Honeywell

Experion PKS
System Management Configuration Guide

EPDOC-X141-en-431A
February 2015

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-X141-en-431A	431	0	February 2015

Disclaimer

Contents

1 About This Document

This document describes the following tasks.

- Configuration of a system management display
- Configuration of the event filter
- Configuration of HCI/OPC components
- System Event and Performance Servers

Revision	Date	Description
A	TBD	Initial release of the document.

1.1 References

The following documents are sources of reference for topics discussed in this publication.

Document Title	Document ID
Experion Server and Client Configuration Guide	
Experion Operators Guide	
System Management Operations Guide	EPDOC-X142-en-410
Redirection Manager User's Guide	EPDOC-X116-en-410
Fault Tolerant Ethernet Status Server and Auxiliary Display User's Guide	EPDOC-XX38-en-410
Integrated Experion-TPS User's Guide	EPDOC-XX66-en-410
Fault Tolerant Ethernet Planning, Installation and Service Guide	EPDOC-XX36-en-410
HCI/OPC Data Access User's Guide	EPDOC-XX52-en-410
TPN Server User's Guide for windows 2003/XP	EPDOC-X143-en-410
Configuration Utility User's Guide	EPDOC-XX14-en-410
OPC Specification Reference Manual	TP41
Windows Domain Implementation Guide	

2 Introduction

2.1 System Management Overview

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 Experion-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.

2.1.1 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. The Snap-ins provide the actual management behavior; MMC does not provide any management functionality.

2.1.2 How Honeywell System Management software works

System Management consists of two installable packages. The System Management runtime package provides the base infrastructure of System Management. It is installed on every managed node. The TPS Domain/ Console Configuration Tool provides an extension to the Active Directory Users and Computers Snap-in and is installed only on Domain Controllers.

The System Management Runtime package includes the System Management Display. The System Management display is an MMC snap-in that interacts with the System Management runtime to determine the status of each managed node. This display provides both status monitoring and configuration of managed nodes.

For a complete list of installable features within the System Management Runtime package, see “What is Available for Installation” on page 22.

System management uses Microsoft's Organizational Units (OUs) as a means of organizing nodes into operational units. These OUs are uniquely identified as TPS domains. System Management treats nodes in a Workgroup as a single TPS domain.

2.1.3 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

2.1.4 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: Role of System Management" shows the various functions of Honeywell System Management software and "Table 1: Software for System Management Tasks" describes each of those functions.

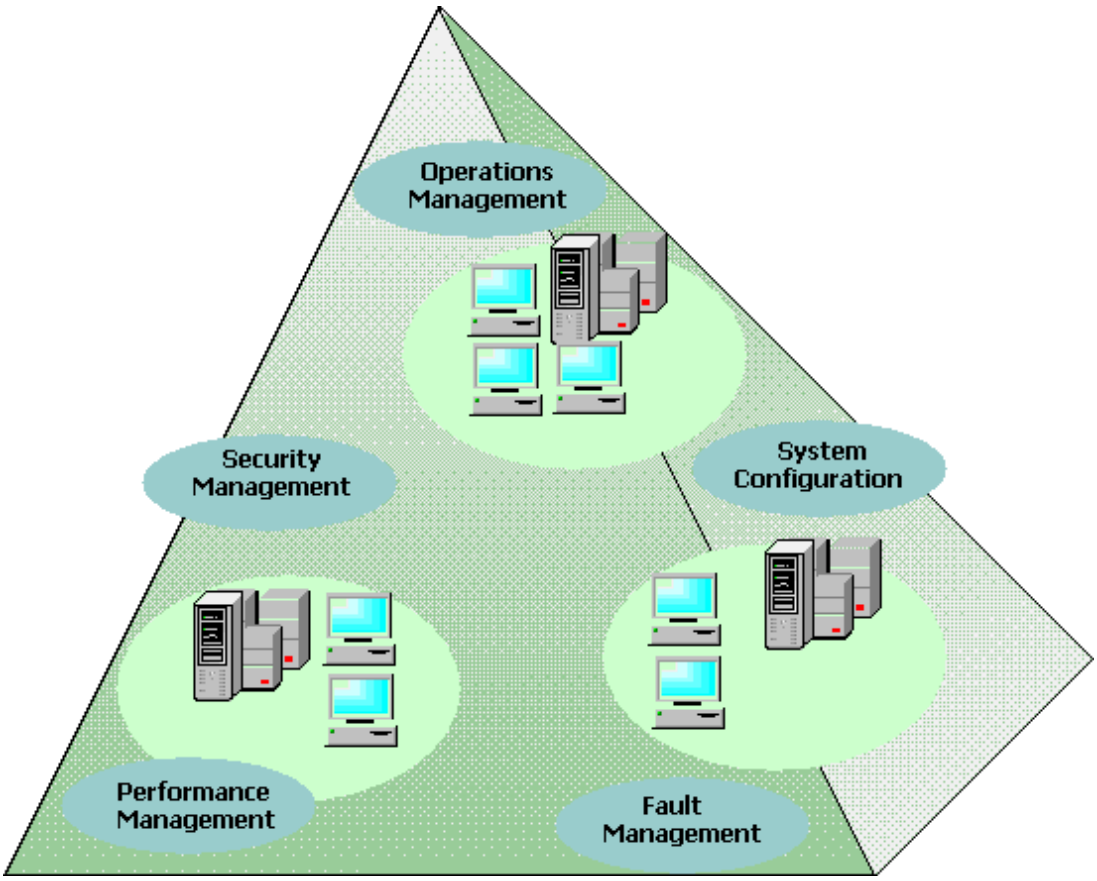


Figure 1: Role of System Management

2.1.5 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 Organizational Units.
- Visibility of system level 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 provides aliasing of managed HCI/OPC components. It also replicates the aliases and configurations across a TPS Domain.

- Remote HCI Component Configuration
- Remote TPS Standard Node Configuration
- Management of local and domain HCI Components
- 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. Use standard Windows facilities running in MMC to perform system and domain configuration, user account administration, and security administration. *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. *The Honeywell HCI Name Service* is used by HCI client applications to resolve an alias name to a server's CLSID and computer name. *The Honeywell System Event Provider* publishes local events as system events and maintains a synchronized local copy of system events within a predefined scope. *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 to be journaled in the Experion Event Journal. *The Honeywell System Event Provider* and *HCI Name Service Provider* maintain a synchronized database of System events and HCI alias names. *The Honeywell Component Admin Service* monitors and manages HCI managed components. Provides on-demand monitoring of non-managed HCI/OPC servers. *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. *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*
Operations Management	*The Honeywell Synchronized Repository Provider (SRP)* performs lower-level inter-node communications necessary to keep event and name server information synchronized. *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 *Honeywell HCI Managed components* help you view Experion Server status displays. (See ' “Configuring HCI/OPC Components” on page 61').	• *System Management Configuration Guide* • *System Management Operations Guide*

To Perform this Task…	Use these Honeywell and Microsoft System Management Components	Refer to this Document
Performance Management	*The Microsoft Performance Management (PerfMon) and third-party tools* monitor Windows system and network performance. System Performance Server provides OPC Data Access to Windows performance data. SPS data can be accessed through GUS or Experion custom displays. In addition, it can be accessed using Experion detail displays.	• *Microsoft documentation* • *System Management Configuration Guide* • • *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.	• *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*
Alias File Generation	Alias File Generation program. (See the Generating a File Using Alias Generator section of this document).	*S*

2.1.6 Focus of this document

Refer to “Table 2: System Configuration Tasks” to find documentation about all Honeywell system configuration and management tasks. This document focuses on the following system configuration tasks.

- Managing Organizational Units and Computers
- Configuring HCI/OPC Components
- Administering HCI Name Service
- Troubleshooting System Management

2.1.7 System configuration tasks

“Table 2: System Configuration Tasks” shows system management and configuration tasks that may be performed remotely or locally, and the documentation that contains details about implementing these tasks.

Table 2: System Configuration Tasks

Task Performed	How to Perform Task		Related Documentation
Remotely	**Locally[2]**		
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*

Task Performed	How to Perform Task		Related Documentation
Remotely	**Locally[2]**		
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*
GUS Remote Displays Server Configuration		X	*GUS Remote Displays User's Guide*
LCNl18N (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*
[1]Remotely - use Node Administration Snap-In. [2]Locally - use Node Administration Snap-In or Configuration Utility.			

2.1.8 System Management communication methods

"Figure 2: System Management Communications Architecture" 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:

- The local Heartbeat and System Event providers
- The remote Heartbeat and System Event providers (optional)
- 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.

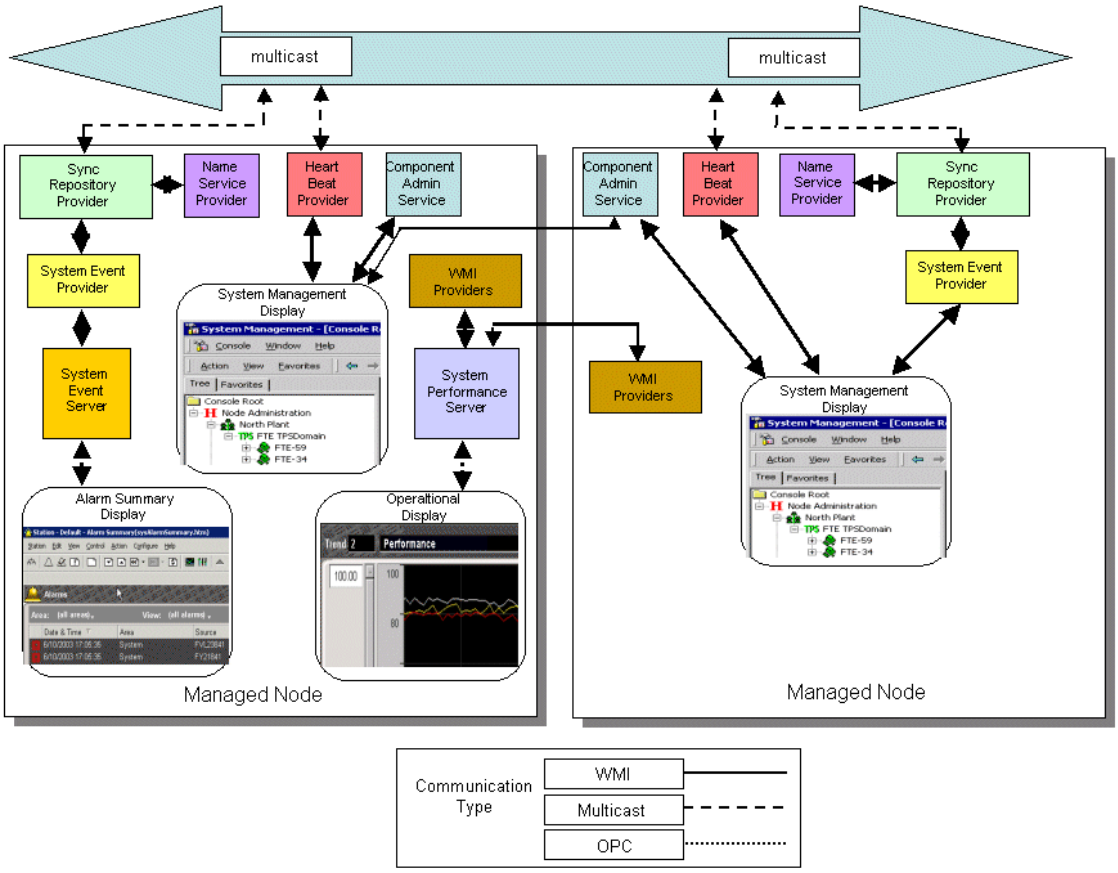


Figure 2: System Management Communications Architecture

3 Getting Started with System Management

3.1 Pre-installation Preparation

3.1.1 Who can install System Management tools

To install the System Management Runtime, you require administrator group membership. To configure System Management Runtime, you require product administrator group membership. This includes the configuration tasks associated with the System Management, such as installing the Snap-in extension of the Domain Controller and configuring HCI/OPC components.

3.1.2 Basic assumptions

Several assumptions include the following:

- Installation and upgrades are performed by a System Administrator
- The Administrator is familiar with administering Windows systems.
- System Management Runtime can be installed on a node running Windows XP, Windows 7, Windows Server 2003 or Windows Server 2008.

3.1.3 System Management implications for a network

The System Management infrastructure makes substantial use of the following.

- IP Multicast communications
- Active Directory and Dynamic DNS if installed in a Windows domain
- Host files
- 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. Make sure multicast is enabled on switches interconnecting the system nodes.

3.1.4 System requirements

You must have the following installed on your PC to install Honeywell System Management software.

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

3.1.5 System Mangement Display 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:

- Automatic enumeration of Experion nodes in the System Management Display.
- Replication of managed 'local' component configurations within the TPS Domain.

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

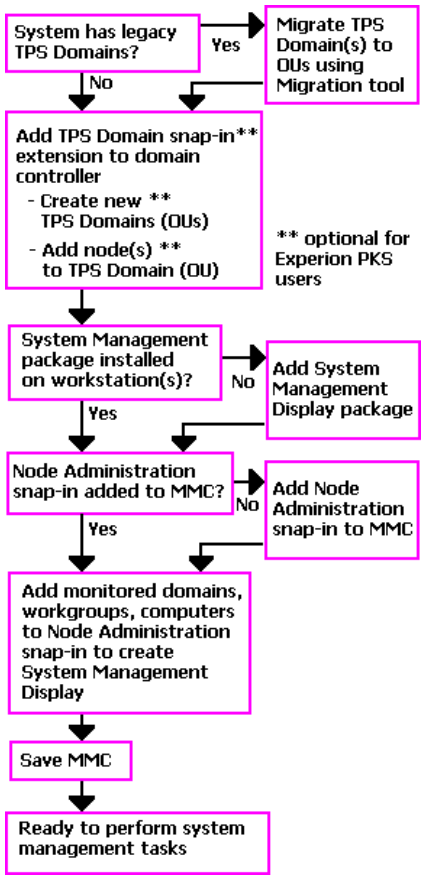
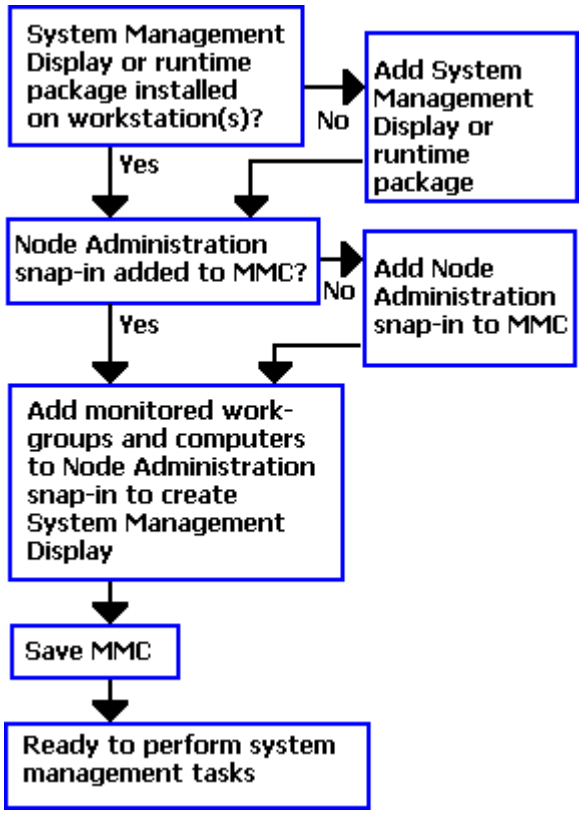
If you are a user with an Experion R400 system, your System Management components are installed during Experion installation from the Experion Application DVD. If you need to perform post or re-installation tasks, use the Experion Application DVD.

3.1.6 System management configuration flow chart

If configuration is required in a domain or workgroup, refer to the flow chart in "Table 3: System Management Communications 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.

Table 3: System Management Communications Flow Chart

If configuring System Management for a domain, refer to this flowchart	If configuring System Management for a workgroup, refer to this flow chart
	

You may be required to make modifications to your Active Directory and networking infrastructure 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 (OUs), Windows NT 4.0 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.

Security Environment	Technology Used	Considerations/Actions
Windows Workgroup	Hosts files, NetBIOS	Hosts file must be maintained and consistent on all nodes.
Windows Domain or Windows Workgroup	Multicast Communications	Ensure that all ports connected to the managed nodes on network switches are enabled to support multicast communications. See switch vendor documentation for details.

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

Refer to the *Windows Domain Implementation Guide* for procedures on how to install or migrate to a Windows 2003 or Windows 2008 domain controller.

4 Installing System Management Tools

4.1 What is Available for Installation

4.1.1 System Management Tools

"Table 4: Description of System Management Tools" describes the various system management tools.

Table 4: 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, Remote Configuration Service, and Component Administration Service Provider.
System Event Filters	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 an 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 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).
Remote Configuration Service	Caches a view of the network browse tree. Runs as either a local user, in a workgroup, or as Network Service (computer account) in a domain. Used by System Management Display and Network Tree provider to populate a network browse tree.
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 to perform the following. • Configure an HCI server from an installed base component, where a base component is identified from its ProgID • Re-configure an existing or previously configured HCI server • 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.
SNMP Monitor	The SNMP Monitor converts SNMP notifications to Windows Events.

4.1.2 When to use System Management tools

"Table 5: Guidelines for using System Management Tools" describes each of the System Management tools, the reason for using each tool, and the type of node on which each tool will be installed, and when they should be used.

Table 5: Guidelines for using System Management Tools

Tool	Reason for Using	Install on Domain Controller?	Install on Workstation?
Node Administration Snap-In	Use for Honeywell node and managed component administration and operations.		X

Tool	Reason for Using	Install on Domain Controller?	Install on Workstation?
Event Filtering Snap-In	Use 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 this tool.		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 need not use this tool.		X
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	Lets you configure Organizational Units (OUs) as TPS Domains or Consoles.	X	
Configuration Utility	Lets you configure your local nodes when the System Management Display is not available for Experion and TPS systems.		X

Attention

DO NOT move a Domain Controller to another OU. The Domain Controllers OU is a special OU and moving the DCs may impact operation.

- To use System Management facilities, your nodes of interest must operate on Windows.
- The following items are required for using TPS Domain/Console Configuration Tool Snap-In extension:
  - Domain Controller using Windows Server and Active Directory
- HCI Components, such as TPN Server, may have additional requirements and are documented in their respective manuals.

For more information about installing System Management in a Domain Controller, refer to the *Windows Domain Implementation Guide*.

5 Configuring a System Management Display

5.1 System Management Display Node Environment

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 previously is not expected to function properly in either of the other environments.

5.2 Adding the Node Administration Snap-In to the MMC

5.2.1 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.

Attention

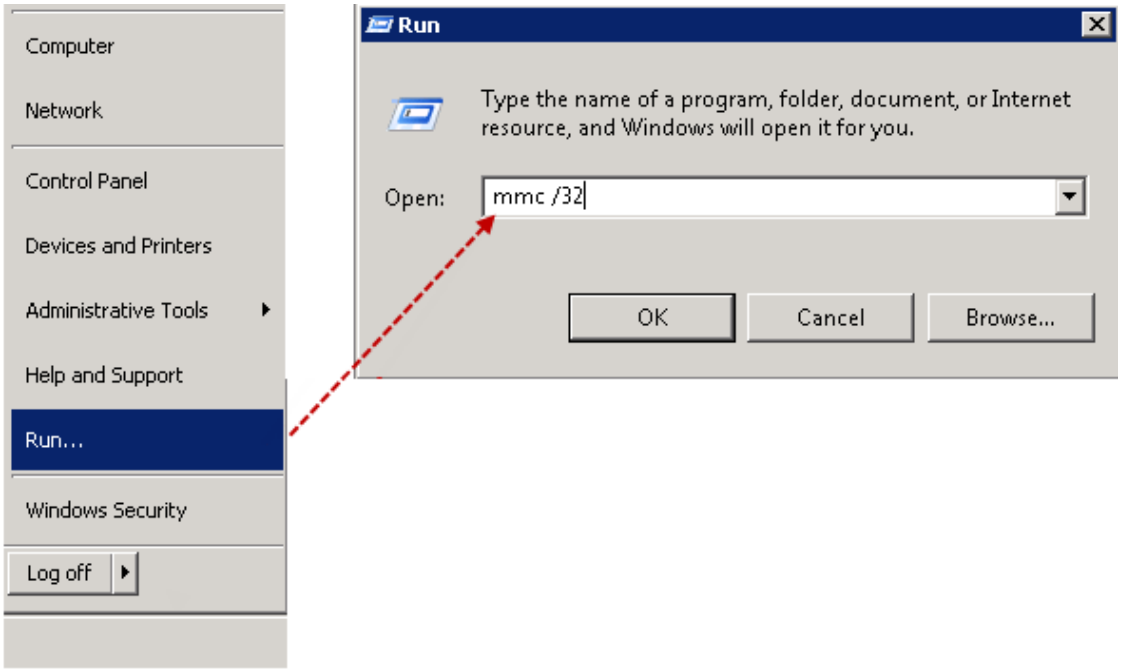
The installation of the System Management Display package creates a shortcut to a default console (*.msc)* file that can be launched from the following path:

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

5.2.2 Add the Node Administration Snap-In

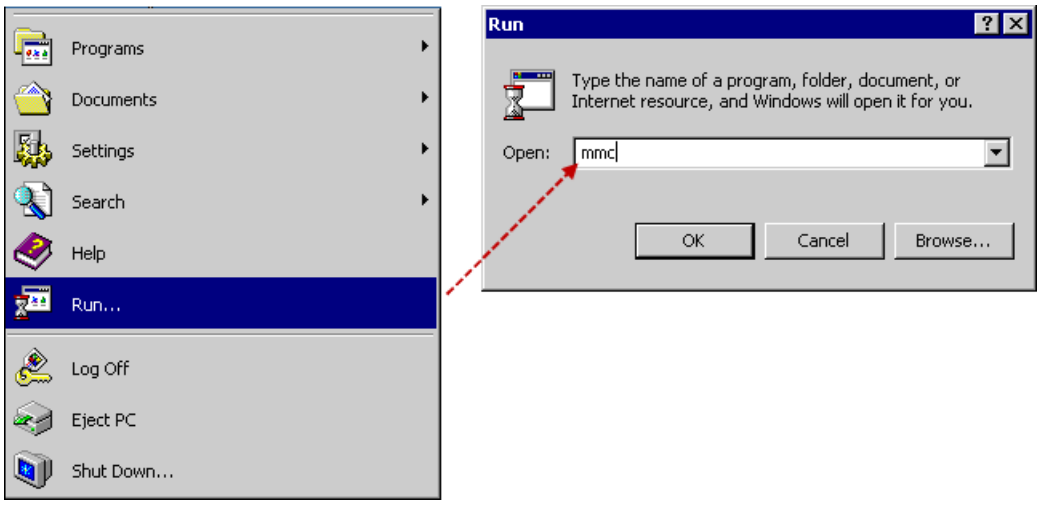
Users who have the Administrator access privileges can add the Node Administration Snap-in to the MMC using the following procedure. A default, empty Node Administration console file is installed in the \ProgramData\Honeywell\System Management directory during System Management Runtime installation and is accessible using the start menu.

1 For 64–bit operating systems, select **Run** from the **Start** menu and type "mmc /32" in the command line.



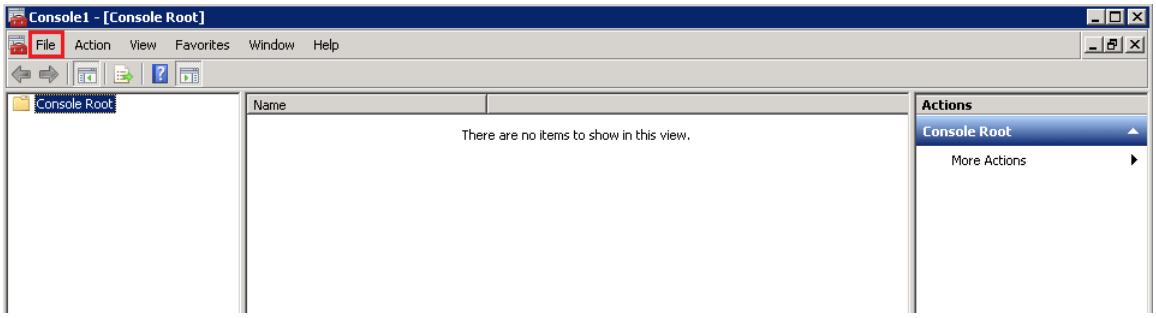
Note

For 32–bit operating systems, select **Run** from the **Start** menu and type "mmc" in the command line.

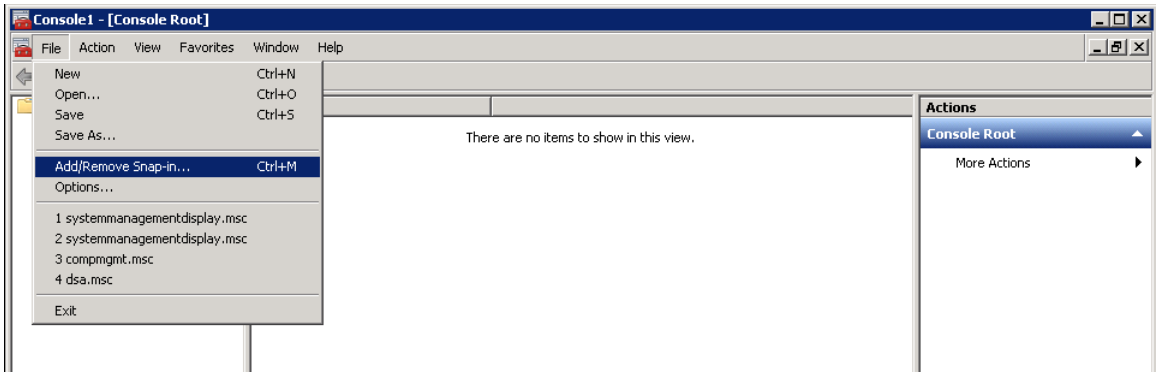


Result: The MMC console appears.

2 Choose File.

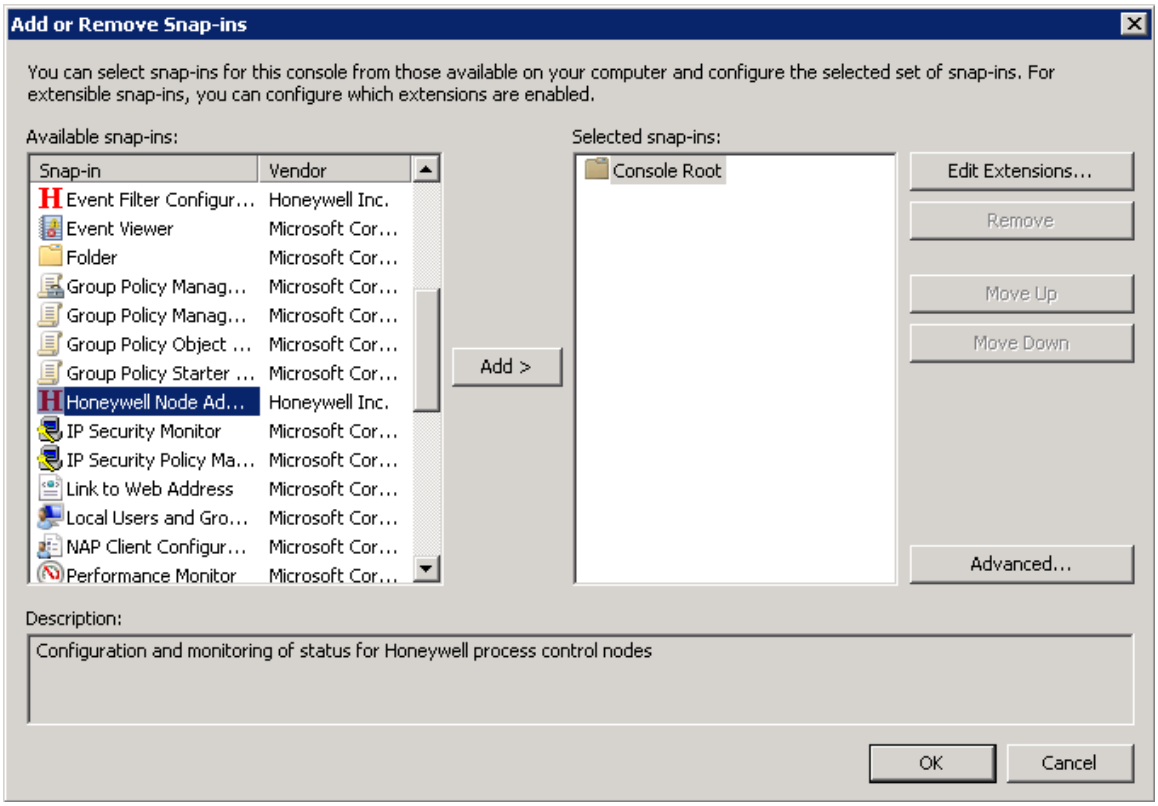


3 Select **Add/Remove Snap-in** command in the menu.

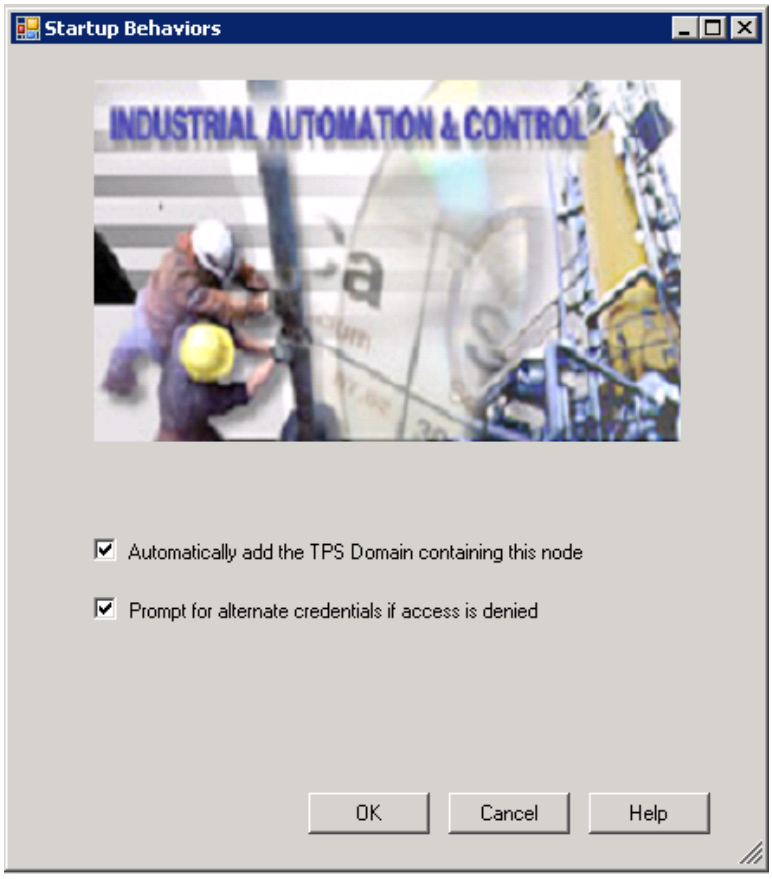


The Add or Remove Snap-ins dialog box appears.

