

# **Integration Objects'**

**Seamless & Secure IT-OT-IIoT Integration  
Platform**

**Smart IoT Highway**

Version 2.4.3

**REDUNDANCY GUIDE**

Integration Objects' Smart IoT Highway Redundancy Guide Version 2.4.3

Published April 2026.

Copyright © 2018 - 2026 Integration Objects. All rights reserved.

No part of this document may be reproduced, stored in a retrieval system, translated, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Integration Objects.

Windows®, Windows NT® and .NET are registered trademarks of Microsoft Corporation.

SIOTH® is a registered trademark of Integration Objects.

# TABLE OF CONTENTS

<b>PREFACE.....</b>	<b>5</b>
<b>INTRODUCTION .....</b>	<b>7</b>
<b>CONFIGURATION .....</b>	<b>9</b>
1. Requirements.....	9
2. Redundancy Modes.....	9
3. Configuration Parameters .....	10
4. Redundancy Configuration Process .....	15
4.1. Define Redundancy Server Architecture.....	17
4.2. Configure the Application on the Primary Server.....	17
4.3. Configure Redundancy .....	20
4.4. Manual Synchronization with Redundancy Node .....	22
4.5. Test Force Switchover.....	23
4.6. Verify End-to-End Solution.....	24
4.7. Configure the Extend Switchover Logic.....	24
4.8. Configure the Exclude from Redundancy .....	31
5. Best Practices .....	33

## TABLE OF FIGURES

Figure 1: SIOTH® Platform Overview .....	7
Figure 2: SIOTH Redundancy Architecture .....	10
Figure 3: SIOTH Redundancy Configuration View .....	11
Figure 4: Workflow Configuration Process .....	16
Figure 5: Data Flow Configuration in Primary Server.....	18
Figure 6: Data Model Menu .....	19
Figure 7: Job Engine Rule Example.....	19
Figure 8: SIOTH Primary Configuration .....	20
Figure 9: Node Status - Primary.....	21
Figure 10: Node Status - Secondary .....	22
Figure 11: Manual Synchronize with Redundant Node .....	23
Figure 12: Force Switchover Button .....	24
Figure 13: Extend Switchover Logic Option .....	25
Figure 14: Extend Switchover Logic - New Rule Configuration View.....	26
Figure 15: Switchover Expression .....	31
Figure 16: Exclude from Redundancy Option.....	32
Figure 17: Exclude OPC UA server from Redundancy Example .....	32

## LIST OF TABLES

Table 1: SIOTH Redundancy Parameters .....	15
Table 2: Extend Switchover Logic - New Rule Configuration Parameters .....	30

# PREFACE

## About This User Guide

This guide:

- Presents Integration Objects' Smart IoT Highway Redundancy Configuration.
- Describes the functions provided by Integration Objects' Smart IoT Highway for Redundancy Configuration.
- Explains each step of the configuration process.

## Target Audience

This document is intended for users, application engineers, and IT/OT integrators who are responsible for configuring Integration Objects' Smart IoT Highway, with a particular focus on the redundancy feature.

## Document Conventions

Convention	Description
<b>Bold</b>	Bolded text indicates user interface elements, such as buttons, menu items, and dialog names.
<b>(!) Note</b>	Information to be noted

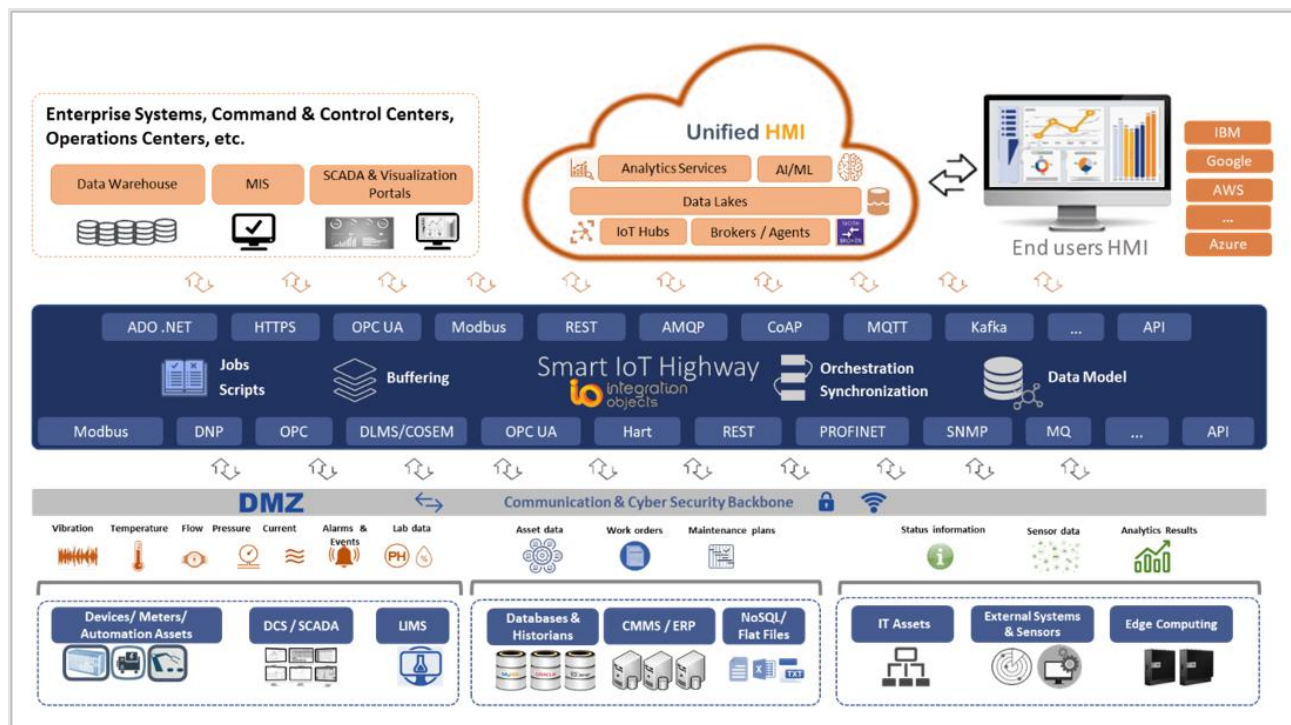
## Customer Support Services

Phone	Email
<b>Americas:</b>  +1 713 609 9208  <b>Europe-Africa-Middle East</b>  +216 71 195 360	Support: <a href="mailto:customerservice@integrationobjects.com">customerservice@integrationobjects.com</a>  Sales: <a href="mailto:sales@integrationobjects.com">sales@integrationobjects.com</a>  Online: <a href="http://www.integrationobjects.com">www.integrationobjects.com</a>

# INTRODUCTION

Smart IoT Highway (SIOTH®) is an advanced IT-OT integration platform designed to facilitate secure data exchange and transformation. It establishes secure end-to-end pipelines to collect and store data from edge IoT devices and various other sources. SIOTH® enables organizations of all sizes to easily connect applications, systems, and services in a managed, scalable, and secure environment. This comprehensive integration solution allows for seamless connectivity between IT and OT, enabling the conversion of industrial data into actionable intelligence and valuable insights.

The SIOTH® platform operates on robust functional architecture, as illustrated in the figure below:



**Figure 1: SIOTH® Platform Overview**



Redundancy is a key mechanism for achieving high availability and minimizing the risk of system outage. It relies on the use of backup or duplicate systems to ensure uninterrupted operation in the event of a failure.

In SIOTH<sup>®</sup>, redundancy is an advanced capability that enhances system fault tolerance and operational reliability. It allows two SIOTH systems to operate in a linked configuration, where one system automatically assumes control if the other becomes unavailable, ensuring seamless continuity without service interruption.

# CONFIGURATION

**SIOTH® Redundancy** is designed for a two-node architecture to ensure solution availability. It is deployed across two separate servers within the same network: the **primary server** that manages active operations and a **secondary server** that remains on standby as the backup, ready to take over in the event of a failure.

