Honeywell

Experion

# System Management Configuration

## Guide

EP-DSX204
EX08
R300
09/05

# Notices and Trademarks

**Copyright 2005 by Honeywell International Inc.**
**Release R300 September, 2005**

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customers.

In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell, PlantScape, Experion, and **TotalPlant** are registered trademarks of Honeywell International Inc.

Other brand or product names are trademarks of their respective owners.

Honeywell International

Process Solutions

2500 West Union Hills Drive

Phoenix, AZ 85027

**1-800 343-0228**

# About This Document

This document describes

- The installation of system management tools
- The installation of TPS domains
- Configuration of a system management display
- Configuration of the event filter
- Configuration of HCI/OPC components
- System Event and Performance Servers

## Release Information

| Document Name | Document ID | Release Number | Publication Date |
|---|---|---|---|
| System Management Configuration Guide - EX08 | EP-DSX204 | 300 | 09/05 |

## References

The following list identifies all documents that may be sources of reference for material discussed in this publication.

| Document Title | Doc ID |
|---|---|
| TPN Server User's Guide | TP11W |
| System Management Operations Guide | EX07 |
| TPS System Administration Guide | TP06W |
| System Configuration Utility User's Guide | TP20W |
| Fault Tolerant Ethernet Planning, Installation and Service Guide | FE05 |
| Fault Tolerant Ethernet Status Server and Auxiliary Display User's Guide | EX22 |
| Redirection Manager User's Guide | EX20 |

| | |
|---|---|
| LCN-connected Server, Station, and ACE Implementation Guide | EX23 |
| OPC Specification Reference Manual | TP41 |
| Experion Server and Client Configuration Guide | |
| Experion Operators Guide | |
| HCI/OPC Data Access User's Guide | GU2B320A |

# Contacts

### World Wide Web

The following Honeywell web sites may be of interest to Process Solution customers.

| Honeywell Organization | WWW Address (URL) |
|---|---|
| Corporate | *http://www.honeywell.com* |
| Honeywell Process Solutions | *http://hpsweb.honeywell.com* |

### Telephone

Contact us by telephone at the numbers listed below.

| Location | Organization | Phone |
|---|---|---|
| United States and Canada | Honeywell IAC Solution Support Center | 1-800-822-7673 |
| Europe | Honeywell TAC-EMEA | +32-2-728-2704 |
| Pacific | Honeywell Global TAC - Pacific | 1300-300-4822<br>(toll free within Australia)<br>+61-8-9362-9559<br>(outside Australia) |
| India | Honeywell Global TAC - India | +91-20-2682-2458 / 1600-44-5152 |
| Korea | Honeywell Global TAC - Korea | +82-2-799-6317 |
| People's Republic of China | Honeywell Global TAC - China | +86-10-8458-3280 ext. 361 |
| Singapore | Honeywell Global TAC - South East Asia | +65-6580-3500 |
| Taiwan | Honeywell Global TAC - Taiwan | +886-7-323-5900 |
| Japan | Honeywell Global TAC - Japan | +81-3-5440-1303 |
| Elsewhere | Call your nearest Honeywell office. | |

## Symbol Definitions

The following table lists those symbols used in this document to denote certain conditions.

| Symbol | Definition |
|---|---|
| | **ATTENTION:** Identifies information that requires special consideration. |
| **CAUTION** | Indicates a situation which, if not avoided, may result in equipment or work (data) on the system being damaged or lost, or may result in the inability to properly operate the process. |

# Contents


**1. INTRODUCTION .....15**

**1.1 System Management Overview .....15**
Background .....15
About the Microsoft Management Console .....15
How Honeywell System Management software works .....15
Terms and Definitions used in this guide .....16
The role of Honeywell System Management software .....16
What System Management provides .....17
Focus of this document .....21
System configuration tasks .....22
System Management communication methods .....24

**2. GETTING STARTED WITH SYSTEM MANAGEMENT .....27**

**2.1 Pre-installation Preparation .....27**
Who should install System Management tools .....27
Basic assumptions .....27
System Management implications for a network .....27
System requirements .....28
Considerations for Experion users .....28
System management configuration flow chart .....28

**3. INSTALLING SYSTEM MANAGEMENT TOOLS .....31**

**3.1 What's Available for Installation .....31**
System Management Tools .....31
When to use System Management tools .....33
Installation requirements - TPS .....35
Re-installation requirements .....35
Installing System Management requires starting services .....36

**3.2 Installation – DC in TPS or pre-R300 Experion System .....37**
Procedure for installing the TPS Domain/Console Configuration tool .....37

**3.3 System Management Installation – DC in Experion R300 System .....38**
Procedure for installing the System Management Runtime .....38
Procedure for installing the TPS Domain Configuration tool .....38
Procedure for installing the TPS Domain Migration tool .....39

**3.4 System Management Installation – Workstation in TPS or pre-R300 Experion .....40**

Procedure for installing System Management ..... 40

**3.5 System Management Installation – Workstation in R300 Experion system 41**

Procedure for installing System Management ..... 41

**4. CREATING A TPS DOMAIN OR CONSOLE ..... 43**

**4.1 TPS Domain or Console Introduction ..... 43**

TPS Domains and Consoles as OUs ..... 43

TPS Domain OU or Console containment rules ..... 44

**4.2 Creating a TPS Domain OU ..... 45**

Procedure to create a TPS Domain OU ..... 45

Creating a Console ..... 55

**4.3 Removing a TPS Domain OU or Console ..... 56**

Procedure to remove a TPS Domain OU or console ..... 56

**5. CONFIGURING A SYSTEM MANAGEMENT DISPLAY ..... 57**

**5.1 System Management Display Node Environment ..... 57**

Environments allowed ..... 57

Limitation ..... 57

**5.2 Adding the Node Administration Snap-In to the MMC ..... 57**

About the Node Administration Snap-In ..... 57

Procedure to add the Node Administration Snap-In ..... 58

**5.3 Node Administration Properties ..... 65**

Startup Behaviors Property Page ..... 65

**5.4 Startup Behavior Configuration ..... 67**

Startup Behaviors defaults ..... 67

Automatically add the TPS Domain behavior ..... 67

Prompt for Alternate Credentials behavior ..... 67

Use Multicast Synchronized Repositories ..... 67

Use Synchronized Repositories on Remote Host ..... 68

Display Multicast/synchronization pages ..... 68

**5.5 Adding the Monitored Domains Tab ..... 69**

Domain display name properties ..... 69

Alternate user ID ..... 70

**5.6 Removing the Monitored Domains Tab ..... 70**

Example display ..... 70

**5.7 Multicast Communications Purpose ..... 71**

Providers use multicast ..... 71

Overview example 1 ..... 72

Overview example 2....73
Overview example 3....74

**5.8 Multicast Heartbeat Settings....75**
Multicast/Heartbeat Settings Property Page....75
Heartbeat settings description....76
Using the Multicast/Heartbeat Settings property page for multiple computers....77
Selecting a Source of Settings to be Viewed/Modified....77

**5.9 Determining the Synchronized Repository Scope....79**
Synchronized Repository Settings Property Page....79
Synchronized Repository Settings example....79
Type of settings....80
Common Synchronized Repository Settings information....80
Synchronized Repository Configurations information....80
Selecting a Source of Settings to be Viewed / Modified....81
Selecting a Repository to Configure....82
Reserved Scope Values....83
System Management Provider Default Scope Values....84

**5.10 Synchronization Scope Scenarios....85**
Scope values set the provider view....85
TPS Domain Computers View only Events for their TPS Domain....86
Multiple TPS Domains and their associated events must be viewable....86
Procedure to modify current scope configuration for setting multiple scope values....86
Restricting users from using the System Management Display....87
Applying Synchronized Repository Settings to multiple computers....88
Procedure for applying changes to settings....88

**5.11 Managing Organizational Units and Computers....89**
About Managed Organizational Units and Computers....89
Procedure for adding a Managed OU to a Monitored Domain....90
Procedure for adding a Computer as Managed item....95

**5.12 Managing Components....101**
About managed components....101
Additional references for managing a component....101

**5.13 Using Monitored Components....102**
About monitored components....102
About Redirection Manager....102
How Redirection Manager uses monitored components....102

**5.14 Invoking from Experion System Status....102**
System Management Display link....102

**6. CONFIGURING HCI/OPC COMPONENTS....105**

**6.1 Using the HCI Component Configuration Page....105**
Overview....105

Key Concepts ..... 105
Procedure for configuring an HCI component ..... 106
Reconfiguring an HCI component ..... 111
Removing an HCI component ..... 112
Using the General Component Configuration Page ..... 112
Configuring a new HCI Server ..... 112
New configuration vs. re-configuration ..... 113
Data Access Options ..... 119
Secured Methods ..... 120
Defining Capabilities ..... 121
Procedure to create and modify a capability for an HCI Component ..... 122
Procedure for disabling shutdown of a component ..... 130
Procedure for configuring a device-specific server ..... 131
Procedure for applying a configuration ..... 131
Procedure for removing a component's configuration ..... 132

**6.2 Configuring HCI/OPC Component Security ..... 133**
About this section ..... 133
Changing Server Identity ..... 133
Procedure for assigning a user id and password ..... 134
Launch, Access and Configuration permissions ..... 136
Procedure for setting permissions ..... 136

## 7. SUPPORTING SYSTEM EVENT SERVER ..... 137

**7.1 Role of the System Event Server ..... 137**
About System Performance Server ..... 137
System Performance Server architecture ..... 137

**7.2 Getting Started with System Event Server ..... 140**
Installation guidelines ..... 140

**7.3 Installing and Configuring System Event Server ..... 141**
Procedure for installing SES in a pre-R300 Experion system ..... 141
Procedure for installing System Event Server in R300 Experion system ..... 142
Procedure for configuring System Event Server ..... 142

**7.4 Verifying SES is Operational ..... 145**
Procedure for verifying SES is Operational ..... 145

**7.5 Troubleshooting SES Configuration ..... 146**

## 8. CONFIGURING EVENT FILTERING ..... 147

**8.1 Role of Event Filtering ..... 147**
About Event Filtering ..... 147
Example of Event Filtering Table ..... 147
How Event Filtering works ..... 148

**8.2 Event Filtering Configuration Procedures ..... 149**
Configuration concepts ..... 149
Event filtering configuration prerequisites ..... 149
Procedure for creating a Filter Table ..... 150
Configuring an Event ..... 153
Analyzing Event Characteristics ..... 156
Procedure for sharing a Filter Table ..... 163

**9. SUPPORTING SYSTEM PERFORMANCE SERVER ..... 165**

**9.1 Role of the System Performance Server ..... 165**
About the System Performance Server ..... 165
System Performance Server architecture ..... 166
SPS data naming ..... 166
What is an SPS Alias ..... 168

**9.2 Installing System Performance Server ..... 169**
Installation guidelines ..... 169
Procedure for installing SPS in TPS or pre-R300 Experion system ..... 169
Procedure for installing System Performance Server in R300 Experion system ..... 170

**9.3 Configuring SPS on Experion Server ..... 171**
Procedure for configuring System Performance Server ..... 171
Configuring the SPS Scope ..... 175
Adding new Aliases ..... 177
Deleting an alias ..... 179
Editing an alias ..... 179

**9.4 Configuring SPS on APP Node ..... 180**

**9.5 Verifying SPS is Operational on Experion Server ..... 181**
Procedure for verifying SPS is Operational ..... 181

**9.6 Verifying SPS is Operational on APP Node ..... 182**

**9.7 Troubleshooting SPS Configuration ..... 182**

**10. SUPPORTING SNMP MONITOR ..... 183**

**10.1 Role of the SNMP Monitor ..... 183**
About SNMP ..... 183
Purpose of the SNMP Monitor ..... 183

**10.2 Installing the SNMP Monitor ..... 183**
Procedure for installing SNMP Monitor in TPS or pre-R300 Experion systems ..... 183
Procedure for installing SNMP Monitor in R300 Experion system ..... 185

**10.3 Configuring the SNMP Monitor ..... 186**

## 11. ADMINISTERING HCI NAME SERVICE ..... 187

**11.1 Role of HCI Name Service .....187**
What the name service provides ..... 187
Example HCI Name Service display..... 188
Description of HCI Components..... 189
Uniqueness of alias names ..... 190

**11.2 Viewing and Setting Scope of HCI Name Service.....191**
About the HCI Name Service tool..... 191
Viewing the name service repository..... 192
Deleting a local component ..... 194
Summary of HCI component deletion..... 195
Procedure for deleting an HCI component ..... 195
Scope of name service provider..... 197
Procedure for setting the scope of name service repository..... 198

## 12. GENERATING A FILE USING ALIAS GENERATOR ..... 199

**12.1 Purpose of Alias File.....199**
How the Alias Generator tool works ..... 199
Scenarios that require an Alias File..... 199
ComponentAlias.XML file is required ..... 200
Adding components to a Component Alias file..... 200
Deleting a Component from an Alias File ..... 206

## 13. TROUBLESHOOTING SYSTEM MANAGEMENT ..... 207

**13.1 How to use this section.....207**
Introduction ..... 207

## Tables

Table 1 Software for System Management Tasks ..... 18
Table 2 System Configuration Tasks ..... 22
Table 3 Description of System Management Tools ..... 31
Table 4 Guidelines for using System Management tools ..... 33
Table 5 Node Administration Properties ..... 66
Table 6 Description of Multicast/Heartbeat Settings ..... 78
Table 7 Values for Common Synchronized Repository Settings ..... 80
Table 8 Synchronized Repository Configurations Description ..... 81
Table 9 Reserved Synchronization Scope Values ..... 83
Table 10 System Management Provider Default Scope Values ..... 84
Table 11 Descriptions of Fields/Buttons of the HCI Component Page ..... 113
Table 12 Descriptions of HCI Components ..... 189
Table 13 Issues That May Occur When Deleting Local Components ..... 194

## Figures

Figure 1 Role of System Management ..... 17
Figure 2 System Management Communications Architecture ..... 25
Figure 3 System Management Communications Flow Chart ..... 29
Figure 4 TPS Domains in a Windows Domain ..... 43
Figure 5 Example Node Administration Properties Page ..... 65
Figure 6 Common Page Properties ..... 68
Figure 7 Domain Display Name Properties ..... 69
Figure 8 Editing the Display Name ..... 69
Figure 9 Removing Domains Display ..... 70
Figure 10 Nodes within the same Multicast scope ..... 72
Figure 11 Nodes outside of an IP Multicast Group ..... 73
Figure 12 Variation of nodes within the same IP Multicast Group ..... 74
Figure 13 Heartbeat Settings ..... 76
Figure 14 Synchronized Repository Settings Property Page ..... 79
Figure 15 Edit scope string dialog box ..... 85
Figure 16 Data Access Configuration Page ..... 119
Figure 17 Listing of Secured Methods and Capabilities ..... 120
Figure 18 Example Event Filtering Table ..... 147
Figure 19 Creating a filter table ..... 149
Figure 20 A Sample HCI Name Service Display ..... 188
Figure 21 Example Alias file ..... 199

# 1. Introduction

## 1.1 System Management Overview

### Background

Honeywell System Management is a software infrastructure that uses open technologies to integrate an individual node into a system of nodes. The Microsoft Management Console (MMC) environment exposes the tools necessary to configure and monitor a system of Experion and/or TPS nodes. Nodes that are integrated as such with System Management are referred to as managed nodes. System Management performs its tasks in either a Windows domain or a workgroup.

### About the Microsoft Management Console

Microsoft Management Console (MMC) is an extensible common presentation service for management applications. MMC provides a common host environment for Snap-ins, provided by Microsoft and Honeywell. Snap-ins provides the actual management behavior; MMC does not provide any management functionality. The MMC environment provides for seamless integration between Snap-ins.

### How Honeywell System Management software works

System Management consists of several installable packages. The System Management runtime package provides the base infrastructure of System Management. It is installed on every managed node.

The System Management display package is an MMC snap-in that can be installed on one or more nodes in the system. The System Management display interacts with the System Management runtime to determine the status of each managed node. For TPS customers, this display enables remote configuration of certain applications.

For a complete list of installable packages within System Management, see section 3.1.

System management utilizes Microsoft's Organizational Units (OUs) as a means of organizing nodes into operational units. We uniquely identify these OUs as TPS domains. System Management treats nodes in a Workgroup as a single operational unit of nodes.

### Terms and Definitions used in this guide

The following terms have specific definitions when used in the TPS system management environment.

| Term | Definition |
|---|---|
| Managed OU | An Organizational Unit is a Microsoft term for a container in the Windows Active Directory that stores users, computers, and other account objects. A TPS Domain or Console is derived from an OU. A Managed OU is a TPS Domain or Console that can be managed using the MMC Node Administration Snap-in. |
| Monitored Domain | Monitored Domains automatically appear in the System Management Display. Monitored Domains may include a TPS Domain or Console, and non-TPS Domains. |
| Managed Components | Managed components automatically appear on the System Management Display. Managed components include TPN Server, Fault Tolerant Ethernet (FTE), CL Server, NWDDB Server, System Event Server (SES) and System Performance Server (SPS). |
| Monitored Components | Monitored components are HCI or generic OPC servers, which are configured to be managed by the Redirection Manager (RDM). |
| CAS | Component Administration Service. |
| WMI | Windows Management Instrumentation. |

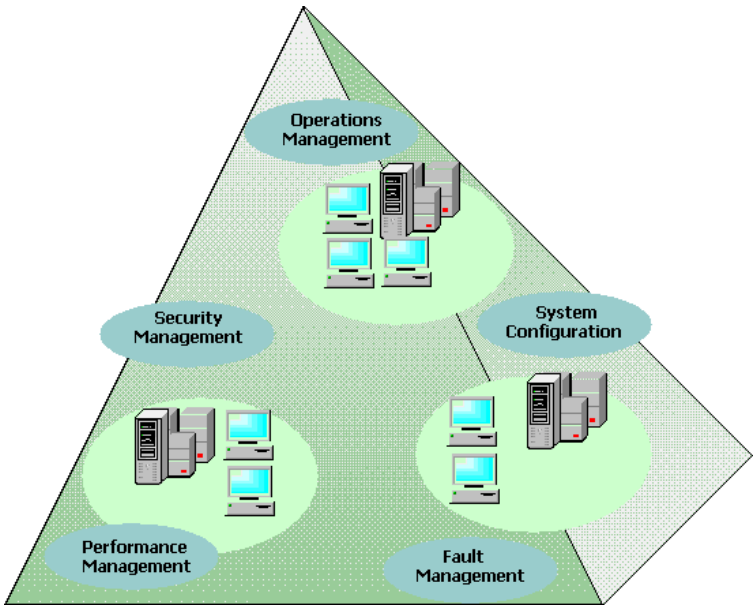
### The role of Honeywell System Management software

Honeywell System Management software helps you perform the following functions:

- Configure, operate and manage the performance of your Honeywell system and processes.
- Communicate with other networks in your enterprise.
- Manage alarms, faults, and security in your Honeywell system.

Figure 1 shows the various functions of Honeywell System Management software. Table 1 describes each of these functions.

**Figure 1 Role of System Management**




### What System Management provides

Honeywell System Management software provides the following:

- Windows MMC-based System Management Display
- Integration of node level Windows events into a system level of Windows events. The system level of Windows events can be separated into operational areas if implemented in a Windows domain by using TPS Domains.
- Visibility of system level of events through the System Management Display or from the Experion System Alarm or Event Summary Display.
- Integration of a node's performance data with Experion or TPS displays
- HCI Name Service
- Remote HCI Component Configuration
- Remote TPS Standard Node Configuration
- Management of local and domain HCI Components
- Monitoring of local HCI components
- Monitoring of local Redirection Managers
- Managed Node status

**Table 1 Software for System Management Tasks**

| To Perform this Task… | Use these Honeywell and Microsoft System Management Components | Refer to this Document |
|---|---|---|
| **System Configuration** | *The Microsoft Management Console* (MMC) is the framework for system configuration, with Honeywell configuration facilities implemented as MMC Snap-ins.<br><br>Use standard Windows facilities running under MMC to perform system and domain configuration, user account administration, and security administration.<br><br>*The Honeywell System Management Display* allows you to configure and monitor managed nodes and their HCI managed components. It helps you perform remote TPS Node and HCI component configuration.<br><br>*The Honeywell HCI Name Service* is used by HCI client applications to resolve an alias name to a server's CLSID and computer name.<br><br>*The Honeywell System Event Provider* publishes local events as system events and maintains a synchronized local copy of system events within a predefined scope.<br><br>*The Honeywell System Event Server* publishes system events as OPC events. This enables integration within the Experion Alarm and Event Subsystem, thereby allowing system events to appear on alarm and message displays and to be journaled in the Experion Event Journal.<br><br>*The Honeywell System Event Provider* and *HCI Name Service Provider* maintain a synchronized database of System events and HCI alias names.<br><br>*The Honeywell Component Admin Service* monitors and manages HCI managed components. Provides on-demand monitoring of non-managed HCI/OPC servers.<br><br>*The Honeywell Heart Beat Provider* (also known as the FTE Provider) supplies connected clients with a list of all nodes currently reporting a heartbeat, and event notification of the addition or removal of a node within its multicast scope.<br><br>*The Honeywell System Performance Server provides* performance and configuration information that is internally maintained on a per-node basis using Microsoft's WMI (Windows Management Instrumentation). This data is accessible as OPC data thus allowing it to be easily integrated into operator displays and process applications in a manner consistent with process data access. | *System Management Configuration Guide* |

| To Perform this Task… | Use these Honeywell and Microsoft System Management Components | Refer to this Document |
|---|---|---|
| **Operations Management** | *The Honeywell Synchronized Repository Provider (SRP)* performs lower-level inter-node communications necessary to keep event and name server information synchronized.<br><br>*The Honeywell HCI managed components* display TPN process and system events on TPS client nodes.<br><br>*The Honeywell System Management Display* replaces the earlier TPS System Status Display, and integrates with the Microsoft Management Console (MMC). All TPS managed components can be individually started and shut down using the System Management Display<br><br>*Honeywell HCI Managed components* help you view Experion Server status displays. (See the Configuring HCI/OPC Component section of this document). | *System Management Configuration Guide*<br><br>*System Management Operations Guide* |
| **Performance Management** | *The Microsoft Performance Management (PerfMon) and third-party tools* monitor Windows system and network performance.<br><br>System Performance Server provides OPC Data Access to Windows performance data. SPS data can be accessed through GUS or Experion custom displays. It can also be access with some Experion Standard operating displays. | *Microsoft documentation,*<br><br>*System Management Configuration Guide, Server and Station Configuration Guide* (Experion), HCI/OPC Data Access User's Guide |
| **Fault Management** | *Windows Management Instrumentation (WMI) Providers* include Heartbeat, CAS and System Events. These Providers periodically query the status of each component on the node and report that status to the System Management Display, using WMI. | *System Management Configuration Guide* |
| **Security Management** | A default *Honeywell Security Policy* is provided, and security configuration is performed using standard Windows tools. | *TPS System Administration Guide, Experion Administration and Startup Guide* |
| **Event Filtering Configuration** | Event Filtering Snap-In. (See the Configuring Event Filtering section of this document). | *System Management Configuration Guide* |

| To Perform this Task… | Use these Honeywell and Microsoft System Management Components | Refer to this Document |
|---|---|---|
| **Alias File Generation** | Alias File Generation program. (See the Generating a File Using Alias Generator section of this document). | *System Management Configuration Guide* |

### Focus of this document

Refer to Table 2 to find documentation about all Honeywell system configuration and management tasks. This document focuses on the following system configuration tasks.

- Installing System Management Tools
- Creating a TPS Domain or Console
- Managing Organizational Units and Computers
- Configuring HCI/OPC Components
- Administering HCI Name Service
- Troubleshooting System Management

## System configuration tasks

Table 2 shows system management and configuration tasks, whether they are performed remotely or locally, and the documentation that contains details about implementing these tasks.

**Table 2 System Configuration Tasks**

| Task Performed | Perform Task Remotely Using Node Administration Snap-In | Perform Task Locally Using Node Administration Snap-In or Configuration Utility | Related Documentation |
|---|---|---|---|
| **HCI Component Configuration** | X | X | *System Management Configuration Guide* |
| **HCI Name Service Administration** | X | X | *System Management Configuration Guide* |
| **LCNP Board (Board 0) Configuration** | | X | *Configuration Utility User's Guide* |
| **Devices/Services Configuration** | X | X | *Configuration Utility User's Guide* |
| **File Transfer Configuration** | | X | *File Transfer Installation User's Guide* |
| **GUS Alarm/Message Group Displays Configuration** | | X | *Configuration Utility User's Guide* |
| **GUS Display Runtime Settings Configuration** | | X | *Configuration Utility User's Guide* |
| **GUS Display Runtime Timers Configuration** | | X | *Configuration Utility User's Guide* |
| **GUS HCI Client Configuration** | | X | *Configuration Utility User's Guide* |
| **GUS Remote Displays Client Configuration** | | X | *GUS Remote Displays User's Guide* |

| Task Performed | Perform Task Remotely Using Node Administration Snap-In | Perform Task Locally Using Node Administration Snap-In or Configuration Utility | Related Documentation |
|---|---|---|---|
| **GUS Remote Displays Server Configuration** | | X | *GUS Remote Displays User's Guide* |
| **LCNI18N (Internationalization) Configuration** | | X | *Configuration Utility User's Guide* |
| **Shutdown Wait Limit Configuration** | | X | *Configuration Utility User's Guide* |
| **System Event Server Usage and Setup** | X | X | *System Management Configuration Guide* |
| **System Performance Server Usage and Setup** | X | X | *System Management Configuration Guide* |

### System Management communication methods

Figure 2 shows communication methods used by system management runtime components.

*Synchronized Repository and Heart Beat providers* use multicast for inter-node communication.

*The System Management Display* uses the Windows Management Instrumentation to communicate with:

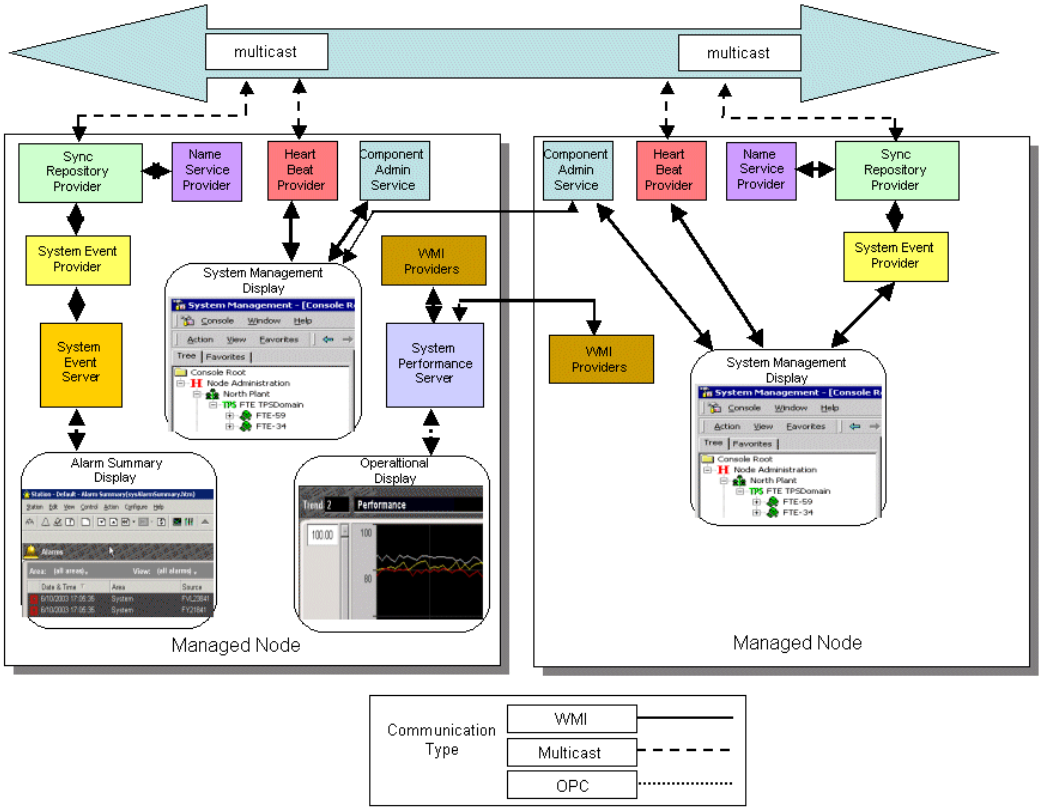
- Its local Heart Beat and System Event providers
- The Component Admin Service on the local and remote managed nodes

*The System Event Server* uses the Windows Management Instrumentation to communicate with the System Event Provider.

*The System Performance Server* uses the Windows Management Instrumentation to communicate with the Windows WMI Provider on each node where performance data has been requested.

*The System Event and System Performance Servers* use OPC to communicate with Experion standard and custom displays. The System Performance Server uses OPC to communicate with GUS custom displays.

**Figure 2 System Management Communications Architecture**



# 2. Getting Started with System Management

## 2.1 Pre-installation Preparation

### Who should install System Management tools

Personnel who implement nodes and client applications in Experion and TPS systems should be the users responsible for installing System Management tools. Those users will require administrator access when performing configuration tasks associated with System Management, such as installing the Snap-in extension of the Domain Controller and configuring HCI/OPC components.

### Basic assumptions

Several assumptions include the following:

- Installation and upgrades will be performed by a System Administrator
- The Administrator is familiar with administering Windows systems.
- System Management runtime can only be installed on a node running Windows 2000 or XP.
- If using a Windows NT4 platform, you must have already performed your upgrade to Windows 2000 or XP prior to installing System Management from the Common Components CD.

### System Management implications for a network

The System Management infrastructure makes substantial use of

- multicast communications,
- Active Directory and Dynamic DNS if installed in a Windows domain, or
- Host files and NetBios if installed in a workgroup.

If you are installing System Management in a Domain make sure you have a functional Active Directory and Dynamic DNS. If you are installing System Management in a Workgroup make sure you have properly configured host files. In both cases if you have nodes connected through routers or switches make sure multicast is enabled.

### System requirements

You must have the following installed on your PC in order to install Honeywell System Management software:

- Windows operating system supported for your release.
- Windows Service Pack and hot fixes that Honeywell has identified as needed for your release.

### Considerations for Experion users

Users with Experion systems operating in a domain security model may consider placing their nodes into Organizational Units (OUs) called TPS Domains. These OUs will then support:

- Definition of a System Event scope for the Experion nodes.
- Automatic enumeration of Experion nodes in the System Management Display.

Users with Experion systems operating in a workgroup security model can also make use of the System Management Display to enumerate the Experion nodes.

**ATTENTION**

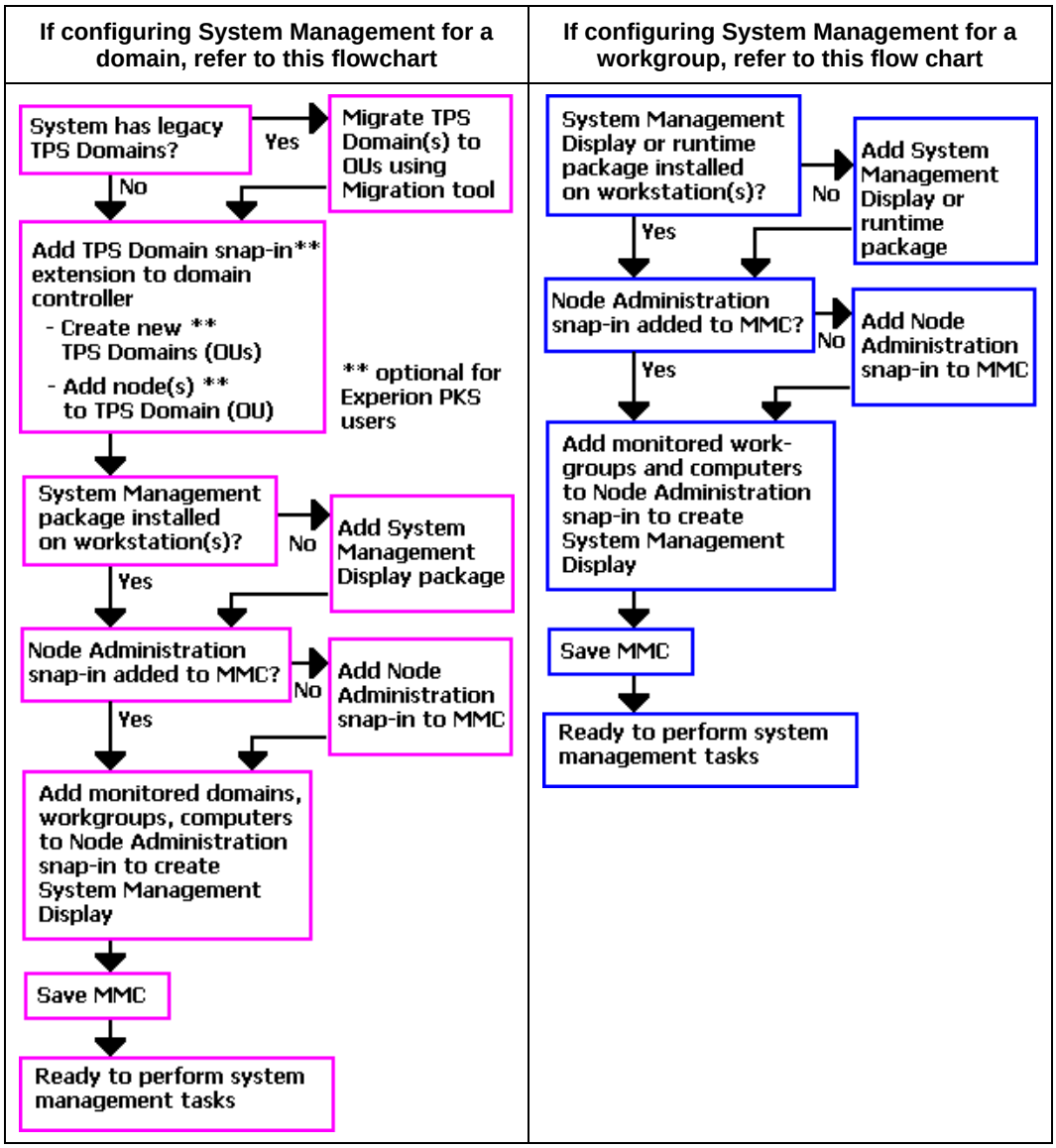
If you are an Experion user with an R300 system, your system management components are installed during Experion installation from the Application DVD. You do not need to install system management from the Common Component media. If you need to perform post or re-installation tasks, use the Application DVD.

### System management configuration flow chart

If configuration is required in a domain or workgroup, refer to the flow chart that is the most representative for your system.

- If nodes are in a domain environment, note that you can optionally add your nodes to a TPS Domain. Refer to the flowchart for configuring System Management in a domain.
- If in a workgroup environment, refer to the workgroup flowchart.

**Figure 3 System Management Communications Flow Chart**



You may be required to make modifications to your Active Directory and networking infrastructure in order to utilize System Management. The following table provides some basic guidelines.

| Security Environment | Technology Used | Considerations / Actions |
|---|---|---|
| Windows Domain | Windows Active Directory | Windows Active Directory is required to support TPS nodes in this release. Since TPS Domains are modeled as Windows Organizational Units (OU's), NT4 era TPS Domains are not supported. |
| Windows Domain | Dynamic DNS (DDNS) | Windows requires implementation of a Dynamic DNS server. DDNS must run on a Windows server machine |
| Windows Workgroup | Hosts files, Netbios | Hosts file must be maintained and consistent on all nodes |
| Windows Domain or Windows Workgroup | Multicast Communications | Ensure all ports connected to the managed nodes on network switches are enabled to support multicast communications. See switch vendor documentation for further details.<br><br>If nodes are connected through routers make sure multicast in enabled to pass through the router. |

**REFERENCE - INTERNAL**

Refer to the *System Management Operations Guide* for procedures on how to monitor the status of nodes and components.

**REFERENCE - INTERNAL**

Refer to the *TPS System Implementation Guide* for procedures on how to migrate or install a Windows 2000 domain controller.

# 3. Installing System Management Tools

## 3.1 What's Available for Installation

**System Management Tools**

**Table 3 Description of System Management Tools**

| Tool | Description |
|---|---|
| System Management Display | Helps you configure and monitor managed nodes and their HCI managed components. |
| WMI Providers | Windows Management Instrumentation (WMI) Providers include: System Event Provider, Heart Beat Provider, Synchronized Repository Provider, Name Service Provider and Component Administration Service Provider. |
| System Event Filter | Each system event of interest is user-enabled in a Filter Table. Filter tables are created using the System Event Filter Configuration Tool, which is implemented as a Microsoft Management Console (MMC) snap-in. |
| System Event Server | OPC Alarm and Event server that publishes system events as reported from a defined set of nodes. The Experion Alarm Summary display is a subscribing client to the System Event Server. |
| System Performance Server | OPC Data Access server that provides access to performance data from a defined set of nodes. GUS custom displays have access to this server as well as Experion operational displays (custom and standard). |
| HCI Name Service Alias Generator | Creates a file of alias names, which is used by the name service provider on that node to publish the alias names of servers outside the Multicast Scope. |

| | |
|---|---|
| HCI Configuration | HCI Component Configuration helps you:<br>• Configure an HCI server from an installed base component, where a base component is identified from its ProgID.<br>• Re-configure an existing or previously configured HCI server<br>• Remove the configuration of an HCI server |
| TPS Domain/Console configuration | Performed using Active Directory Users and Computers MMC snap-in, in conjunction with TPS Domain/Console configuration extension snap-in. |
| High Security Policy Model | Provides a user environment for each of the operational user types such as Supervisors, Engineers, and Administrators. Each user type is granted the privileges and system access required to perform their required functions while at the same time protecting the system resources. This functionality is delivered as two separately installable packages: one for domain controllers and one for workstations. It includes Experion security templates, accounts, and groups. |
| SNMP Monitor | The SNMP Monitor converts SNMP notifications into Windows Events. |

### When to use System Management tools

Table 4 describes each of the System Management tools, the reason for using each tool, and the type of node on which each tool should be installed when you should use them.

**Table 4 Guidelines for using System Management tools**

| Tool | Reason for using | Install on a Domain Controller? | Install on a Workstation? |
|---|---|---|---|
| **Node Administration Snap-In** | Use the Node Administration snap-in common facility for Honeywell node and managed component administration and operations. | | X |
| **Event Filtering Snap-In** | Use the Event Filtering tool to receive notification when a system or process event occurs. If there is an event you are interested in viewing, you define it in a filter table using the Event Filtering Snap-in. | | X |
| **Alias Generator** | The Alias File Generator creates an alias file when you need to access the name service repository of a remote node that is not within the scope of the multicast group. If your monitored nodes are within the multicast group, you do not need to use this tool. | | X |

| Tool | Reason for using | Install on a Domain Controller? | Install on a Workstation? |
|---|---|---|---|
| **HCI Name Service display** | Access the HCI Name Service display when you need to examine a list of available published HCI/OPC alias names, or remove alias names from a computer that is no longer available. | | X |
| **TPS Domain/Console Configuration Tool** | A tool that let's you configure Organizational Units (OUs) as TPS Domains or Consoles. | X | |
| **Configuration Utility** | A tool that allows you to configure your local nodes when the System Management Display is not available for Experion and TPS systems. | | X |
| **Migrate Your TPS Domain** | Migrate legacy TPS domains to OUs. | X | |

### Installation requirements - TPS

**ATTENTION**

The APP is not supported on the Domain Controller.
DO NOT put a Domain Controller inside a TPS Domain OU.

