

---

# SIFWorks® ZIS™ Enterprise Integration Guide

Version 3.5

January 2011

The Pearson logo consists of a dark blue rectangular box with the word "PEARSON" written in white, uppercase, sans-serif font in the center.

Data Solutions  
9815 S. Monroe St.,  
Ste. 400  
Sandy, UT 84070  
1.877.790.1261

[www.pearsondatasolutions.com](http://www.pearsondatasolutions.com)

*Copyright © 2011 Pearson Education, Inc. All rights reserved.  
This document is provided to Data Solutions customers and partners and may not be reproduced—in part or whole—in any form without the express written permission of NCS Pearson, Inc. Information provided herein is subject to change without notice.  
SIFWorks and Data Solutions are registered trademarks of NCS Pearson, Inc.  
SIF and Schools Interoperability Framework are registered trademarks of the Schools Interoperability Framework Association.  
All other trademarks mentioned herein are the property of their respective owners.*

# Contents

<b>Contents .....</b>	<b>3</b>
<b>Part I .....</b>	<b>5</b>
<b>1. About This Guide .....</b>	<b>5</b>
Purpose .....	5
Overview .....	5
Rule Sets .....	5
Workflow Editor.....	5
User Management.....	5
<b>2. Companion Documents .....</b>	<b>5</b>
SIFWorks ZIS Administration Guide.....	5
SIFWorks ZIS Installation Guide.....	6
<b>Part II.....</b>	<b>7</b>
<b>3. Introduction to Rule Sets and Workflows.....</b>	<b>7</b>
<b>4. Rule Sets .....</b>	<b>7</b>
Rule Set Importing/Exporting.....	8
SIFWorks ZIS Rule Set Editor .....	8
Basic Rule Sets.....	8
Advanced Rule Sets.....	9
Conditions .....	9
Life Cycle Event is (Advanced Rule Sets Only) .....	9
Message Type Is .....	9
Event Type Is .....	10
ObjectName Is.....	10
DestinationId Is .....	10
SourceId Is.....	10
SIF Version Is .....	10
XPath Expression .....	10
Actions .....	10
Log.....	11
Delete Message .....	11
Hold Message .....	11
Reject Message.....	11
Remove Elements.....	11
Replace Element Values .....	11
XSL Transform.....	11
Log Message Properties.....	12
<b>Part III .....</b>	<b>13</b>
<b>5. Workflows .....</b>	<b>13</b>
SIFWorks ZIS Workflow Editor.....	13
Enterprise Workflow.....	13

Zone Template Workflow .....	13
Zone Workflow .....	14
<b>6. XPath and XSLT Examples .....</b>	<b>14</b>
Working with XPath and XLST .....	14
XPath Examples .....	14
XSLT Examples .....	15
<b>Part IV.....</b>	<b>18</b>
<b>7. User Management Overview .....</b>	<b>18</b>
Background .....	18
Configuration (the “conf” directory) .....	19
Permissions.....	20
Security (User) Groups .....	22
Users.....	23
<b>8. External LDAP Mode .....</b>	<b>23</b>
Apache Directory Studio Setup .....	23
Directory Service Configuration.....	25
ZIS “External LDAP” Configuration .....	25
External LDAP Configuration Fields.....	27
<b>Part V .....</b>	<b>29</b>
<b>9. SIF Messaging Version Translation .....</b>	<b>29</b>
Translation Engine.....	30
Valueset Tables .....	30
Field Rules .....	31
<b>Part VI.....</b>	<b>33</b>
<b>10. Contacting Data Solutions .....</b>	<b>Error! Bookmark not defined.</b>
Support for SIFWorks ZIS .....	<b>Error! Bookmark not defined.</b>
Telephone Support.....	<b>Error! Bookmark not defined.</b>
On-Line Customer Support Center.....	<b>Error! Bookmark not defined.</b>
Remote Access .....	<b>Error! Bookmark not defined.</b>
On-Site Support Service .....	<b>Error! Bookmark not defined.</b>

# Part I

---

## INTRODUCTION

---

# 1. About This Guide

## Purpose

The SIFWorks ZIS Integration Guide provides a detailed and technical treatment of Rule Sets (for filtering or transforming messages), Workflow (the application of Rule Sets to zones and agents in order to modify the ways in which the ZIS handles messages), and User Management.