4 Select the **Honeywell Node Administration** snap-in and then click **Add**.



A **Startup Behaviors** dialog box appears for the snap-in.

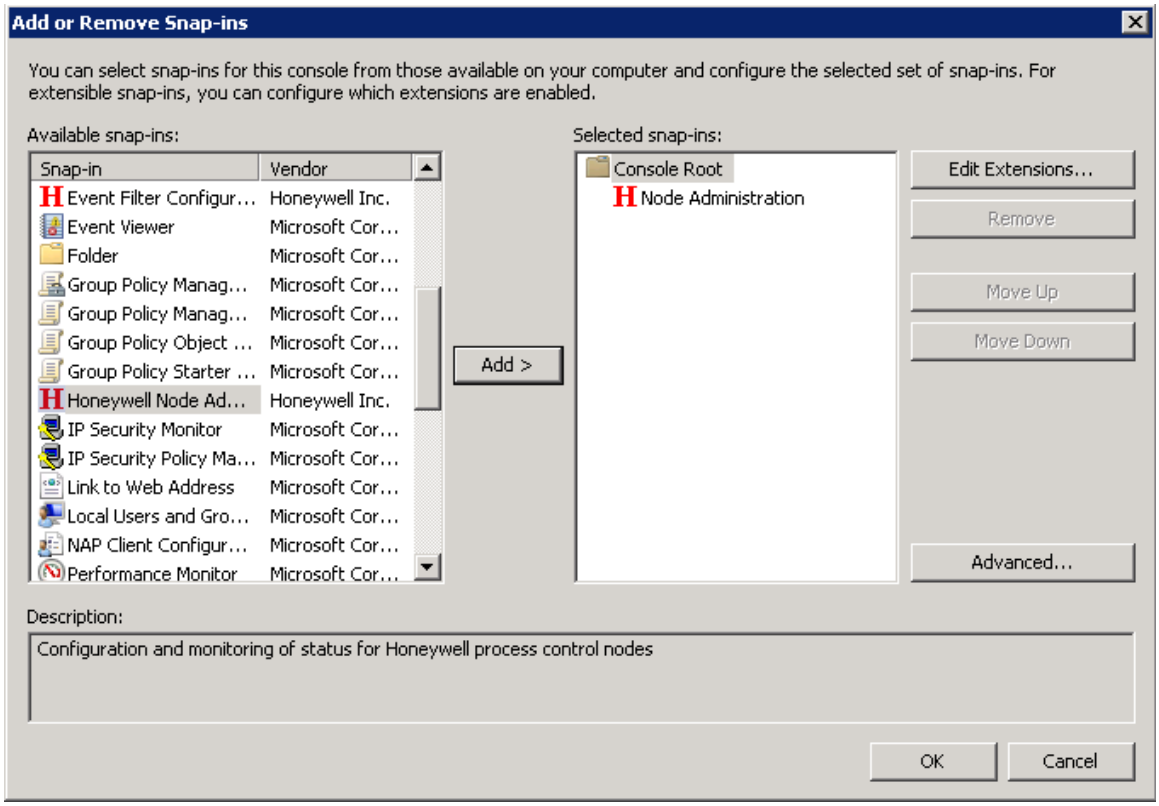


5 In the **Startup Behaviors** dialog box, the defaults are shown as selected.

- Review the default behaviors (you can always modify these properties later from the MMC), and click OK.

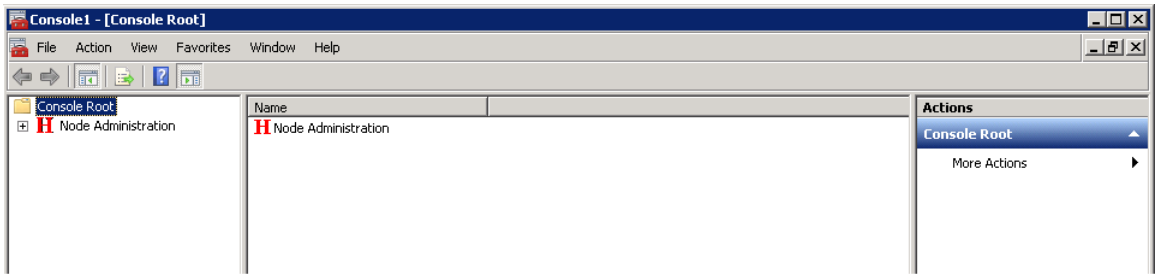
If you selected **Automatically add the TPS Domain containing this node**, the system automatically adds the domain that the node is in and the TPS domain and/or console to the System Management Display.

6 The Add or Remove Snap-ins dialog box appears with Honeywell Node Administration in its selection window.



7 Click **OK**.

Result: The Node Administration Snap-in appears in the MMC.



8 Save your console settings in the *ProgramData\Honeywell\System Management* directory if this console is to be accessed using the start menu shortcut. The console file may be saved to the user documents directory if this is a personalized configuration.

5.3 Node Administration Properties

5.3.1 Startup Behaviors Property Page

This section describes how to configure Node Administration properties. An example Node Administration Properties page appears in “Figure 3: Example Node Administration Properties Page” and “Table 6: Node Administration Properties” describes the function of each property (tab).

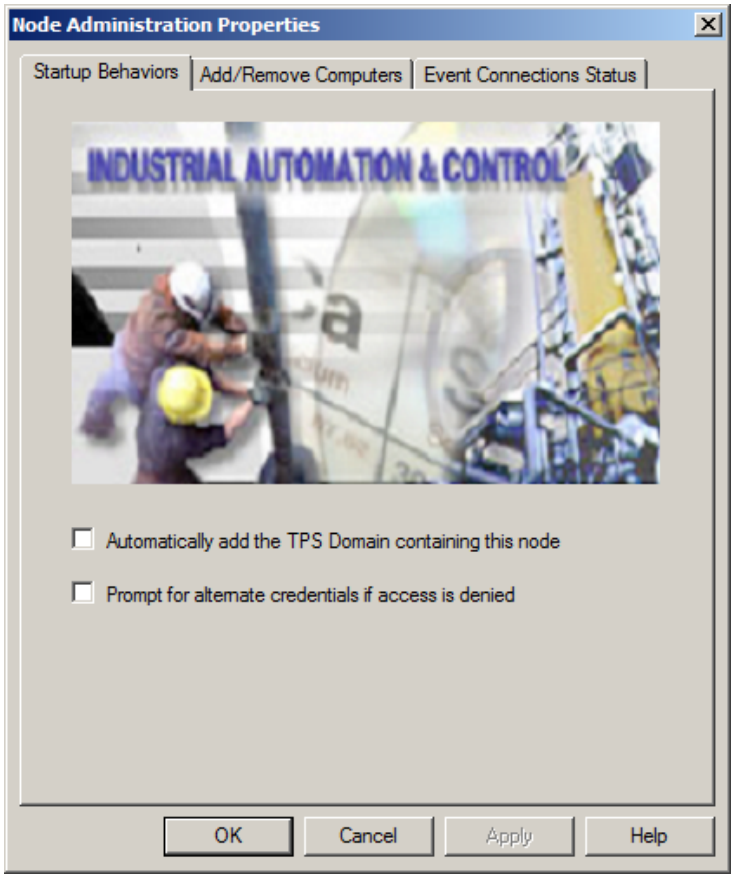


Figure 3: Example Node Administration Properties Page

Table 6: Node Administration Properties

Property (tab)	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/Remove Computers	In this page you can add/remove domains, organizational units and computers to the MMC console.
Event Connection Status	This page displays the computer name, IP Multicast Address and connection status of Multicast/ Heartbeat sources and system events sources.

Property (tab)	Description
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

5.4.1 Startup Behaviors defaults

Startup behaviors represent the initial behavior of the Node Administration Snap-in when the MMC is initiated. The behavior defaults are shown in “Figure 3: Example Node Administration Properties Page”. In most cases, you will accept the enabled defaults, and then enable other entries as needed.

5.4.2 Automatically add the TPS Domain behavior

If you:

- Enable the **Automatically add the TPS Domain containing this node** behavior and
- 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.

During startup, the active directory path of the local node is searched for a containing TPS Domain. The containing domain will be added automatically to the display, followed by the containing TPS Domain. The TPS Domain will automatically add any contained TPS Console organizational units or Computers.

5.4.3 Prompt for Alternate Credentials behavior

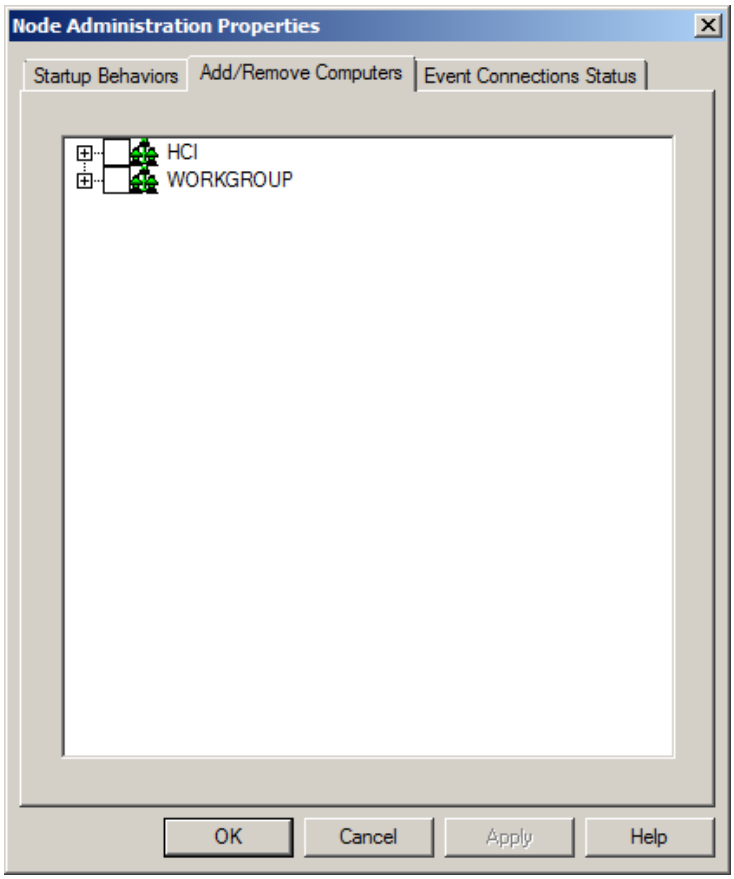
When you enable the Alternate Credentials behavior, it represents the enabling of a request for user id and password to allow access to a domain or component that the requesting user otherwise does not have.

If an access violation occurs when connecting to a remote computer, and this option is selected, the user will be prompted to enter alternate credentials for the connection. If the connection attempt with the specified credentials is successful, the credentials will be used for all subsequent accesses in the containing domain.

5.5 Add/Remove Computers

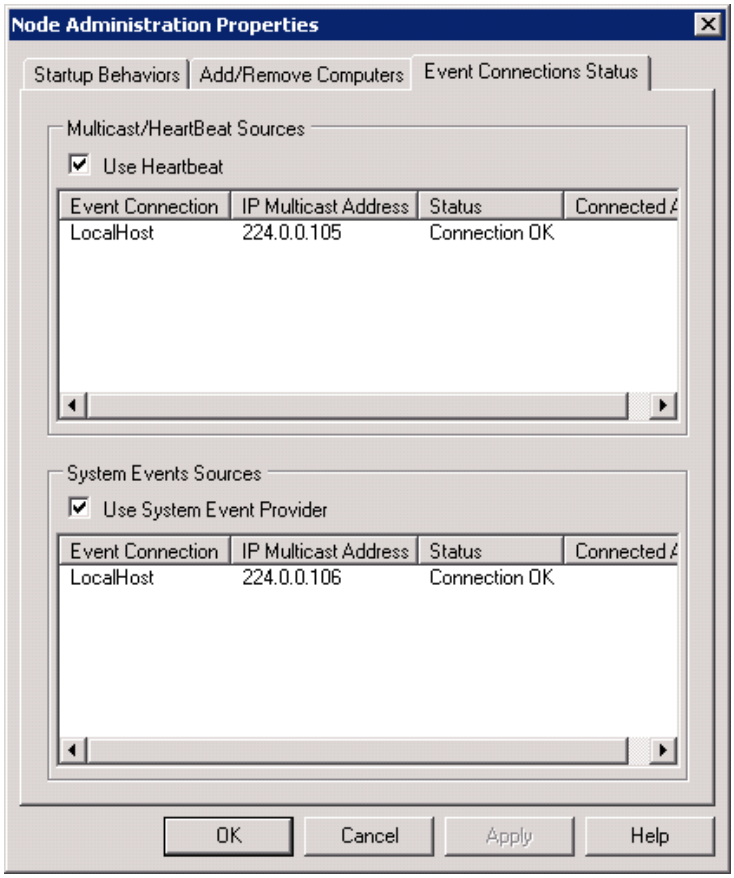
5.5.1 Select Computers to Display

Expand the domains, organizational units, and computers checking those that should be included in the display. TPS Domains that are selected will automatically be expanded to include all contained computers at run-time. Organizational Units not flagged as TPS Domains have no function other than organization. Contained computers must be added/removed manually using the browse tree.



5.6 Event Connection Status

The Event Connection Status page provides a list of all Event Connections being maintained by the System Management Display snap-in and their current status. Checkboxes enable/disable the use of the Heartbeat or System Event connections.



5.6.1 Multicast/Heartbeat Sources Use Heartbeat option

When enabled, the connections listed are used for determining whether the remote computers are currently on-line. If heartbeats (FTE diagnostic messages) are being received on the connection from a remote computer, it is considered on-line. If no messages are received for the disjoin period (defaults to 3 seconds) then the remote computer status will be displayed as off-line. When a computer is off-line, no DCOM connection attempt is made. When a computer status changes to on-line a new connection to that computer is made.

Disabling this option will cause the snap-in to consider all configured computers as on-line and a DCOM connection will be attempted to each one. This process can take an extended period to determine that a remote computer is off-line. This mode should only be used to help in troubleshooting the system. Generally, this will only be useful if either the local or remote node FTE settings have not been configured correctly.

The connections listed are configured in the properties of the computers added to the display in the Event Connection Options property page. The local node connection is always configured by default. Use the computer *Event Connection Options* property page \ *Used as Multicast/Heartbeat Source* option to add a high availability node, usually a server, in the remote community to enable heartbeat detection across communities.

5.6.2 System Events Sources Use System Event Provider option

When enabled, system events are gathered on the listed connections.

The connections listed are configured in the properties of the computers added to the display in the Event Connection Options property page. The local node connection is always configured by default.

System Event collection scope (Synchronized Repository scope) is normally configured to be the same as the contained Experion cluster. Each Experion cluster is normally configured with a different IP Multicast address segmenting event collection for the Experion system at the cluster level.

To view the events from another cluster, select a computer in the remote cluster as an event source in the computer properties. Use the computer *Event Connection Options* property page *Used as System Event Source* option to add a high availability node, usually a server, in the remote cluster to enable collection of system event across clusters.

Disable this option if the collection of system events is not needed or is interfering with status display performance. This would be a rare condition.

5.7 Multicast Communications Purpose

5.7.1 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 uses IP Multicast to process information between nodes. Multicast must be enabled on all network switches that interconnect participating nodes.

Overview example 1

"Figure 4: Nodes within the same Multicast Scope" shows all nodes within the same IP Multicast Group using the same synchronized repository for name service and system event provider.

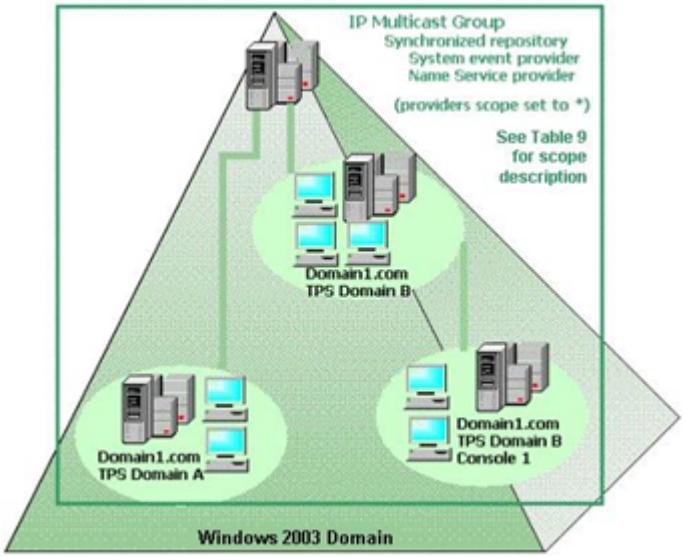


Figure 4: Nodes within the same Multicast Scope

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.

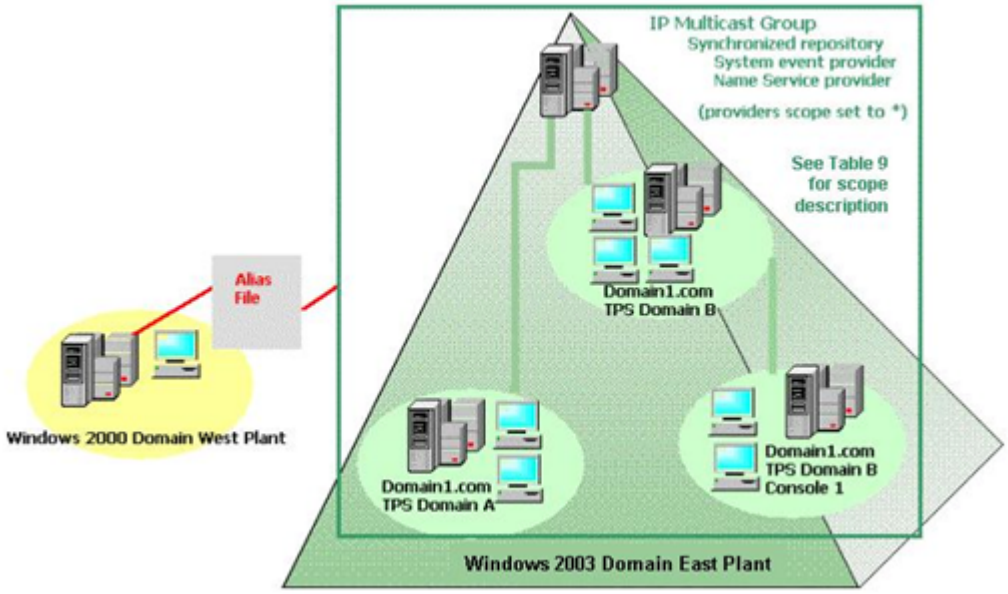


Figure 5: Nodes outside of an IP Multicast Group

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.

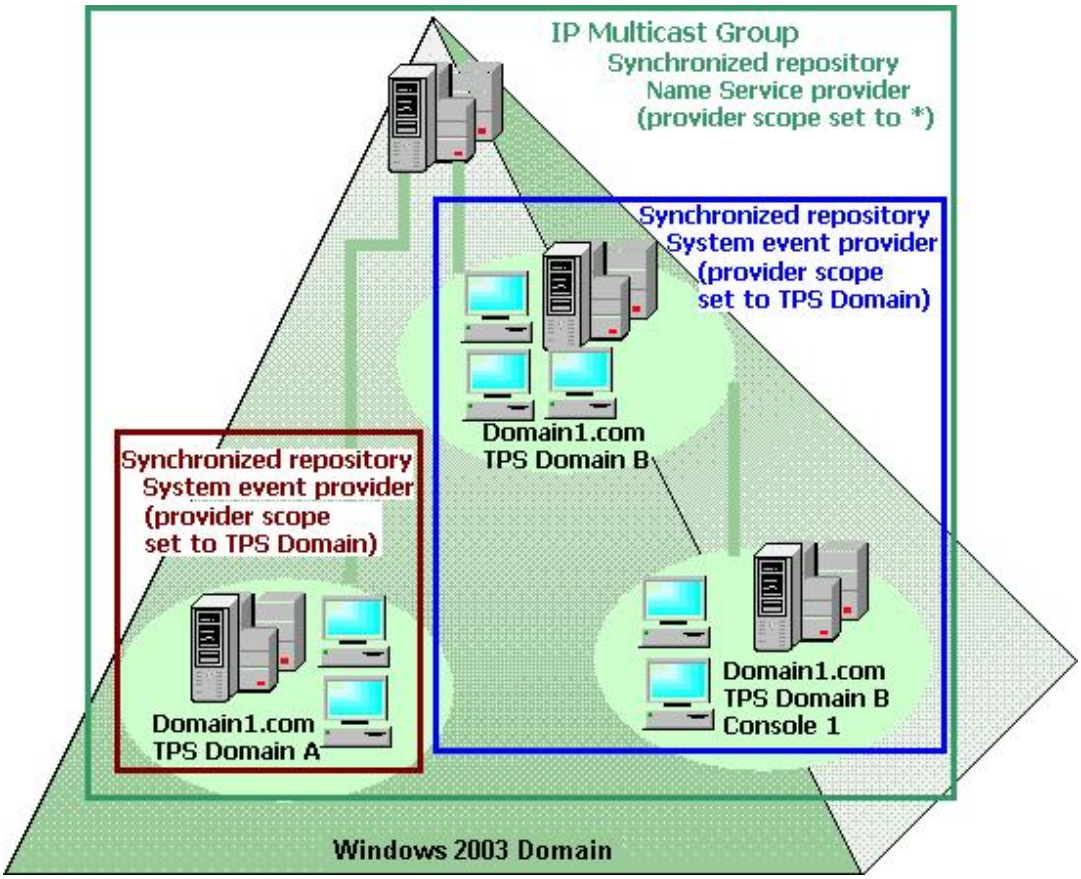


Figure 6: Variation of nodes within the same IP Multicast Group

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

5.8 Multicast Heartbeat Settings

5.8.1 Multicast/Heartbeat Settings Property Page

This page lets 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.

5.8.2 Heartbeat settings description

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

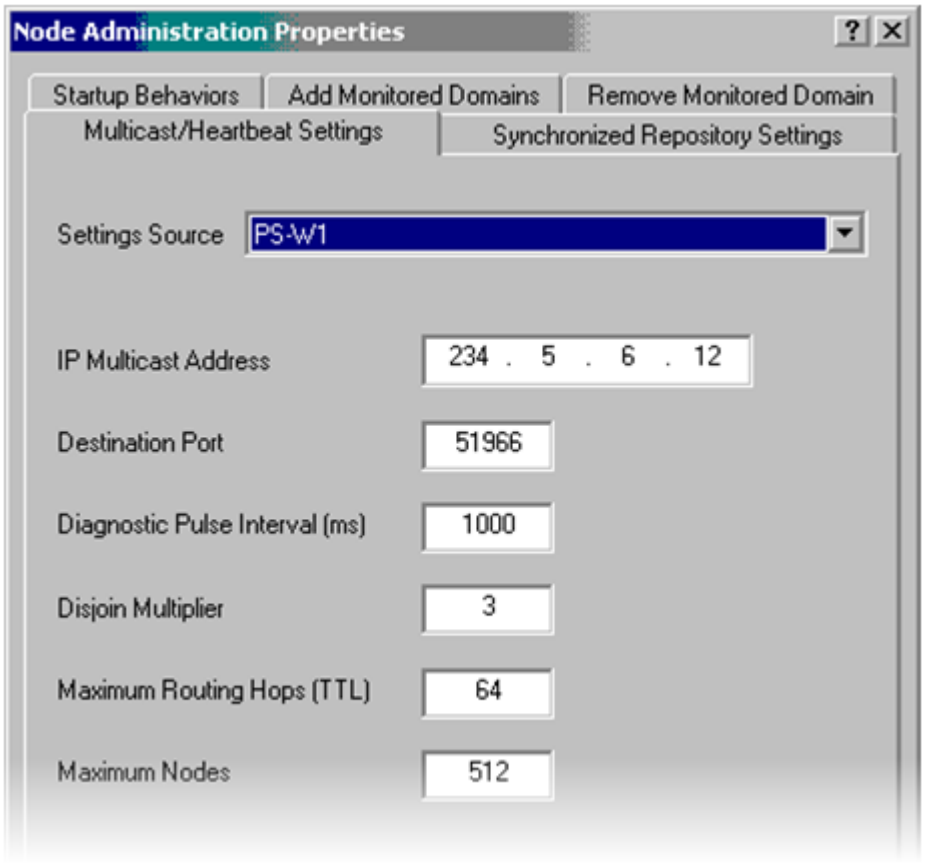


Figure 7: Heartbeat Settings

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

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 **Properties** from the context menu, the changes made on the Multicast/ Heartbeat settings page will be applied to all computers contained by the domain item selected.

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 if there are unavailable nodes in the selected group.

5.8.4 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 7: Description of Multicast/Heartbeat Settings" describes each of the settings in the *Multicast/Heartbeat Settings* property page.

Table 7: 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

5.9.1 Synchronized Repository Settings Property Page

From this page you configure the communication between synchronized repository nodes. Only members of the Product Administrators group may change values on this page.

5.9.2 Synchronized Repository Settings example

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

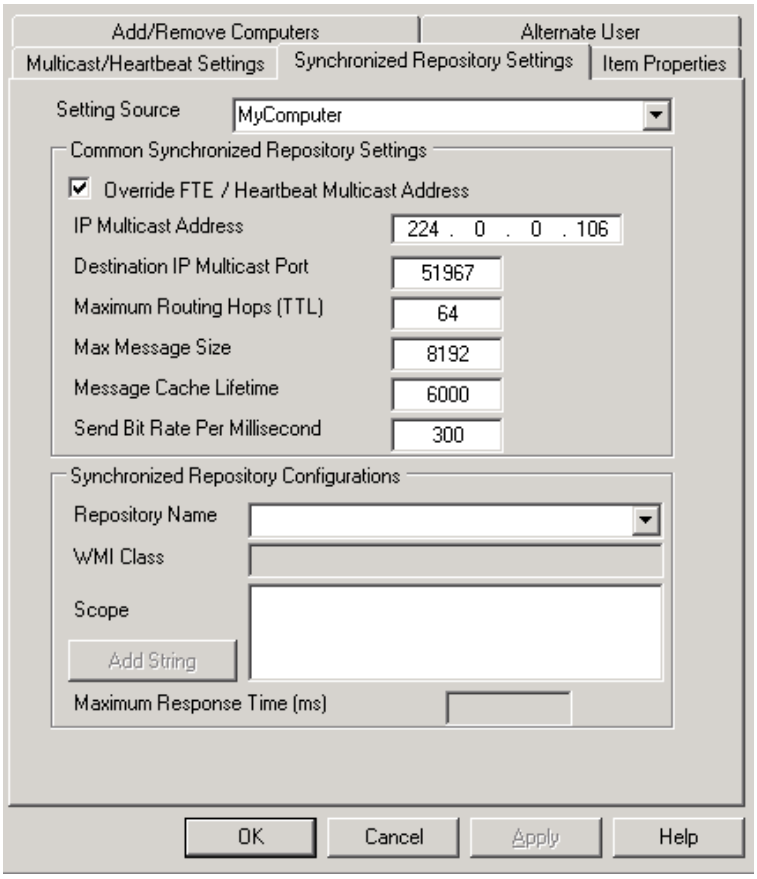


Figure 8: Synchronized Repository Settings Property Page

5.9.3 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).

5.9.4 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 8: Values for Common Synchronized Repository Settings” shows values for Common Synchronized Repository Settings.

Table 8: Values for Common Synchronized Repository Settings

Value	Description
Override FTE / Heartbeat Multicast Address	Check this to use an IP Multicast Address different than the default FTE multicast address. ALWAYS select this option and enter an IP Multicast address that is different from the FTE IP Multicast address in use.
IP Multicast Address	The IP Multicast Address to use for the synchronized repository provider (SRP).
Destination IP Multicast Port	UDP destination port for all synchronized repository messages. The IP multicast address specified above 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.
Send Bit Rate per millisecond	Throttles multicast sends to the specified maximum bit rate.

5.9.5 Synchronized Repository Configurations information

Attention

Although this method of limiting synchronization scope continues to be supported, it is no longer the primary method of segmenting synchronization scope. Use the Synchronized Repository IP Multicast Address to assign a different address to each synchronized repository multicast group. Use the default scope strings.

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 9: Synchronized Repository Configurations Description” shows information about Synchronized Repository Configurations.

Table 9: 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: **Domain**: The domain containing this computer. T**PSDomain**: The organizational unit containing this computer that is marked as a TPS Domain. Workgroups will resolve this value to the workgroup name. **Console**: The organizational unit containing this computer that is marked as a console. 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.

5.9.6 Selecting a Source of Settings to be Viewed / Modified

The *Settings Source* 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.

5.9.7 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**.**

5.9.8 Reserved Scope Values

To simplify scope setting and installation, use reserved scope values when defining the synchronization scope of a provider. “Table 10: Reserved Synchronization Scope Values” describes possible reserved scope values.

Table 10: 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.

5.9.9 System Management Provider Default Scope Values

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

Table 11: 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 that 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 - Preferred

5.10.1 General Guidance

Use the Synchronized Repository IP Multicast Address to define the synchronized repository scope. This IP Multicast Address should always be selected as different from the FTE / heartbeat multicast address. In all cases leave the **Override FTE / Heartbeat Multicast Address** option checked.

Configuration of Synchronization Scope depends on several factors including:

- FTE community configuration
- Experion system DSA configuration
- Physical network topology

The configuration selected will also impact:

- System Event Server installation/configuration
- FTE Filter file usage (SES server specific configuration)
- HCI Name Service replication of local component configurations
- System Management Display configuration

Tip

System Management Multicasts allows multiple System Managements to be configured on the same FTE multicast so that they operate exclusive to each other. It is recommended to configure separate System Management Multicast addresses for each cluster server so that an SES can be installed on each server. You can also select an appropriate SES alarm scope for your system with this configuration.