- You must install the following prior to installing System Management Runtime:
  - The Service Pack and hot fixes (for TPS, these are provided on the Common Components CD)
  - Honeywell Repackaged a Redistributable Files package (provided on the Common Components CD)

**ATTENTION**

To identify the latest Microsoft hot fixes and updates that you should have installed on your TPS or Experion system, go to

http://hpsweb.honeywell.com/Cultures/en-US/ContactsSupport/Support/MicrosoftSecurityHotfixInformation/Default.htm.

- To use System Management facilities, your nodes of interest must operate on Windows.
- The following items are required for using Snap-In extensions:
  a) Domain controller using Windows Server and Active Directory
  b) Workstations using a Windows Professional operating system.
- HCI Components, such as TPN Server, may have additional requirements and are documented in their respective manuals.

### Re-installation requirements

You must remove the following prior to re-installing System Management software:

#### *Domain Controller*

- Domain/Console Configuration tool

#### *Work Station*

- Honeywell System Management Runtime

- Honeywell System Management Status Display
- Honeywell TPS Admin Support Files
- Honeywell FTE Status (if installed)

### Installing System Management requires starting services

An installation of System Management will require a reboot of your PC.

## 3.2 Installation – DC in TPS or pre-R300 Experion System

**Procedure for installing the TPS Domain/Console Configuration tool**

**ATTENTION :** This procedure is performed on the Domain Controller only. The Domain Controller is in a TPS only system or pre-R300 Experion system.

| Step | Action |
|---|---|
| 1 | Install the Microsoft Windows Service Pack and Microsoft hot fixes, available on the Honeywell Common Components CD. Then reboot the node. |
| 2 | Install the Honeywell Repackaged Redistributable Files from the Honeywell Common Components CD. Then reboot your system. |
| 3 | From the Common Components CD, select the **TPS Domain/Console Configuration Tool**. |
| 4 | From the TPS Domain/Console Configuration Tool, select **Licensed Package Installer**. |
| 5 | If your TPS system currently has a legacy TPS Domain configured, select the **Migrate TPS Domain Structures to OUs** tool. Follow the instructions for using this tool to complete your migration. Refer to the *TPS System Implementation Guide* for more information on how to use the **Migrate TPS Domain Structures to OUs** tool.<br><br>If your migration is successful, click OK on the message box that appears.<br><br>If your migration was unsuccessful, a message appears that the Domain Controller migration failed. |
| 6 | If errors occur, navigate to the file shown on the pop-up screen file to view a list of errors:<br>C:\Program Files\Honeywell\SystemManagement\migrationlog.txt. |
| 7 | Click **Exit** to remove the **Honeywell Common Components** screen. |

# 3.3 System Management Installation – DC in Experion R300 System

### Procedure for installing the System Management Runtime

**ATTENTION :** This procedure is optionally performed on the Domain Controller only. The Domain Controller is used in a R300 Experion system that consists of Experion and/or TPS nodes. Install system management on your DC if you want the DC to appear in the system management tree and related displays.

| Step | Action |
|---|---|
| 1 | Insert the Experion Application DVD, click “Browse DVD contents”, and launch the Honeywell software Installation application at <drive letter>:\Packages\Install.exe |
| 2 | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| 3 | Enter license and authorization numbers. Click Next to continue. |
| 4 | Click System Management Runtime. |
| 5 | Click **Install Package**. |
| 6 | Click **Exit** when done |

### Procedure for installing the TPS Domain Configuration tool

**ATTENTION :** This procedure is performed on the Domain Controller used in a R300 Experion system that consists of Experion and/or TPS nodes. The tool is loaded in order to support or continue usage of TPS Domains in an Experion system.

| Step | Action |
|---|---|
| 1 | Insert the Experion Application DVD, click “Browse DVD contents”, and launch the Honeywell software Installation application at <drive letter>:\Packages\Install.exe |

| Step | Action |
|---|---|
| 2 | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| 3 | Enter license and authorization numbers. Click **Next** to continue. |
| 4 | Click TPS Domain Configuration Tool. |
| 5 | Click **Install Package**. |
| 6 | Click **Exit** when done |

### Procedure for installing the TPS Domain Migration tool

#### *About TPS Domain Migration*

The TPS Domain Migration tool only needs to be run on a Windows Domain Controller that supports earlier legacy TPS Domains that were not built as Organizational Units. Most users should not have to use this tool. TPS users migrating or integrating an Experion System who have not already migrated their TPS Domains to OUs would use this tool. The migration tool reads the registry on the Domain Controller and creates Organizational Units that represent the TPS Domains of an earlier TPS release. It populates created OU's with the computer names assigned to the original TPS Domain(s).

**ATTENTION :** This procedure is performed only once the Domain Controller.

| Step | Action |
|---|---|
| 1 | Insert the Experion Application DVD, click “Browse DVD contents”, and launch the migration application at <drive letter>:Packages\TPSDomainMigration\migration.exe |
| 2 | At the Command Prompt, enter **Y** to continue.<br>RESULT: TPS Domain OU's are created in Active Directory Users and Computers. |

| Step | Action |
|---|---|
| **3** | Review the results.<br>• If your migration is successful, a message appears that Domain Controller migration succeeded.<br>• If your migration is unsuccessful, navigate to C:\Program Files\Honeywell\SystemManagement\migrationlog.txt to interpret an error listing for corrective action. |

## 3.4 System Management Installation – Workstation in TPS or pre-R300 Experion

### Procedure for installing System Management

**ATTENTION**

R300 Experion users do not need to perform these steps, as system management is installed during Experion node installation.

Follow these steps to install System Management software.

| Step | Action |
|---|---|
| **1** | Install the Microsoft Service Pack and Microsoft hot fixes, available on the Honeywell Common Components CD. Then, reboot the node. |
| **2** | Install the Honeywell Repackaged Redistributable Files by selecting Main>Honeywell Repackaged Redistributable Files. Then reboot. |
| **3** | If you did not purchase a licensed package, (such as FTE, Redirection Manager or System Management Display) for this system, then install System Management Runtime by selecting it from the Common Components main menu. |
| **4** | If you purchased a licensed package, (such as FTE, Redirection Manager or System Management Display) for this system, then select Licensed Package Installer from the Common Components CD. |
| **5** | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| **6** | Enter license and authorization numbers. Click **Next** to continue. |

| | |
|---|---|
| **7** | Click **System Management Display**. (Note: If System Management Display does not appear in the list, verify that the licensing and authorization numbers are appropriate for this package). |
| **8** | Click Install Package. |
| **9** | Verify that these are the components you wish to install. Click **OK**.<br><br>**Result:** The installation process occurs, which usually takes a few minutes. |
| **10** | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |
| **11** | Reboot your workstation. |

## 3.5 System Management Installation – Workstation in R300 Experion system

### Procedure for installing System Management

**ATTENTION**

R300 Experion users do not need to perform these steps on Experion Stations, as system management is installed during R300 Experion node installation. R300 Experion users only need to perform this procedure on a non-Experion node communicating within an Experion system and there is a desire to add system functionality to that node.

Follow these steps to install System Management software on non-Experion nodes.

| Step | Action |
|---|---|
| **1** | Insert the Experion Application DVD, click “Browse DVD contents”, and launch the Honeywell software Installation application at <drive letter>:\Packages\Install.exe |
| **2** | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| **3** | Enter license and authorization numbers. Click **Next** to continue. |
| **4** | Click **System Management Runtime.** |
| **5** | Click Install Package. |
| **6** | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |

| | |
|---|---|
| **7** | Reboot your workstation. |

# 4. Creating a TPS Domain or Console

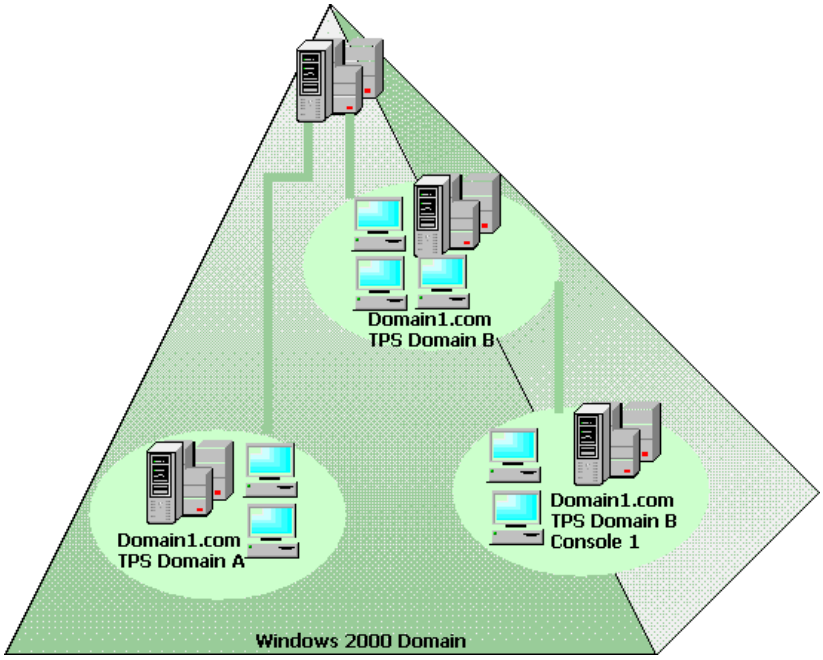
## 4.1 TPS Domain or Console Introduction

### TPS Domains and Consoles as OUs

A TPS Domain or Console is derived from an Organizational Unit (OU) in the Windows Active Directory. Creating a TPS Domain or Console allows you to organize and manage plant nodes of interest from a System Management Display. In this sense, Plant Control Network nodes can be organized along the lines of classic DCS systems into areas of interest or responsibility.

**Note:** If you are configuring nodes in a workgroup, skip this section and go to Section 5.

**Figure 4 TPS Domains in a Windows Domain**



### TPS Domain OU or Console containment rules

Both a TPS Domain OU and Console can contain computers and organizational units with the following rules:

- A TPS domain OU cannot be contained in another TPS Domain OU.
- A TPS Domain OU is contained within a Windows Domain.
- A console must be contained in a TPS Domain OU.

A console as presented in this description is an Organizational Unit within a TPS Domain.

**ATTENTION**

TPS Domain OU and Console configuration cannot be performed on workgroups.

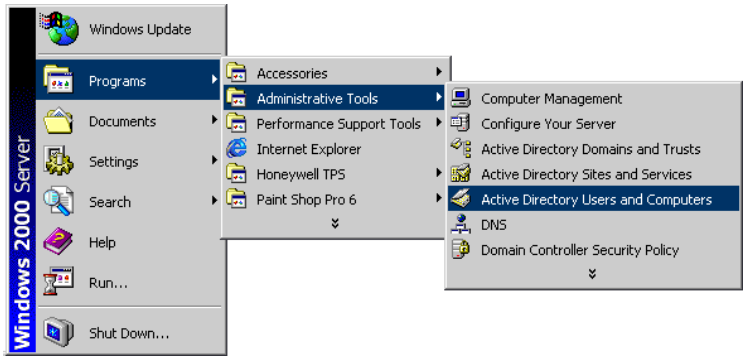
## 4.2 Creating a TPS Domain OU

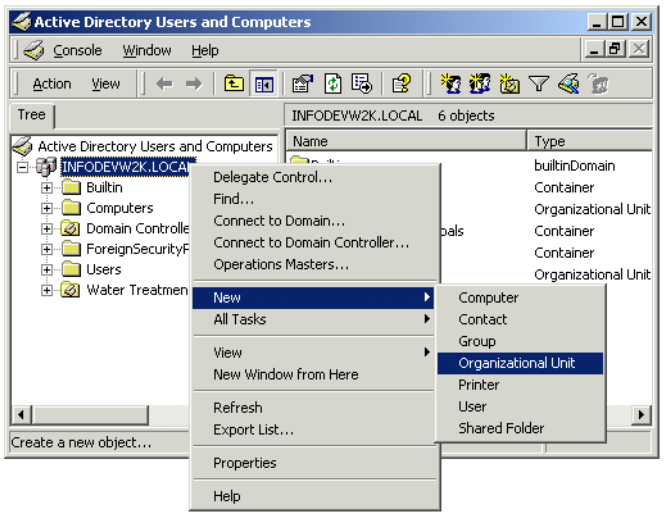
### Procedure to create a TPS Domain OU

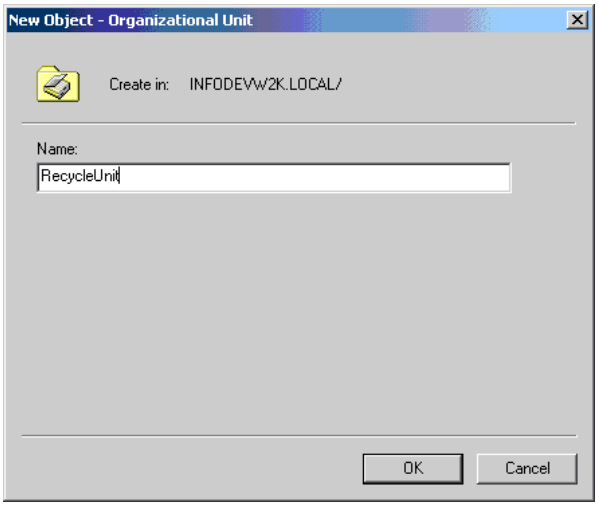
Follow these steps to create a TPS domain OU from a domain controller.

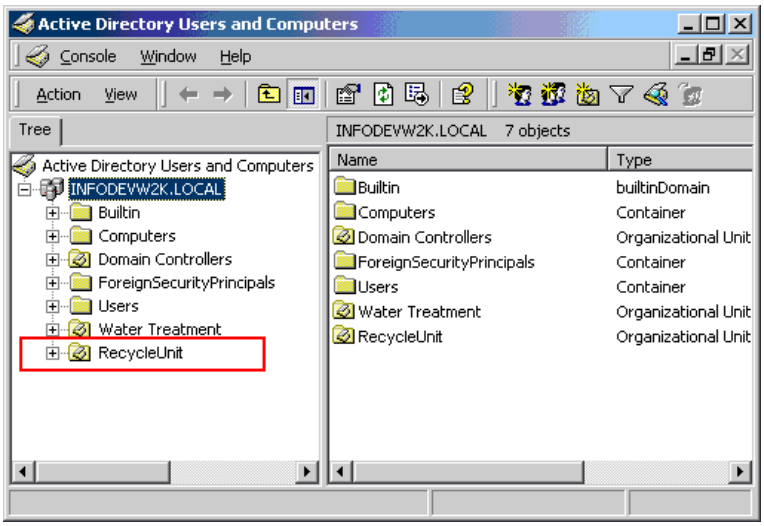
**ATTENTION**

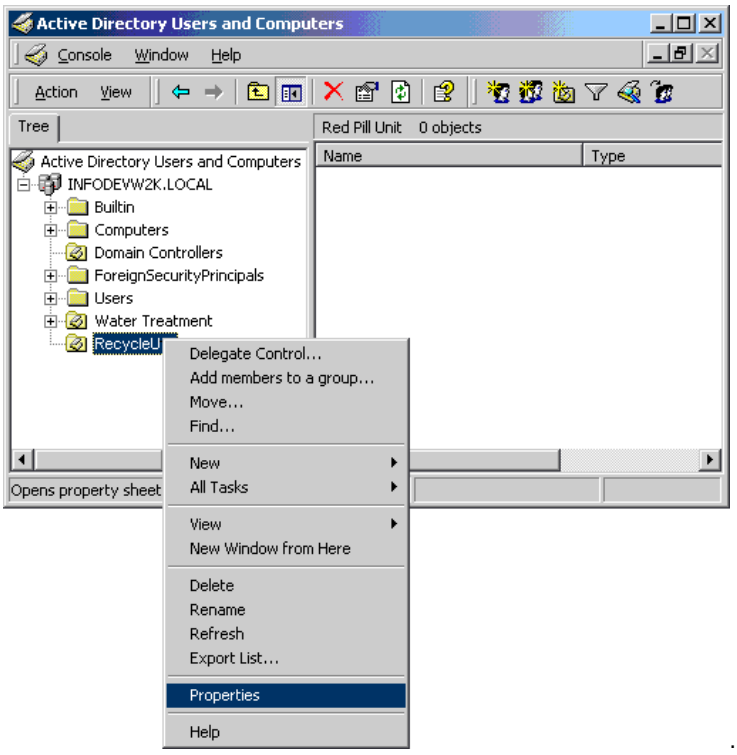
The following procedure is performed on domain controllers with domain administrator privileges.

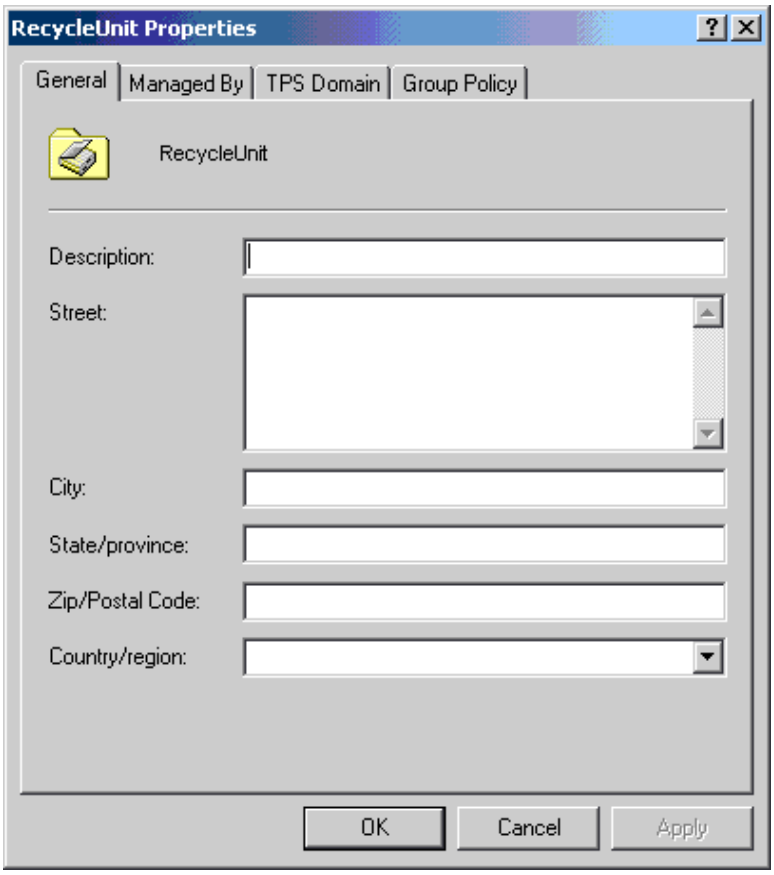
| Step | Action |
|---|---|
| 1 | To create a TPS Domain OU, start the Active Directory Users and Computers MMC Snap-In.   |

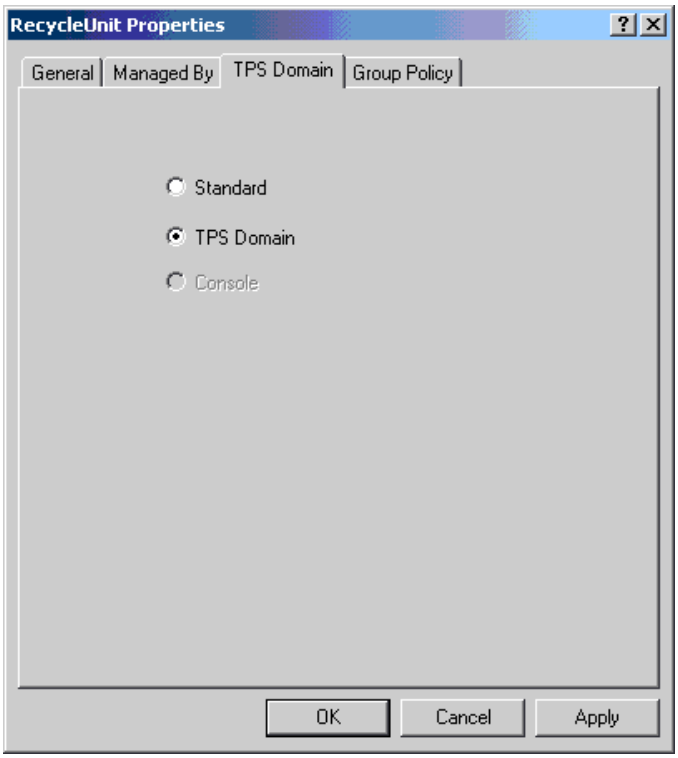
| Step | Action |
|---|---|
| **2** | Create a new organizational unit that will contain the TPS Domain in the directory tree for the domain of interest.<br>  <br><br>**Result:** A New Object for the organizational unit appears. |

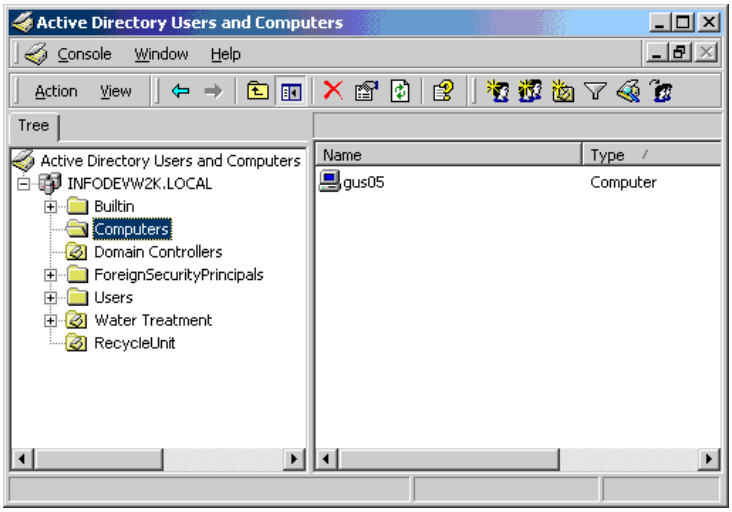
| Step | Action |
|---|---|
| **3** | In the dialog box for the organizational unit, enter a meaningful TPS Domain name. Click **OK**.<br>  |

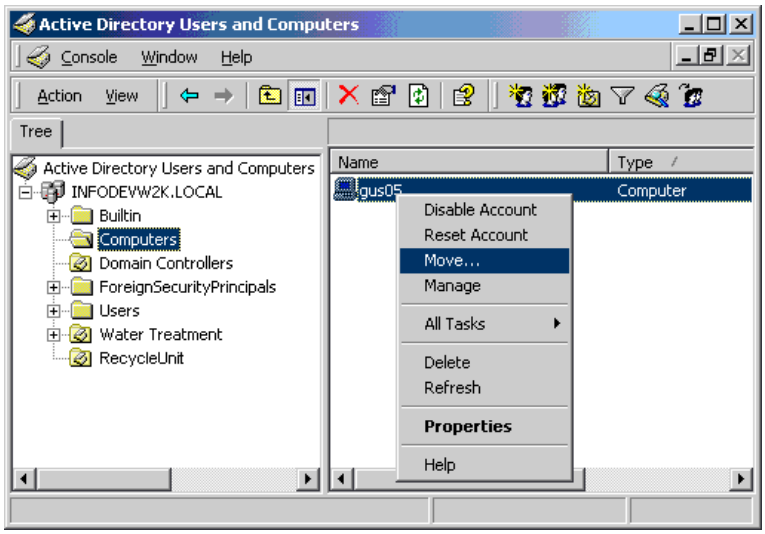
| Step | Action |
|---|---|
| **4** | The newly created OU appears in the directory tree. Select the newly created OU, then right-click the [organizational unit] to configure it as a TPS Domain.<br>  |

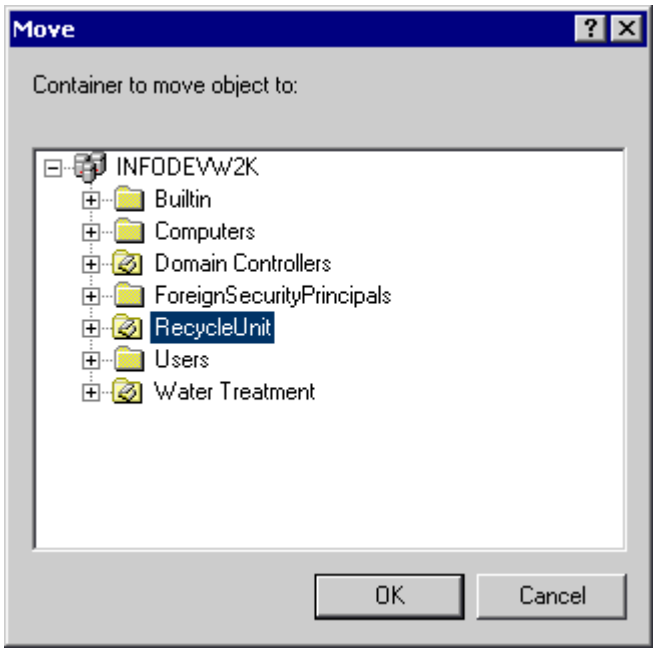
| Step | Action |
|---|---|
| **5** | Select **Properties** from the menu.<br>  |

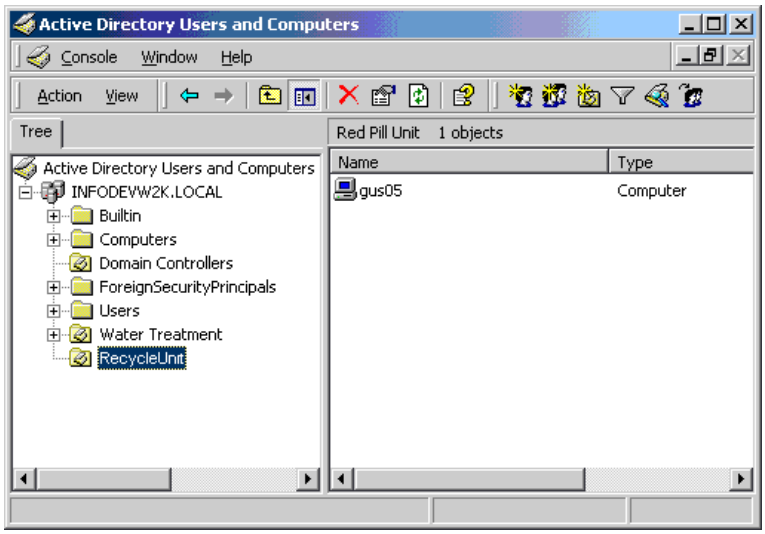
| Step | Action |
|---|---|
| **6** | Click the **TPS Domain** tab. (The TPS Domain tab appears on an OU's property sheet only if you installed the TPS Domain/Console Configuration tool on the domain controller).<br><br>**Result:** The TPS Domain Properties sheet appears.<br><br>  |

| Step | Action |
|---|---|
| 7 | Select **TPS Domain**. Then click **OK**.<br>**Note:** If a TPS Domain already exists, the TPS Domain radio button will be grayed out.<br><br>**Result:** The OU is configured with a TPS Domain attribute.<br><br>  <br><br><br>**ATTENTION**<br><br>Remember to use the following *TPS Domain OU or Console Containment Rules*, which allow both a TPS Domain OU and Console to contain computers and organizational units:<br><br>• A TPS domain OU cannot be contained in another TPS Domain OU.<br>• A TPS Domain OU is contained within a Windows Domain.<br>• A console must be contained in a TPS Domain OU. |

| Step | Action |
|---|---|
| **8** | Click the object that contains computers that you need to move to a TPS Domain OU. For example, click **Computers**.<br>  |

| Step | Action |
|---|---|
| **9** | Right-click the computer and select **Move**.<br>  <br><br>**CAUTION**<br>The following applies when moving managed nodes between TPS domain OUs. Moving a managed node in the Active Directory changes its identity. You must shutdown and re-start the node before it knows its new identity. Moving a node will affect its Name Service Identity and possibly its System Event Scope**.** |

| Step | Action |
|---|---|
| **10** | Click the TPS Domain OU of interest and then **OK**.<br>  |

| Step | Action |
|---|---|
| **11** | The computer appears as a node in the TPS Domain OU.<br>  <br><br>At this point, you can continue to add nodes and/or create additional TPS Domains repeating the previous steps. |

## Creating a Console

The steps to create a Console are similar to those for creating a TPS Domain OU, except that a Console is created as an OU within the TPS Domain OU. To create a console, simply select the Console radio button in the property sheet.

**ATTENTION**

A console must be contained in a TPS Domain OU. If there is no TPS Domain OU existing in the network tree structure, the Console radio button will be grayed out.

## 4.3 Removing a TPS Domain OU or Console

### Procedure to remove a TPS Domain OU or console

To remove the TPS Domain OU/Console attribute of an organizational unit, select the Standard radio button of its property sheet.

**ATTENTION**

Any time you remove a TPS Domain OU or Console, make sure you follow these steps.

| Step | Action |
|---|---|
| 1 | Select the **TPS Domain OU**. |
| 2 | Select the **Properties** tab for the TPS Domain you just created**.** |
| 3 | Select the **TPS Domain** tab. |
| 4 | Select the radio button for Standard. |
| 5 | Click **OK.** |
| 6 | Right-click the TPS Domain in the Active Directory and select **Delete**. |

# 5. Configuring a System Management Display

## 5.1 System Management Display Node Environment

### Environments allowed

The System Management Display can be configured to function in the following environments:

- On a node not connected to the network (Standalone Node)
- A node in a workgroup
- A node in a Windows domain

The display can be operated, created, and saved in each of these three environments.

### Limitation

**ATTENTION**

A console configured and saved in one of the three environments listed above is not expected to function properly in either of the other environments.

## 5.2 Adding the Node Administration Snap-In to the MMC

### About the Node Administration Snap-In

The Node Administration snap-in is a common facility used for Honeywell node and managed component administration and operations.

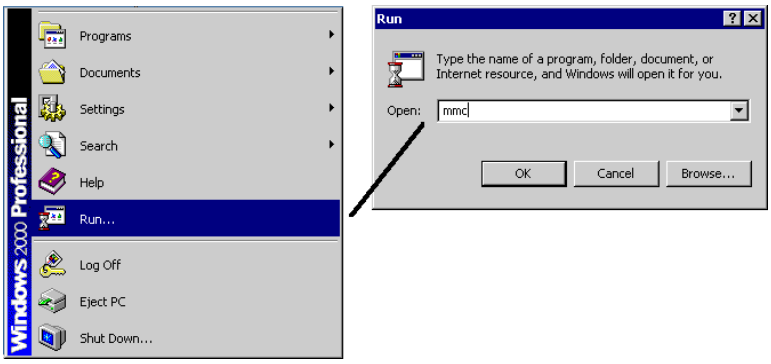
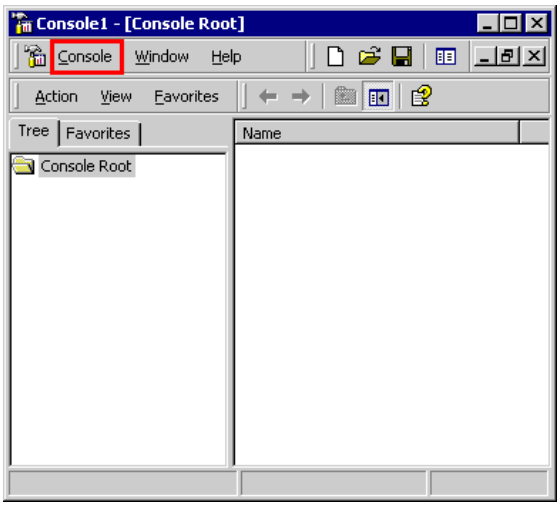
**TIP**

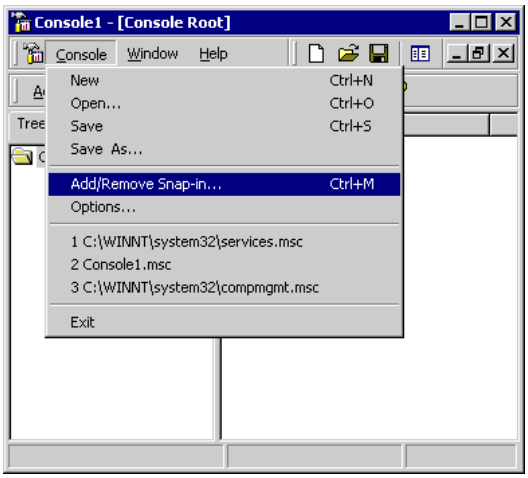
The installation of the System Management Display package creates a shortcut to a default console (.msc) file that can be launched from the following path:

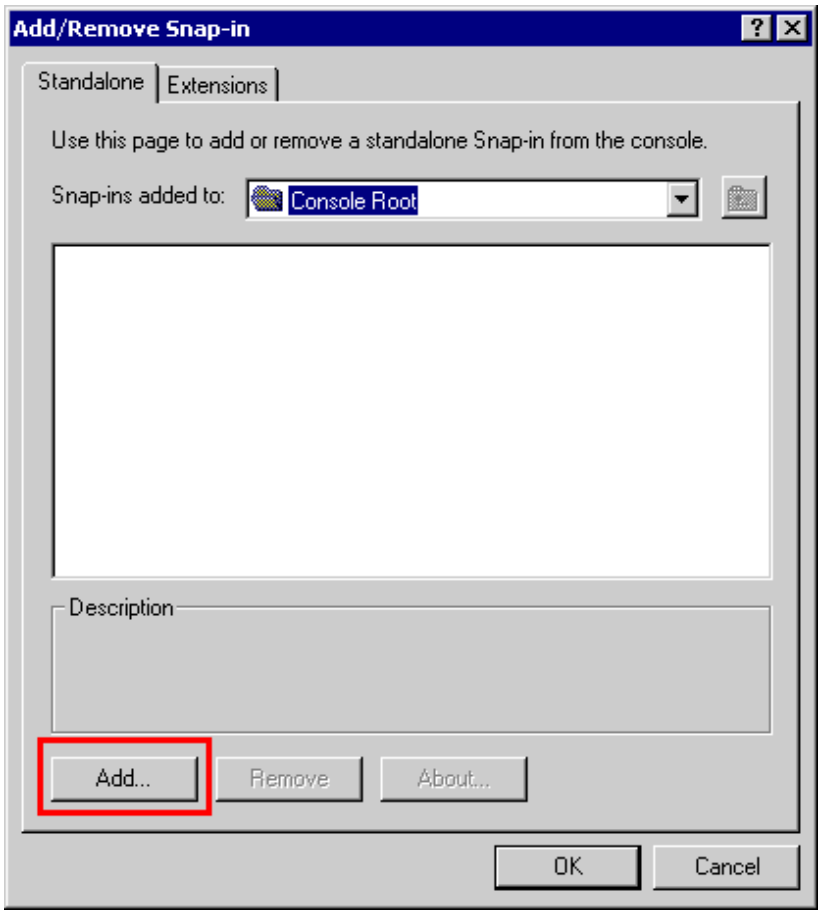
**Start > Programs > Honeywell Experion PKS > System Management > System Management Display**.