## Overview

### Rule Sets

Explains how Rules and Rule Sets are built, and how they influence the Workflow.

### Workflow Editor

Describes the function of the Workflow Editor in building and editing Rule Sets to manage and optimize message and data flow through the ZIS.

### User Management

Describes and the creation and management of user accounts, including security groups and permissions. Instruction for configuring External LDAP user account sources is also provided.

# 2. Companion Documents

## SIFWorks ZIS Administration Guide

The Administration Guide is intended for IT professionals tasked with managing a school or district SIF information system infrastructure (end users). The Administration Guide provides an introduction to SIF and the SIFWorks ZIS, as well as steps for installing and configuring the ZIS. Creation and management of

Zones (including templates and default settings) are also provided, along with steps for establishing Transports settings, User Accounts, and Logging Settings.

## **SIFWorks ZIS Installation Guide**

This Guide is intended for end users, and provides basic steps for installing and starting the ZIS.

# Part II

## 3. Introduction to Rule Sets and Workflows

SIFWorks ZIS Enterprise Edition supports validating, filtering and transforming SIF\_Request, SIF\_Response and SIF\_Event messages at defined points in the message lifecycle within the SIFWorks ZIS.

Message workflows exist at the enterprise and zone levels, and include zero or more rule sets. Workflows only see SIF\_Event, SIF\_Request and SIF\_Response messages as they pass through the SIFWorks ZIS.

The SIFWorks ZIS routes messages normally if a zone workflow has no rule sets. A zone workflow with one or more rule sets may validate, filter or transform messages. The end result of any message transformation must be a valid SIF message.

Workflows and rule sets allow a SIFWorks ZIS administrator to repair SIF messages sent by abnormally behaving agents, prevent destination agents from seeing specific messages, modify SIF response messages and perform detailed message tracing.

## 4. Rule Sets

A SIFWorks Rule Set is a set of one or more rules. Each rule has a list of conditions and actions. You can navigate to the Rule Sets screen using either of the following paths.

- SIFWorks ZIS > Server Settings > Rule Sets
- SIFWorks ZIS > MyEnterprise > Enterprise Settings > Rule Sets

Conditions are checked to determine if a rule's actions should be executed. A single condition may have a "true" or "false" result. The results from a rule's conditions are checked against the "perform actions when" option which may be one of "all conditions are true," "any condition is true," or "all conditions are false" options. The final result from "perform actions when" condition collation determines if a rule's actions should be executed.

When a rule's condition collation determines that the rule's actions should execute, each action is then executed in order. Each action has one or more properties that may be set to customize the action's log entry or control the behavior of the action. The basic actions that are provided in SIFWorks are "Reject," "Delete," "Hold," "Remove Elements," "Log," "Replace Element Values," and "XSL Transform" may be available in the SIFWorks ZIS Enterprise Edition Rule Set Editor.

Each rule set should be authored to not rely on the behavior of another rule set. Authoring rule sets to be self-contained allows them to be combined into Workflows without risking unexpected behavior due to interdependencies.

## Rule Set Importing/Exporting

SIFWorks ZIS Enterprise Edition offers Rule Set importing and exporting. This feature may be used to export a rule set from a test ZIS and then import it into a production ZIS. Rule sets may be exported to a file and emailed to support personnel for debugging. Common rule sets may be maintained by Data Solutions support and made available for importing.

A ZIS administrator with access to the install directory of the ZIS may copy rule set files directly into the "workflows/rules" directory and then restart the ZIS. The copied rules will be shown in the enterprise "Rule Sets" node after the ZIS restarts.

## SIFWorks ZIS Rule Set Editor

Rule Sets may be created using the SIFWorks ZIS Enterprise Edition Rule Set Editor. The rule set editor provides a graphical user interface for quickly constructing rule sets and using them immediately in a Workflow.

The rule set editor expects that an author is familiar with SIF messaging, XPath and XSLT technologies. The rule set editor does not provide a mechanism for testing rule sets, so each XPath and XSLT should be tested against a valid SIF message using an appropriate tool.

## Basic Rule Sets

Basic rule sets include rule actions that are only performed on the Message Inbound and Message Ready To Process message lifecycle events. Within a rule set, any rule that contains a Reject Message action is run on the Message Inbound event, and all other rules are run on the Message Ready To Process event. In

basic rule sets only the existence of the Reject Message action determines when a rule is run – the conditions do not affect this behavior.