## 1. Requirements

- **Identical hardware and software configurations**

Both servers must have the same hardware specifications and software versions to ensure compatibility and consistent performance.

- **Reliable network connectivity**

A stable, high-speed network connection is required to allow continuous synchronization between the two servers without latency or data loss.

- **Time synchronization**

System clocks on both servers must be synchronized to prevent data inconsistencies and to ensure accurate event logging and timestamping.

## 2. Redundancy Modes

SIOTH® supports two redundancy modes:

- **Cold Redundancy**

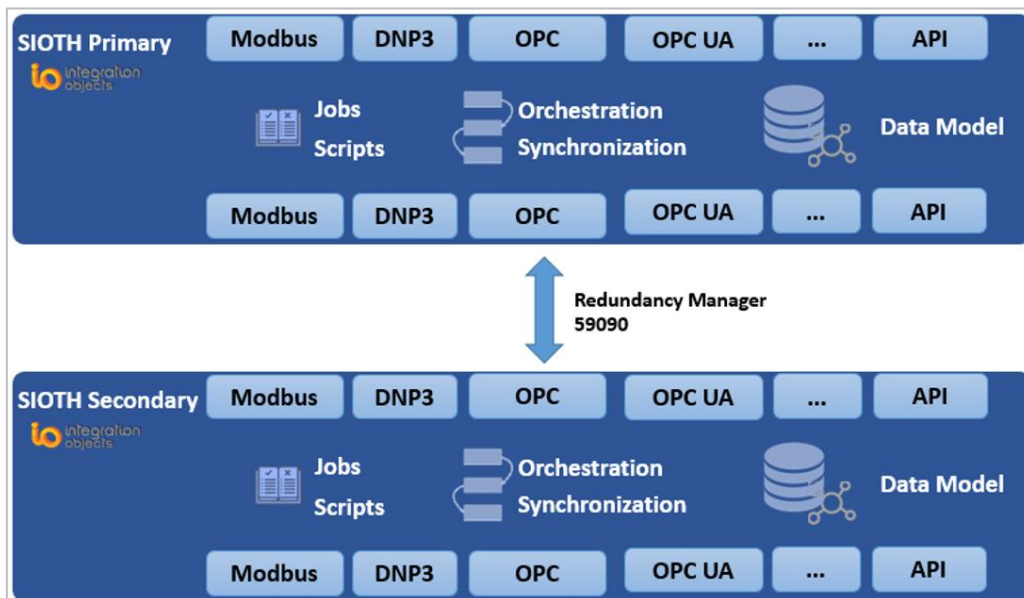
In this mode, the secondary server remains inactive while the primary server handles all operations. If the primary server fails, the secondary server is activated and assumes control.

- **Hot Redundancy**

In this mode, both servers operate simultaneously. The secondary server continuously mirrors the primary server's state. If the primary server becomes unavailable, the secondary server takes over immediately, ensuring seamless operation with no service interruption.

Redundancy is supported for **standalone SIOTH installations only** and is not available for **distributed SIOTH architectures**. As a result, redundancy applies exclusively to deployments where SIOTH is installed on a dedicated pair of servers, rather than across multiple distributed system.

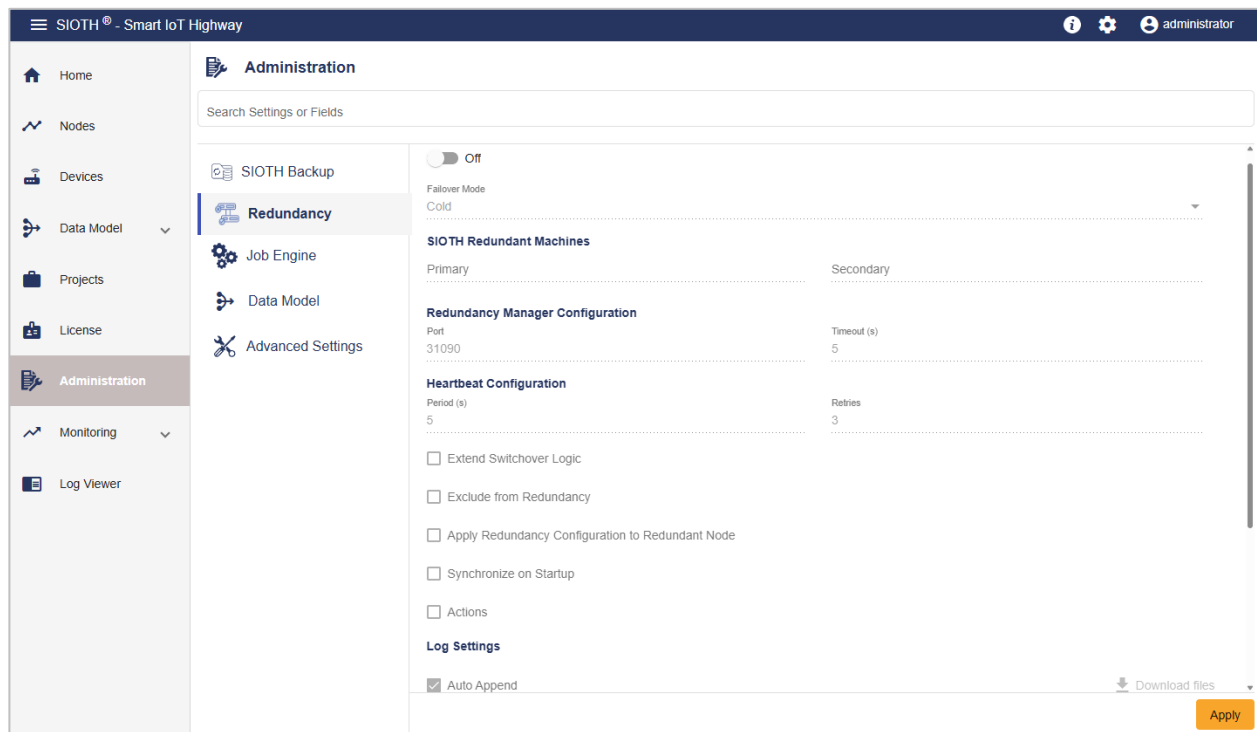
The high-level SIOTH redundancy architecture is illustrated in the figure below, which presents the overall system configuration between the primary and secondary servers.



**Figure 2: SIOTH Redundancy Architecture**

### 3. Configuration Parameters

Navigate to the **Administration** section in the left-side menu, then click the **Redundancy** menu section.



**Figure 3: SIOTH Redundancy Configuration View**

Parameter	Description	Default Value
<b>On/Off</b>	Enables or disables redundancy on the SIOTH server. Enabling or disabling redundancy from the SIOTH® user interface starts or stops the <b>SIOTH Redundancy Manager</b> service.	Off
<b>Failover Mode</b>	Defines the redundancy behavior: <ul style="list-style-type: none"> <li><b>Cold Redundancy:</b> The secondary server remains offline and is activated only if the primary server fails, which may result in brief downtime.</li> <li><b>Hot Redundancy:</b> Both servers run concurrently, allowing immediate failover with</li> </ul>	Cold

	no service interruption.	
<b><i>SIOTH Redundant Machines</i></b>		
<b><i>Primary</i></b>	IP address or host name of the Primary server. The primary server acts as the master node, managing synchronization and listening for connections from the secondary server.	
<b><i>Secondary</i></b>	IP address or host name of the Secondary server. The secondary server connects to the primary server to receive system updates and synchronization data.	
<b><i>Redundancy Manager Configuration</i></b>		
<b><i>Port</i></b>	Communication port used by redundancy managers on both servers to maintain the redundancy link. If this connection fails, both systems are set to Primary mode to maintain operational continuity.	31090
<b><i>Timeout (s)</i></b>	Maximum time the redundancy manager waits for a response from the remote node. If no response is received within this period, the remote server is considered unavailable and a switchover is triggered.	5
<b><i>Heartbeat Configuration</i></b>		
<b><i>Period (s)</i></b>	Interval at which the system checks the operational status of the redundant SIOTH® server.	5
<b><i>Retries</i></b>	Number of retry attempts made to reconnect or verify the status of the redundant server before declaring it unavailable and initiating a switchover.	3
<b><i>Extend</i></b>	By default, switchover occurs when a manual	Disabled