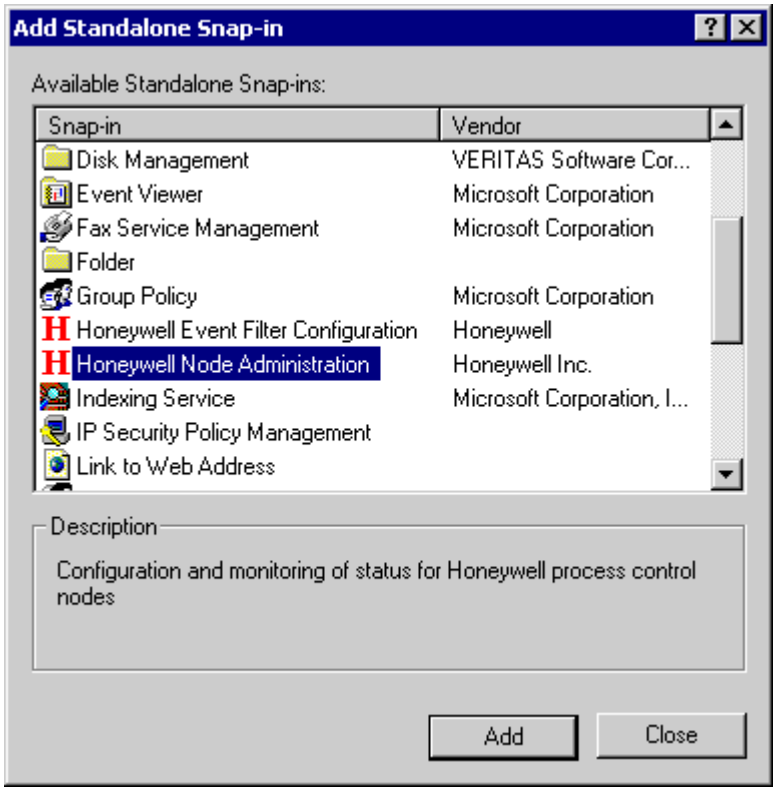
## Procedure to add the Node Administration Snap-In

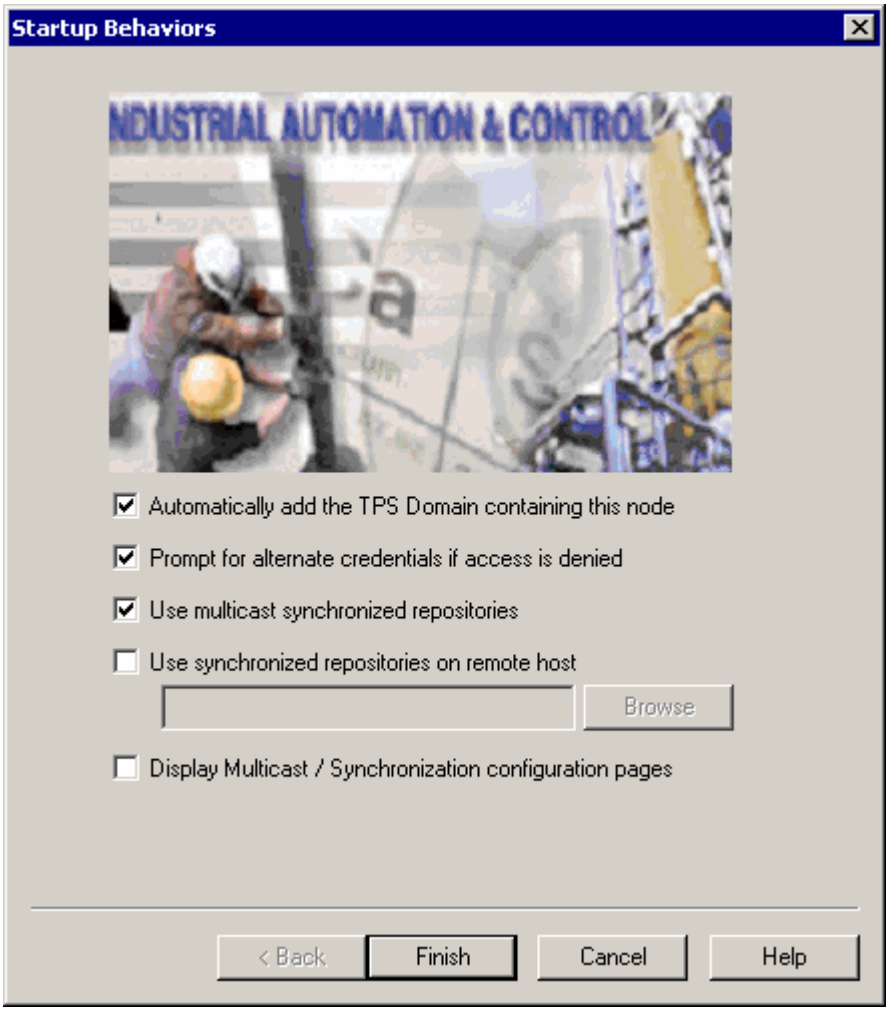
TPS users who have the Administrator access privileges can add the Node Administration Snap-in to the MMC using the following procedure. Experion users have the snap-in automatically added during node installation.

| Step | Action |
|---|---|
| 1 | Select **Run** from the **Start** menu and enter MMC in the command line.<br>  <br>**Result:** The MMC console appears. |
| 2 | From the MMC Console menu bar, select **Console**.<br>  |

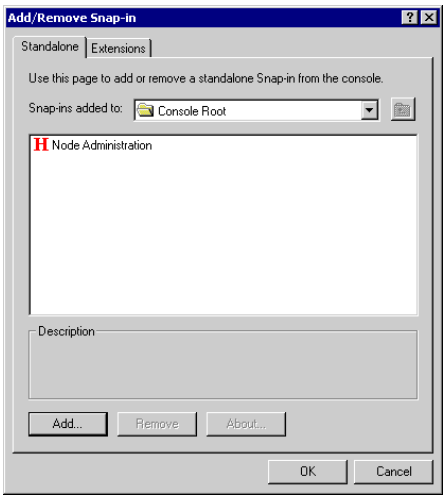
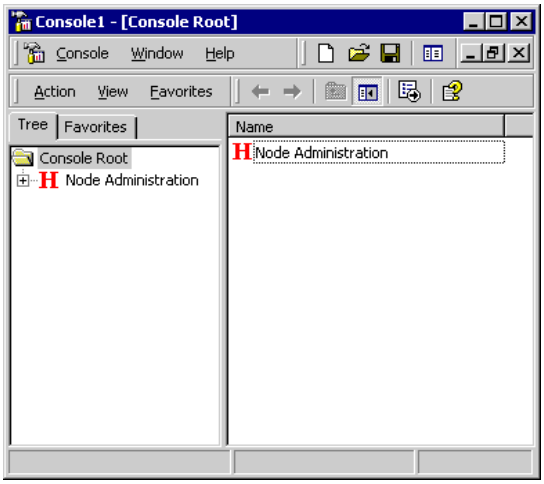
| Step | Action |
|---|---|
| **3** | Select **Add/Remove Snap-in** from the menu.<br>  <br><br>**Result:** The Add/Remove Snap-in dialog box appears. |

| Step | Action |
|---|---|
| **4** | From the Add/Remove Snap-in dialog box that appears, click **Add**.<br>  <br><br>**Result:** The Add Standalone Snap-in dialog box appears. |

| Step | Action |
|---|---|
| **5** | From the Add Standalone Snap-in dialog box, scroll to and select the **Honeywell Node Administration** Snap-In.  |

| Step | Action |
|---|---|
| **6** | Click **Add** in the Add Standalone Snap-in dialog box.<br><br>**Result:** A Startup Behaviors dialog box appears for the Honeywell Node Administration Snap-In.<br><br>  |

| Step | Action |
|---|---|
| **7** | In the Startup Behaviors dialog box, the default Startup Behaviors are shown with a checkmark next to them.<br><br>**Note:** If this node is not in a workgroup, review the default behaviors (you can always modify these properties later from the MMC), and then click **Finish.**<br>If this node is in a workgroup, uncheck the defaults, including the **Automatically add the TPS Domain containing this node** box.<br>If you check the box for **Automatically add the TPS Domain containing this node**, the system automatically adds the domain that the node is in and the TPS domain and/or console to the System Management Display.<br>**Result:** The Add Standalone Snap-in dialog box appears. |
| **8** | From the Add Standalone Snap-In dialog box, click **Close**.<br><br>**Result:** The Add/Remove Snap-In dialog box appears with Honeywell Node Administration in its selection window. |

| Step | Action |
|---|---|
| **9** | From the Add/Remove Snap-in dialog box, click **OK**.<br>  <br><br>**Result:** The Node Administration Snap-in appears in the MMC.<br>  <br> |
| **10** | Save your console settings in the **Start Menu>Programs>Administrative Tools** default directory. Your next step is to configure the Node Administration properties. |

## 5.3 Node Administration Properties

### Startup Behaviors Property Page

This section describes how to configure Node Administration properties. An example Node Administration Properties page appears in Figure 5.

**Figure 5 Example Node Administration Properties Page**

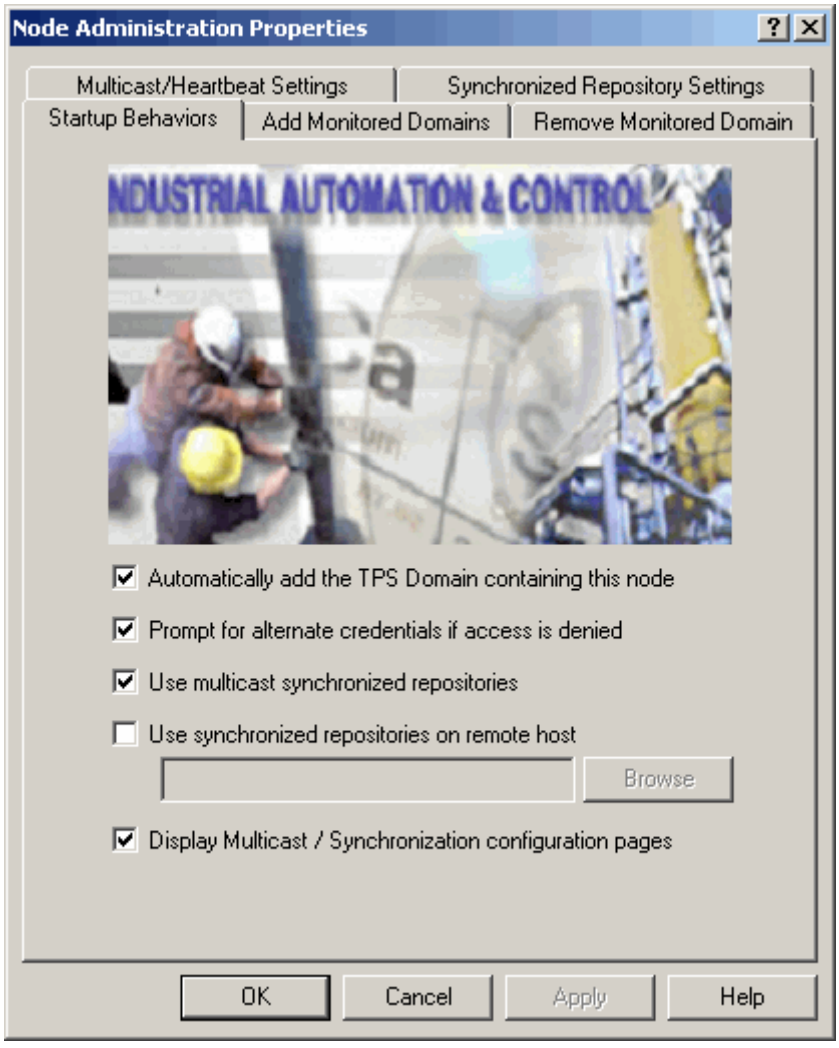


**Table 5 Node Administration Properties**

| Property | Description |
|---|---|
| **Startup Behaviors** | This page displays as a Wizard page when the Node Administration Snap-in is added to the MMC console. Once the snap-in has been added to the console, this page appears within a property sheet. It contains settings that configure the behavior of the Node Administration Snap-in at startup. Use this page to customize network connection behaviors when interoperating with a workgroup or when accessing nodes on a network connection where IP Multicast is disabled. |
| **Add Monitored Domains** | Use this page to add a domain or workgroup Item to the MMC console. |
| **Remove Monitored Domains** | This page allows removal of domains or workgroups that were previously added using the Add Monitored Domains page. |
| **Multicast/Heartbeat Settings** | This page is displayed for users that are members of the administrators group only. It applies IP Multicast and Heartbeat settings to all contained computer nodes. The page will only be displayed if the Node Administration Startup Behaviors property page Display *Multicast/Synchronization configuration pages* option is checked. |
| **Synchronized Repository Settings** | This page is displayed for users that are members of the administrators group only. This page applies Synchronized Repository Settings to all contained computer nodes. The page will only be displayed if the Node Administration item *Startup Behaviors* property *page Display Multicast/Synchronization configuration pages* option is checked. |

# 5.4 Startup Behavior Configuration

### Startup Behaviors defaults

Startup behaviors represent the initial behavior of the Node Administration Snap-in when the MMC first starts. The behavior defaults are shown in Figure 5. In most cases, you will accept the enabled defaults, and then enable other entries as needed.

### Automatically add the TPS Domain behavior

If you:

1. Enable the **Automatically add the TPS Domain containing this node** behavior and
2. The node has been added to a TPS domain

Then:

The system automatically adds the Windows domain and the TPS domain in which the local computer resides, into the System Management Display.

**ATTENTION**

If this node is in a workgroup, **DO NOT** select the **Automatically add the TPS Domain containing this node** behavior.

### Prompt for Alternate Credentials behavior

When you enable the Alternate Credentials behavior, it represents the enabling of a request for user id and password to allow access to a domain or component that the requesting user otherwise does not have.

### Use Multicast Synchronized Repositories

The default setting for this option is **Enabled** (checked). When unchecked, the connection to Heartbeat provider and System Event Provider will be bypassed. **Do not change this setting** except when working around problems related to connecting to synchronized repositories.

**ATTENTION**

Unchecking the **Use Multicast Synchronized Repositories** box disables system events for this System Management display.

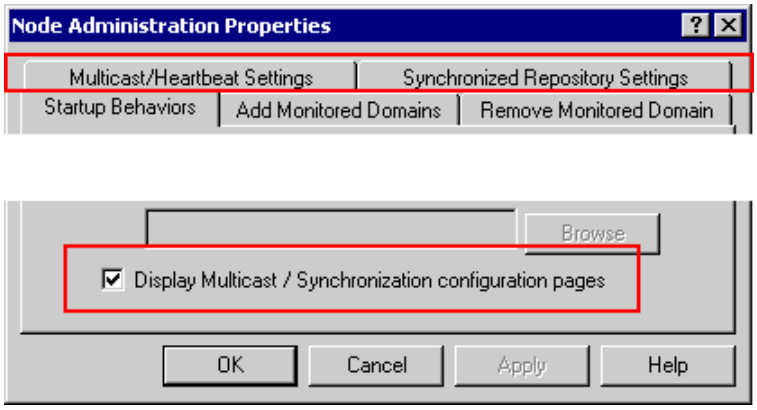
### Use Synchronized Repositories on Remote Host

The **Use Synchronized Repositories on Remote Host** behavior redirects the Node Administration tool to use the System Event Provider and the Heartbeat Provider on a remote node, rather than on the local repositories. This behavior is useful in cases where multicast traffic is restricted due to a firewall or router.

### Display Multicast/synchronization pages

When the Display Multicast/synchronization pages feature is enabled, additional tabs appear on the properties dialog boxes for the snap-in root, Windows domain, and TPS domain property dialog boxes. Only users who are members of the System Administrators Group can view this display.

**Figure 6 Common Page Properties**

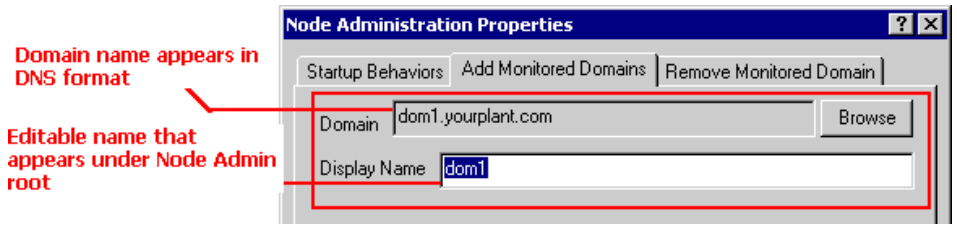


# 5.5 Adding the Monitored Domains Tab

### Domain display name properties

When you select a domain or workgroup for monitoring, the system updates the properties to display the **Windows** domain name in DNS format. Use the **Browse** button to find the domain that you want to monitor.

**Figure 7 Domain Display Name Properties**




You can edit the displayed name to be a more meaningful name from the root or domain properties dialog boxes.

**Figure 8 Editing the Display Name**

### Alternate user ID

Multiple **Windows** Domains may be displayed in a single console. This requires that each domain be associated with a user identity. User identity will default to the logged on user unless an alternative identity is specified during console configuration (or at run-time, if an access permission error occurs).

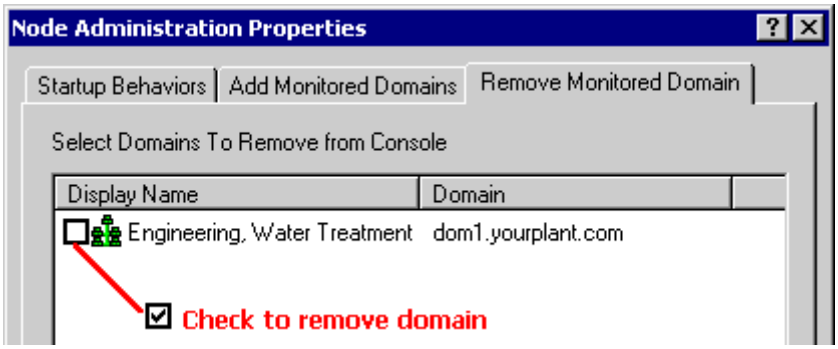
An alternate user identity may be specified for each domain added to the console display and may be edited using a **domain item property page**. Alternate user identity information may be saved to the console file when saving the console configuration. If saved, the alternate user identity for each domain will be read from the console file during console loading and will be used in reconnecting to the configured domain resources. If user identity is not saved, the user will be prompted for authentication information on the first denied access to an unauthorized domain. The user identity will then be used for authentication throughout the remainder of the session.

## 5.6 Removing the Monitored Domains Tab

### Example display

Check the domains or workgroups you want to remove. Checking domains removes any **Windows** domains, TPS Domains, or static computers contained within a domain, from the Node Administration root.

**Figure 9 Removing Domains Display**



# 5.7 Multicast Communications Purpose

### Providers use multicast

Both the heartbeat provider and the synchronized repository provider use IP Multicast. IP Multicast Group may be determined by setting the IP Multicast address or destination port for a group of nodes. Multiple independent multicast groups may be used to create communities that are exclusive of each other. Heartbeats and synchronization messages from such communities will not cross the Multicast group boundary. This isolates name service, system events and heartbeats between the communities.

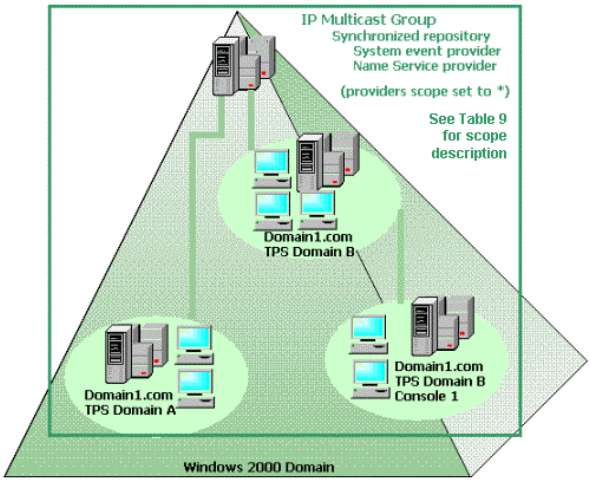
**ATTENTION**

System Management Runtime utilizes Multicast to process information between nodes. Multicast must be enabled on all network switches and routers that interconnect participating nodes.

### Overview example 1

Figure 10 shows all nodes within the same IP Multicast Group using the same synchronized repository for name service and system event provider.

**Figure 10 Nodes within the same Multicast scope**

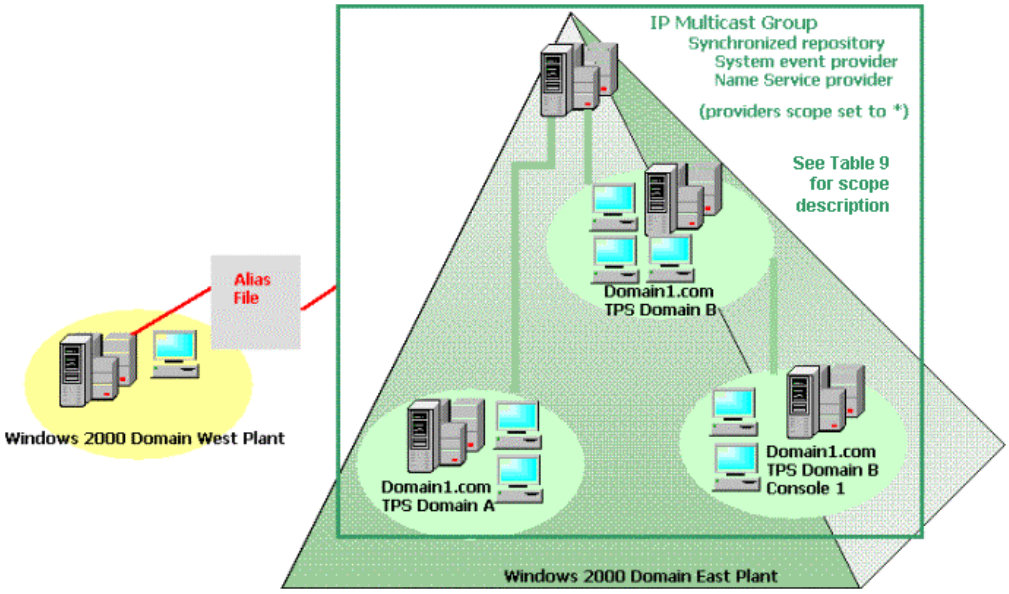


### Overview example 2

The following figure shows nodes outside of an IP Multicast Group. In order for HCI Client applications nodes to communicate with HCI/OPC servers within the Multicast Group, an alias name file must be deployed in the nodes that are outside of the IP Multicast group.

The System Management Display uses the **Remote Repository** behavior to view system events and node status information.

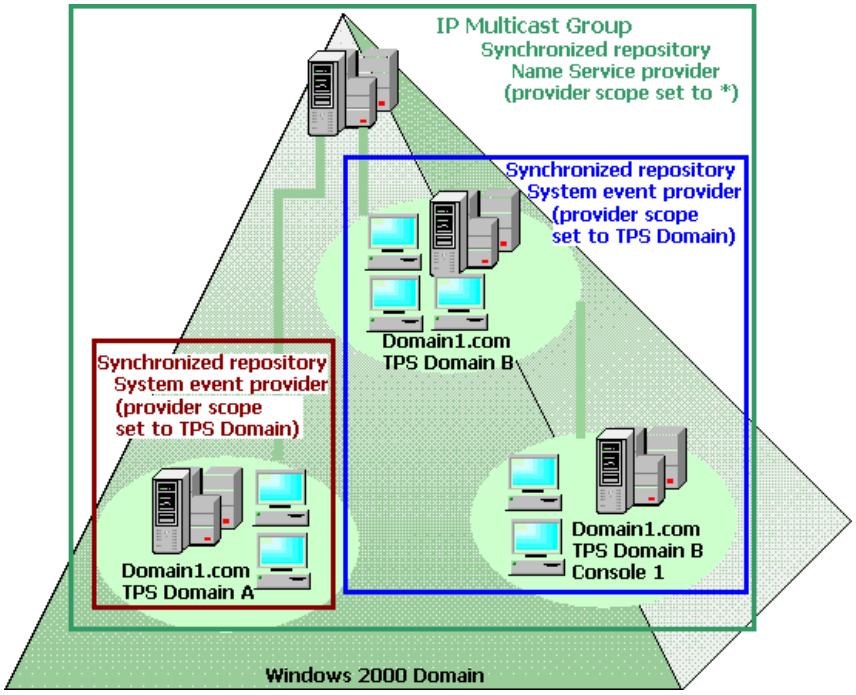
**Figure 11 Nodes outside of an IP Multicast Group**



### Overview example 3

The following figure is a variation of example 1. It shows all nodes within the same IP Multicast Group using the same synchronized repository for name service, but a different repository for system events. In this case, system events are processed within their own TPS Domain.

**Figure 12 Variation of nodes within the same IP Multicast Group**




The configuration of these settings and additional scenarios are described in the following sections.

# 5.8 Multicast Heartbeat Settings

### Multicast/Heartbeat Settings Property Page

From this page you configure the IP Multicast group and other operational parameters affecting the heartbeat community. These settings should only be changed by personnel familiar with the use of the IP Multicast protocol and Honeywell Fault Tolerant Ethernet (if installed).

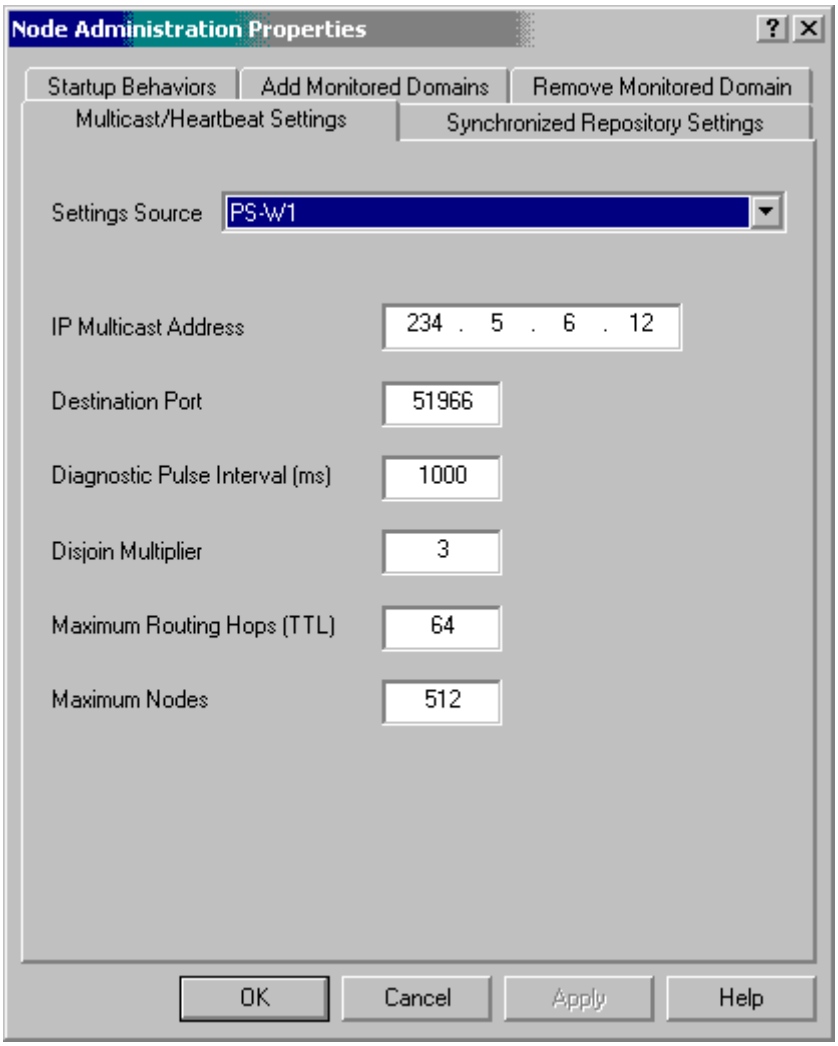
**ATTENTION**

When the settings from the page are applied, by default all computers contained by the item that invoked this property page will be affected. A selection list will allow customization of the application of these settings prior to being applied.

### Heartbeat settings description

The following figure shows an example Multicast/Heartbeat settings configuration.

**Figure 13 Heartbeat Settings**



### Using the Multicast/Heartbeat Settings property page for multiple computers

**ATTENTION**

This page will only be displayed for administrator group members.

This page will only be displayed if the Display Multicast /Synchronization configuration pages box is checked on the Startup Behaviors property page of the Node Administration item.

The system applies changes to settings on the *Multicast/Heartbeat Settings* property page to all computers contained by the System Management Display item for which the page was invoked. For example, if you right-click a domain object and select the Properties item from the context menu, the system applies the settings made on the Multicast/Heartbeat settings page to all computers contained on the display below the control domain.

When applying setting changes, the property page attempts to connect to each contained computer and validate that the settings can be applied. A selection list box appears, which displays the results of this validation and allows you to change the selection state of the computers. Normally, if a computer cannot be configured, refrain from applying the changes until the situation is remedied.

The *Multicast/Heartbeat Settings* property page does not use the heartbeat state of a computer to determine whether a connection should be made. As a result, completing the evaluation of node configurability may be a time-consuming task.

### Selecting a Source of Settings to be Viewed/Modified

A list of all contained computers is presented in the *Settings Source* pull-down list. Each selection from this pull-down list identifies the computer from which the displayed settings are obtained. This computer is used when populating the Settings page. Once changes are made to these values, the changes are applied to ALL computers within the list.

Table 6 describes each of the settings in the *Multicast/Heartbeat Settings* property page.

**Table 6 Description of Multicast/Heartbeat Settings**

| Setting | Description |
|---|---|
| IP Multicast Address | Use the IP Multicast address for both heartbeat (FTE compatible) messages and synchronization of repositories (name and service events). |
| Destination Port | UDP destination port for heartbeat settings. |
| Diagnostic Pulse Interval (ms) | The period between diagnostic multicast message transmission. |
| Disjoin Multiplier | The number of diagnostic messages that may be missed before a node is disjoined from the heartbeat community. |
| Maximum Routing Hops (TTL) | The maximum number of routing devices that the message may pass through. This is the IP Multicast time-to-live value set in each multicast message. |
| Maximum nodes | The maximum number of heartbeat nodes that the configured heartbeat provider can provide status for in its heartbeat message. |

# 5.9 Determining the Synchronized Repository Scope

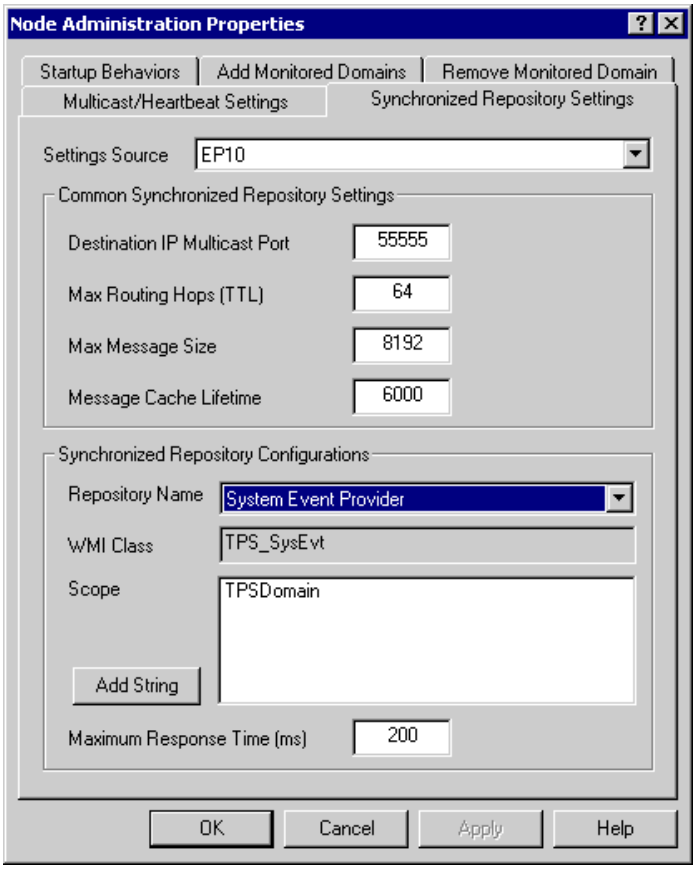
### Synchronized Repository Settings Property Page

From this page you configure the communication between synchronized repository nodes. Members of the administrator user group may only display this page.

### Synchronized Repository Settings example

The following figure shows an example Synchronized Repository Settings Property page.

**Figure 14 Synchronized Repository Settings Property Page**



### Type of settings

The Synchronized Repository Settings property page contains two types of information:

- Common Synchronized Repository Settings information (located in the upper portion of the page)
- Synchronized Repository Configurations information (device-specific information located in the lower portion of the page).

### Common Synchronized Repository Settings information

This information includes values used by the Synchronized Repository provider (SRP) on behalf of all synchronized repositories (Name Service and System Event Providers). Table 7 shows values for Common Synchronized Repository Settings.

**Table 7 Values for Common Synchronized Repository Settings**

| Value | Description |
|---|---|
| **Destination IP Multicast Port** | UDP destination port for all synchronized repository messages. The IP multicast address specified on the *Multicast/Heartbeat Settings* page will be used for synchronized repository communications. |
| **Max Routing Hops (TTL)** | The maximum number of routing devices that the message may pass through. This is the IP Multicast time-to-live value set in each multicast message. |
| **Max Message Size** | The maximum size of the synchronized repository message (IPMC UDP packet). The default value of 8192 should be adequate. Increase the value only if buffer overflow errors are reported in the event log. |
| **Message Cache Lifetime** | The length of time (in milliseconds) that a message is cached for detection of lost messages and for re-transmittal if requested. |

### Synchronized Repository Configurations information

This information is provider specific. Use this information to configure the scope of synchronization for registered synchronized repositories. This section is not populated until a specific provider has been selected from the *Repository Name* pull-down list. Table 8 shows information about Synchronized Repository Configurations.

**Table 8 Synchronized Repository Configurations Description**

| Setting | Description |
|---|---|
| **Repository Name** | A pull-down list used to select repository settings to view and configure for either the Name Service provider or the System Event Provider. |
| **WMI class** | A read-only field that contains the WMI class implemented by the selected synchronized repository provider. |
| **Scope** | The values entered in this list describe the Active Directory scope of synchronization. Values may be Active Directory paths of container objects (domains and organizational units) or reserved strings that are resolved automatically to the following definitions:<br>**Domain** The domain containing this computer.<br>**TPSDomain** The organizational unit containing this computer that is marked as a TPS Domain. Workgroups will resolve this value to the workgroup name.<br>**Console** The organizational unit containing this computer that is marked as a console.<br>* The full scope of the Multicast group. |

If reserved strings are entered and cannot be resolved, the effective scope will be the local computer only.

### Selecting a Source of Settings to be Viewed / Modified

The *Settings Source* pull-down list displays a list of all contained computers. Select a computer from this list when populating the settings page. Once changes are made to the values of the selected computer, the system applies the changes to ALL computers within the list.

### Selecting a Repository to Configure

All registered synchronized repositories are displayed in the *Repository Name* pull-down list. The system retains changes made in this section until the changes are either applied or cancelled. By selecting a repository by name and making changes, and then selecting the next repository and making changes, all configurations can be tailored and applied to all computers contained by the selected *System Management Display* item.

**CAUTION**

When assigning Active Directory Scope Values to computers, it is extremely important that scopes for a given repository do not overlap.

For example: If computer A is in Domain 1 and TPS Domain 1 and computer B is in Domain 1 and TPS Domain 2, it is illegal to set a System Event Provider scope on computer A to be Domain and the scope on computer B to TPSDomain.

It is legal to set both computers to Domain. It is also legal to set computer A to TPSDomain and computer B to TPS Domain.

The configuration pages do not enforce these rules. Failure to follow these rules will result in inconsistent information in your Name Service and System Events.

### Reserved Scope Values

To simplify scope setting and installation, use reserved scope values when defining the synchronization scope of a provider. Table 9 describes possible reserved scope values.

**Table 9 Reserved Synchronization Scope Values**

| Scope Value | Scope Description |
|---|---|
| ***** | All sources are included in the synchronization. This scope will be the entire scope of the IP Multicast group. |
| **Domain** | Synchronization messages will be processed from all nodes within the same Windows domain. For workgroup nodes this will include all nodes in the workgroup. |
| **TPSDomain** | Synchronization messages will be processed from all nodes within the containing Organizational Unit marked as a TPSDomain. If the node is not in a TPSDomain, the value will default to the containing domain. For workgroup nodes this will include all nodes in the workgroup. |
| **Console** | Synchronization messages will be processed from all nodes within containing Organizational Unit marked as a Console. If the node is not in a Console, the value will default to the containing domain. For workgroup nodes this will include all nodes in the workgroup. |
| **Active Directory Path in UNC format. For example: OU=MyTpsDomain DC=MyDomain,DC=Local)** | All nodes contained by the Active Directory object specified will be included in the synchronization scope. |
| **[blank]** | No scope string values will disable synchronization with all other nodes. |

### System Management Provider Default Scope Values

The following scope values are installed by default for the specified providers.

**Table 10 System Management Provider Default Scope Values**

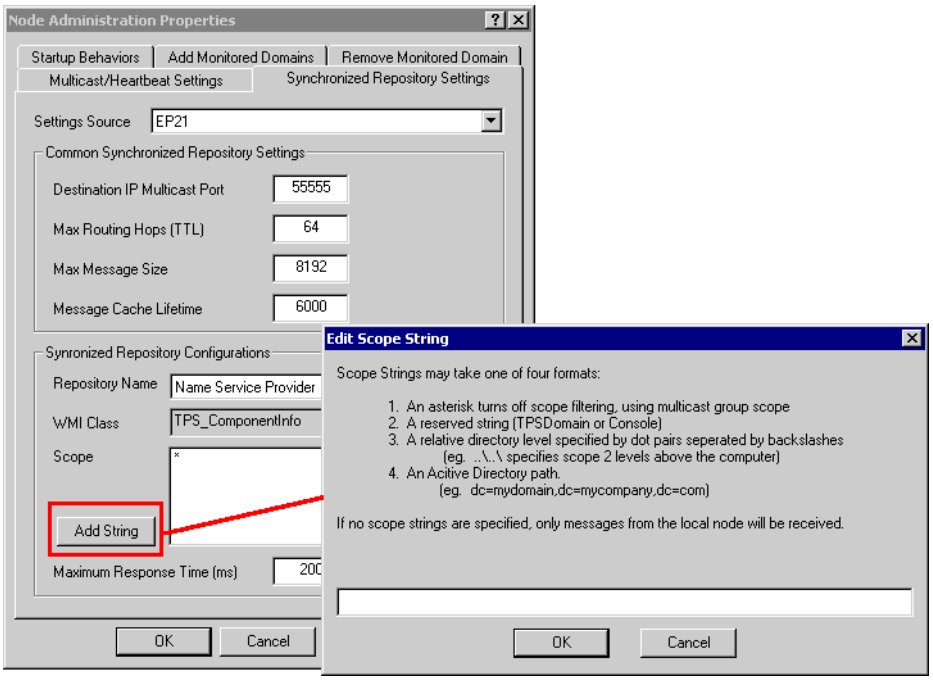
| Provider | Scope Value | Effective Scope |
|---|---|---|
| **Name Service Provider** | * | All nodes within the specified IP Multicast group will be included in the synchronized view. This allows client applications to access servers across TPS Domains and across Windows Domain boundaries – assuming permissions have been set to allow this. |
| **System Event Provider** | Domain | System events will be synchronized between all members of a Windows Domain or workgroup. Use this scope value if you want to view and control System Events across multiple TPS Domains that are in the same Windows Domain. See the Synchronization Scope Scenarios section for more details on this setting. |

# 5.10 Synchronization Scope Scenarios

### Scope values set the provider view

The following scenarios describe common uses of the synchronization scope values to tune the view of a provider. Since this will most often apply to the System Event Provider, it will be used as the provider described in the scenarios. Scope settings can be modified using the Edit Scope String dialog box.

**Figure 15 Edit scope string dialog box**



### TPS Domain Computers View only Events for their TPS Domain

If you want to limit the ability to view and control System Events to only those nodes contained within the TPS Domain organizational unit, set the scope value to ***TPSDomain***. If multiple TPS Domains exist, each TPS Domain has its own view of System Events.

### Multiple TPS Domains and their associated events must be viewable

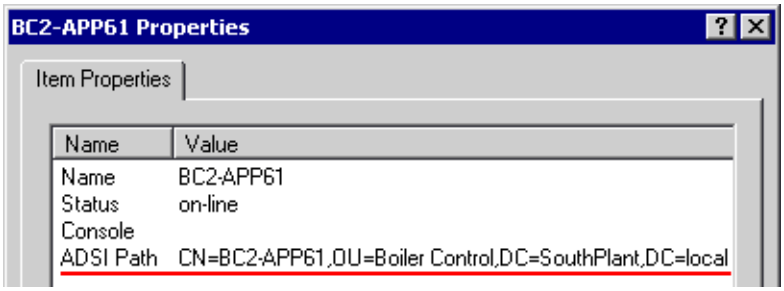
Use the default settings (***Domain***) for this scenario.

If you want to view (and control) System Events across multiple TPS Domains and the TPS Domains are in the same Windows Domain, set the scope value to ***Domain***. If the TPS Domains are in different Windows Domains, either set the scope to ***** or specify the multiple domain paths explicitly using multiple scope values.

### Procedure to modify current scope configuration for setting multiple scope values

Follow these steps to modify the current scope configuration for multiple scope values.

| Step | Action |
|---|---|
| **1** | From the **Synchronized Repository Settings Property Page**, double-click the name of the current repository name in the **Repository Name** list box. |
| **2** | The **Edit Scope String** window appears. Delete the entry from the edit box in this window. |

| Step | Action |
|---|---|
| **3** | Add the following string commands in UNC format:<br>First value: ***DC=Domain1,DC=MyCompany,DC=com***<br>Second Value: ***DC=Domain2,DC=MyCompany,DC=com***<br>Where the first and second values are from your system.<br>**Result:** System Events will be synchronized between all members of the containing domain(s). With this configuration, you can set up a System Management Display console that displays System Events of multiple TPS Domains and even Windows Domains.<br>**TIP**<br>To help you determine the UNC format for a scope, you can check a computer's properties and examine its ADSI path as shown in the following example.<br>  |
| **4** | Click **OK**. |

### Restricting users from using the System Management Display

To restrict users from viewing the System Management Display, create an MMC console file that includes only the desired TPS Domain. Make sure that the **Startup Behaviors** property page does NOT have the *Log all system events to the Node Administration item* box checked. With this configuration, a single System Event Server can be used to service multiple TPS Domains.

### Applying Synchronized Repository Settings to multiple computers

**ATTENTION**

This page will only be displayed for administrator group members.

This page will only be displayed if the *Display Multicast / Synchronization configuration pages* box is checked on the *Startup Behaviors* property page of the *Node Administration* item.