For more information, please refer to Server and Client Configuration Guide.

5.10.2 Single Experion Server, Single FTE Community

- Use the default Synchronized Repository IP Multicast Address.
- SES is installed and configured on the Experion Server (pair).
- Include FTE events in SES Server Specific configuration on Server (pair).

5.10.3 Multiple Experion Server clusters, DSA Notifications enabled, Single FTE Community

- Identify a server that will collect events from each node in the system. Some nodes will be loosely associated with a server, but need to be configured into a synchronized repository community that can collect their system events. Configure the Synchronized Repository IP Multicast Address for each node so that it matches the unique IP Multicast address assigned to the server.

Tip

Organize the system Active Directory so that Experion Servers and their associated computers are organized in an OU. Use the Synchronized Repository Settings page in the Organization Unity properties to configure all contained computers at one time.

- Identify one server (pair) that will collect FTE alarms. Configure the SES on each server - including FTE events on the server(s) identified and disabling the option on all others.
- In the System Management Display, by default, only the events from the local synchronized repository will be displayed. To see events from other communities, select Properties on a high availability node in each remote community and turn on the *Event Connection Options -> Used as System Event Source* option. Save the console once all event sources have been configured.

5.10.4 Multiple Experion Server clusters, DSA Notifications disabled, Single FTE Community - All system events seen by each Experion Server

- Configure each server as though it is the only server. See “Single Experion Server, Single FTE Community” on page 46, above.
- Configure all computers with the same synchronized repository IP Multicast address.

Tip

Organize the system Active Directory so that Experion Servers and their associated computers are organized in an OU. Use the Synchronized Repository Settings page in the Organization Unity properties to configure all contained computers at one time.

5.10.5 Multiple Experion Server clusters, DSA Notifications disabled, Single FTE Community - Only system events for associated computers are seen by each Experion Server

- Configure each server as though it is the only server. See “Single Experion Server, Single FTE Community” on page 46, above.
- Configure the computers in each cluster with different synchronized repository IP Multicast addresses.

Tip

Organize the system Active Directory so that Experion Servers and their associated computers are organized in an OU. Use the Synchronized Repository Settings page in the Organization Unity properties to configure all contained computers at one time.

- In the System Management Display, by default, only the events from the local synchronized repository will be displayed. To see events from other communities, select Properties on a high availability node in each remote community and turn on the *Event Connection Options -> Used as System Event Source* option. Save the console once all event sources have been configured.

5.10.6 Multiple FTE Communities

Configure the servers and synchronized repository groups as described above. In addition:

- In System Management Display - select a high availability node in the remote FTE community that will provide heartbeat status for the remote FTE community. From the remote computer's property page *Event Connection Options,*select the *Used as Multicast/Heartbeat Source* option. Save the console once the event sources have been configured.

5.11 Synchronization Scope Scenarios - Deprecated

5.11.1 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.

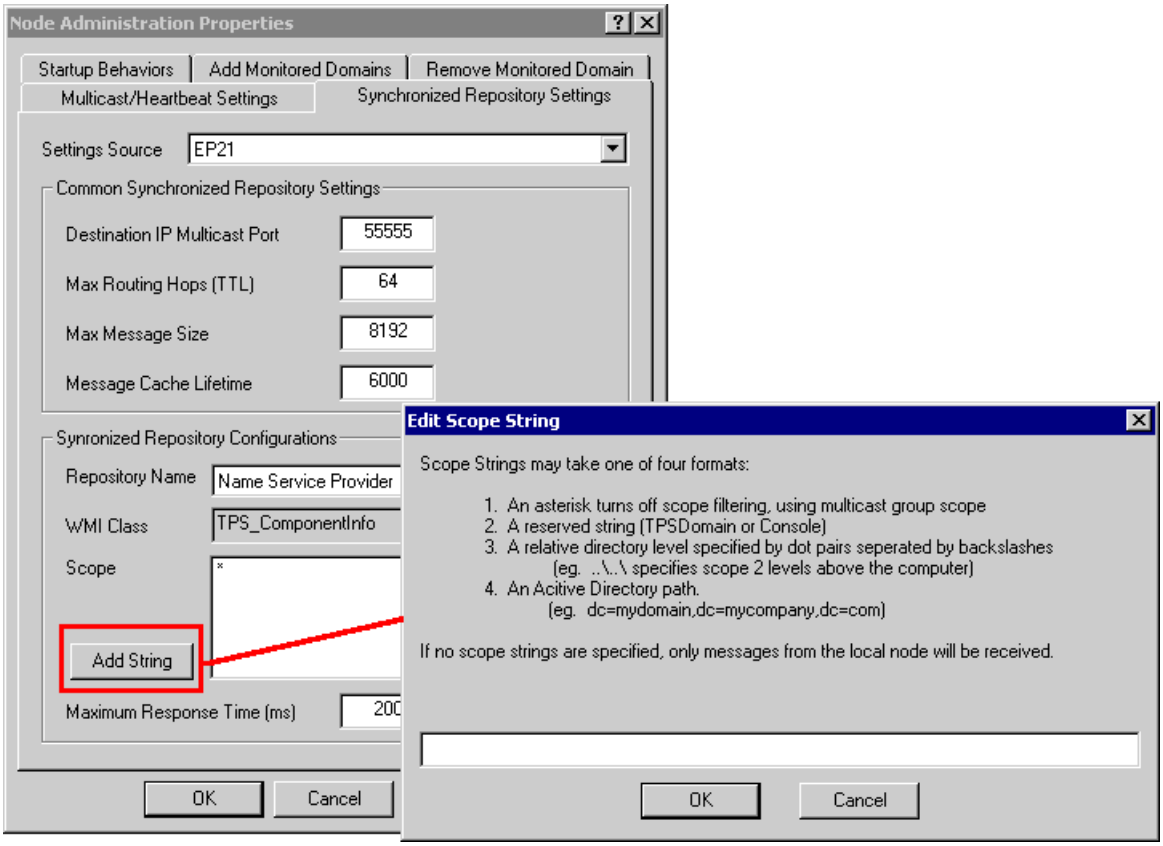


Figure 9: Edit Scope String Dialog Box

5.11.2 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.

5.11.3 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.

5.11.4 Modifying current scope configuration for setting multiple scope values

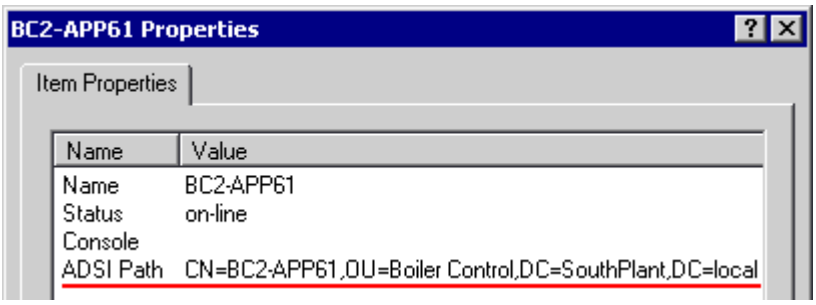
1. From the **Synchronized Repository Settings Property Page**, double-click the name of the current repository name in the **Repository Name** list box.
2. The **Edit Scope String**window appears. Delete the entry from the edit box in this window.
3. Add the following string commands in UNC format:
   First value: *DC=Domain1,DC=MyCompany,DC=com*

   Second Value: *DC=Domain2,DC=MyCompany,DC=com*

   Where the first and second values are from your system.

   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.

   Tip
   To help 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.



4. Click **OK**.

5.11.5 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.

5.11.6 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 by the selected domain object.

5.11.7 Applying changes to settings

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 do 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 if there are unavailable nodes in the selection group.

5.12 Managing Organizational Units and Computers

5.12.1 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.

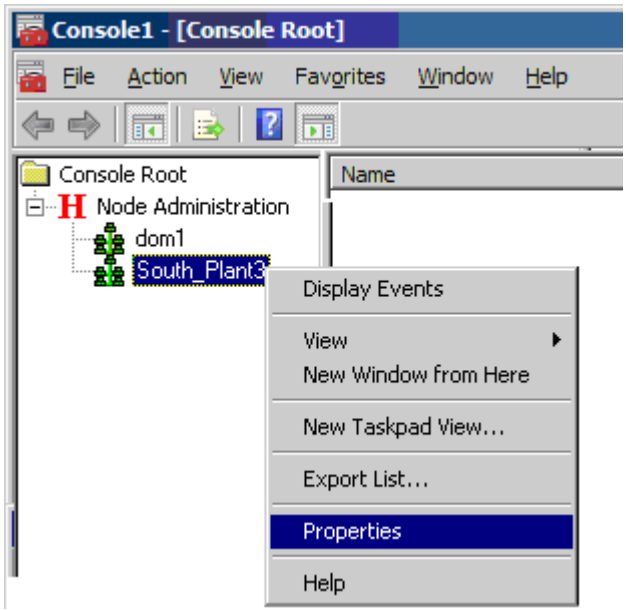
5.12.2 Adding a Managed OU to a Monitored Domain

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

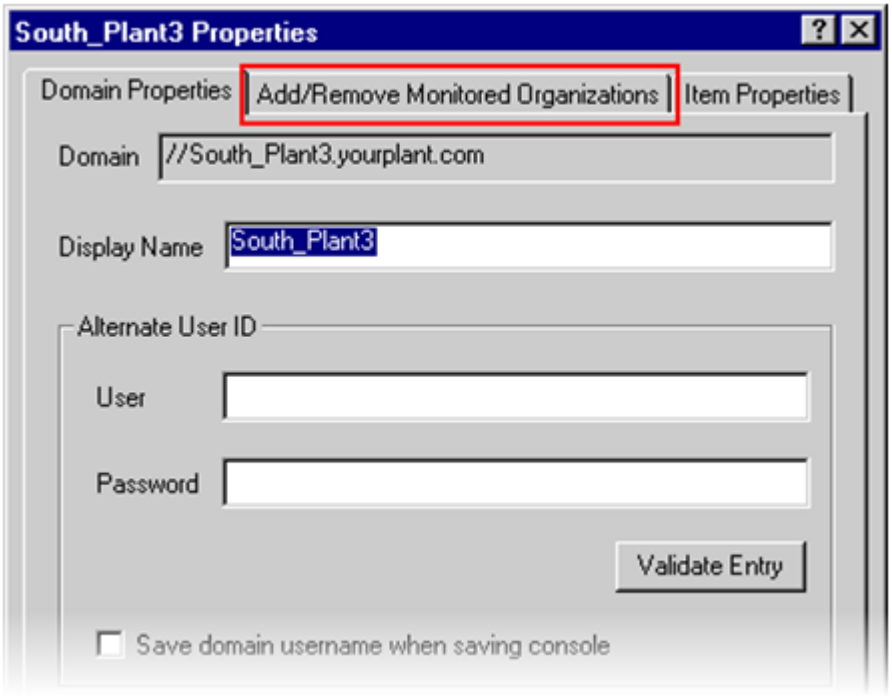
This procedure assumes that Organizational Units (OUs) such as TPS Domains have been created and that you are aware of which domains already contain an OU such as a TPS Domain. If you do not know which of your plant's domains contain TPS Domains, you can always browse for OUs from the domain's **Properties**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

1 From the MMC scope pane, right-click a domain that contains a TPS Domain and then select **Properties** from the menu.



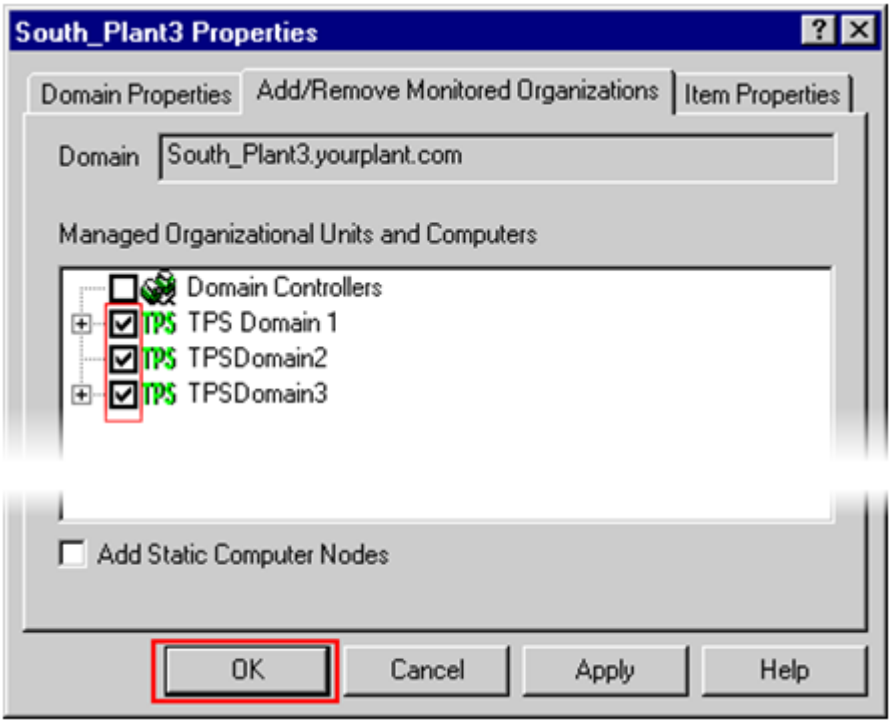
Result: The selected domain's **Properties**dialog box appears.

2 From the domain's **Properties** dialog box, select the **Add/Remove Monitored Organizations** tab.

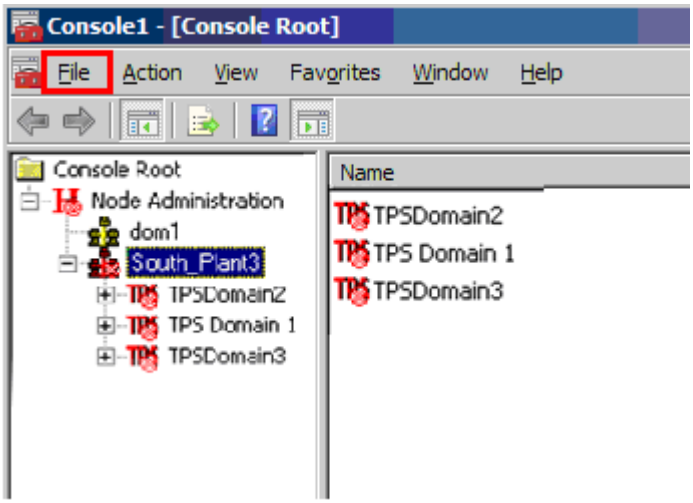


Result: The monitored organizations appear in the selection window of the **Add/Remove Monitored Organizations** tab.

3 Check the TPS Domain(s) you want to manage. In this example, three TPS Domains are selected as managed OUs. Click **OK**.



4 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.



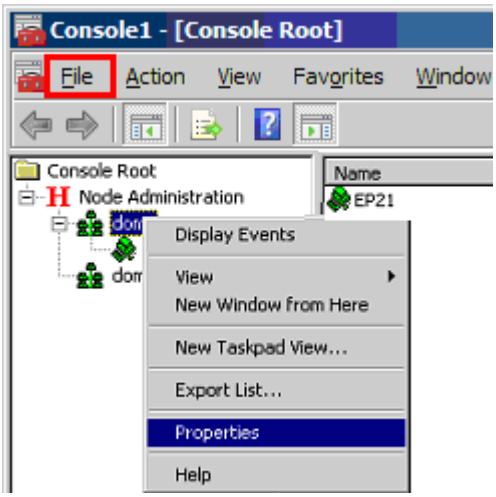
5.12.3 Adding a Computer as Managed item

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

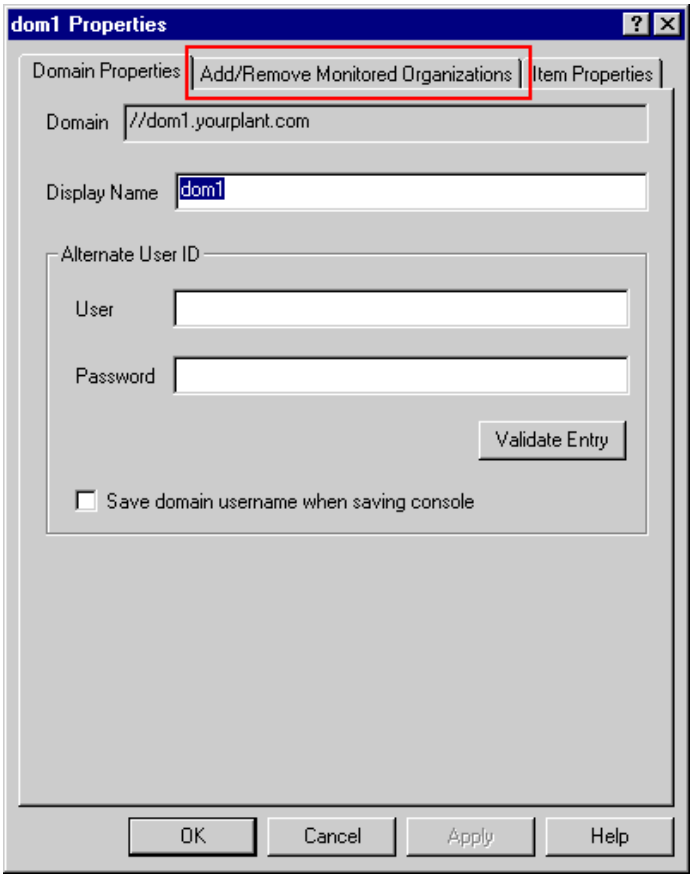
This procedure assumes you are aware of which domain contains the desired computer. If you do not know which of your plant's domains contain the desired computer, you can always browse for the computer from the domain's **Properties** tab.

1 From the MMC scope pane, right click a domain that contains the computer of interest and select **Properties** from the menu.



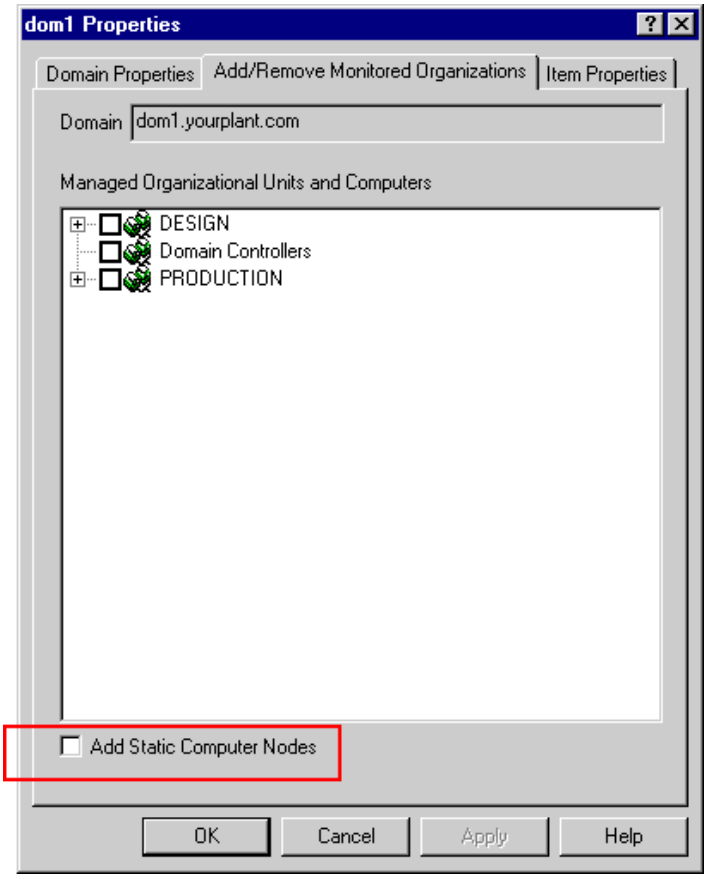
Result: The selected domain's **Properties** dialog box appears.

2 From the **Domain Properties** dialog box, select the **Add/Remove Monitored Organizations**tab.



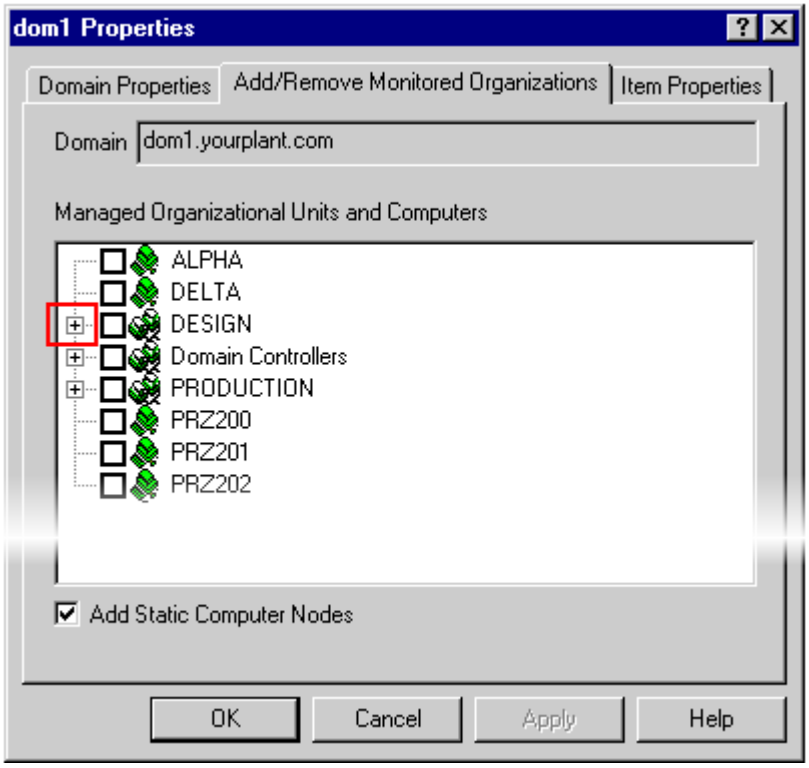
Result: The monitored organizations appear in the selection window of the **Add/Remove Monitored Organizations**tab.

3 Check the **Add Static Computers** checkbox so that you can browse to the computer(s) of interest.

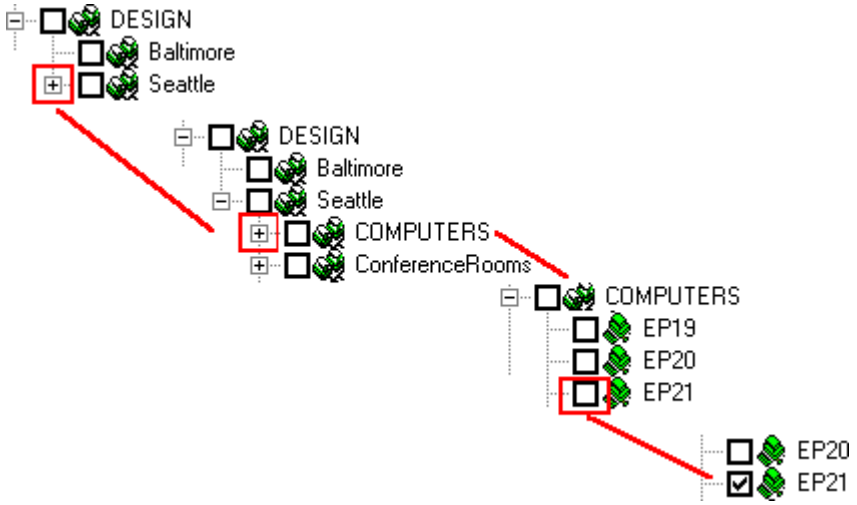


Result: The selection window refreshes to include computers that are not members of a Managed Organizational Unit.

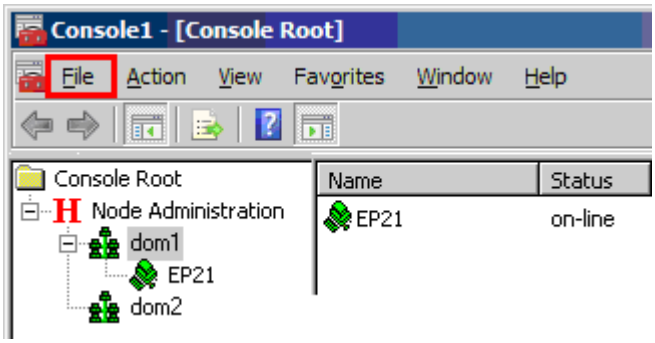
4 From the updated selection window, expand the domain's tree view to locate the computer of interest. In this example, the computer of interest resides in the domain named 'DESIGN.' It is not necessary to click the checkbox of the domain (otherwise you would be monitoring all the computers in that domain),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



5 Continue to expand the view until you locate the computer of interest. Click the checkbox for the computer of interest then click **OK**.



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.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Node Administration
dom1
EP21
dom2
Name
Status
EP21
on-line

5.13 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

5.13.1 Additional references for managing a component

Type of component	Reference
TPN Server	*TPN Server User's Guide*
Redirection Manager (RDM)	' “About Redirection Manager” on page 59' *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	' “Supporting System Event Server” on page 85'
System Performance Server	' “Supporting System Performance Server” on page 109'
HCI Components	' “Using the HCI Component Configuration Page” on page 62'

5.14 About Monitored Components

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

5.14.1 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*.

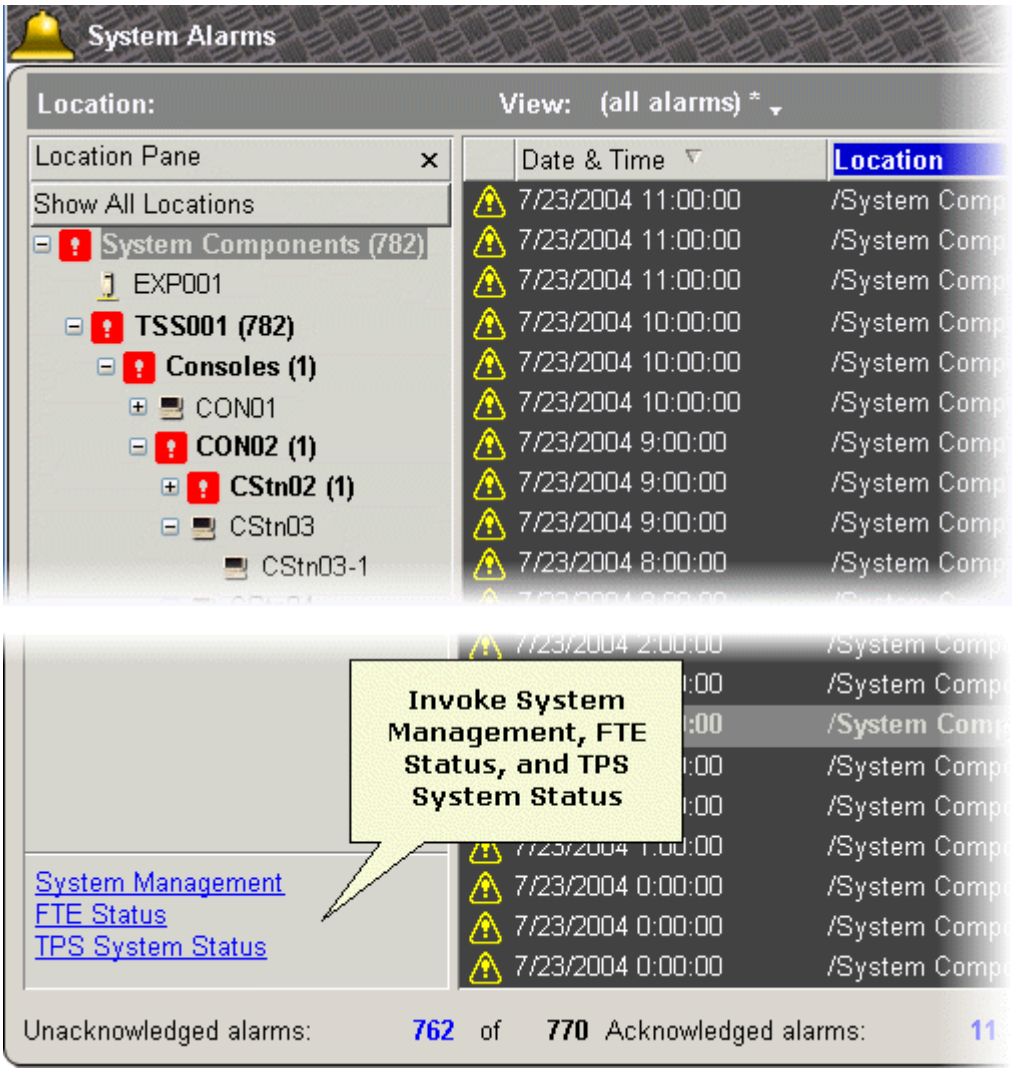
5.14.2 How Redirection Manager uses monitored components

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.

5.15 Invoking from Experion System Status

5.15.1 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.



6 Configuring HCI/OPC Components

6.1 Using the HCI Component Configuration Page

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).

6.1.1 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.

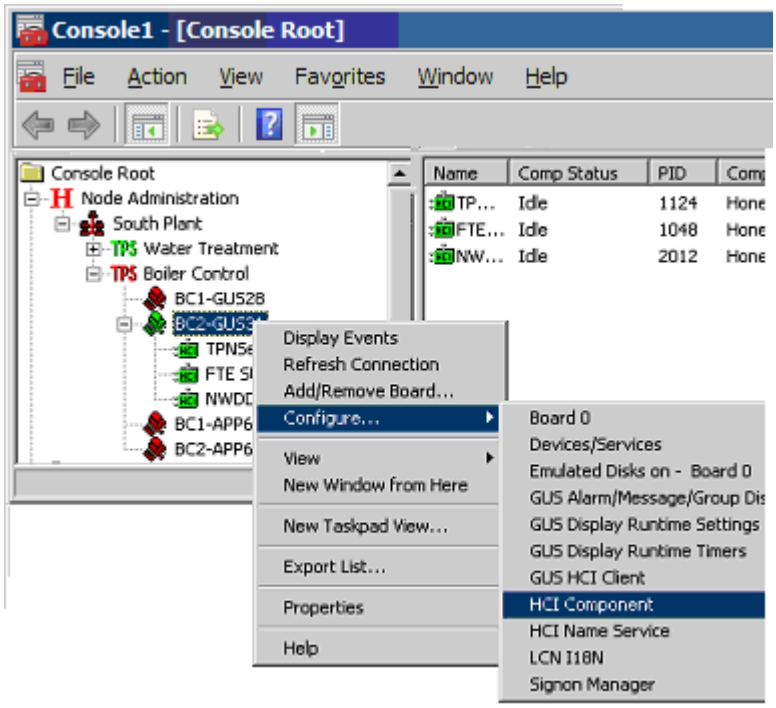
HCI Component Configuration operates within the System Management Display implemented as a Microsoft Management Console (MMC) Snap-in. It has a hierarchical view of computer and managed component status.