<b>Switchover Logic</b>	<p>switchover is initiated or when the primary server becomes unavailable.</p> <p>This option allows users to define custom rules, evaluated only on the Primary server using the switchover Expression, to determine when a switchover should occur.</p>	
<b>Exclude from Redundancy</b>	<p>Specifies whether selected connectors on the secondary server should be excluded from the configured redundancy mode or not. This option is applicable only in Cold Redundancy mode.</p> <p><i>Example:</i> Source connectors may remain active on the secondary server to ensure both servers maintain connectivity to devices.</p>	Disabled
<b>Apply Redundancy Configuration to Redundant Node</b>	<p>Enables synchronization of redundancy-related configurations from the primary server to the secondary server. This includes <b>rules</b>, <b>exclusions</b>, and <b>action</b> configurations. Once synchronized, the configuration is automatically applied to the redundant node.</p>	Disabled
<b>Synchronize on Startup</b>	<p>Determines whether data or configuration synchronization is initiated when the redundancy service starts or not. When the secondary server comes online, it requests synchronization from the primary server.</p>	Disabled
<b>Actions</b>	<p>Allows the server status to be exposed to external applications using standard protocols. This enables</p>	Disabled

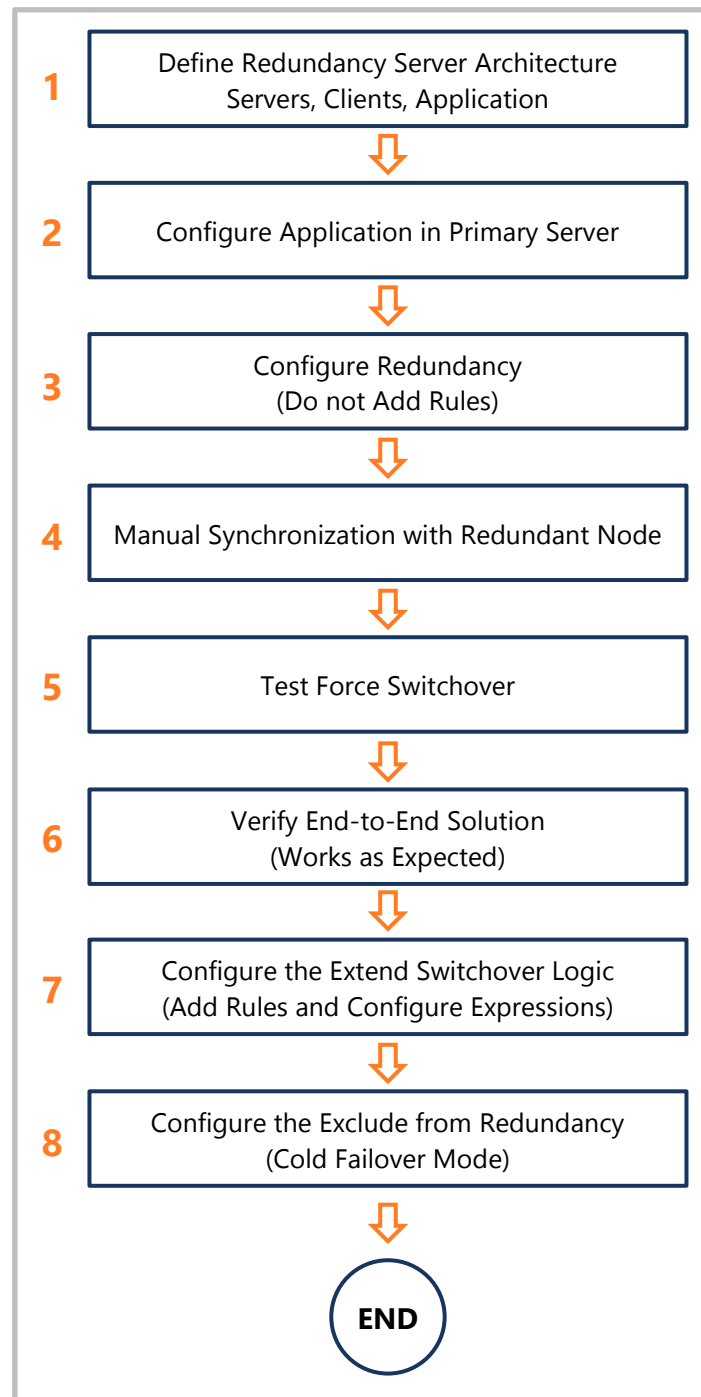
	external systems to determine which server is active.  <i>Example:</i> A writable OPC UA tag can be configured to indicate whether the node is operating as <i>Primary</i> or <i>Secondary</i> .	
<b>Log Settings</b>		
<b>Auto Append</b>	Enables automatic insertion or appending of log entries to the current log file.	Enabled
<b>Log Level</b>	Specifies the minimum severity level of log messages to be recorded. Available levels include: <ul style="list-style-type: none"> <li>Information</li> <li>Debug</li> </ul>	Information
<b>Buffer Size (MB)</b>	Defines the amount of data temporarily stored in memory before being written to the log file.	100
<b>Maximum Files</b>	Specifies the maximum number of log files that can be generated. A value of <b>0</b> indicates no limit.	10
<b>Log File Max Size (MB)</b>	Defines the maximum size of each log file before a new file is created.	10
<b>Auto Save Timeout (s)</b>	Specifies the time interval, in seconds, after which the system automatically saves log data or configuration changes.	5
<b>Download Files</b>	Allows users to download log files from the system.	
<b>Force Switchover</b>	Allows a manual role switch from the Primary server to the Secondary server. This operation can only be initiated from the Primary server.	

**Table 1: SIOTH Redundancy Parameters**

## 4. Redundancy Configuration Process

This section outlines the redundancy configuration workflow in SIOTH®. It describes the overall process and the logical sequence of actions required to successfully configure and validate redundancy between the primary and secondary servers.



**Figure 4: Workflow Configuration Process**

## 4.1. Define Redundancy Server Architecture

The first step in configuring redundancy is to define the overall server architecture. This step establishes how servers, clients, and applications are organized to support a redundant SIOTH deployment.

- **Servers**

Identify and configure the servers participating in the redundancy setup. This includes two servers: a **Primary server** and a **Secondary (standby) server**. The Primary server manages active operations, while the Secondary server remains available to take over in the event of failure. Both servers must be capable of synchronizing data and configuration changes to ensure a seamless failover without service disruption.

- **Clients:**

Define how client applications and devices interact with the redundant environment. Clients should be configured to recognize both redundant servers, allowing uninterrupted access to services even if one server becomes unavailable.

- **Application Configuration:**

Configure applications to operate in a redundant environment. This includes enabling support for multi-server operation, ensuring proper data synchronization, and handling failover scenarios efficiently. Correct application configuration is essential to minimize downtime and maintain data consistency.

