Honeywell

Experion PKS
Redirection Manager User's Guide

EPDOC-X116-en-431A
February 2015

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-X116-en-431A	431	0	February 2015

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

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

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

Copyright 2015 - Honeywell International Sàrl

Contents

1 About This Document 7

2 References 9

3 Introduction to Redirection Manager 11

3.1 Role of Redirection Manager 12

3.1.1 Who should use this guide 12

3.1.2 Prerequisite skill sets 12

3.1.3 Terms and acronyms 12

3.2 Architectural Overview 14

3.2.1 Redirection Manager OPC interface support 14

3.2.2 Redirection Manager itself is an OPC server 14

3.2.3 Standalone RDM 14

3.2.4 Redirection Manager Redundancy Modes 14

3.2.5 Redirection Manager Characteristics 15

3.2.6 Failures that cause switchover 15

3.2.7 Special failure detection for TPN Server 15

3.2.8 Passive Redundancy behavior for redundant Experion Servers 15

3.2.9 TPS Domain independence 16

3.2.10 Experion workgroup support 16

3.2.11 Mixed domain and workgroup connections are not supported 16

3.3 How Redirection Manager works 17

3.3.1 Redirection Manager operation overview 17

3.3.2 Multiple client connection support 17

3.3.3 Server versus server node 17

3.3.4 Redirection Manager Redundancy modes 17

3.4 Redirection Manager Operations with Active Redundancy 18

3.4.1 RDM with active redundancy 18

3.4.2 Active Redundancy switchover scenarios 18

3.4.3 Scenario 1: Both target servers are available and running. Switchover occurs 18

3.4.4 Scenario 2: At startup only the Primary server is running. The Secondary server starts up later 18

3.4.5 Scenario 3: The Secondary server is unavailable and the Primary server has failed 19

3.4.6 Scenario 4: The Primary and/or Secondary server(s) become available after having previously failed 19

3.5 Redirection Manager operations with Passive Redundancy 20

3.5.1 Passive redundancy before EPKS switchover 20

3.5.2 Passive redundancy after EPKS switchover 20

3.5.3 Passive Redundancy failover scenarios 21

3.5.4 Scenario 1: Both target servers are available and running. Failover occurs 21

3.5.5 Scenario 2: At startup only the Primary server is running. The Secondary server starts up later 21

3.5.6 Scenario 3: The Secondary server is unavailable; the Primary server has failed 21

3.5.7 Scenario 4: The Primary and/or Secondary server(s) become available after having previously failed 22

3.6 OPC Server availability detection 23

3.6.1 Classic RDM 23

3.6.2 Standalone RDM 23

4 Redirection Manager Planning 25

4.1 Planning Checklist for Redirection Manager 26
4.1.1 Planning Checklist 26
5 Redirection Manager Installation 29
5.1 Installation Requirements 30
5.1.1 Installation strategy 30
5.1.2 Installation media 30
5.1.3 Summary of installation requirements 30
5.1.4 Standalone RDM Installation Requirements 31
5.2 Installing Redirection Manager 32
5.2.1 Installing RDM in a TPS system 32
5.2.2 Installing RDM in a pre-R300 Experion system 32
5.2.3 Installing RDM in R300 and later Experion system 33
5.3 Installing Standalone RDM 34
5.3.1 Installing Standalone RDM in non-Experion or non-TPS system, in a TPS system or in a R300 or later an Experion 34
5.4 Installing Classic RDM 35
6 Redirection Manager Configuration 37
6.1 Configuring Redirection Manager 38
6.1.1 RDM configuration limits 38
6.1.2 Configuration Overview 38
6.1.3 RDM from HCI Component Configuration page 38
6.1.4 RDM from Standalone RDM Configuration page 39
6.1.5 Replicating RDM on nodes in an Experion workgroup 40
6.1.6 Replicating RDM on nodes in a TPS Domain 40
6.1.7 Replicating RDM on nodes in a non-TPS domain 41
6.1.8 Standalone RDM does not support replication 41
6.1.9 Experion and TPN systems component requirements 41
6.1.10 Passive RDM Blocking Time for Experion servers 41
6.1.11 Accessing the RDM Server Specific configuration 41
6.1.12 Configuring RDM Primary and Secondary servers 42
6.1.13 User defined ProgID for Standalone RDM 49
6.2 Configuring status items 50
6.2.1 Status item configuration overview 50
6.2.2 Status item retry count 50
6.2.3 Status item configuration limits 50
6.2.4 Limits Validated at Configuration Time 50
6.2.5 Limits Validated by the RDM at Runtime 51
6.2.6 Configuring status items 51
6.3 Securing Redirection Manager Methods 55
6.3.1 Securing methods for an RDM 55
6.3.2 Securing RDM: manual switchover method 55
6.3.3 Defining Security on Synchronization 61
6.4 Configuring Remote Node Status Detection 62
6.4.1 About remote node status detection 62
6.4.2 ICMP Echo alternative to WMI client notification 62
6.4.3 ICMP Echo configuration settings 62
6.4.4 Detection mechanism applies to specific Redirection Manager 63
6.4.5 Configuring ICMP Echo for remote node status detection 63
7 OPC Client and OPC Server Support 65
7.1 Support for OPC Interfaces 66
7.1.1 Support OPC DA and A&E interfaces and methods 66
7.1.2 Support OPC HDA interfaces and methods 66
7.1.3 Maintaining state information 66

7.1.4 About client callbacks 67
7.2 OPC Alarm and Event Interfaces 68
7.2.1 Alarm and Event interface approach 68
7.2.2 Constraints for third-party OPC Alarm and Event Servers 68
7.3 OPC Historical Data Access Interfaces 69
7.3.1 Historical Data Access approach 69
7.4 HCI Value-Added Interfaces 70
7.4.1 Support for HCI added-value interfaces 70
7.5 Error Handling 71
7.5.1 Types of errors 71
7.5.2 I/O request error behavior 71
7.5.3 Non I/O request error behavior 71
7.5.4 OPC call and error matrix 71
7.5.5 WMI Provider errors 71
8 Redirection Manager Status 73
8.1 Monitoring RDM Status 74
8.1.1 About Redirection Manager Status monitoring 74
8.1.2 Monitoring Redirection Manager from the Auxiliary Status Display 74
8.2 Viewing RDM on system displays 75
8.2.1 Viewing RDM on Experion's System Status Display 75
8.2.2 RDM on the System Management Display 76
8.2.3 Viewing RDM on System Management Display 76
8.2.4 RDM on the Standalone RDM configuration display 77
8.2.5 Redirection Manager Auxiliary Status Display when Active RDM connected 78
8.2.6 Auxiliary Status Display when Passive RDM connected 79
8.2.7 Redirection Manager Auxiliary Status Display description 80
8.3 Viewing logged events 81
9 Notices 83
9.1 Documentation feedback 84
9.2 How to report a security vulnerability 85
9.3 Support 86
9.4 Training classes 87

1 About This Document

This document describes how to plan, configure, and support Redirection Manager. It also describes how to support OPC client and server. This guide is intended for the following users:

- *System Engineers* who need to configure Redirection Manager.
- *HCI/OPC Client Developers* who want to provide high availability to their HCI/OPC client applications.
- *System Administrators* who need to install Redirection Manager and secure its methods.

Revision history

Revision	Date	Description
A	December 2013	Initial release of document.

Revision history

Revision	Date	Description
A	February 2015	Initial release of document.

2 References

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

Document Title	Doc ID
HCI Client Developer's Guide	TP60
OPC Specifications Reference Manual	TP41
System Management Configuration Guide	EX08
TPS System Implementation Guide for Windows 20003/XP	TP08X
TPS System Planning Guide	TP10X
Experion Server and Client Configuration Guide.	

3 Introduction to Redirection Manager

Related topics

“Role of Redirection Manager” on page 12
“Architectural Overview” on page 14
“How Redirection Manager works” on page 17
“Redirection Manager Operations with Active Redundancy” on page 18
“Redirection Manager operations with Passive Redundancy” on page 20
“OPC Server availability detection” on page 23

3.1 Role of Redirection Manager

Redirection Manager (RDM) provides high availability and reliability of OPC client connections to OPC Servers. The Redirection Manager enables OPC clients to transparently redirect requests to an alternate OPC server. Redirection occurs whenever RDM detects a failure in the Active server of a configured Primary OPC server and Secondary OPC server pair. OPC clients needing redirection connect to the Redirection Manager instead of connecting to the Primary OPC server. Redirection Manager supports connection to HCI/OPC server pairs hosted on Experion PKS and TPS platforms.

3.1.1 Who should use this guide

This guide is intended for the following users:

- *System Engineers* who need to configure Redirection Manager.
- *HCI/OPC Client Developers* who want to provide high availability to their HCI/OPC client applications.
- *System Administrators* who need to install Redirection Manager and secure its methods.

3.1.2 Prerequisite skill sets

This guide assumes a user's configuration support team is familiar with

- Configuring OPC Servers and OPC Client applications,
- Configuring the target server of interest. The target server can be, for example, an Experion HCI Server hosted on an Experion Server node or a TPN Server hosted on an APP Node, and
- Configuring System Management components. These components provide an infrastructure that includes configuration displays and status monitoring.

3.1.3 Terms and acronyms

The following terms and acronyms specific to Redirection Manager are used in this guide in the following context.

Attention
Redundancy, when supported with Redirection Manager, has additional meaning that differs from conventional usage of the term. Review the terms as needed in the context of the system you are intending to support Experion or TPN.

Term	Definition
Primary OPC Server	The Primary OPC server communicates with client data sources, and is configured to be the Primary for an RDM. The same OPC Server could be configured as a Secondary Server for another RDM.
Secondary OPC Server	A Secondary OPC server that can provide the same functionality as the Primary server and is configured as the backup server for the Primary OPC server. This server can be configured as a Primary OPC server for another RDM.
Active OPC server	The Active OPC server that is currently servicing OPC calls. It can be either the Primary Server or the Secondary Server. The Secondary server becomes the Active server when the Primary server fails.
Windows Management Instrumentation (WMI)	WMI is a unified architecture for describing, accessing, and instrumenting objects. WMI has a large database of WMI classes used to carry out remote management tasks on specific objects.
Redundancy	Redundancy is the mode by which data flow is switched from one OPC server to another in the event of a failure. For RDM there are two distinct redundancy mechanisms: Active Redundancy and Passive Redundancy. During installation, target OPC servers establish the redundancy mode.

Term	Definition
Active Redundancy	An RDM in the Active Redundancy mode detects failures and initiates failover. In this mode, RDM maintains the secondary server as a hot standby when it echoes client-to-primary OPC calls to the secondary. On detecting a failure, the RDM promotes the secondary server to primary status and re-initiates pending calls on that new primary. A TPN Server is an example of a Honeywell HCI server that operates under the active redundancy mode.
Passive Redundancy	Passive Redundancy is called 'passive' because a failover in this mode is initiated from the redundant server node platform and not from RDM. RDM also detects that the failover is in progress and blocks all OPC calls pending failover completion or a user-configured timeout. An RDM in the Passive Redundancy mode detects node failover and reacts to such a failover by injecting the new Primary server (running on the new primary node) with a snapshot of the failed server's OPC state. The Experion OPC Server hosted on redundant Experion Server nodes is an example of an OPC server that operates under the passive redundancy mode.
Status Item	OPC Data Access item that represents in some way the status associated with the Target OPC Data Access server and its underlying communication system. This status item is 'owned' by the target OPC server. Therefore, the OPC server is responsible for establishing the status item, defining valid values, obtaining values from the underlying communication system, etc. OPC Data Access clients are able to access that item with any of the existing OPC Data Access read mechanisms. An OPC server may not allow writes to the status item.
Standalone RDM	Standalone RDM, also called 'Simplified RDM' is a fully functional RDM that has no dependency on System management components and WMI. This is an optional feature included with the existing RDM product that is selected by the user during product installation.

REFERENCE: For more information, refer to the *Dictionary* for Experion and TPS_Reference for TotalPlant systems.

3.2 Architectural Overview

3.2.1 Redirection Manager OPC interface support

Redirection Manager supports the following OPC interfaces:

- OPC Data Access 2.05
- OPC Data Access 2.0
- OPC Data Access 1.0A
- OPC Alarms and Events 1.0
- OPC Historical Data Access (HDA) 1.2

The extent of OPC support is described later in this guide.

3.2.2 Redirection Manager itself is an OPC server

The Redirection Manager has the registry settings required by an OPC server per OPC specifications. From the perspective of an OPC client, these OPC registry settings make the Redirection Manager look like any other OPC server. An RDM server is also an HCI server. Existing HCI clients connect to the RDM server the same way as they connect to HCI servers. Each configured RDM has a unique HCI alias name.

3.2.3 Standalone RDM

The Standalone RDM is a new version of RDM that does not require any system management components to be installed on either client or server nodes. The core functionality of RDM remains unchanged in this version. Features in the classic RDM that were provided by the System management components have now been built into the Standalone RDM. Examples are:

- OPC Server availability and node detection
- Configuration utility
- Status display

These changes are described later in this guide.

The Standalone RDM is appropriate for situations where 3rd party client or server nodes are involved and installation of System management components is cumbersome or in most cases users do not want the tighter system integration provided by these components. Examples include,

1. PHD, a Honeywell OPC client application that requires robust OPC connectivity without having to install and configure System management components on the PHD node.
2. Experion systems install a thin version of System management that does not support the classic version of RDM. The Standalone RDM is appropriate for this system.
3. Experion OPC client applications that connect to redundant 3rd party OPC server nodes and Honeywell components cannot be installed on the OPC server nodes.

The classic RDM is still the best option when tighter integration with the entire Experion system is needed.

3.2.4 Redirection Manager Redundancy Modes

Redirection Manager has two redundancy modes:

Active Redundancy	An RDM in the Active Redundancy mode detects failures and initiates failover. In this mode, RDM maintains the secondary server as a hot standby when it echoes client-to-primary OPC calls to the secondary. On detecting a failure, the RDM promotes the secondary server to primary status and re-initiates pending calls on that new primary. A TPN Server is an example of a Honeywell HCI server that operates under the active redundancy mode.
Passive Redundancy	Passive Redundancy mode is called “passive” because a failover in this mode initiates from the redundant server node platform and not from RDM. RDM detects that the failover is in progress and blocks all OPC calls pending failover completion or a user-configured timeout. An RDM in the Passive Redundancy mode detects node failover and reacts to such a failover by injecting the new Primary server (running on the new primary node) with a snapshot of the failed server’s OPC state. The Experion OPC Server hosted on redundant Experion Server nodes is an example of an OPC server that uses passive redundancy mode.

3.2.5 Redirection Manager Characteristics

Redirection Manager has the following characteristics:

- Forwards client calls to OPC servers.
- Maintains information for switching to a Secondary OPC server when the Primary OPC server fails.
- Establishes or re-establishes connection to the Primary OPC server and its Secondary OPC server.
- Monitors the availability of Primary and Secondary OPC servers, and takes appropriate actions that prevent a ‘bad' status from being returned to the client when servers fail.
- Allows manual switchover to a Secondary OPC server from the RDM Auxiliary Status Display. This only applies to target OPC servers using Active Redundancy.

3.2.6 Failures that cause switchover

Typical failures that cause switchover to occur include:

- The OPC server process fails (Active Redundancy only)
- The node hosting the OPC server fails.
- The network fails between client and OPC server node.
- Status item values match the criteria established by the user on the status item configuration page.

3.2.7 Special failure detection for TPN Server

A TPN server is running but has a Warning status due to a bad connection to the LCN.

3.2.8 Passive Redundancy behavior for redundant Experion Servers

Experion Server Nodes can be switched over following Experion Servers procedures or scenarios described in the Server and Client Configuration Guide > Configuring and Monitoring a Redundant Server System. When connected to a target server that uses the Passive Redundancy mode, users should note the following:

- In the RDM's Auxiliary Status Display, Manual SwitchOver is disabled for the Experion HCI Server.
- In the RDM's Auxiliary Status Display, Manual Synchronization is disabled for the Experion HCI Server.
- OPC entities (groups, items, subscriptions, etc.) are added to the secondary Experion HCI Server only after an Experion node failover.
- RDM configuration allows the user to establish additional blocking time. Blocking time refers to the maximum time in seconds that the RDM will wait for the switchover to complete. All client methods are blocked until the switchover completes or the blocking time expires.
- Redirection Manager Automatic SwitchOver of OPC client calls to the backup Experion Server occurs only after Experion node failover from primary Experion Server to backup Experion server.
- RDM configuration enforces a node-naming convention: Names may differ only by suffix 'A' and 'B'.

3.2.9 TPS Domain independence

A TPS Domain is not required for RDM configurations. RDM utilizes System Management components designed to execute within or without a TPS Domain. These System Management components provide the HCI Name Service support of earlier TPS Domain configurations as well as other services described in the *System Management Configuration Guide*.

3.2.10 Experion workgroup support

An Experion workgroup can support RDM configuration as described in this guide. RDM utilizes System Management components designed to execute within a workgroup configuration. This requires installation of System Management runtime components described in the *System Management Configuration Guide*.

3.2.11 Mixed domain and workgroup connections are not supported

Redirection Managers connections are not supported when

- The client application resides on a node in a workgroup and the target server resides on a host node in a domain, or
- The client application resides on a node in a domain and the target server resides on a host node in a workgroup.

Attention
Configuring an RDM connection across workgroup and domain nodes is not supported.

3.3 How Redirection Manager works

3.3.1 Redirection Manager operation overview

When RDM is deployed, the OPC client application connects to RDM exactly as it connects to any OPC server. OPC client application issues requests to RDM in the same way it would issue calls to the target OPC server as if it were directly connected to the target OPC server. No user configuration changes are required to the OPC Server to support Redirection Manager.

3.3.2 Multiple client connection support

Both examples in the following figures for Experion and TPN systems illustrate a *single client* connection through RDM to target servers. It is also possible to have *multiple client* connections to target servers. The clients can:

- Reside either on the same node or on different nodes.
- Connect through the same RDM or a different RDM.

Furthermore, a single client application can have multiple connections to different RDMs.

3.3.3 Server versus server node

This document frequently refers to target OPC servers, HCI servers, Experion HCI servers, and TPN servers. In this context, 'server' represents a software component residing on a server node.

When the document refers to 'server node,' the terms represent a hardware device such as a redundant Experion server or an APP node.

3.3.4 Redirection Manager Redundancy modes

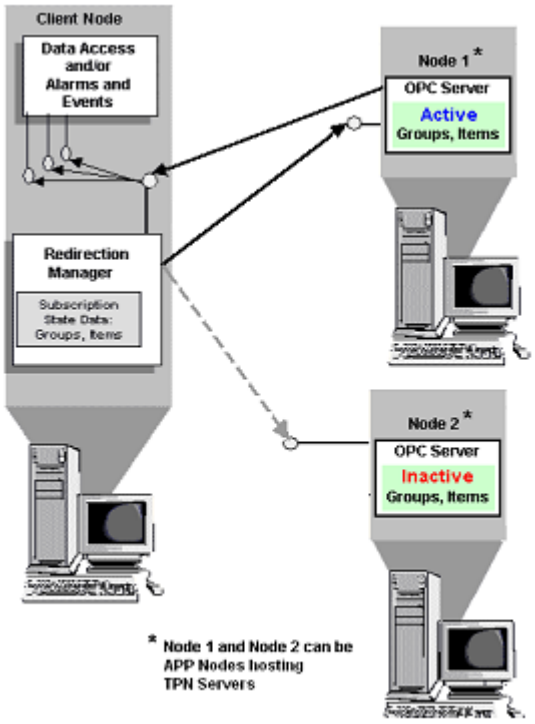
Redirection Manager Operation is influenced through the enabling of either a Passive Redundancy or Active Redundancy mode. When connecting RDM to an Experion HCI server hosted on redundant Experion Server nodes, the target OPC server enables a Passive Redundancy mode. When connecting RDM to an OPC server such as the TPN Server hosted on an APP Node, the target OPC server enables an Active Redundancy mode.