Changes to settings on the *Synchronized Repository Settings* property page are applied to all computers contained by the System Management Display item for which the page was invoked. For example, if you right-click a domain object and select the *Properties* item from the context menu, the system applies settings changes made on the *Synchronized Repository Settings* page to all computers contained on the display below the domain item.

### Procedure for applying changes to settings

| Step | Action |
|---|---|
| 1 | When applying setting changes, the *Synchronized Repository Settings* property page attempts to connect to each contained computer and validate that the settings can be applied. A selection list box appears, displaying the results of this validation and allowing the selection state of the computers to be changed. |
| 2 | Normally, if any computer cannot be configured, then you should not apply changes until the situation is remedied. |

**ATTENTION**

This page does not use the heartbeat state of a computer to determine whether a connection should be made – as a result the evaluation of node configurability may be a time-consuming task.

# 5.11 Managing Organizational Units and Computers

### About Managed Organizational Units and Computers

After you select the domain(s) you want to monitor, you can add managed organizational units or computers in each domain. For example, a TPS Domain is an example of an Organizational Unit (OU).

Organizational Units are Active Directory containers into which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains. An organizational unit is the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority. Using organizational units, you can create containers within a domain that represent the hierarchical, logical structures within your organization.

You create TPS Domains and Consoles as Organizational Units in the domain controller. A Console is an OU created within the TPS Domain OU. To add TPS Domains and Consoles to an existing Node Administration configuration, by simply add them and refresh the connection. The console is contained within the TPS Domain and is not added separately.

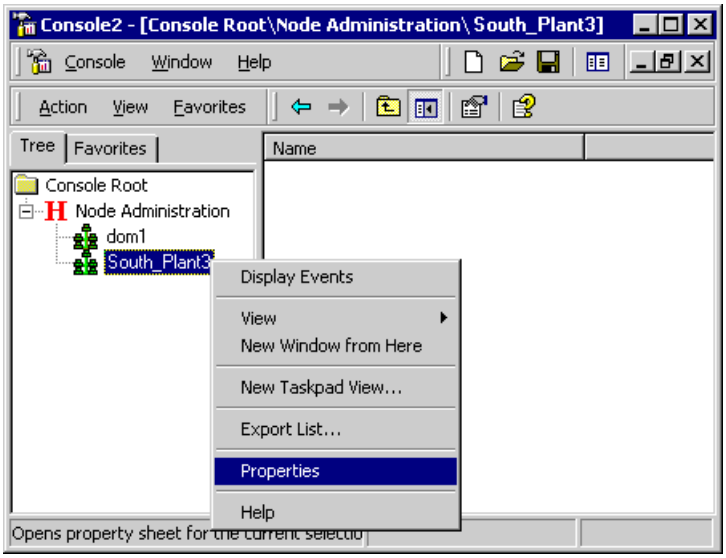
In addition to managing organizational units, you can add computers such as TPS nodes, non-TPS nodes, Experion  servers, or office desktops to the monitored domain. These items do not necessarily have to be contained within a TPS Domain or Console OU for them to appear in the System Management Display.

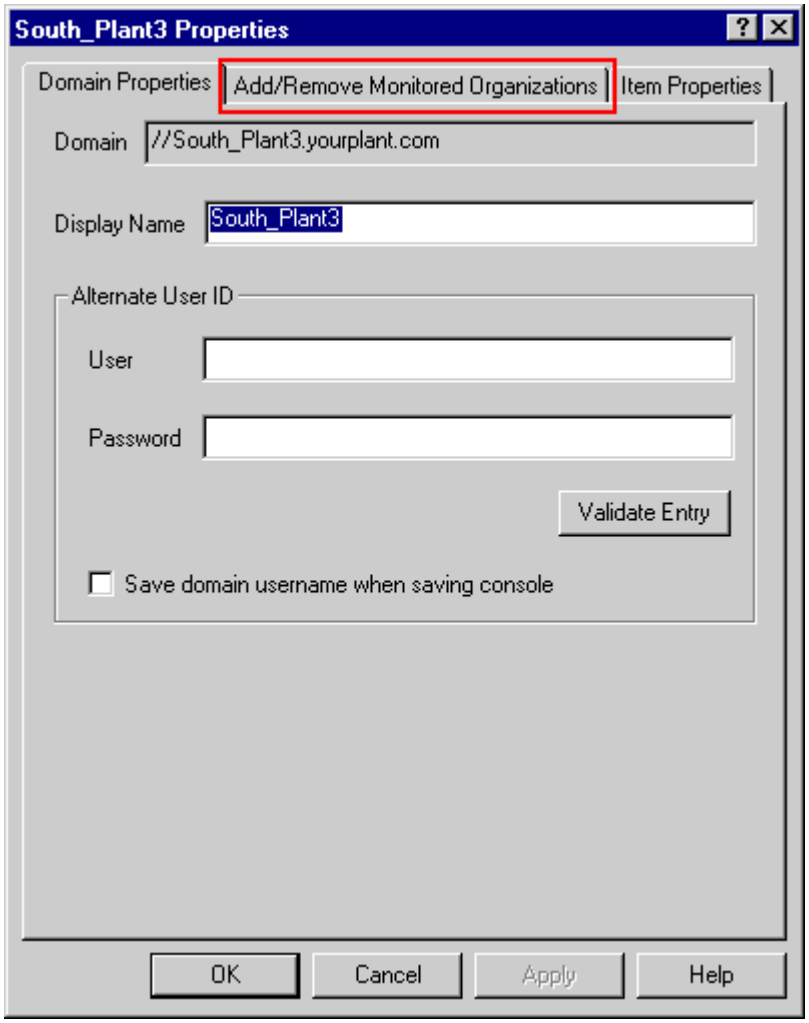
## Procedure for adding a Managed OU to a Monitored Domain

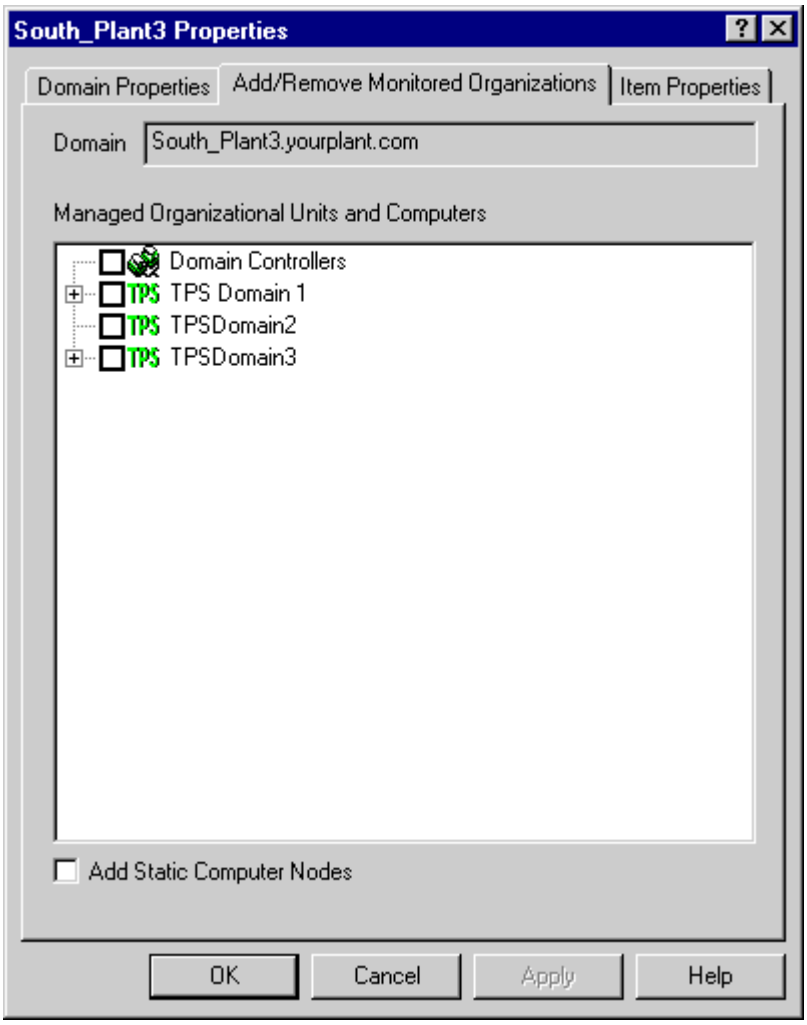
The following procedure describes how to add a managed OU (such as a TPS Domain) to be monitored by the **Node Administration** Snap-In. After performing this procedure, you can perform node-specific tasks, such as HCI Component Configuration.

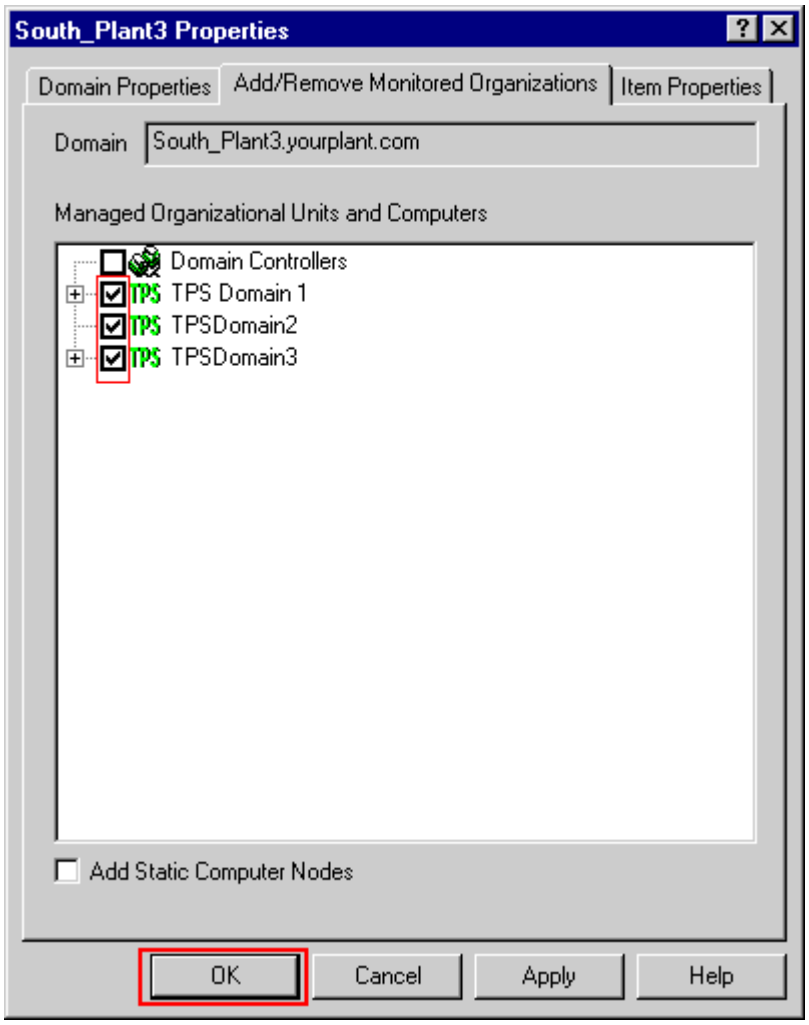
**TIP**

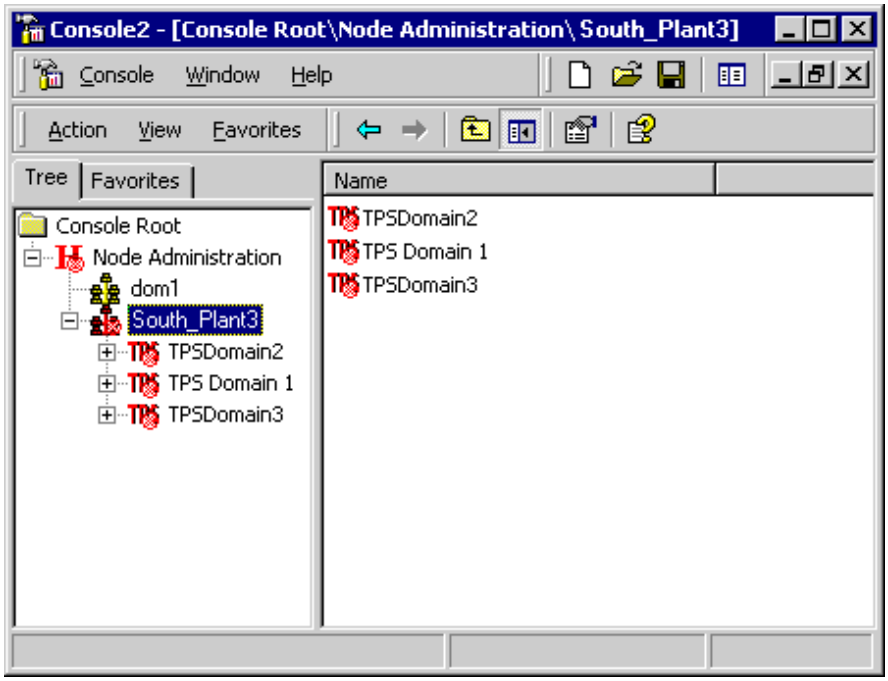
This procedure assumes that Organizational Units (OUs) such as TPS Domains have been created and that you are aware of which domains already contain an OU such as a TPS Domain. If you don't know which of your plant's domains contain TPS Domains, you can always browse for OUs from the domain's **Properties** tab.

| Step | Action |
|---|---|
| 1 | From the MMC scope pane, right-click a domain that contains a TPS Domain and select **Properties** from the menu.<br>  <br>**Result:** The selected domain's **Properties** dialog box appears. |

| Step | Action |
|---|---|
| **2** | From the domain's **Properties** dialog box, select the **Add/Remove Monitored Organizations** tab.<br>  <br><br>**Result:** The monitored organizations appear in the selection window of the Add/Remove Monitored Organizations tab. |

| Step | Action |
|---|---|
| **3** | Check the TPS Domains you want to manage.<br>  |

| Step | Action |
|---|---|
| 4 | In this example, three TPS Domains are selected as managed OUs. Click **OK**.<br>  |

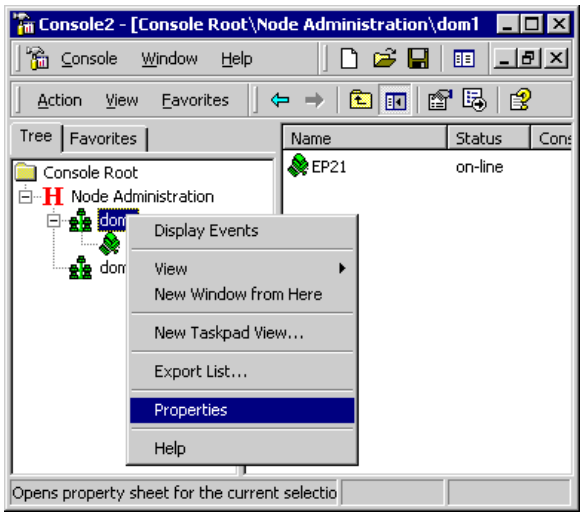
| Step | Action |
|---|---|
| **5** | The TPS Domains appear in the scope and results pane. After completing the OU configuration, you can proceed with other administration tasks or continue to modify and save the console view.<br>  |

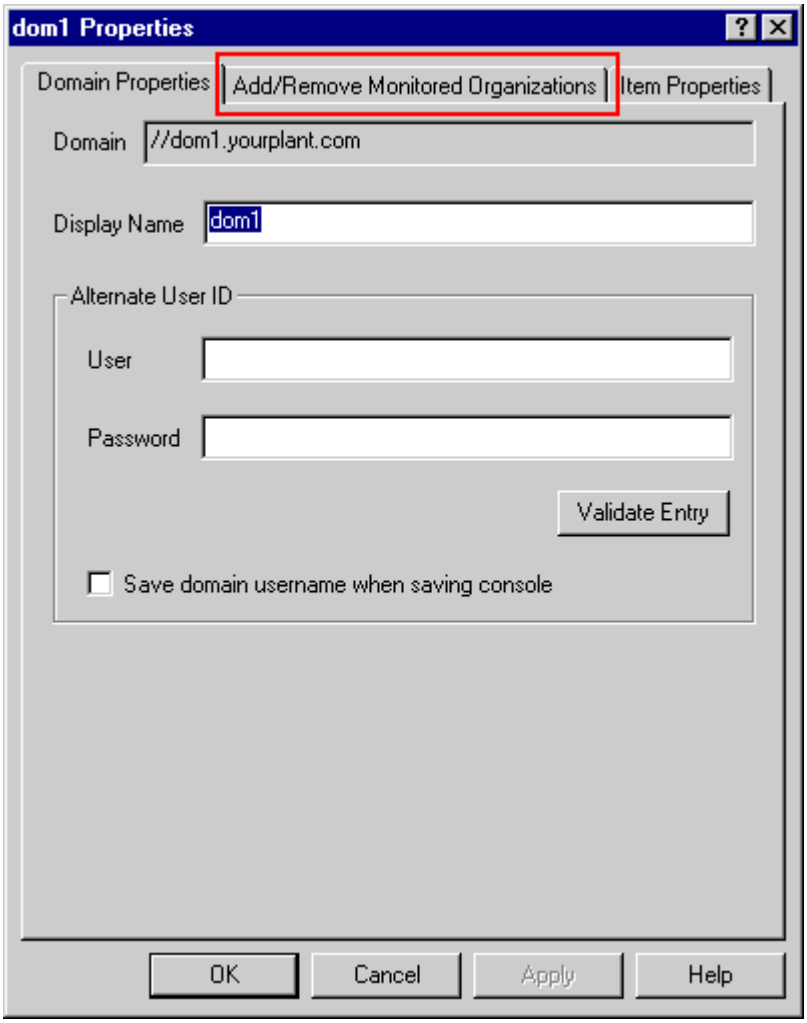
### Procedure for adding a Computer as Managed item

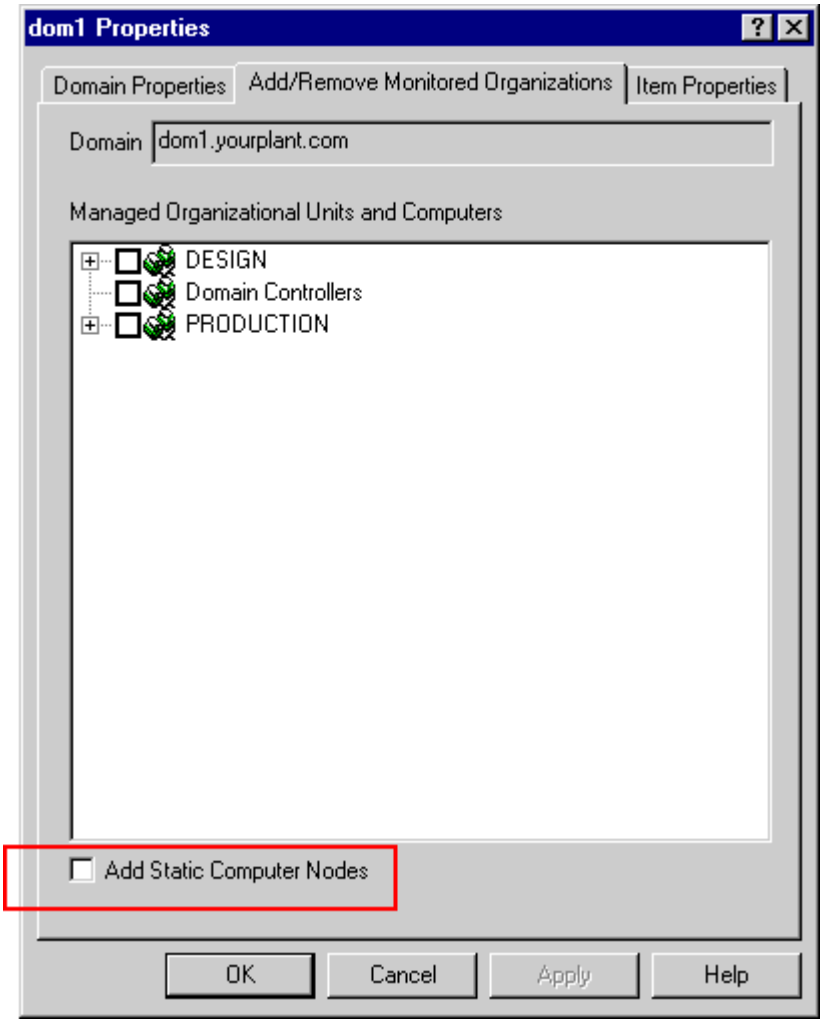
The following procedure demonstrates how to add a computer to be monitored by the Node Administration Snap-In. After performing this procedure, you can then perform specific tasks, such as HCI Component Configuration. This procedure can also be done at the same time as selecting an OU for management.

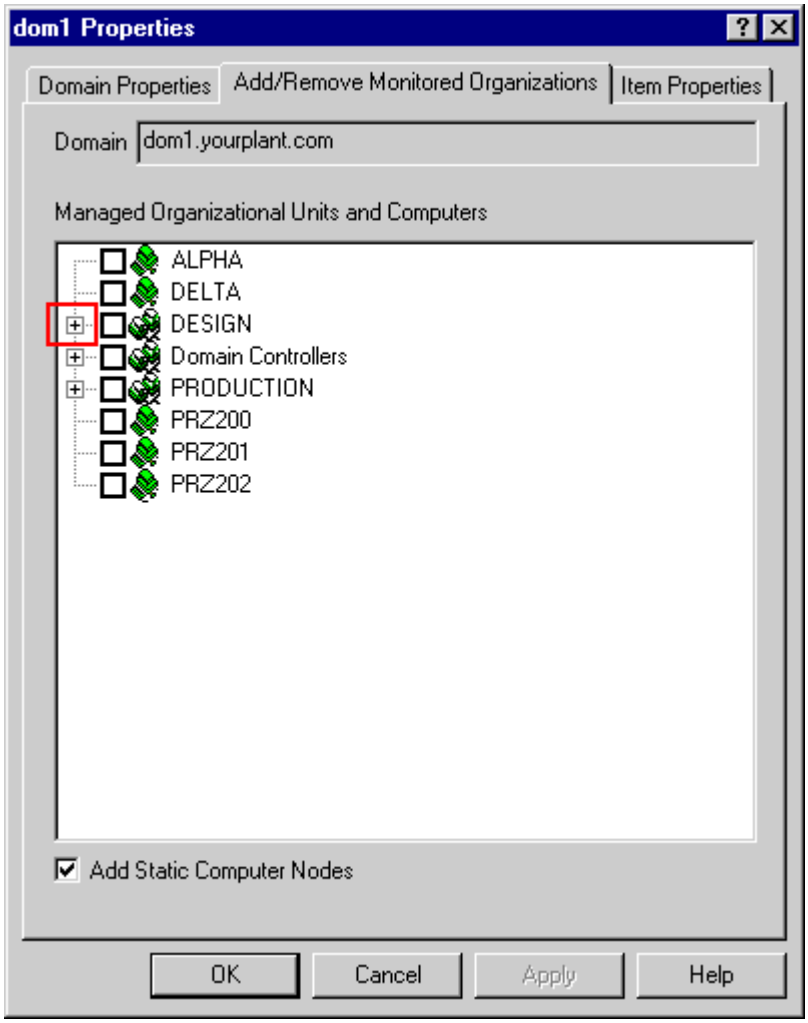
**TIP**

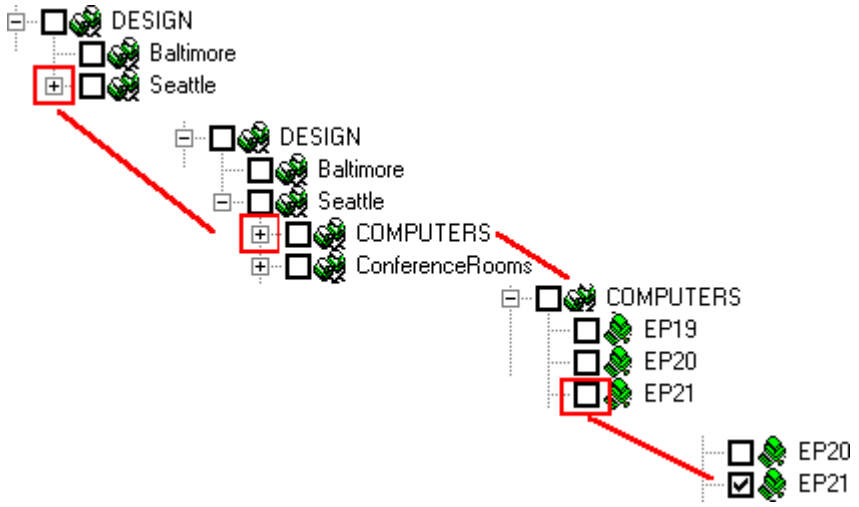
This procedure assumes you are aware of which domain contains the desired computer. If you don't know which of your plant's domains contain the desired computer, you can always browse for the computer from the domain's **Properties** tab.

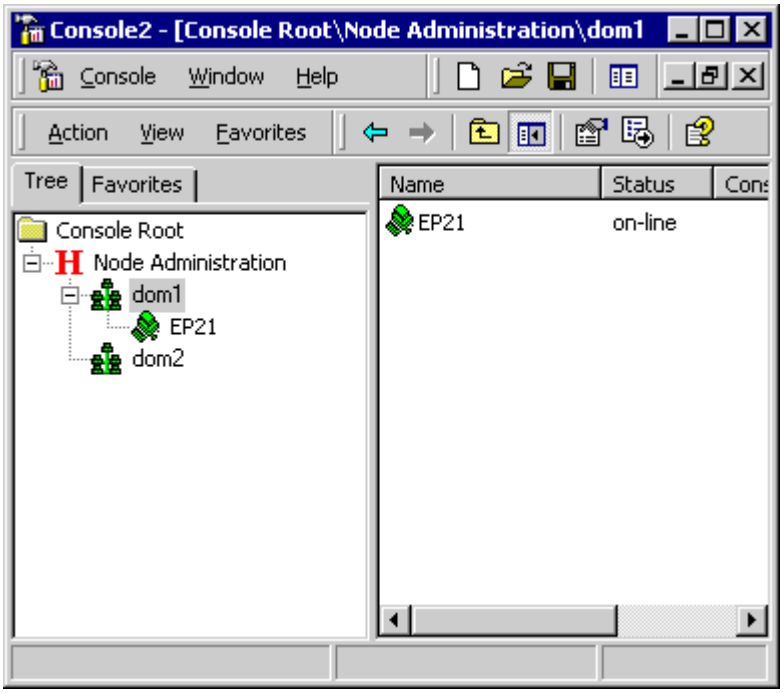
| Step | Action |
|---|---|
| 1 | From the MMC scope pane, right click a domain that contains the computer of interest and select Properties from the menu.<br>  <br>**Result:** The selected domain's **Properties** dialog box appears. |

| Step | Action |
|---|---|
| **2** | From the **Domain Properties** dialog box, select the **Add/Remove Monitored Organizations** tab.<br>  <br><br>**Result:** The monitored organizations appear in the selection window of the **Add/Remove Monitored Organizations** tab. |

| Step | Action |
|---|---|
| **3** | Check the **Add Static Computers** checkbox so that you can browse to the computer(s) of interest.<br>  <br><br>**Result:** The selection window refreshes to include computers that are not members of a Managed Organizational Unit. |

| Step | Action |
|---|---|
| **4** | From the updated selection window, expand the domain's tree view to locate the computer of interest. In this example, the computer of interest resides in the domain named DESIGN. It is not necessary to click the checkbox of the domain (otherwise you would be monitoring all the computers in that domain), just click the + icon to expand the view.<br>  <br> |

| Step | Action |
|---|---|
| **5** | Continue to expand the view until you locate the computer of interest. Click the checkbox for the computer of interest then click **OK**.<br>  |

| Step | Action |
|---|---|
| **6** | The computer of interest appears in the MMC (Microsoft Management Console) view. You can proceed with other administration tasks or continue to modify and save the console view.<br>  |

# 5.12 Managing Components

### About managed components

Managed components are components that, once configured, automatically appear on the System Management Display.

Managed components can be started, stopped or optionally checkpointed (depending on the type of server. Not all servers support checkpointing. For more information about checkpointing, see the *TPN Server Guide*).

Managed components include the following:

- TPN Server
- Fault Tolerant Ethernet (FTE)
- CL Server
- NWDDB Server
- System Event Server
- System Performance Server

### Additional references for managing a component

| Type of component | Reference |
|---|---|
| TPN Server | *TPN Server User's Guide* |
| Redirection Manager (RDM) | *This manual*<br>*Redirection Manager User's Guide* |
| Fault Tolerant Ethernet (FTE) | *Fault Tolerant Ethernet Overview and Implementation Guide* |
| CL Server | *CL Server User's Guide* |
| NWDDB Server | *GUS HCI/OPC Data Access Manual* |
| System Event Server | *This manual* |
| System Performance Server | *This manual* |
| HCI Components | *This manual, Section 6.1* |

## 5.13 Using Monitored Components

### About monitored components

Monitored components are HCI or generic OPC servers, which are configured to be managed by the Redirection Manager (RDM).

### About Redirection Manager

The Redirection Manager is optional server software that provides your system with high availability and reliability. Redirection Manager supports OPC clients and servers. It allows servers to be configured so that, if a Primary server fails, RDM automatically redirects existing HCI/OPC clients to a Secondary server, without interruption to network communications. For more information about the Redirection Manager, refer to the *Redirection Manager User's Guide*.

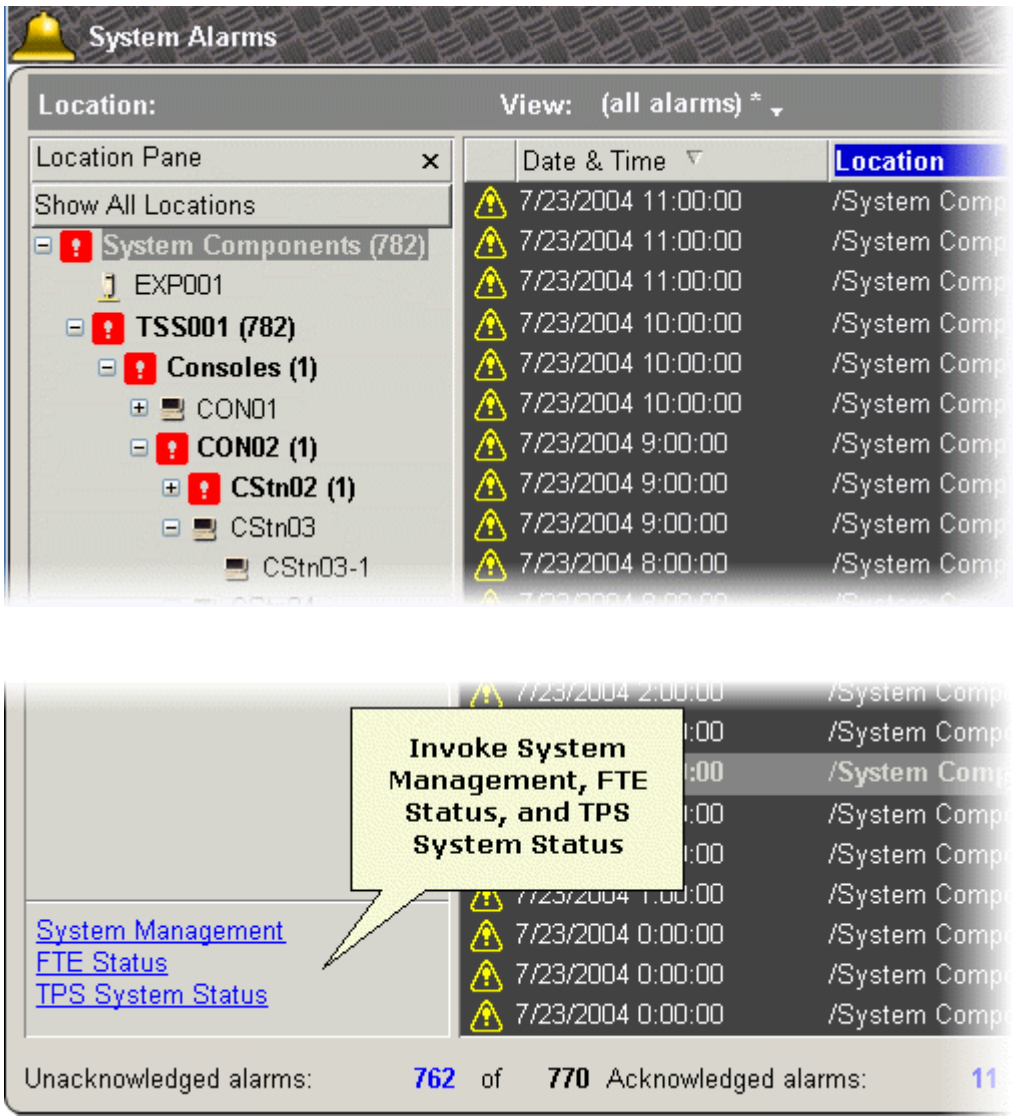
### How Redirection Manager uses monitored components

The Redirection Manager requests CAS of a node to monitor the state/status of a redirection (Primary) server. This server is also a monitored server. When monitored, the server appears in the System Management Display. The server is removed when the Redirection Manager requests the CAS to stop monitoring the server.

## 5.14 Invoking from Experion System Status

### System Management Display link

The Experion System Status provides a tree view status of entities within the system. If System Management is installed on an Experion node, an additional link appears to launch the System Management display. The Experion System Status also provides links to support Fault Tolerant Ethernet (FTE) and the TPS System Status if the options are present.


System Alarms
Location:
View: (all alarms) *
Location Pane
Show All Locations
System Components (782)
EXP001
TSS001 (782)
Consoles (1)
CON01
CON02 (1)
CStn02 (1)
CStn03
CStn03-1
Date & Time
Location
7/23/2004 11:00:00 /System Comp
7/23/2004 11:00:00 /System Comp
7/23/2004 11:00:00 /System Comp
7/23/2004 10:00:00 /System Comp
7/23/2004 10:00:00 /System Comp
7/23/2004 10:00:00 /System Comp
7/23/2004 9:00:00 /System Comp
7/23/2004 9:00:00 /System Comp
7/23/2004 9:00:00 /System Comp
7/23/2004 8:00:00 /System Comp
Invoke System Management, FTE Status, and TPS System Status
System Management
FTE Status
TPS System Status
7/23/2004 0:00:00 /System Comp
7/23/2004 0:00:00 /System Comp
7/23/2004 0:00:00 /System Comp
Unacknowledged alarms: 762 of 770 Acknowledged alarms: 11

# 6. Configuring HCI/OPC Components

## 6.1 Using the HCI Component Configuration Page

### Overview

The HCI Component Configuration page helps you perform the following functions:

- Configure a new HCI/OPC server from an installed base component, where a base component is identified from its ProgID. For example, create TPNServer1 from HCI.TPNServer because HCI.TPNServer is a base component ProgID.
- Re-configure an existing or previously configured HCI server.
- Remove the configuration of an HCI server using the edit combo box.
- Launch a server-specific configuration page.
- Assign an alias name that can be referenced by HCI client applications. (HCI references the alias name through the **Get Component info** method on the HCI Client utility).

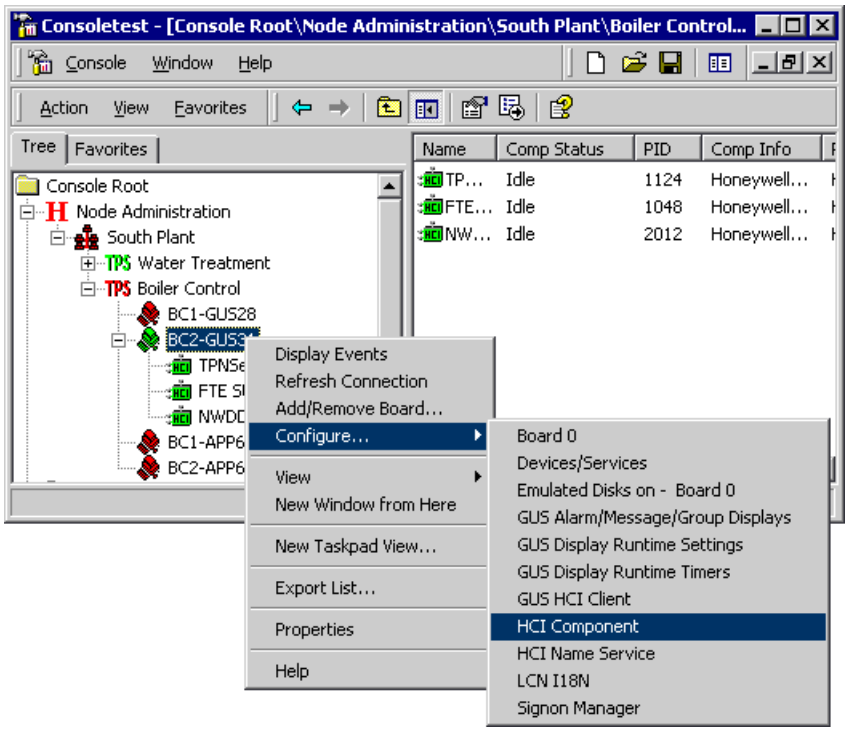
### Key Concepts

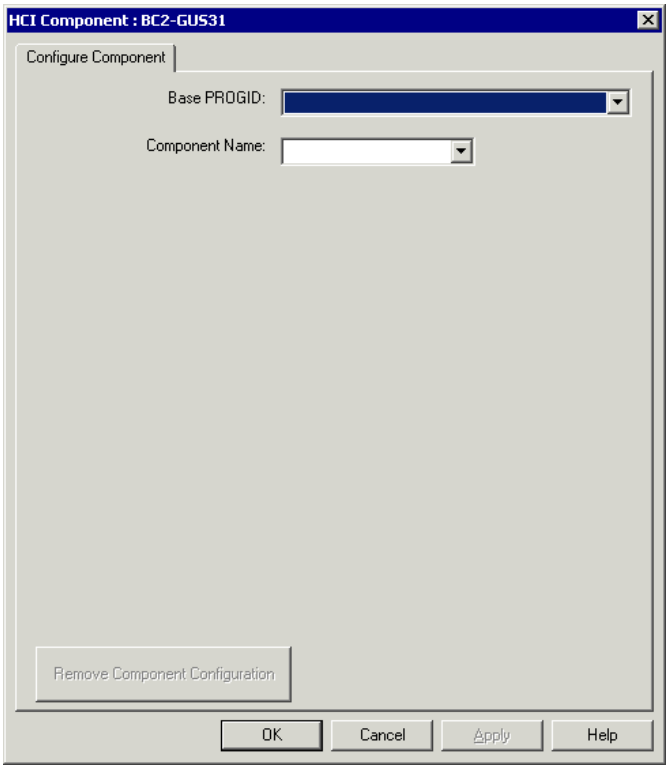
Base HCI Components are self-registration enabled. Each installed base component is identified in the registry with a ProgID under the registry hive HKEY_CLASSES_ROOT. The creation of a new HCI component uses the self-registration information as the starting point of configuration. Since the self-registration information is known to the system as a result of installation, base components must be installed prior to component configuration. Furthermore, installation must occur on each TPS node in the TPS domain, to support client connectivity.