The default behavior of the ZIS rule set editor is to only allow editing of basic rule sets, but does support viewing of advanced rule sets.

## Advanced Rule Sets

Advanced rule sets are identified by the existence of the “Life Cycle Event is” condition in rules. This additional condition may be used to control when a rule is run by specifying a ZIS message lifecycle event. Knowledge of the ZIS message lifecycle is necessary to take advantage of this feature.

The ZIS rule set editor supports editing advanced rule sets, but must be manually enabled.

## Conditions

SIFWorks ZIS Enterprise Edition supports a pre-defined set of conditions. Note that when there are multiple conditions in a rule that the “perform actions when” condition collation should be used to determine how the condition results are evaluated for rule action execution.

### Life Cycle Event is (Advanced Rule Sets Only)

This condition is only available when the ZIS is started with the “zis.ruleset.lifecycle” property. This condition is not available to customers, and should only be used internally within Data Solutions. See the “Message Workflow Events” section for details regarding each event type. The options for this condition are:

- Inbound
- Rejected
- Accepted
- Ready To Transform
- Outbound
- Delivered
- Not Delivered
- Deleted

### Message Type Is

This condition may be used to select a specific SIF message type. When the selected option is “SIF Response,” the condition applies to all response packets that are part of the response message. The options for this condition are:

- SIF Event
- SIF Request
- SIF Response

### **Event Type Is**

This condition must be used with the “Message Type is” condition, and may be used to specify which SIF\_Event type to select for the rule. The options for this condition are:

- Add
- Change
- Delete

### **ObjectName Is**

This condition may be used to select a specific event, request or response based on the ObjectName in the SIF message. This condition handles the ObjectName differences between each of the message types. The author must enter a valid SIF data object name.

### **DestinationId Is**

This condition may be used to select a message based on the destination agent of the SIF message. Note that the destination ID of the message is not valid until the message enters the agent’s queue. The exception to this case is when a SIF message is targeted to a specific agent. The author must enter a valid agent ID.

### **SourceId Is**

This condition may be used to select a message based on the source agent of the SIF message. The author must enter a valid agent ID.

### **SIF Version Is**

This condition may be used to select a message based on a specific SIF version of the message. This condition should be used in a rule set when the actions taken are different for different versions of SIF messages. The author must enter a valid SIF version.

### **XPath Expression**

This condition allows an author to use an XPath expression on the raw SIF message XML to select the message. The XPath expression must return a Boolean value, and should be tested against a valid SIF message using an external tool. See the “XPath Examples” section for details about using an XPath expression as a condition.

## **Actions**

After a rule’s conditions are tested, the rule’s actions may be executed. The rules are executed in sequence.

Actions that successfully transform the SIF message will cause subsequent transformation actions to operate on the transformed message. Care must be taken when performing multiple message transformations in a rule set or

workflow to not introduce message format dependencies in the later transformations.

## **Log**

This action creates a log entry in the zone's log. The rule author may enter any descriptive log message. This action does not create a SIF\_LogEntry event. Note that other actions may include a log message as part of the action's options. Log messages may include properties that are replaced before the log entry is created. See the "Log Message Properties" section for a detailed discussion of this feature.

## **Delete Message**

This action deletes a SIF message from an agent's queue, or discards a message before it is entered into a queue. All deleted messages trigger the "Message Deleted" message lifecycle event. The rule author may enter a log message with this action.

## **Hold Message**

This action holds a message in an agent's queue. Held messages must be specifically released or deleted from the queue by an administrator. The rule author may enter a log message with this action.

## **Reject Message**

This action rejects an inbound message. Rejected messages trigger the "Message Rejected" lifecycle event. The rule author may enter a log message with this action.

## **Remove Elements**

This action uses an XPath expression to remove elements from a SIF message. This action transforms the message. See the Examples section for practical XPath expressions that may be used with this action.

## **Replace Element Values**

This action uses an XPath expression to select a set of XML nodes and replace their text values. This action transforms the message. See the Examples section for practical XPath expressions that may be used with this action.

## **XSL Transform**

This action uses an XSL Transformation XML to transform the message. The XSLT transformation needs to produce a valid SIF message. See the Examples section for details on XSLT identity transformations.