3.4 Redirection Manager Operations with Active Redundancy

Redirection Manager is an OPC server installed on client nodes.

3.4.1 RDM with active redundancy

In the following figure, a configured Redirection Manager connects to two OPC servers from a client node. The client node uses standard COM connections to connect to the Redirection Manager instead of, as in our example, the OPC Server. The example shows Redirection Manager configured to recognize one OPC server as the Primary (Active) server and the other OPC server as the Secondary (Inactive) server.



3.4.2 Active Redundancy switchover scenarios

RDM forwards the client requests to the target servers based on their availability, as described in the following Active Redundancy scenarios. These scenarios typically apply to TPN Server and other HCI/OPC servers.

3.4.3 Scenario 1: Both target servers are available and running. Switchover occurs

RDM creates *active* groups and subscriptions on the Primary; however, the groups and subscriptions are *inactive* on the Secondary. If the Primary fails, RDM performs the switchover to the Secondary server by activating the existing entities.

3.4.4 Scenario 2: At startup only the Primary server is running. The Secondary server starts up later

For a redundant Experion Server configuration, this scenario is the same as the previous because RDM does not add any OPC entities until the failover is complete.

3.4.5 Scenario 3: The Secondary server is unavailable and the Primary server has failed

If the Primary server fails, RDM has no alternate server to switchover to, and therefore returns an ‘E_FAIL' error message for any calls made by the client.

3.4.6 Scenario 4: The Primary and/or Secondary server(s) become available after having previously failed

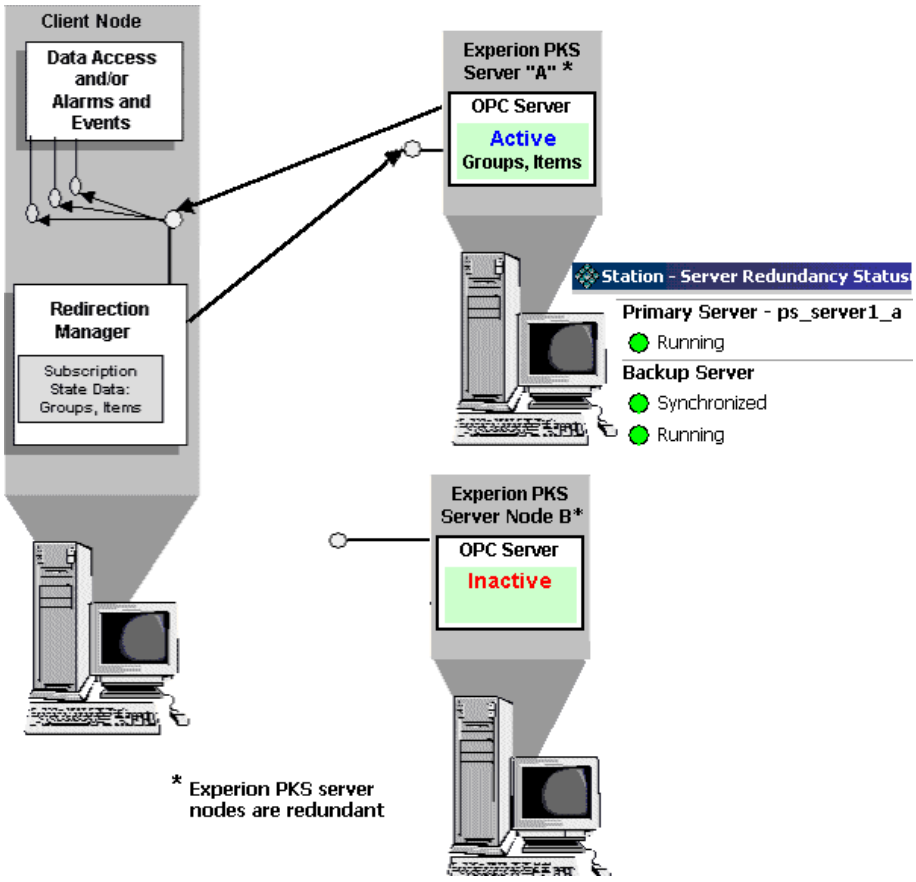
RDM creates *active* groups and subscriptions on the new Primary, however the groups and subscriptions are *not* created on the new Secondary.

3.5 Redirection Manager operations with Passive Redundancy

Redirection Manager is an OPC Server installed on client nodes.

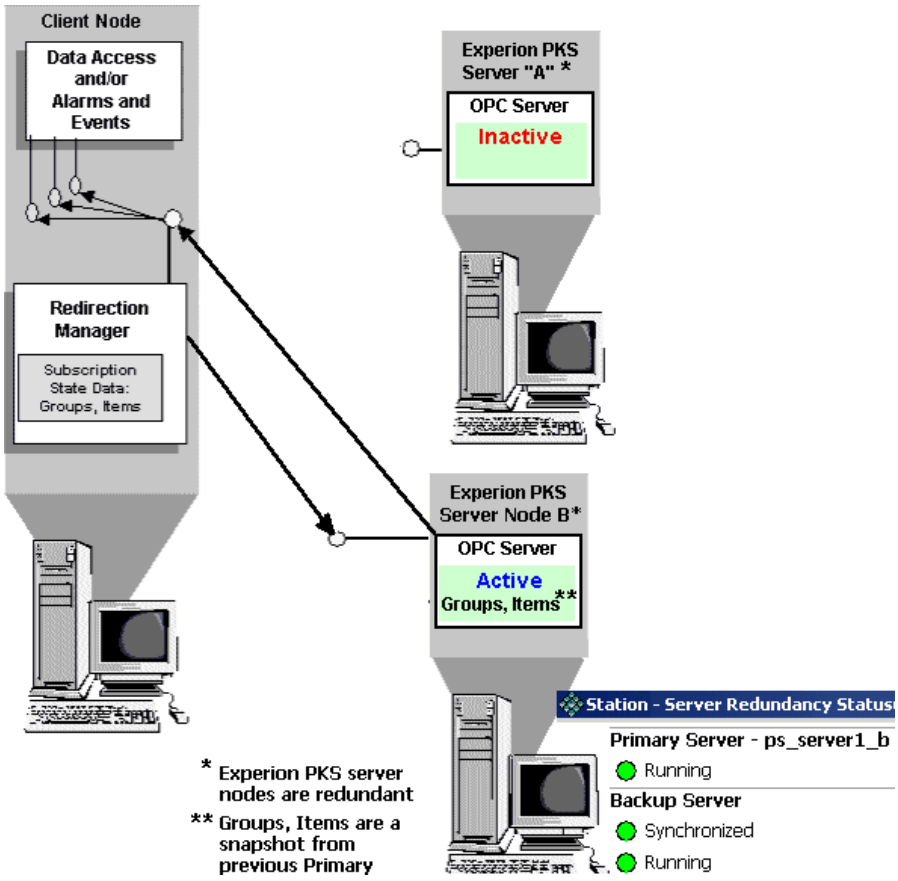
3.5.1 Passive redundancy before EPKS switchover

In the following figure, a Redirection Manager connects to an Experion HCI server residing on redundant Experion Server nodes. The figure also shows that Experion Server node 'A' is currently the primary and Node 'B' is currently the backup. The example shows RDM configured to connect to an Experion HCI server, which is an OPC server. RDM regards the OPC server hosted on the Experion Server 'A' as the Active server. Since the Experion OPC Server participates in the Experion redundant server scheme, the secondary OPC server is not a hot standby. Furthermore, RDM must wait for the Experion server node switchover to complete before switching over to the secondary OPC server.



3.5.2 Passive redundancy after EPKS switchover

The following figure shows that after switchover occurs, the Experion server node switches over to the backup node. RDM then adds to the new primary a snapshot of all of the OPC entities that existed on the former primary.



3.5.3 Passive Redundancy failover scenarios

RDM forwards the client requests to the target OPC server based on its availability, as described in the following Passive Redundancy scenarios. These scenarios apply to Experion HCI servers hosted on redundant Experion Server nodes.

3.5.4 Scenario 1: Both target servers are available and running. Failover occurs

RDM creates *active* groups and subscriptions on the Primary, however the groups and subscriptions are *not* created on the Secondary. If the Primary node fails, the Experion server fails over to the backup node. RDM then adds to the new primary all of the OPC entities that existed on the former primary. During a failover, client requests are blocked. If the node failover completes within blocking timeout, all pending client requests resume execution on the new primary. If the node failover does not complete within that blocking time, all pending client requests fail.

3.5.5 Scenario 2: At startup only the Primary server is running. The Secondary server starts up later

For a redundant Experion Server configuration, this scenario is the same as the previous because RDM does not add any OPC entities until the failover is complete.

3.5.6 Scenario 3: The Secondary server is unavailable; the Primary server has failed

If the Primary server fails, RDM has no alternate server to switchover to, and therefore returns an ‘E_FAIL' error message for any calls made by the client after the blocking timeout occurrence.

3.5.7 Scenario 4: The Primary and/or Secondary server(s) become available after having previously failed

RDM creates *active* groups and subscriptions on the new Primary, however the groups and subscriptions are *not* created on the new Secondary.

3.6 OPC Server availability detection

3.6.1 Classic RDM

Redirection Manager's mechanism for detecting OPC server availability leverages Windows Management Instrumentation (WMI) Providers that are installed with the Honeywell System Management Runtime package.

Windows Management Instrumentation providers service clients with database-like query capabilities and event notification. Redirection Manager has a built-in WMI client that notifies Redirection Manager when the status of the Primary and/or Secondary OPC server changes. The WMI client queries the providers for the following information:

- Availability of the nodes on which the OPC servers are running.
- Availability of the OPC servers.

3.6.2 Standalone RDM

In the case of the Standalone RDM, detecting OPC server availability is done by periodically calling GetStatus() on the OPC servers. To detect node availability, the existing ICMP Ping mechanism is used and will be the only mechanism supported in this version.

4 Redirection Manager Planning

Related topics

“Planning Checklist for Redirection Manager” on page 26

4.1 Planning Checklist for Redirection Manager

4.1.1 Planning Checklist

The following checklist identifies several planning considerations and references.

☑	Planning Consideration	Reference
	OPC Client and OPC Server	
	Verify software requirements (Windows operating system) for OPC Client and OPC server hosting nodes.	Software Change Notice (SCN) with product
	Determine which OPC Servers are to be in a primary and secondary relationship for each RDM.	Your site's documentation
	For the OPC Servers that are to be in a primary and secondary relationship, do the following for each RDM: • Verify that Class Ids are the same • Verify that OPC interfaces support a common set of initiatives (per Data Access and per Alarm and Events) • Verify that primary and secondary servers reside on different nodes • Have similar LCN personalities on the Primary and Secondary target nodes if target nodes are Experion or TPS nodes (that is, AM to AM, US to US). • If the OPC server is hosted in a redundant Experion server, determine if system loading may require allowing additional time for switchover. • If the OPC server is hosted in a TPN node, verify that Device Ids are the same	• Redirection Manager Configuration section in this manual • Your site's documentation
	• Review multicast support to verify if client and server can communicate across a firewall or router. If multicast is not supported between client and server nodes due to router or firewall constraints, verify that ICMP echo ('ping') is supported.	• Redirection Manager Configuration section 4.3 in this manual
	Install and configure System Management components on client and server.	EX08 System Management Configuration Guide
	Install Redirection Manager on OPC client.	Redirection Manager Installation section
	Code OPC client application to connect to RDM instead of OPC Server.	TP60 HCI Client Developer's Guide
	Experion System	
	If the client nodes are configured in a workgroup and they require client data, install RDM on each node.	Redirection Manager Installation section
	If the client nodes are configured in a workgroup and they require client data, configure RDM on each node.	Redirection Manager Configuration section
	Secure methods for OPCRead and OPCWrite on target OPC server (not on RDM).	• TP60 HCI Client Developer's Guide • EX08 System Management Configuration Guide
	TPN System	
	If the GUS nodes *are not* configured in a TPS Domain and GUS nodes require client data, install RDM on each node.	Redirection Manager Installation section

☑	Planning Consideration	Reference
	If the GUS nodes *are not* configured in a TPS Domain and GUS nodes require client data, configure RDM on each node.	Redirection Manager Configuration section
	If the GUS nodes *are* configured in a TPS Domain and GUS nodes require client data, install RDM on each node. (Configuration of RDM on each TPS Domain resident node occurs automatically as a result of replication.)	Redirection Manager Installation section
	Determine who can access secured methods for switching over and synchronizing an RDM.	Redirection Manager Configuration > Securing Methods section
	Secure methods for OPCRead and OPCWrite on target OPC server (not on RDM).	• TP60 HCI Client Developer's Guide • EX08 System Management Configuration Guide

5 Redirection Manager Installation

Related topics

“Installation Requirements” on page 30
“Installing Redirection Manager” on page 32
“Installing Standalone RDM” on page 34
“Installing Classic RDM” on page 35

5.1 Installation Requirements

5.1.1 Installation strategy

The RDM installation package includes the Redirection Manager, HCI Runtime, and System Management Runtime. This package should be installed on every node that runs an OPC client requiring redirection.

Attention
Make sure that RDM is installed on every node that runs an OPC client requiring redirection.

The System Management Runtime package contains the WMI Providers used for server availability notification on all nodes that have OPC servers. This package MUST be installed on server nodes that host target OPC servers if the OPC servers are to be part of the redundant pair of OPC servers for a configured Redirection Manager.

5.1.2 Installation media

System	Description
Experion	Use the Experion Application DVD on Client and Server nodes to implement Redirection Manager in an R300 and later Experion system. For Experion systems, the Network tree in the Experion System Status display supports monitoring RDM status - installation of the System Management display is optional.
TPS	Use the TPS System Software CD on Client and Server nodes to implement Redirection Manager in a TPS or pre-R300 Experion system.

5.1.3 Summary of installation requirements

If node contains an…	Install these packages…	The packages contain:
OPC Client	Redirection Manager	• System Management Runtime • HCI Runtime components • Redirection Manager
	(Optional) System Management Display Package	• System Management Display
OPC Server	System Management Runtime	• System Management Runtime • HCI Runtime components
	(Optional) System Management Display Package	• System Management Display

Attention
Honeywell recommends installation of the System Management Display. Without it, you will have difficulty knowing the RDM status.

REFERENCE: Refer to the *System Management Configuration Guide* for procedures on how to install the System Management Display or System Management runtime components.

5.1.4 Standalone RDM Installation Requirements

For Standalone RDM, install the RDM package on the client node. No Honeywell software needs to be installed on the server nodes. The package comes with a built in application that can be used for both configuring and viewing status of Standalone RDMs. When installing on non-TPS or non-Experion nodes, minimum OS requirements are Windows XP SP3 or higher for workstation platforms and Windows Vista SP2 or higher for server platforms. Both 32 bit and 64 bit platforms are supported.

5.2 Installing Redirection Manager

This section contains instructions for the following installation procedures:

- "Installing RDM in a TPS system" on page 32
- "Installing RDM in a pre-R300 Experion system" on page 32
- "Installing RDM in R300 and later Experion system" on page 33

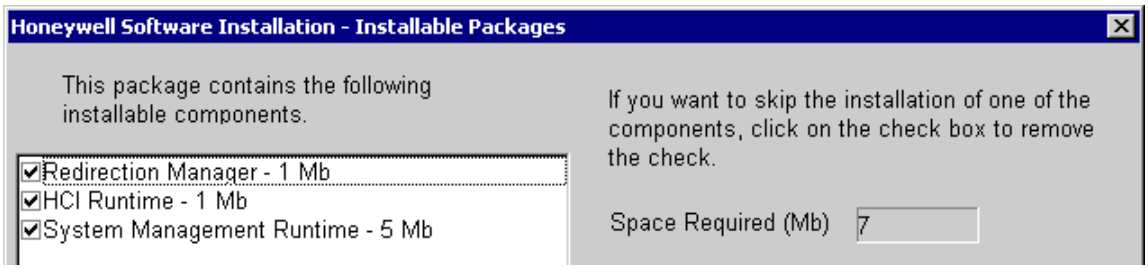
5.2.1 Installing RDM in a TPS system

1. Insert the **TPS System Software CD** into the CD-ROM drive.
   Note: If the menu does not appear**,** select**<drive>:\I386\Packages>Install.**
2. Select **Licensed Package Installer** from the menu.
3. Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue.
4. Enter license and authorization numbers. Click **Next** to continue
5. Select **Redirection Manager** from the list box and click **Install Package**.
6. When the **Honeywell Software Installation - Installable Packages** screen appears, click **OK**.
   Result: The installation process occurs, which can take a few minutes.
7. After a successful installation, the screen in the previous step appears. Click **Exit** and **Yes** to end the RDM installation process.
8. Repeat the previous steps for any other client nodes requiring an RDM installation.

5.2.2 Installing RDM in a pre-R300 Experion system

Attention
R300 and later Experion users do not need to follow these steps, because the Redirection Manager can be installed as part of the Experion installation. Users of Experion R210 and earlier should follow these steps to install Redirection Manager.

1. Insert the **Common Components CD** into the CD-ROM drive.
   Note: If the menu does not appear, select **<drive>:\Package>Install**.
2. Select **Licensed Package Installer** from the menu.
3. Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue.
4. Enter license and authorization numbers. Click **Next** to continue
5. Select **Redirection Manager** from the list box and click **Install Package**.
6. When the **Honeywell Software Installation ? Installable Packages** screen appears, click the **OK** button.



Result: The installation process occurs, which can take a few minutes.

7 After a successful installation, the screen in the previous step appears. Click **Exit** and **Yes** to end the RDM installation process.

8 Repeat the previous steps for any other client nodes requiring an RDM installation.

5.2.3 Installing RDM in R300 and later Experion system

Attention

R300 and later Experion users *may not need* to perform these steps on an Experion node, as Redirection Manager can be installed during Experion node installation. Experion users only need to perform this procedure if there is a need to add Redirection Manager to a client or Experion node.

1 Insert the **Experion Application DVD** and launch the Honeywell software Installation application at **<drive>:\Packages\Install.exe**

2 Review the information about installing software, license agreements, and third-party compatibility on the next several screens. Click **Next** to continue.