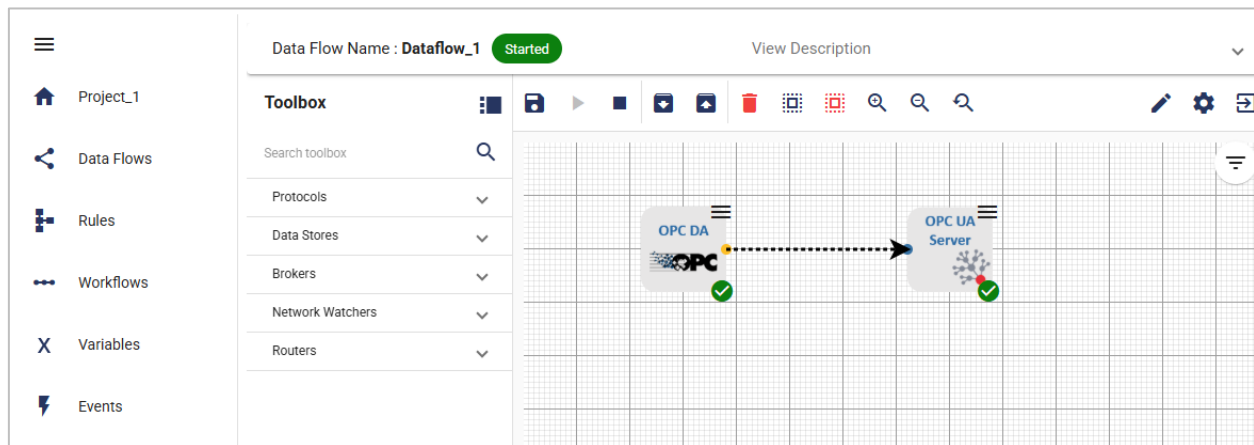
By clearly defining the architecture of these components, a robust and reliable redundancy configuration can be achieved.

## 4.2. Configure the Application on the Primary Server

The next step is to configure the application on the **Primary Server**. This phase involves setting up the project and its associated components to ensure reliable operation, efficient data flow, and full compatibility with the redundancy mechanism. The following configurations must be completed on the Primary server.

- **Data Flow Configuration:**

Define the data flow within the application on the Primary server. This includes configuring how data is collected, processed, transferred, and managed across the system using **Protocols**, **Data Stores**, **Brokers** and **Network Watchers**. A properly defined data flow ensures that all processes operate as expected during normal operation and appropriately routed to continue to function correctly in the event of a failure.



**Figure 5: Data Flow Configuration in Primary Server**

- **Data Model Configuration:**

Configure the Data Model on the Primary server to define the structure, hierarchy, and relationships of application data. The **SIOTH® Data Model** is based on a hierarchical, object-oriented design that organizes data into **classes** with **attributes**, from which **instances** are created. These instances can reference data from **SIOTH® connectors**.

Proper data model configuration ensures:

- Efficient data storage, retrieval, and management.
- Real-time access to attribute values and historical data.
- Consistent synchronization between the Primary and Secondary servers.
- Support for **Job Engine** operations, such as analysis and automation.

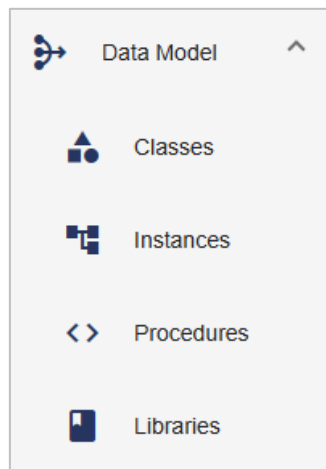


Figure 6: Data Model Menu

#### • Job Engine Configuration:

Configure the Job Engine on the Primary server to manage scheduled tasks, workflows, and background processes. The **SIOTH® Job Engine** combines a rule engine and a workflow engine, enabling the execution of scripts, workflows, and rules for complex event detection and automation. The Job Engine transforms and aggregates data obtained through **SIOTH® Data Flow** from IoT devices, data sources, and related assets. Proper configuration ensures reliable execution, adaptability to system changes, and continued operation during failover scenarios.

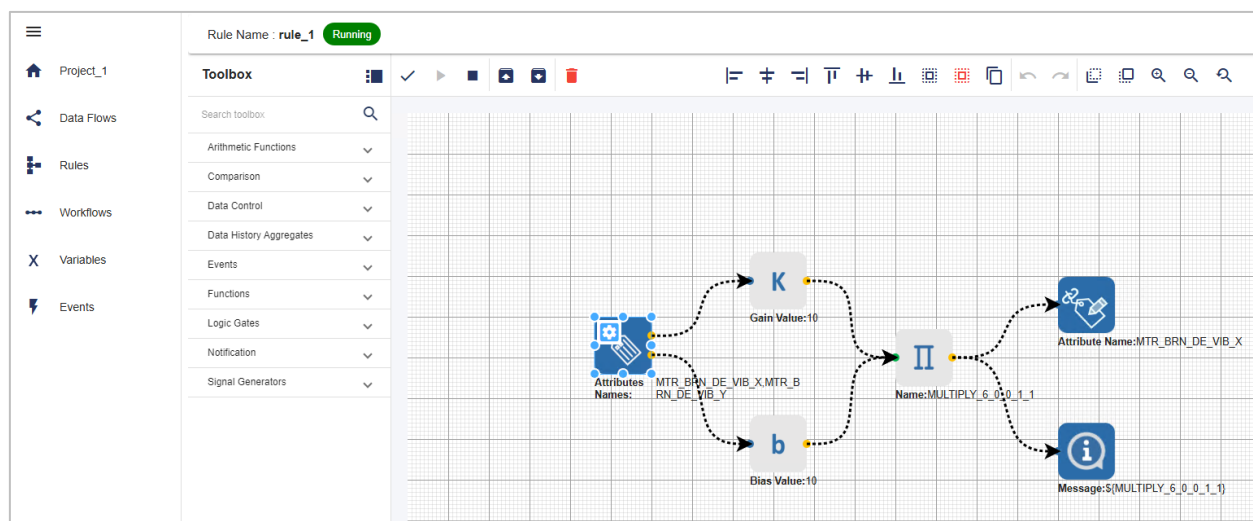


Figure 7: Job Engine Rule Example

By completing these configurations on the Primary server, the application is fully prepared to support redundancy, ensuring consistent data management, reliable rules and workflow execution, and seamless continuity of operation.

### 4.3. Configure Redundancy

#### Configure the Primary Server:

To configure the first SIOTH server as the Primary server, follow these steps:

- 1- Log in to **SIOTH®** in the Primary server.
- 2- Click the **Administration** section located at the left side menu (1).
- 3- Click the **Redundancy** tab (2).
- 4- Click the **switch** button to enable redundancy (3).
- 5- Select the redundancy mode: **Cold** or **Hot** (4).
- 6- Enter the **Primary** and **Secondary** SIOTH IP Addresses (5).
- 7- Click **Apply** to save the configuration.