## Log Message Properties

Log messages may include property value replacement strings. This feature may be used to produce specific formatting in the zone's log file to assist with debugging rule sets, or to analyze the behavior of the ZIS through the zone's log.

Replacement String	Property Value
<code>\${actionName}</code>	The name of the current rule action being executed. The action name is defined by the rule's author.
<code>\${authenticationLevel}</code>	SIF_AuthenticationLevel of the message. Value may be "0," "1," "2," or "3."
<code>\${destinationId}</code>	The ID of the agent that will receive the message. The agent's destination ID must exist in the zone's agent registration records in order for the message to be accepted by the ZIS.
<code>\${encryptionLevel}</code>	SIF_EncryptionLevel of the message. Value may be "0," "1," "2," "3," or "4."
<code>\${lifeCycleEvent}</code>	The name of the ZIS message lifecycle event being handled.
<code>\${messageId}</code>	The SIF message ID of the message being handled.
<code>\${messageType}</code>	SIF type of message being handled. Value may be "SIF_Event," "SIF_Request," or "SIF_Response."
<code>\${ruleName}</code>	The name of the current rule being executed. The rule name is defined by the rule's author.
<code>\${ruleSetName}</code>	The name of the current rule set being executed. The rule set name is defined by the rule's author.
<code>\${version}</code>	The SIF message version of the message being handled.
<code>\${zoneId}</code>	The ZIS zone ID that is managing the message being handled.

## 5. Workflows

A SIFWorks ZIS Workflow may consist of one or more rule sets. The rule sets in a workflow are executed in sequence. A rule set must be added to a workflow for that rule set to be executed. A rule set may be added to more than one workflow.

### **SIFWorks ZIS Workflow Editor**

The SIFWorks ZIS Enterprise Edition Workflow Editor is used to set up workflows. Rule sets may be added to or removed from a workflow. A rule set is only executed when it is part of a workflow.

The SIFWorks ZIS Enterprise Edition defines three types of workflows: enterprise, zone template and zone workflows. Each workflow type has the same basic behavior—that it executes a list of rule sets in sequence.

### **Enterprise Workflow**

The enterprise workflow defines a list of rules that may be executed before and after the zones' workflow. The enterprise workflow will always be wrapped around a zone workflow before the zone workflow is executed. The enterprise workflow may be used to perform any set of actions consistently across all zones within the enterprise.

### **Zone Template Workflow**

The zone template workflow defines the default workflow for all zones that are created from the zone template. When the zone template workflow changes, all zones that are based on that zone template will see the workflow changes. A zone may override the zone template workflow and use a zone-specific workflow.

The zone template workflow will display any enterprise workflow rule sets as non-editable rule sets before and after the zone template workflow rule sets.

## Zone Workflow

The zone workflow will only be used if a zone administrator specifically changes the “Use Zone Template Workflow” setting in the zone workflow editor. Once an administrator has changed the zone template workflow setting, the administrator may create a workflow that is specific to the zone. An administrator always has the option of changing the “Use Zone Template Workflow” setting back to its original value (to use the zone template workflow).

The zone workflow will display any enterprise workflow rule sets as non-editable rule sets before and after the zone workflow rule sets.

# 6. XPath and XSLT Examples

## Working with XPath and XSLT

Many tools exist for working with XML, XPath and XSLT files. Commercial tools include features like XSLT debuggers and XPath expression builders, but may cost up to several hundred dollars per license. Free tools lack many features.

The recommended tool for XPath and XSLT development and testing is oXygen XML Editor Professional Edition, which runs on Windows and Mac OS X, and includes full syntax highlighting, a complete visual XPath expression builder, and XSLT debugger.

## XPath Examples

XPath expressions may be used in rule conditions and actions. The key to XPath expression nirvana is to use a valid SIF message, an XPath reference and an XPath expression execution tool for development and testing.

**Note that XPath expression execution in the SIFWorks ZIS ignores XML namespaces. This requires removal of the default XML namespace (xmlns=“...”) from every SIF message used for XPath expression development.**

The first several examples demonstrate an XPath expression when used as a rule condition. An XPath expression condition must return a Boolean value.