3 Enter license and authorization numbers. Click **Next** to continue.

4 Click **Redirection Manager.**

5 Click **Install Package**.

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

7 Repeat the previous steps for any other client nodes requiring an RDM installation.

5.3 Installing Standalone RDM

This section contains instructions for the following installation procedures:

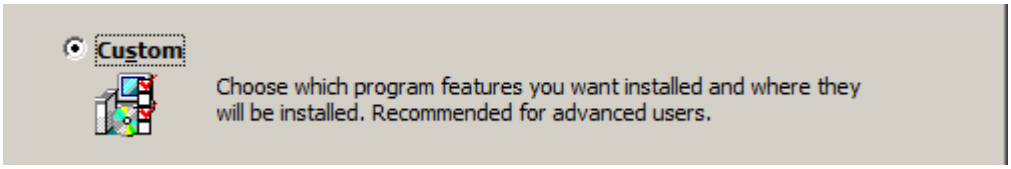
- Installing Standalone RDM on a non-Experion system
- “Installing RDM in a TPS system” on page 32
- “Installing RDM in R300 and later Experion system” on page 33

5.3.1 Installing Standalone RDM in non-Experion or non-TPS system, in a TPS system or in a R300 or later an Experion

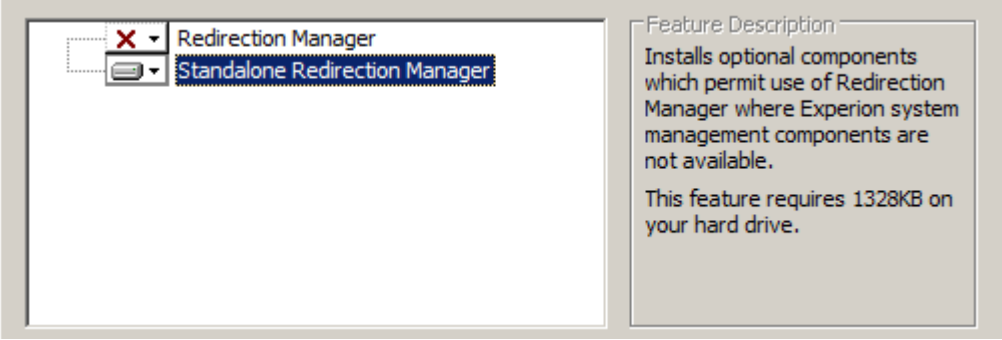
1. Insert the media which contains the Standalone Redirection Manager installation package and browse to <DiskDrive>\Packages\Honeywell_Redirection_Manager.msi.

   Note: Package may have been obtained via OLS download in lieu of physical media.
2. Launch the package installation by double clicking 'Honeywell_Redirection_Manager.msi' or via command line using 'msiexec /I Honeywell_Redirection_Manager.msi'

   Note: User performing the installation must be an administrator or belong to the local administrators security group.
3. Review the license agreement. Click **Next** to continue.
4. Enter customer information. Click **Next** to continue
5. When the **Setup Type** screen appears, select **Custom**. Click **Next** to continue.



6. At the **Custom Setup** screen, select '**This feature will not be available**' for feature 'Redirection Manager' and select '**This feature will be installed on the local hard drive**' for feature 'Standalone Redirection Manager'. Click **Next** to continue.



7. Click **Install**.

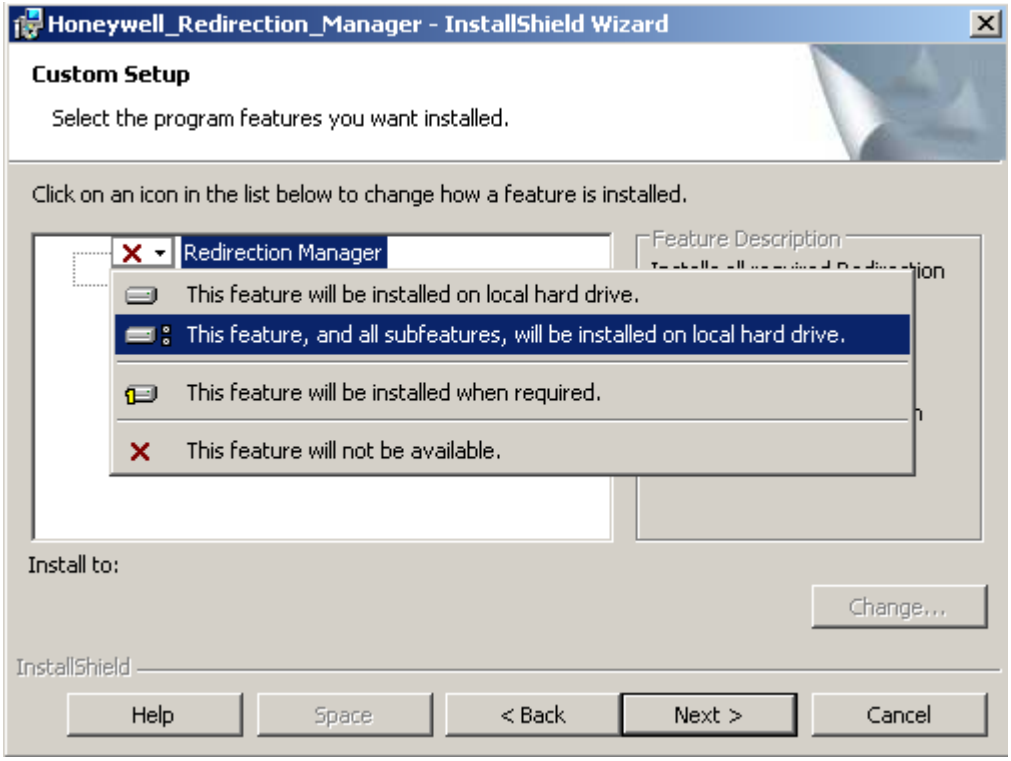
   Note: If User Account Control is enabled, you will be presented with an authorization dialog. Select **Yes.**
8. Click **Finish**.

5.4 Installing Classic RDM

To install a Classic RDM

1. Run the **Honeywell_Redirect_manager.exc** (<Disk Drive>\packages\Honeywell_Redirect_manager.exc) from the command prompt, as an Administrator. The **InstallShield Wizard** window appears.
2. Click **Next** to navigate to the next screen. The **License Agreement** window appears.
3. Accept the terms in the License Agreement and click **Next**. The **Customer Information** window appears.
4. Enter the **User Name** and **Organization** details in the respective text filed and select the **Anyone who uses this computer (all users)** option. Then, click **Next**. The **Setup Type** window appears.
5. Select the **Custom** option and click **Next**. The **Custom Setup** window appears.

   The **Custom Setup** window displays both Classic and Standalone installation modes. By default, Standalone installation mode is selected.
6. To shift to Classic installation mode, click the Classic installation icon and select **This feature, and all subfeatures, will be installed on the local hard drive**. Then, click **Next**.



Attention

Ensure that you unselect the Standalone installation mode by clicking the Standalone installation icon and selecting **This feature will not be available**.

7. In the **Ready to Install the Program** window that appears, click Install and follow the on-screen instruction to complete the installation.

6 Redirection Manager Configuration

Related topics

“Configuring Redirection Manager” on page 38
“Configuring status items” on page 50
“Securing Redirection Manager Methods” on page 55
“Configuring Remote Node Status Detection” on page 62

6.1 Configuring Redirection Manager

This section contains information describing how to configure Redirection Manager.

For information regarding System Management component configuration, refer to the *System Management Configuration Guide.*

6.1.1 RDM configuration limits

If you install the Redirection Manager package in

- *A workgroup*, you can configure as many as twenty RDMs per *node*.
- *A TPS domain*, you can configure as many as twenty RDMs per *domain*.
- *A standalone node*, you can configure as many as twenty RDMs per *node*.
- *A non-TPS domain but within a Windows domain*, you can configure as many as twenty RDMs per *Organizational Unit (OU)*.
- There are no limits on the number of RDMs that can be configured on a node when using the Standalone version of RDM

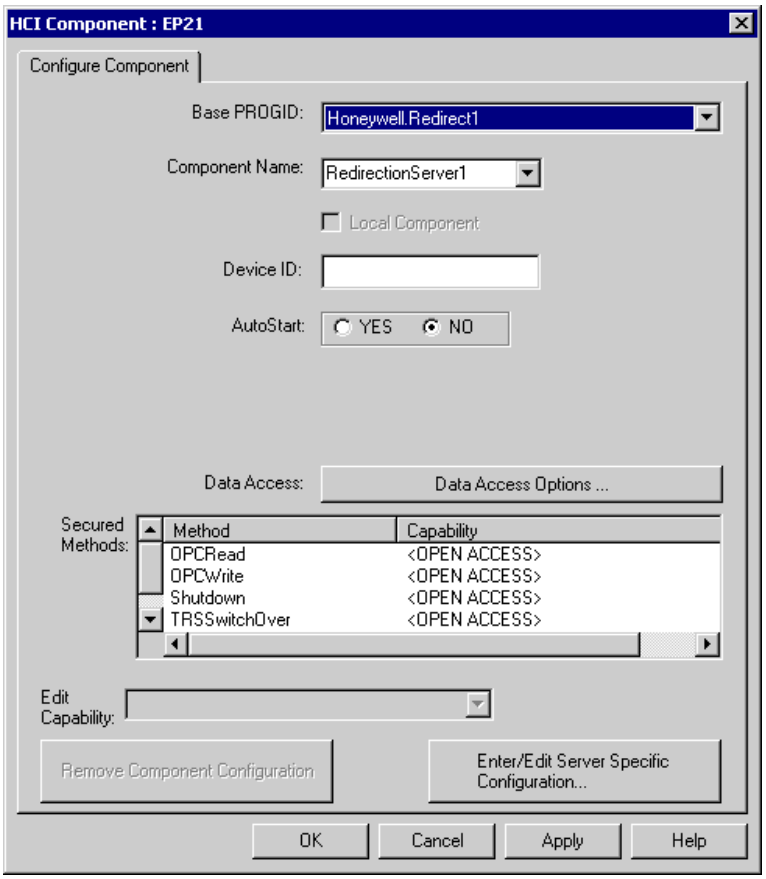
6.1.2 Configuration Overview

Redirection Manager Configuration involves the following:

- Enter a unique name for the Redirection Manager. This name appears in status displays and may be referenced in OPC client applications.
- Secure the methods for synchronizing and switchover when the RDM targets an HCI/OPC server. This step only applies to target OPC servers that establish an Active Redundancy mode.
- Assign the primary and secondary server nodes to the Redirection Manager.
- Optionally configure one to five status items

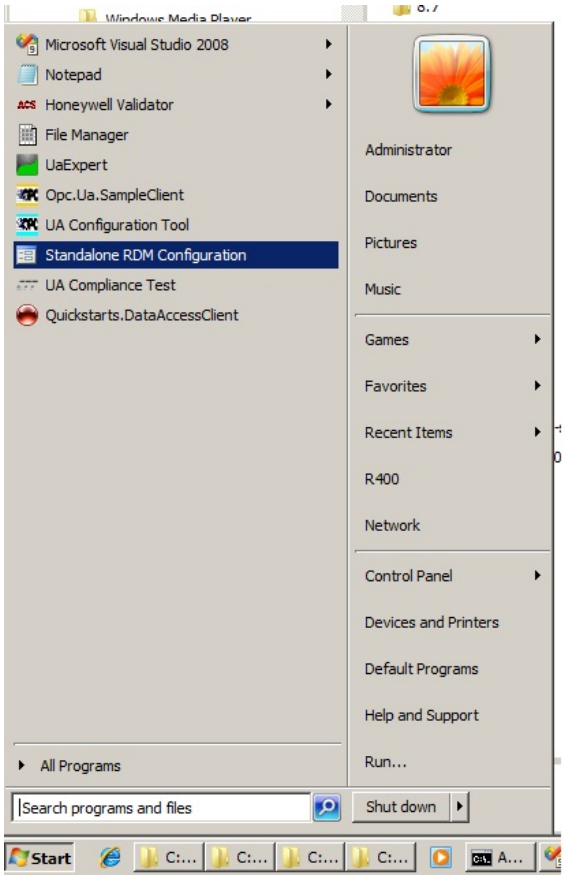
6.1.3 RDM from HCI Component Configuration page

Configure the RDM from the HCI Component Configuration Page. This page is accessed from the System Management Display or from the Configuration Utility. R300 and later Experion users can also access the page from the Network tree in Configuration Studio. An example HCI Component Page appears in the following figure.

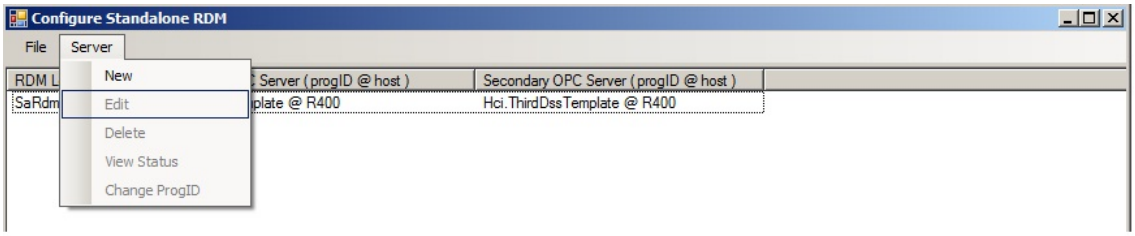


6.1.4 RDM from Standalone RDM Configuration page

For the Standalone RDM, click on the Start menu and select Standalone RDM configuration



From the Configure Standalone RDM page, select Server->New to configure a new RDM.



6.1.5 Replicating RDM on nodes in an Experion workgroup

If a client application using RDM needs to be re-hosted on different stand-alone client nodes, then the user/system administrator must configure identical RDMs on all the nodes on which the client application will run.

6.1.6 Replicating RDM on nodes in a TPS Domain

Redirection Manager servers are local servers available only to clients running on the same node as the RDM(s). Configuration information is also local to the node. A built-in replication capability replicates configuration information on all nodes in TPS Domains that have RDM loaded.

For example, this type of replication allows a GUS node to connect as a client to Redirection Manager, as well as connect as the same client from a different GUS node. This is usually the case when GUS displays are deployed. The replication capability eliminates the need for an Administrator to configure similar Redirection Managers on the second GUS node.

6.1.7 Replicating RDM on nodes in a non-TPS domain

The built-in replication capability is only available within a TPS Domain. Therefore, if a client application using RDM needs to be re-hosted on different stand-alone nodes, then the user/system administrator must configure identical RDMs on all the nodes on which the client application will run.

6.1.8 Standalone RDM does not support replication

The replication feature is unavailable when using the standalone RDM even when the client and server nodes are within a TPS domain. The replication function is provided by System management components which are not installed in the case of Standalone RDM.

6.1.9 Experion and TPN systems component requirements

For all components (Experion and TPN systems), the selected Primary and Secondary target OPC server must:

- Have the same CLSID (class ID).
- Reside on different nodes
- Have similar LCN personalities on the different Primary and Secondary target nodes if target nodes are Experion or TPS nodes. For example, Experion Server \ TPS nodes and APP nodes use an underlying AM personality and can be used as primary and secondary targets. Similarly, Experion Station \ TPS nodes and GUS nodes use an underlying US personality and can be used as primary and secondary targets. However, a node using an AM personality must not be targeted as a primary or secondary with a node using a US personality type.
- Support a common set of OPC interfaces within each OPC initiative (that is, 'per Data Access' and 'per Alarm and Events'). For example, if the selected primary supports OPC DA 1.0 and DA 2.0 and the selected secondary supports only DA 1.0, the configuration is allowed but with a warning that only the DA 1.0 interface will be used. Similarly, if one server supports only OPC AE 1.0 and the other does not, the configuration is not allowed.

6.1.10 Passive RDM Blocking Time for Experion servers

RDM configuration includes a Blocking Time property to support redundant Experion servers. Blocking time is the maximum time to allow for switchover. Client methods are blocked during switchover. If the switchover completes before the blocking timeout expires, blocked methods resume running on the 'new' primary. If the switchover does not finish before the blocking time expires, blocked methods fail. A default blocking time is provided. For heavily loaded systems, the blocking time can be increased. Loading factors include number of OPC groups, items, and subscriptions, and network traffic. Determining failover times for a redundant Experion server configuration is described in the *Server and Client Configuration Guide.*

For a target OPC server establishing Passive Redundancy (for example, Experion HCI servers hosted on redundant Experion server configurations), the Blocking Time entry will be present. For a target OPC server establishing Active Redundancy (for example, TPN Server hosted on an APP node), the Blocking Time entry is not applicable and not present.

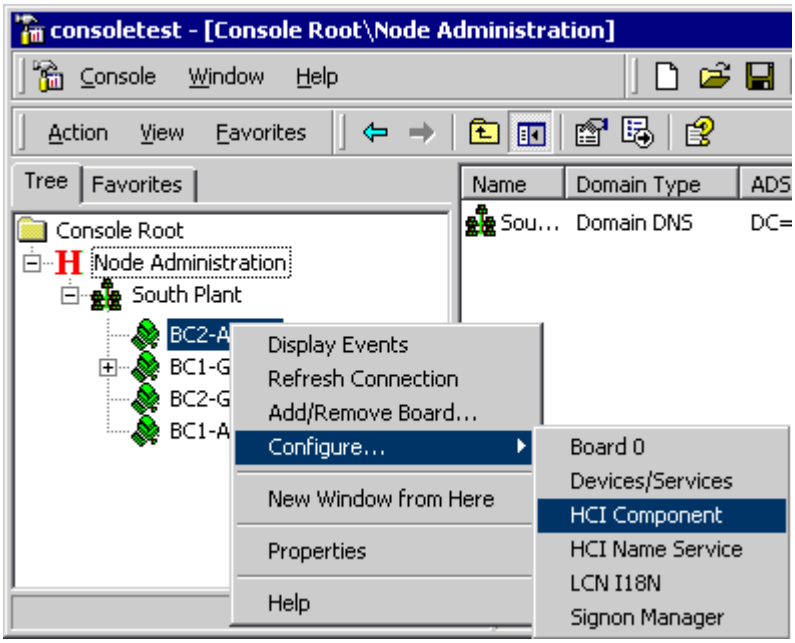
6.1.11 Accessing the RDM Server Specific configuration

Use the RDM's Server-Specific Configuration page to configure RDM connections to Primary and Secondary servers and reconfigure existing OPC servers. Examples of the Server-Specific Configuration page appear in the following procedure.

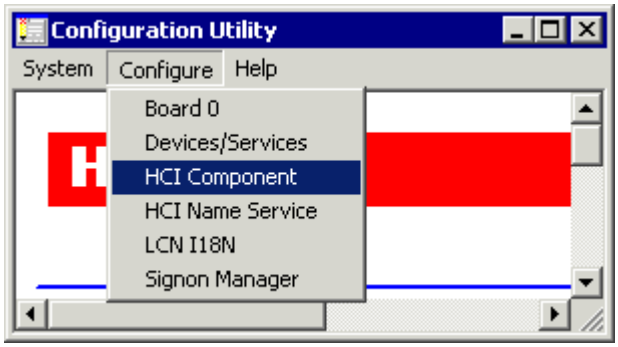
6.1.12 Configuring RDM Primary and Secondary servers

1 Access the HCI Component Configuration Page from either the

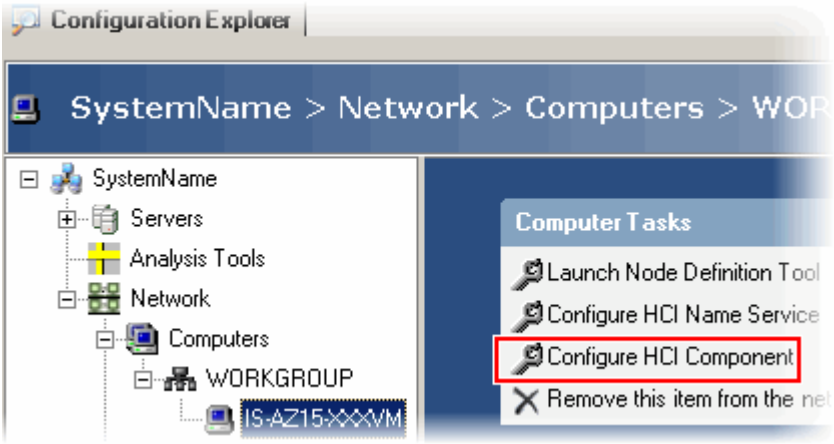
- System Management Display when you right-click the client node and select **Configure** > **HCI Component**. Or,



- Configuration Utility when you select **HCI Component** from the **Configure** menu.