6.1.2 Configuring an HCI component

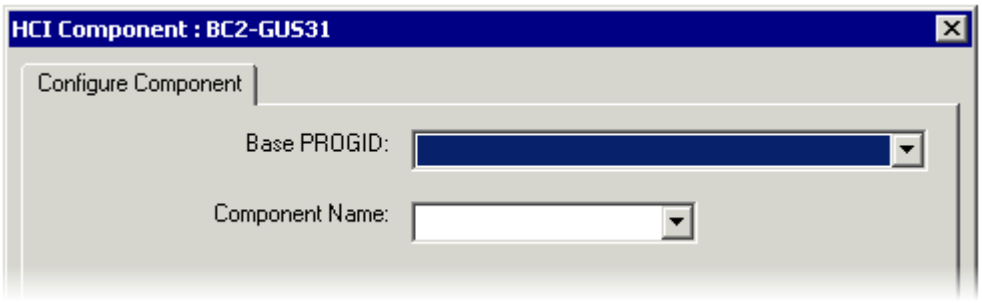
Follow these steps to configure an HCI component.

1 From the System Management Display, right-click the computer item.

2 Select **Configure** and then **HCI Component** from the menus.
Result: The configuration page appears.



3 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.



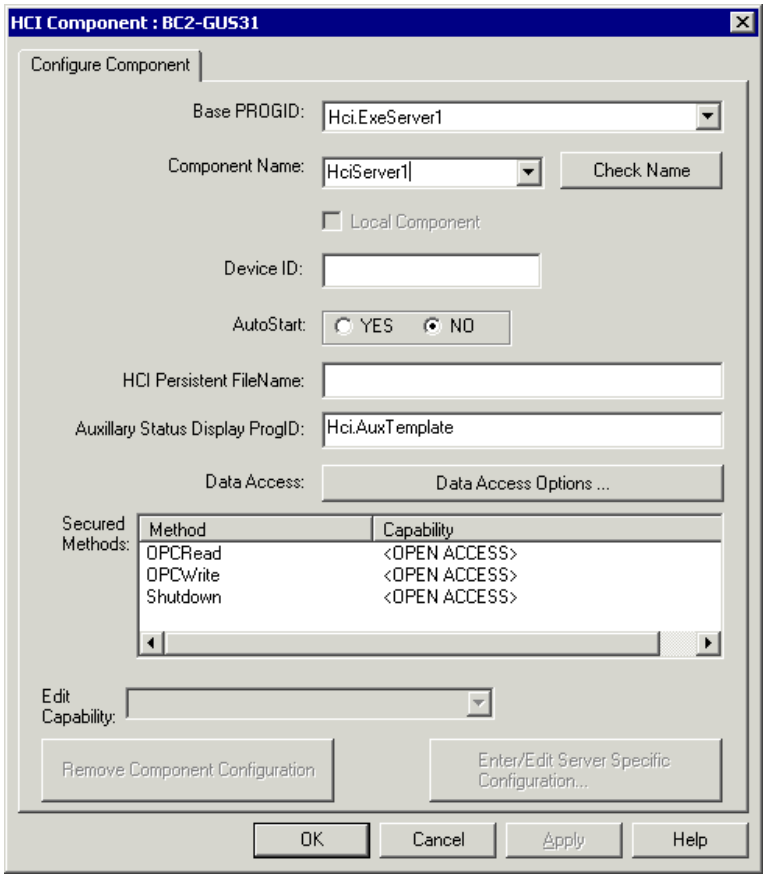
Result: The **Configuration** property sheet appears.

4 Click the edit combo box of the **Component Name**, and then type the name.

Result: The **Check Name** button appears. After verifying the component name, the system enables the **Apply** button.

After information is saved to the registry, this base component will no longer be in the list of the base PROGID for the next new configuration.

5 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.



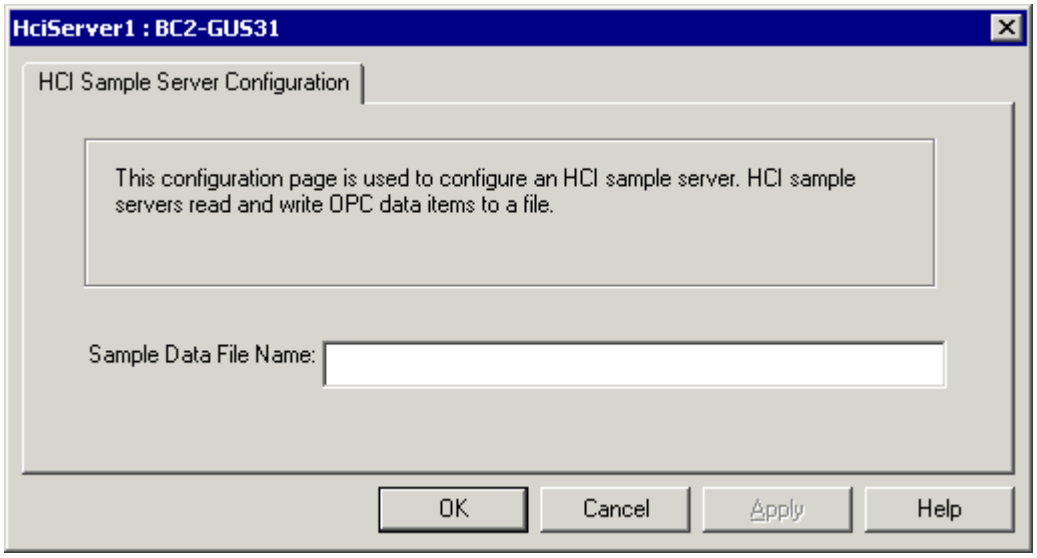
The **Check Name** button is enabled after you enter the component name. If you are configuring a third-party OPC server, you must check the **Local Component** field prior to clicking **Check Name**. (**Check Name** must know the component type before verifying its name).

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.

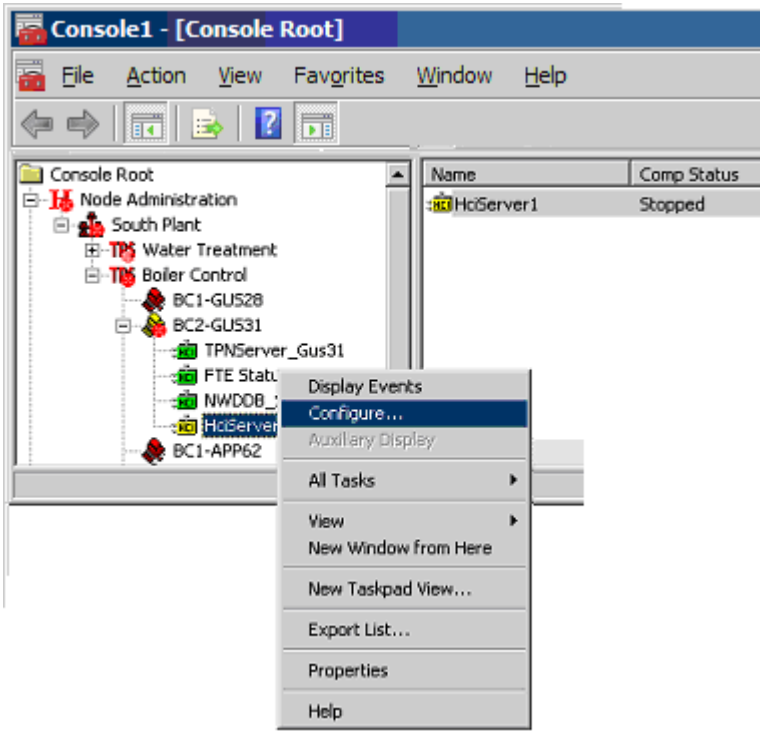
Clients anywhere in the domain can access unchecked components.

6 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.

The following figure displays the Device-Specific Server configuration page.



7 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.

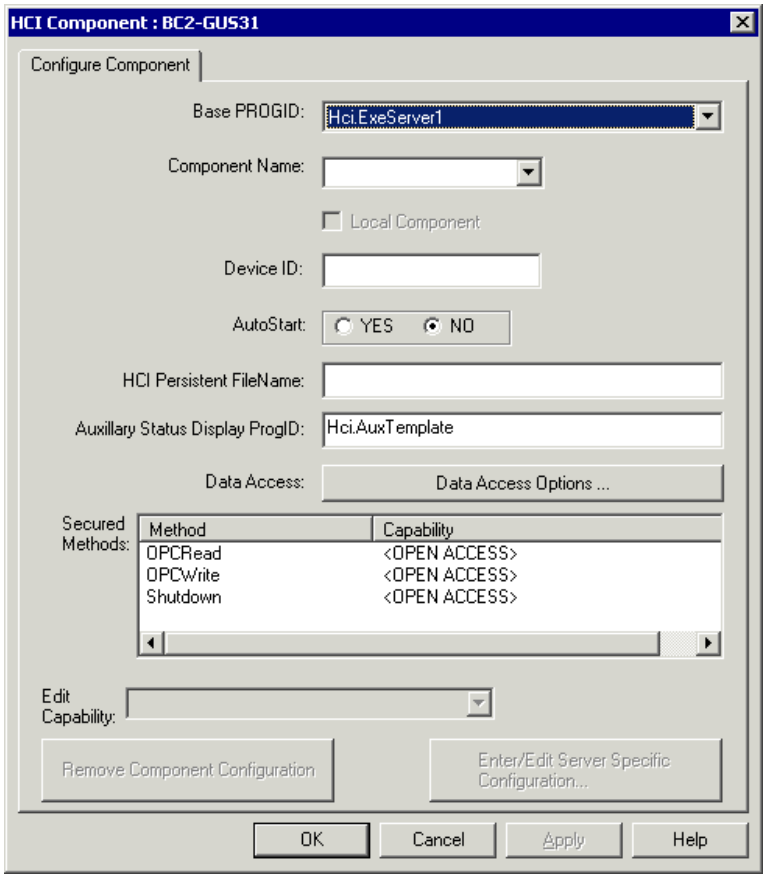


6.1.3 Reconfiguring an HCI component

Follow these steps to re-configure an HCI component.

1 Perform steps 1 through 4 as in the previous “Configuring an HCI component” on page 62 procedure.

2 Click the down arrow button on the edit combo box of the **Component Name** to get a list of pre-configured components. HCI/OPC component configuration reads from the registry of the host node.



3 Modify the properties of interest.

4 Click **OK**. All applied updates are written to the registry of the host node.

6.1.4 Removing an HCI component

Follow these steps to remove an HCI component.

1 Do steps 1 thru 4 in the previous ' “Configuring an HCI component” on page 62' procedure.

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 **Remove Component Configuration** to remove an HCI component configuration.

6.1.5 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.

6.1.6 Configuring a new HCI Server

Step 5 in ' “Configuring an HCI component” on page 62' 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.

6.1.7 New configuration vs. re-configuration

“Table 12: Descriptions of Fields/Buttons of the HCI Component Page” identifies each field or button on the HCI Component page with a description of its initial value and usage.

Table 12: 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. For re-configurations, select the component from the list. 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.
AutoStart	A **Yes** value indicates CAS should start that component when the node starts up. This field is valid only for TPS managed components. See the *TPN Server User's Guide* 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.

Field/Button	Description	Initialized Value	Enabled/Visible
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.
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.
Secured Methods	A list of methods that can be associated with a capability. Proxy's files with ACLs represent capabilities. *Shutdown/Start method:* 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. 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 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. 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. 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.
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 cannot be cancelled.
Help	On-line help.		Always visible and enabled.

6.1.8 Data Access Options

OPC Servers may set several I/O options via the **Data Access Options** button on the component configuration page. There are four data access options as shown in “Figure 10: Data Access Configuration Page”.

Maximum Threads Per Group

- 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 value.

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.

Time Threshold

- 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 to 10,000 milliseconds. If the polling thread has not made an update within the specified time period, then a background device read is issued.

Single Scan Per Data

- 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.

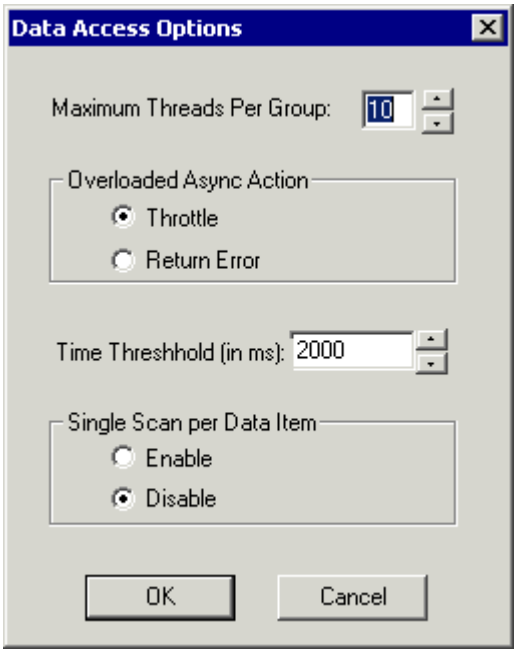


Figure 10: Data Access Configuration Page

6.1.9 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 (shown in "Figure 11: Listing of Secured Methods and Capabilities") to display the pull-down list of capabilities that currently exist on the host node.

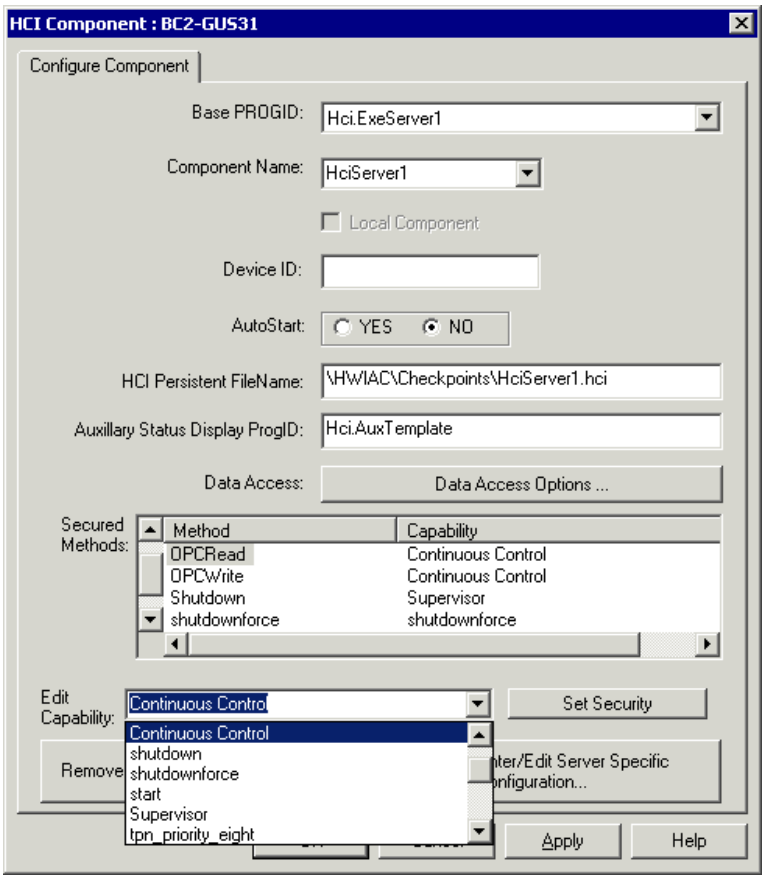


Figure 11: Listing of Secured Methods and Capabilities

6.1.10 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 capability architecture is defined, the capabilities must be put in place, and then configured.

Attention

Capability names must 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.

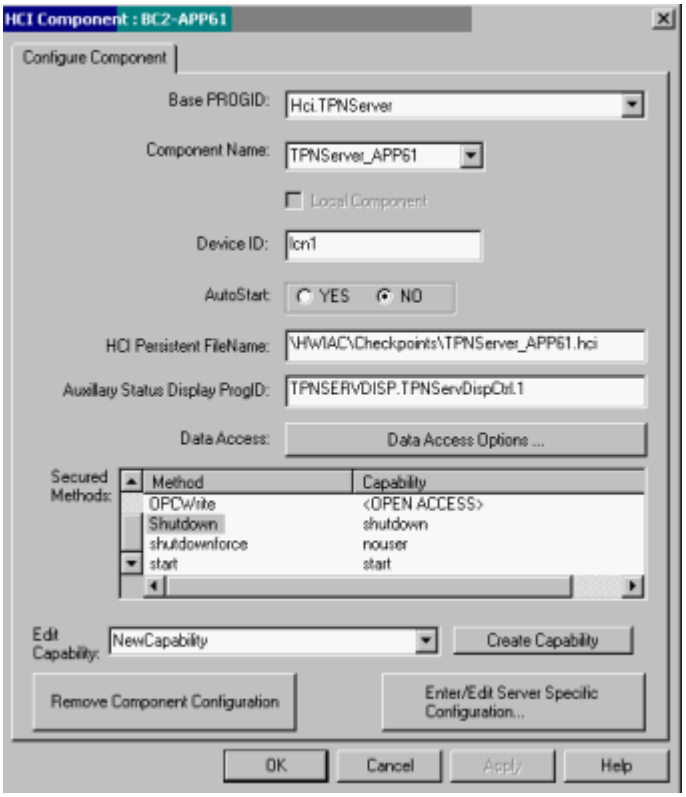
Click the **Set Security** button to invoke the property of the proxy file and modify the default security settings.

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.*

6.1.11 Creating and modifying a capability for an HCI Component

To create and modify a capability for an HCI component perform the following steps.

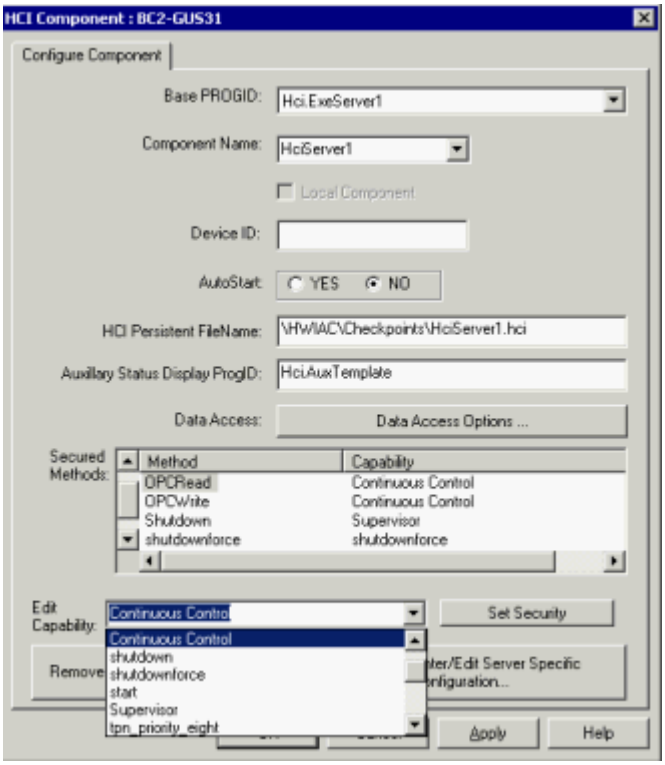
1 To create a new capability, select a method in the **Secured Methods** box. Type the name of the capability in the **Edit Capability** combo box. This enables the **Create Capability** button.



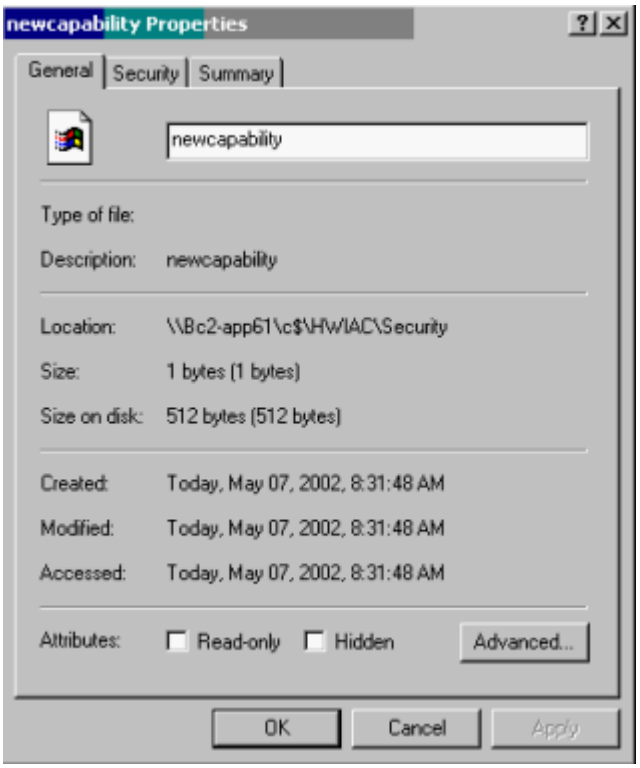
2 Click **Create Capability** to create the capability file on the host node. You must select an item inside the **Secured Methods** list box to enable the pull-down list of the **Edit Capability** combo box, as shown in the figure.

3 When a confirmation dialog appears, click **Yes** and then **OK** at the next screen to confirm your selection.

4 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.

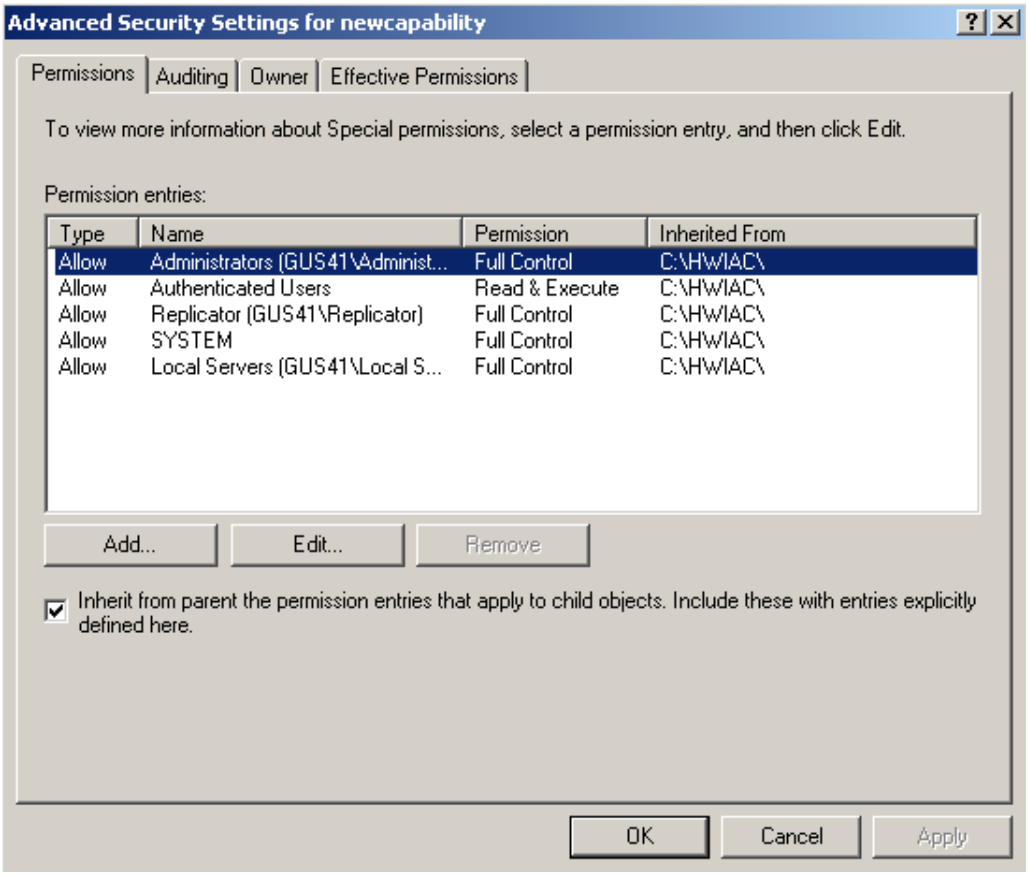


5 Click **Set Security** to invoke the property of the capability file that sets security permissions for the new capability. The capability file **Properties** window appears.

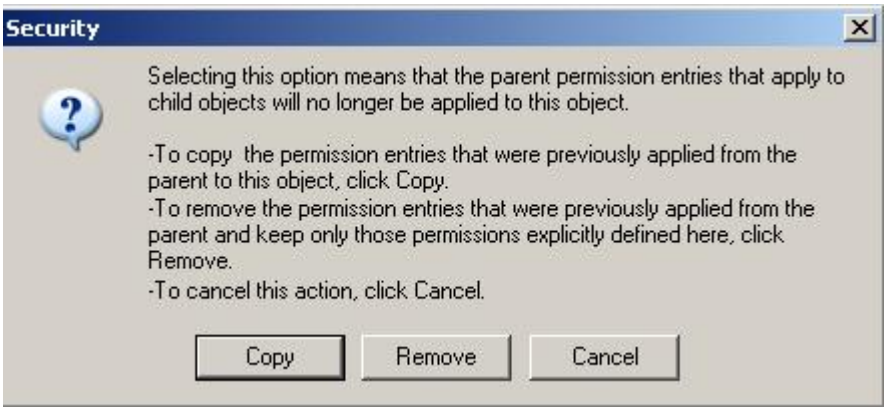


6 Click the **Security** tab, and then click **Advanced Settings**.

7 Clear the checkbox **Inherit from parent the permission entries that apply to child objects**.



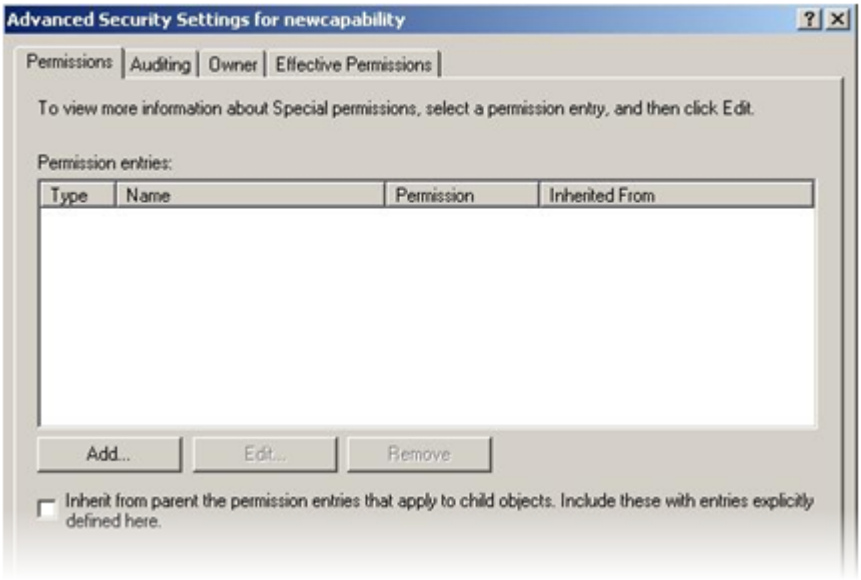
The following Security screen appears:



8 If you want to set a new security account, click **Remove**.

9 If you want to work from the permissions provided by the parent, click **Copy**.

10 The **Advanced Security Settings** window for the new account appears.

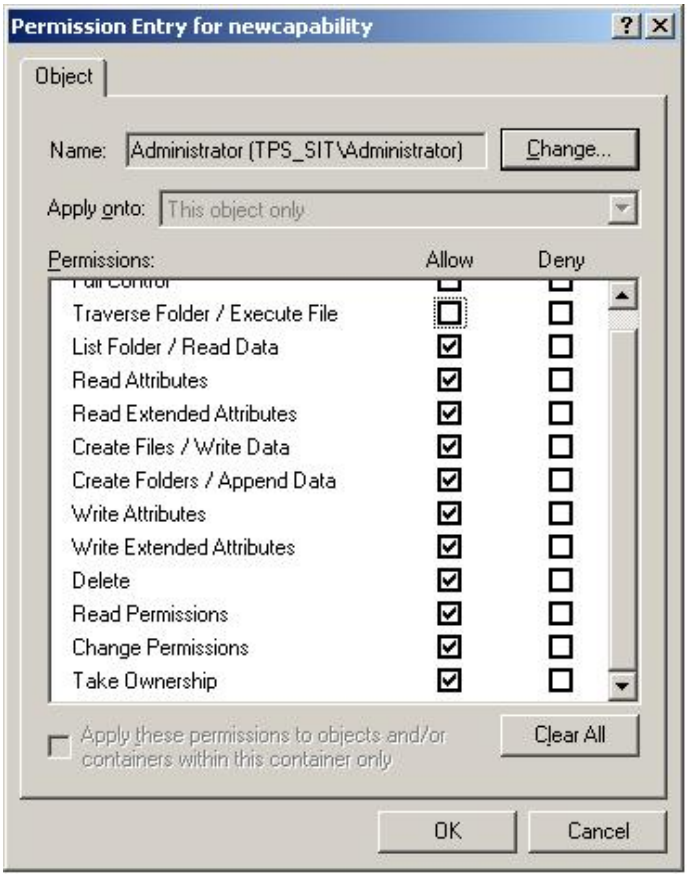


11 Click **Add**.

The **Select User, Computer, or Group** window appears.

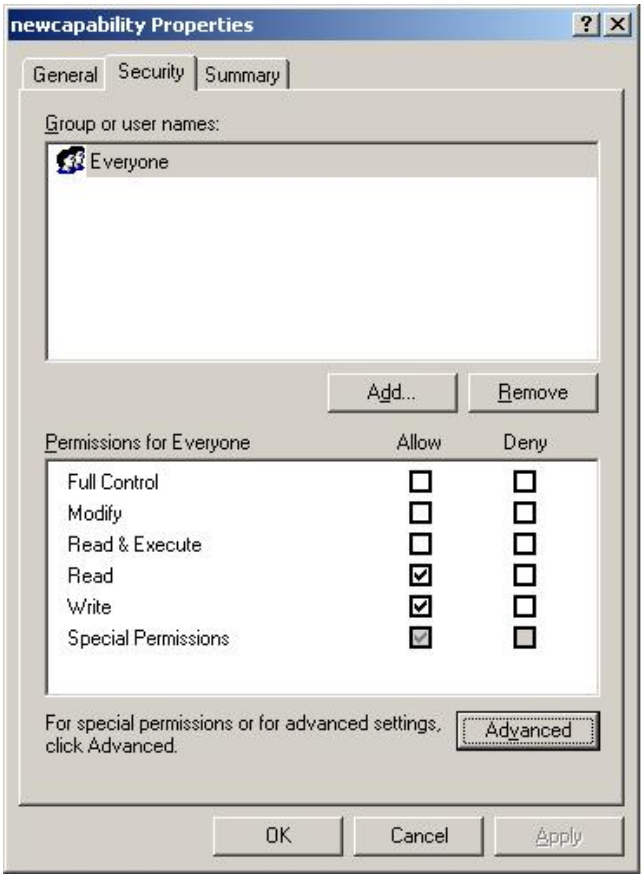
12 In the **Enter the Object Name to Select** box, type the name of the user or group to which you want to assign capabilities.

