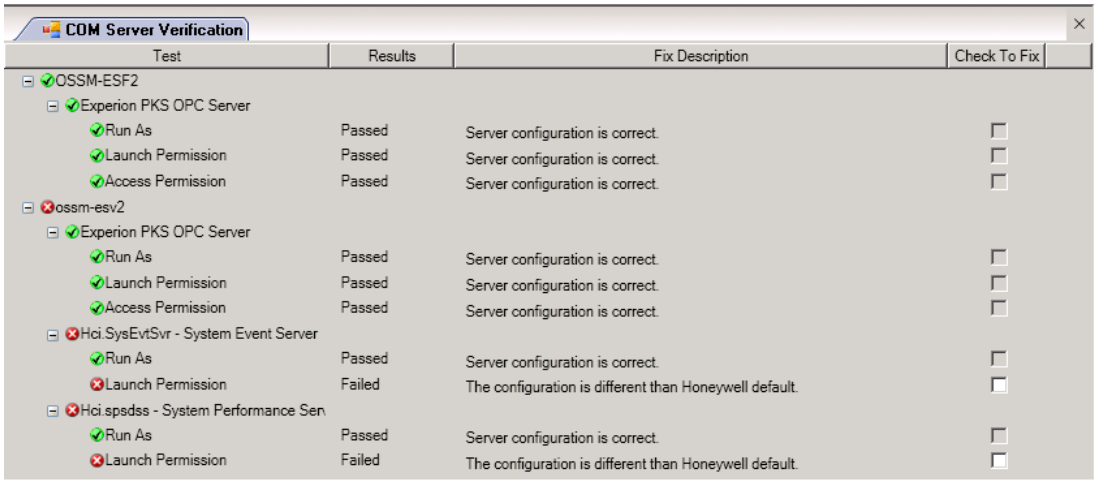
- RunAs account
- Launch Permission
- Access Permission settings

If they are not, the tool flags inconsistencies and gives you the option of configuring the settings to be consistent with Honeywell's recommendations.

If the node is in a domain, you must log on with the Domain Administrator account in order to run the fix action for remote nodes. Even if the Local Administrator account exists on all the nodes in a system (for example, ". \mngr" account), logging on with this account and performing the Run Fix action would succeed on R3xx nodes, but fail for R400 nodes. This is due to more strict Windows security changes. However, if you have set up your R400 system in a workgroup environment, and if a problem is identified, you must go to that local node to open Diagnostic Studio and run this test and run the fix action there.

To verify COM Server settings are consistent with Honeywell recommendations

1. Launch the Diagnostic Studio and click the **Diagnostic tests** button at the bottom on the left pane.
2. From the **Select a test to perform** list, select **Security Analysis Test**.
3. Click the **COM Server Settings Verification** option.
4. From the network tree on the left pane, select each computer that needs the COM Server settings verified. The **COM Server verification** tab appears on the right pane with the results.
5. Review the results and determine if any further actions are needed.



6. Click **Fix** to fix the errors.
7. Click **Save to File** to save this file for future reference.

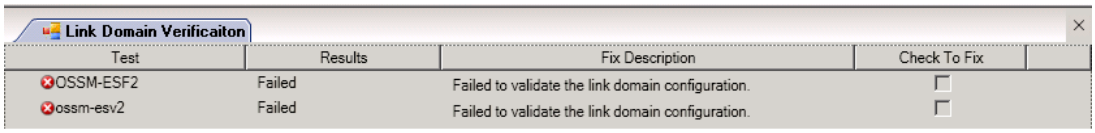
4.2 Verifying Link Domains

After a node is installed in the domain, the link domains script must be manually run in order to link Domain Groups to Local Groups. Use this tool to verify the script was applied to the node. If the tool determines it was not, you will be given the option of running the script.

You must have Domain Administrator privilege in order to execute this test and run the fix action.

To verify link domains script

1. Launch the Diagnostic Studio and click the **Diagnostic tests** button at the bottom on the left pane.
2. From the **Select a test to perform** list, select **Security Analysis Test**.
3. Click the **Link Domain Verification** option.
4. From the network tree on the left pane, select each computer that needs the link domains script verified. The **Link Domain Verification** tab appears on the right pane appears with the results.
5. Review the results and determine if any further actions are needed.



6. Select the Link domain configuration that is erroneous and click **Fix** to fix the errors.
7. Click **Save to File** to save this file for future reference.