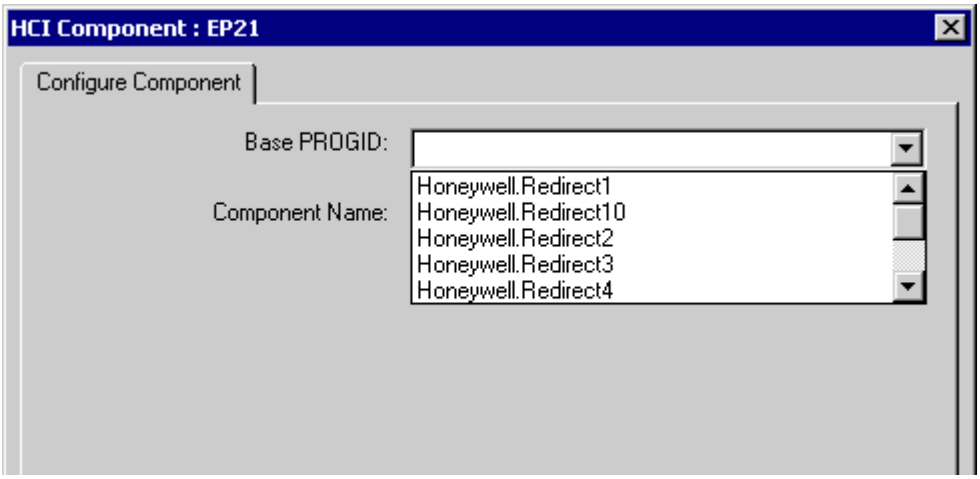


- Configuration Explorer when you click the client node and select **HCI Component** from the **Computer Tasks** menu.

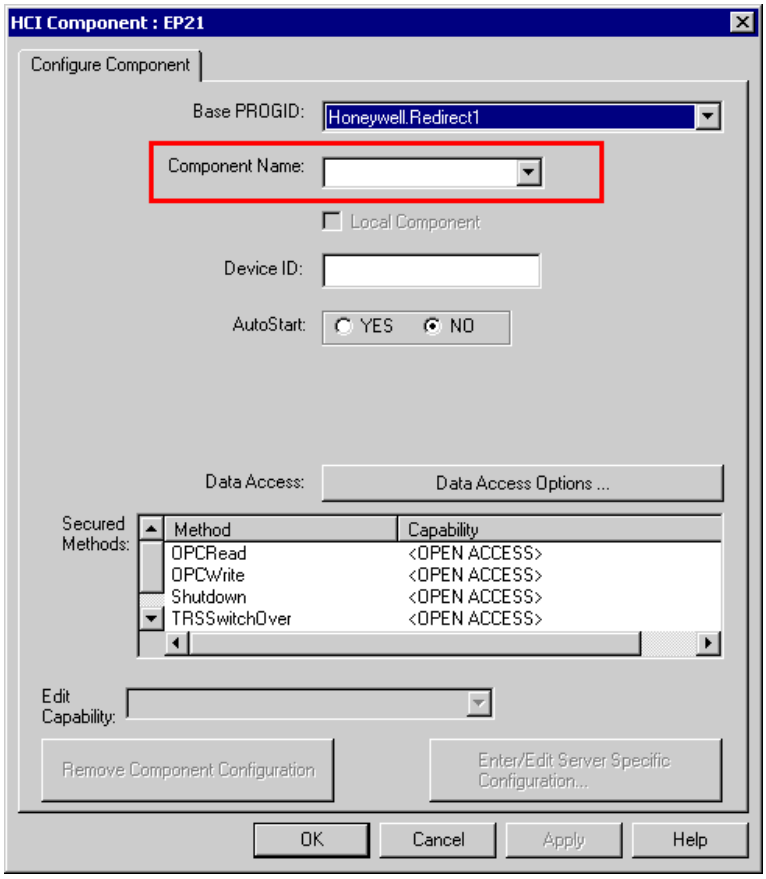


2 From the HCI Component Page, click the **Base PROGID** drop-down menu.

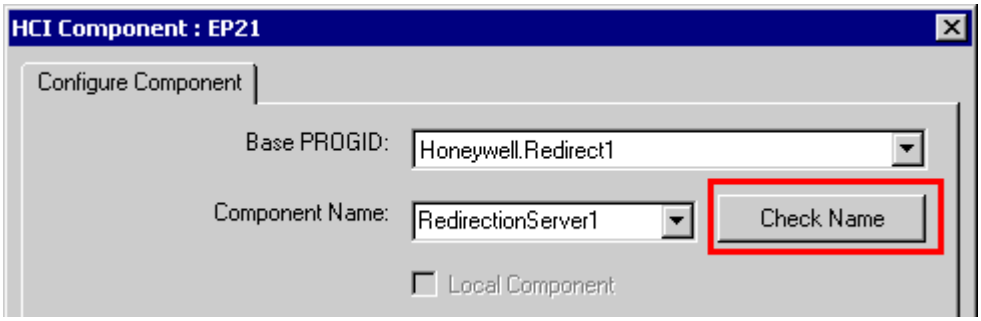
3 Select an available Redirection component .



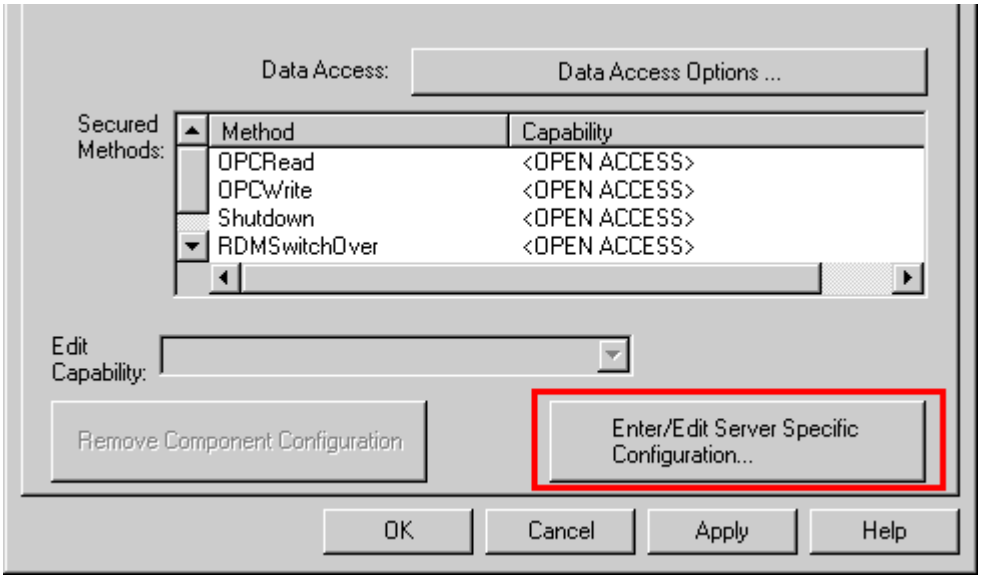
4 Enter a Component name for your Redirection Manager.



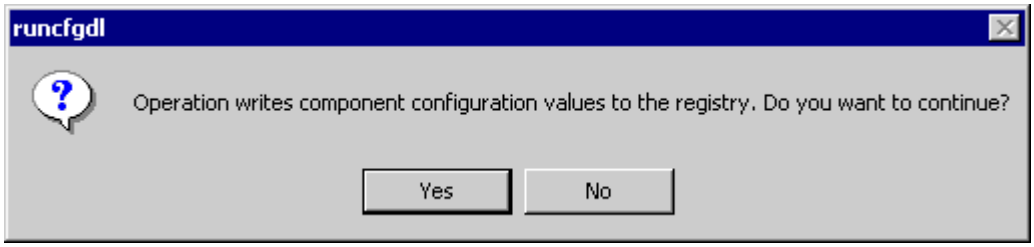
5 Click the **Check Name** button to ensure the name is not already in use.



6 Click the **Enter/Edit Server Specific Configuration** button to assign Primary and Secondary servers.

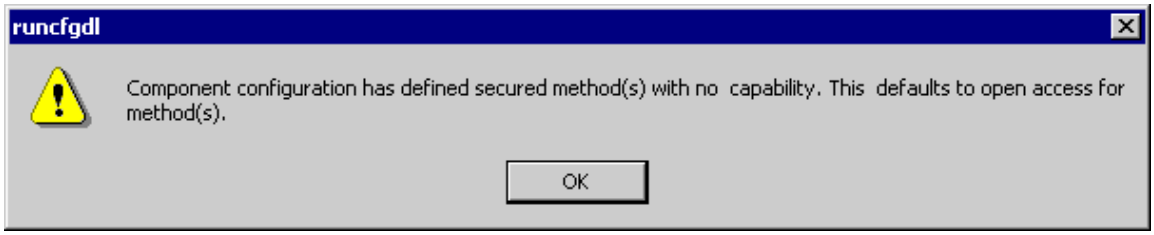


7 Respond to the dialog by clicking the **Yes** button.



8 Click **OK.**

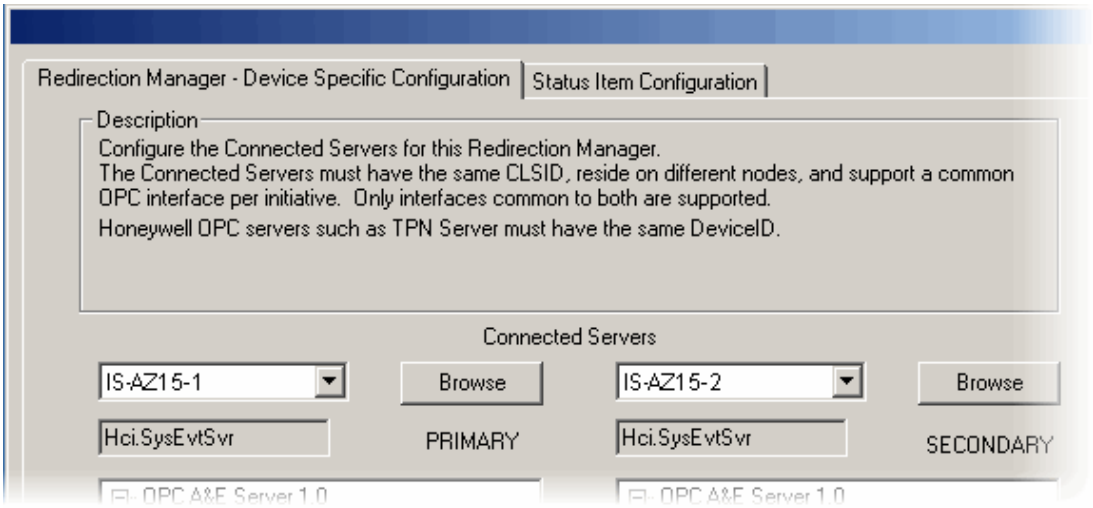
Note: If RDM establishes a connection to a HCI/OPC server requiring RDM secured methods, then refer to section “Securing Redirection Manager Methods” on page 55 in this document for information on how to secure the methods for switchover and synchronization.



9 From the Device Specific Configuration page, select the hosting server nodes using the drop down selection lists, or click **Browse** and navigate to the nodes. Once the node has been selected, choose a Primary and Secondary target OPC server from the lists provided.

For all Experion and TPN systems components, verify that the selected Primary and Secondary:

- Have the same CLSID (class ID).
- Reside on different nodes.
- Support a common set of OPC interfaces within each OPC initiative.



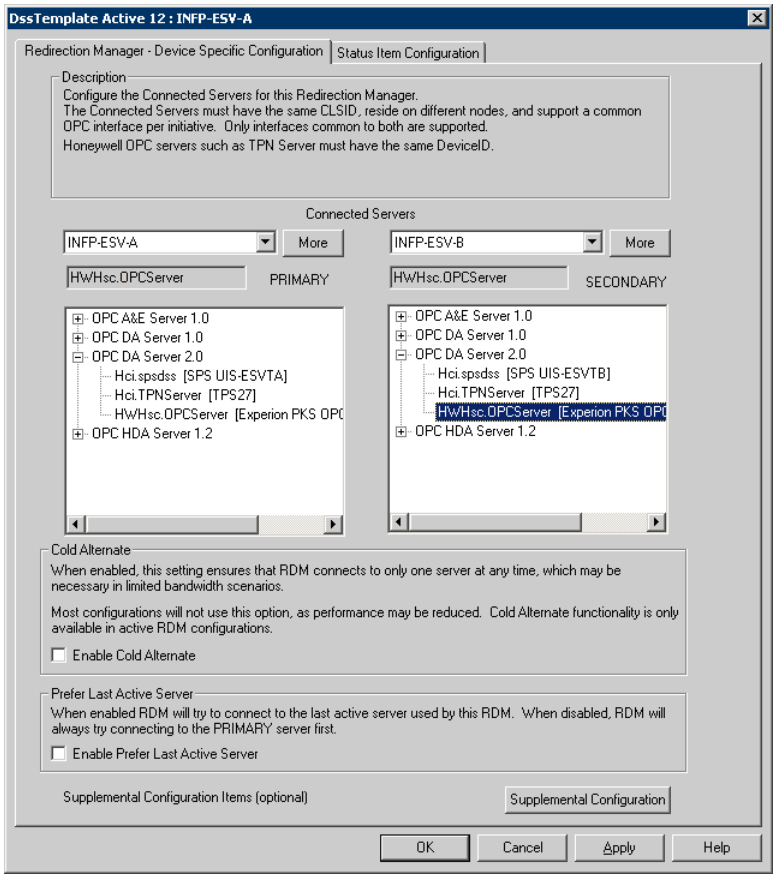
10 If you are connecting to a TPN Server or other HCI/OPC component hosted on an APP Node, complete this step, then go to step 12.

Verify that the selected components have the same Device ID; this applies to TPN Server or other HCI components. (Note: If you do not know the Device ID, examine the Device ID on the device specific configuration page for each of the target servers.)

Two additional options are available for Active RDM configurations. These options are not visible if an applicable server is not selected.

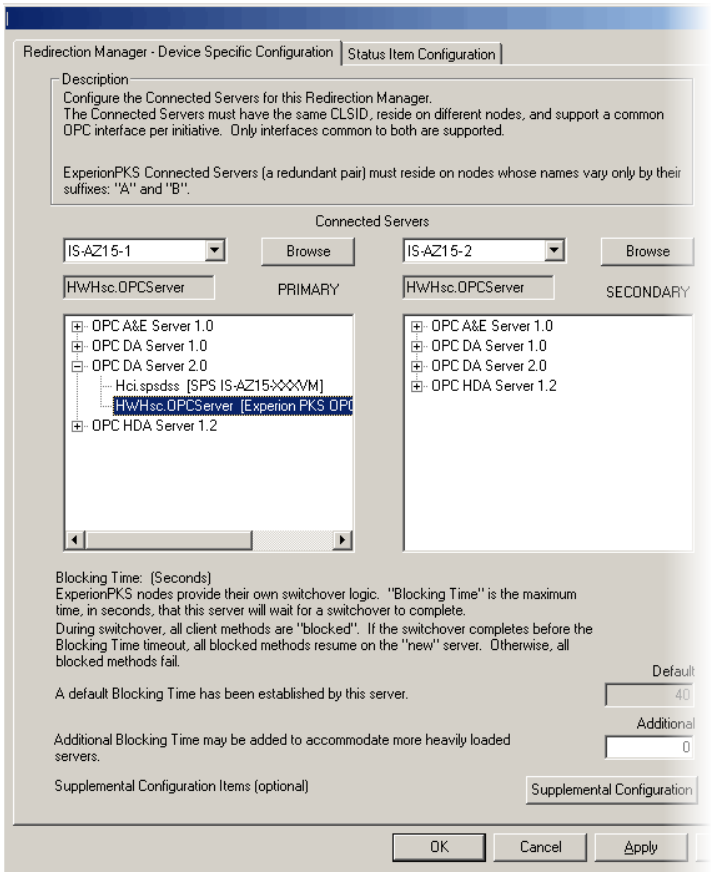
The Cold Alternate option causes RDM to connect to only one redundant server at a time. This option supports devices with limited bandwidth and can cause longer switchover time. In the event of switchover, RDM completely disconnects from the primary server before establishing a connection with the backup server. This option is not enabled by default.

The Prefer Last Active Server option allows RDM to keep track of the connection to the previous server. Therefore, the new instance of RDM connects to the previous server. If this option is not enabled, RDM connects to the server configured as PRIMARY. This option is not enabled by default.



11 If you are connecting to an Experion HCI server hosted on redundant Experion Server nodes, complete this step.

For redundant Experion Server components, if necessary, increase the blocking time if RDM is used in a heavily loaded system. Loading factors include number of OPC groups, items, and subscriptions, and network traffic. (Note: Establishing a connection to Experion Server components establishes a default blocking time).

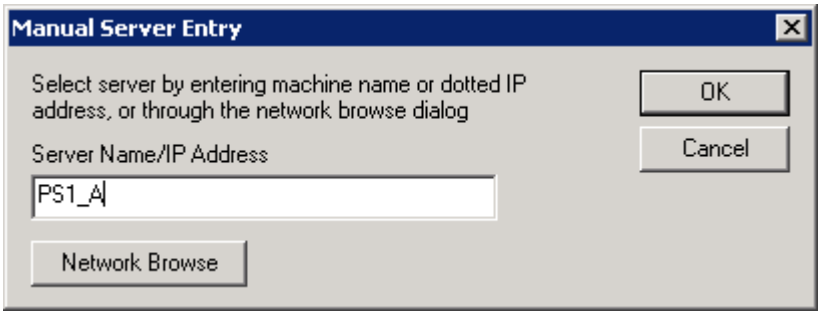


Blocking time is the maximum time allowed for a switchover. Client methods are blocked during a switchover. If a switchover completes before the blocking timeout expires, the blocked methods resume running on the 'new' Primary server. If a switchover is not complete before the blocking time expires, the blocked methods fail.

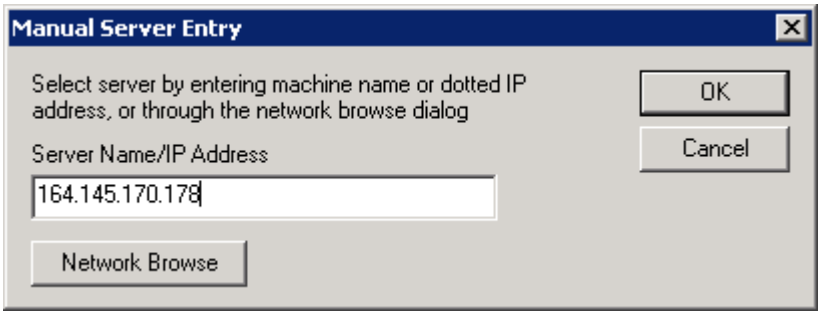
For servers using Passive Redundancy, the Blocking Time options are available in the Device Specific Configuration page. For servers using Active Redundancy (the default), the Blocking Time options are not available/displayed in the Device Specific Configuration page.