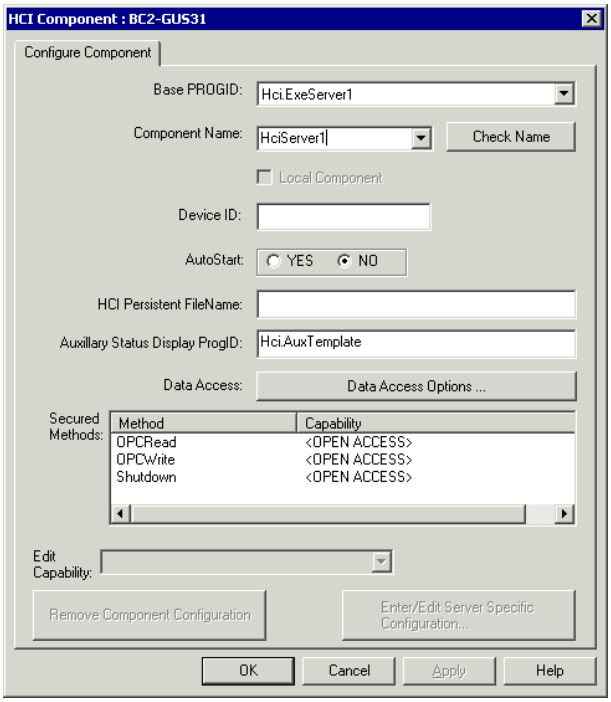
HCI Component Configuration operates within the System Management Display implemented as a Microsoft Management Console (MMC) Snap-in. It has a hierarchical view of computer and managed component status.

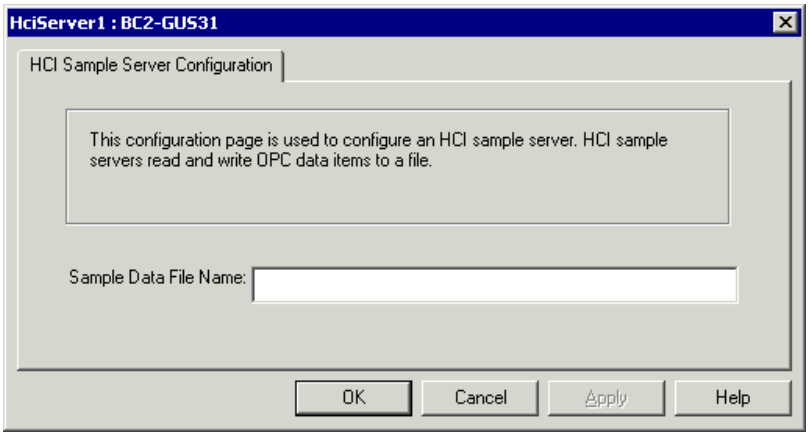
## Procedure for configuring an HCI component

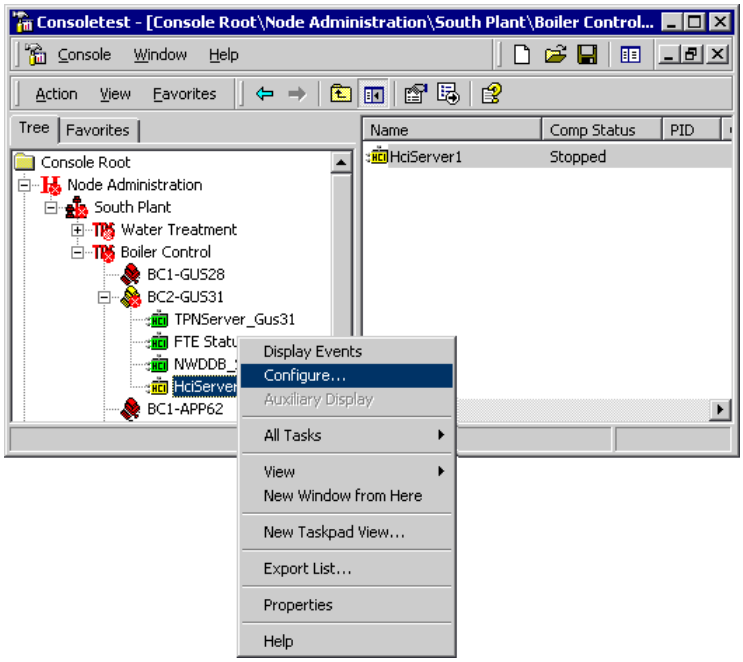
Follow these steps to configure an HCI component.

| Step | Action |
|---|---|
| 1 | From the hierarchy of the System Management Display, right-click the computer item. |
| 2 | Select **Configure** from the context menu. |
| 3 | Select HCI Component from another context menu. |
| 4 | The resulting configuration page appears.  |

| Step | Action |
|---|---|
| **5** | For new configurations, click the down arrow on the combo box of the Base PROGID to get a pull-down list of pre-installed base components. Select one.<br>  <br><br>**Result:** The **Configuration** property sheet appears. |
| **6** | Click the edit combo box of the **Component Name**, and then enter the name.<br>**Result:** The **Check Name** button appears. After verifying the component name, the system enables the **Apply** button. After the system saves the information to the registry, this base component will no longer be displayed in the list of the base PROGID for the next new configuration. |

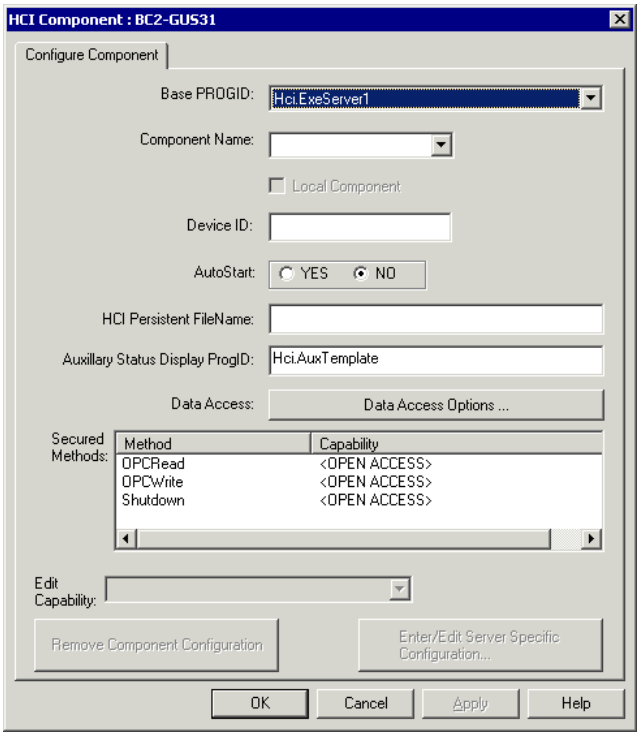
| Step | Action |
|---|---|
| **7** | When you select the PROGID, all fields are updated with the default values from the installation. For example, the **Local Component** check box is grayed out unless this component is a third-party OPC. This box is checked if it is an InProc server or a local component dedicated during the installation.<br>  <br><br>The **Check Name** button is enabled after you enter the component name. If you are configuring a third-party OPC server, you must check the **Local Component** field prior to clicking the **Check Name** button. (**Check Name** must know the component type before verifying its name).<br><br>**Local Component Checked** means the component is a local component that can only be accessed by local host node clients. Local component unchecked means the component is a domain component. You cannot configure a local component unless it is enabled.<br><br>Clients anywhere in the domain can access unchecked components. |

| Step | Action |
|---|---|
| **8** | Invoke a server-specific configuration page by clicking the **Enter/Edit Server Specific Configuration** button. This button is visible when the base component has been defined to have a Device Specific Server configuration and the component name is validated.<br><br>The Device-Specific Server configuration page is shown below.<br><br>  |

| Step | Action |
|---|---|
| **9** | For Device-Specific Server configurations, you can also right-click the HCI component item on the hierarchy of the System Management Display, and select **Configure** from the context menu.<br>  |

### Reconfiguring an HCI component

Follow these steps to re-configure an HCI component.

| Step | Action |
|---|---|
| **1** | Follow steps 1-4 from the previous procedure, "*Procedure for configuring an HCI component*." |
| **2** | Click the down arrow button on the edit combo box of the **Component Name** to get a pull-down list of pre-configured components. HCI/OPC component configuration reads from the registry of the host node.<br>  |
| **3** | Modify the properties of interest. |
| **4** | Click **OK.** All applied updates are written to the registry of the host node. |

### Removing an HCI component

Follow these steps to remove an HCI component.

| Step | Action |
|---|---|
| 1 | Follow steps 1-4 from the earlier procedure, "*Procedure for configuring an HCI component*." |
| 2 | Click the down arrow button on the edit combo box of the **Component Name** to get a pull-down list of pre-configured components. |
| 3 | Click the **Remove Component Configuration** button to remove an HCI component configuration. |

### Using the General Component Configuration Page

The following functions are available from the HCI Component Configuration page:

- Configure a component for the first time (component is automatically added).
- Edit a previously configured component.

All of these functions are handled in the configuration page. Select the **BaseProg ID** combo box to configure a new component, and select the edit combo box to update or remove a pre-configured component. If the type of the base server type, as defined by the BaseProg ID, is OPC, then the user has access to Asynchronous IO Thread Throttling options. If the base server, as defined by the BaseProgID, has a Device-Specific Server configuration page, then the user has access to those pages.

### Configuring a new HCI Server

Step 5 in section 6.1, *Procedure for configuring an HCI component*, shows the component configuration page information that appears when you configure a new HCI Server. Note that only the **Base ProgID** field, **Component Name** field and the **Cancel** button are enabled at this time. Once you select a **Base ProgID** from the pull-down list, then the dialog box is updated to enable applicable fields for the type of server selected.

### New configuration vs. re-configuration

Table 11 below identifies each field or button on the HCI Component page with a description of its initial value and usage.

**Table 11 Descriptions of Fields/Buttons of the HCI Component Page**

| Field/ Button | Description | Initialized Value | Enabled/Visible |
|---|---|---|---|
| **Base ProgID** | Identifies the type of installed HCI component as the Base ProgID, which is listed from HKEY_CLASSES_ROOT | Blank. | Always enabled and visible. |
| **Component Name** | Edit combo box to enter the name of new configurations.<br>For re-configurations, select the component from the list.<br>This field is validated when the **Check Name** button is selected. If the entered value is blank, then the following message is issued: *You must enter the component name before applying.* If the entered value is a duplicate component name, then the following message is issued: *Component name already exists*. | Blank | Always enabled and visible. |
| **Local Component** | Identifies that it is a local or domain component. | This field is checked when it is used only by Local clients. | Always visible and only enabled when the component is a third-party OPC server. |
| **Check Name** | Validates that the component name is unique within the TPS domain. | [Hidden]. | Only visible when text is edited in the **Component Name** edit combo box. |

| Field/ Button | Description | Initialized Value | Enabled/Visible |
|---|---|---|---|
| **AutoStart** | A **Yes** value indicates CAS should start that component when the node starts up.<br><br>This field is valid only for TPS managed components. See for a list of TPS managed components. | For new configurations, set the Yes/No value to the registry value of the installed component that has self-registered. For re-configurations, set to the current value. | Only visible and enabled for domain components. |
| **Device ID** | This field is used by the Redirection Manager (RDM) option. RDM uses this field to identify the device to which a server is connected. HCI components must have the same Device Ids to be used as a Primary/Secondary pair by Redirection Manager, | | Always visible and enabled. This is a mandatory field if the server is participating in a redundancy scheme with Redirection Manager. |
| **HCI Persistent FileName** | HCI checkpoint, which contains OPC items and associated DSS handle. | For new configurations, this field is set to \HWIAC\Checkpoints\<component name>.hci after the component name is entered and validated. For re-configurations, the field is set to the current value. | Only visible and enabled for those servers which enable checkpointing. |

| Field/ Button | Description | Initialized Value | Enabled/Visible |
|---|---|---|---|
| **Auxiliary Status Display ProgID** | Display the ProgID of the ActiveX control for the Auxiliary Status Display. | For a new configuration, the value is set to registry value of installed component if component has self-registered this field. Otherwise, the field is initialized to Hci.AuxTemplate. For re-configurations, the field is set to the current value. | Only visible and enabled for those servers that support Auxiliary status. |
| **Data Access Options…** | Invokes the Data Access Options dialog box. | If the button is not selected, max thread per group is 10; Overloaded Async Action is Throttle, and Time Threshold is 2000 milliseconds (2 seconds). | Only visible for OPC servers. |

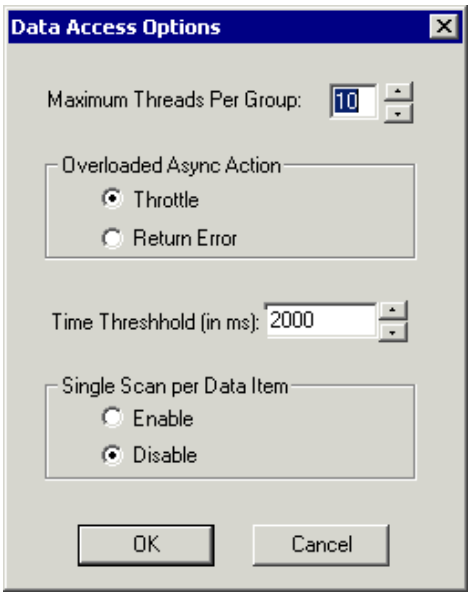
| Field/ Button | Description | Initialized Value | Enabled/Visible |
|---|---|---|---|
| **Secured Methods** | A list of methods that can be associated with a capability. Proxy's files with ACLs represent capabilities.<br><br>*Shutdown/Start method:*<br>The Status Checkpoint Display uses the Shutdown face to control who can initiate a Start. | Methods are listed from minimally set to Shutdown for servers of any type. For OPC servers, OPCRead and OPCWrite are also listed. If DSS has defined additional methods, then those will also be included in the list. | Only visible if the component has secured methods. |
| **Edit Capability** | Combo box to enter capability for a selected Secured Method. Select a method in the Secured Methods list control to enable this combo box. Use the pull-down list to select an existing capability. Enter text in the edit box to create a new capability. | Blank | Only visible if the component has secured methods.<br><br>Enabled if a method in the combo box is selected. |
| **Create Capability** | Confirmable operation, which creates a capability file on the security path of the host node. | | Only visible if the component has secured methods and the user enters text in the edit box portion of the **Edit Capability** combo box. |
| **Set Security** | This button is overlapped with the **Create Capability** button to Invoke the property of the capability file in order to change it. | | Only visible if the component has secured methods and the capability file exists. |

| Field/ Button | Description | Initialized Value | Enabled/Visible |
|---|---|---|---|
| **Remove Component Configuration** | Removes the entire component configuration from the registry of the computer selected, and from HCI Name Service.<br><br>Prior to removal, the system prompts you to confirm the operation. If confirmed, the system displays a warning reminding you to shutdown the component. | | Only enabled on re-configuration or after a new configuration has been applied. |
| **Enter/Edit Server Specific Configuration** | Writes the current values to the selected computer. Prior to the write, the system requests the user to confirm the operation.<br><br>If the DSS has not been configured, then invoke the DSS page. If the DSS has been configured, prompt the user for DSS configuration. | | Only visible for servers that have defined a DSS Configuration page. Enabled when user has entered a valid component name and BaseProgID combination |
| **OK** | Applies if there are outstanding changes, then exits from the HCI Component property sheet. | | Always visible. Enabled when a user enters a valid component name and BaseProgID combination If the **DSS Configuration** page is defined, this value is enabled after user performs DSS configuration. |

| Field/ Button | Description | Initialized Value | Enabled/Visible |
|---|---|---|---|
| **Apply** | Writes the current values to the selected computer. Prior to the write, user is asked to confirm the operation. | | Only visible if base server has no DSS configuration page defined. Enabled when user has entered a valid component name and BaseProgID combination. |
| **Cancel** | Cancel this configuration and exit from the HCI Component configuration page | | Cancel is always visible and enabled. However, once "apply" has occurred, registry updates can't be cancelled. |
| **Help** | On-line help | | Always visible and enabled. |

### Data Access Options

**Figure 16 Data Access Configuration Page**




OPC Servers may set several I/O options via the **Data Access Options** button on the component configuration page. There are four modifiable data access options, as shown in Figure 16:

1. **The Maximum Threads Per Group** option defines the number of outstanding asynchronous threads per group. Use this setting to prevent any one OPC group from using all system resources. Use the up/down arrows to adjust the maximum number of threads per group.
2. **Overloaded Async Action** refers to the desired action when the maximum number of threads is exhausted. Select **Throttle** to wait until a thread completes before processing the max+1 asynchronous thread. Select **Return Error** to receive an error condition from the asynchronous call.
3. The **Time Threshold** option allows you to configure the amount of time to wait before a background device read is performed. It is the amount of time (in milliseconds) that will pass after the items are set to active. The valid range of entry is 500 – 10000 milliseconds. If the polling thread has not made an update within the specified time period, then a background device read is issued.

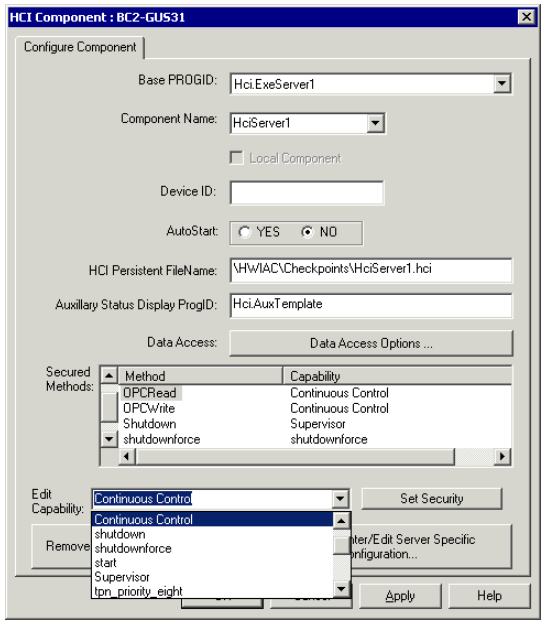
4. The **Single Scan Per Data** option, when disabled, allows a client to get fresh data within the requested update rate, providing the server does not get overloaded with requests. (A server is considered to be overloaded if the total number of items being collected by all clients exceeds 800 per second).

   With this option disabled, active groups function independently of one another. When each update rate expires within a group, the server requests data from the system and reports the data back to the client.

## Secured Methods

If the base server has secured methods, then the **Component Configuration** page displays a **Secured Methods** list control box with an **Edit Capability** pull-down list. To update the capability (for example, the proxy file) associated with a secured method, select the desired Method in the **Secured Methods** list control box (as shown in Figure 17) to display the pull-down list of capabilities that currently exist on the host node.

**Figure 17 Listing of Secured Methods and Capabilities**



### Defining Capabilities

Defining and maintaining capabilities for controlling access to TPS objects is a major task for TPS system administrators. Successful completion of this task strongly affects the ease or difficulty of maintaining an effective security system over time. Once a capability architecture is defined, the capabilities must be put in place, and then configured.

**ATTENTION**

Capability names should be limited to using upper- and lower-case letters, numbers, and the following special characters " (space), "$", "_" (underscore), "-" (dash), "+" (plus), "." (period), and ":" (colon). There is no validation of capability names in TPS beyond that performed by the NTFS file system where the capability proxy files reside.

Names will fail if they include "\" (backslash), and "/" (forward slash), as these are filename delimiters.

**ATTENTION**

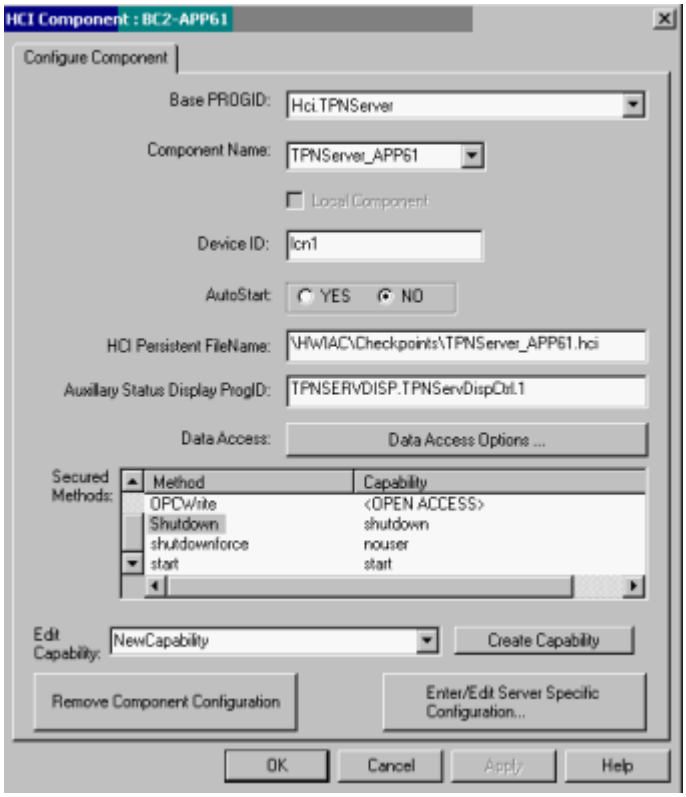
HCI method security is configured on a component basis. The **workstation security package** installs a default set of proxy files on the host node. This default set of proxy files is created based on roles of users and applications and they are implemented using local groups.

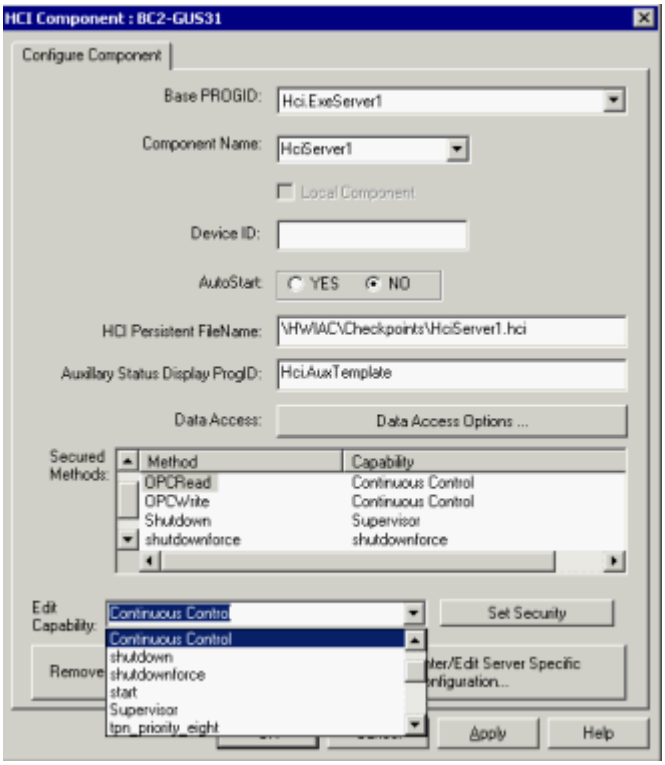
Click the **Set Security** button to invoke the property of the proxy file and modify the default security settings.

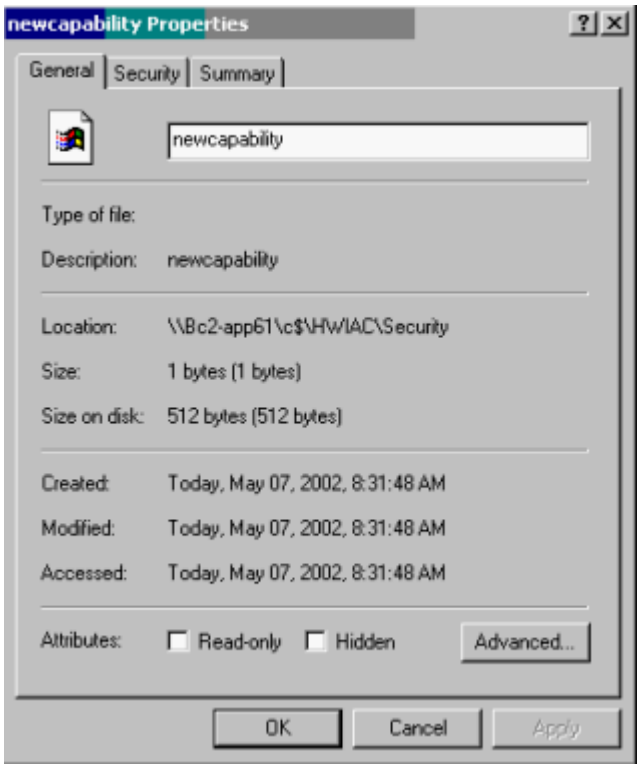
To initiate Windows group administration, open a Group Policy from **Active Directory Users and Computers** from the domain controller. For more information about MS Windows security, refer to the *TPS System Administration Guide* or the *Experion Network and Security Planning Guide.*

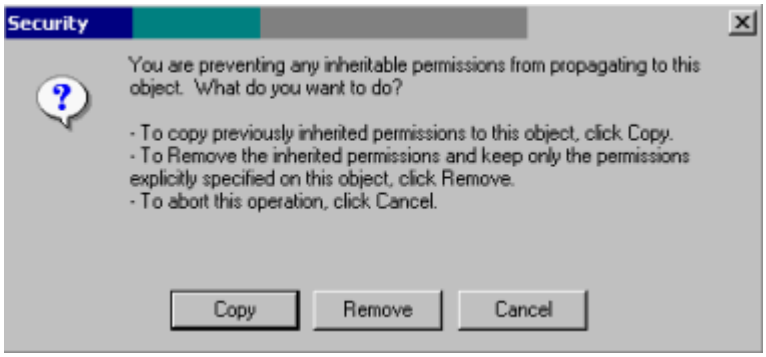
### Procedure to create and modify a capability for an HCI Component

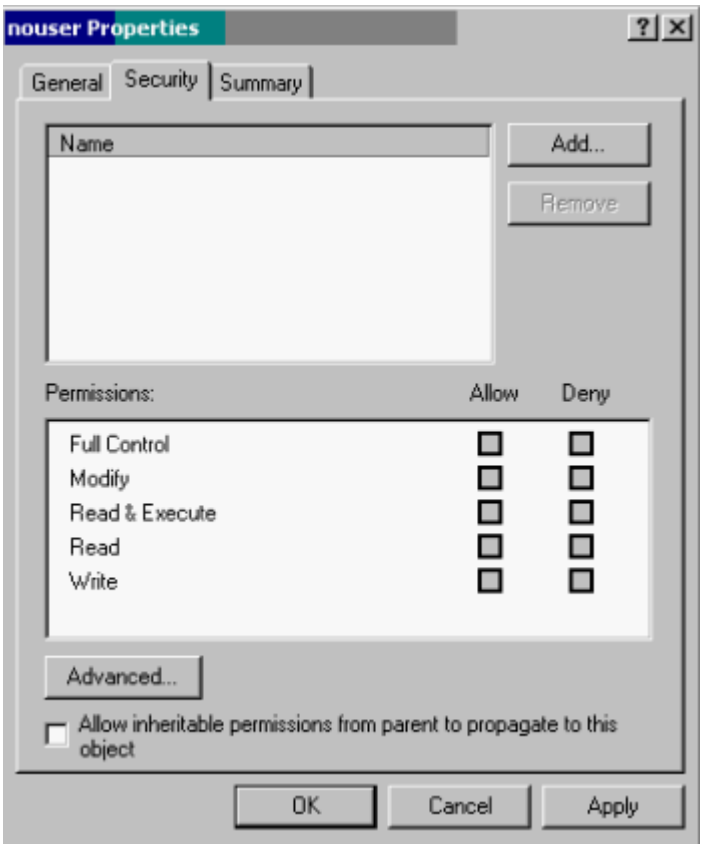
Follow the steps below to create and modify a capability for an HCI component.

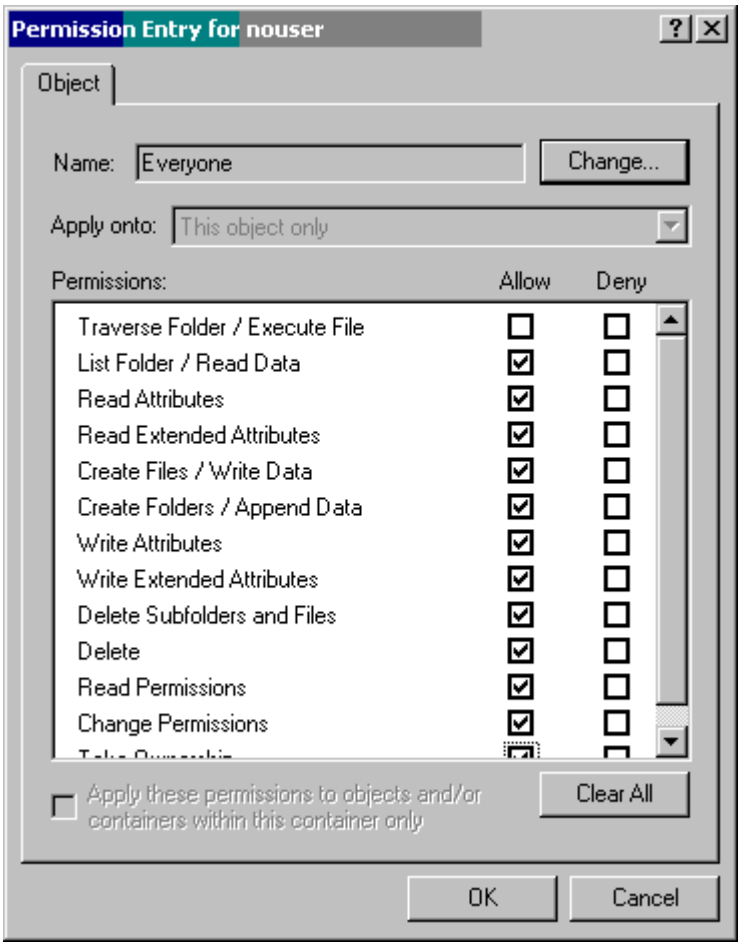
| Step | Action |
|---|---|
| 1 | To create a new capability, select a method in the **Secured Methods** box. Type the name of the capability in the **Edit Capability** combo box. This enables the **Create Capability** button.<br>  <br><br>Click the **Create Capability** button to create the capability file on the host node. You must select an item inside the **Secured Methods** list box to enable the pull-down list of the **Edit Capability** combo box, as shown in the previous figure. |
| 2 | When a confirmation dialog appears, click **Yes** and then **OK** at the next screen. to confirm your selection. |

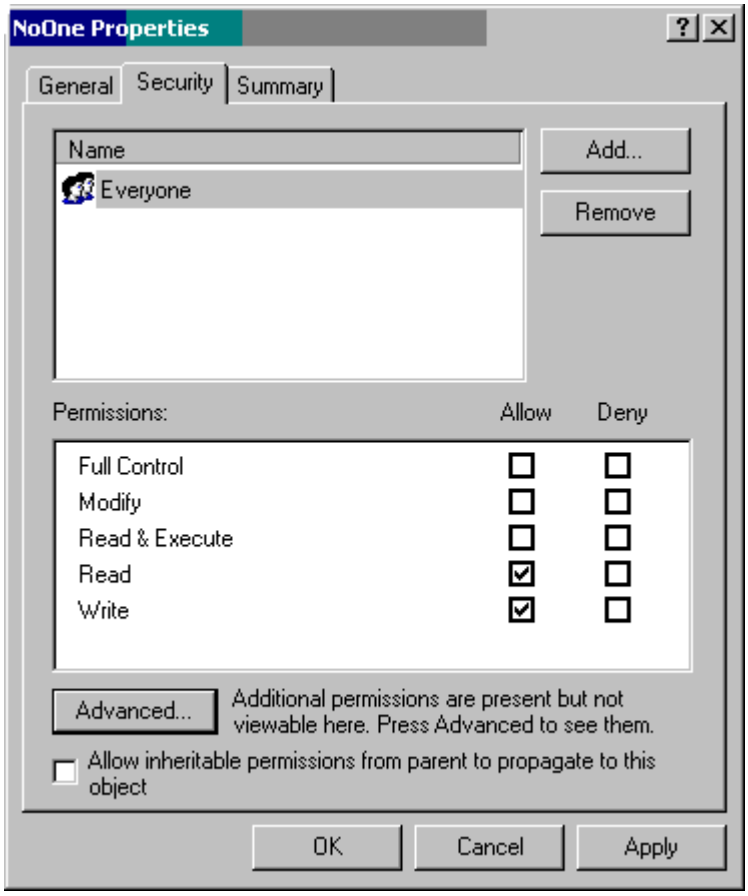
| Step | Action |
|---|---|
| **3** | To modify the capability, select the desired method and capability file displayed in the **Edit Capability** combo box if it is not <OPEN ACCESS>. This enables the **Set Security** button.<br>  |

| Step | Action |
|---|---|
| **4** | Click the **Set Security** button to invoke the property of the capability file that sets security permissions for the new capability. The capability file **Properties** window appears.<br>  |
| **5** | Select the **Security** tab. |

| Step | Action |
|---|---|
| **6** | Uncheck the **Allow inheritable permissions from parent to propagate to this object** check box. The following screen appears:<br>  <br><br>If you want to set a new security account, click the **Remove** button.<br>If you want to work from the permissions provided by the parent, click the **Copy** button. |

| Step | Action |
|---|---|
| **7** | The **Properties** window for the new account appears:<br>  <br>Click the **Advanced** button. The **Access Control Settings** window appears. |
| **8** | Click the **Add** button. |
| **9** | You'll see the **Select User Computer or Group** window.<br>Browse the list box for the name of the user or group to which you want to assign capabilities. Select the domain from the **Look In** pull-down menu. Click **OK**. |

| Step | Action |
|---|---|
| **10** | You'll see the **Permission Entry** for user window.<br>  <br>**Note:** If the **Allow** box for the **Traverse Folder/Execute File** capability is unchecked, then the user has no capability. |

| Step | Action |
|---|---|
| **11** | Click **OK** to apply the change(s). **The Access Control Settings** for new capability window appears. Click **OK** again. The **Properties** page appears.<br><br>Click **OK.**<br><br>  |

**ATTENTION**

Removal of a component does not remove capability files.

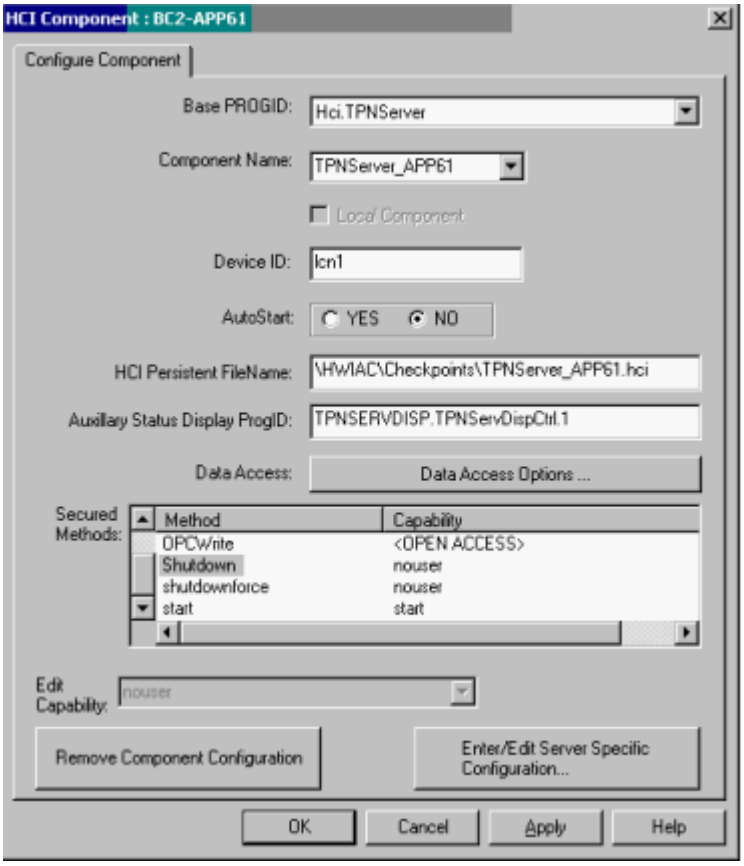
The capability field can be set to blank.

A secured method with no defined capability is interpreted at runtime to mean that all users have access to the method.

If the system detects undefined (or blank) capability names associated with one or more secured methods, the Configuration page issues a warning during any write operation that secured method(s) have open access.

### Procedure for disabling shutdown of a component

| Step | Action |
|---|---|
| 1 | To totally disable shutdown, make sure you set the same policy for the shutdown and shutdown force from the **Secured Methods** list box. |



### Procedure for configuring a device-specific server

A Device Specific Server developer may optionally provide a configuration page. Follow the steps below to configure a device-specific server.

| Step | Action |
|---|---|
| **1** | If a configuration page has been defined, it displays the **Enter/Edit with Server Specific Configuration…** button, and hides the **Apply** button.<br><br>If you select the **Enter/Edit with Server Specific Configuration…** button, the system writes to the registry, and then configures the Device-Specific Server (DSS). |
| **2** | HCI component configuration is not considered complete unless you click the **Apply** button, which invokes successful completion of the DSS configuration (unless you **Cancel** the configuration).<br>The system disables the **OK** button until at least one Device-Specific Server configuration has successfully completed. |

### Procedure for applying a configuration

Applying the component configuration means writing the entered values to the Windows registry of the selected computer.

| Step | Action |
|---|---|
| **1** | From the **Component Configuration** page, click the **OK**, **Apply** or **Enter/Edit with Server Specific Configuration** button.<br><br>These buttons are enabled if you entered a valid component name and BaseProgID/hostname combination. If valid values for these fields are not entered, the only other choice is to **Cancel** the configuration. |
| **2** | The system prompts you to confirm. If you select **NO**, the write does not occur. Otherwise, the registry is updated. Note that once the operation completes, it cannot be undone via the **Cancel** button. It can, however, be undone via the **Remove Component Configuration** button. |

### Procedure for removing a component's configuration

Follow these steps to delete a component's registry entries from the Windows registry.

| Step | Action |
|---|---|
| **1** | Click the **Remove Component Configuration** button to delete the registry entries from the **Windows** registry, from the node where the server is installed. This operation does not execute if the component is running.<br><br>Renaming the component is the same as deleting the existing component and adding a new component. The system displays a warning that it may be necessary to shutdown the component prior to removing a component configuration. |
| **2** | The local component can be removed by clicking the **Remove Component Configuration** button. The system displays the following confirmation message:<br>"*This operation will remove all local component configurations from the registry and repository on all nodes within the same TPS domain. If you want to remove it from the local node, please uninstall it from the node instead of deletion. Do you want to continue*?" |

# 6.2 Configuring HCI/OPC Component Security

### About this section

This section includes information for HCI server developers and end users pertaining to the setup and maintenance of a reasonably secure application environment.