The first example returns “true” when the SIF message is the first response packet. Do not use this condition in conjunction with a Delete Message action, as it will create a packet order error condition.

```
compare(//SIF_Response/SIF_PacketNumber/text(), '1') = 0
```

The next example will return “true” when OtherId elements of Type “0495” exist in the OtherIdList. Note that only one OtherId element in the whole response packet has to have Type “0495” for this expression to be “true.”

```
exists(//OtherIdList/OtherId[@Type='0495'])
```

The following example is similar to the above example, but uses the “count” function to compare the number of matching elements against another number—in this case “0.” The number “0” could be replaced with another count (of the number of StudentPersonal elements).

```
count(//OtherIdList/OtherId[@Type='0495']) > 0
```

This next example may be used with the “Remove Elements” action to remove the Demographics node from all StudentPersonal records. This same behavior may also be accomplished with an XSLT as shown in the next section.

```
//StudentPersonal/Demographics
```

When used with the “Remove Elements” action, the following XPath expression will remove all OtherId elements where the Type attribute is “0004”.

```
//StudentPersonal/OtherIdList/OtherId[@Type='0004']
```

The above XPath expression may be used with the “Replace Element Values” action to replace all students’ SSN values with “000-00-0000,” if subsequent processing or reporting requires a SSN value to be present.

## XSLT Examples

The most common XSL transform that will be used is the XSL identity transform with modifications. Any good XSLT reference or cookbook will include a more detailed description of the XSL identity transform than is provided in this document.

**Note that the XSL transformation engine in the SIFWorks ZIS ignores XML namespaces. This may require removal of the default XML namespace (xmlns=“..”) from every SIF message used for XSL transform development.**

The base XSL identity transform for SIF messages is as follows:

```
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" encoding="UTF-8" standalone="yes" />
  <xsl:template match="node() | @*">
    <xsl:copy>
      <xsl:apply-templates select="@* | node()" />
    </xsl:copy>
  </xsl:template>
</xsl:stylesheet>
```

The identity transform presented above reproduces its input as the output of the transform. The “@\*” matches all attributes and the “node ()” matches all elements.

The following XSLT example has the same output as one of the previous XPath expression examples when used in a “Replace Elements” action. The XSLT, however, will be more efficient and easier to maintain if many elements are being removed from the SIF message.

```
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" encoding="UTF-8" standalone="yes" />
  <xsl:template match="node() | @*">
    <xsl:copy>
      <xsl:apply-templates select="@* | node()" />
    </xsl:copy>
  </xsl:template>
  <xsl:template match="Demographics" />
</xsl:stylesheet>
```

To remove additional elements in each StudentPersonal record, the above XSLT may be modified as follows:

```
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" encoding="UTF-8" standalone="yes" />
  <xsl:template match="node() | @*">
    <xsl:copy>
      <xsl:apply-templates select="@* | node()" />
    </xsl:copy>
  </xsl:template>
  <xsl:template match="Demographics" />
  <xsl:template match="AddressList" />
  <xsl:template match="PhoneNumberList" />
  <xsl:template match="EmailList" />
</xsl:stylesheet>
```

Where the previous few examples strip elements using an empty template, the following example explicitly includes specific elements.

```
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" encoding="UTF-8" standalone="yes" />
  <xsl:template match="node() | @*">
    <xsl:copy>
      <xsl:apply-templates select="@* | node()" />
    </xsl:copy>
  </xsl:template>
  <xsl:template match="//StudentPersonal">
    <xsl:copy>
      <xsl:apply-templates select="./LocalId | ./StateProvinceId | ./OtherIdList | ./Name" />
    </xsl:copy>
  </xsl:template>
</xsl:stylesheet>
```

In addition to removing elements, an XSLT may be used to replace element values. The following example replaces all StateProvince element values with "NV".

```
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" encoding="UTF-8" standalone="yes" />
  <xsl:template match="node() | @*">
    <xsl:copy>
      <xsl:apply-templates select="@* | node()" />
    </xsl:copy>
  </xsl:template>
  <xsl:template match="//Address/City" priority="1">
    <City><xsl:value-of select="."/;></City>
    <StateProvince>NV</StateProvince>
  </xsl:template>
  <xsl:template match="//Address/StateProvince" priority="0" />
</xsl:stylesheet>
```

## 7. User Management Overview

### Background

SIFWorks ZIS Enterprise Edition supports fine-grained administration of ZIS resources using security groups and permissions. A permission grants access (“View” or “Modify”) to a specific ZIS resource. One or more permissions may be assigned to a security group, and one or more groups may be assigned to a ZIS user account.