You can select the server by name or IP address as shown in the following figures:

- Selecting a server by name



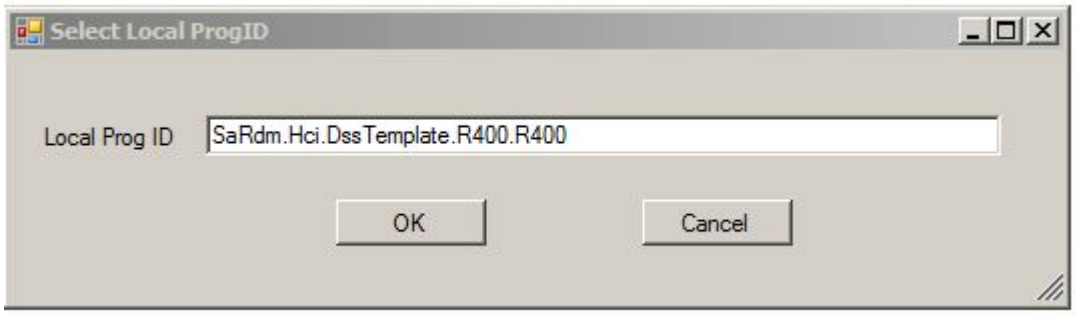
- Selecting a server by the IP address



12 Click **OK** after selecting a Primary and Secondary server.
Result: The servers are validated and any errors or warnings are displayed in message boxes.

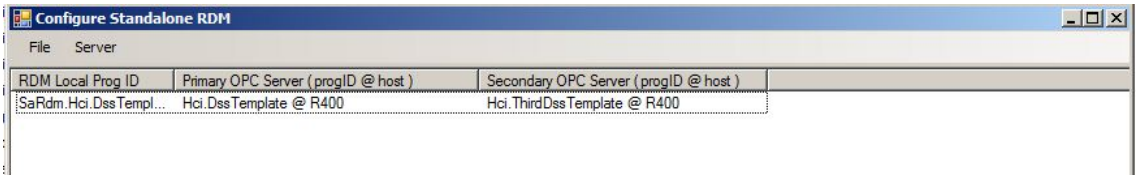
6.1.13 User defined ProgID for Standalone RDM

Standalone RDM allows the user to specify the ProgID for the new server rather than picking a ProgID from a pre-defined set as is the case in classic RDM.

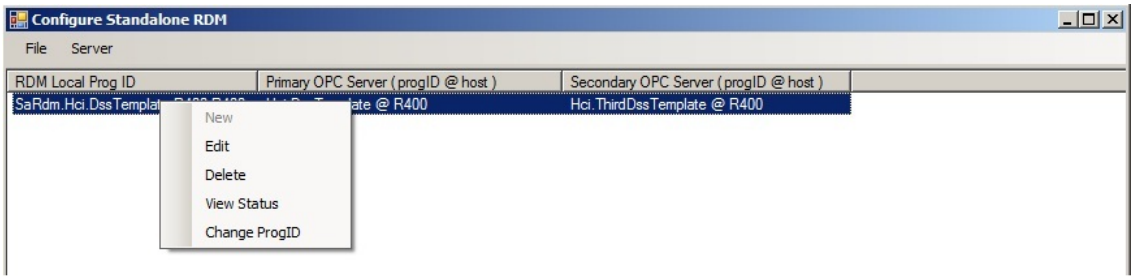


Based on target servers selected a ProgID is suggested but can be modified by the user.

The new server now shows up under the list of configured servers.



Right-click on any item in the list to edit or delete configuration. The submenu ‘Change ProgID' can be used to change the ProgID of the selected server.



6.2 Configuring status items

6.2.1 Status item configuration overview

Status items can be particularly useful where the RDM is connecting to two third-party servers. Many third-party servers maintain internal item IDs which represent the health of the communication channel between the server and its underlying device. You can configure these item IDs as status items thus giving RDM the capability to take action in the event of a failure of the link between the third-party server and its device. Status item configuration is an optional capability and if no status items are configured, the RDM behaves exactly as earlier releases.

The RDM status item configuration page allows the user to configure up to a maximum of five separate status items. Each status item is presented to the user in the form of a triplet - Item ID, Operator, Item Value - on the status item configuration page. In the item ID field, the user will enter the fully-qualified path to the status item on the primary and secondary servers. The user then selects one of the arithmetic operators and enters a value.

At runtime, the RDM will create a separate OPC group on the target servers to which it will add these items. The RDM will periodically read the item values from both the active server and the inactive server and compare these values to the values established by the user on the configuration page using the selected operator. If the values received from either server meet the criteria established by the user during configuration, then the RDM will declare the server to be failed.

6.2.2 Status item retry count

The RDM reads status item values at a fixed periodic rate and declares the target server to be failed whenever the values returned meet the failure criteria. By default, switchover begins immediately after the first such read which meets the criteria. You can change this behavior by adjusting the value of the Retry Count. A Retry count set 1 or higher means that the Redirection Manager will read the item 'Retry Count' number of additional times following the first failure and then only after all retries meet the failure criteria will the status item be declared 'bad'.

Note that in order for the Retry Count to apply, the RDM must first establish a connection with the target server where at least one status item returns a good value. In other words, the Retry Count will not apply in the case where the RDM attempts to connect to a target server but finds that the initial read of all status items is bad. In this case, the target server is declared failed immediately.

6.2.3 Status item configuration limits

The status item configuration page enforces certain limitations on the format and type of status items which can be entered by the user. Some limitations are validated at configuration time by the page itself, other limitations are validated by the RDM at runtime. Item validation problems encountered at configuration time will be reported to the user in the form of pop-up error messages. Item validation problems flagged by the RDM during runtime will result in a target server displaying a failed status (e.g., on the System Management display) along with a detailed error reported to the Windows application event log.

6.2.4 Limits Validated at Configuration Time

- The user must enter all three parts - item ID, item operator, and item value - for each status item. Note that the following defaults apply: Item operator, 'equal to'; item value, 0. The item ID field may be left empty (default) which indicates that no status item is assigned to the that triplet.
- The item value must be an integer between -2147483647 and 2147483647.
- Item IDs are limited to 254 characters in length
- Duplicate item IDs are not allowed.

- The user editing the status item configuration must have sufficient access to write to the HCI Component registry subkey.
- The Retry Count must be an integer within the range 0 to 1000.

6.2.5 Limits Validated by the RDM at Runtime

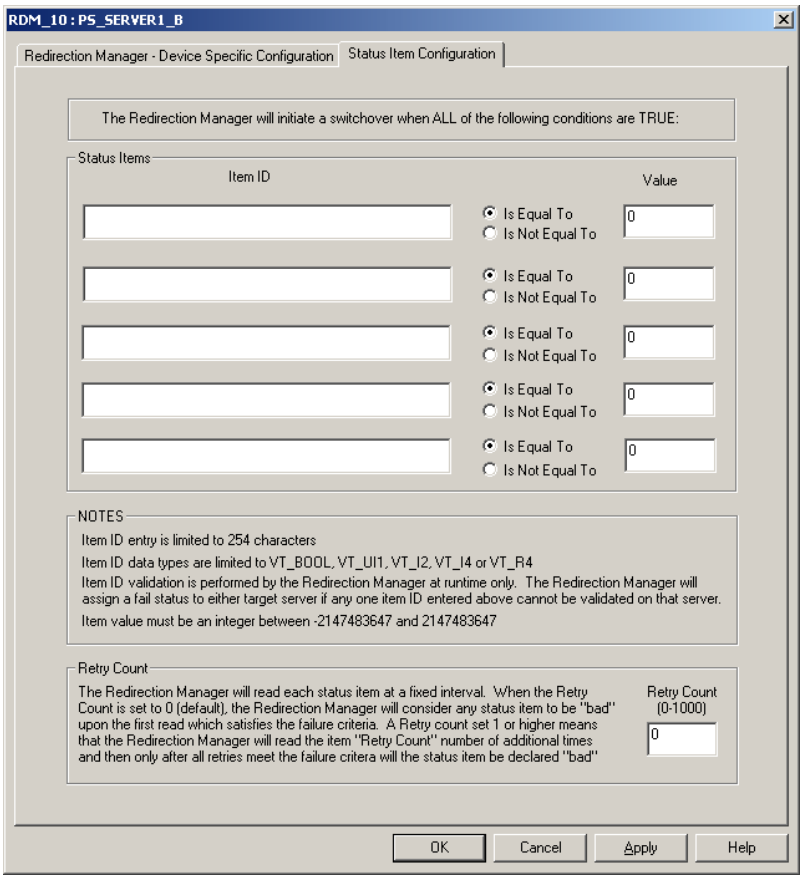
- The item ID must exist on the target server and must be readable.
- The item ID must report a canonical data type of VT_BOOL, VT_UI1, VT_I2, VT_I4 or VT_R4.

6.2.6 Configuring status items

After the user has completed the sequence of steps for configuring the target nodes and servers, status items may be configured. Note that configuring status items is optional and if no status items are configured, the RDM behaves exactly as earlier releases. Examples of the status item configuration page appear in the following procedure.

1 Access the Status Item Configuration page by clicking the tab labeled Status Item Configuration on the RDM's server-specific configuration page.

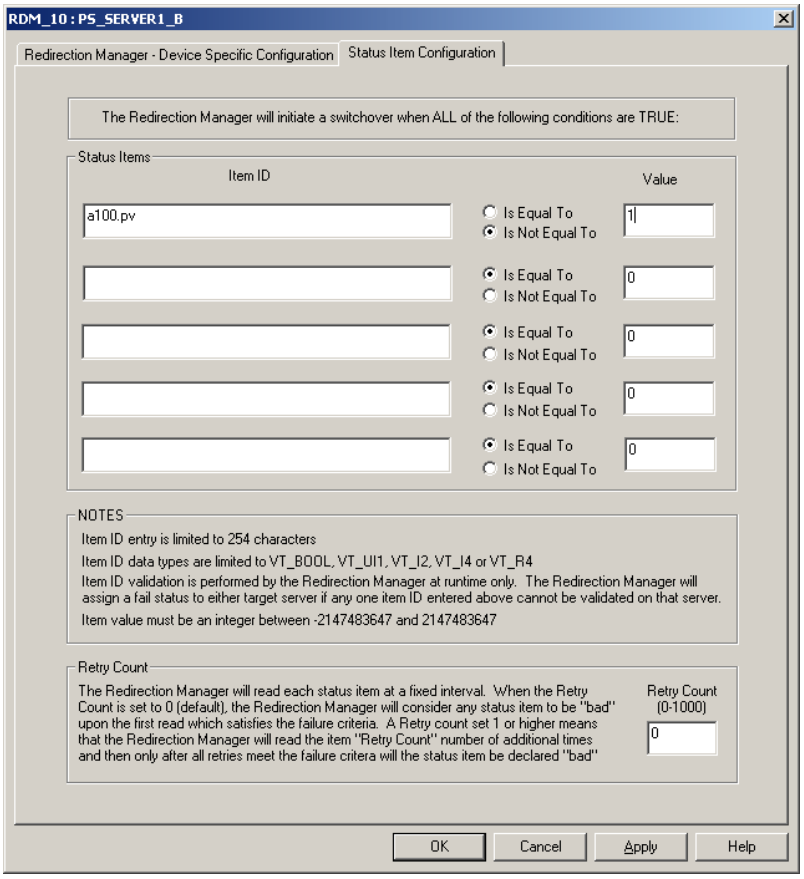
The example status item configuration page below, shows the default settings for this page. The defaults are displayed for the RDM components which have no status items configured.



2 Enter a valid item ID in the first edit box. Then enter a target value and select an operator.

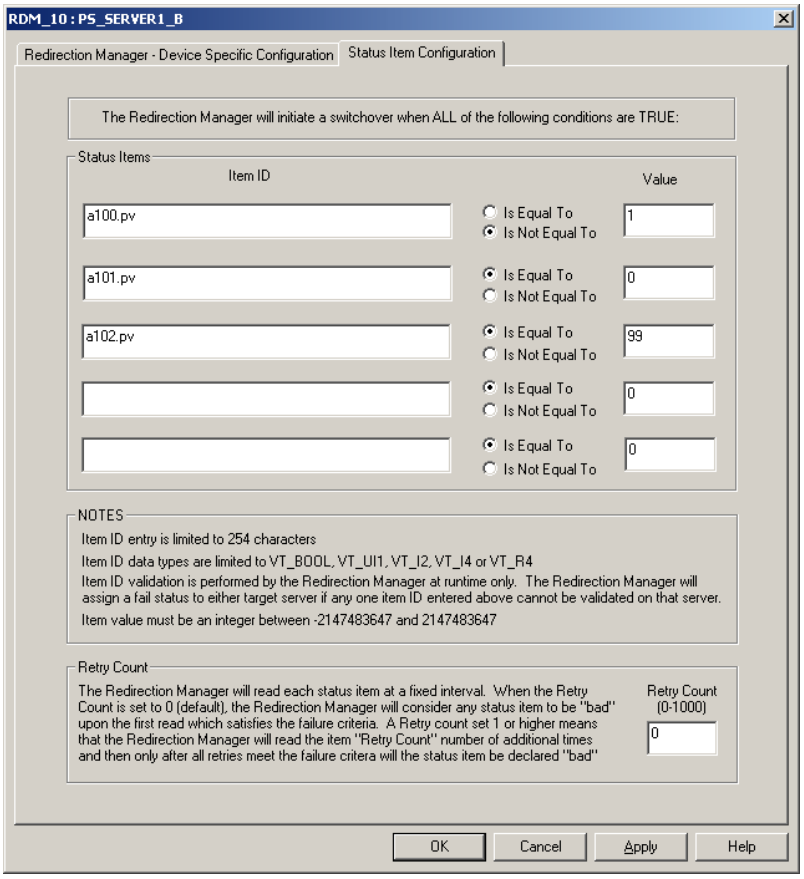
In the example below, the user has entered 'A100.pv' as an item ID, a target value of 1 and has selected the arithmetic operator 'Is Not Equal To'. Applying the configuration at this point has the following effect on the RDM execution logic: As the RDM component starts, it connects to its configured primary and secondary target servers as usual. Seeing that the user has configured a status item, the RDM creates a special status item group on each target server. To this special group, the RDM adds the item A100.pv. The RDM

periodically reads the value of A100.pv on each server. After each read, the RDM compares this real time value with the value established by the user during configuration, '1' in this case. If the real time value obtained from the target server is *not equal to 1*, the RDM declares that server failed.



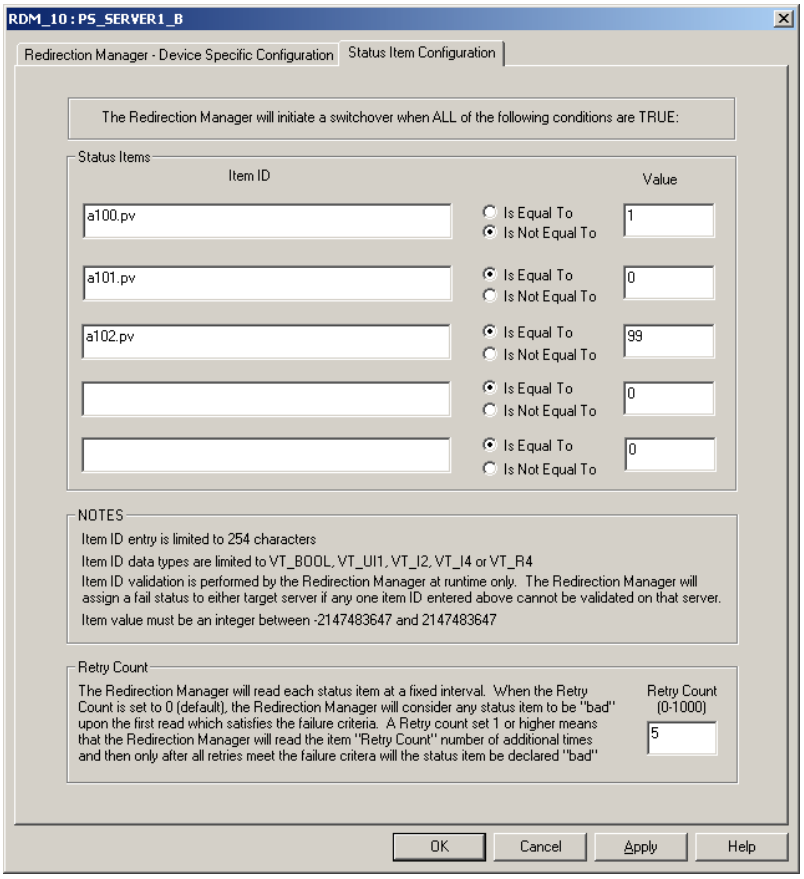
3 The user may continue to enter item ID, item operator, item value triplets up to a maximum of 5 status items. The RDM adds all items to just one read group and reads all values together. At runtime, ALL conditions must be TRUE before the RDM will consider the target server as failed.

In the example below, in order for the RDM to declare a target server failed, A100.pv must not be equal to 1 AND A101.pv must be equal to 0 AND A102.pv must be equal to 99.



4 Finally, you can choose to configure a Retry Count.

In the example below, the user has set the Retry Count to 5. What this means is that once the RDM reads failed values for all three status items, it will not declare that server to be failed unless and until the next five reads all return bad status item values. If at any point during the accumulation of failed status item reads, at least one status item returns a good value, the number of retries remaining until failure resets back to 5. This gives the RDM the capability to 'ride through' reads of status items whose values may occasionally fluctuate and would otherwise cause RDM to declare a premature failure.


RDM_10 : PS_SERVER1_B
Redirection Manager - Device Specific Configuration
Status Item Configuration
The Redirection Manager will initiate a switchover when ALL of the following conditions are TRUE:
Status Items
Item ID
Value
a100.pv
Is Equal To
Is Not Equal To
1
a101.pv
Is Equal To
Is Not Equal To
0
a102.pv
Is Equal To
Is Not Equal To
99
Is Equal To
Is Not Equal To
0
Is Equal To
Is Not Equal To
0
NOTES
Item ID entry is limited to 254 characters
Item ID data types are limited to VT_BOOL, VT_UI1, VT_I2, VT_I4 or VT_R4
Item ID validation is performed by the Redirection Manager at runtime only. The Redirection Manager will assign a fail status to either target server if any one item ID entered above cannot be validated on that server.
Item value must be an integer between -2147483647 and 2147483647
Retry Count
The Redirection Manager will read each status item at a fixed interval. When the Retry Count is set to 0 (default), the Redirection Manager will consider any status item to be "bad" upon the first read which satisfies the failure criteria. A Retry count set 1 or higher means that the Redirection Manager will read the item "Retry Count" number of additional times and then only after all retries meet the failure critera will the status item be declared "bad"
Retry Count (0-1000)
5
OK
Cancel
Apply
Help

6.3 Securing Redirection Manager Methods

This section describes how to secure the switchover and synchronization methods for an RDM connection to an OPC Server, such as a TPN Server, that establishes an Active Redundancy mode. Note that the manual switchover and synchronization methods do *not* apply to target OPC servers establishing a Passive Redundancy mode, such as target OPC servers hosted on redundant Experion Servers. For methods that apply to both Experion and TPN users -- OPCRead and OPC Write -- secure the OPC methods on the target OPC servers themselves and not on RDM.

6.3.1 Securing methods for an RDM

Because System Management views the RDM as an HCI server supporting OPC interfaces, the standard secured methods OPCRead and OPCWrite become visible. However, these methods are not actually secured through RDM. You should configure OPC method security on the target OPC servers themselves.

Attention

For RDMs establishing Active Redundancy, secure the methods for RDMSwitchover and RDMSynchronize. Setting security on other methods (for example, OPCRead and OPC Write) has no effect and should not be done during RDM configuration. For those methods, secure the OPC methods on the target OPC servers themselves.

6.3.2 Securing RDM: manual switchover method

Follow the steps below to secure the RDM switchover method for an OPC component or an HCI component such as a TPN Server.