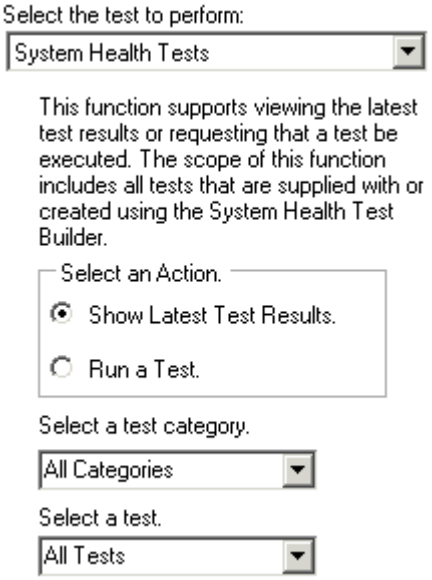
5 System Health Tests

Use System Health Tests to view the status of the system health monitoring tests running on each node in the network . You can view the status (Pass/Fail) of the tests and when the test was last executed. In addition to viewing the test results, you can request to run/execute a test.

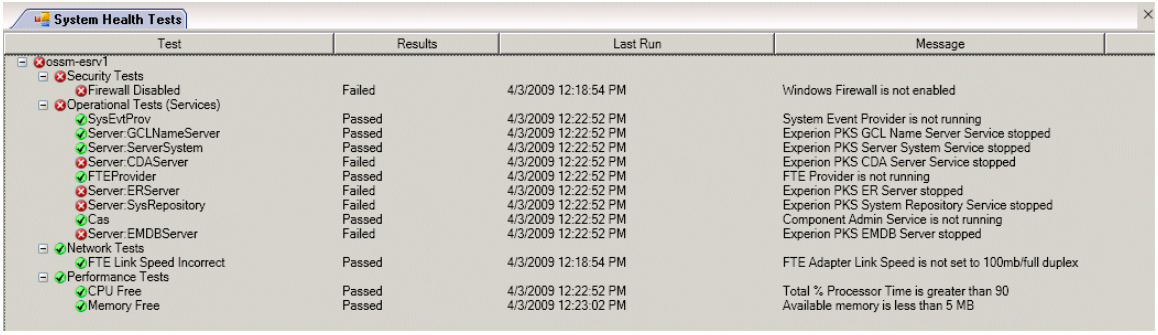
5.1 Viewing current status of a test

To view the current status of a test

1. Launch the Diagnostic Studio and click the **Diagnostic tests** button at the bottom on the left pane.
2. From the **Select a test to perform** list, select **System Health Tests**.
3. Select the **Show Current Test Status** option.
4. Select the category under which the test whose status you want to view is saved from the **Select Test Category** list.
5. The Select Test list displays all tests that have been defined for the selected test category. Select the test whose status you want to view from the **Select Test** list.
6. From the network tree on the left pane, select each computer on which the test you selected was run.



7. The **System Health Test Results** tab appears on the right pane with the results. Review the results and determine if any further actions are needed.



5.2 Run tests

To run tests

1. Launch the Diagnostic Studio and click the **Diagnostic tests** button at the bottom on the left pane.
2. From the **Select a test to perform** list, select **System Health Tests**.
3. Select the **Run Tests** option.
4. Select the category under which the test that you want to run is saved from the **Select Test Category** list. The **Select Test** list displays all tests that have been defined for the selected test category.
5. Select the test that you want to run from the **Select Test** list.
6. From the network tree on the left pane, select each computer on which you want to run the test. The **System Health Test Results** tab appears on the right pane with the results.
7. Review the results and determine if any further actions are needed.

6 Password Setup

The password of a local or Domain account used for DCOM servers or Windows services must be in sync. Sometimes, after you change the password for an account, you may forget to change the password for the DCOM servers or Windows services that run under this account. This tool enables you to change the password on the Domain or Local Accounts and then update all DCOM Servers and windows services in the system that uses those accounts with the new password. When using this tool, all selected computers that are operational and connected to the network are updated. This tool does not require the IDB.

This tool requires Domain Administrator privilege. If the node is in a domain, you must log on with the Domain Administrator account in order to set the password for remote nodes. Although the Local Administrator account exists on all the nodes in a system (for example, ".\mngr" account), logging on with this account and performing the Set Password action would succeed on R3xx nodes, but fail on R400 nodes. This is due to more strict Windows security changes. However, if you have set up your R400 system in a workgroup environment, you must go to that local node to open Diagnostic Studio and run this tool there.

6.1 Setting up passwords

Use this tool to change the password on the Domain or Local Accounts, then update all DCOM Servers and windows services in the system that use those accounts with the new password. When you use the password tool, you update all selected computers that are operational and connected to the network (that is, usage of the Password Tool does not require the IDB).