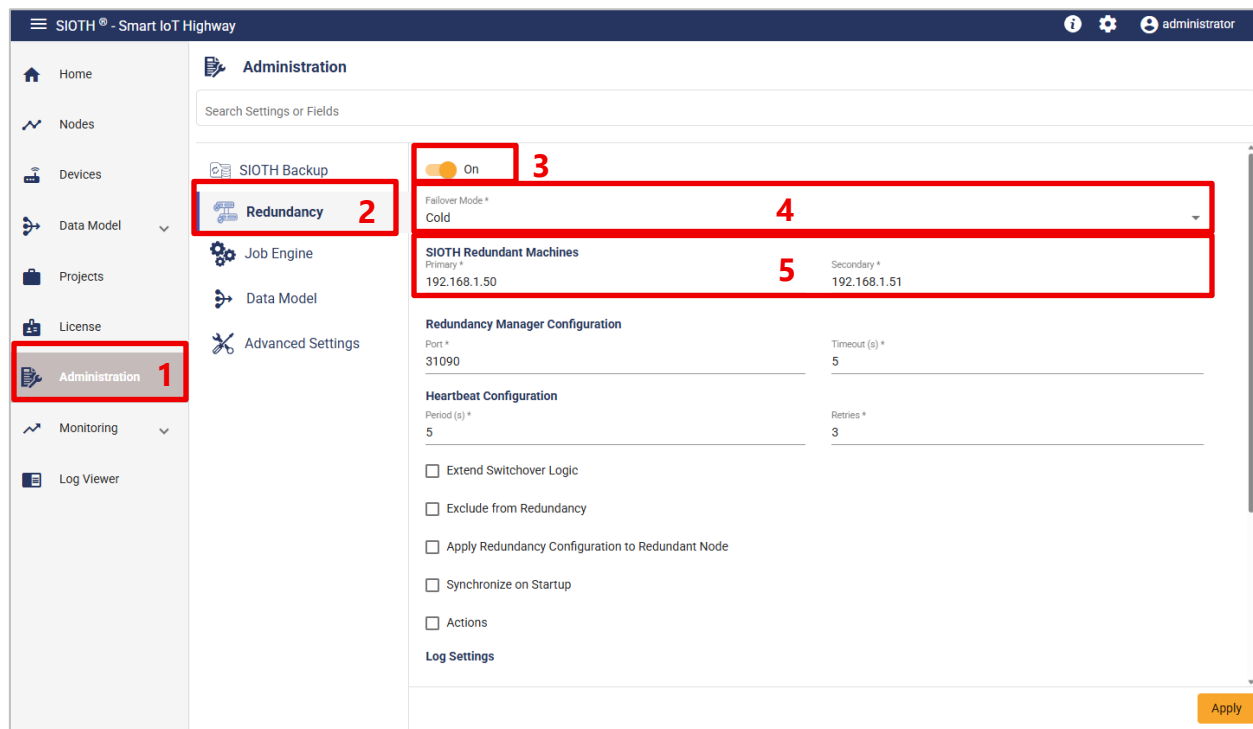
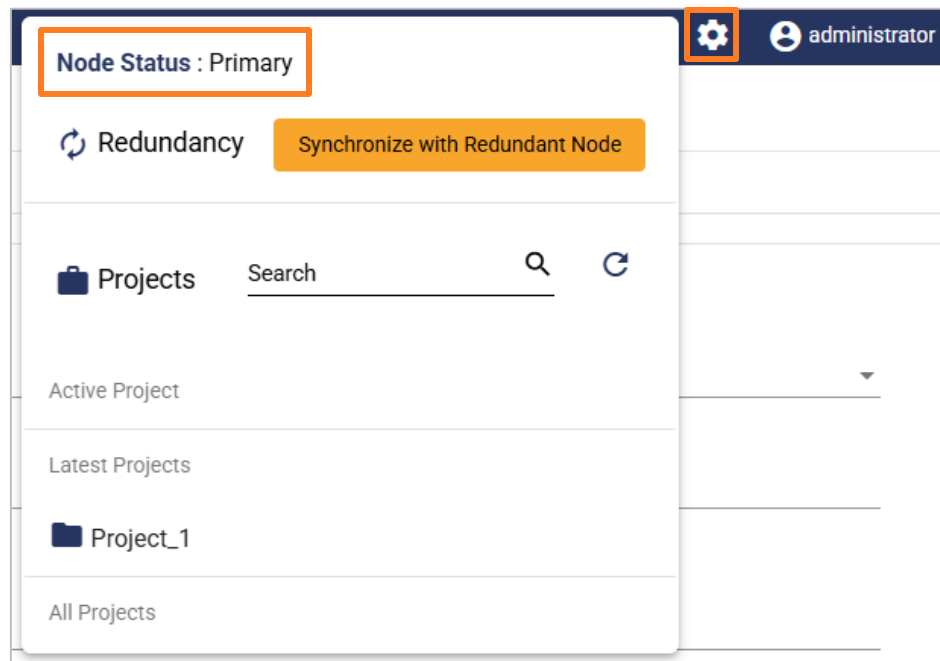


Figure 8: SIOTH Primary Configuration

After the configuration is applied, the server is designated as the **Primary** server. To verify the node status, click the **Configuration** button at the top of the page.



**Figure 9: Node Status - Primary**

#### (!) Note

Switchover logic rules must not be configured at this stage.

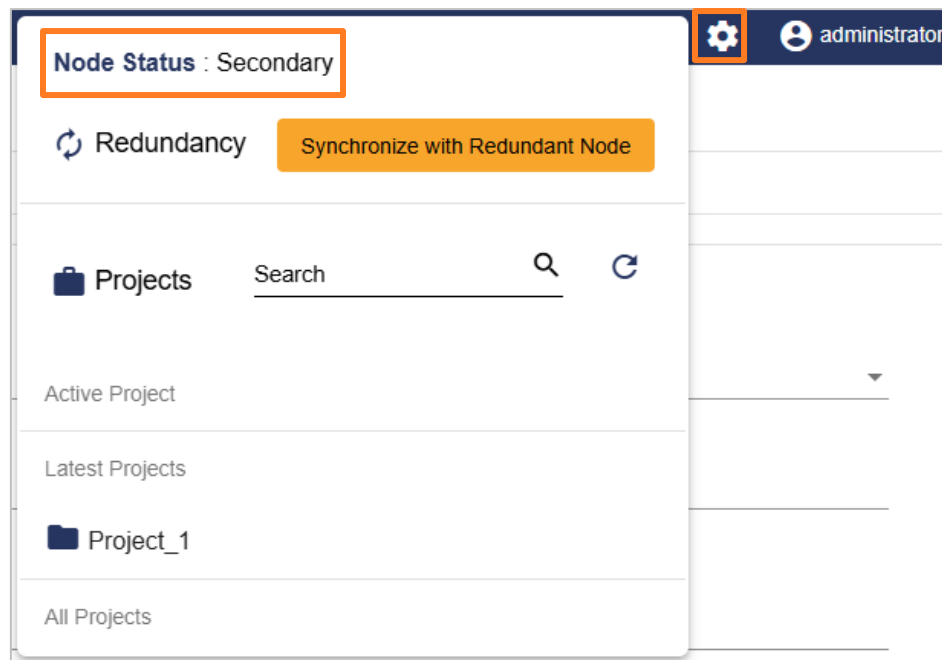
### Configure the Primary Server:

To configure the second SIOTH server as the Secondary server, follow these steps:

- 1- Log in to **SIOTH®** in the Secondary server.
- 2- Click the **Administration** section located at the left side menu.
- 3- Click the **Redundancy** tab.
- 4- Click the **switch** button to enable redundancy.
- 5- Select the same redundancy mode (**Cold** or **Hot**) that was configured on the Primary server.

- 6- Enter the **Primary** and **Secondary** SIOTH IP Addresses exactly as defined on the Primary server.
- 7- Click **Apply** to save the configuration.

After the configuration is applied, the server is designated as the **Secondary** server. To verify the node status, click the **Configuration** button at the top of the page.

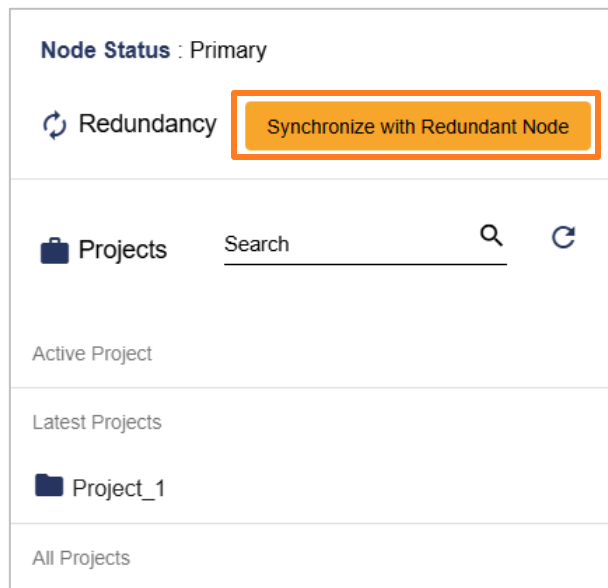


**Figure 10: Node Status - Secondary**

#### 4.4. Manual Synchronization with Redundancy Node

After redundancy has been configured on both the Primary and Secondary servers, the configuration can be manually synchronized to the redundant node.