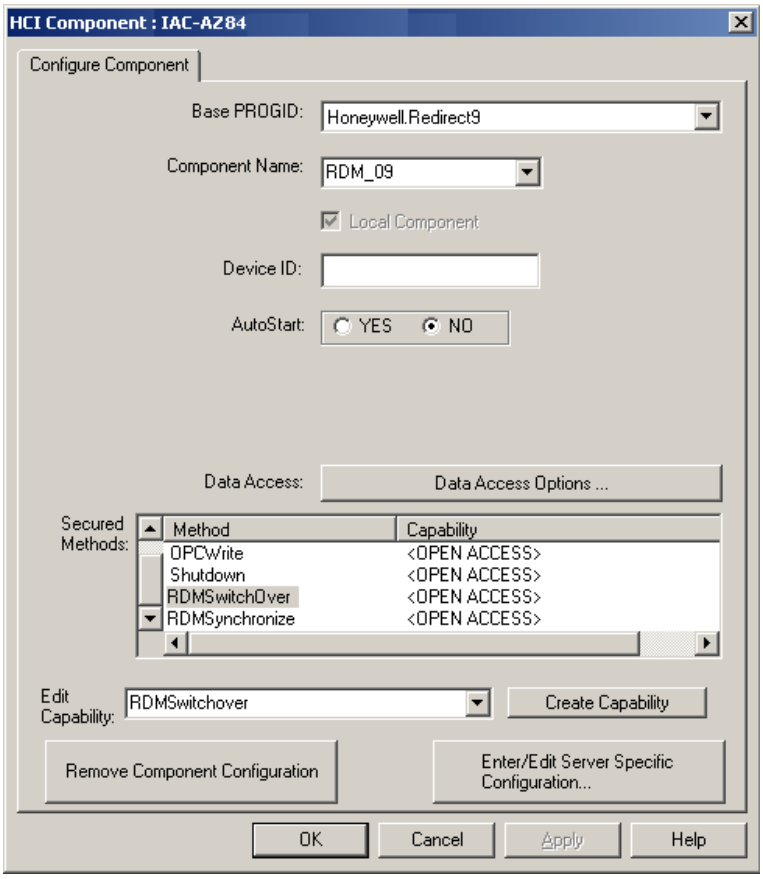
Attention

Manual switchover does *not* apply to RDM connections to redundant Experion Servers hosting target Experion OPC servers because RDM establishes a Passive Redundancy mode with those servers.

Consequently, this procedure does not apply to the RDM for the PHD/Experion Link.

1 To define the security for a manual switchover method:

- Select RDMSwitchover in the **Secured Methods** box.
- Enter RDMSwitchover as the filename in the **Edit Capability** field.

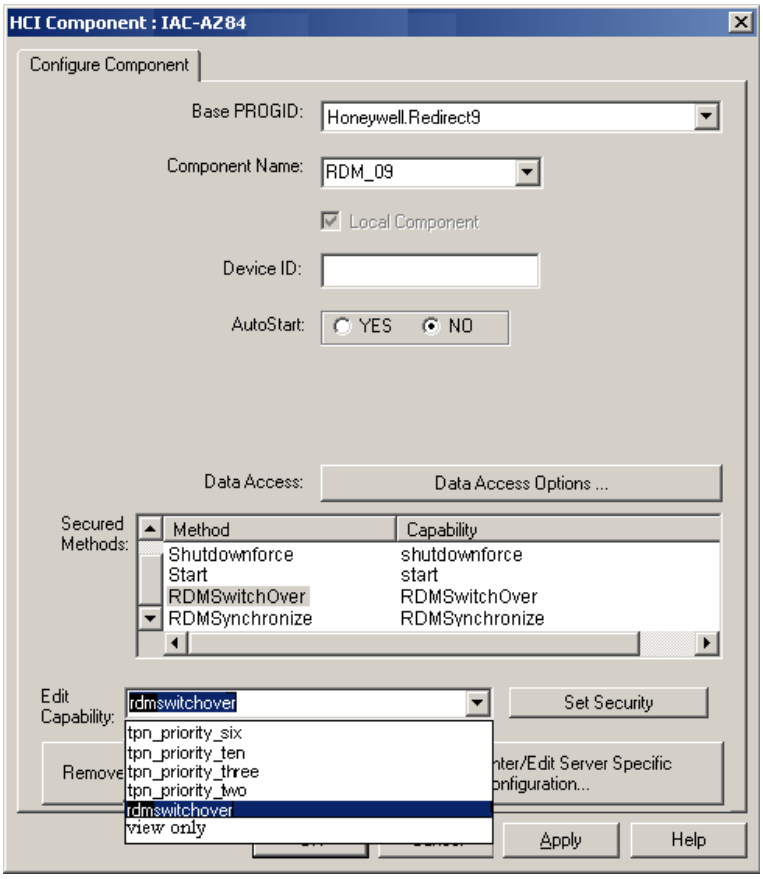


2 Click **Create Capability** to create the new capability file on the host node.

3 Click **Yes** and **OK** to confirm your selections.

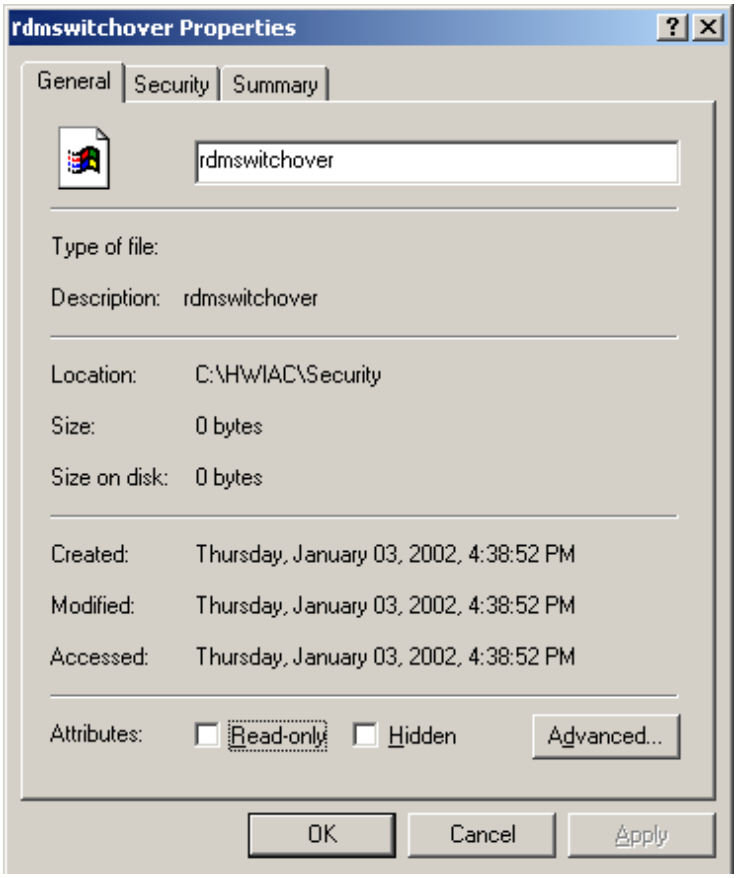
4 To modify the new capability, select the desired method (RDMSwitchOver) and capability file displayed in the **Edit Capability** combo box (if it is not <OPEN ACCESS>).

This enables the **Set Security** button.

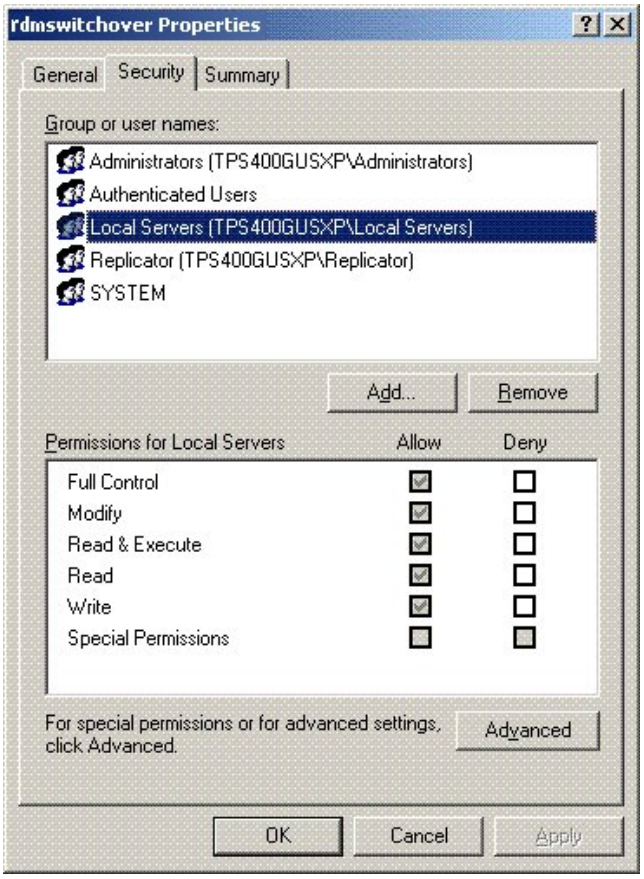


5 Click **Set Security to** invoke the properties of the capability file that sets security permissions for the new capability.

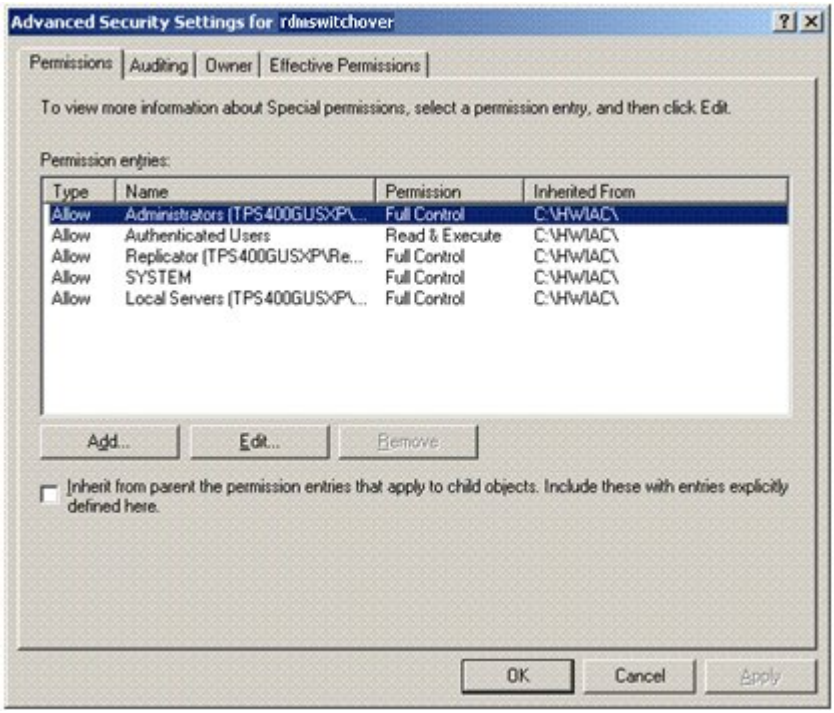
6 The Properties dialog box for the new capability file appears.
Select the **Security** tab.



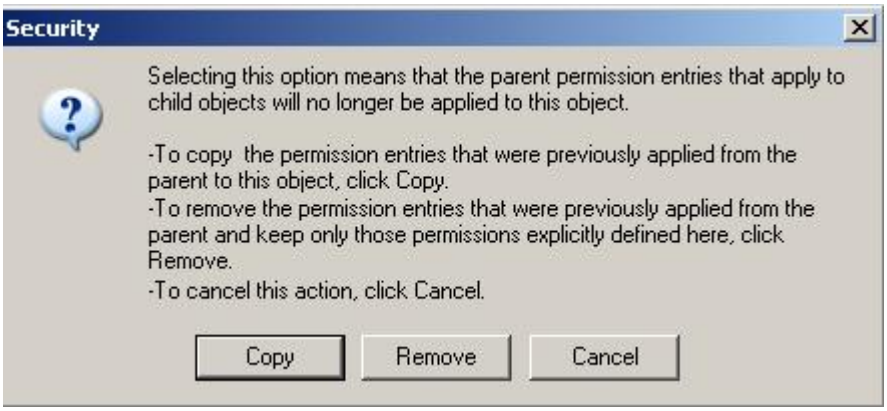
7 Click **Advanced**.



8 The **Advanced Security Settings** window appears.
Uncheck (clear) the **Inherit from parent the permission entries that apply to child objects** checkbox.



9 The following screen appears:

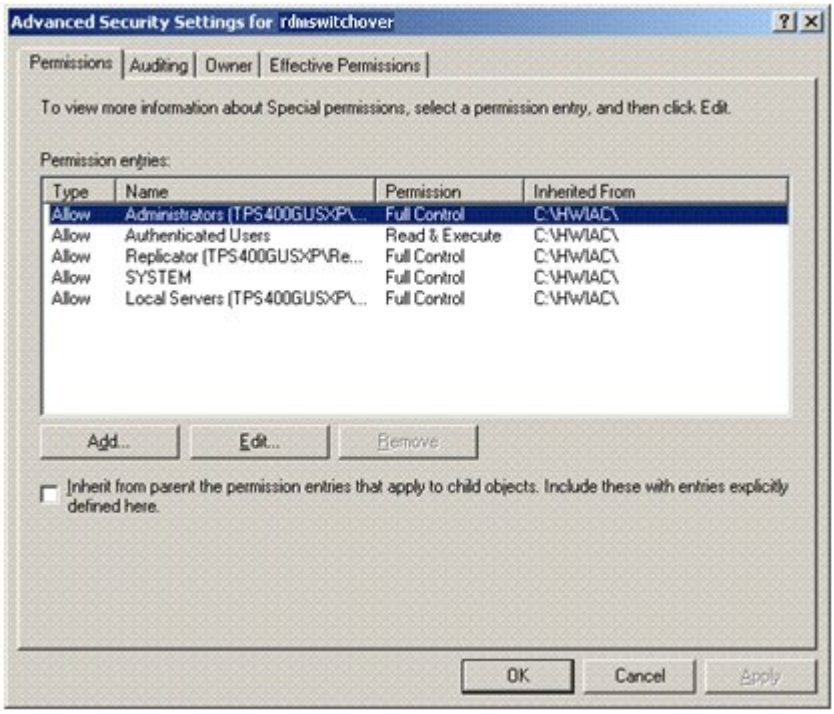


If you want to set a new security account, click the **Remove** button.

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

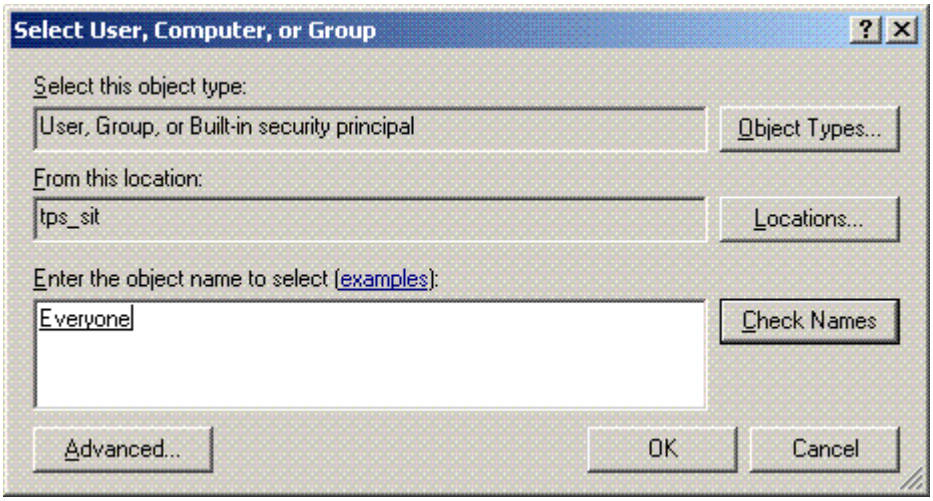
10 The **Advanced Security Settings** window for the new account appears.
In this example, Read/Execute is included in Full Control, so all of the users listed below will be able to switchover.

Click **Add**.



11 In the **Select User, Computer, or Group** window, click **Locations** and select the domain of interest.
In the **Enter the object name to select** box, enter the name of the user or group to which you want to assign capabilities.

Click **OK**.



12 Assign capabilities to the user or group of your choice. Click **OK** to apply and save the capabilities you select.

6.3.3 Defining Security on Synchronization

Repeat the steps outlined in the previous procedure when securing the RDMSynchronize method:

- Select the RDMSynchronize method,
- Enter the string 'RDMSynchronize' when you create a capability file for the RDMSynchronize method.
- Complete the access control assignments.

Note that manual synchronization does *not* apply to target OPC servers hosted on redundant Experion server nodes because those target OPC servers establish a Passive Redundancy mode.

6.4 Configuring Remote Node Status Detection

When Redirection Manager needs to determine Remote Node Status, it subscribes to a locally-hosted WMI Provider to provide the notifications. Redirection Manager also supports a configurable alternative technique to the default WMI Provider notification called ICMP Echo.

Attention

Configuring the Remote Node Status Detection mechanism is optional. If the exchange of multicast messages between the client node and the target server nodes is possible, then use the default WMI client mechanism. No further user configuration is necessary. You configure the Remote Node Status Detection mechanism to use ICMP Echo when you need to determine remote node status or availability across routers or firewalls that do not permit multicasting.

6.4.1 About remote node status detection

Redirection Manager incorporates a WMI client which subscribes to the locally-hosted WMI Provider for Remote Node Status. The WMI client relies on the ability to send and receive multicast messages in order to provide notice of node status changes to the Redirection Manager. If you have an OPC client application separated by routers and/or firewalls from the OPC server hosting nodes (for example, L2 Level 2 servers used with a L3 Level 3 client), exchanging multicast messages across the router or firewall may not always be possible.

6.4.2 ICMP Echo alternative to WMI client notification

As an alternative to the WMI client mechanism, you can configure the Redirection Manager to use ICMP Echo as the mechanism to determine remote node status. When you select this technique, the Redirection Manager periodically broadcasts an ICMP echo message (also known as a 'ping') to each target OPC server node. Upon receipt of a response from the targeted remote server node, the Redirection Manager considers the target node available. The remote server node is considered available until the Redirection Manager broadcasts its next ICMP Echo.

Standalone RDM only supports ICMP Echo

The only node detection mechanism available when using the Standalone RDM is ICMP ping which is in fact the preferred mechanism even in classic RDM.

6.4.3 ICMP Echo configuration settings

The Redirection Manager waits a configured period of time for a response from the remote target node. The default timeout setting is 1000 milliseconds with a configurable range of 500 to 5000 milliseconds. If the Redirection Manager does not receive a response from the remote node within the configured timeout, the Redirection Manager then must fail to receive consecutive ICMP Echo responses before it considers the remote node unavailable. You configure the number of missed consecutive ICMP Echo responses using the Count setting. The default Count setting is 2 with a configurable range of 1 to 5. For example, if the Count setting is 2 it means that the Redirection Manager must fail to receive 2 consecutive ICMP Echo responses before considering the remote node unavailable. When the Redirection Manager considers the target node unavailable, no connection is possible between the Redirection Manager and the OPC server hosted on that node.