### Changing Server Identity

Typically, HCI servers should be assigned an identity (user id and password) at install time. This may be done in one of two ways:

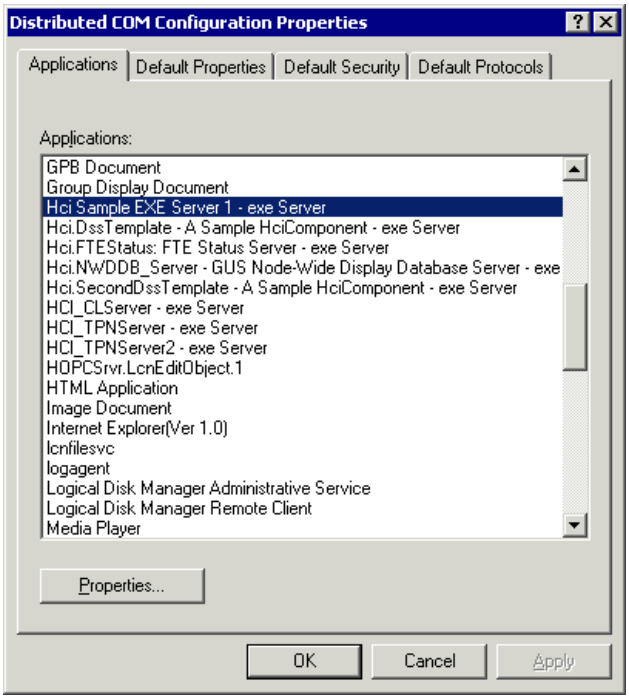
1. *Automatically* using a predefined user ID (such as TPSComServer). This approach is recommended.

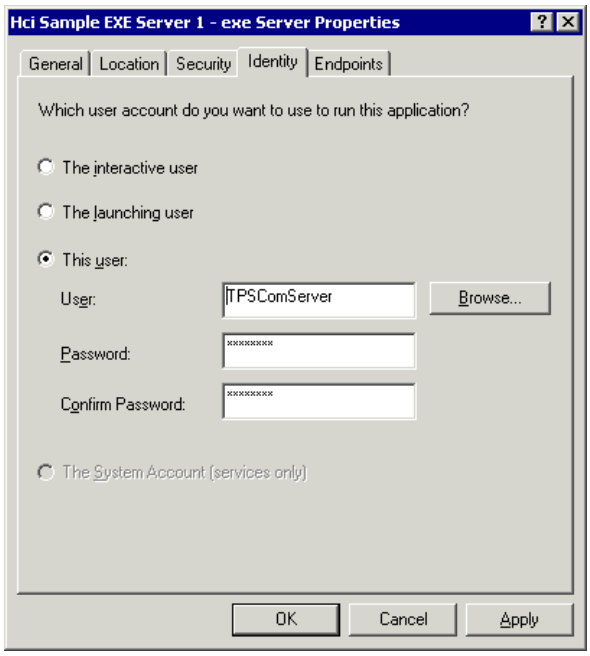
2. *Via a dialog* box that requests the installer to enter a user id for the server.

With both approaches, there are cases where a system administrator may need to change the identity of a server. This procedure must be user-documented. Presumably a single description could work for all servers, with a reference to that description and any server-specific notes (including the specific ProgID) supplied in the server documentation.

Note that in a control environment, an HCI component must run as a specific user rather than an Interactive or Launching user. If a user is not logged in, or if a user logs out while a component is set to Interactive, then the component process terminates. Likewise, the Launching user option prevents clients, which run under different accounts, from connecting to the same server process.

### Procedure for assigning a user id and password

| Step | Action |
|---|---|
| 1 | Type “dcomcnfg” in the **Run** dialog box, and click **OK**. |
| 2 | When dcomcnfg starts, select the ProgID of the server in question, and click **Properties**.  |

| Step | Action |
|---|---|
| **3** | Select the **Identity** tab to assign User Ids.<br>  <br><br>To assign a specific user ID: Select the **This user** radio button, and then type (or browse) the name and password to use into the appropriate fields. This user ID and password will be validated immediately, so the ID must already exist.<br>Click **OK**. |
| **4** | Close dcomcnfg. |

### Launch, Access and Configuration permissions

The installation of a server sets reasonable defaults for both Launch and Access permissions to the server. Configuration permissions for HCI components should be set to allow access only to local and TPS administrators, and Local System administrators. Administrators may need to change these settings on some servers, according to their own documented procedures.

**ATTENTION**

When setting access permissions, the default access list in dcomcnfg is normally empty. This is interpreted by DCOM as No Access. If one or more specific users or groups are inserted in the list for custom access security in dcomcnfg, ensure that SYSTEM, LocalServers, and the Administrators group are added as well, or the COM object will fail.

### Procedure for setting permissions

Follow these steps to set permissions.

| Step | Action |
|---|---|
| **1** | Select **Start>Run.** |
| **2** | Type *dcomcnfg* in the **Run** dialog box, and click **OK**. |
| **3** | When dcomcnfg starts, select the ProgID of the server in question, and click **Properties.** |
| **4** | Select the **Security** tab. |
| **5** | Set the radio button to **Custom permissions**. |
| **6** | Click the **Launch** (or **Access**) **Edit** button. |
| **7** | Add, remove, or modify access rights. |
| **8** | Click **OK** to close the edit window. |
| **9** | Click **OK** to complete the component update. |
| **10** | Close dcomcnfg. |

# 7. Supporting System Event Server

## 7.1 Role of the System Event Server

### About System Performance Server

The System Event Server (SES) is an Experion system component that issues Windows events as OPC alarms or events to subscribing OPC clients. An example of a subscribing client provided with Experion is the Alarm Summary Display. The Experion Alarm and Event subsystem is integrated with the System Event Server such that system related alarms or events can be viewed from the Alarm Summary display. The features of the alarm summary display that apply to process alarms and messages can now be utilized with Windows system events. For example, the operator can acknowledge a system alarm from the Alarm Summary display in the same manner that a process alarm is acknowledged.

**REFERENCE - INTERNAL**

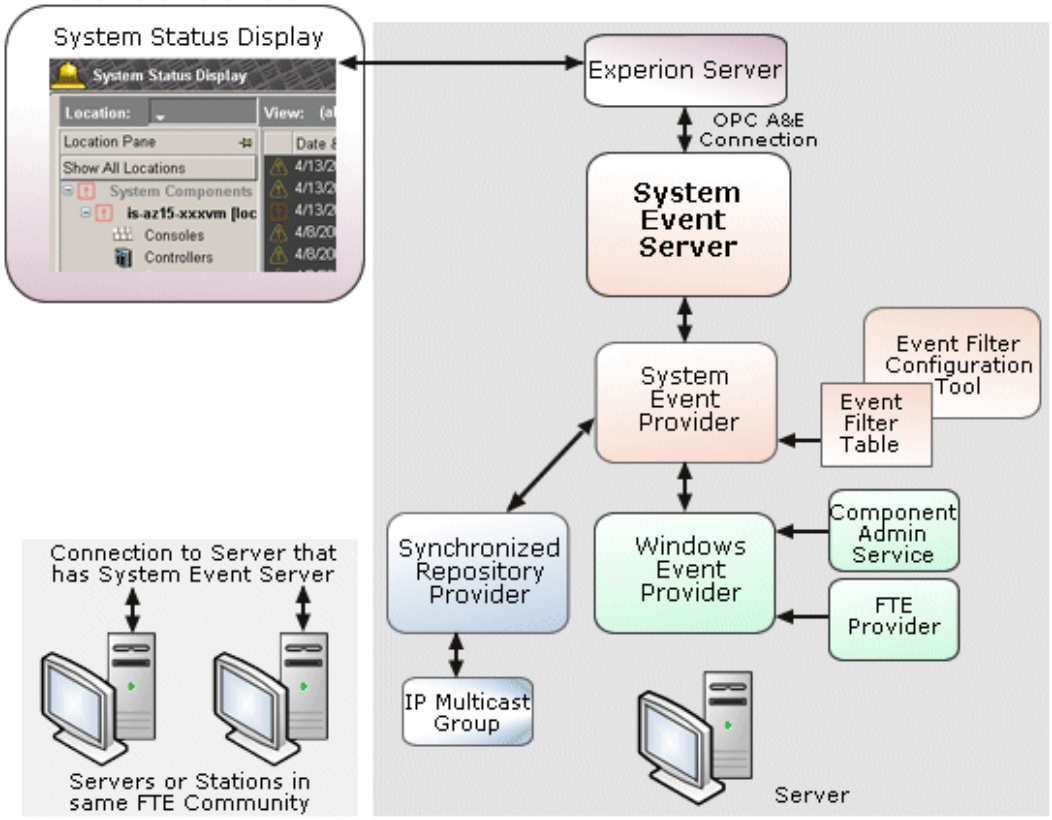
Refer to the Experion Operators Guide for procedures on how to operate the Experion Alarm Summary Display.

**REFERENCE - INTERNAL**

The System Event Server is an HCI Managed Component. Refer to the System Management Operations Guide for procedures on how to monitor the status of the System Event Server.

### System Performance Server architecture

The System Event Server interfaces with the System Event Provider through WMI as a WMI client. The System Event Provider, which is part of the existing System Management event subsystem, maintains a synchronized list of Windows Events produced from set of nodes within a scope definable by a user. A filter file resident on each node determines which Windows Events are placed into the synchronized list. The System Event Provider provides event notification to System Event Server (SES) for event creation, deletion and modifications. Therefore SES serves primarily to convert Windows events into OPC event notifications.




System components, such as FTE Provider and the Component Admin Service send events to the standard Windows Event logs. Each managed node will have a filter table generated using an MMC based tool. The filter table contains a list of Windows events, which identifies Windows event, log entries to capture and expose to the System management infrastructure via WMI. The filter table allows the customer to identify the event and indicate the type of event to pass on to the System Event Server (e.g., Simple, Tracking, Condition). The filter table is constructed by using a configuration tool that easily allows the user to select individual Windows events by event source. An example of this capability is a customer who would like an OPC event generated when a node reports, via the Windows event log, that the disk is nearly full. If the customer has identified Windows disk subsystem event log messages as “interesting” via the filter table, disk errors such as disk full will be identified and forwarded to the System Management infrastructure such that the System Event Server can capture and expose as an OPC alarm and event.

**REFERENCE - INTERNAL**

Refer to the section Event Filtering Configuration Procedures in this document for procedures on how to configure an event filter file.

**ATTENTION**

The network environment requires the use of multicast communication between all nodes.

## 7.2 Getting Started with System Event Server

### Installation guidelines

The following checklist identifies several key planning considerations and references when implementing SES in an Experion system.

| ☑ | Planning Consideration |
|---|---|
| | If your system is not currently using the System Management Event subsystem (i.e. System Event Provider, Event Filter Table, Event Summary window on the System Management Display) then you should become familiar with the information in this document related to multicast communications and synchronized repository scope. Refer to sections 5.4, 5.7, 5.8, 5.9, and 5.10 in this document.<br><br>If your system is currently using the System Management Event subsystem, then skip this planning item. |
| | Determine where to install the System Event Server. The System Event Server is installed on Experion Server or LCN-connected Server nodes only. If you have redundant servers, then you can install SES on both nodes. |
| | Upgrade System Management Runtime on all nodes. |
| | It is recommended that you install System Management software including SES after installing the Experion server software. Be sure the Experion Server is stopped before installing the System Management software including SES. |
| | When a System Event Server is used, the time should be synchronized between all nodes in a cluster that the System Event Server is monitoring (including Flex Stations). |
| | There should be only one System Event Server per FTE community. If FTE is not implemented then there should be only one System Event Server per Experion System as long as the Experion system in contained within a routable multicast scope. The System Event Server is installed on an Experion Server. If the Experion Server is configured as redundant then the System Event Server is installed on both. (Note: Not following this guideline will result in duplicate System Events in the Experion Alarm list) |
| | The System Event Server is not installed in a TPS only system. |

# 7.3 Installing and Configuring System Event Server

### Procedure for installing SES in a pre-R300 Experion system

The System Event Server is a licensed package.

**ATTENTION**

R210 and earlier Experion users should follow these steps to install System Event Server. R300 Experion users do not use these steps as the System Event Server can be installed as part of the Experion installation.

| Step | Action |
|---|---|
| 1 | Install the Microsoft Service Pack and Microsoft hot fixes, available on the Honeywell Common Components CD. Then, reboot the node. |
| 2 | Select Licensed Package Installer from the Common Components CD, as shown here. |
| 3 | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click Next to continue. |
| 4 | Enter license and authorization numbers. Click Next to continue. |
| 5 | Click **System Event Server**. (Note: If System Event Server does not appear in the list, verify that the licensing and authorization numbers are appropriate for this package). |
| 6 | Click **Install Package.** |
| 7 | Verify that these are the components you wish to install. Click **OK**.<br><br>**Result:** The installation process occurs, which usually takes a few minutes. |
| 8 | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |
| 9 | Reboot your node. |

### Procedure for installing System Event Server in R300 Experion system

**ATTENTION**

R300 Experion users may not need to perform these steps on an Experion Server, as System Event Server can be installed during R300 Experion node installation using the Application DVD. R300 Experion users only need to perform this procedure if there is a need to add System Event Server to an Experion Server. Alternatively, you can also install optional software using the Node Definition Tool; see its related guide for more information.

| Step | Action |
|---|---|
| 1 | Insert the Experion Application DVD, click “Browse DVD contents”, and launch the Honeywell software Installation application at <drive letter>:\Packages\Install.exe |
| 2 | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| 3 | Click System Event Server**.** |
| 4 | Click Install Package. |
| 5 | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |
| 6 | Reboot your node. |

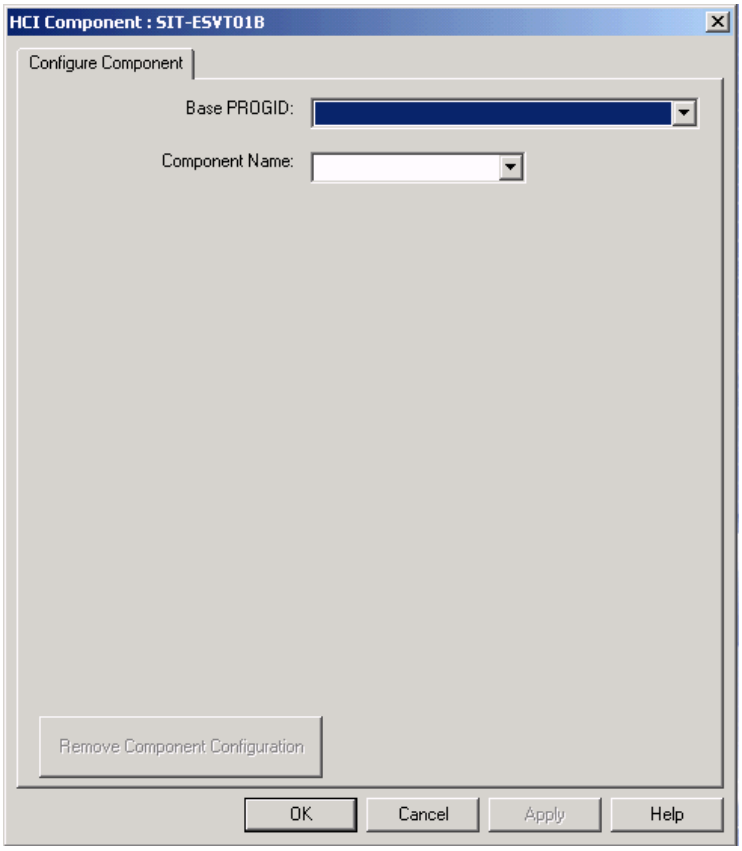
### Procedure for configuring System Event Server

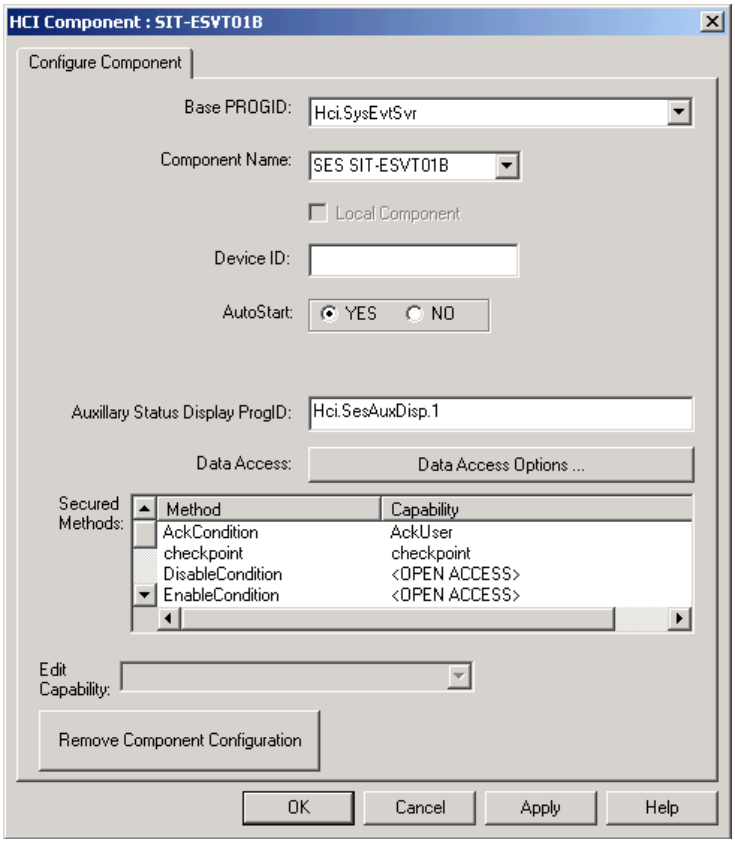
The Experion Server is integrated with the System Event Server such that user configuration is not required. When the Experion Server starts, it connects to the System Event Server using a set of pre-configured properties.

**ATTENTION**

When configuring SES Server component, do not change any property values except for method security. The method security should only be changed if the pre-configured settings do not meet your needs. Using the pre-configured settings for all fields except possibly the method security enables the System Event Server to work properly with the Experion Server.

Follow these steps to view the default settings of the System Event Server or to adjust its security settings.

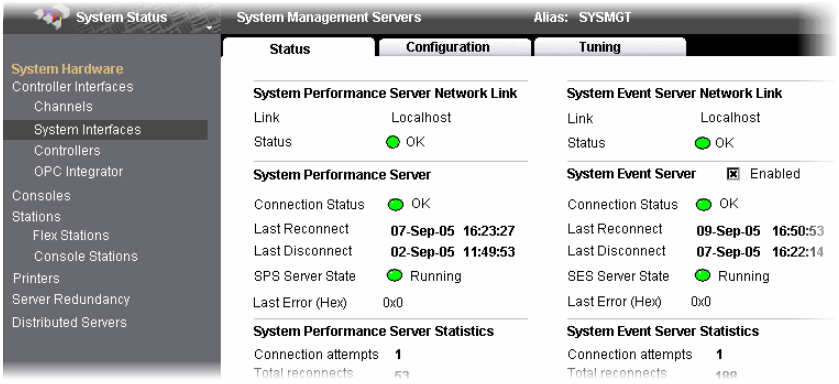
| Step | Action |
|---|---|
| **1** | From the hierarchy of the System Management Display, right-click the computer item. (See section 6.1of this document for detailed instructions.) |
| **2** | Select **Configure** from the context menu. |
| **3** | Select HCI Component from another context menu. The resulting configuration page appears.   |

| Step | Action |
|---|---|
| **4** | Click the down arrow button on the edit combo box of the **Component Name** to get a pull-down list of pre-configured components. HCI/OPC component configuration reads from the registry of the host node. Select the component named **SES** <machine name where SES is installed>. In this example, the component is named **SES SIT-ESVT01B**.<br>  |
| **5** | Use the procedure described in section 6.1, Secured Methods, to adjust the secured access to AckCondition, DisableCondition or EnableCondition. |
| **6** | Click **OK.** All applied updates are written to the registry of the host node. |

# 7.4 Verifying SES is Operational

### Procedure for verifying SES is Operational

Verify that SES is operational on an Experion Server or LCN-connected Server node.

| Step | Action |
|---|---|
| 1 | Start the Experion Server and Experion Station. |
| 2 | From the station menu bar, **select View->System Status->System Management Servers**. The resulting status display appears.   |
| 3 | Verify that the System Event Server Network Link is **OK** and that System Event Server is **Enabled**. Refer to the section “Configuring system performance and event monitoring” in the *Server and Client Configuration Guide* (see the subsection “Setting up system performance and event monitoring”). Refer to the section “Monitoring System Status“in the *Experion Operators Guide* (see the subsection “Monitoring System Management Servers” ). |
| 4 | Invoke the System Alarm Summary display to view system alarms. To see simple and tracking events, invoke the Event Summary display. This can be accomplished from the Experion station menu bar by clicking **View->Events->Event Summary**. |

## 7.5 Troubleshooting SES Configuration

The following table describes symptoms of possible problems you might encounter when configuring your System Event Server, and recommended solutions to these problems.

| Symptom | Solution |
|---|---|
| System Management Servers Status indicates that the SES is not OK and not Enabled (black lights rather than green lights). | The System Event Server is installed to run as a predefined account name with predefined password. If the password for this account is changed, then connection to SES will fail. In order to synchronize passwords with accounts, a tool is available that allows the user to change the account and password on all Windows services or DCOM servers running as an account.<br><br>This tool can be accessed from Start>Programs>Honeywell Experion >System Management>Windows Services & DCOM Servers Logon tool<br><br>Follow the instructions provided on the tool. Note that this tool does not change the password on the account.<br><br>Once the tool successfully completes, start the System Event Server from the System Management Display. |

# 8. Configuring Event Filtering

## 8.1 Role of Event Filtering

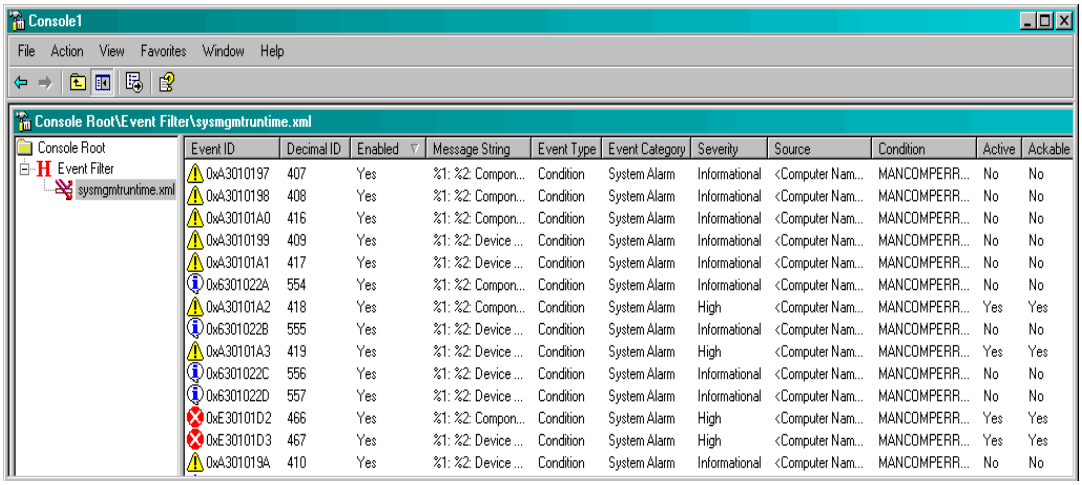
### About Event Filtering

Event Filtering defines a subset of Windows events that will be augmented and exposed as OPC events. These events are then available to users of process control displays. System events can be generated by the **Windows** system, Honeywell applications, or third-party applications. OPC events require more information than can be obtained in Event Viewer logs, such as event category and event source. Using the Event Filtering tool, a table of events is configured that identifies the additional OPC event properties required to translate the Windows event into an OPC compliant event.

### Example of Event Filtering Table

Figure 18 shows an example Filter Table. The filter table is an XML file accessed from the Honeywell Event Filter Snap-in.

**Figure 18 Example Event Filtering Table**



### How Event Filtering works

When you create a filter table, it lets the System Event Provider perform the following tasks:

- Determine if the event should be processed or ignored
- Augment filtered events with OPC Event properties
- Determine whether the event should be included only in the local event list

Subscribing event clients, such as the System Management Display or System Event Server, then detect the new event and add it in their event lists.

Filtered events are synchronized among all nodes within the System Event Provider scope.

If no filter files exist, the System Event Provider will process no events. As a result, subscribing clients will not receive any events.

**TIP**

System Event Provider only reads its filter tables from the \HWIAC\Filter directory. Therefore, all configured filter tables need to be saved in this directory.

# 8.2 Event Filtering Configuration Procedures

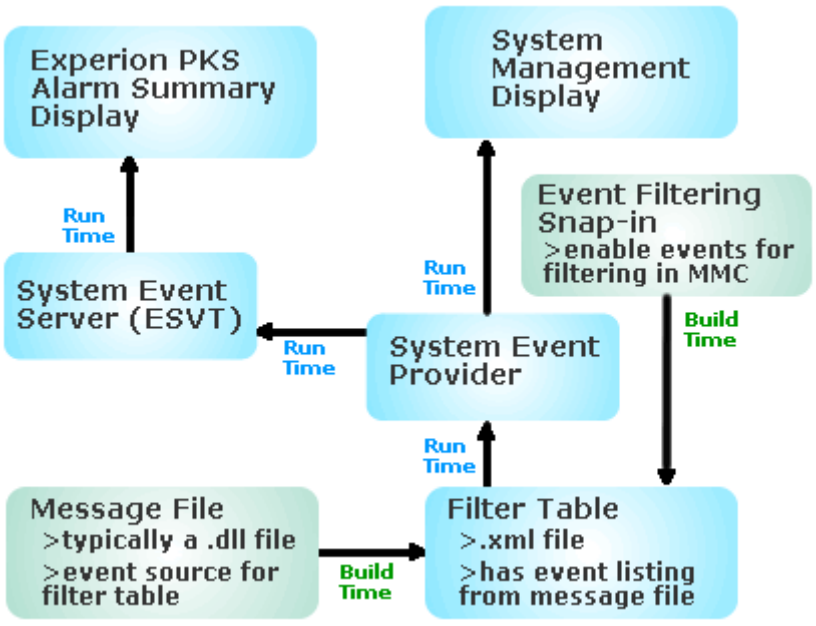
### Configuration concepts

When you configure an event filter table using the Event Filtering snap-in, you reference a message file for the event source at build time. The events within this message file are listed in an .xml filter table. Each event can be configured to be enabled for filtering. At run time, the System Event Provider processes and distributes only enabled events to the System Management Display's Event Summary or the System Event Server.

### Event filtering configuration prerequisites

- You must add the Event Filter Snap-In to the MMC console.
- You must have necessary access privileges to configure event filtering.

**Figure 19 Creating a filter table**

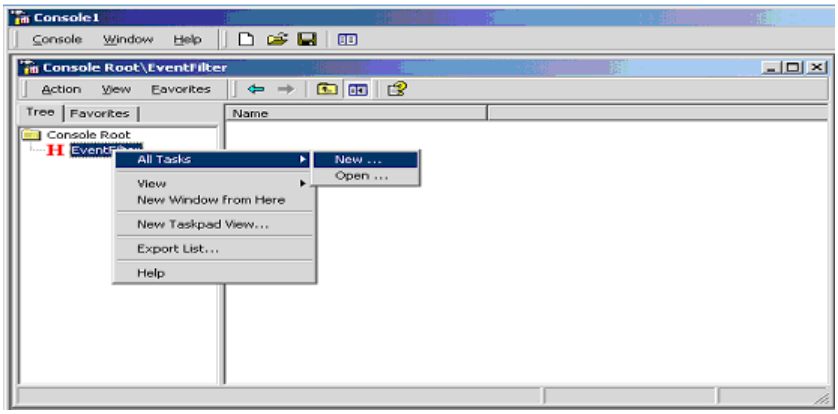


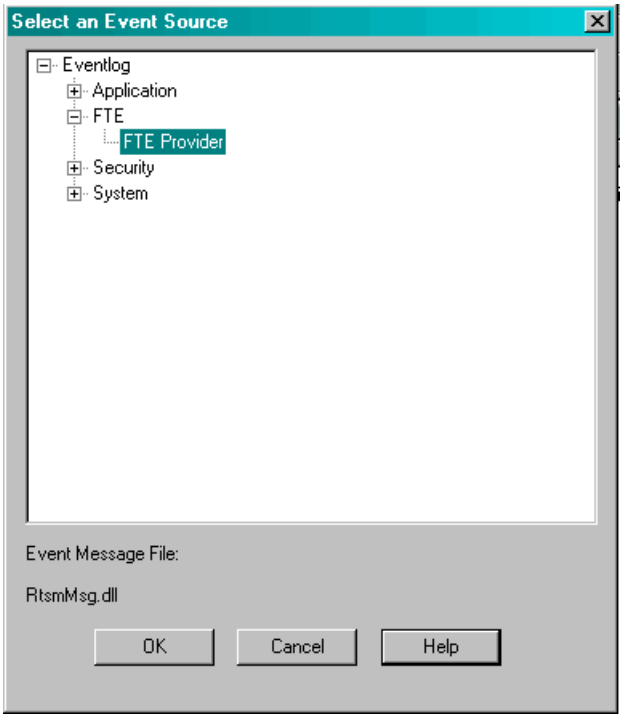
### Procedure for creating a Filter Table

**ATTENTION**

The Honeywell supplied filter file is the base set of filtered events. Create your own filter file to supplement the set of filtered events supplied by Honeywell. Do not edit the Honeywell filter file.

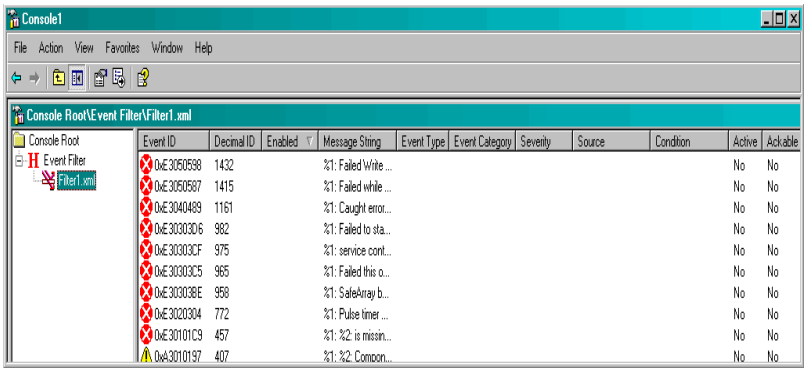
Follow these procedures to create a Filter Table.

| Step | Action |
|---|---|
| 1 | To create an event filter table, right-click the Event Filter Tool and select **All Tasks>New.**<br>  <br><br>**Result:** A dialog box appears listing the available event sources. |

| Step | Action |
|---|---|
| **2** | From the dialog box, select the event source of interest. In this example, FTE provider is the selected event source.<br>  <br><br>**Result:** The Event source is highlighted and the message file is identified that contains a listing of events for the event source.<br>For example: **RtsmMsg.dll** contains the event listing for FTE Provider. |

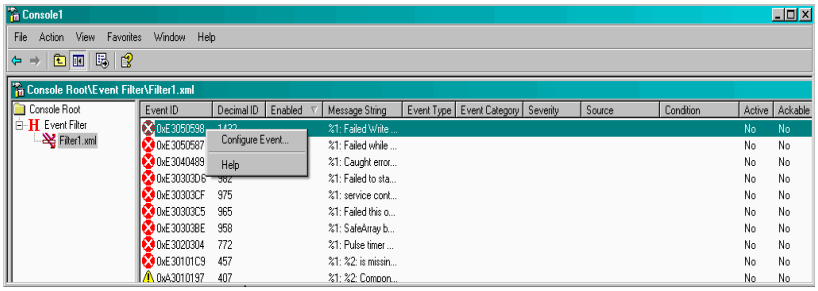
**ATTENTION**

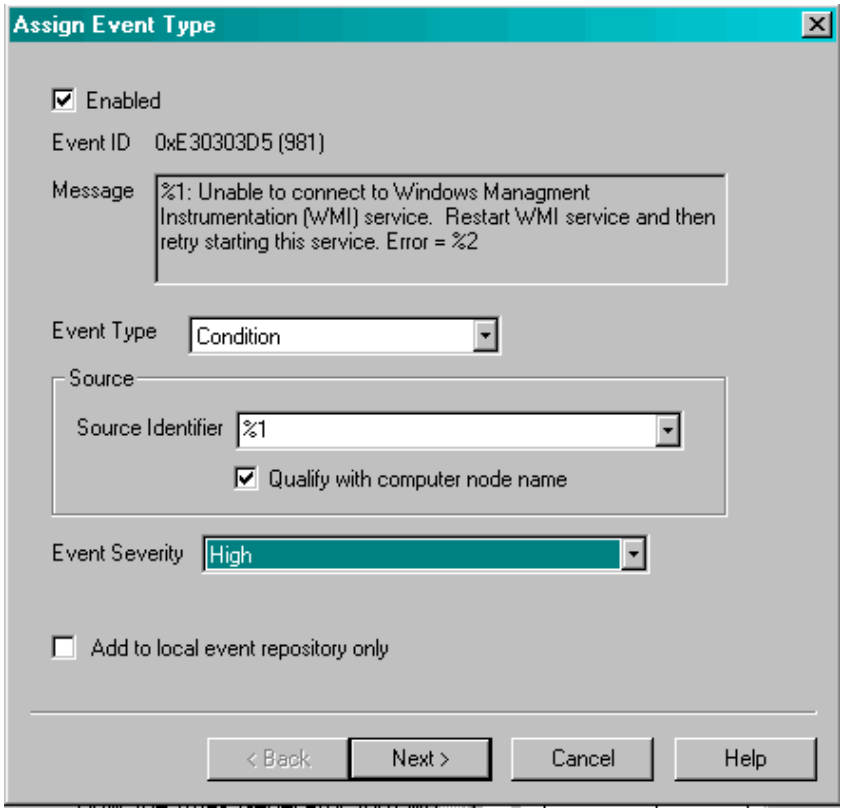
An Event source can be contained in more than one filter table. However, if an event ID is contained in more than one filter table the system event provider ignores the second duplicate Event. For this reason, it is recommended that an Event ID be contained in only one filter table.

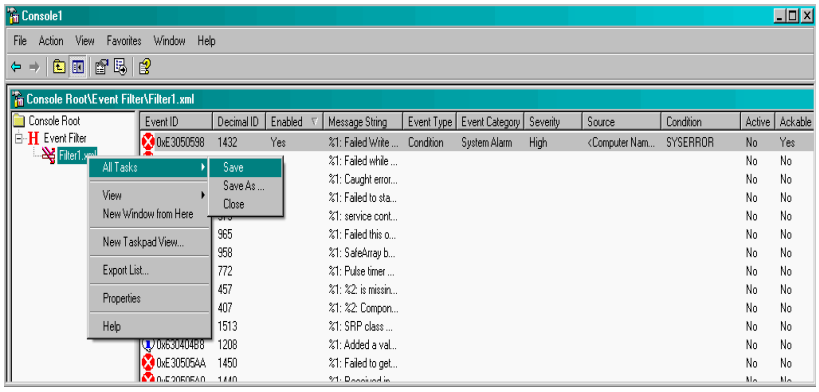
| Step | Action |
|---|---|
| **3** | Click **OK**.<br><br>**Result:** A filter table is created with a default file name of Filter#.xml. The filter table appears in the scope pane of the MMC. The events that are available for filtering appear in the results pane.<br><br>  <br><br><br>**ATTENTION**<br><br>Although events are listed in the results pane, initially all events are disabled for filtering. You must enable an event of interest during event configuration (described later) so that an interested client, such as a System Management Display or System Event Server, can receive the event notification. |

## Configuring an Event

Follow these steps to configure an event.

| Step | Action |
|---|---|
| **1** | Select the event on the result pane and select **Configure Event…** from the pop-up context menu.<br>  |

| Step | Action |
|---|---|
| 2 | Use the **Assign Event Type** page of an event to assign an Event Type, Event source and other properties to an event. The configuration page of an event is shown below. You must check the **Enabled** checkbox in order to configure the event.   |

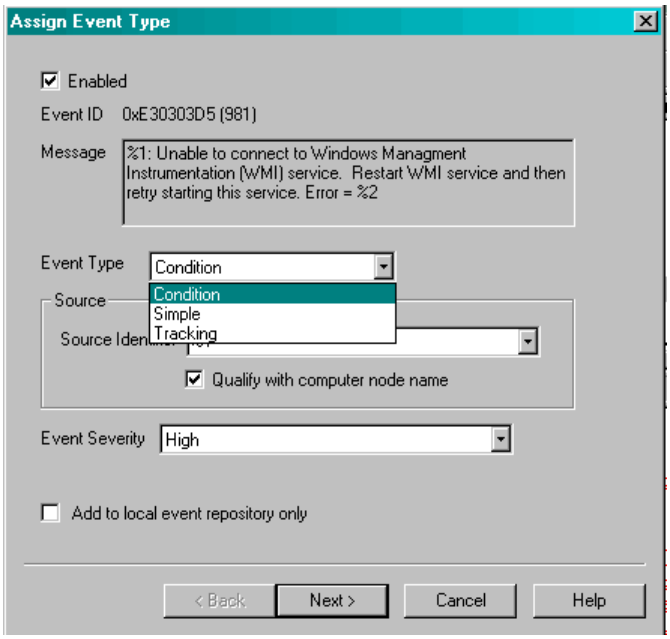
| Step | Action |
|---|---|
| **3** | Use the information in the following section, Analyzing Event Characteristics, to configure the event you selected.<br><br>Right-click the filter table, then click **All Tasks>Save** to save the filter table.<br><br>  <br><br><br>**TIP**<br><br>You can rename the filter table file to a more meaningful name when you use **Save As.**<br><br>Because \HWIAC\Filters is a very critical directory for System Event provider, Honeywell recommends that you DO NOT edit a filter table in that directory. We highly recommend you create a new filter table in another directory and edit it. Once you finish editing the filter table, copy it to the \HWIAC\Filters directory.<br><br>Save the filter table under \HWIAC\Filters, so that the System Event provider (SEP) can be notified that the file has been modified. Upon notification, SEP will reload all its filter tables. |

## Analyzing Event Characteristics

This section will present the concepts of defining an OPC event using the Event Filtering Tool. Detailed on-line help is available within the Event Filter Configuration Tool.

### *Determine Event Type*

There are three types of OPC Events: Simple, Tracking, and Condition Related.




Both Simple and Tracking Events are delivered only to clients connected and listening for events at the time of the event generation. Simple and Tracking events are not maintained in the event repository and are not acknowledgeable. The client receiving the event maintains the view of each event. Simple and Tracking events are distributed to all nodes via multicast.

Condition Related Events are acknowledgeable events that describe a condition of a system entity or a general system alarm. These events are maintained in the system event repository and delivery is guaranteed. Condition Related Events have an Active state that indicates whether the alarm condition is currently in affect. When the alarm conditon is cleared the Condition Related Event related to the alarm condition will become inactive. Once a Condition Related Event has become inactive and has been acknowledged, the event will be removed from the event repository.