About DCOM and services passwords

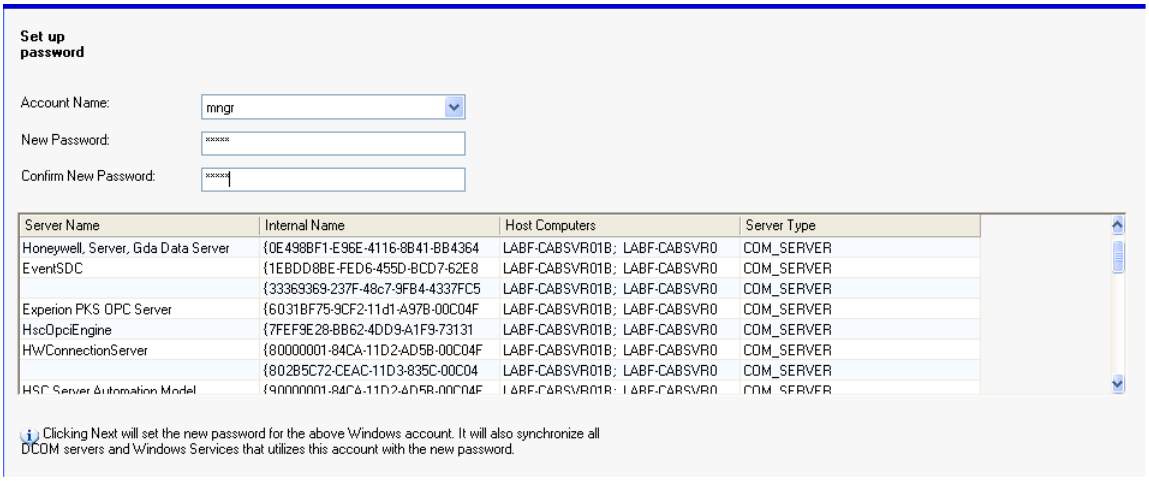
When the password of a local or Domain account used for DCOM servers or Windows services has been changed, you must update the password for all DCOM Servers and windows services in the system using that account.

Attention

Any password changes may not be effective until the listed service or application is restarted.

Setting up and synchronizing DCOM and services passwords

1 Launch the Diagnostic Studio and click the **Password Setup** button at the bottom on the left pane.



2 Select each computer that has an account needing a password update. The **Setup password** tab appears on the right pane.

3 Select the **Account Name**.

4 Enter and confirm the new password. If necessary, confirm any messages.

5 Review the results and determine if any further actions are needed.

6 Click **Next** to set the new password for the selected Windows account. All COM servers and Windows services that utilize this account will also be synchronized.

7 Configuring System Performance and Event Monitoring

The Windows environment contains event and performance information, which can be used for the proactive and reactive management of your system. System errors such as disk errors or a problem with the FTE network can be detected through performance and event monitoring. You integrate Windows-based system event and performance information with Experion by using the System Event Server, System Performance Server, and System Management software components. You can enable specific notifications and performance data to be collected by the System Event Server and the System Performance server using Configuration Studio. The SES and SPS then send these notifications and data to the Experion server as OPC events and data items, using a system interface that is automatically configured. As a result, notifications are included in the System Status display and the Event Summary. You can also add Windows data to HMIWeb displays.

7.1 Enabling notifications using an Event Filter

This topic describes the tasks required to enable notifications so that they are included in the System Status display. To do this, you create event filters.

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

About event filters

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

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

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

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

Considerations

The Event Filter tool provides Help with detailed descriptions of the event characteristics that are useful when assigning event types to your event filter.

To enable notifications using an event filter:

1. Choose **Start** > **Programs** > **Honeywell Experion PKS** > **System Management** > **System Management Display**.
2. If the Honeywell Event Configuration snap-in is installed and configured, go to step 6. Otherwise, continue to step 3.
3. Choose **File** > **Add/Remove Snap-in**. The **Add/Remove Snap-in** dialog appears.
4. Click **Add.** A list of available stand-alone snap-in programs appears.
5. Scroll through the list and double-click **Event Filter Configuration**. The Event Filter snap-in is added to the tree in the **Management Console** window.
6. Right-click **Event Filter** and choose **All Tasks** > **New** in the pop-up menu. The **Select an Event Source** dialog box appears.
7. Expand the **Application** tree and select appropriate event source.
8. Click **OK**. Under **Event Filter**, an xml file appears.
9. Click the xml file name.
10. Review the events.
    If you want an event to be displayed in the System Status display, do the following:
    - Right-click on the event and choose Configure Event in the pop-up menu.
    - The Assign Event Type dialog box appears.
    - Select the Enabled check box.