13 The **Permission Entry for** <*user*> window appears.



Note: If the **Allow** checkbox for the **Traverse Folder/Execute File** capability is unchecked, then the user has no capability.

14 Click **OK** to apply the change(s). When the **Advanced Security Settings** window appears, click **OK**. When the **Properties** page appears, click **OK**.



Attention

Removal of a component does not remove capability files.

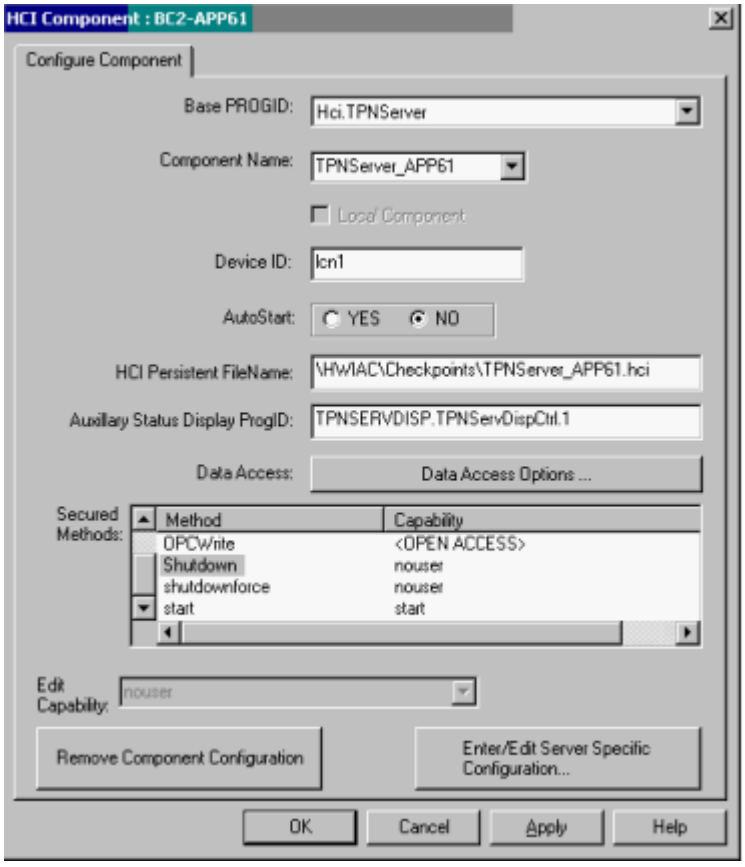
The capability field can be set to blank.

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.

6.1.12 Disabling shutdown of a component

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



6.1.13 Configuring a device-specific server

A Device Specific Server developer may optionally provide a configuration page. To configure a device-specific server, perform the following steps.

1 If a configuration page has been defined, it displays the **Enter/Edit with Server Specific Configuration…** button, and hides the **Apply** button.

If you click **Enter/Edit with Server Specific Configuration…**, 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 **Apply**, which invokes successful completion of the DSS configuration (unless you **Cancel** the configuration).

The system disables **OK** until at least one Device-Specific Server configuration has successfully completed.

6.1.14 Applying a configuration

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

1 From the **Component Configuration** page, click **OK**, **Apply** or **Enter/Edit with Server Specific Configuration**.

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 though **Cancel**. It can, however, be undone through **Remove Component Configuration**.

6.1.15 Removing a component's configuration

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

1. Click **Remove Component Configuration** 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.

   Renaming the component is identical to deleting the existing component and adding a new component. A warning is displayed that it may be necessary to shutdown the component before removing a component configuration.

2. The local component can be removed by clicking **Remove Component Configuration**. The system displays the following confirmation message: '*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

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

6.2.1 Changing Server Identity

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

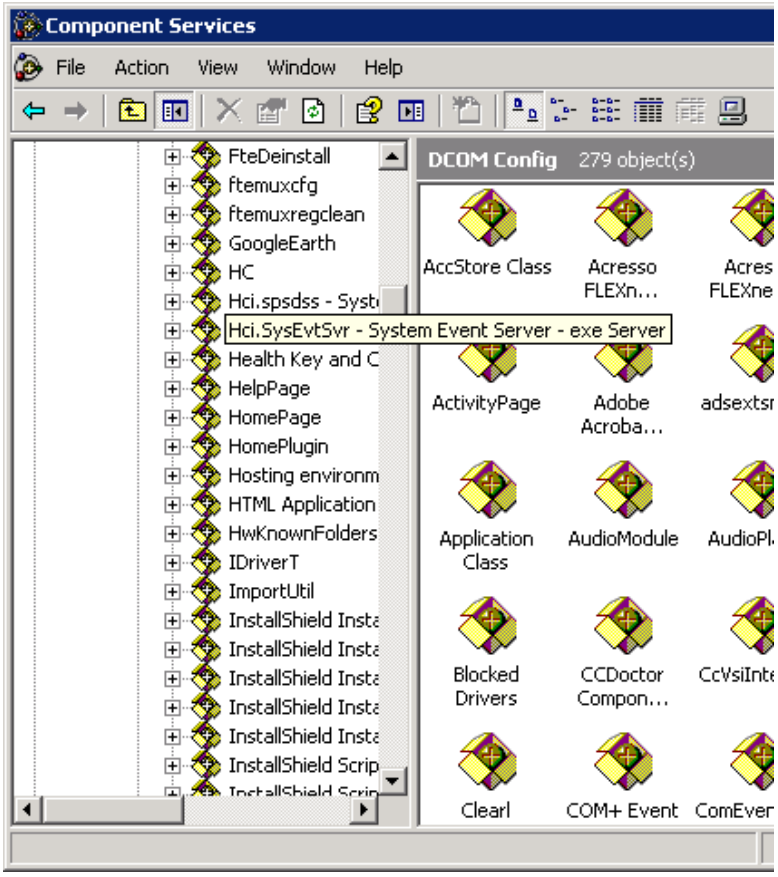
- *Automatically* (recommended) using a predefined user ID (such as TPSComServer).
- *Via a dialog* box that requests the installer to enter a user id for the server.

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.

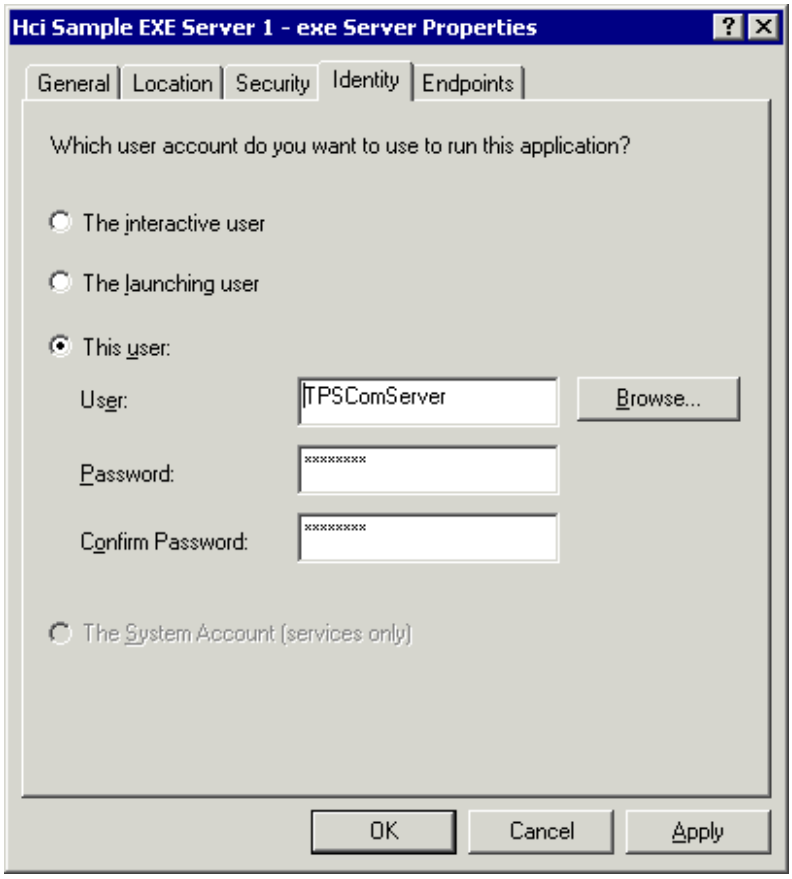
6.2.2 Assigning a user id and password

1. Type '**dcomcnfg**' in the **Run** dialog box, and then click **OK**.
2. The **Component Services** snap-in will start. Expand **Component Services** > **Computers** > **My Computer** > **DCOM Config**.



3 Select the ProgID of the server to configure, right-click and select **Properties**in the context menu.

4 Select the **Identity** tab to assign User Ids.



To assign a specific user ID: Select **This user**, 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.

Click **OK**.

5 Close the **Components Services**console.

6.2.3 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 members of the Product Administrators security group.

Attention

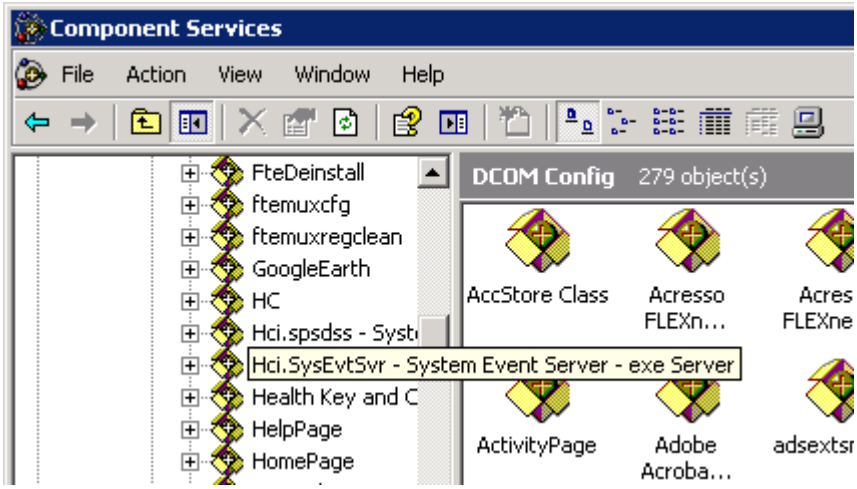
When setting access permissions, the default access list in dcomcnfg is normally empty. This is interpreted by DCOM as No Access. If one or more specific users or groups are inserted in the list for custom access security in dcomcnfg, ensure that SYSTEM, Local Servers, and the Administrators group are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

6.2.4 Setting permissions

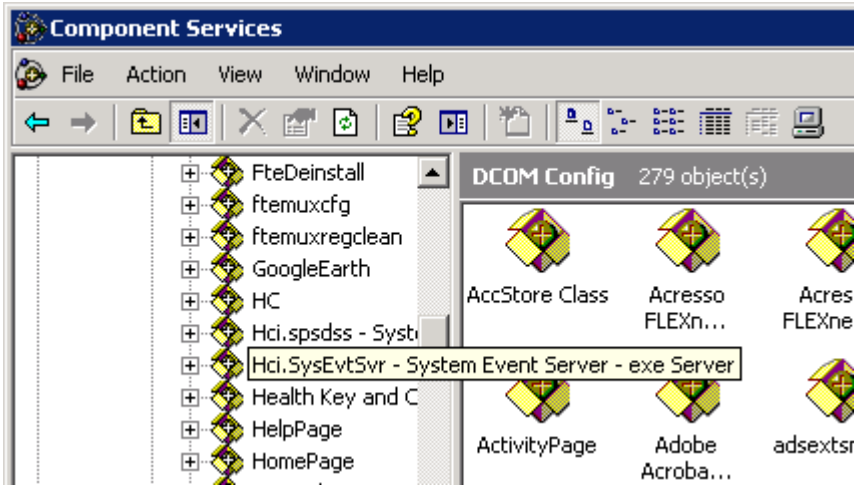
Follow these steps to set permissions.

1 Type '**dcomcnfg**' in the **Run** dialog box, and then click **OK**.

2 The **Component Services** snap-in will start. Expand **Component Services** > **Computers** > **My Computer** > **DCOM Config**.



3 Select the ProgID of the server to configure, right click and select **Properties** in the context menu.



4 Select the **Security** tab.

5 Select **Custom permissions**.

6 Click **Launch**(or **Access**) **Edit**.

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 the **Component Services** console.

7 Supporting System Event Server

7.1 Role of the System Event 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.

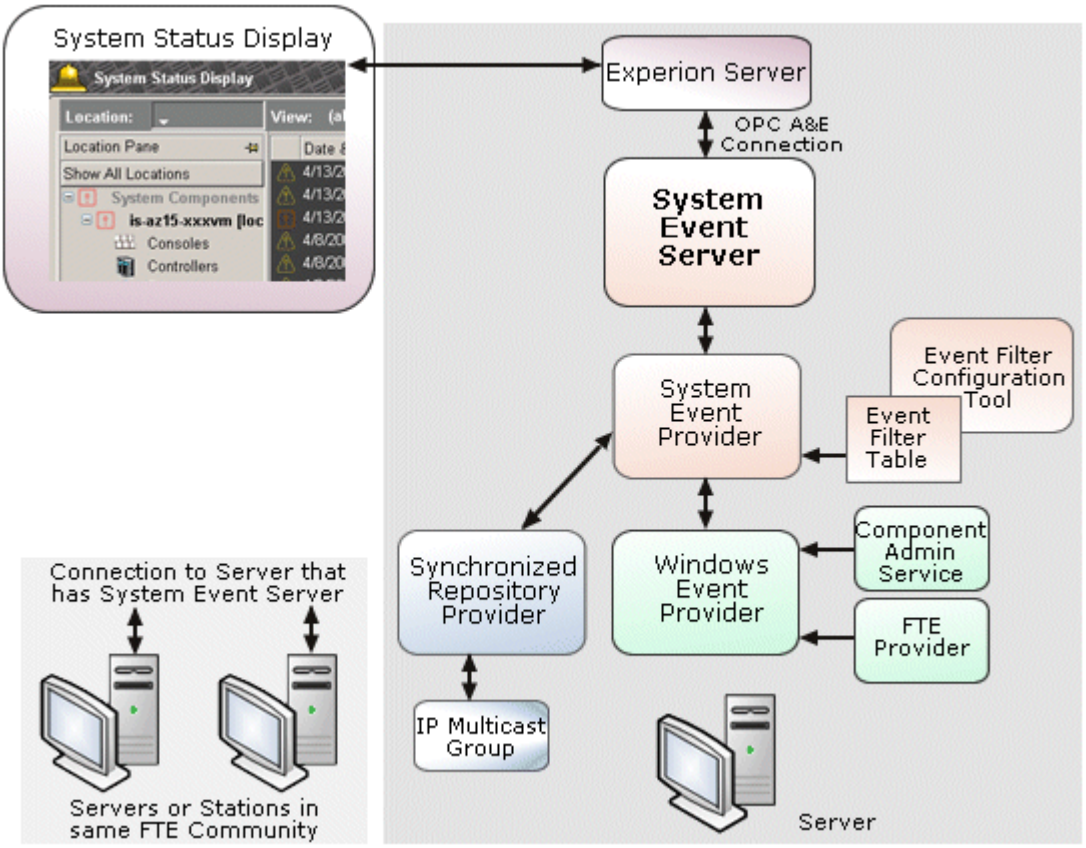
Refer to the *Experion Operators Guide* for procedures on how to operate the Experion Alarm Summary Display.

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.

7.1.1 System Event 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. Refer to ' “Event Filtering Configuration Procedures” on page 97' for procedures on how to configure an event filter file.

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



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 (For example, 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.

7.2 Getting Started with System Event Server

7.2.1 Installation guidelines

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

☑	Planning Consideration
	Review the information in this document related to multicast communications and synchronized repository scope.
	Upgrade System Management Runtime on all nodes.
	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 must install SES on both nodes.
	In a DSA connected system, there is normally one System Event Server per Experion Server (pair). Each DSA connected Experion cluster is configured with a unique synchronized repository multicast address.
	If there are multiple Experion Clusters that are not DSA connected, and it is desired that all system events be viewable in both clusters, configure an SES on each Experion Server, but include all nodes in a single synchronized repository multicast group.
	If there are multiple Experion Clusters that are not DSA connected, and each cluster displays only its own system events - configure an SES on each Experion Server and configure each cluster with a unique synchronized repository multicast group.
	When a System Event Server is used, the time must be synchronized between all nodes in its synchronized repository multicast group. Time synchronization of less than 2 seconds deviation is required.
	The System Event Server is not installed in a TPS only system.

7.3 Installing and Configuring System Event Server

7.3.1 Installing SES in a pre-R300 Experion system

The System Event Server is a licensed package.

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

1. Install the Microsoft Service Pack and Microsoft hot fixes, available on the Honeywell TPS System Software CD or Experion Application DVD. Then, reboot the node.
2. Select **Licensed Package Installer** from the TPS System Software CD or Experion Application DVD.
3. Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue.
4. Type 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 want to install. Click **OK**.
   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 then **OK** to end the Installation process.
9. Reboot the node.

7.3.2 Installing System Event Server on R300 and later Experion system

> **Attention**
> R300 and later Experion users may not need to perform these steps on an Experion Server, as System Event Server can be installed during the Experion node installation using the Application DVD. R300 and later 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 install optional software using the Node Definition Tool; see its related guide for more information.

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 then **OK** to end the Installation process.
6. Reboot the node.

7.3.3 Configuring System Event Server

The System Management Runtime package installs and configures a System Event Server Component on all process server nodes.

Attention

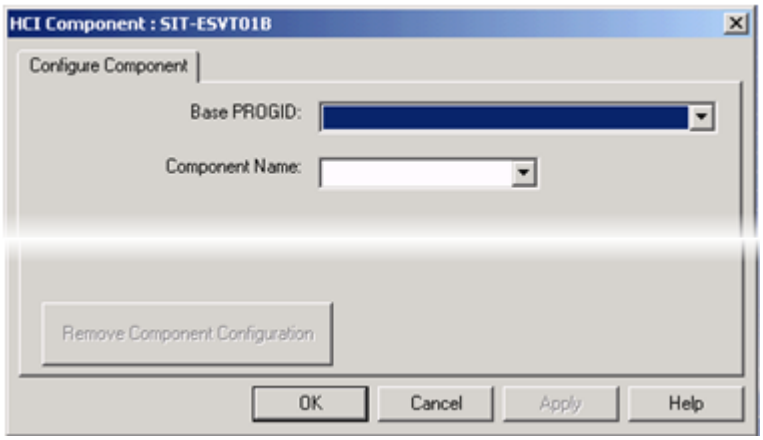
When configuring SES Server component, do not change any property values except for method security. The method security should only be changed if the pre-configured settings do not meet your needs. Using the pre-configured settings for all fields except possibly the method security enables the System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

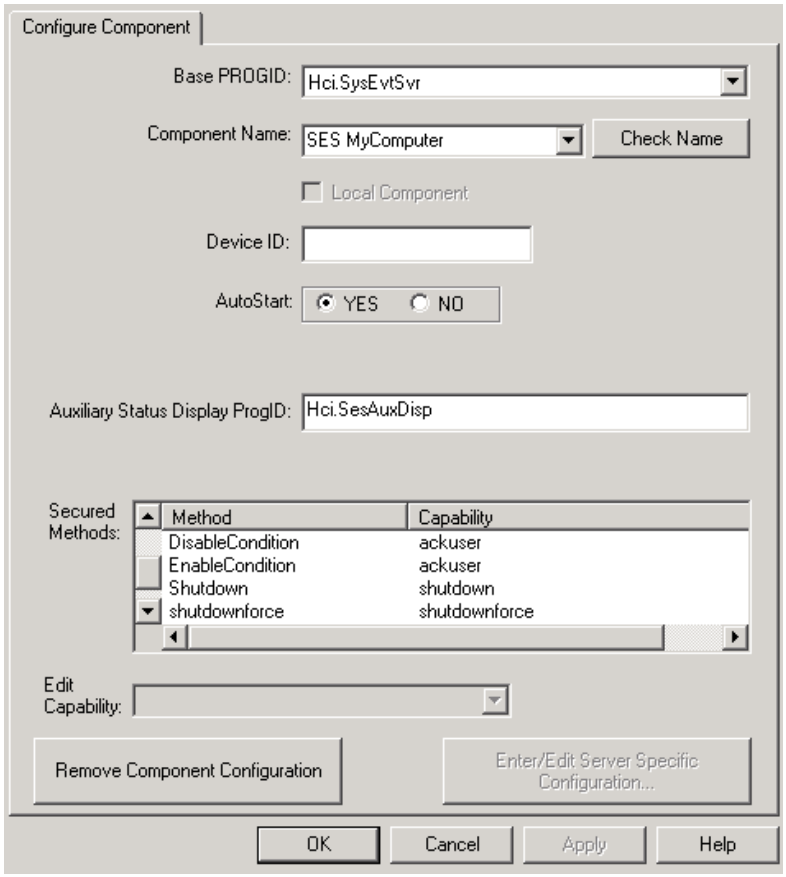
1 From the System Management Display, right-click the computer item. (See section “Using the HCI Component Configuration Page” on page 62 of this document for detailed instructions.)

2 Select **Configure** from the context menu.

3 Select **HCI Component** from another context menu. The resulting configuration page appears.



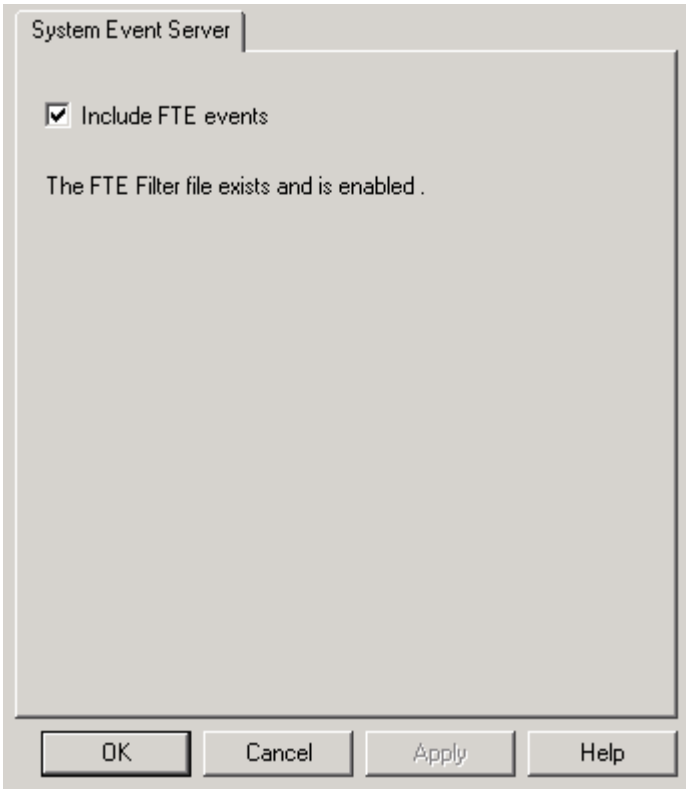
4 Click the down arrow on the edit combo box of the **Component Name** to get a pull-down list of pre-configured components. HCI/OPC component configuration reads from the registry of the host node. Select the component named **SES** <machine name where SES is installed>. In this example, the component is named **My Computer**.



5 Use the procedure described in ' “Secured Methods” on page 70' to adjust the secured access to AckCondition, DisableCondition or EnableCondition. The proxy file must be configured as 'ackuser.

6 Click **OK.**All applied updates are written to the registry of the host node.

7 For R400 SES components, a server specific configuration page is available. **Enter/Edit the Server Specific Configuration**.



Normally, one server (pair) should be enabled to collect FTE events per FTE community. Other servers must have this capability disabled. Enable the **Include FTE events** checkbox to collect FTE events on this server. Disabling the checkbox will rename the filter file and will disable FTE event collection.

If servers do not have DSA notifications enabled it may be desirable to turn on FTE events on multiple servers.

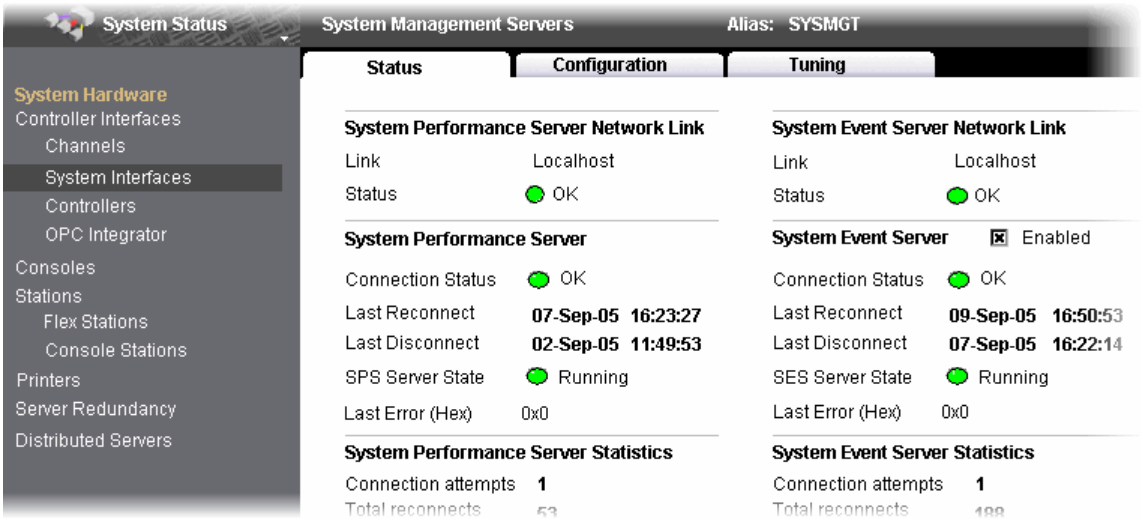
8 Click OK to complete the configuration and exit the configuration page.

7.4 Verifying SES is operational

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

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. 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. This tool can be accessed from **Start** > **Programs** > **Honeywell Experion** > **System Management** > **Windows Services & DCOM Servers Logon tool**. Follow the instructions provided on the tool. Note that this tool does not change the password on the account, but does verify that the entered password matches the current password for the account.. 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

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.

8.1.1 Example of Event Filtering Table

"Figure 12: Example Event Filtering Table" shows an example Filter Table. The filter table is an XML file accessed from the Honeywell Event Filter Snap-in.

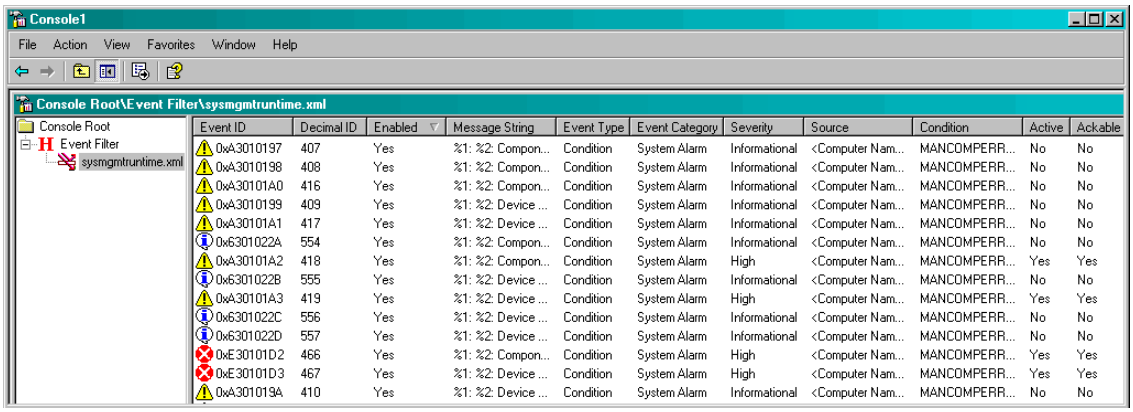


Figure 12: Example Event Filtering Table

8.1.2 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

8.2.1 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.

8.2.2 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.