Attention

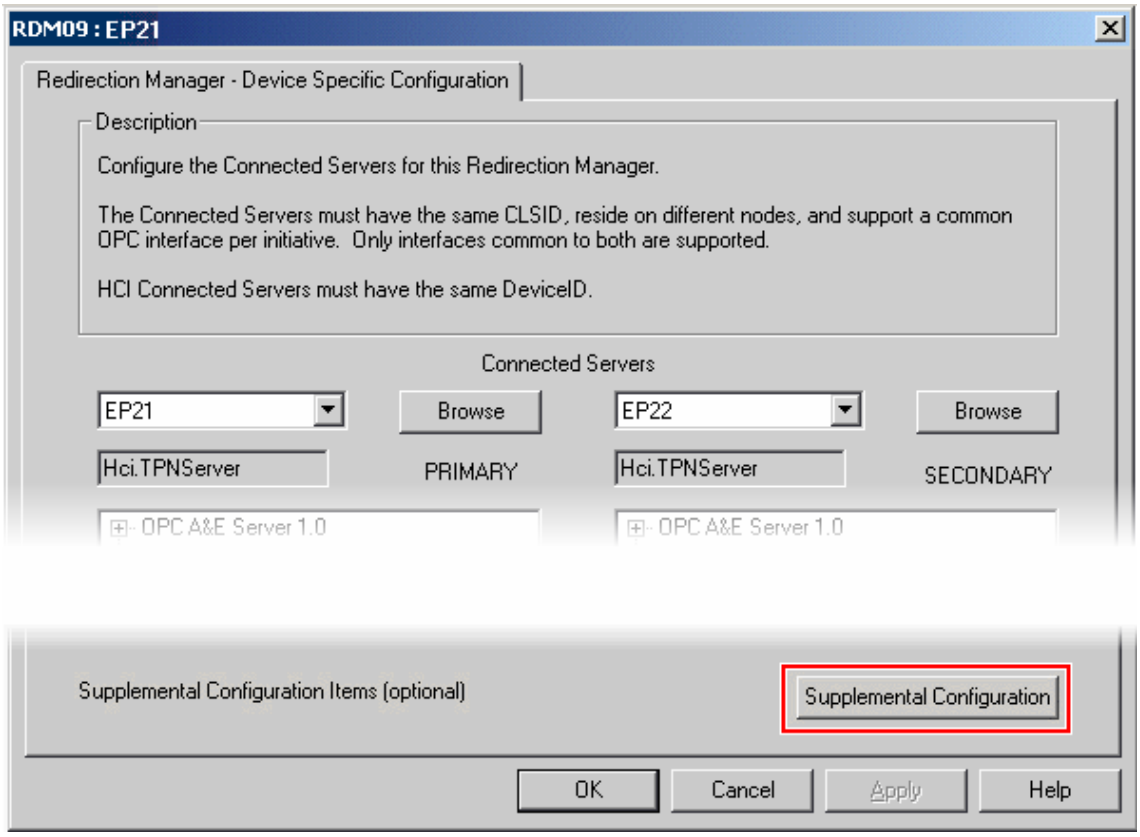
Whether you configure the remote node detection using WMI client or the ICMP Echo mechanism, the Redirection Manager behavior in terms of switchover and information displayed on the System Status Display remains the same.

6.4.4 Detection mechanism applies to specific Redirection Manager

Any configured node status detection mechanism applies only to the specific configured Redirection Manager. That is, you can create a Redirection Manager configuration on the client node which utilizes the WMI node status mechanism while on another Redirection Manager configuration on the same client node you can create a configuration that uses the ICMP Echo mechanism.

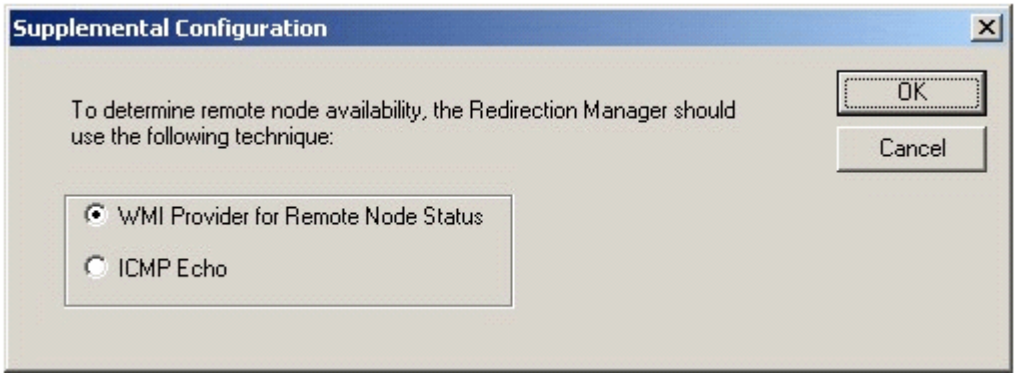
6.4.5 Configuring ICMP Echo for remote node status detection

1 Click **Supplemental Configuration** from the Redirection Manager's Device-Specific Configuration page.



The Supplemental Configuration dialog appears with the default setting of 'WMI Provider for Remote Node Status' selected.

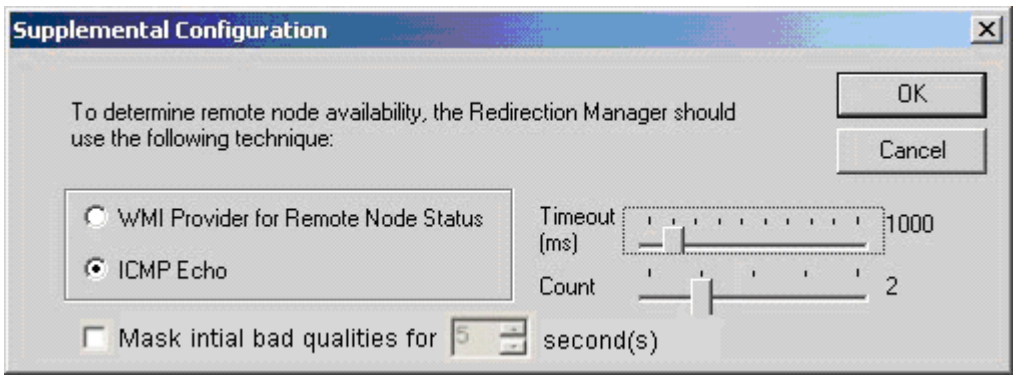
2 Select **ICMP Echo** to enable the alternate node status detection mechanism.



Additional ICMP Echo configuration settings appear.

3 Set the ICMP Echo timeout and count settings. If you do not know what to enter, accept the defaults.

- Set the Timeout slider, if necessary, from its default wait timeout setting of 1000 milliseconds to a setting from 500 milliseconds to 5000 milliseconds.
- Set the Count slider, if necessary, to represent the number of missed ICMP Echo responses, from its default Count setting of 2, to a setting from 1 to 5.



Attention

You should only need to make ICMP Echo adjustments to both the Timeout and Count settings if network conditions cause the Redirection Manager to incorrectly report remote nodes as being unavailable when displayed on the System Status display and reported in the Windows' application event log.

4 Select **Mask initial bad qualities for** to mask the initial bad qualities received from a server.

Note: This option is not recommended for general use when the servers return the initial bad values. It is only intended for clients which cannot handle this initial bad value. Enabling this option affects the following calls:

- IOPCItemMgt::AddItem
- IOPCItemMgt::SetActive
- IOPCGroupStateMgt::SetState

When one of these calls is initiated, the RDM blocks the client, if the client receives an initial bad value, for a period up to the time configured in the Supplemental Configuration dialog. So, if an instance of RDM was configured to mask the initial bad qualities for 5 seconds, then any of those three calls could potentially be blocked for 5 seconds. Blocking the call for the entire configured period is dependent on the target server's behavior.

Therefore, this option is not enabled by default.

5 Click **OK** to close the Supplemental Configuration displays and return to other Redirection Manager configuration tasks.

7 OPC Client and OPC Server Support

Related topics

“Support for OPC Interfaces” on page 66
“OPC Alarm and Event Interfaces” on page 68
“OPC Historical Data Access Interfaces” on page 69
“HCI Value-Added Interfaces” on page 70
“Error Handling” on page 71

7.1 Support for OPC Interfaces

7.1.1 Support OPC DA and A&E interfaces and methods

Redirection Manager supports all OPC Data Access interfaces as well as Alarm and Events interfaces and methods, except for the following optional interfaces:

- IOPCServerPublicGroups
- IPersistFile

Redirection Manager forwards all calls to either the Primary or Secondary server, or both, while maintaining state information related to the calls for redirection purposes.

7.1.2 Support OPC HDA interfaces and methods

Redirection Manager incorporates OPC Historical Data Access (HDA) 1.2 capabilities that are listed in this section.

7.1.3 Maintaining state information

The Redirection Manager saves the state-of-client requests, so that RDM can redirect or reissue the requests to the Secondary server in the event the Primary server fails. Redirection Manager categorizes client calls as I/O and non-I/O requests. The classification is made as follows:

- OPC requests that alter the state of the client connection but do not request I/O are classified as non-I/O requests. These include:
  - AddGroup
  - AddItem
  - CreateEventSubscription
  - SetFilter
- Client I/O calls are classified as I/O requests. These include:
  - Read and Write
  - AckCondition
- The Persisting state of these calls is handled differently. Non-I/O calls are maintained as long as the client is running. For example, this information is required when synchronizing a Secondary server that comes up after the client makes AddGroup and AddItems calls. The I/O call information persists until either the Primary or Secondary server services the call. Once the call goes through, the IO information about the call is deleted.
- Browsing Data Access Servers: RDM maintains the fully qualified name (as returned by GetItemID) anytime the browse position is changed. RDM uses this value to synchronize the alternate server's browse position during switchover. This feature is only available for OPC servers that support DA 2.0 and later, as the OPC_BROWSE_TO switch is new in 2.0. For OPC 1.0 servers the alternate server position can't be synchronized and will always default to root.
- Browsing Alarm and Event Servers: RDM maintains the current browse position in the hierarchical address space. During switchover the RDM uses this saved value to synchronize the alternate server's position.

7.1.4 About client callbacks

Redirection Manager intercepts all callbacks flowing from the Active server to the client. The RDM is thus able to examine callback values and re-issue the original request that generated the callback, as needed, during a callback scenario

7.2 OPC Alarm and Event Interfaces

7.2.1 Alarm and Event interface approach

Redirection Manager is designed to support Alarm and Event interfaces and follows the approach used for Data Access. The following tasks are handled the same way as in Data Access:

- Creation of OPC objects
- Implementation of connection points
- Callbacks.

The RDM initiates a refresh on all active subscriptions on the client's behalf when a switchover has completed. This gives the client an opportunity to verify that its view of known process conditions is consistent with that of the Alternate server. The client should treat these refresh event notifications just as if the client, itself, had requested the refresh.

Attention
For HCI servers, an HCI added-value feature ensures that acknowledgements are synchronized among servers servicing the same event source.

7.2.2 Constraints for third-party OPC Alarm and Event Servers

Redirection Manager supports the management of third-party OPC Alarm and Event Servers, with the following constraints:

1. As part of the switchover, the RDM refreshes each of the Active server's subscriptions. This method call forces refresh event notifications for all active conditions and all inactive but unacknowledged conditions. RDM Alarm and Event clients must be able to handle these unsolicited (that is, not requested directly by the client) refresh event notifications.
2. Individual conditions of both the Primary and alternate servers must carry the same cookie value and the same timestamp value. This is required so that when a switchover occurs, the client receiving the unsolicited refresh events from the alternate can determine that these events are simply refreshed copies of events previously received from the Primary server

7.3 OPC Historical Data Access Interfaces

7.3.1 Historical Data Access approach

Redirection Manager incorporates OPC Historical Data Access (HDA) 1.2 capabilities that are listed in the following table. Both Active (TPN Server, for example) and Passive (Experion Server, for example) Redirection Manager will support OPC HDA. The following table identifies all the supported HDA interfaces and methods.

Interface	Method
IOPCHDA_Server	• GetItemAttributes() • GetAggregates() • GetHistorianStatus() • GetItemHandles() • ReleaseItemHandles() • ValidateItemIDs() • CreateBrowse()
IOPCHDA_Browse	• GetEnum() • ChangeBrowsePosition() • GetItemID() • GetBranchPosition()
IOPCHDA_SyncRead	• ReadRaw() • ReadAttribute() • ReadProcessed()
IOPCHDA_SyncUpdate	• QueryCapabilities() • Insert()
IConnectionPoint	• Advise() • UnAdvise()
IOPCHDA_AsyncRead	• ReadRaw() • AdviseRaw() • ReadProcessed() • AdviseProcessed() • ReadAttribute() • Cancel()
IOPCHDA_Playback	• ReadRawWithUpdate() • ReadProcessedWithUpdate() • Cancel()
IOPCHDA_DataCallback	• OnDataChange() • OnReadComplete() • OnReadAttributesComplete() • OnPlayback() • OnCancelComplete()

7.4 HCI Value-Added Interfaces

7.4.1 Support for HCI added-value interfaces

HCI provides specific interfaces that clients can use; Redirection Manager supports all these interfaces. While returning HCI-specific interfaces to clients, Redirection Manager ensures that Primary and Secondary servers support these interfaces. If the interfaces are not supported, Redirection Manager returns an error.

Examples of HCI value-added interfaces include IHciAttributes and IHciClientUtil.

7.5 Error Handling

7.5.1 Types of errors

This section describes how Redirection Manager passes server errors back to the client. The errors discussed are those returned by the server during normal operating conditions. These errors are different from errors that cause Redirection Manager to initiate a switchover, such as an RPC/network error.

7.5.2 I/O request error behavior

Redirection Manager forwards OPC I/O calls only to the Active server. Redirection Manager sends any error returned by the Active server back to the client. The client handles these errors as if it were connected to the servers directly.

7.5.3 Non I/O request error behavior

For TPNServer and generic OPC connections, all OPC calls categorized as non-I/O are sent to both the Primary and Secondary servers. For Experion connections, no calls are ever sent to a secondary. Experion calls are forwarded only after a failover has completed, therefore the server has been promoted to primary when the call occurs.

7.5.4 OPC call and error matrix

The following table lists a matrix of error scenarios. The approach is the same for other non-I/O requests such as AddItems, Advise, and UnAdvise.

OPC call	Primary	Secondary
AddGroup	Fails - errors are returned to the client	NA - Call is not forwarded to the Secondary
AddGroup	Succeeds	Succeeds
AddGroup	Succeeds	Fails - Flags the Secondary server to be out of sync. Attempts to retry the call before switchover.

In the case of AddItems, the HRESULT returned could be S_FALSE, which indicates that the operation completed with partial success and one or more items were not added to the group. The RDM only forwards items that were successfully added to the Primary to the Secondary server. The RDM flags the Secondary to be in the ‘out of sync' status for any return value other than S_OK.

Since Redirection Manager saves the state of all non-I/O calls, it can attempt the re-synchronization. If re-synchronization fails, Redirection Manager DOES NOT switch over to the Secondary server. Use the manual **Synchronization** feature provided in the Redirection Manager Auxiliary Status Display (shown in the following section) to attempt re-synchronization.

7.5.5 WMI Provider errors

Redirection Manager's built-in WMI Client connects to the WMI Providers on the server node through the WMI service. When any Honeywell Provider fails, the WMI service sends an asynchronous error back to the RDM WMI client. The RDM WMI client handles this error by setting the RDM status to Warning and logging the error in the Windows 2000 event log. The error appears on your RDM Status Display.

If the providers are unavailable during startup, RDM does not connect to the servers but returns an error back to the client. In the case where the providers fail after the RDM has started, RDM logs the error in the event log, but continues to remain connected to the servers. Once the providers become available, RDM receives a WMI event and reconnects to the provider.

8 Redirection Manager Status

Related topics

“Monitoring RDM Status” on page 74
“Viewing RDM on system displays” on page 75
“Viewing logged events” on page 81

8.1 Monitoring RDM Status

8.1.1 About Redirection Manager Status monitoring

You can view the status of each Redirection Manager client connection in system displays. The displays contain information about whether the RDM is running. This status is the same as the status for an HCI server (for example, Running, Warning, or Stopped).

8.1.2 Monitoring Redirection Manager from the Auxiliary Status Display

The Auxiliary Status Display contains information about the RDM's Primary and Secondary servers, such as:

- Name of the Primary and Secondary servers
- Status of the Primary and Secondary nodes
- Status of the Primary and Secondary servers
- Whether the Primary or Secondary server is *Active* or *Inactive*
- Whether the Servers are running and synchronized.

8.2 Viewing RDM on system displays

The displays that are available include

- Experion's System Status Display -- available on R300 and later Experion systems.
- System Management Display -- available on Experion and TPS systems.
- Standalone RDM configuration tool also doubles up as a monitoring tool that can be used to view RDM status.

A client connection to Redirection Manager causes the connection to appear automatically in the system displays. A client disconnect causes the connection to disappear from the system displays. Successive client connections to the same Redirection Manager appear as multiple instances.

Attention

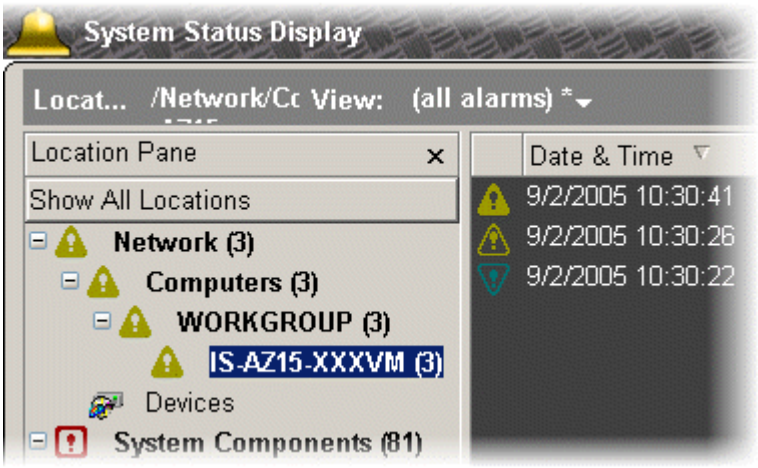
RDM displays a subscript each connection, with the exception of the first connection, which has no subscript. The subscript incrementally counts RDM connections to a client node. If a client has multiple connections, disconnects a subset of them, and then subsequently reconnects, the connection will be incrementally numbered. For example: If you disconnect RM01(2), then reconnect, the new connection will appear as RM01(3).

8.2.1 Viewing RDM on Experion's System Status Display

RDM status appears in the Experion System Status Display when you double-click the node of interest from the Network Tree. The node's computer detail display then presents RDM status for any instantiated RDMs.