- Click Finish to return to the list of events.

11 Right-click the xml file and choose **All Tasks** > **Save** in the pop-up menu. Save this file in the C:\HWIAC \filter folder.

7.2 Setting up System Performance Servers

This topic describes enablers such as SNMP Monitoring for System Performance Server to provide you performance data. System Performance Server does not require user configuration, unless you need to change default settings described in this section.

7.2.1 Changing the System Performance Server scope

In general the default scope of domain is sufficient. If errors are being generated in the event logs because of access problems to specific nodes, change the scope to exclude the problematic nodes.

To change the scope of the System Performance Server

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

7.2.2 Adding system performance data to displays

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

To create a custom display and to display system data

1. Start HMIWeb Display Builder:
   - If you are on the Experion server, choose **Start** > **Programs** > **Honeywell Experion PKS** > **Server** > **HMIWeb Display Builder**.
   - • If you are on a client computer, choose **Start** > **Programs** > **Honeywell Experion PKS** > **Client Software** > **HMIWeb Display Builder**.
2. Choose **File** > **New** > **Display**.
   A blank display appears.
3. Click the (Alphanumeric) icon on the **Toolbox** toolbar and then drag the pointer on the display to define the size, shape and position of an alphanumeric.
4. Double-click the alphanumeric to open the **Properties** window, which shows the alphanumeric's current properties.
5. Click the **Data** tab and make sure that **Point/Parameter** is selected in **Type of database link**.
6. Select **SYSMGT** from the point list.
7. In the **Parameter** box, type the alias for the data item you want to display in the format computername.alias, for example, localhost.BiosVersion.

7.2.3 Common performance data items

The following table lists the default aliases that have been created for the most common performance data items.

Alias	Description
BiosSerialNumber	The BIOS serial number of the specified computer.
BiosVersion	The BIOS version number of the specified computer.
DiskCFreeMegabytes	The amount of free disk space in Megabytes on the C drive of the specified computer.
DiskCFreeSpace	The amount of free disk space in bytes on the C drive of the specified computer.
DiskCPercentFreeSpace	The amount of free disk space as a percentage of the total disk space on the C drive of the specified computer.
DiskCSize	The size of the C drive of the specified computer.
DiskDFreeMegabytes	The amount of free disk space in Megabytes on the D drive of the specified computer.
DiskDFreeSpace	The amount of free disk space in bytes on the D drive of the specified computer.
DiskDPercentFreeSpace	The amount of free disk space as a percentage of the total disk space on the D drive of the specified computer.
DiskDSize	The size of the D drive of the specified computer.
FreePhysicalMemory	The amount of free physical memory on the specified computer.
FreeVirtualMemory	The amount of free virtual memory on the specified computer.
OS_Name	The name of the operating system installed on the specified computer.
OS_SerialNumber	The serial number of the operating system installed on the specified computer.
OS_ServicePackMajorVersion	The major version number of the latest operating system service pack installed on the specified computer.
OS_ServicePackMinorVersion	The minor version number of the latest operating system service pack installed on the specified computer.
OS_Version	The version number of the operating system installed on the specified computer.
Processor0ClockSpeek	The clock speed of the first processor on the specified computer.
Processor0LoadPercentage	The processor load as a percentage of the first processor on the specified computer.
Processor0Name	The name of the first processor on the specified computer.
Processor1ClockSpeed	The clock speed of the second processor on the specified computer.
Processor1LoadPercentage	The processor load as a percentage of the second processor on the specified computer.
Processor1Name	The name of the second processor on the specified computer.
TotalPhysicalMemory	The total amount of physical memory on the specified computer.

Alias	Description
UserName	The name of the user currently logged on to the specified computer.

8 Notices

Trademarks

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

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

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

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

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.

8.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

8.2 How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.

  or

- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

8.3 Support and other contacts

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC).

North America

Country	Phone	Facsimile	Email
Canada and United States	800-822-7673	973-455-5000	asksscc@honeywell.com

Northern Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Denmark	07:00 – 18:00	80–252165	+45 6980 2349	hpscustomersupport@honeywell.com
Finland	08:00 – 19:00	0800–9–15938	+358 (0)9 2319 4396	hpscustomersupport@honeywell.com
Ireland	06:00 – 17:00	1800939488	+353 (0)1 686 4905	hpscustomersupport@honeywell.com
Netherlands	07:00 – 18:00	0800 020 3498	+31 (0)20 524 1609	hpscustomersupport@honeywell.com
Norway	07:00 – 18:00	800–11478	47–852–287–16	hpscustomersupport@honeywell.com
Sweden	07:00 – 18:00	0200883167	+46 (0)8 509 097 84	hpscustomersupport@honeywell.com
United Kingdom	06:00 – 17:00	08002797226	+44 (0)20 3031 1064	hpscustomersupport@honeywell.com