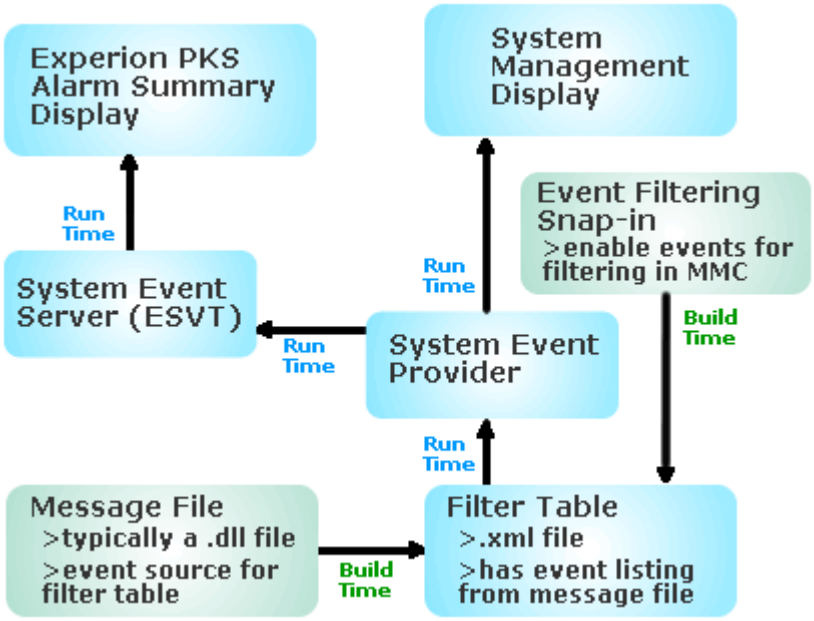


Figure 13: Creating a Filter Table

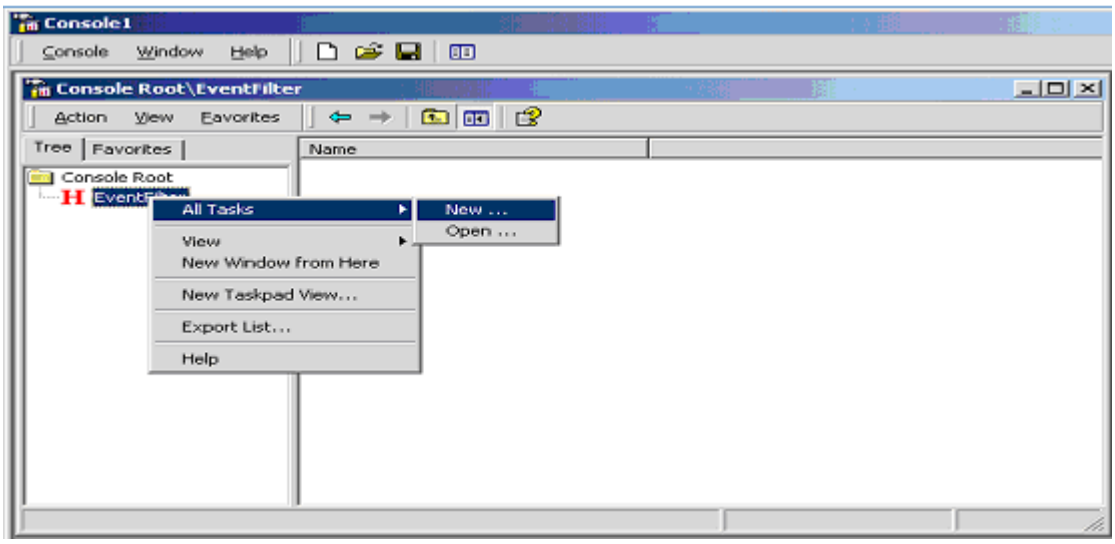
8.2.3 Creating a Filter Table

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.

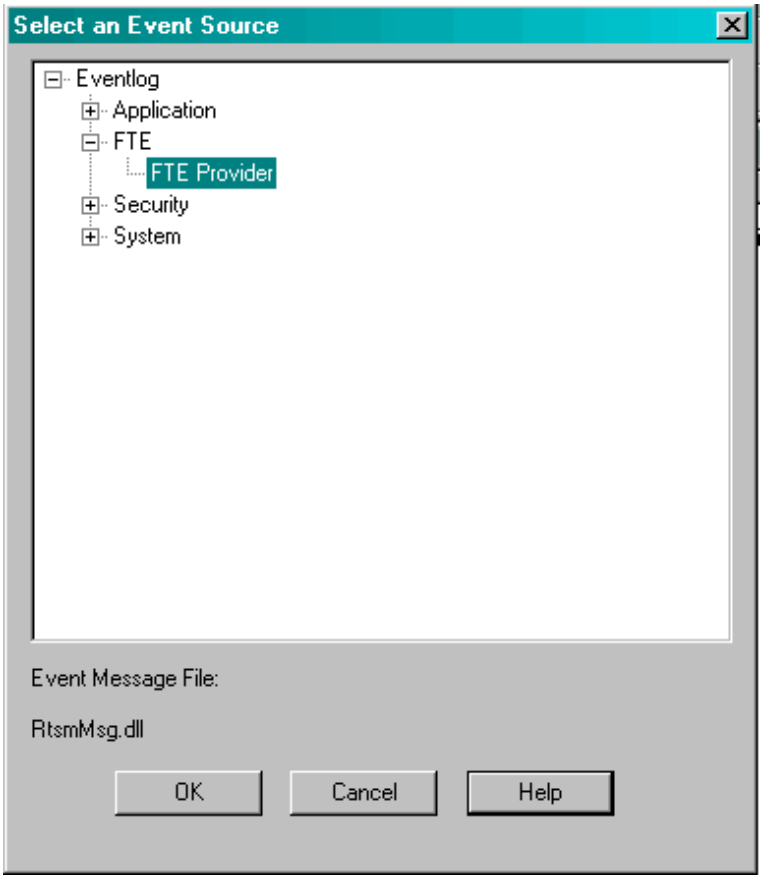
Follow these procedures to create a Filter Table.

1 To create an event filter table, right-click the Event Filter Tool and select **All Tasks** > **New.**



Result: A dialog box appears listing the available event sources.

2 From the dialog box, select the event source of interest. In this example, FTE provider is the selected event source.



Result: The Event source is highlighted and the message file is identified that contains a listing of events for the event source.

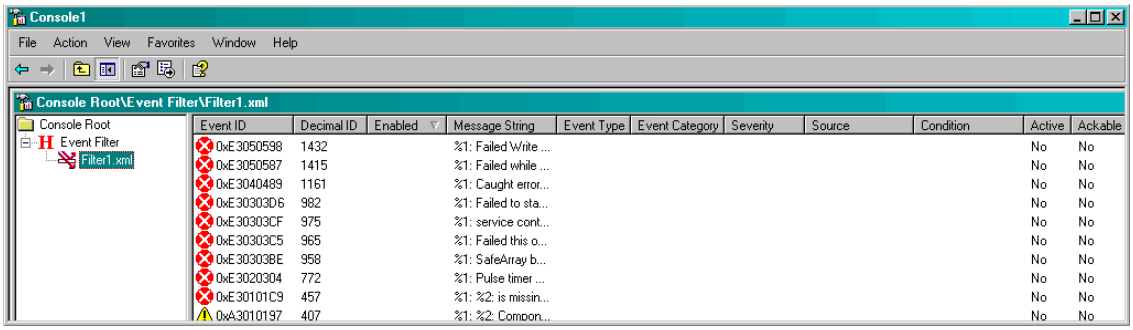
For example: **RtsmMsg.dll** contains the event listing for FTE Provider.

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.

3 Click **OK**.

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.



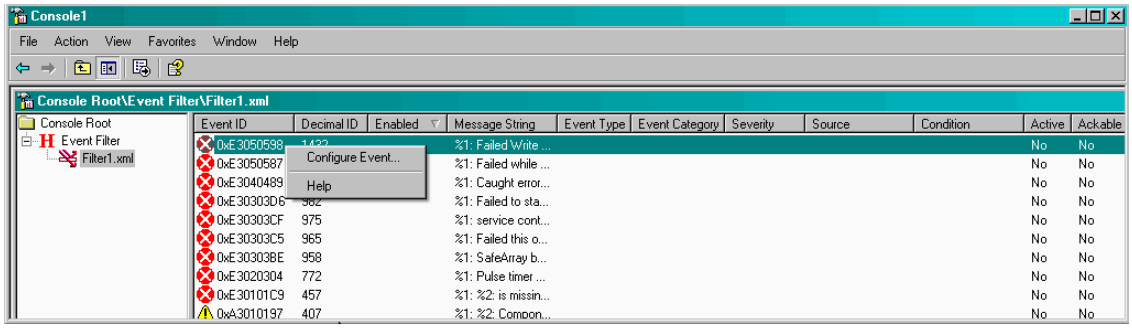
Attention

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.

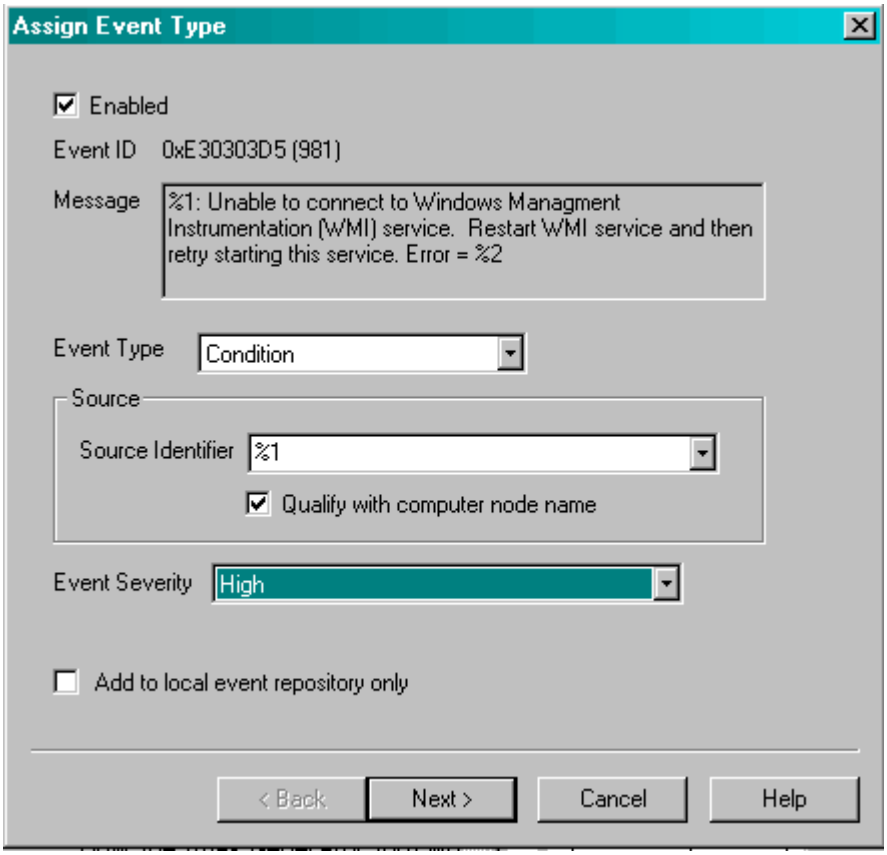
8.2.4 Configuring an Event

Follow these steps to configure an event.

1 Select the event on the result pane and then select **Configure Event**.

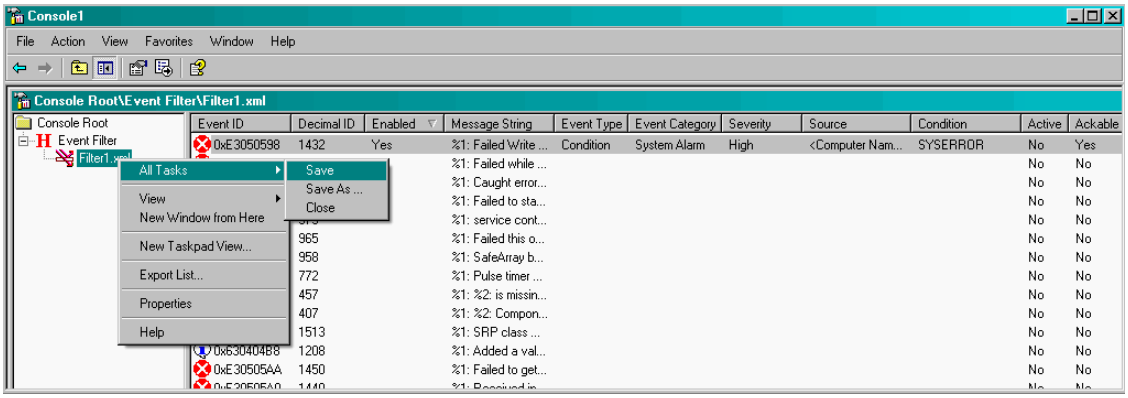


2 Use the **Assign Event Type** page of an event to assign an Event Type, Event source, and other properties to an event. You must check the **Enabled** checkbox to configure the event.



3 For more information about how to configure the selected event, see the ' “Analyzing Event Characteristics” on page 101' section.

Right-click the filter table, then click **All Tasks** > **Save** to save the filter table.



Save the filter table in *\ProgramData\Honeywell\ProductConfig\Filters*, so that the System Event provider (SEP) can be notified that the file has been modified. On notification, SEP will reload all its filter tables.

Note: You can rename the filter table file to a more meaningful name when you use **Save As**.

CAUTION

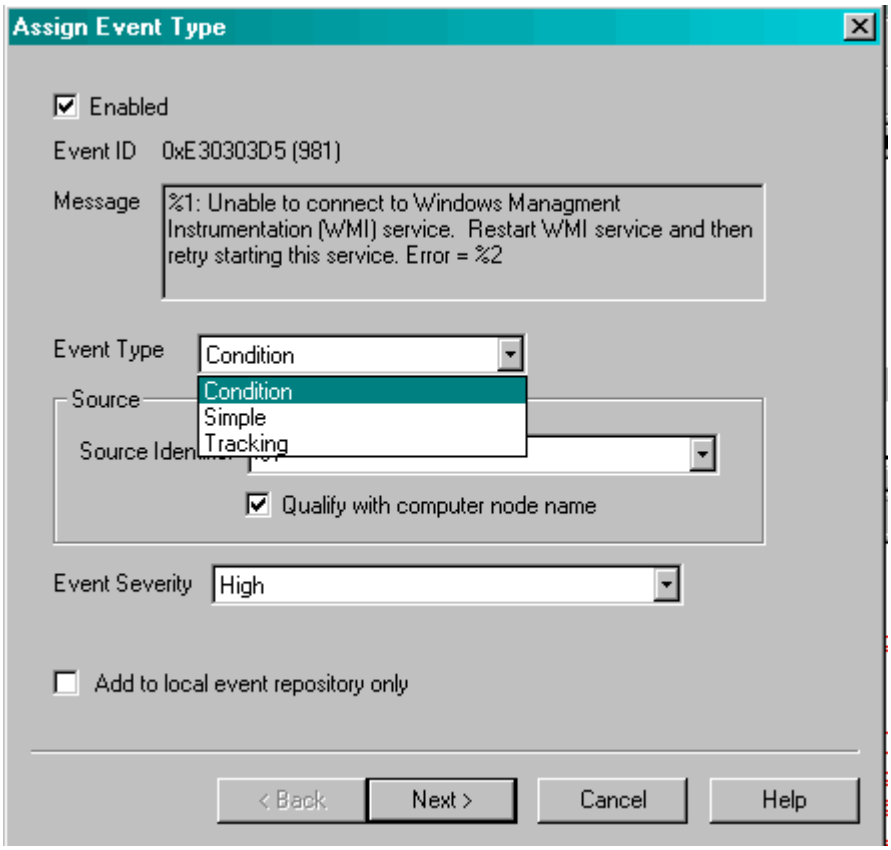
Because *ProgramData\Honeywell\ProductConfig\Filters* is a critical directory for System Event provider, Honeywell recommends that you *DO NOT* edit a filter table in that directory. Honeywell highly recommends that you create a new filter table in another directory and edit it. Once you finish editing the filter table, copy it to the *\ProgramData\Honeywell\ProductConfig\Filters* directory.

8.2.5 Analyzing Event Characteristics

This section details 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*.



Simple and *Tracking* events are delivered only to clients connected and listening for events at the time of event generation. *Simple* and *Tracking* events are not maintained in the event repository and not acknowledgeable. The client receiving the event maintains the view of each event. *Simple* and *Tracking* events are sent 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 condition 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.

Event Characteristic	Simple	Tracking	Condition Related
Guaranteed Delivery			X
Requires Acknowledgement			X

Event Characteristic	Simple	Tracking	Condition Related
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
Represents 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

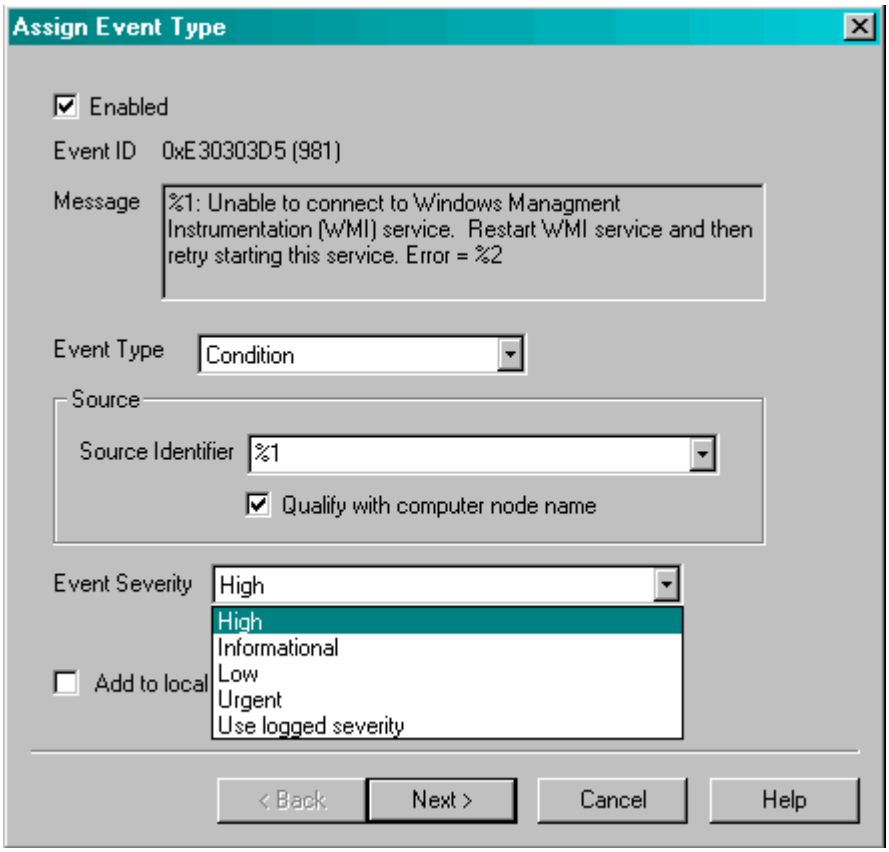
The event source identifies the subject of an event. This may be system entity such as a computer node or a managed component running on a computer node. For condition related events, all events relating to the same entity must use the same event source definition. The combination of event source and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

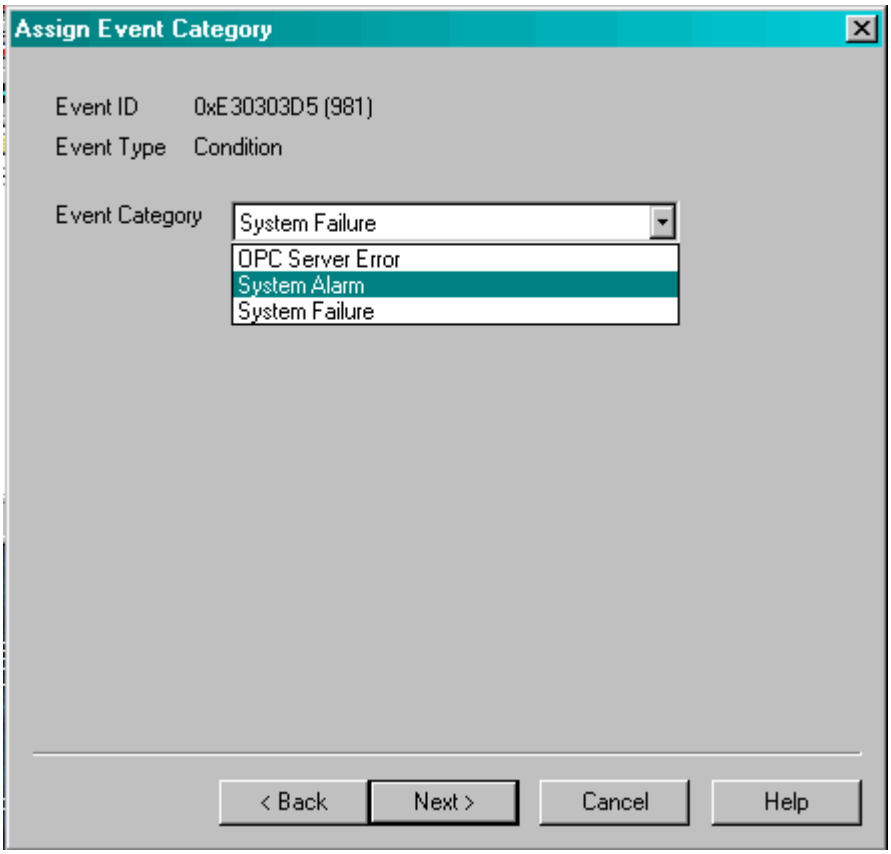


Add to Local Event Repository Only

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, click **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.

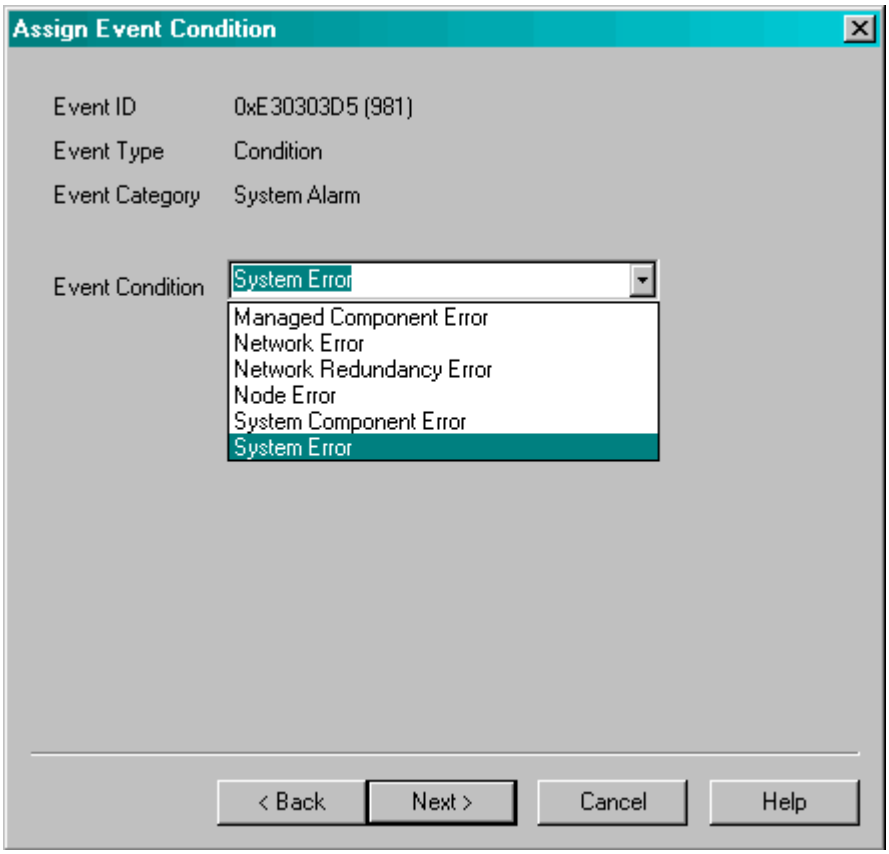


For detailed information regarding selection of Event Category, see the System Event Filter configuration tool on-line help.

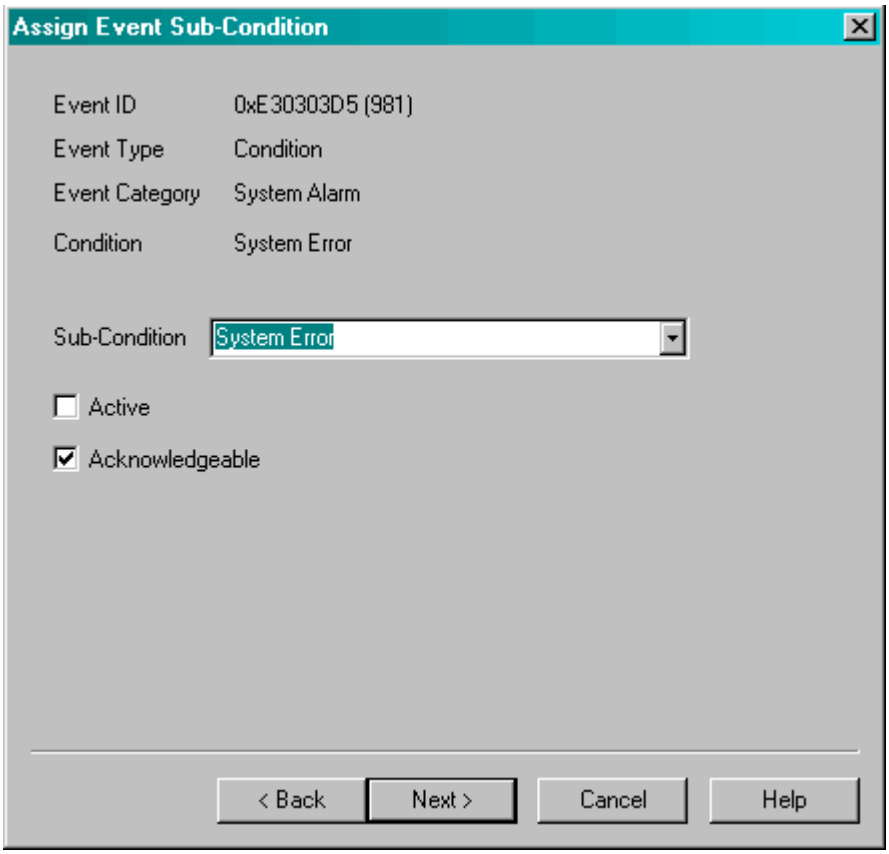
To continue event configuration, select **Next**.

Assign Event Condition/Sub condition (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, such as a 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.

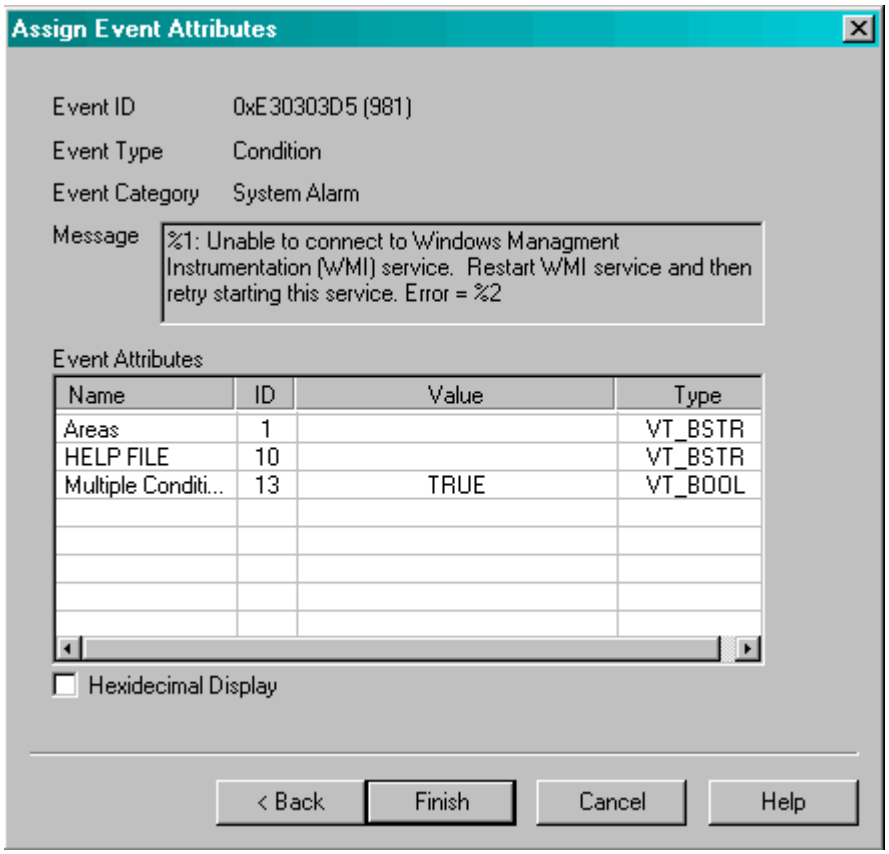
Determine Active/Acknowledgeable State (Condition Related events only)

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.



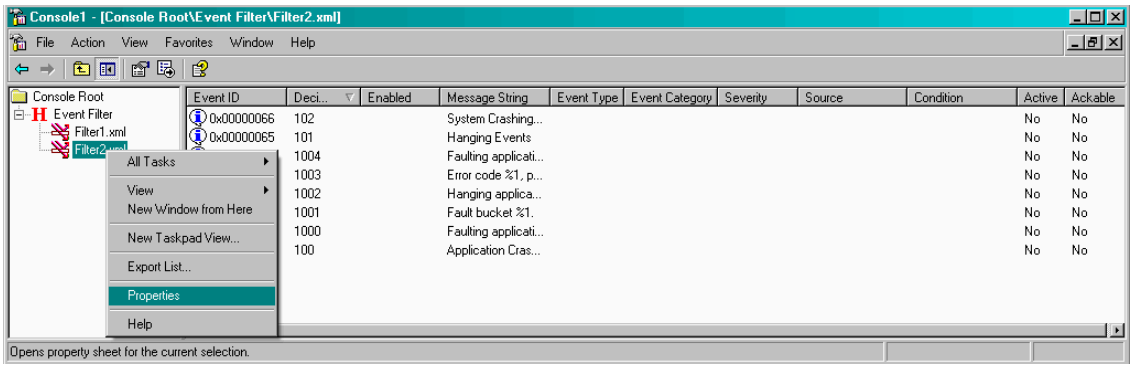
Click **Finish** to complete configuration of the selected event.

8.2.6 Sharing a Filter Table

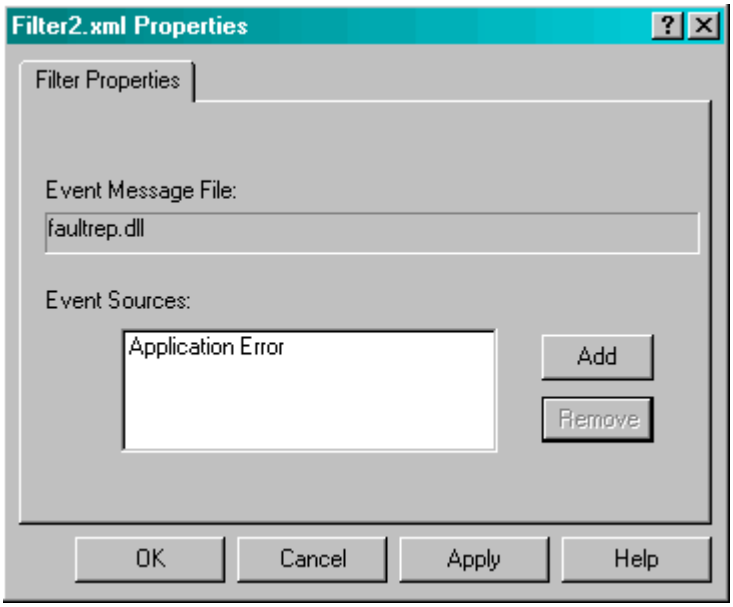
If a message file is shared by more than one event source, each event source can have its own filter table, or multiple event sources can share a common filter table.