By clicking the **Synchronize with Redundant Node** button, all relevant configurations - including application settings defined on the Primary server - are replicated to the Secondary server.



**Figure 11: Manual Synchronize with Redundant Node**

#### (!) Note

The **Synchronize with Redundant Node** action can only be performed from the Primary server.

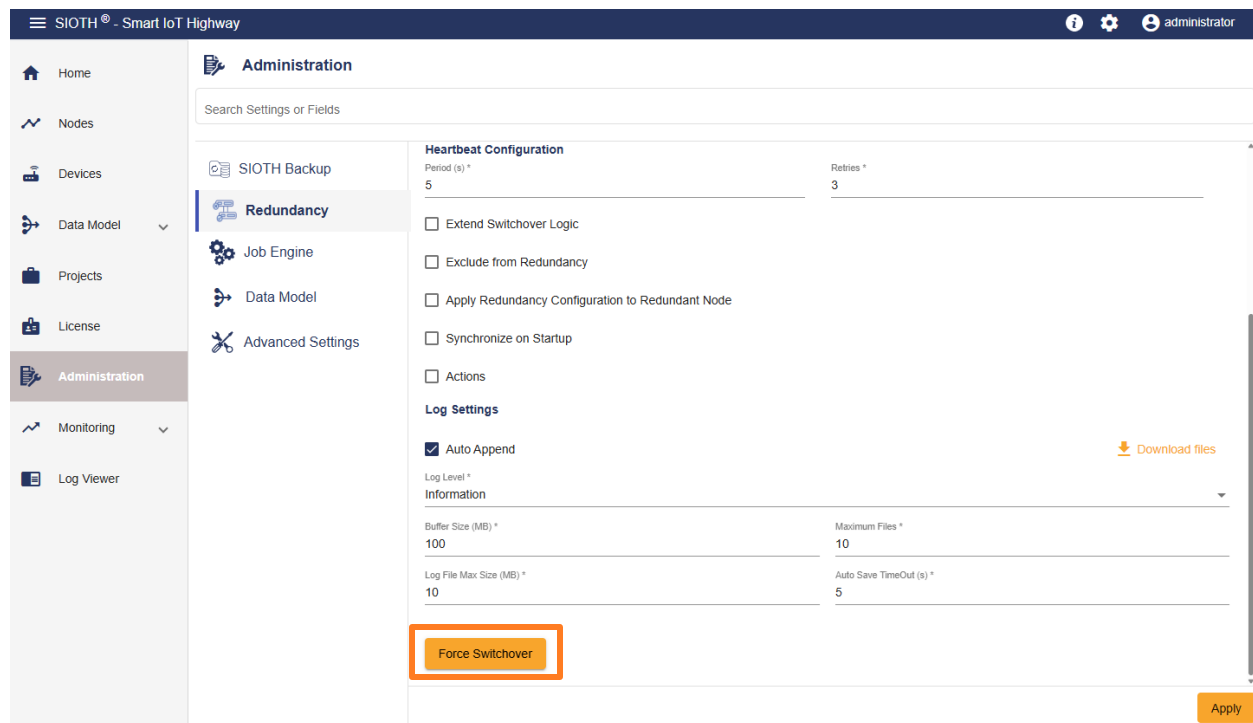
This synchronization ensures configuration consistency between both servers, with the Secondary server mirroring the Primary server's setup. As a result, the system is prepared for seamless failover and sustained high availability.

## 4.5. Test Force Switchover

The **Force Switchover** feature allows to manually transfer the active role from the **Primary server** to the **Secondary server**. This capability is typically used to validate failover behavior or to perform maintenance activities by immediately promoting the Secondary server to handle active operations.

Click the **Force Switchover** button to initiate a manual switchover.





**Figure 12: Force Switchover Button**

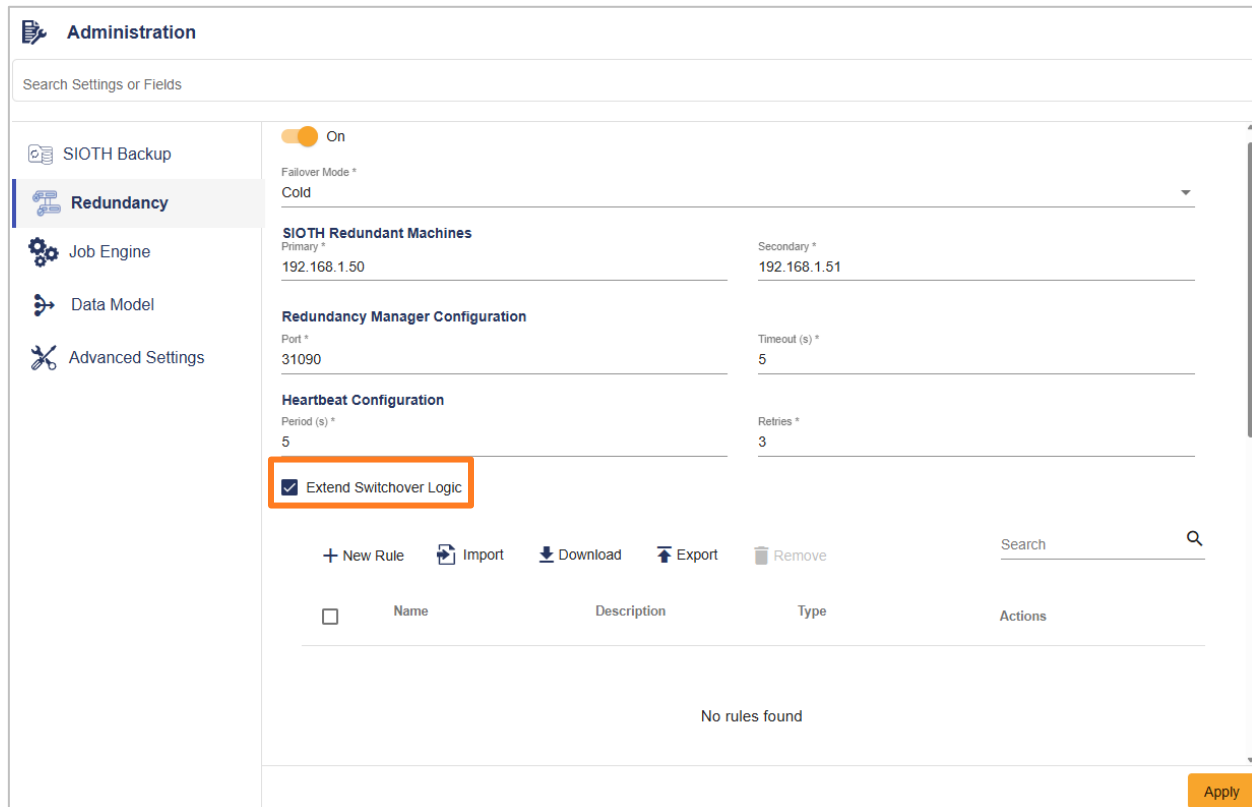
## 4.6. Verify End-to-End Solution

Verify the complete end-to-end solution to ensure it operates as expected. This includes validating synchronization between the Primary and Secondary servers, confirming that the redundancy configuration is correctly applied, and testing switchover behavior to ensure seamless role transitions and uninterrupted operation.

## 4.7. Configure the Extend Switchover Logic

The **Extend Switchover Logic** feature allows to define custom rules that are evaluated on the **Primary server**. Based on the evaluation of these rules, the Primary server automatically executes the switchover logic, enabling a controlled and seamless transition between the Primary and Secondary servers according to predefined conditions.

Enable the **Extend Switchover Logic** option to enable this feature.