Southern Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Belgium	07:00 – 18:00	080048580	+32 (0)2 791 96 02	hpscustomersupport@honeywell.com
France	07:00 – 18:00	0805100041	+33 (0)1 72 74 33 44	hpscustomersupport@honeywell.com
Luxembourg	07:00 – 18:00	8002–8524	+352 24611292	hpscustomersupport@honeywell.com
Spain	07:00 – 18:00	800099804	+34 91 791 56 25	hpscustomersupport@honeywell.com
Portugal	06:00 – 17:00	800–8–55994	+34 91 791 56 25	hpscustomersupport@honeywell.com

Eastern Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Bulgaria	08:00 – 19:00	700 20771	+359 (0)2 489 7384	hpscustomersupport@honeywell.com
Croatia	07:00 – 18:00	0800 80 6392	+420 227 204 957	hpscustomersupport@honeywell.com
Czech Republic	07:00 – 18:00	800 142 784	+420 227 204 957	hpscustomersupport@honeywell.com
Hungary	07:00 – 18:00	06 800 20 699	+36 (06) 1 577 7371	hpscustomersupport@honeywell.com
Poland	07:00 – 18:00	00 800 121 50 46	+48 22 485 35 10	hpscustomersupport@honeywell.com
Romania	08:00 – 19:00	0 800 800 178	+40 (0)31 710 7590	hpscustomersupport@honeywell.com
Russia Federation	09:00 – 20:00	8.10.80 02-412 50 11	+7 495 796 98 94	hpscustomersupport@honeywell.com

Country	Local Time Business Hours	Phone	Facsimile	Email
Slovakia	07:00 – 18:00	0800 002 340	+421 (0)2 3301 0376	hpscustomersupport@honeywell.com

Central Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Austria	07:00 – 18:00	0800 006438	+43 (0)1 253 6722 4904	hpscustomersupport@honeywell.com
Germany	07:00 – 18:00	0800 7239098	+49 (0)30 6908 8463	hpscustomersupport@honeywell.com
Greece	08:00 – 19:00	00800 12 9493	+30 21 1 268 6973	hpscustomersupport@honeywell.com
Israel	08:00 – 19:00	1 809 407 309	+972 (0)2 591 6148	hpscustomersupport@honeywell.com
Italy	07:00 – 18:00	8000 35205	+39 06 96681356	hpscustomersupport@honeywell.com
Switzerland	07:00 – 18:00	00 080 035	+41 (0)31 560 41 60	hpscustomersupport@honeywell.com

Middle East and South Africa

Country	Local Time Business Hours	Phone	Email
Bahrain	08:00 – 19:00	8008 1343	hpscustomersupport@honeywell.com
Oman	08:00 – 19:00	8007 7595	hpscustomersupport@honeywell.com
Qatar	08:00 – 19:00	800 5460	hpscustomersupport@honeywell.com
Saudi Arabia	08:00 – 19:00	800 844 5309	hpscustomersupport@honeywell.com
South Africa	07:00 – 18:00	0800 983 634	hpscustomersupport@honeywell.com
Turkey	08:00 – 19:00	00800 448823587	hpscustomersupport@honeywell.com
United Arab Emirates	09:00 – 20:00	8000 444 0300	hpscustomersupport@honeywell.com

Other regions

In other regions, contact your local Honeywell Technical Assistance Center (TAC) for support.

Region	Phone	Facsimile	Email
Pacific	1300-364-822 (toll free within Australia) +61-8-9362-9559 (outside Australia)	+61-8-9362-9564	GTAC@honeywell.com
India	+91-20-6603-2718 / 19 1800-233-5051	+91-20-6603-9800	Global-TAC-India@honeywell.com
Korea	+82-80-782-2255 (toll free within Korea)	+82-2-792-9015	Global-TAC-Korea@honeywell.com
People's Republic of China	+86-21-2219-6888 800-820-0237 400-820-0386		Global-TAC-China@honeywell.com
Singapore	+65-6823-2215	+65-6445-3033	GTAC-SEA@honeywell.com
Japan		+81-3-6730-7228	Global-TAC-JapanJA25@honeywell.com

World Wide Web

Honeywell Process Solutions support website:

http://www.honeywellprocess.com/support

Elsewhere

Contact your nearest Honeywell office.

8.4 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.

Index