Use the following table to assist in determining the type to assign an event.

| | Simple | Tracking | Condition |
|---|---|---|---|
| Guaranteed Delivery | | | X |
| Requires Acknowledgement | | | X |
| Historized | X | X | X |
| Delivered to currently connected clients only | X | X | |
| Reflects a change in the system or operating parameters | | X | |
| Represents an alarm for a system entity | X | | X |
| Represets a normal state for a system entity | | | X |
| Represents a general system alarm condition not tied to a specific system entity | X | | X |

### *Assign Event Source*

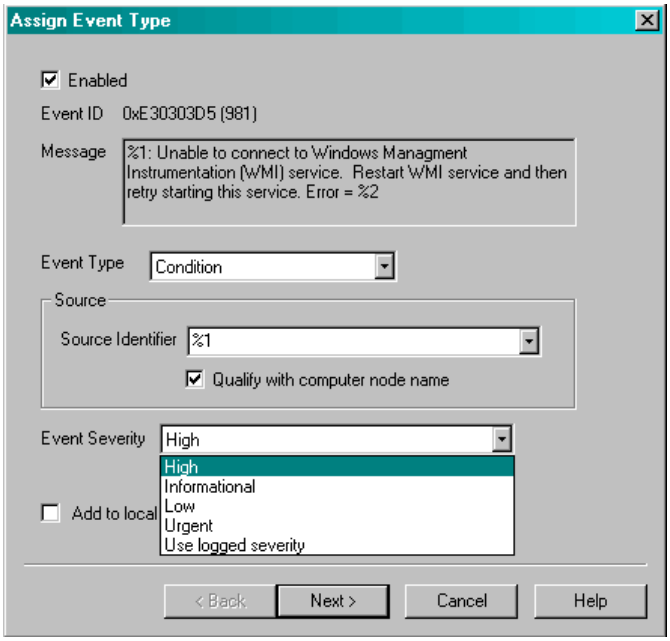
The event source identifies the subject of an event. This may be system entity such as a computer node or a managed component running on a computer node. For condition related events, all events relating to the same entity must use the same event source definition. The combination of event source and condition ties Windows events together in the system event repository.

Example: PKS01 is a computer with a managed component PKS01_SERVER. The managed component will have a source name of PKS01.PKS01_SERVER and changes in the component state will be reflected in condition related events for PKS01.PKS01_SERVER. At the same time a disk error may occur on PKS01 and is logged against the source PKS01. The source names are different and distinguish the events from each other. The alarm caused by the disk error will not affect the managed component state events.

For detailed information regarding formatting an event source name, see the System Event Filter configuration tool on-line help.

### *Assign Event Severity*

The event severity defines the OPC event severity for the specified event. OPC event is an indication of urgency or priority. The OPC severity options are Urgent, High, Low or Informational. If the **Use Logged Severity** option is selected from the drop-down list then the Windows Event Log severity will be translated as indicated in System Event Configuration tool on-line help.

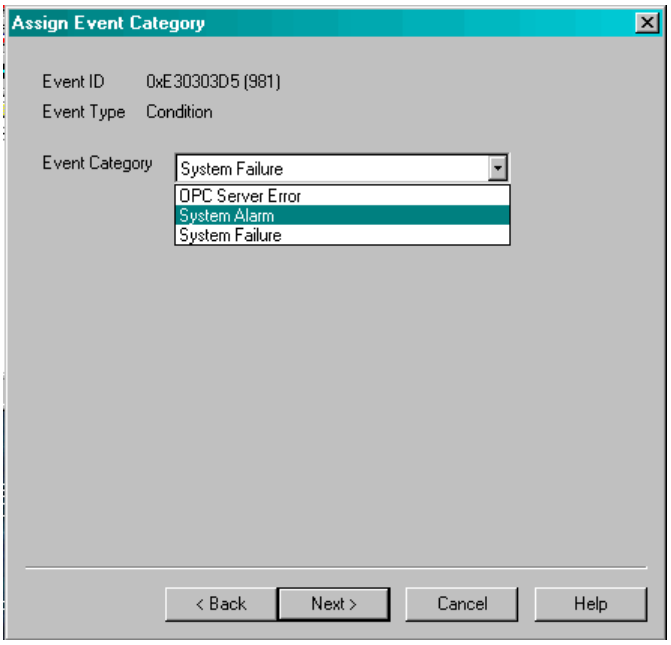



### *Add to Local Event Repository Only*

Check to add this event only to the local repository. This event will not be replicated in the repository of other nodes. To continue event configuration, select **Next**.

### *Determine Event Category*

Event types are subdivided into event categories. The System Event Filter configuration tool will present a drop-list of predefined categories for the selected event type.

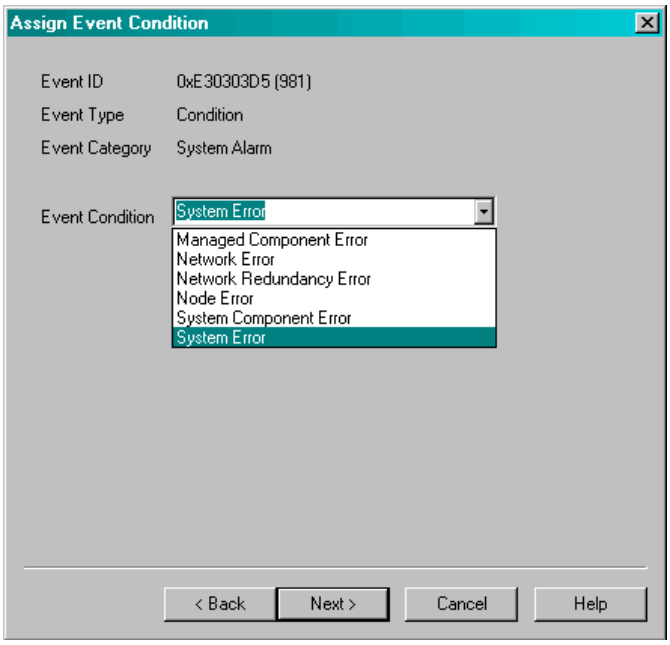



For detailed information regarding selection of Event Category, see the System Event Filter configuration tool on-line help.

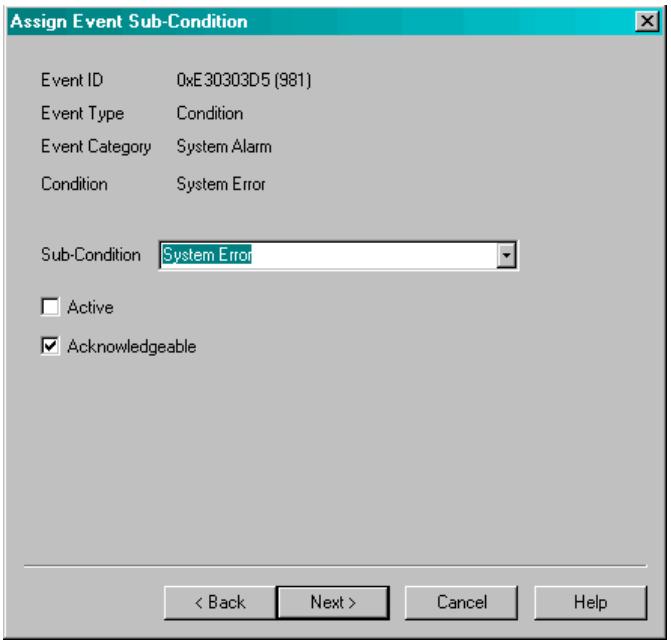
To continue event configuration, select **Next**.

### *Assign Event Condition / Subcondition (Condition Related Events only)*

If the event type selected was a Condition Related Event type, the event state being described by the event is defined by a combination of the event source and a condition. The condition may be selected from a list of predefined conditions or may be user defined. The condition name should indicate the state that is being modified (i.e. System Error – indicating an error at the system level, possibly a Windows error).



A Condition always has a Subcondition. In most cases this Subcondition is the same as the Condition. The Subcondition may be selected from the drop-list of predefined Subconditions or may be user defined.




For detailed information regarding selection of Event Condition or Subcondition, see the System Event Filter configuration tool on-line help.

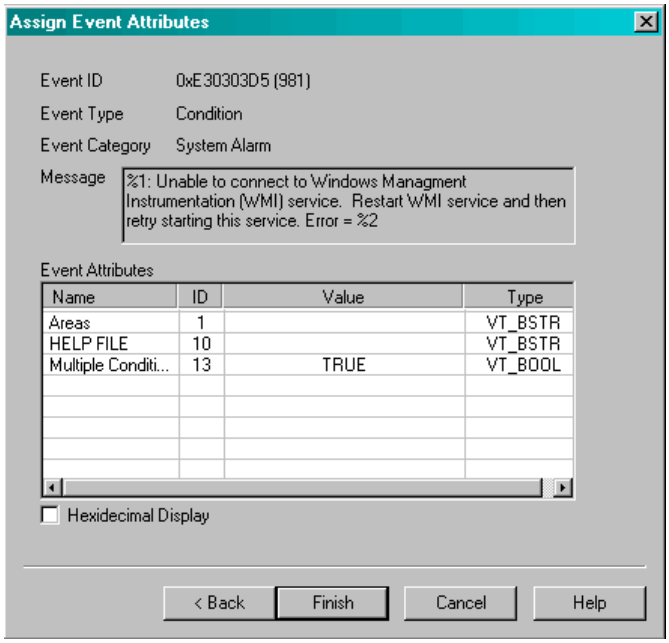
### *Determine Active / Acknowledgeable State (Conditon Related Events only)*

Condition Related Events are generally alarms representing certain entity states. Each condition related event has an active and acknowledged state. When assigning the Active and Acknowledgeable properties for an event, determine first whether the event represents an alarm condition. If so, the event would be Acknowledgeable. If the alarm condition event has a corresponding event that indicates when the alarm condition has cleared, then also make the event Active. The corresponding cleared (return to normal) condition event will be defined as Inactive and Unacknowledgeable.

For detailed information regarding use of the active and acknowledgeable properties, see the System Event Filter configuration tool on-line help.

### *Event Attributes*

Event Attributes are associated with event categories. For detailed information regarding use of the event attributes, see the System Event Filter configuration tool on-line help.




Select **Finish** to complete configuration of the selected event.

### Procedure for sharing a Filter Table

If a message file is shared by more than one event source, each event source can have its own filter table, or multiple event sources can share a common filter table.

Follow these steps to share a filter table:

| Step | Action |
|---|---|
| **1** | To allow a filter table to be shared by multiple event sources, right-click a filter table, and select **Properties** from the pop-up context menu. |
| **2** | On the Properties page, select **Add** and then select another event source from the **Event Source Section** dialog box. |
| **3** | In this example, a message file is shared by two event sources. Application Error and Application Hangshare a filter table. |

# 9. Supporting System Performance Server

## 9.1 Role of the System Performance Server

### About the System Performance Server

The System Performance Server is an OPC Data Access server that provides an efficient mechanism of retrieving performance and configuration information. This information is internally maintained on a per-node basis using Microsoft's WMI. The availability of this data through OPC interfaces allows it to be easily integrated into operator displays and process applications in a manner consistent with process data access.

By representing WMI data as OPC data items, the DCS infrastructure is able to display, trend, and/or historize Windows performance information. This information is vital for system monitoring and problem analysis. While Microsoft and third parties provide tools that allow some trending and analysis of PC performance information, few can match the capabilities available in the process control environment.

**REFERENCE - INTERNAL**

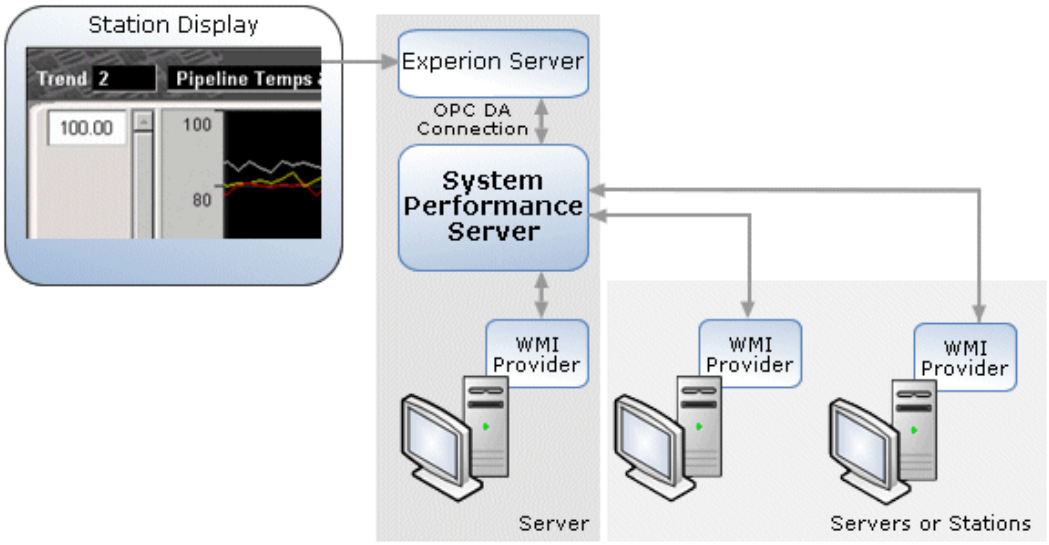
The System Performance Server is an HCI Managed Component. Refer to the System Management Operations Guide for procedures on how to monitor the status of the System Event Server.

**ATTENTION**

SPS is an OPC Data Access Server that is compliant with version 2.05 of the OPC Data Access specification. However, since the data provided by SPS is performance and configuration information supplied by other sources, write operations are not allowed. All write operations will return an HResult of S_FALSE and data item pp_errors of OPC_E_BADRIGHTS.

### System Performance Server architecture

System Performance Server data can be accessed from several Experion operational displays such as Trend. It can also be accessed from custom HMIWeb or GUS displays. The figure shown here illustrates high-level architecture of the System Performance Server.




SPS provides performance (and other WMI) data from a defined set of computers to its clients.

SPS sets the range of computes that can be accessed by a client of SPS to all computers in the unit containing the node on which SPS is running. The containing unit can be one of: Windows Domain, or Windows Workgroup. The System Performance Server runs on any Experion or TPS Windows platform based on Windows (Windows 2000 or XP and as outlined in definitions, above). Similarly, the System Performance Server can monitor any Experion or TPS Windows node within its containing unit..

### SPS data naming

The OPC item names recognized by SPS are based on the names WMI uses to access data. SPS item names are of the form:

```
host.[namespace].class.instance.property
```

where

| SPS Item Name Component | Description |
|---|---|
| host | the name of the Windows platform on which the WMI data item resides. Data items within the same OPC group may reside on different nodes. |
| Namespace | the identifier of the name space within the CIM Repository which contains the data item. Specification of the namespace is required. |
| Class, instance and property | CIM Repository name components of the data item. See WMI documentation (within MSDN) for a more detailed description. |

Two examples of SPS data items are shown here:

Node37.\root\CIMV2.Win32_PerfRawData_PerfOS_Processor**.**Name="0"**.**PercentIdleTime

APP28.\root\CIMV2**.**Win32_PerfRawData_PerfOS_Memory=@**.**AvailableBytes

There is one special form of the name that WMI defines, for objects for which there can be one and only one instance (in WMI terms, a singleton object). In this case, the name for WMI would be:

```
\\host\namespace\class=@
```

For SPS, the corresponding name would be:

```
host.[namespace].class=@
```

### What is an SPS Alias

Due to the complexity of the names required by WMI, SPS provides shortcuts to some items in the form of an alias table. The nameform for aliases is **`host.aliasname`**.

The table below lists several example aliases with the corresponding WMI name.

| Example Alias | WMI name |
|---|---|
| `cpu_percent_user` | `[root\CIMv2].Win32_PerfFormattedData_PerfOS_Processor.Name="_Total". PercentUserTime` |
| `cpu_0_percent_user` | `[root\CIMv2].Win32_PerfFormattedData_PerfOS_Processor.Name="0". PercentUserTime` |
| `cpu0clockspeed` | `[root\CIMV2].Win32_Processor.DeviceID="CPU0".CurrentClockSpeed` |
| `disk_c_percent_free` | `[root\CIMV2].Win32_PerfFormattedData_PerfDisk_LogicalDisk.Name="C:".PercentFreeSpace` |

**TIP**

Use the SPS Configuration page to view the complete set of default aliases. This page can also be used to add or delete an alias. See section 9.3 for configuration details. The subsection titled "*Adding new Aliases*" contains specific information related to aliases for pure singleton objects and single instance objects.

For a complete list of the possible status values and associated meanings, refer to the online help for the SPS configuration page.

# 9.2 Installing System Performance Server

### Installation guidelines

For Experion, the System Performance Server should be installed on every Experion Server or LCN-connected Server. In a redundant server configuration the System Performance server should be installed on both servers and their scope should be configured the same. (Note: Having different scopes on redundant nodes will not restrict data access but will affect the presentation of the SPS Auxiliary status display).

The System Performance Server in a TPS only system would be installed on an APP node.

Care should be taken to avoid scope overlap. Scope overlap occurs when two or more System Performance Servers pulls the same data from the same PC.

### Procedure for installing SPS in TPS or pre-R300 Experion system

The System Performance Server is a licensed package. TPS users should follow these steps to install System Performance Server software.

**ATTENTION**

TPS and pre-R300 Experion users should follow these steps to install System Performance Server. R300 Experion users should not follow these steps as the System Performance Server can be installed as part of the Experion installation.

| Step | Action |
|---|---|
| 1 | Install the Microsoft Service Pack and Microsoft hot fixes, available on the Honeywell Common Components CD. Then, reboot the node. |
| 2 | Select Licensed Package Installer from the Common Components CD, as shown here. |
| 3 | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| 4 | Enter license and authorization numbers. Click **Next** to continue. |
| 5 | Click **System Performance Server**. (Note: If System Performance Server does not appear in the list, verify that the licensing and authorization numbers are appropriate for this package). |

| | |
|---|---|
| **6** | Click **Install Package.** |
| **7** | Verify that these are the components you wish to install. Click **OK**.<br><br>**Result:** The installation process occurs, which usually takes a few minutes. |
| **8** | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |
| **9** | Reboot your node. |

### Procedure for installing System Performance Server in R300 Experion system

**ATTENTION**

R300 Experion users may not need to perform these steps on an Experion Server, as System Performance Server can be installed during R300 Experion node installation. R300 Experion users only need to perform this procedure on an Experion Server if there is a need to add System Performance Server to the server.

| Step | Action |
|---|---|
| **1** | Insert the Experion Application DVD, click “Browse DVD contents”, and launch the Honeywell software Installation application at <drive letter>:\Packages\Install.exe |
| **2** | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| **3** | Click System Performance Server**.** |
| **4** | Click Install Package. |
| **5** | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |
| **6** | Reboot your node. |

# 9.3 Configuring SPS on Experion Server

### Procedure for configuring System Performance Server

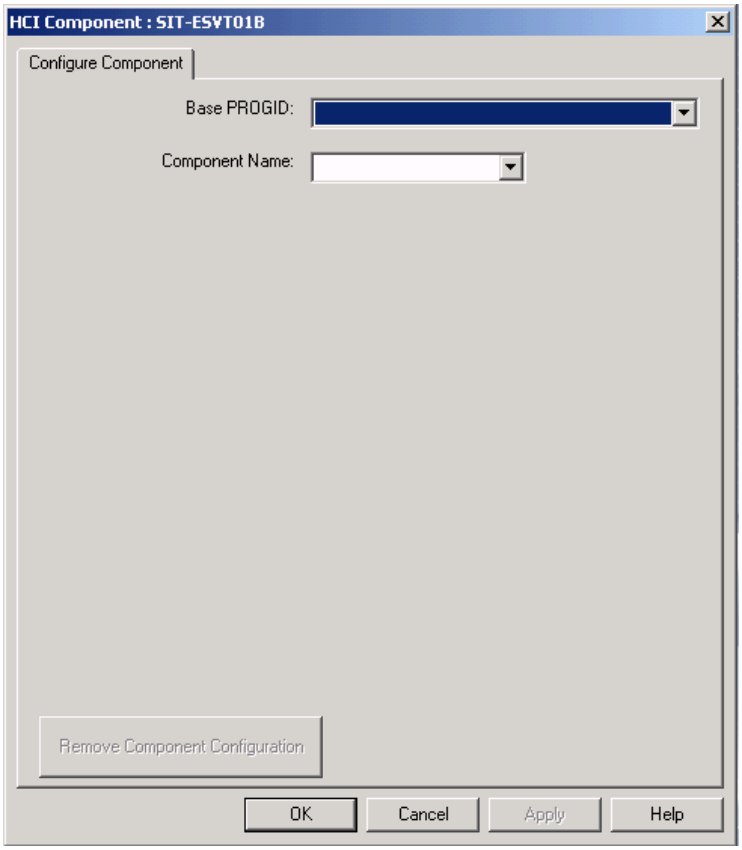
The Experion Server is integrated with the System Performance Server such that user configuration is not required. When the Experion Server starts, it connects to the System Performance Server using a set of pre-configured properties.

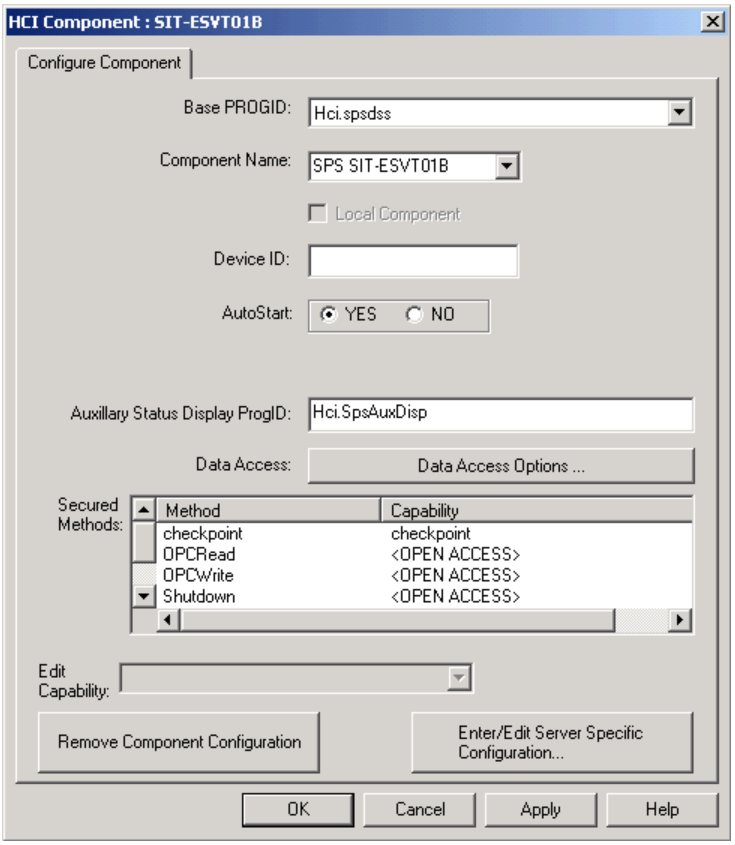
**ATTENTION**

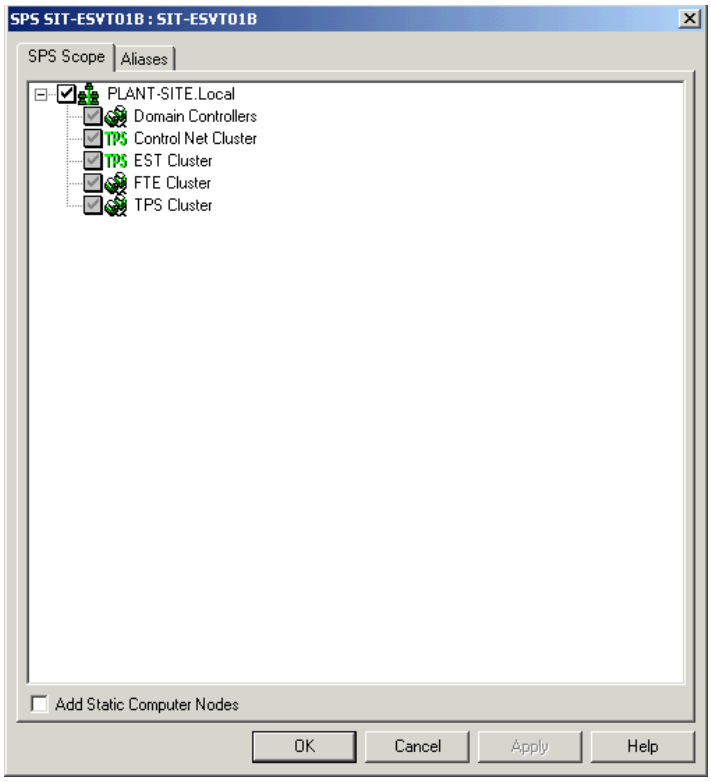
When configuring SPS Server component, do not change any property values except for method security, SPS Scope or Aliases. These items should only be changed if the pre-configured settings do not meet your needs. Using the pre-configured settings for component name and auto start enables the System Performance Server to work properly with the Experion Server.

Follow these steps to view the default settings of the System Performance Server or to adjust settings not required by the Experion Server.

| Step | Action |
|---|---|
| 1 | From the hierarchy of the System Management Display, right-click the computer item. (See section 6.1of this document for detailed instructions.) |
| 2 | Select **Configure** from the context menu. |

| Step | Action |
|---|---|
| **3** | Select HCI Component from another context menu. The resulting configuration page appears.<br>  |

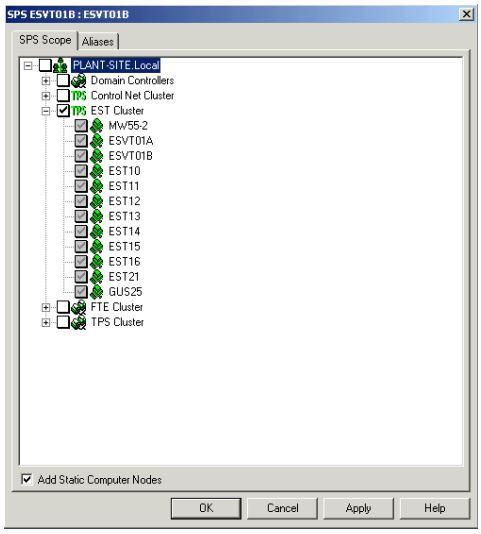
| Step | Action |
|---|---|
| **4** | Click the down arrow button on the edit combo box of the **Component Name** to get a pull-down list of pre-configured components. HCI/OPC component configuration reads from the registry of the host node. Select the component named **SPS** <machine name where SPS is installed>. In this example, the component is named **SPS SIT-ESVT01B**.<br>  |
| **5** | Use the procedure described in section 6.1, Secured Methods, to adjust the secured access to OPCRead, Shutdown, etc. It is not necessary to adjust the settings of OPCWrite since the SPS server is read only. All attempts to write to a WMI item through the System Performance Server are denied. |

| Step | Action |
|---|---|
| 6 | Click the **Enter/Edit Server Specific Configuration** button to display the SPS Server configuration pages. The resulting configuration page appears.<br>  |
| 7 | Continue to the following “Configuring the SPS Scope” section that describes configuration selections. |

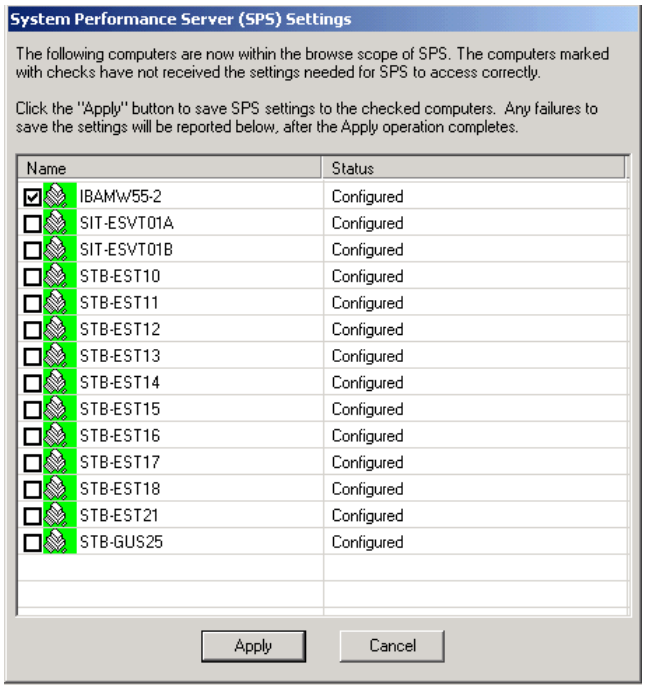
## Configuring the SPS Scope

Use the SPS Scope page to perform the operations describe in the table below.

| Operation | Background | Procedure |
|---|---|---|
| Configure WMI on the nodes in the configured SPS scope to enable SPS to monitor those nodes.. | SPS needs to establish monitoring capability with all the nodes in the container (domain or workgroup). | Check **Add Static Computer Nodes** to list all the nodes. Check or uncheck the checkboxes, as appropriate, to limit the SPS Scope to any combination of OUs and/or computers. |
| Define the set of computers displayed in the SPS Auxiliary Status display, where the user can view the SPS connection status to those computers. | SPS Auxiliary Status display includes a tabular list of the connection status to SPS. Only the nodes checked in the browse tree are included in the tabular list. Refer to section 3.5 in the System Management Operations Guide for procedures on how to invoke the Auxiliary Status display. | Select the nodes you are interested in monitoring. Select **OK** or **Apply** on the SPS Scope page. |



As a result of clicking the Apply button, SPS configuration attempts to enable SPS access on remote nodes. The following display is shown:



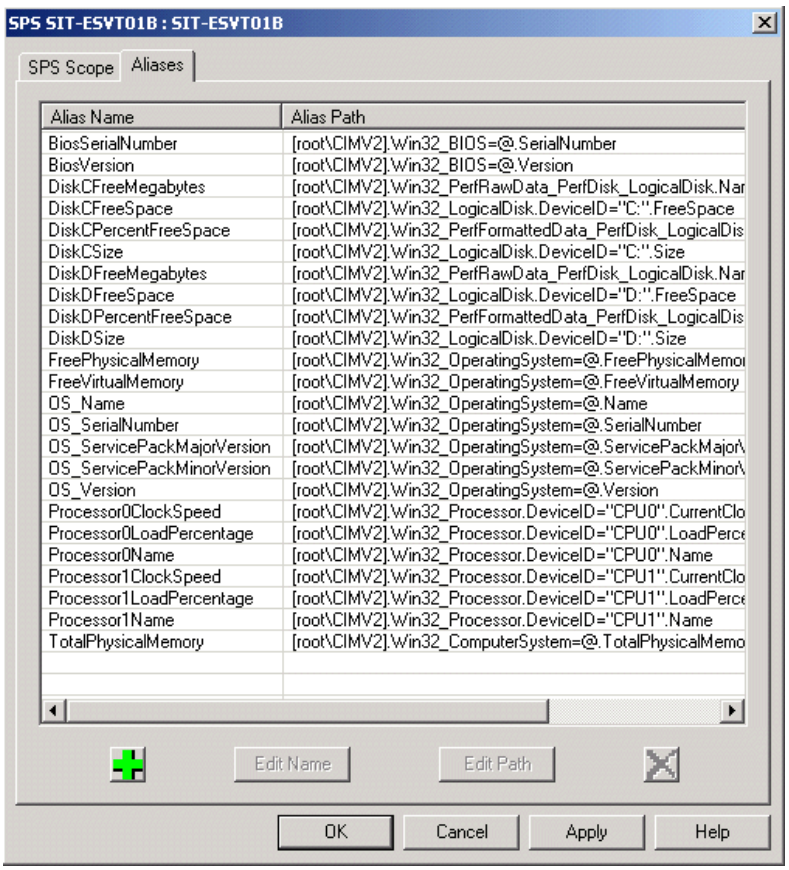

For a complete list of the possible status values and associated meanings, refer to the online help for the SPS configuration page.

**ATTENTION**

Default SPS aliases include some that are available only for use on Windows XP and Server 2003 operating systems. Those aliases will not work on Windows 2000 family systems. Microsoft provides a WMI toolkit which includes a WMI browser that lets you view the WMI objects on a given machine. You can download this free toolkit from Microsoft.com, search on "WMI Administrative Tools".

### Adding new Aliases

Follow these steps to view and/or add SPS aliases.

| Step | Action |
|---|---|
| **1** | Select the Aliases tab from the SPS Server specific configuration page. See above figure. The resulting page is displayed.   |
| **2** | To **add** a new Alias Name, click the green **+** button. This will enable the first blank line in the list to receive the name of the new alias. |
| **3** | Type the alias name. |
| **4** | Type a tab character. This will move the cursor to the Alias Path field. |

| Step | Action |
|---|---|
| **5** | Type the alias path. |
| **6** | Click elsewhere in the dialog to end editing the path, or click **Apply** or **OK** to save the change. |

Some WMI items have node or hardware specific names that could make defining aliases difficult. Two examples of this are:

> Win32_BIOS.Name="Default System BIOS",SoftwareElementID="Default System BIOS",SoftwareElementState=3,TargetOperatingSystem=0,Version="DELL - 8"
>
> Win32_OperatingSystem.Name="Microsoft Windows XP Professional|C:\\WINDOWS|\\Device\\Harddisk0\\Partition2"

In the first example, the WMI item is dependent on the PC brand and the BIOS version. In the second example, the WMI item is dependent on the installed OS and its location. In order to develop useful aliases for these names, SPS aliases extend the WMI singleton naming convention to include objects for which there is only one instance. This is in addition to pure singleton objects. In most cases a PC has only one installed BIOS and operating system. Using the above examples as a reference, the following aliases can be defined that will work in most cases:

> “Win32_BIOS=@” (e.g. “Win32_BIOS=@. SerialNumber” to get a the serial number of a node)
>
> “Win32_OperatingSystem=@” (e.g. “Win32_OperatingSystem=@.FreePhysicalMemory” to find the current amount of available physical memory on a node)

While this mechanism can be very useful for defining generic aliases, the results will depend on the specific content of WMI.

### Deleting an alias

Follow these steps to delete SPS aliases.

| Step | Action |
|---|---|
| **1** | From the SPS Aliases configuration page (see step 1 above), click on the line or lines to be deleted. (The **Shift** key or the **Ctrl** key can be used to select multiple lines.). As a result, the line(s) are highlighted. |
| **2** | Click the **X** button. |
| **3** | Click **Apply** or **OK.** |

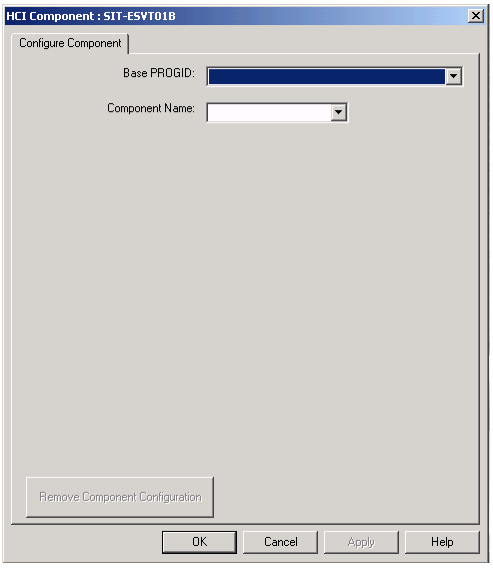
### Editing an alias

Follow these steps to edit SPS aliases.

| Step | Action |
|---|---|
| **1** | From the SPS Aliases configuration page (see step 1 above), click on the field to be changed. |
| **2** | Click a second time in the field to be changed, or click the **Edit Name** or **Edit Path** button. Enter the change. |
| **3** | Press the tab key to edit the next field, if desired. |
| **4** | Click elsewhere in the dialog to complete the edit. Click **Apply** or **OK** to save the change. |

## 9.4 Configuring SPS on APP Node

Follow these steps to configure the System Performance Server on an Application Processing Platform (APP) node.

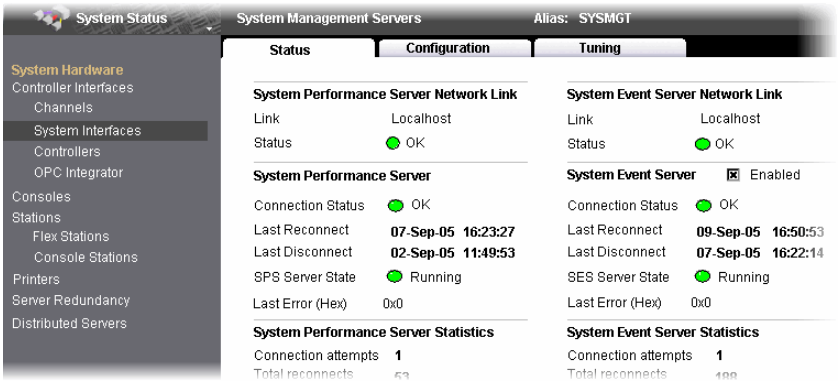
| Step | Action |
|---|---|
| **1** | From the hierarchy of the System Management Display, right-click the computer item. (See section 6.1of this document for detailed instructions.) |
| **2** | Select **Configure** from the context menu. |
| **3** | Select HCI Component from another context menu. The resulting configuration page appears.<br>  |
| **4** | Click the down arrow on the combo box of the Base PROGID to get a pull-down list of pre-installed base components. Select Hci.spsdss. |
| **5** | Click the edit combo box of the **Component Name**, and then enter the name.<br><br>**Result:** The **Check Name** button appears. After verifying the component name, the system enables the **Apply** button. After the system saves the information to the registry, this base component will no longer be displayed in the list of the base PROGID for the next new configuration. |
| **6** | Continue with step 5 in section 9.3. The remainder of SPS configuration for a |

| Step | Action |
|---|---|
| | APP Node is identical to that of an Experion node. |

## 9.5 Verifying SPS is Operational on Experion Server

### Procedure for verifying SPS is Operational

Follow these steps to verify that SPS is operational on an Experion Server node.

| Step | Action |
|---|---|
| **1** | Start the Experion Server. |
| **2** | Start the Experion Station. |
| **3** | From the station menu bar, **select View->System Status->System Management Servers**. The resulting status display appears.   |
| **4** | Verify that the System Performance Server Network Link is **OK**. Refer to the section “Configuring system performance and event monitoring” in the *Server and Client Configuration Guide* (see the subsections “Setting up system performance and event monitoring”). Refer to the section “Monitoring System Status“in the *Experion Operators Guide* (see the subsection “Monitoring System Management Servers”). |
| **5** | To add SPS items to a custom display or a standard trend, refer to the section “Configuring system performance and event monitoring” in the *Server and Client Configuration Guide* (see the subsection “Adding system performance data to displays”). |

## 9.6 Verifying SPS is Operational on APP Node

Use this procedure to verify that your System Performance Server works properly.

| Step | Action |
|---|---|
| **1** | From the System Management Display, select the System Performance Server |
| **2** | If the **AutoStart** option for the SPS was selected, then the System Management Display should show that the SPS has started.<br><br>If the **AutoStart** option was not selected, then start the server by right clicking on its name in the System Management Display. From the resulting context menu, click **All Tasks> Start**. After a few seconds the SPS component goes to the idle/running state.. |
| **3** | To add SPS items to a custom GUS display, refer to the section 5, “Named Data Access Syntax, in the *HCI/OPC Data Access User’s Guide*. |

## 9.7 Troubleshooting SPS Configuration

The following table describes symptoms of possible problems you might encounter when configuring your System Event Server, and recommended solutions to these problems.

| Symptom | Solution |
|---|---|
| System Management Servers Status indicates that the SPS is not OK and not Enabled (black lights rather than green lights). (Experion Server node) | The System Performance Server is installed to run as a predefined account name with predefined password. If the password for this account is changed, then connection to SPS will fail. In order to synchronize passwords with accounts, a tool is available that allows the user to change the account and password on all Windows services or DCOM servers running as an account.<br><br>This tool can be accessed from Start>Programs>Honeywell Experion PKS>System Management>Windows Services & DCOM Servers Logon tool.<br><br>Follow the instructions provided on the tool. Note that this tool does not change the password on the account. |

# 10. Supporting SNMP Monitor

## 10.1 Role of the SNMP Monitor

### About SNMP

Simple Network Management Protocol (SNMP) is an industry standard protocol for managing network appliances. Equipment such as routers and switches implement an SNMP agent that provides access to configuration information and operating parameters. Operational event notifications can be sent to listening SNMP managers to notify them of the event occurrence without polling.