**Administration**

Search Settings or Fields

**Redundancy**

On

Fallover Mode \*  
Cold

**SIOTH Redundant Machines**

Primary *	Secondary *
192.168.1.50	192.168.1.51

**Redundancy Manager Configuration**

Port *	Timeout (s) *
31090	5

**Heartbeat Configuration**

Period (s) *	Retries *
5	3

☒ Extend Switchover Logic

+ New Rule   Import   Download   Export   Remove   Search




Name	Description	Type	Actions
No rules found			

Apply

**Figure 13: Extend Switchover Logic Option**

Once enabled, an explorer panel displays all configured rules, with each rule listed on a separate line.

For each rule, the following actions are available:

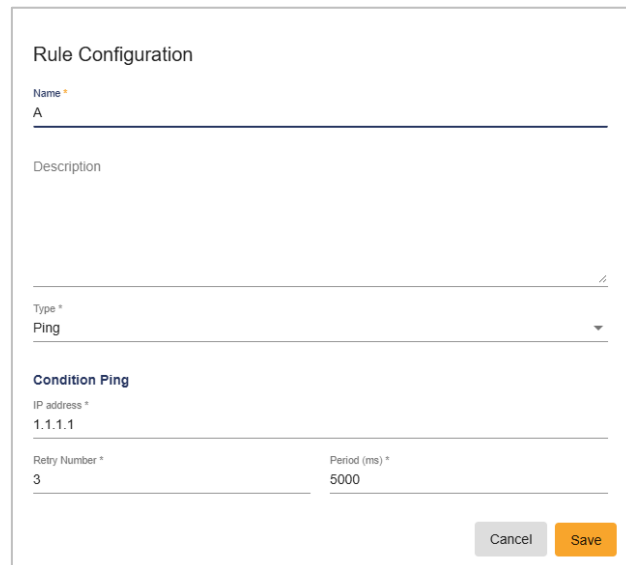
-  **Duplicate:** Creates a copy of the selected rule.
-  **Edit:** Allows you to modify the selected rule.
-  **Delete:** deletes the selected rule from the list when it is no longer required or valid.

The **Extend Switchover Logic** menu also provides the following actions:

- **New Rule:** Adds a new rule to the switchover rules table.
- **Import:** Imports preconfigured switchover rules from an external file, enabling reuse of standardized configurations or replication across multiple SIOTH® installations.

- **Download:** Downloads rules of a selected type (PING, TCPING, Process Monitor, or Device Status). The system generates a file containing only the chosen rule type.
- **Export:** Exports all configured switchover rules into a downloadable file for backup or transfer to another SIOTH® installation.
- **Delete:** Deletes selected rules from the switchover rules table, allowing cleanup or optimization of switchover logic.

Click the **New Rule** button to add a new rule. A configuration dialog appears, displaying the configuration parameters for the rule.



The image shows a 'Rule Configuration' dialog box. It contains the following fields and controls:

- Name \***: A text input field containing the value 'A'.
- Description**: A large text area for describing the rule.
- Type \***: A dropdown menu currently set to 'Ping'.
- Condition Ping**: A section header for ping-specific settings.
- IP address \***: A text input field containing '1.1.1.1'.
- Retry Number \***: A text input field containing '3'.
- Period (ms) \***: A text input field containing '5000'.
- Buttons**: 'Cancel' and 'Save' buttons at the bottom right.

**Figure 14: Extend Switchover Logic - New Rule Configuration View**

Parameter	Description	Default Value
<b><i>Name</i></b>	Name of the rule.	A
<b><i>Description</i></b>	Description of the rule.	

<b>Type</b>	<p>Type of the rule. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>Ping:</b> Verifies network connectivity and reachability between the SIOTH server and the specified machine or device using the <b>ICMP (Internet Control Message Protocol)</b>. Useful for detecting network or device availability issues.</li> <li>• <b>Tcping:</b> Checks connectivity by attempting a TCP connection to a specified port, typically used to verify service availability.</li> <li>• <b>Process Monitor:</b> Triggers switchover based on the operational status of a specific process or service running on the server.</li> <li>• <b>Device Status:</b> Triggers switchover based on the connectivity status of a selected device associated with a connector.</li> </ul>	Ping
<b>Type = Ping</b>		
<b>IP address</b>	IP address of the target machine or device.	1.1.1.1
<b>Retry Number</b>	Number of ping operation attempts before the target is considered unavailable.	3
<b>Period (ms)</b>	Interval between successive ping attempts.	5000
<b>Timeout (ms)</b>	Maximum wait time for a response before a ping attempt fails.	5000

<b>Expected Result</b>	<p><b>Reachable:</b> Target machine or device responds to ping requests, indicating it is online and accessible over the network.</p> <p><b>Not Reachable:</b> Target machine or device does not respond to ping requests, suggesting it may be offline, disconnected, or blocking the request.</p>	Not Reachable
<b>Type = Tcping</b>		
<b>IP address</b>	IP address of the target machine or device.	1.1.1.1
<b>Port</b>	TCP port to be tested.	31001
<b>Retry Number</b>	Number of ping operation attempts before the target is considered unavailable.	3
<b>Period (ms)</b>	Interval between successive ping attempts.	5000
<b>Timeout (ms)</b>	Maximum wait time for a response before a ping attempt fails.	5000
<b>Expected Result</b>	<p><b>Port is Open:</b> Connection to the specified port was successful, indicating that the port is open, and the service is reachable.</p> <p><b>No Response:</b> Connection attempt to the specified port failed, indicating that the port is closed or not responding.</p>	No Response
<b>Type = Process Monitor</b>		

<b>Process Name</b>	Name of the process or service to monitor.	
<b>Expected Result</b>	<p><b>Started:</b> Process is running and active on the system, indicating that the process is successfully started.</p> <p><b>Stopped:</b> Process is not running or has been terminated, which suggests that the process has either stopped unexpectedly or has never been started.</p>	Stopped
<b>Type = Device Status</b>		
<b>Node</b>	Specifies whether the monitored device belongs to the <b>Primary</b> or <b>Secondary</b> node.	Primary
<b>Connector</b>	Connector that contains the device.	
<b>Device</b>	Device to be monitored.	
<b>Retry Number</b>	Number of times the system will attempt to check the device connectivity before considering it as permanently down.	3
<b>Period (ms)</b>	Interval between connectivity checks.	5000
<b>Timeout (ms)</b>	Maximum wait time for a response before the attempt fails.	5000
<b>Expected Result</b>	<p><b>Connected:</b> Device is operational.</p> <p><b>Not Connected:</b> Device is not connected or not functioning, suggesting that it is unreachable or</p>	Not Connected