Follow these steps to share a filter table:

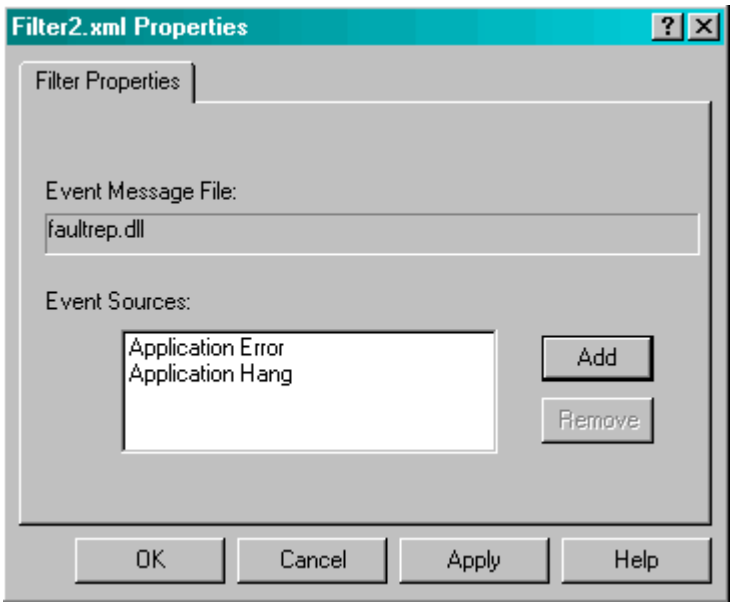
1 To allow a filter table to be shared by multiple event sources, right-click a filter table, and select **Properties** from the pop-up context menu.



2 On the Properties page, click **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

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.

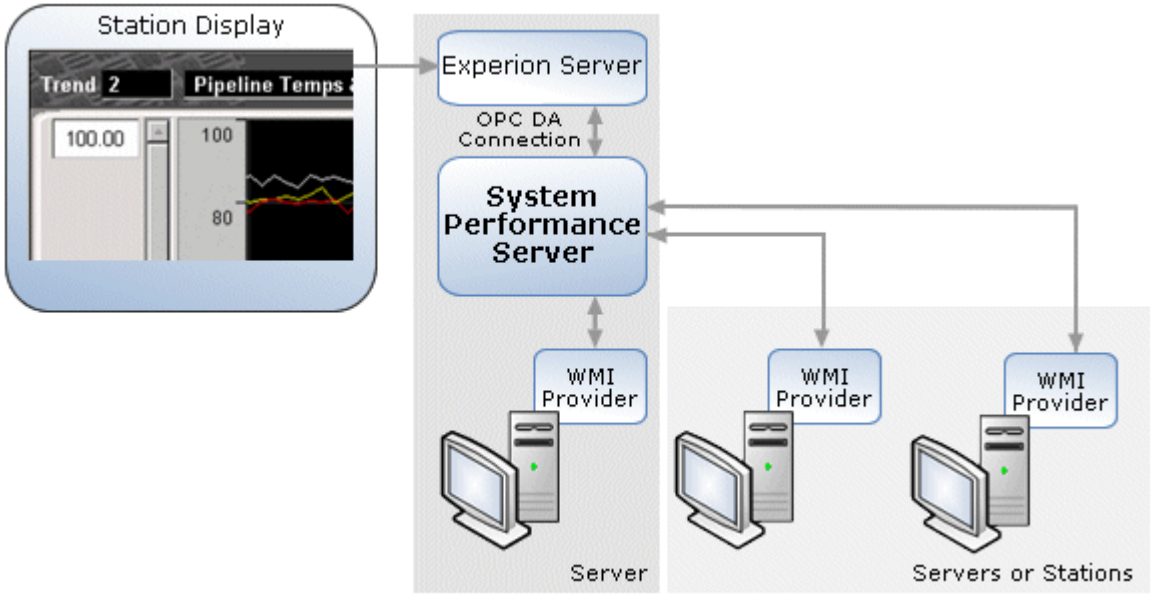
The System Performance Server is an HCI Managed Component. Refer to the System Management Operations Guide for procedures on how to monitor the status of the System Event Server.

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 a HResult of S_FALSE and data item pp errors of OPC_E_BADRIGHTS.

9.1.1 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 2003 or XP). Similarly, the System Performance Server can monitor any Experion or TPS Windows node within its containing unit.

9.1.2 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,

- 'host' is 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' is the Identifier of the name space within the CIM Repository which contains the data item. Specification of the namespace is required.
- 'class.instance.property' are the 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=@

9.1.3 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 name form for aliases is **host.aliasname**.

The following table 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 ' “Configuring SPS on Experion Server” on page 114' for configuration details. The ' “Configuring SPS on Experion Server” on page 114' subsection therein 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

9.2.1 Installation guidelines

For Experion, the System Performance Server is installed on every Experion Server. In a redundant server configuration the System Performance server is 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).

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.

9.2.2 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 and later Experion users should not follow these steps as the System Performance Server can be installed as part of the Experion installation.

1. Install the Microsoft Service Pack and Microsoft hot fixes, available on the Honeywell TPS System Software CD or Experion Application DVD. Then, reboot the node.
2. Select **Licensed Package Installer** from the TPS System Software CD or Experion Application DVD, 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. Type 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 want to install. Click **OK**.
   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 the node.

9.2.3 Installing System Performance Server on R300 and later Experion system

Attention
R300 and later Experion users *may not need* to perform these steps on an Experion Server, as System Performance Server can be installed during the Experion node installation. R300 and later 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.

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 then **OK** to end the Installation process.

6 Reboot the node.

9.3 Configuring SPS on Experion Server

9.3.1 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

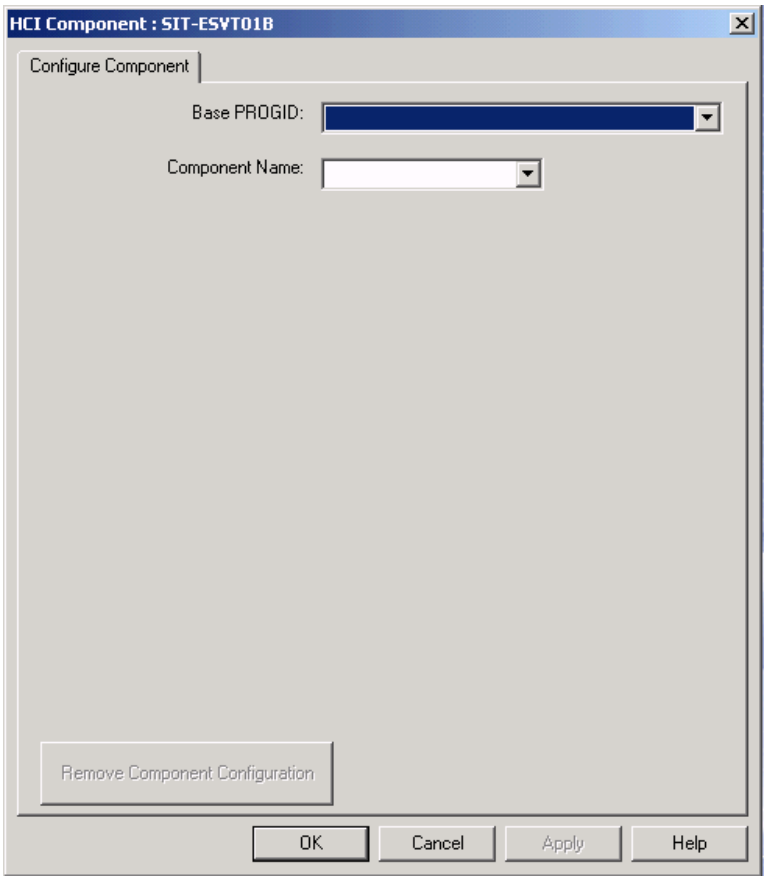
When configuring SPS Server component, do not change any property values except for method security, SPS Scope or Aliases. These items must only be changed if the pre-configured settings do not meet your needs. Using the pre-configured settings for component name and auto start enables the System Performance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

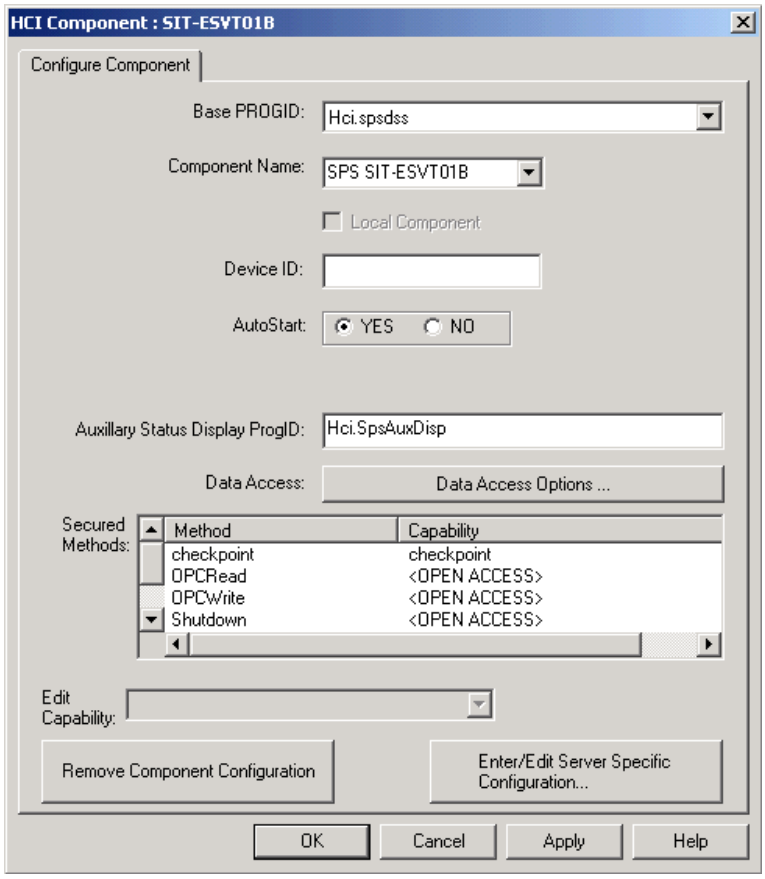
1 From the System Management Display, right-click the computer item. (See 'Using the HCI Component Configuration Page' for detailed instructions.)

2 Select **Configure** from the context menu.

3 Select **HCI Component** from another context menu. The resulting configuration page appears.

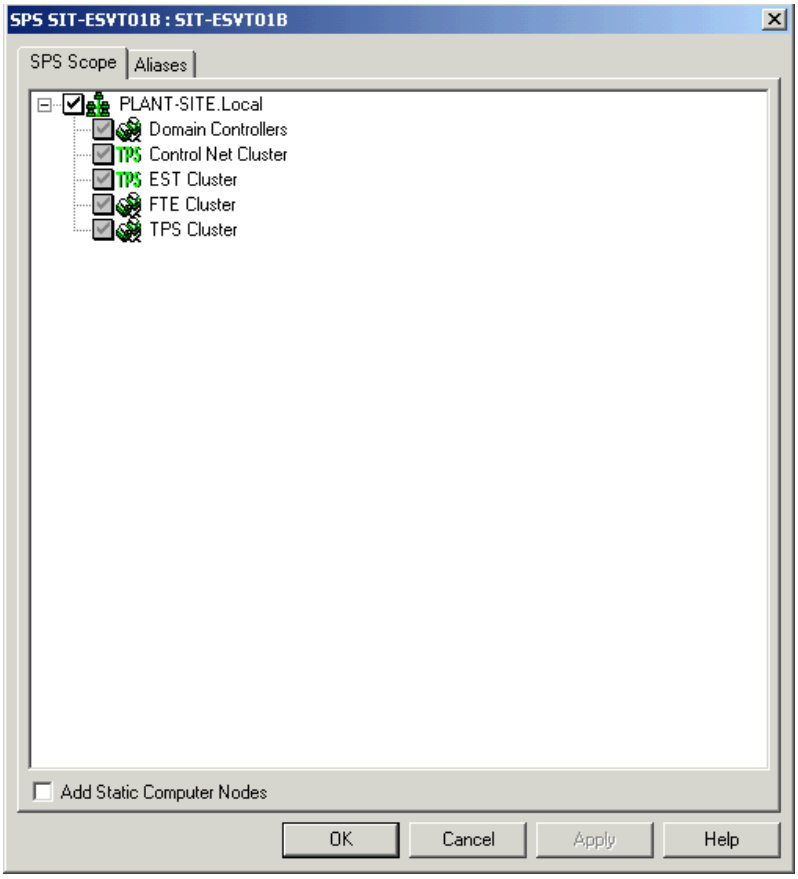


4 Click the down arrow on the edit combo box of the **Component Name** to get a pull-down list of pre-configured components. HCI/OPC component configuration reads from the registry of the host node. Select the component named **SPS** <machine name where SPS is installed>. In this example, the component is named **SPS SIT-ESVT01B**.



5 Use the procedure described in ' “Secured Methods” on page 70' to adjust the secured access to OPCRead, Shutdown, and so on. 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.

6 Click **Enter/Edit Server Specific Configuration** to display the SPS Server configuration pages. The resulting configuration page appears.



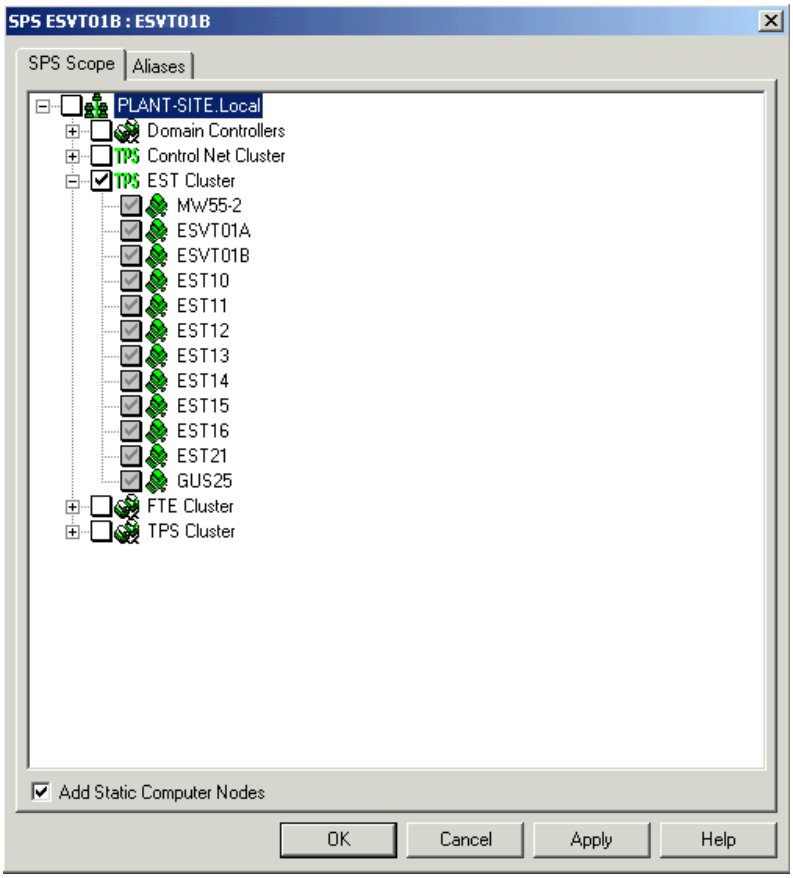
7 Proceed to ' “Configuring the SPS Scope” on page 116' that describes configuration selections.

9.3.2 Configuring the SPS Scope

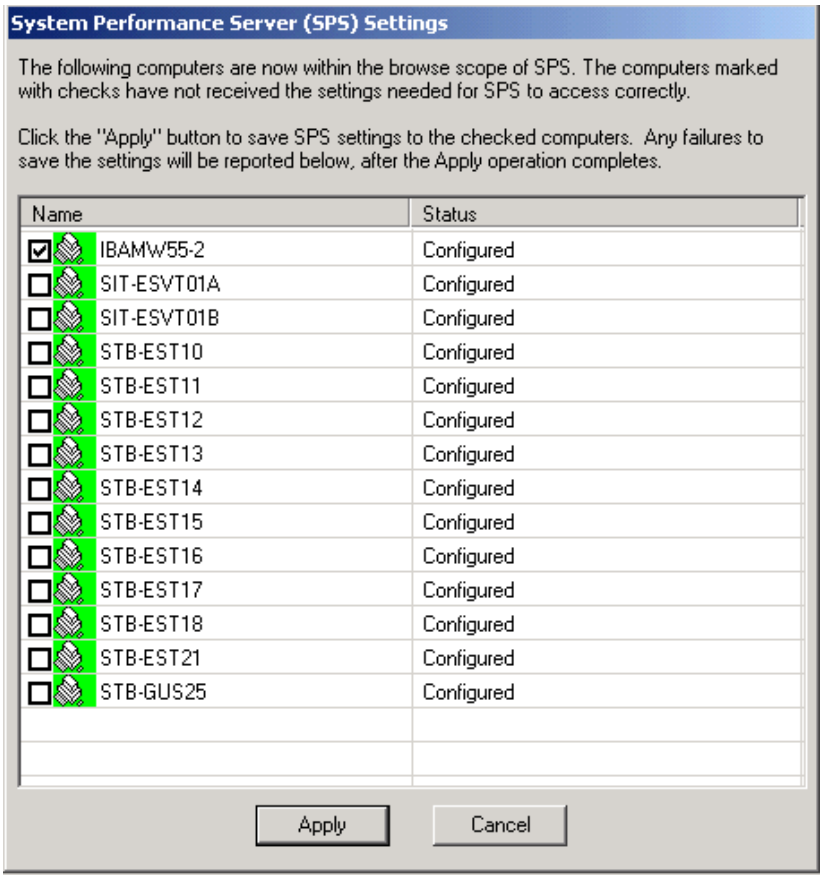
NOTE: SPS Scope is set automatically when downloading the EMDB Network model. Computers in scope are configured by assigning a monitoring server in the Network tree.

Use the SPS Scope page to perform the operations described in the following table.

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. Select the nodes you are interested in monitoring. Click **OK** or **Apply** on the SPS Scope page.
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.	



When you click Apply, 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.

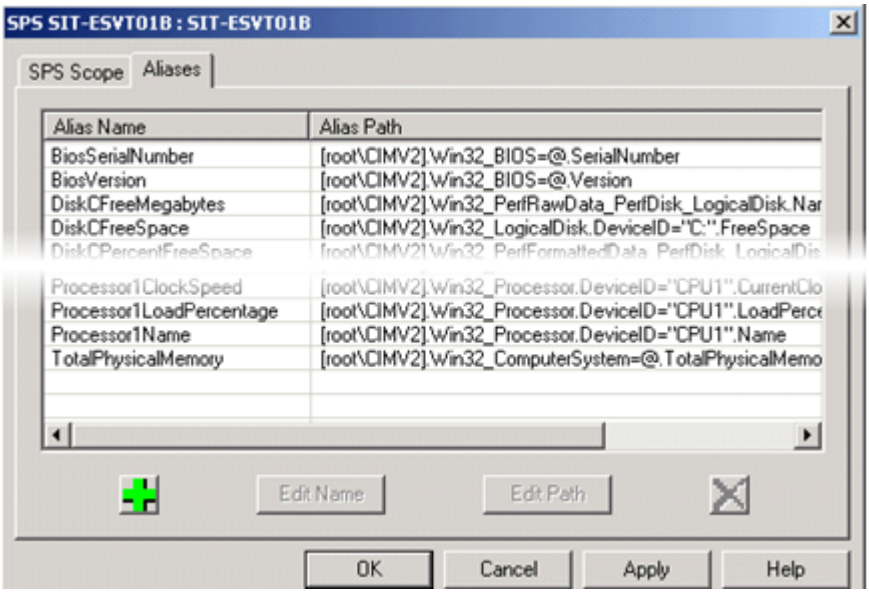
Attention

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'.

9.3.3 Adding new Aliases

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

1 Select the **Aliases** tab from the SPS Server specific configuration page.



2 To add a new **Alias Name**, click the green +. 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.

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 previous 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.

9.3.4 Deleting an alias

Follow these steps to delete SPS aliases.

1 From the SPS Aliases configuration page (see step 1 in ' “Adding new Aliases” on page 118'), select 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**.

3 Click **Apply** or **OK.**

9.3.5 Editing an alias

Follow these steps to edit SPS aliases.

1 From the SPS Aliases configuration page (see step 1 in ' “Adding new Aliases” on page 118'), select the field to be changed.

2 Click a second time in the field to be changed, or click **Edit Name** or **Edit Path**. Type 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.

1. From the hierarchy of the System Management Display, right-click the computer item. (See 'Configuring HCI/OPC Components' for instructions.)
2. Select **Configure** from the context menu.
3. Select **HCI Component** from another context menu. The resulting configuration page appears.
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 type the name.

   Result: **Check Name** appears. After verifying the component name, the system enables **Apply**. 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 ' “Configuring SPS on Experion Server” on page 114'. The remainder of SPS configuration for an APP Node is identical to that of an Experion node.

9.5 Verifying SPS is Operational on Experion Server

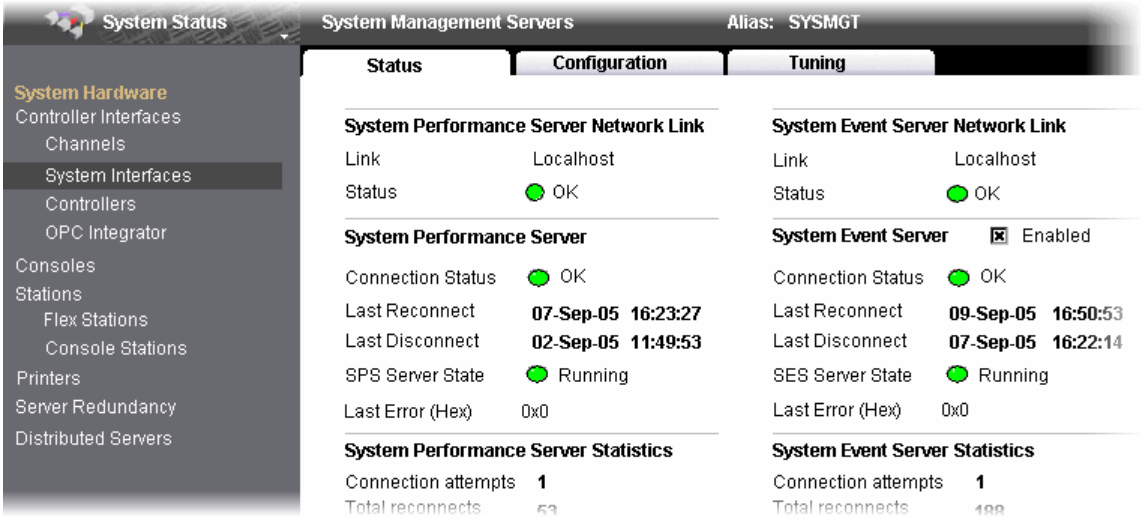
9.5.1 Verifying SPS is Operational

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

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.

1 From the System Management Display, select **System Performance Server**.

2 If the **AutoStart** option for the SPS was selected, then the System Management Display must show that the SPS has started.

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. 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. This tool can be accessed from **Programs** > **Honeywell Experion PKS** > **System Management** > **Windows Services & DCOM Servers Logon tool**. Follow the instructions provided on the tool. Note that this tool does not change the password on the account, but does verify that the entered password matches the current password.

10 Supporting SNMP Monitor

10.1 Role of the SNMP Monitor

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.

10.1.1 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 is installed on a node running System Management Runtime. For Experion users, the SNMP Monitor is 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.

10.2.1 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.

1. Install the Microsoft Service Pack and Microsoft hot fixes, available on the Honeywell TPS System Software CD or Experion Application DVD. Then, reboot the node.
2. Install the Honeywell Repackaged Redistributable Files by selecting **Main** > **Honeywell Repackaged Redistributable Files**. Reboot the node.
3. Select **Licensed Package Installer** from the TPS System Software CD or Experion Application DVD.
4. Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue.
5. Type 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 want to install. Click **OK**.
   Result: The installation process occurs, which usually takes a few minutes.

   Attention
   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 the Experion Server.

10.2.2 Installing SNMP Monitor in R300 and later Experion system

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

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. Type license and authorization numbers. Click **Next** to continue.
4. Click **SNMP Protocol and Monitor.**
5. Click **Install Package**.

Attention
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.

6 After a successful installation, the screen in the previous step appears. Click **Exit** and **OK** to end the Installation process.

7 Reboot the 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 should 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 will be sent. The link-up and link-down notifications should be enabled.

11 Administering HCI Name Service

11.1 Role of HCI Name Service

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 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.

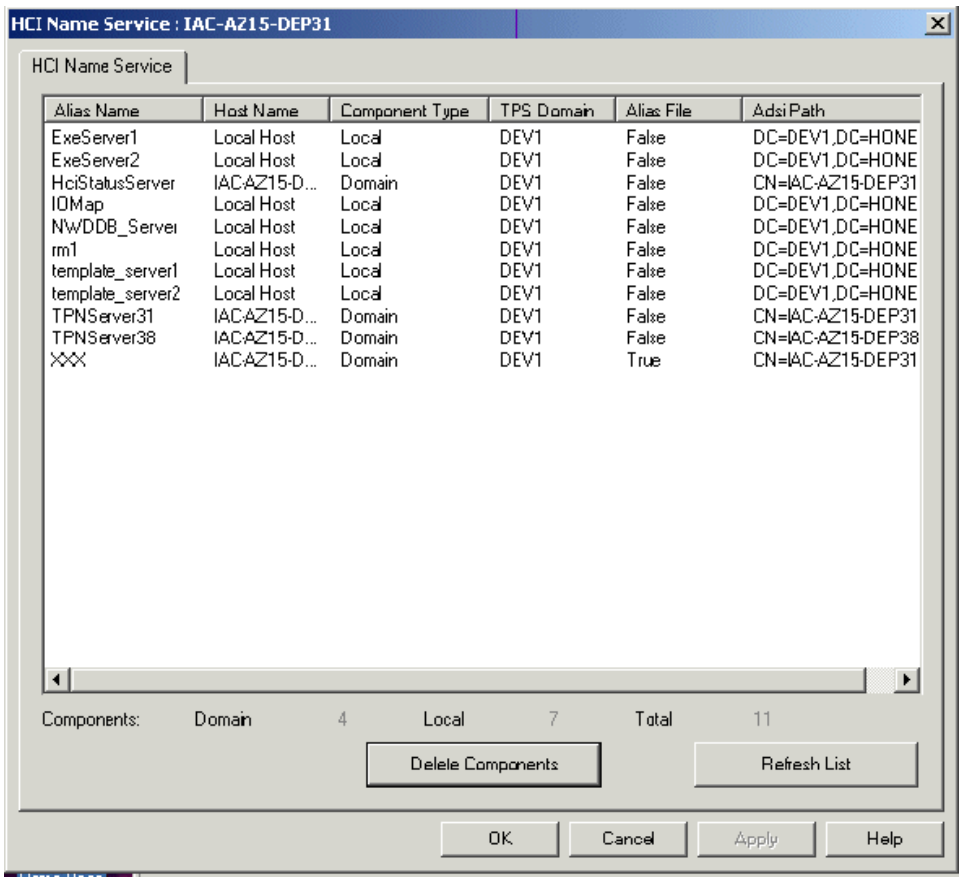


Figure 14: Sample HCI Name Service Display

11.1.1 Description of HCI Components

The HCI Name Service Display shown in “Figure 14: Sample HCI Name Service Display” contains the following information:

Table 13: Descriptions of HCI Components

HCI Component	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.

HCI Component	Description
CLSID	Class Identifier of the server.

11.1.2 Uniqueness of alias names

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

A client application may function inconsistently if a remotely accessed component is given the same name as another domain component. A unique alias name allows a client application to be written such 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 is 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 is 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.

11.2 Viewing and Setting Scope of HCI Name Service

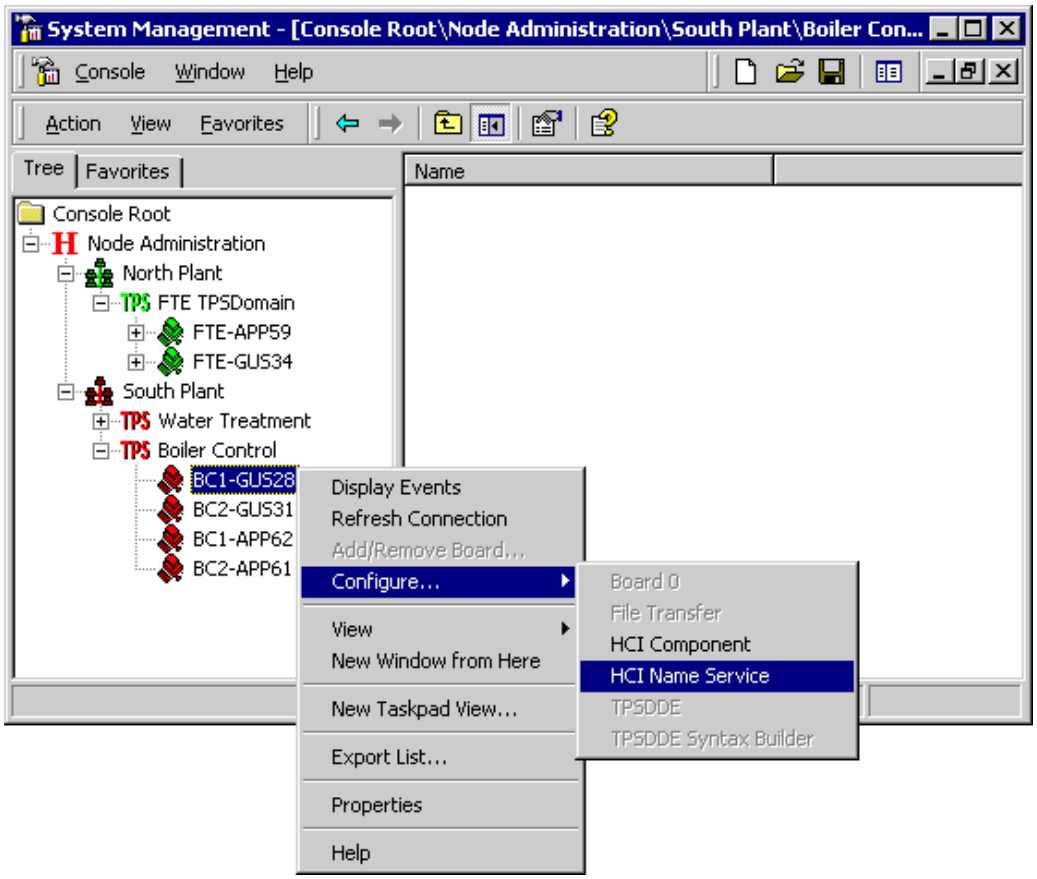
11.2.1 About the HCI Name Service tool

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. During an HCI Component Configuration session, this tool helps you to delete unused data entries in the repository and refresh the listing.