### Purpose of the SNMP Monitor

The SNMP Monitor converts SNMP notifications into Windows Events. A System Event Filter file is installed by the SNMP Monitor package to convert the Windows Event into an OPC event. The event is then made available to the System Management Display and to the Experion Alarm Summary display via the System Event Server. As a result, alarms are logged when router or switch interface connections are lost.

## 10.2 Installing the SNMP Monitor

The SNMP Monitor should be installed on a node running System Management Runtime. For Experion users, generally the SNMP Monitor should be installed on the same computers as the System Event Server. In complex topologies, the SNMP Monitor is typically installed on the server that provides the most direct and reliable path to a network appliance such as a switch. The package will install the Microsoft SNMP Agent service and the Microsoft SNMP WMI Provider as well as the Honeywell SNMP Monitor. The Honeywell SNMP Monitor is a permanent WMI consumer application and will auto-start when an SNMP notification is received

### Procedure for installing SNMP Monitor in TPS or pre-R300 Experion systems

The SNMP Monitor is a licensed package. Follow these steps to install SNMP Monitor software.

| Step | Action |
|---|---|
| 1 | Install the Microsoft Service Pack and Microsoft hot fixes, available on the Honeywell Common Components CD. Then, reboot the node. |
| 2 | Install the Honeywell Repackaged Redistributable Files by selecting it from the Common Components screen shown in Step 2 of section 3.4 to install the libraries. Then reboot. |

| | |
|---|---|
| **3** | Select Licensed Package Installer from the Common Components CD. |
| **4** | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| **5** | Enter license and authorization numbers. Click **Next** to continue. |
| **6** | Click **SNMP Protocol and Monitor**. (Note: If SNMP Protocol and Monitor do not appear in the list, verify that the licensing and authorization numbers are appropriate for this package). |
| **7** | Click **Install Package.** |
| **8** | Verify that these are the components you wish to install. Click **OK**.<br><br>**Result:** The installation process occurs, which usually takes a few minutes.<br><br> If the Microsoft SMNP Agent has not already been installed, then you will be prompted to insert the Windows 2000 or XP operating system CD. |
| **9** | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |
| **10** | Reboot your Experion Server. |

### Procedure for installing SNMP Monitor in R300 Experion system

**ATTENTION**

R300 Experion users may not need to perform these steps on an Experion Server, as SNMP Monitor can be installed during R300 Experion node installation. R300 Experion users only need to perform this procedure on an Experion Server if there is a need to add SNMP Monitor.

| Step | Action |
|---|---|
| **1** | Insert the Experion Application DVD and launch the Honeywell software Installation application at <drive letter>:\Packages\Install.exe |
| **2** | Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue. |
| **3** | Enter license and authorization numbers. Click **Next** to continue. |
| **4** | Click SNMP Protocol and Monitor**.** |
| **5** | Click Install Package.<br><br>If the Microsoft SMNP Agent has not already been installed, then you will be prompted to insert the Windows operating system media. |
| **6** | After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process. |
| **7** | Reboot your node. |

## 10.3 Configuring the SNMP Monitor

There is no configuration necessary for the SNMP Monitor itself. The switches or routers from which notifications are to be received must be configured to send those notifications or traps to the node on which the SNMP Monitor has been installed. This configuration is device specific and will be detailed in the vendor documentation. Configuration of these devices usually entails enabling the types of notifications to send and entering the IP Addresses to which notifications should be sent. The link-up and link-down notifications should be enabled.

# 11. Administering HCI Name Service

## 11.1 Role of HCI Name Service

### What the name service provides

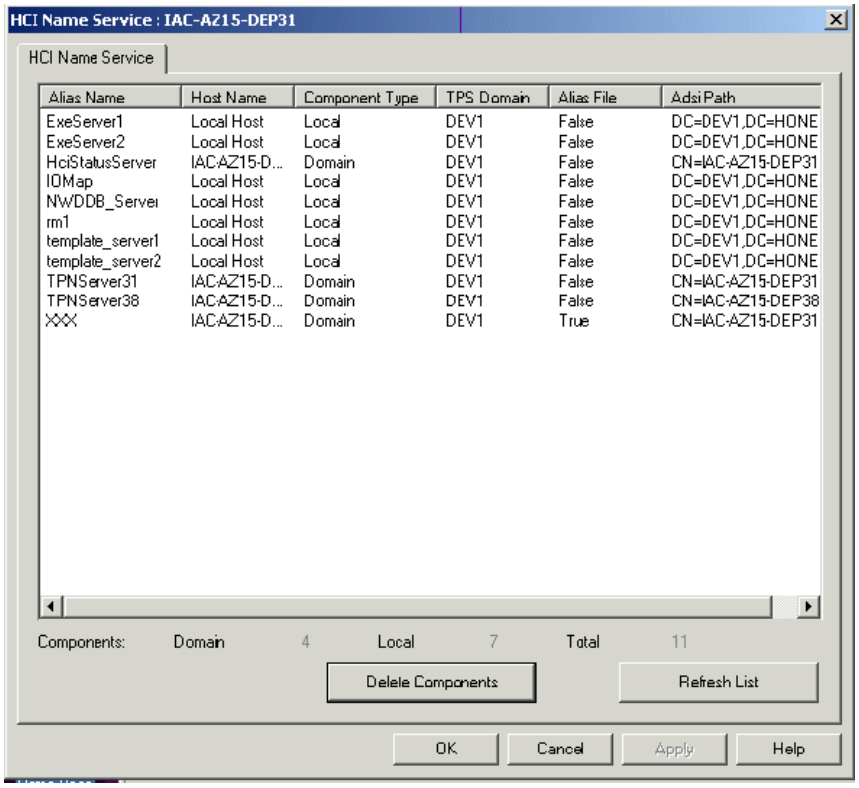
The HCI Name Service provider (HCI-NSP) is responsible for resolving HCI/OPC alias names. Each node containing HCI clients or servers must have Name Service provider installed and running locally in order to reduce the impact of partial network failure. HCI-NSP creates and maintains a repository of alias names found on the local machine and within the scope of a defined multicast group.

Name Service uses Alias files to identify remote HCI/OPC servers that reside outside the multicast scope.

### Example HCI Name Service display

Figure 20 shows an example of an HCI Name Service display.

**Figure 20 A Sample HCI Name Service Display**



### Description of HCI Components

The HCI Name Service Display contains the following information about HCI Components, as shown in Figure 20.

**Table 12 Descriptions of HCI Components**

| HCI Component Information | Description |
|---|---|
| Host Name | Name of the computer hosting the server. |
| Component Type | Identifies a server for local only access or local and remote access. |
| TPS Domain (OU) | Name of the TPSDomain / Organizational Unit containing the host node. |
| Alias File | Identifies an alias name that came from an alias file (TRUE) or did not (FALSE). |
| AdsiPath | Active directory-distinguished name of the node. |
| Alias Name | User-configured name applied to component during HCI Component configuration. |
| CLSID | Class Identifier of the server. |

### Uniqueness of alias names

Alias names need to be unique within a TPS Domain (OU).

A client application will function inconsistently if a remotely accessed component is given the same name as a Local Only component. A unique alias name allows a client application to be written so that it can access the same HCI/OPC server, no matter which node the client runs on. Some HCI/OPC servers are intended to be accessed locally or remotely, and some are intended to be accessed as Local Only.

During HCI Component configuration, when you check alias names usage, the configuration tool recognizes Local Only components, as well as remote and locally accessed domain components.

You define the intended access of a server during HCI Component configuration. The intended access of the component affects how it is maintained in the alias name repository. A remotely accessed component will be unique within a TPSDomain, so there is only one possible entry in the repository. A Local Only component is different; it can exist on multiple nodes within a TPSDomain, and thus is displayed differently.

If a Local Only alias name item exists on multiple nodes in the TPSDomain, there will be only one entry for it in the repository. If the component is configured on a local node in the TPS domain, then the repository will reflect the local node as the host name. See Figure 20, *An Example HCI Name Service Display*.

## 11.2 Viewing and Setting Scope of HCI Name Service

### About the HCI Name Service tool

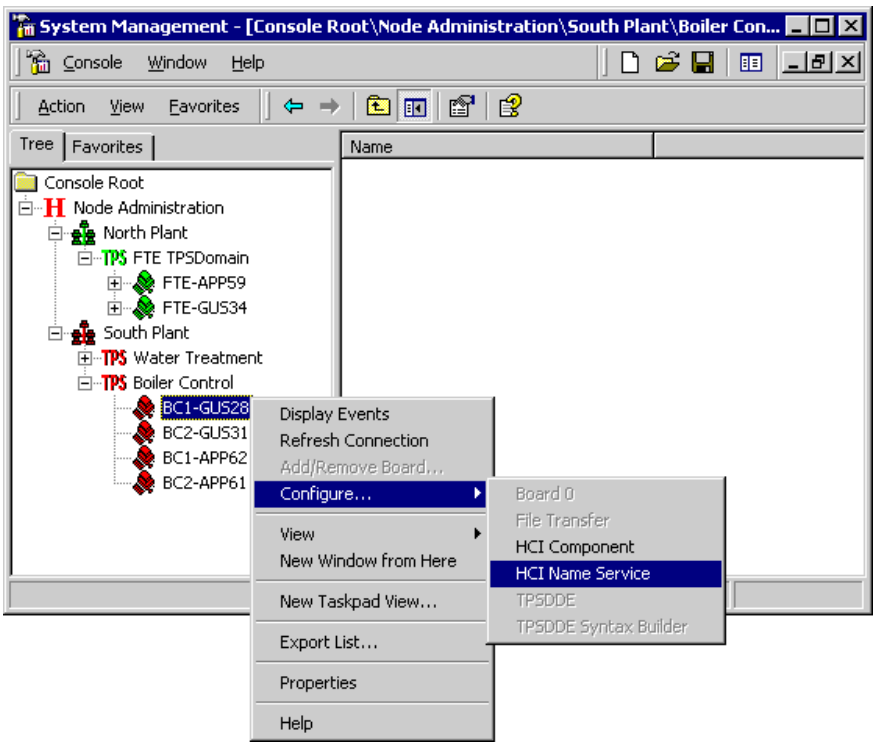
The HCI Name Service tool displays the contents of the name service repository that resides either in the local node or a selected remote node. The HCI Name Service Repository display is invoked from the System Management Display.

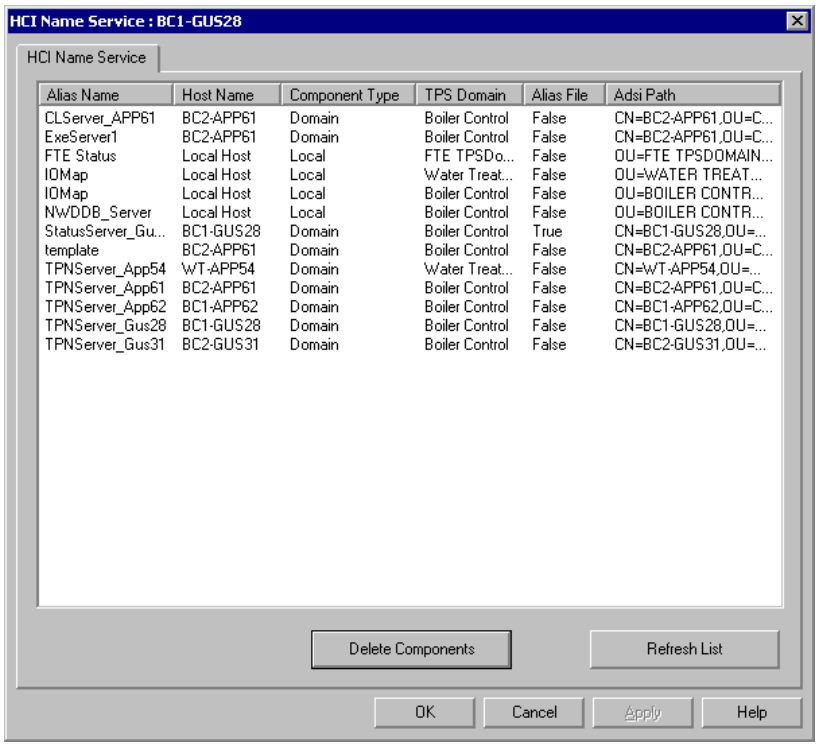
This tool helps you perform the following two operations during an HCI Component Configuration session:

- Delete unused data entries in the repository
- Refresh the listing.

### Viewing the name service repository

Follow these procedures to view the Name Service repository.

| Step | Action |
|---|---|
| **1** | From the System Management Display, right-click the node of interest and select **Configure>HCI Name Service**.<br>  <br>**Result:** The HCI Name Service tool appears. |

| Step | Action |
|---|---|
| **2** | From the HCI Name Service tool, you can:<br>• Refresh the list.<br>• Delete a component (if you have access privileges).<br>  |

### Deleting a local component

Honeywell recommends you use the HCI Configuration Page to delete all components.

**ATTENTION**

**DO NOT** delete a local component from the HCI Name Service configuration page unless you are deleting Alias names that are no longer being used.

Deleting a local component from the HCI Name Service configuration page removes the local component Alias name and associated configuration from all (Running) nodes in the same TPS Domain. The actual component is not being uninstalled, nor is its DCOM registration.

Table 13 describes issues that may occur when deleting a local component, why these issues occur, and recommended solutions to these issues.

**Table 13 Issues That May Occur When Deleting Local Components**

| Issue | Why Issue May Occur | Recommended Solution |
|---|---|---|
| **A deleted Local Component reappears** | If a node is not running during the deletion, the local component Alias name and associated configuration still exists in its registry.<br><br>When the node is restarted the Name Service Provider adds the Alias Name back into the repository, and because it is a local component, replicates the Alias name and associated configuration to the registry of all nodes with in the same TPS Domain. | Make sure all nodes in a TPS Domain are running before deleting local components. |
| **A Local Component has multiple Alias names** | The HCI Component configuration page does not allow you to give a second Alias name to an already configured local or domain component.<br><br>Multiple Alias names can occur when you delete the alias name of the local component and reconfigure it with a new/different Alias Name while one or more nodes in the TPS Domain are not running. The old alias name for the local component is restored in the name service repository and the registry of every node in the TPS Domain. | Make sure all nodes in the TPS Domain are running and delete the unwanted alias name(s). |

### Summary of HCI component deletion

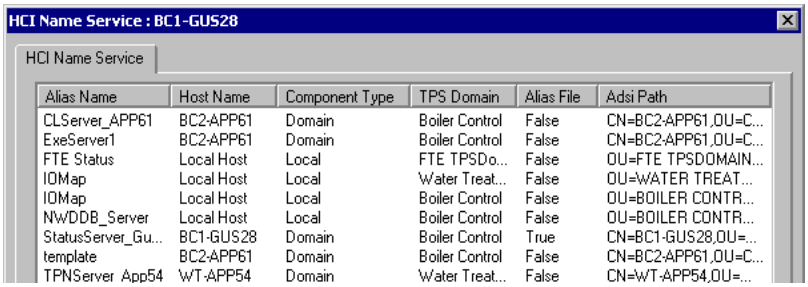
- When you delete a local component, you delete its component name and component configuration from **ALL** nodes in the TPS domain.
- When you delete a domain component name that does not reside in the registry, its name is deleted from the repository.
- A domain component configuration can only be deleted from the HCI Component Configuration page.
- If an off-line node containing a deleted domain component name returns online, and does not have its domain component configuration deleted, its name will be re-inserted into the list.

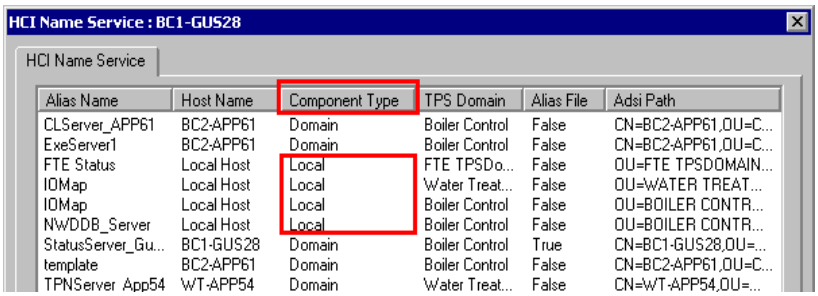
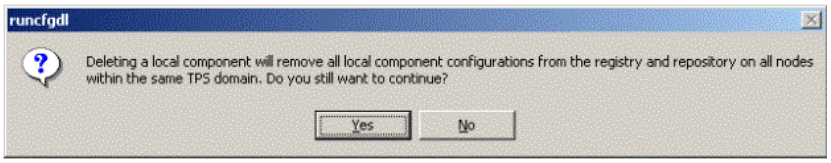
### Procedure for deleting an HCI component

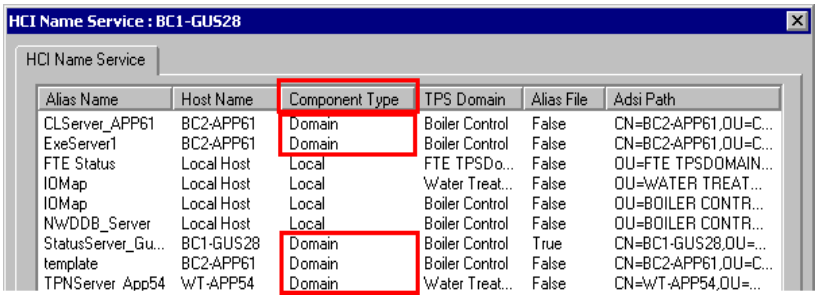
#### *Prerequisites*

Make sure you have been assigned access privileges to delete a component. You will not see the **Delete Components** button in the Name Service page if you have not been assigned access privileges.

Follow these steps to delete an HCI component.

| Step | Action |
|---|---|
| **1** | From the HCI Name Service tool, select the component you want to delete.  |

| Step | Action |
|---|---|
| **2** | If you select a local component…<br>  <br><br>You'll see the following prompt message:<br>  <br><br>**TIP**<br>A local component deletion removes all local component configurations from the registry and repository on all nodes within the same TPS domain. |

| Step | Action |
|---|---|
| **3** | If you select a domain component, it cannot be removed from the repository if it is configured in the registry of a node within the same TPS domain. Domain components can only be removed using the HCI Component page.<br><br>If you want to delete a domain component from the HCI Name Service tool, you must put it in an off-line state, or stop the name service in order to delete it.<br><br>  |



### Scope of name service provider

The HCI-NSP keeps its synchronized repository of component alias names in synchronization with all computers within a specified Active Directory scope.

For example:

A path to the TPS Domain indicates that all computers with the TPS Domain Organizational Unit (OU) are synchronized.

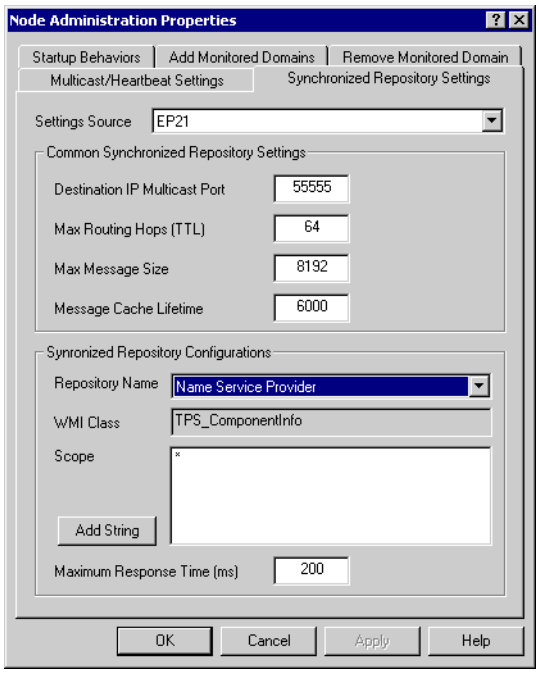
A path to the Domain level synchronizes all HCI-NSPs within the Domain – regardless of TPS Domain OU. This setting is specific to the HCI-NSP and must be set on every node containing the HCI-NSP and SRP and residing within the specified scope. This path will default to * indicating all nodes within the IP Multicast group is independent of the Active Directory path.

**TIP**

The SRP utilizes a single IP Multicast group to synchronize ALL subscribed providers. Each provider specifies the scope of synchronization by registering itself with the SRP with an Active Directory Path.

### Procedure for setting the scope of name service repository

Prerequisites -- All computers in the console must be on-line, since configuration affects registry. Scope options are described in section 5.9, *Synchronized Repository Scope Determination*

| Step | Action |
|---|---|
| **1** | Select the Domain or OU within which you want all HCI-NSs to be synchronized. To synchronize multiple domains, select the Node Administration item. |
| **2** | Right-click the item and select **Properties**. |
| **3** | From the **Synchronized Repository Settings** page, set the HCI Name Service to the desired Repository Scope.<br>  |
| **4** | The Snap-In enumerates all contained computers, connects to their registry, and sets the scope according to the Snap-In item level selected.<br><br>**Result:** Snap-In level synchronization will apply the "*" path as the scope, resulting in synchronization of all nodes within the IP Multicast group. |

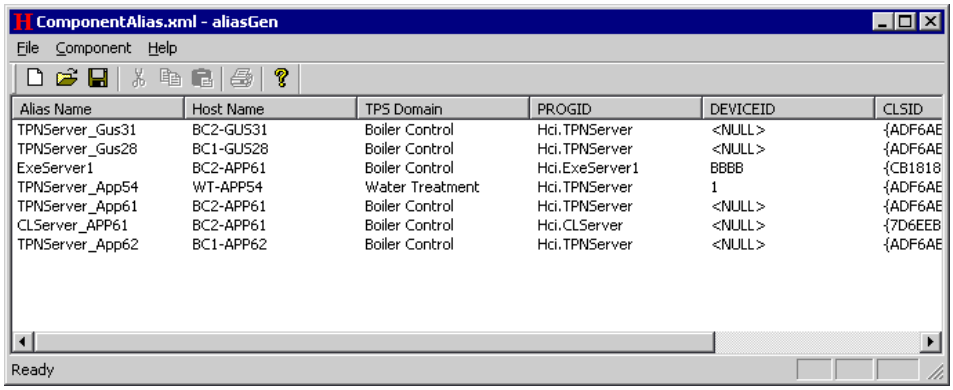
# 12. Generating a File using Alias Generator

## 12.1 Purpose of Alias File

### How the Alias Generator tool works

The Alias Generator tool creates a file for alias names. The name service provider on that node uses the file to monitor alias names. An alias file is typically used to retrieve information about the name service repository from a remote node, which is not within the scope of the configured multicast group.

**Figure 21 Example Alias file**




### Scenarios that require an Alias File

A component alias file for alias names allows you to manually include HCI/OPC servers to the alias name repository that are not within the scope of the configured multicast group. HCI Alias files should be distributed to nodes that cannot participate in the multicast-based name resolution mechanism (for example, nodes separated by a firewall that restricts multicast traffic). The component alias file alias names are not synchronized with other node repositories. Component alias files can be different on each node, making it impractical to attempt to synchronize the repositories with their information.

### ComponentAlias.XML file is required

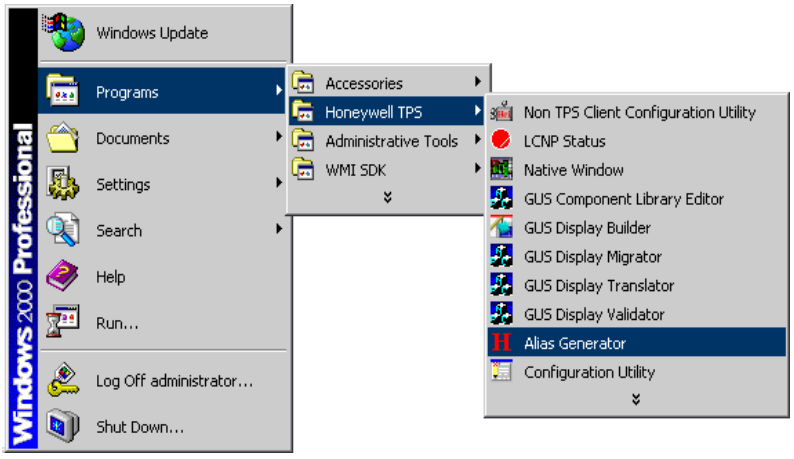
A blank XML file named ComponentAlias.XML is installed under the \HWIAC\ ComponentAlias directory by default. Honeywell highly recommends using this file to configure an alias file. This file's default setting is read-only. You must change this setting to read/write so you can modify the file and write to it.

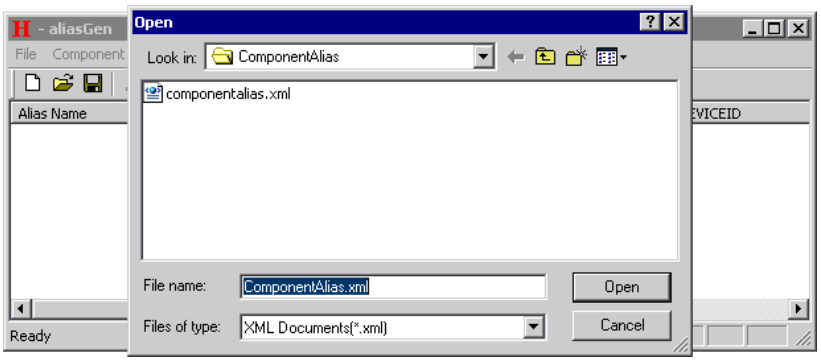
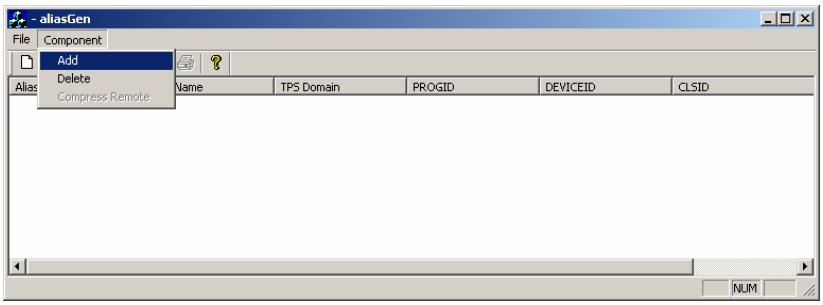
### Adding components to a Component Alias file

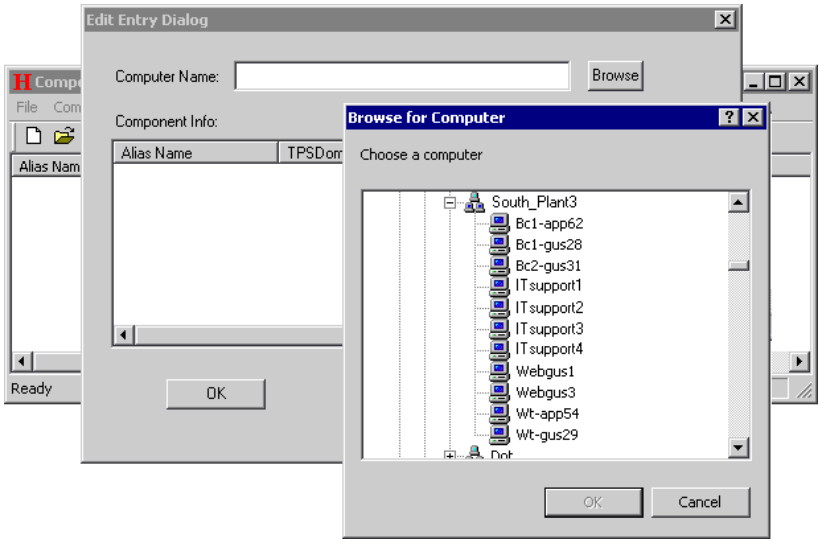
**ATTENTION**

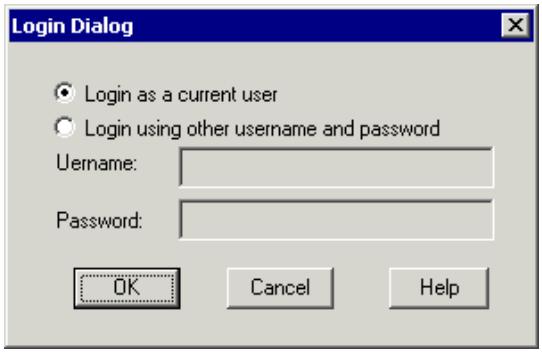
You can also create a new Alias file.
If this file is not named ComponentAlias.XML, or not stored under the \HWIAC\ComponentAliasdirectory, then the Name Service provider **WILL NOT** read the contents into the repository of this node.

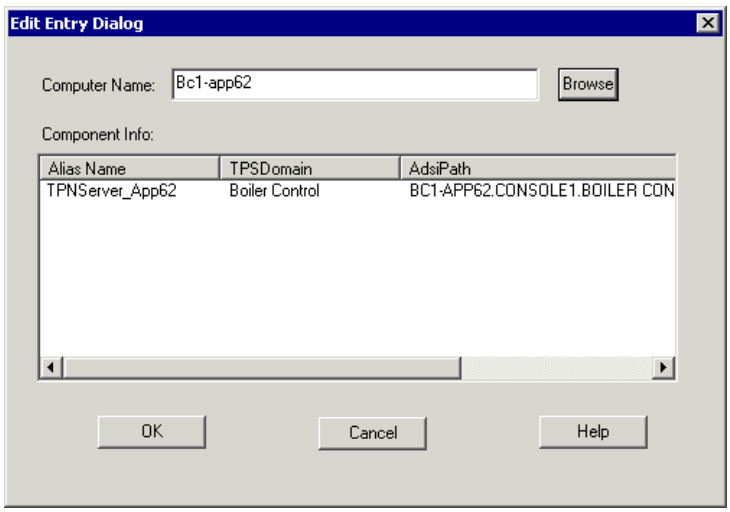
Follow these steps to add components to a Component Alias file.

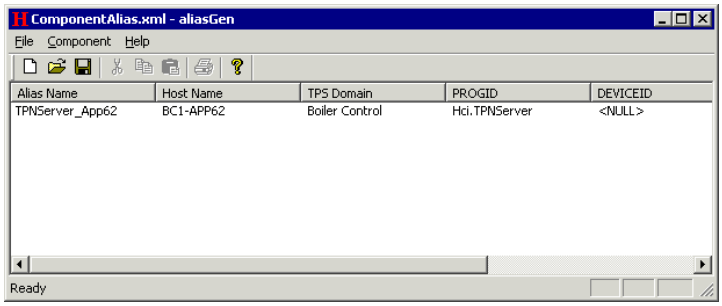
| Step | Action |
|---|---|
| 1 | Select **Programs>Honeywell TPS>Alias Generator** to start the Alias Generator program.  |

| Step | Action |
|---|---|
| **2** | Select **File>Open** to open the ComponentAlias.xml file.<br>  |
| **3** | To add an entry to your file, select **Component>Add**:<br>  |

| Step | Action |
|---|---|
| 4 | Once you click **Add**, an **Edit Entry** dialog box with blank names appears. Click **Browse** to locate the computer that contains HCI components.   |

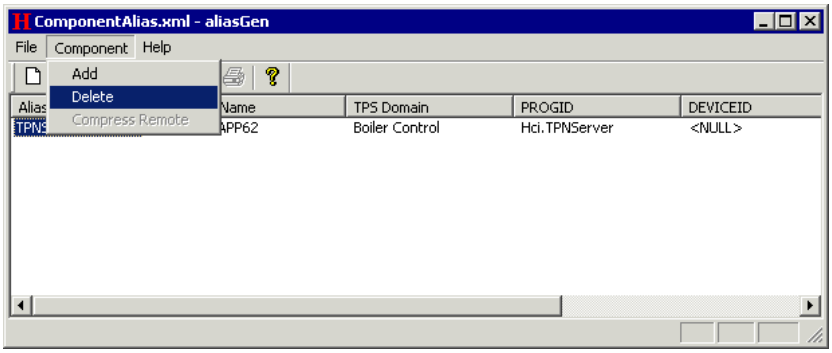
| Step | Action |
|---|---|
| **5** | Select a computer name from the **Browse for Computer** dialog box, and click **OK.** A new **Login** dialog appears:<br>  <br><br>The default username and password are NULL, which means the default user (usually the system administrator) has authority to connect to any computers residing within a specific domain.<br>If you do not have authority to connect to a specific computer, you must input the username and password for that specific computer, in order to connect to it. |

| Step | Action |
|---|---|
| **6** | If both the username and the password you entered for a specific computer are correct, the system connects with the name service provider on that specified remote node.<br><br>**Result:** The **Edit Entry** dialog box appears with the component information.<br><br>  |

| Step | Action |
|---|---|
| **7** | Select the alias names from the multi-selection list box. You can select one or more alias items simultaneously. Click **OK** to display the selected alias items.<br>  <br><br>**Note:** Repeat these steps if you want to continue adding some new items to an alias file. For your convenience, when the **Add Entry** dialog box pops up for the second time, it contains the same contents you previously entered.<br>If you select the same items as the ones that have already been selected for that alias file, a pop-up a reminder appears, informing you that the alias name you selected is already in use. |
| **8** | Click **File>Save** to save an Alias File to this directory:<br>\HWIAC\ComponentAlias\ComponentAlias.xml |
| **9** | Repeat Steps 1-8 for additional nodes of interest. |

### Deleting a Component from an Alias File

Follow these steps to delete an entry from an open Alias file:

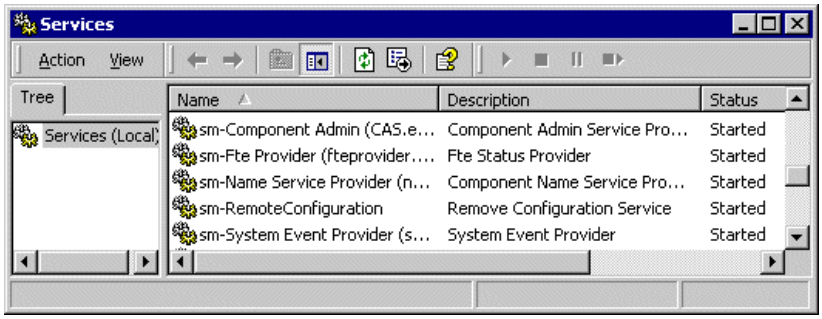
| Step | Action |
|---|---|
| 1 | Select the items to be deleted. |
| 2 | Select **Component> Delete**<br>  |
| 3 | Save the file. |

# 13. Troubleshooting System Management

## 13.1 How to use this section

### Introduction

The following table describes symptoms of possible problems you might encounter when configuring your system, and recommended solutions to these problems.

| Symptom | Solution |
|---|---|
| Nodes display off-line when they are really on-line. | Check the multicast group setting to see if the nodes are in the same multicast group. Check the version of the software. Go to Add/Remove programs and select the Honeywell System Management software package (e.g., Runtime, Status Display, TPS Admin support files). Click on Support Information to identify the version.<br><br>Identify the system Software is running on both the local and remote node. You can check that the providers are running by going to **Control Panel>Administrative Tools>Services.** Locate the services starting with an "sm-" prefix and verify that they are started as shown in the following figure. |
|  | |
| Component does not get deleted from the Name Repository. | Component was in a node that was offline when the deletion occurred. |
| Node that is moved from one TPS node to another appears in two TPS domains. | Refresh the display (Select Node, Display Events>Refresh). |

| | |
|---|---|
| HCI Component fails after attempted startup. | Refer to the Event Viewer logs for additional help that can narrow your problem resolution. In general failures to start may be caused by access rights and permissions. Refer this problem to your system administrator. The respective HCI Component's user guides contain additional information about security and the use of dcomcnfg. |
| An Auxiliary Status Display does not appear when selected even though it is enabled as a menu selection. | The Auxiliary Status Display is an ActiveX control that must be loaded onto the requesting node for it to appear on the requesting node. Ask your system administrator to load the respective client connectivity package on the requesting node. |
| HCI Component appears in Warning state. | For TPN HCI managed components, such as TPN Server and CL Server, a warning state indicates that the TPS Node Personality is not loaded into the node or its connection to the TPN has been lost. Verify that the node's personality is loaded and that it has a connection to the TPN. |
| HCI Name Service does not contain a full list of alias names. Or see SRP Provider messages in the Application Event log indicating synchronization problems. | Network Configuration Problem: Possible port Auto Negotiation problem. Configure network port on Ethernet card to use 10 or 100 Mbps full duplex communication instead of Auto Negotiate |
| Nodes appear as offline in the System Management display despite being online and operational | Network Configuration Problem: Enable multicast communications for each port in the network switches attached to the TPS nodes. |
| Nodes disappear from the FTE status display intermittently | Network Configuration Problem: Enable multicast communications for each port in the network switches attached to the TPS nodes. |
| FTE Status Display reports a problem with the interconnection between switches. | Network Configuration Problem: Check interconnection cable. Check switch configuration. If Nortel switches are utilized, also disable Snooping and Spanning Tree |
| DNS Resolution Problems | HOSTS / LMHOSTS Configuration Problem: Ensure HOSTS / LMHOSTS files are up to date and do not conflict with DDNS registrations. |

| | |
|---|---|
| Nodes do not appear within a TPS Dmain (OU) | Active Directory / TPS Domain Configuration:<br>• Ensure node was moved from computers OU to the TPS Domain OU. Use the Active Directory Users and Computers MMC snap-in to correct. Reboot the node.<br>• Run ADSITest program to help diagnose the problem<br>• From the properties display of the TPS Domain OU select the TPS Domain tab. Verify TPS Domain has been selected. If found not selected, select and reboot all nodes defined in the TPS Domain OU. |
| Nodes do not appear in the System Management Display but they are up and running. | DDNS Configuration Problem<br>• System Management Infrastructure is not loaded on the particular node. Install the System Management Infrastructure or System Management Display to correct the problem.<br>• Ensure primary and secondary DNS configuration settings on each TPS node point at the Windows DNS server.<br>• Ensure the primary DNS configuration on the DNS Server machine points to itself. Type netdiag –fix at a command prompt on the DNS server for further information.<br>• Other DNS configuration problem. Open a command prompt and type nslookup. The IP address and name of the DNS server should appear.<br>Account Permissions Problem<br>• Log in as a Domain User. Local users have a restricted view of domain resources.<br>Network Configuration Problem<br>• Possible port Auto Negotiation problem. Configure network port on Ethernet card to use 10 or 100 Mbps full duplex communication instead of Auto Negotiate |

**13. Troubleshooting System Management**

13.1. How to use this section

Honeywell

Honeywell International
Process Solutions
2500 West Union Hills Drive
Phoenix, AZ  85027