	offline.	
--	----------	--

**Table 2: Extend Switchover Logic - New Rule Configuration Parameters**

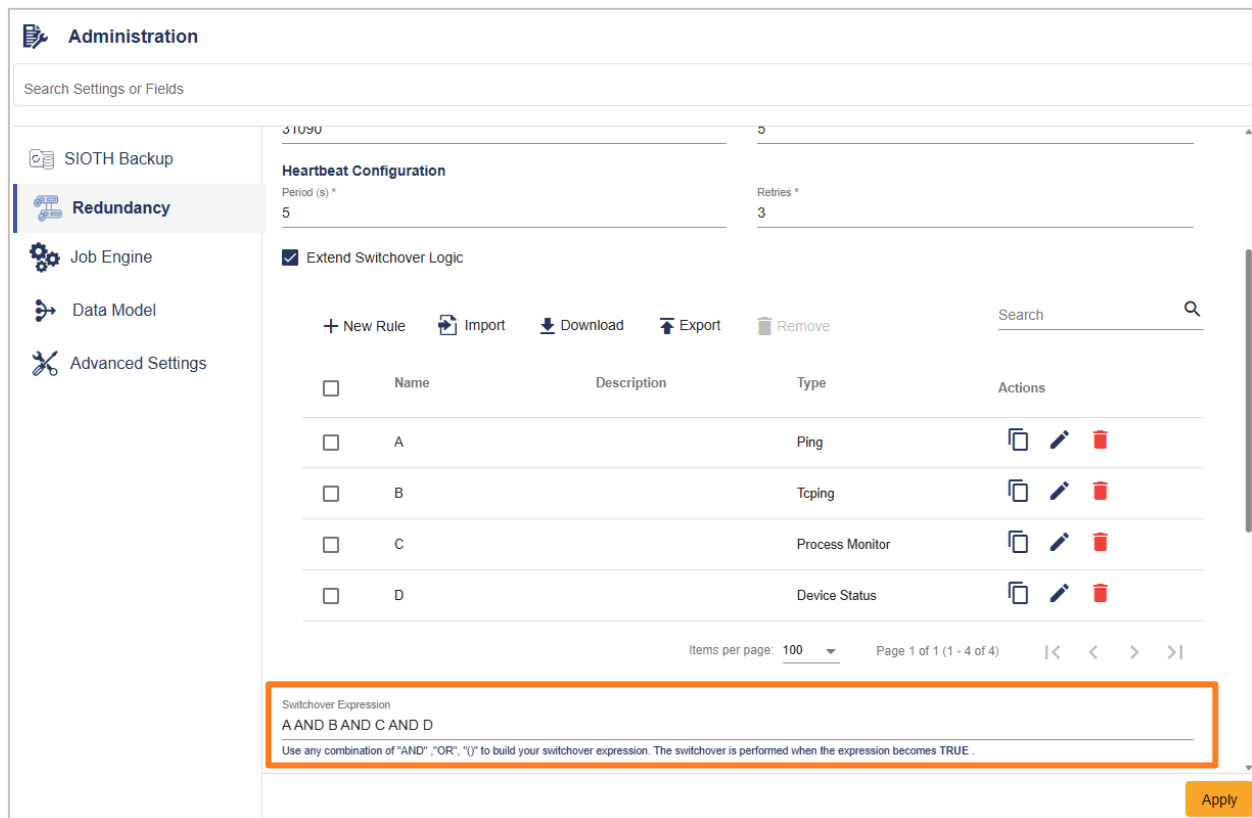
After defining the individual rules, the overall redundancy logic can be configured using the **Switchover Expression** field. Rules can be combined using logical operators such as **AND**, **OR**, and parentheses ( ) to define complex switchover conditions.

When the switchover expression is evaluated to **TRUE**, the system automatically initiates a switchover from the Primary server to the Secondary server.

This flexible mechanism allows redundancy behavior to be precisely tailored to the operational requirements and complexity of the deployment, ensuring high availability and uninterrupted operation of critical workflows.

#### **Example:**

In the figure below, a switchover is triggered when the expression **A AND B AND C AND D** evaluates to **TRUE**.



**Administration**

Search Settings or Fields

SIOth Backup

**Redundancy**

Job Engine

Data Model

Advanced Settings

Heartbeat Configuration

Period (s) \*  
5

Retries \*  
3

☒ Extend Switchover Logic

+ New Rule Import Download Export Remove

Search

Name	Description	Type	Actions
A		Ping	
B		Tcping	
C		Process Monitor	
D		Device Status	

Items per page: 100 Page 1 of 1 (1 - 4 of 4)

Switchover Expression  
A AND B AND C AND D  
Use any combination of "AND", "OR", "()" to build your switchover expression. The switchover is performed when the expression becomes TRUE.

Apply

**Figure 15: Switchover Expression**

## 4.8. Configure the Exclude from Redundancy

The **Exclude from Redundancy** option is available only in **Cold Redundancy** mode and allows specific services or connectors on the Secondary server to remain active during a switchover.

Enable the **Exclude from Redundancy**. A list of available services is displayed, allowing you to filter entries by **Connector Name**, **Project**, **Dataflow**, **Connector Type**, **Category**, and **Node**. Using these filters, you can select the services that should continue running on both the Primary and Secondary servers during redundancy operations.

This configuration is useful in scenarios where certain connectors must maintain continuous connectivity, regardless of which server is active.



Administration

Search Settings or Fields

SIOTH Backup

**Redundancy**

Job Engine

Data Model

Advanced Settings

On

Failover Mode \*  
Cold

SIOTH Redundant Machines

Primary \*  
192.168.1.50

Secondary \*  
192.168.1.51

Redundancy Manager Configuration

Port \*  
31090

Timeout (s) \*  
5

Heartbeat Configuration

Period (s) \*  
5

Retries \*  
3

☐ Extend Switchover Logic

☒ **Exclude from Redundancy**

Select the SIOTH services to be excluded from the redundancy management. The selected services will be available all the time in both primary and backup machines.

☐ Connector Name

☐ Project

☐ Dataflow

☐ Type

☐ Category

☐ Node

☐ OPCDA\_Connector\_0

Project\_1

Dataflow\_1

OPCDA

Source

SIOTHMasterNode

☐ OPCUASERVER\_6

Project\_1

Dataflow\_1

OPCUASERVER

Destination

SIOTHMasterNode

Apply

**Figure 16: Exclude from Redundancy Option**

In the figure below, the **OPC UA Server** connector is excluded from redundancy, ensuring that it remains operational on both servers.

Administration

Search Settings or Fields

SIOTH Backup

**Redundancy**

Job Engine

Data Model

Advanced Settings

On

Failover Mode \*  
Cold

SIOTH Redundant Machines

Primary \*  
192.168.1.50

Secondary \*  
192.168.1.51

Redundancy Manager Configuration

Port \*  
31090

Timeout (s) \*  
5

Heartbeat Configuration

Period (s) \*  
5

Retries \*  
3

☐ Extend Switchover Logic

☒ **Exclude from Redundancy**

Select the SIOTH services to be excluded from the redundancy management. The selected services will be available all the time in both primary and backup machines.

☒ Connector Name

☐ Project

☐ Dataflow

☐ Type

☐ Category

☐ Node

☒ OPCUASERVER\_6

Project\_1

Dataflow\_1

OPCUASERVER

Destination

SIOTHMasterNode

☐ OPCDA\_Connector\_0

Project\_1

Dataflow\_1

OPCDA

Source

SIOTHMasterNode

Apply

**Figure 17: Exclude OPC UA server from Redundancy Example**

## 5. Best Practices

Follow the recommendations below to ensure a stable and reliable redundancy setup:

- Perform a **fresh installation** on the Secondary (backup) node. Enabling redundancy will overwrite its existing configuration; therefore, ensure it does not contain any critical data before proceeding.
- Ensure that **all system-level configurations** are consistent on both nodes. For example, OPC UA endpoints and database connections must use addresses that are reachable from both servers.
- **Disable Automatic Synchronization** while configuring or updating node settings to prevent excessive communication between the two redundant servers during configuration changes.
- Maintain **identical configurations** on both nodes, including projects, system settings, and network parameters (such as Primary and Secondary IP addresses).
- Before enabling redundancy from the user interface, verify that the Redundancy Manager service is enabled and running on both the Primary and Secondary servers.
- After enabling redundancy, perform a **Manual Synchronization** to replicate all configurations from the Primary server to the Secondary server.
- After any synchronization (automatic or manual), **verify that all configurations** applied on the Primary server are correctly reflected on the Secondary server.
- Use the **Exclude from Redundancy** option to keep selected connectors active on both nodes when required in **Cold Redundancy** mode.
- Do **not enable redundancy** on the Secondary server before it is enabled on the Primary server once configurations are finalized.

### (!) Note

Failure to follow the above best practices may result in incomplete synchronization, potential configuration loss, and increased switchover time between the Primary and Secondary servers.

For additional information on this guide, questions or problems to report, please contact:

**Offices**

- Americas: +1 713 609 9208
- Europe-Africa-Middle East: +216 71 195 360

**Email**

- Support Services: [customerservice@integrationobjects.com](mailto:customerservice@integrationobjects.com)
- Sales: [sales@integrationobjects.com](mailto:sales@integrationobjects.com)

To find out how you can benefit from other Integration Objects' products and services, please visit our website:

**Online**

- [www.integrationobjects.com](http://www.integrationobjects.com)