11.2.2 Viewing the name service repository

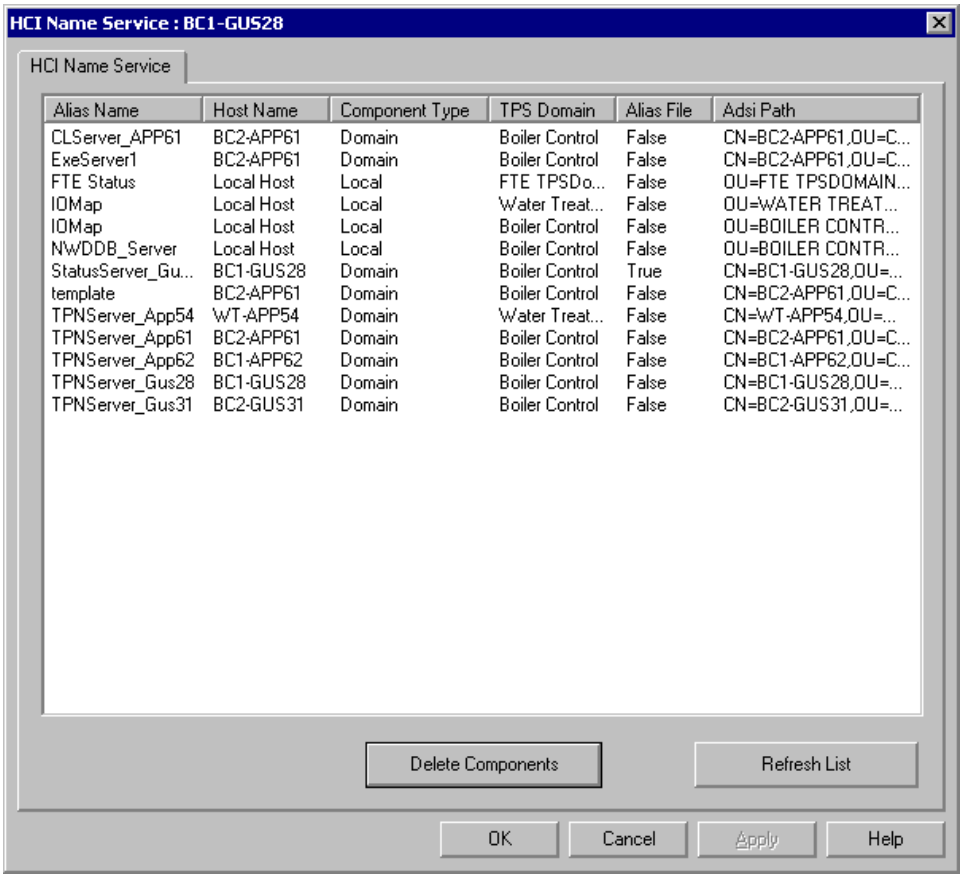
Follow these procedures to view the Name Service repository.

1 From the System Management Display, right-click the node of interest and select **Configure** > **HCI Name Service**.



Result: The **HCI Name Service** tool appears.

2 From the **HCI Name Service** tool, you can refresh the list or delete a component (if you have access privileges).



11.2.3 Deleting a local component

Honeywell recommends you to use the HCI Configuration Page to delete all the 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 14: Issues that May Occur when Deleting Local Components” describes issues that may occur when deleting a local component, why these issues occur, and recommended solutions to these issues.

Table 14: 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. 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 within the same TPS Domain.	Make sure all nodes in a TPS Domain are running before deleting local components.

Issue	Why Issue May Occur	Recommended Solution
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. 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).

11.2.4 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.

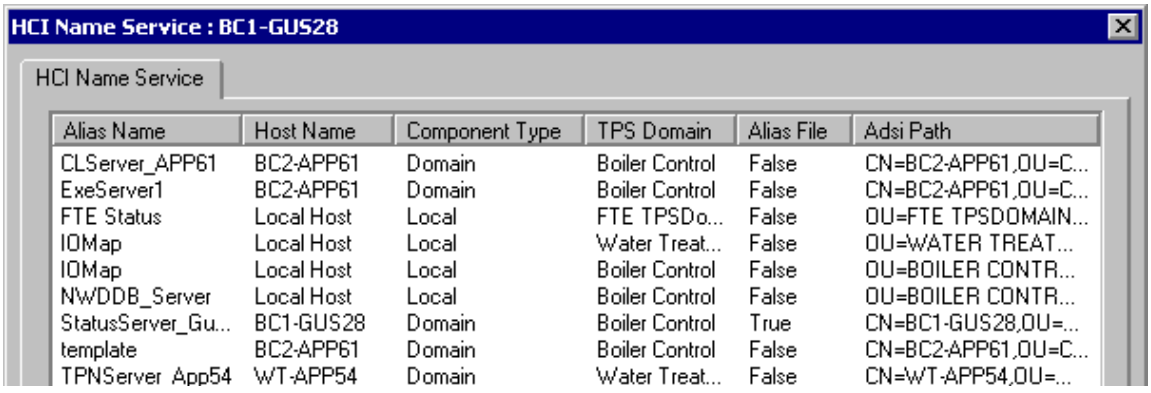
11.2.5 Deleting an HCI component

Prerequisites

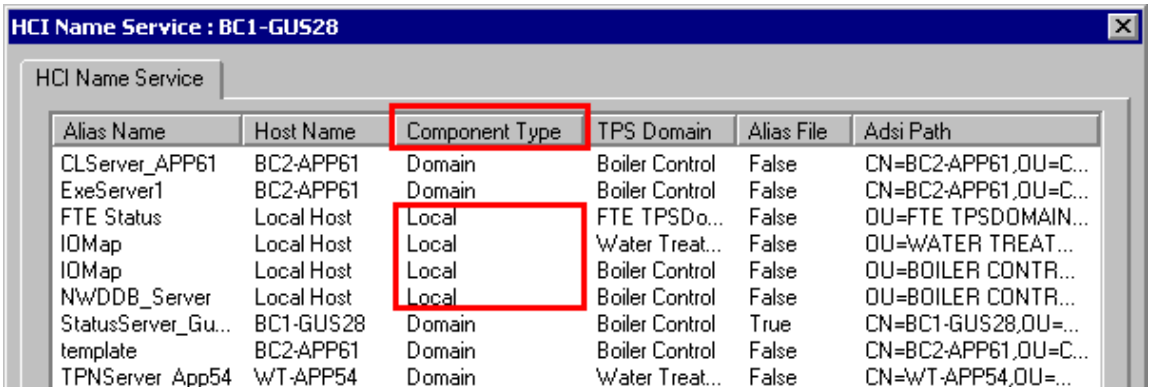
Make sure you have been assigned access privileges to delete a component. You will not see the **Delete Components** button in the Name Service page if you have not been assigned access privileges.

Follow these steps to delete an HCI component.

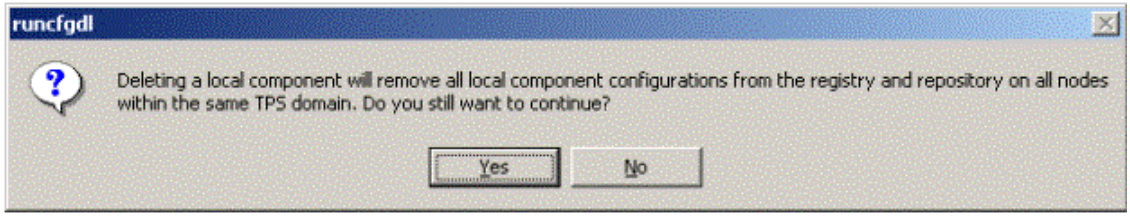
1 From **the HCI Name Service** tool, select the component you want to delete.



2 If you select a local component…



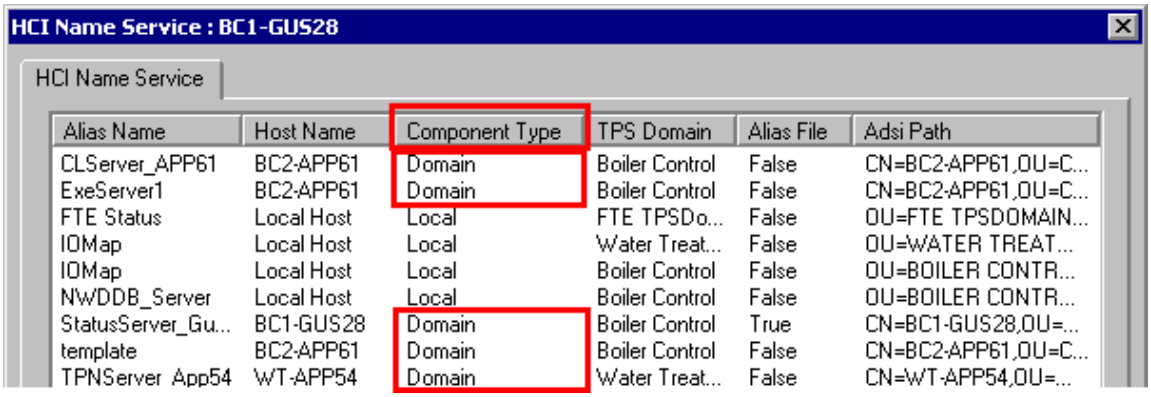
The following prompt message is displayed.



Tip
A local component deletion removes all local component configurations from the registry and repository on all nodes within the same TPS domain.

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.

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.



11.2.6 Scope of the 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 defaults to * indicating all nodes within the IP Multicast group is independent of the Active Directory path.

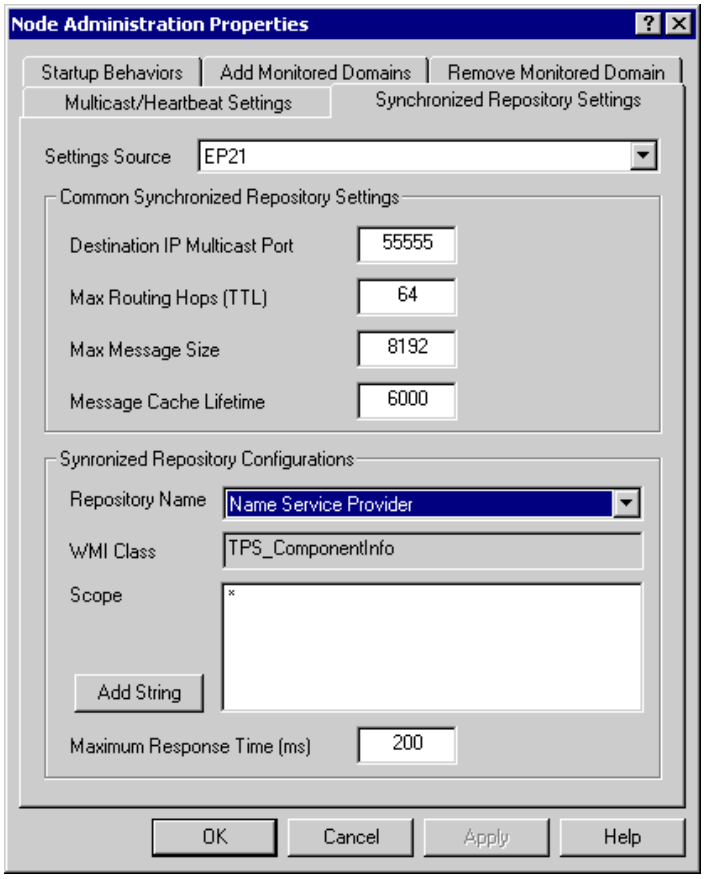
Tip
The SRP uses a single IP Multicast group to synchronize ALL subscribed providers. Each provider specifies the scope of synchronization by registering itself with the SRP with an Active Directory Path.

11.2.7 Setting the scope of the name service repository

Prerequisites

All computers in the console must be on-line, as configuration affects registry. Scope options are described in “Determining the Synchronized Repository Scope” on page 42.

1. Select the Domain or OU within which you want all HCI-NSs to be synchronized. To synchronize multiple domains, select **Node Administration**.
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.



4. The Snap-In enumerates all contained computers, connects to their registry, and sets the scope according to the Snap-In item level selected.

   Snap-In level synchronization applies 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

12.1.1 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.

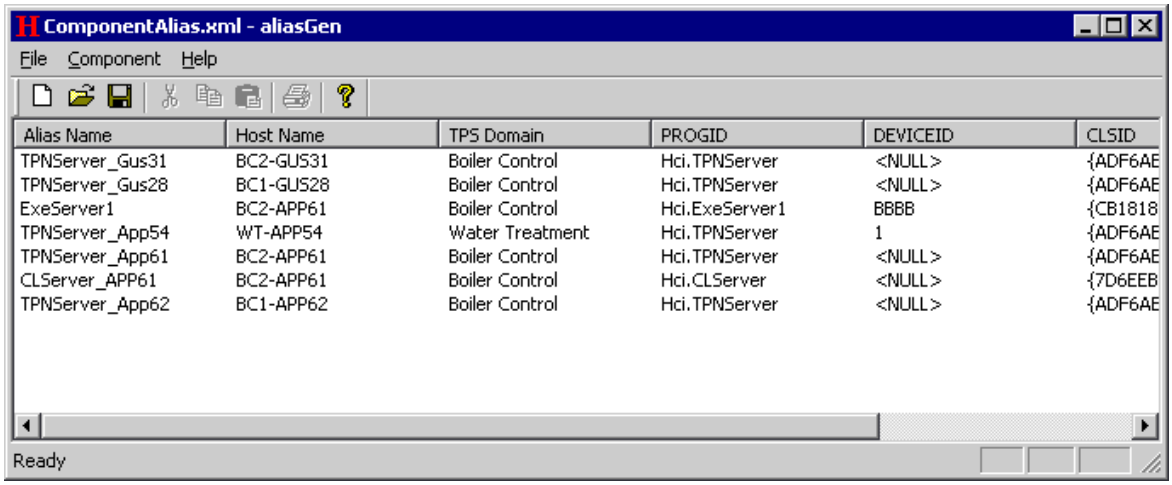


Figure 15: Example Alias File

12.1.2 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 may 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.

12.1.3 ComponentAlias.XML file is required

A blank XML file named ComponentAlias.XML is installed in the *C:\ProgramData\Honeywell\ProductConfig\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. Subsequently you can modify the file and write to it.

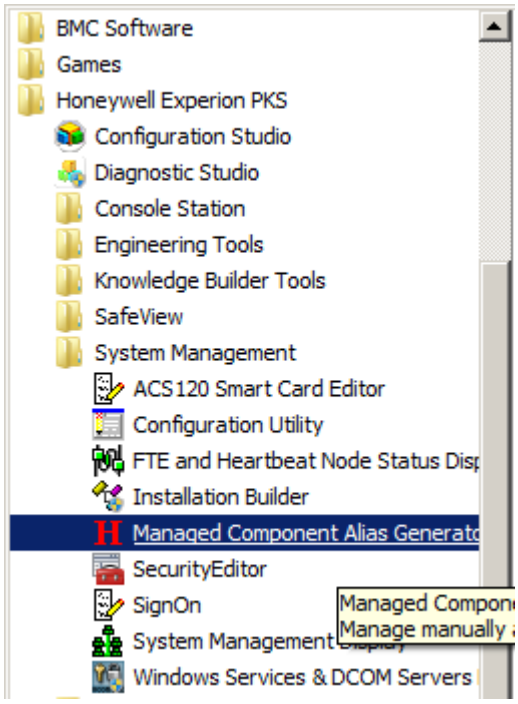
12.1.4 Adding components to a Component Alias file

Attention

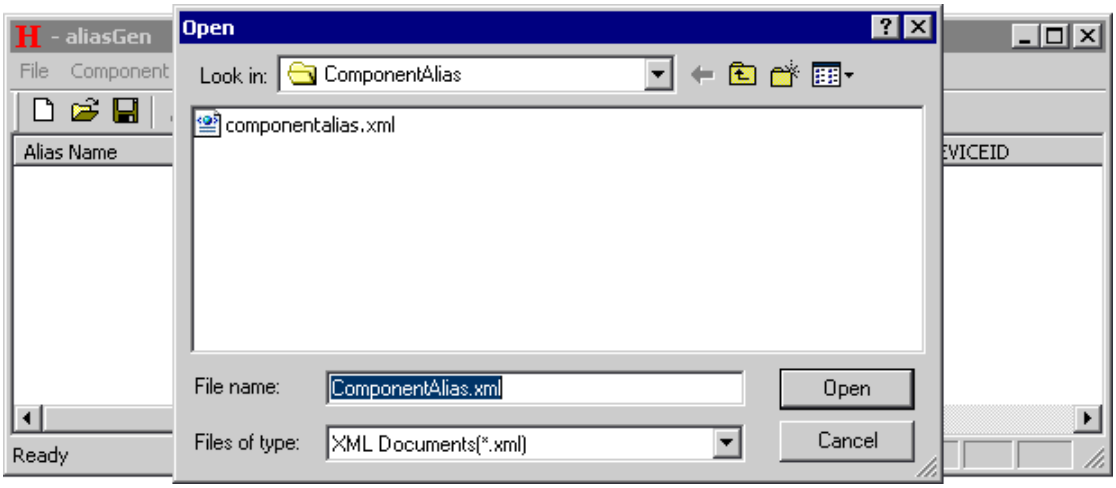
You can create a new Alias file. If this file is not named ComponentAlias.XML, or not stored in the *ProgramData\Honeywell\ProductConfig/Component/Alias* directory, then the Name Service provider WILL NOT read the contents into the repository of this node.

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

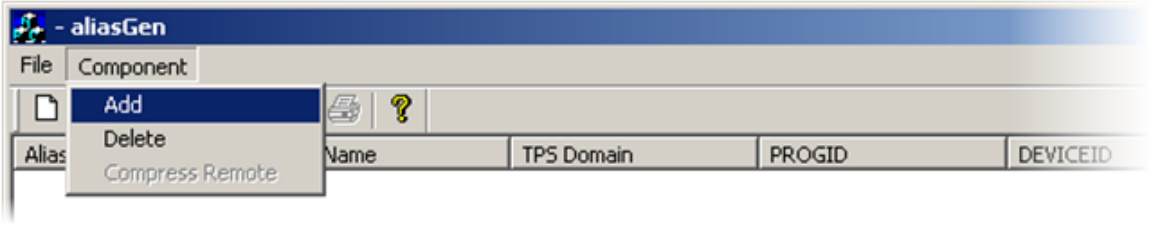
1 Select **Programs** > **Honeywell Experion PKS** > **Managed Component Alias Generator** to start the Alias Generator program.



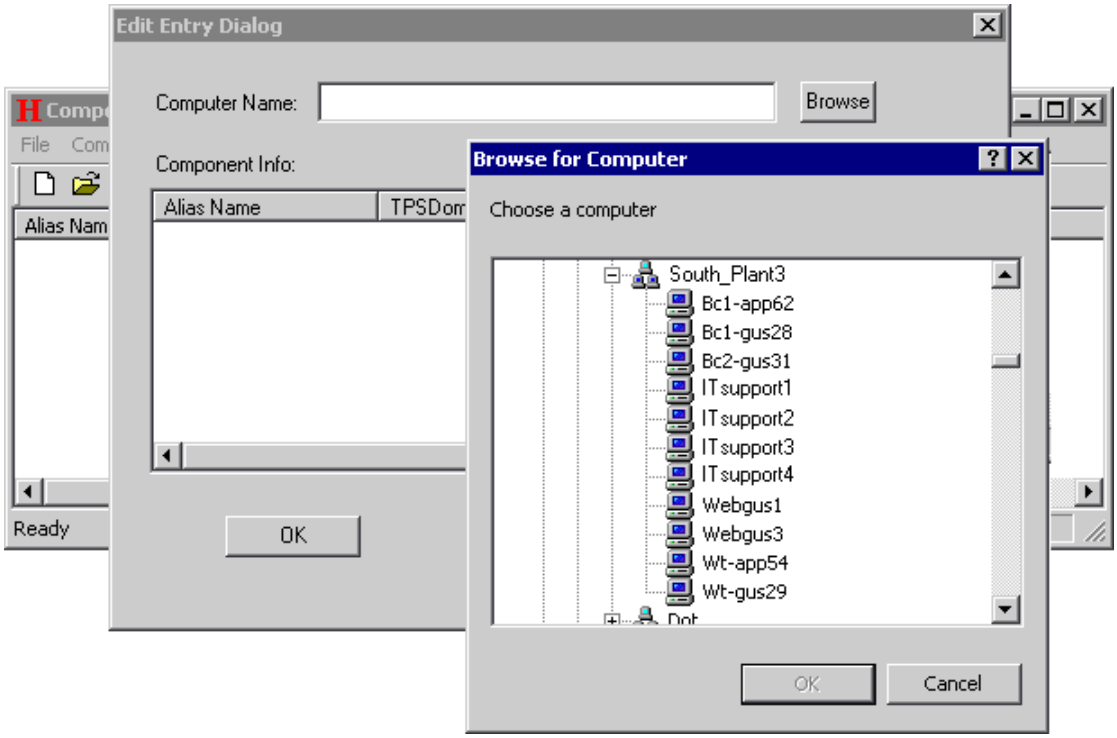
2 Select **File** > **Open** to open the *componentalias.xml* file.



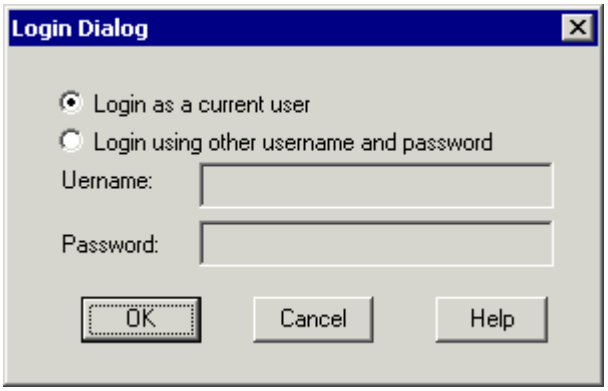
3 To add an entry to your file, select **Component** > **Add**.



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



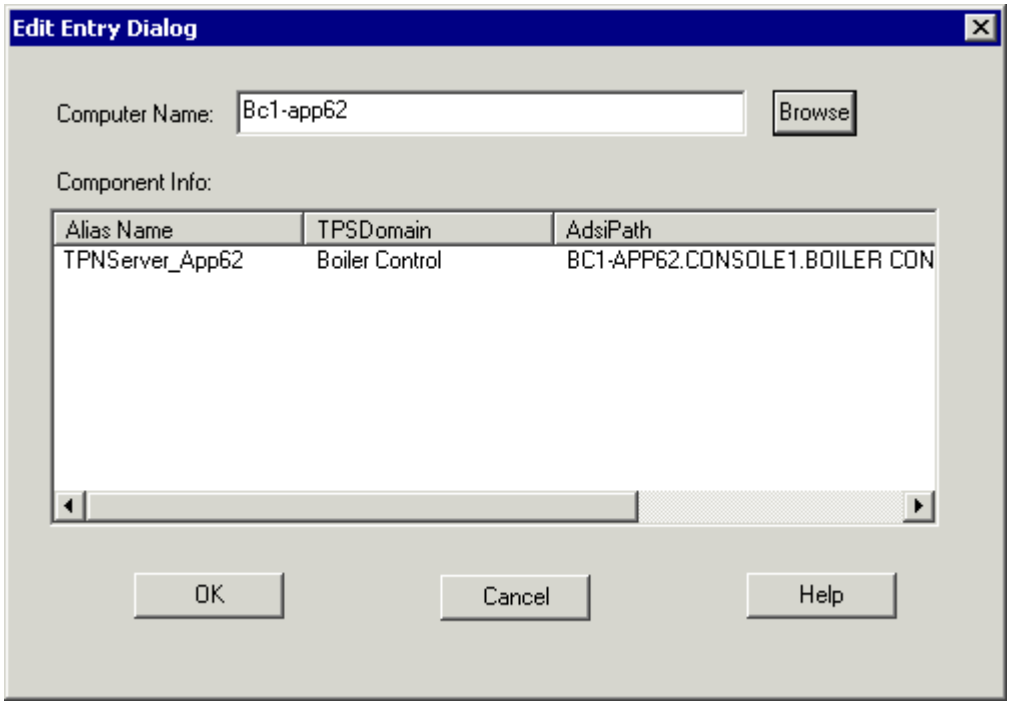
5 Select a computer name from the **Browse for Computer** dialog box, and click **OK.** A new **Login** dialog appears:



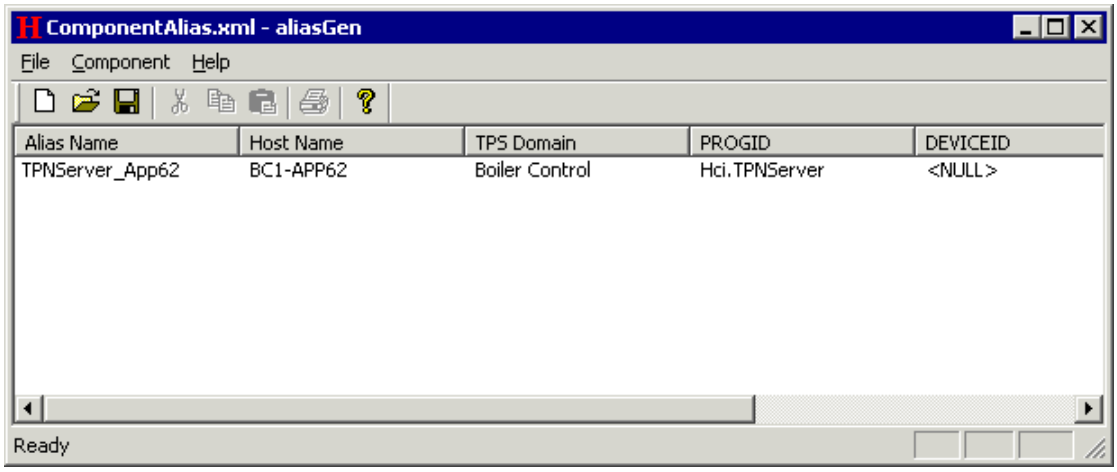
The default username and password are NULL, which means the default user (usually the system administrator) has authority to connect to any computers residing within a specific domain. If you do not have authority to connect to a specific computer, you must input the username and password for that specific computer to connect to it.

6 If both the username and the password you typed for a specific computer are correct, the system connects with the name service provider on that specified remote node.

Result: The **Edit Entry** dialog box appears with the component information.



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.



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.

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:
\ProgramData\Honeywell\ProductConfig\ComponentAlias \ComponentAlias\ComponentAlias.xml

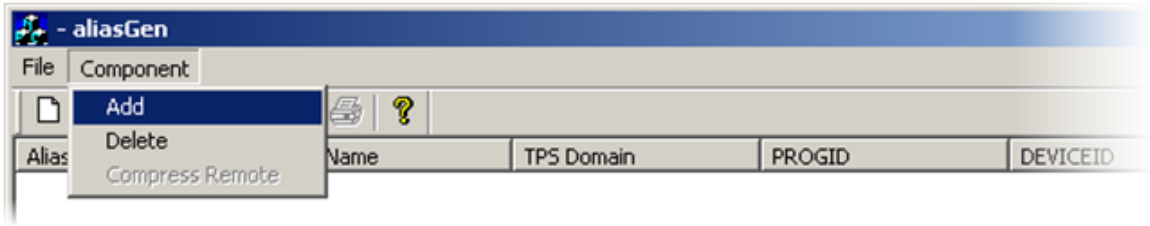
9 Repeat Steps 1-8 for additional nodes of interest.

12.1.5 Deleting a Component from an Alias File

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

1 Select the items to be deleted.

2 Select **Component** > **Delete**.

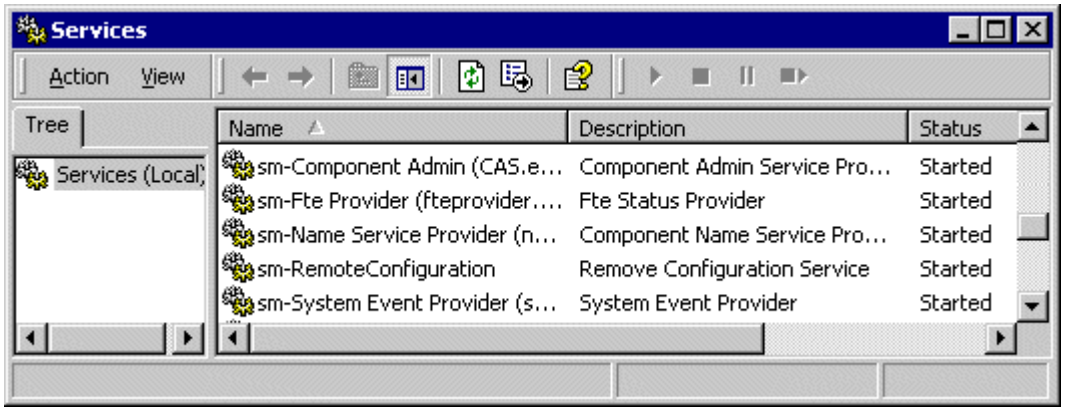


3 Save the file.

13 Troubleshooting System Management

13.1 How to use this section

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 offline when they are really online.	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 Support Information to identify the version. 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.

Symptom	Solution
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 interconnection between switches.	Network Configuration Problem: Check interconnection cable. Check switch configuration. If Nortel switches are utilized, 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 Domain (OU).	Active Directory / TPS Domain Configuration: • 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. • Run ADSITest program to help diagnose the problem. • 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: • System Management Infrastructure is not loaded on the particular node. Install the System Management Infrastructure or System Management Display to correct the problem. • Ensure primary and secondary DNS configuration settings on each TPS node point at the Windows DNS server. • 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. On Server 2008 DCs use the 'dcdiag' command. • Other DNS configuration problem. Open a command prompt and type 'nslookup'. The IP address and name of the DNS server should appear. Account Permissions Problem: • Log in as a Domain User. Local users have a restricted view of domain resources. 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.