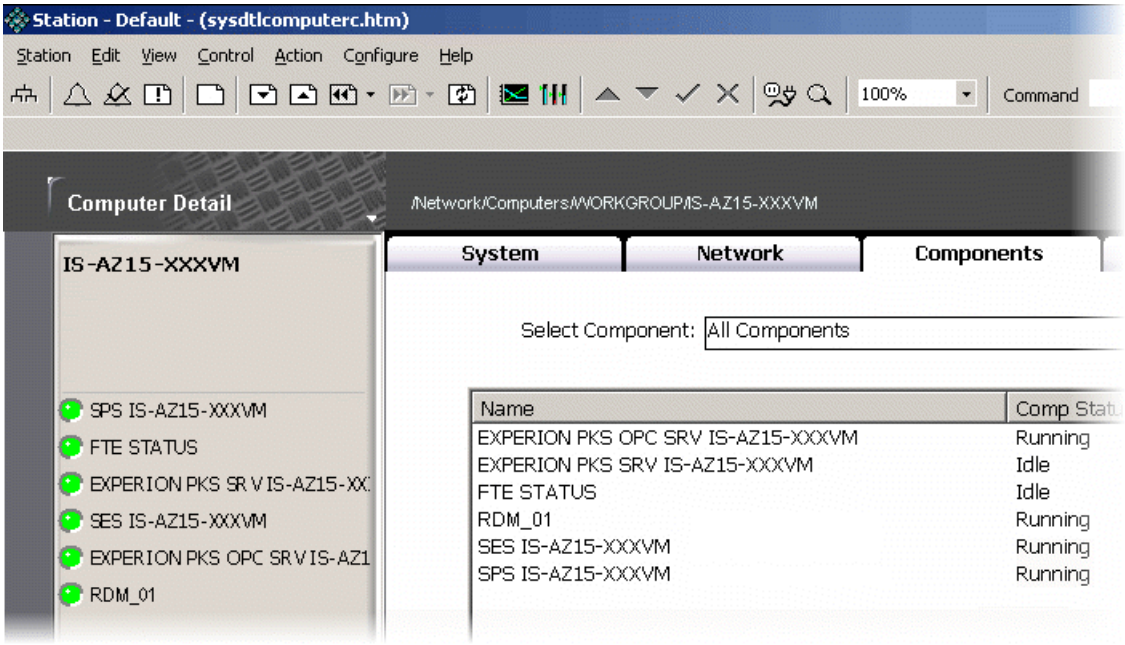
Prerequisite: You must have mngr access level to view computer detail displays.

1 Double click the node of interest from the Network Tree in the System Status display.



The node's computer detail display appears.

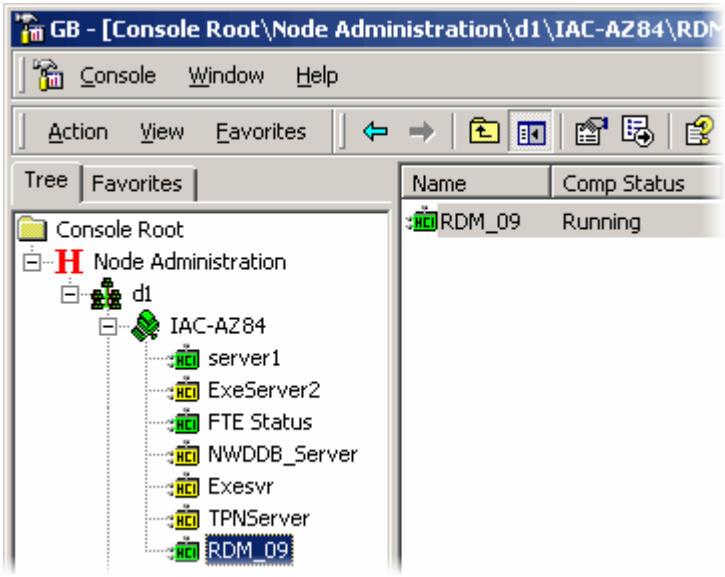
2 Click the Components tab while in the computer detail display.



3 Select the RDM of interest and click **Aux. Display**.
Result: The RDM Auxiliary Status Display appears

8.2.2 RDM on the System Management Display

The following figure shows the System Management Display, with expanded details of a computer node This display shows that this node currently has a single connection to RDM_09.

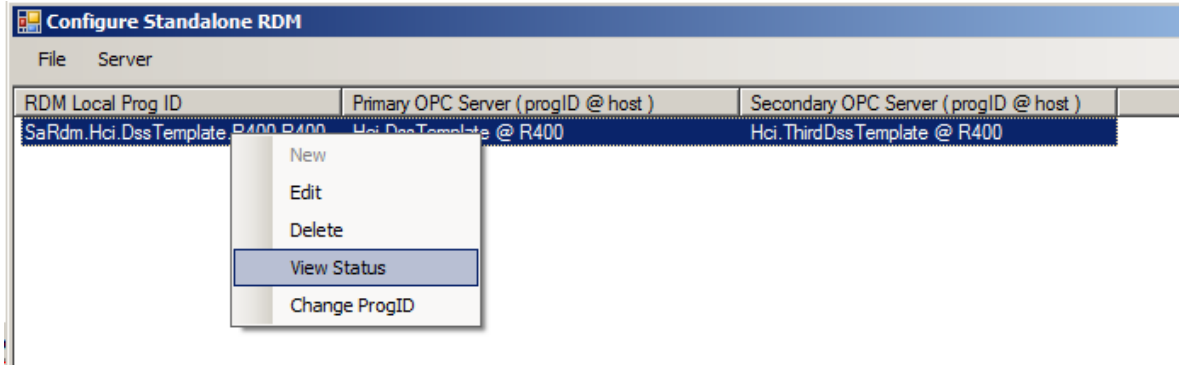


8.2.3 Viewing RDM on System Management Display

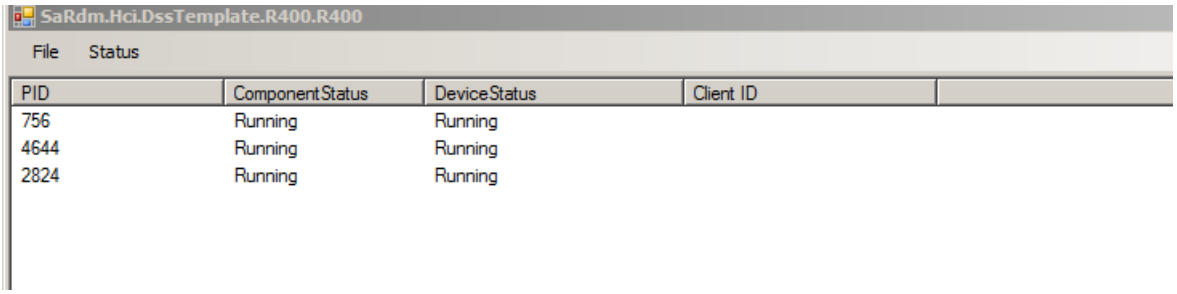
1 Select a connection (for example, RDM_10) from the System Management Display.
2 Right-click the selection and select **Auxiliary Display** from the menu.
Result: The RDM Auxiliary Status Display appears.

8.2.4 RDM on the Standalone RDM configuration display

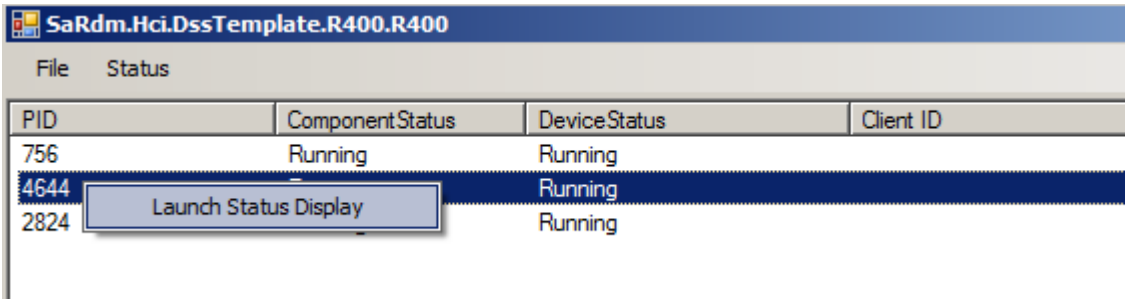
As shown in the figure below, select a configuration and click ‘View status'.



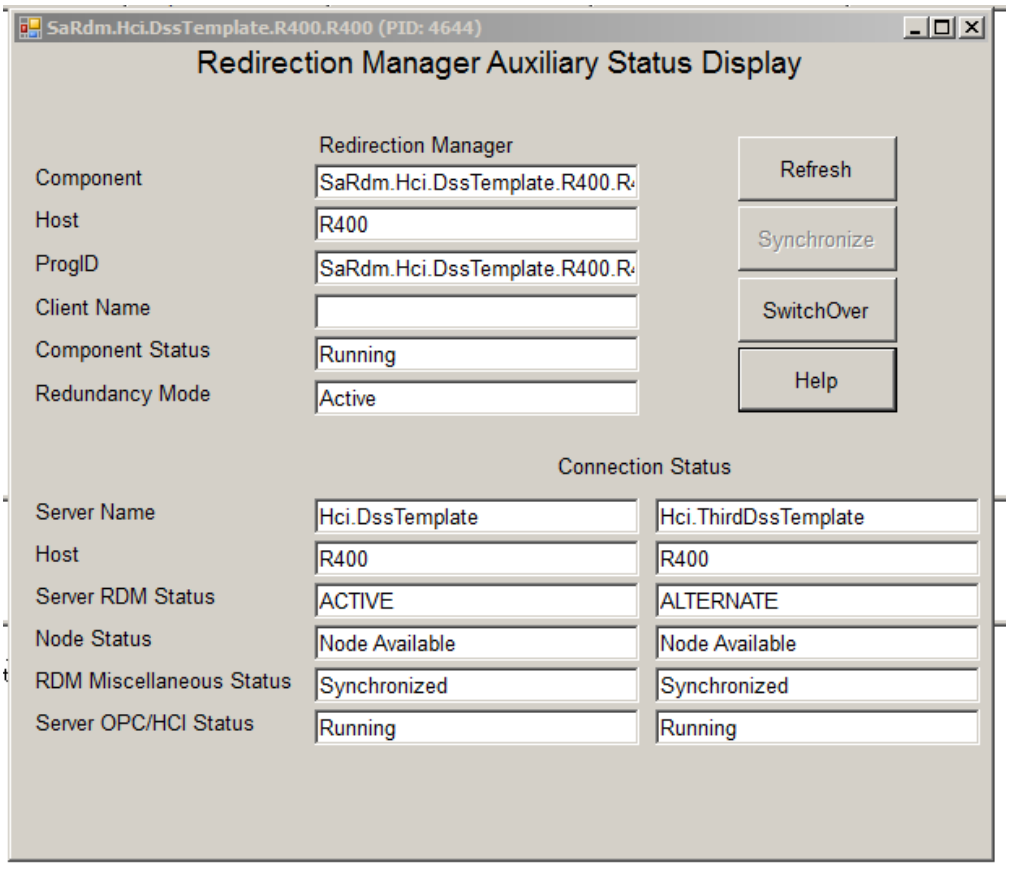
This brings up a summary component status form which shows all running standalone RDM instances launched with this configuration/progID. The form updates automatically as instances are created and deleted and displays summary status (e.g., ‘Running', ‘Initializing') of the PID instance.



Select a connection (for example, 4644) from the form. Right-click the selection and select Launch Status Display from the menu.

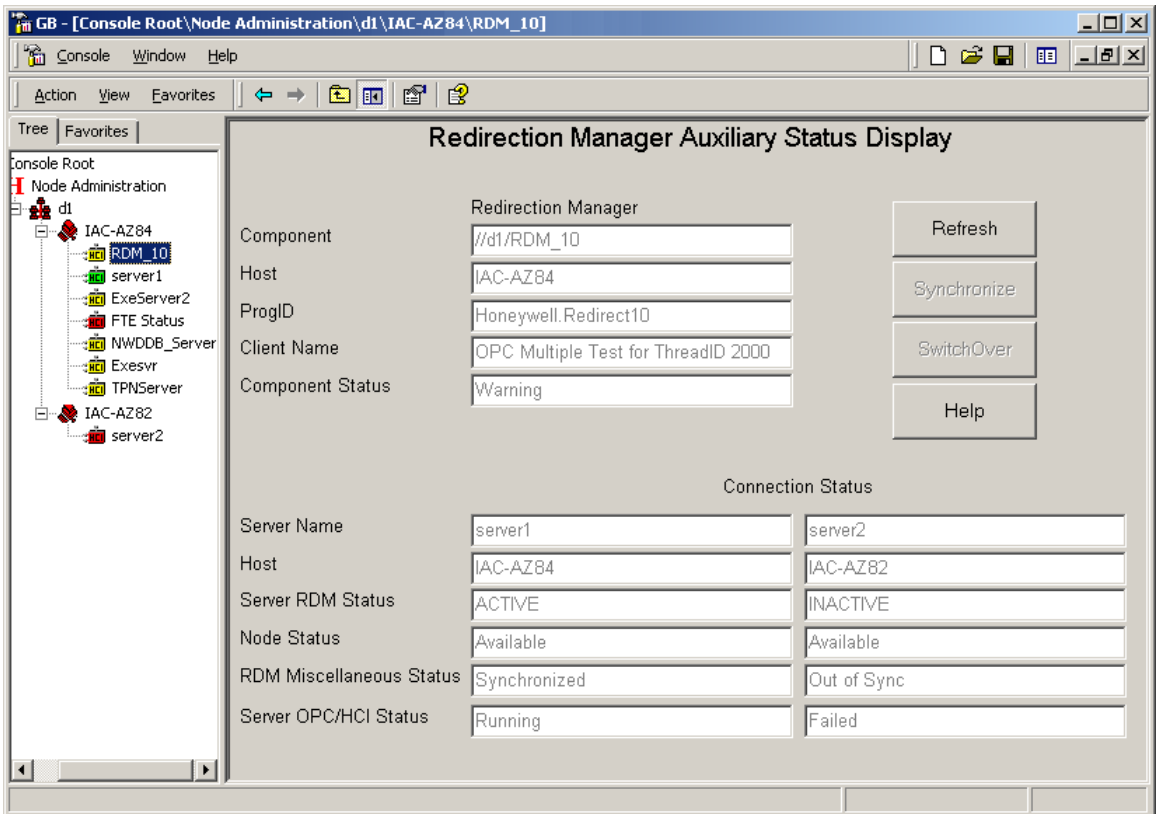


The RDM Auxiliary status display appears as a separate form on the screen. It is possible to bring up auxiliary displays for multiple instances at the same time.



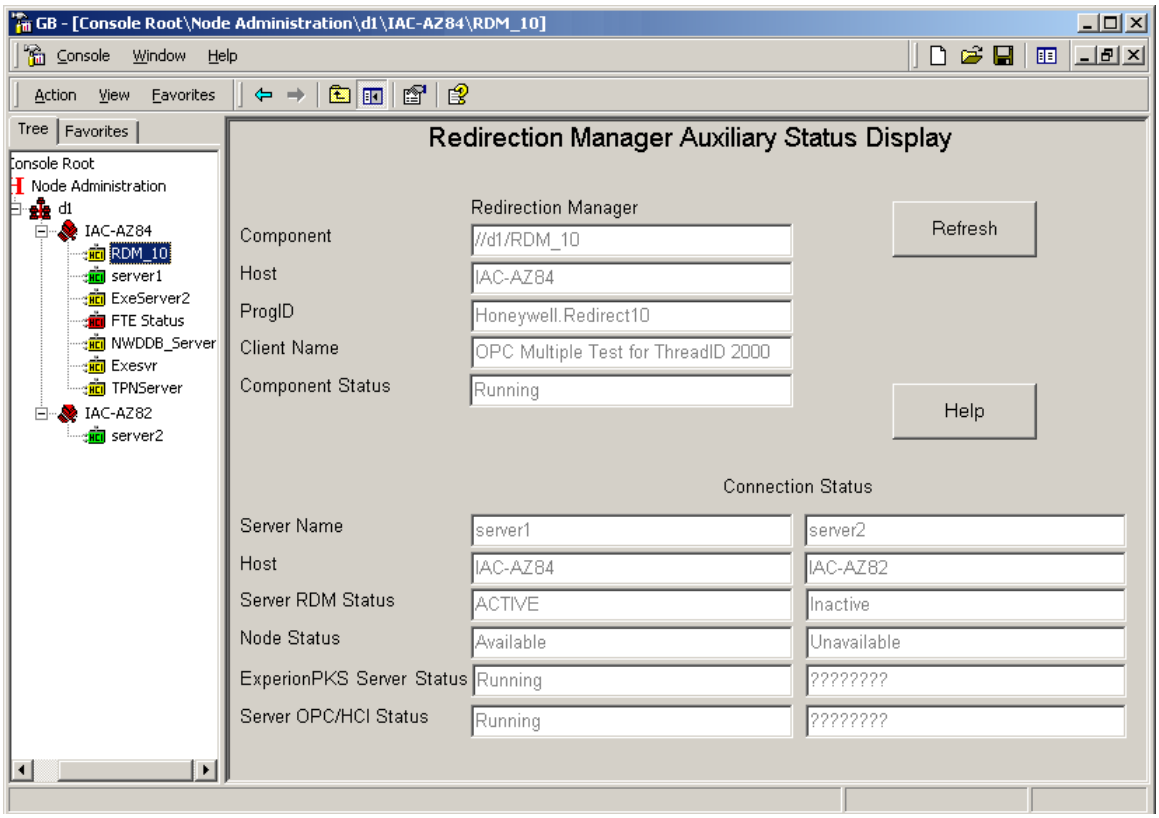
8.2.5 Redirection Manager Auxiliary Status Display when Active RDM connected

The RDM Auxiliary Status Display has textual representation of data shown in a multi-column list. In the following figure, the Connection Status shows the RDMs status for the Primary/Secondary pair, either 'Synchronized' or 'Out Of Synch'. Buttons for switchover and synchronization allow the user to influence the redundant behavior when conditions permit.



8.2.6 Auxiliary Status Display when Passive RDM connected

For target OPC servers that require passive RDM (such as Experion connections as shown in the following figure) the Connection Status shows the 'Redundancy Status' as reported by the Status Components running on the Primary and Secondary nodes. The buttons for switchover and synchronization are not available for passive RDM connections because the redundancy mode for those servers operates independently from the RDM. This figure also demonstrates the status hierarchy whereby lower level status information is shown as question marks when a higher-level status has made that data unavailable. In the example, the secondary node is unavailable so the Experion server status and the OPC server status are unknown.



8.2.7 Redirection Manager Auxiliary Status Display description

The following table lists the descriptions of RDM Auxiliary Status Display components.

Button	Purpose
Switchover[1]	Initiates a manual switchover to the Secondary server from a Primary server, or from a Secondary server to a Primary server.
Refresh	Refreshes the display contents with new information.
Synchronize[1]	Attempts a re-synchronization of the state of non-I/O calls
Help	Accesses online documentation about RDM.

Field	Primary and Secondary Status Descriptions
Server Name	Name of HCI/OPC or OPC Server
Host	Host node name
Server RDM Status	Currently Active or Inactive server
RDM Misc[1] **Status**	State of non-I/O calls—synchronized or non-synchronized
Redundancy[2] **Status**	State of the node hosting the Experion server: Running, Backup[2], Failed, etc.
Server OPC/HCI Status	Current state of the OPC Server: Running, Idle, Stopped, Warning, Failed, etc.

1. Not available when target OPC server requires passive RDM (such as Experion Connections).
2. Available only for target OPC Servers that require passive RDM (such as Experion Connections).

8.3 Viewing logged events

RDM logged events represent the same status changes you would see in an R300 and later Experion System Status Display or System Management Display. The Redirection Manager logs all events and errors into the Windows Event Log.

Typical event entries in the Event Log include:

- Switchovers to the Secondary server when the Primary server fails.
- Errors returned during OPC calls made to an Alternate server. Errors from the Active server are returned directly back to the client.
- 'Out of sync' error messages may appear on the Alternate server. If you see this message, check the event log for more information.

9 Notices

Trademarks

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

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

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

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

Third-party licenses

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

9.1 Documentation feedback

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

http://www.honeywellprocess.com/support

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

hpsdocs@honeywell.com

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

9.2 How to report a security vulnerability

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

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

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

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

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

- Send an email to security@honeywell.com.

  or

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

9.3 Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

9.4 Training classes

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