The default behavior of the ZIS is to store users and security groups in local XML files in the “conf” directory. The ZIS may also be configured to use an LDAP directory service for authentication of users. When user management is configured for “External LDAP” mode, all users are maintained and administered on the LDAP directory. When the ZIS is in “External LDAP” mode, LDAP groups or LDAP user account attributes must be mapped to ZIS local security groups.

## Configuration (the “conf” directory)

The ZIS “conf” directory contains all user management configuration and data files. The following list describes the behavior and contents of each file. These files are managed by the ZIS and should not be manually edited.

Configuration File	Behavior
<b>user_conf.xml</b>	Stores the “Local File” or “External LDAP” configuration that is loaded by the ZIS at startup. Any change to the user management configuration through the ZIS administration console does not require a restart of the ZIS. Removing this file will cause the ZIS to write the default “Local File” configuration on startup.
<b>user_super.xml</b>	Stores the super-user account information. The super-user account login is “sifworks”, and may never be changed. Removing this file will cause the ZIS to prompt for setting the super-user account password when the administration console is opened. An administrator may control this reset behavior by making the file read-only using the operating system’s file access controls.
<b>user_users.xml</b>	Stores user account information when the ZIS user management is configured for “Local File” mode. This file is not used in “External LDAP” mode.
<b>user_attributes.xml</b>	Stores user account local attribute information when the ZIS user management is configured for “External LDAP” mode. This file is not used in “Local File” mode.
<b>user_roles.xml</b>	Stores ZIS security groups for both modes. Each security group contains one or more permissions. When ZIS user management is configured for “External LDAP” mode, mappings must be setup between LDAP group or user account attributes and ZIS local security groups.
<b>user_other.properties</b>	Stores last login time for each user.

## Permissions

Permissions are constructed by the ZIS during startup. The default set of ZIS permissions includes access to server and enterprise level resources, and are always present in permissions lists. Zone permissions are created at startup, and then created and destroyed as ZIS zones are created and destroyed.

Zone permissions are presented in the administration console with a tree table widget instead of a flat list. The zone permissions tree table mirrors the zone group hierarchy.

The following list is a description of the permissions available to an administrator when creating a security group.

Permission	View	Modify
<b>Server Certificates</b>	Permits viewing the list of server and trusted agent certificates. Also permits download of certificates to local computer.	Permits creation and deletion of certificates. Also permits upload of trusted agent certificates. Implies "Server Certificates View" permission.
<b>Server Settings</b>	Permits viewing of general ZIS server settings including "Console," "Transports," "Software Updates," and "Logging." Access to other ZIS resources requires a resource specific permission.	Permits modification of general ZIS server settings including "Console," "Transports," "Software Updates," and "Logging." Implies "Server Settings View" permission. Access to other ZIS resources requires a resource specific permission.
<b>Enterprise User Groups</b>	Permits viewing the list of ZIS Enterprise User Groups and each Group's settings.	Permits creation and deletion of ZIS Enterprise User Groups, and modification of existing User Group settings. Implies "Enterprise User Groups View" permission.
<b>Enterprise Users</b>	Permits viewing the list of ZIS Users and each User's settings.	Permits creation and deletion of ZIS Users, and modification of existing User settings. Implies "Enterprise Users View" permission.
<p><b>Note:</b> Enterprise Users also have "Reset User Password" permissions.</p>		
<b>Enterprise Workflow</b>	Permits viewing Enterprise Workflow and Enterprise Rule Sets.	Permits modification of the Enterprise Workflow and Enterprise Rule Sets. Implies the "Enterprise Workflow View" permission.

<b>Enterprise Zones</b>	Permits viewing the list of ZIS enterprise zones. Zone groups are always visible, as they have no permissions associated with them.	Permits creation and deletion of ZIS zones. Also permits modification of Zone Templates. Implies “Enterprise Zones View” permission.
<b>Enterprise Any Zone</b>	Permits the viewing of any enterprise zone and zone agent.	Permits modification of any existing ZIS zone. Implies “Enterprise Any Zone View” Permission. Includes permission to edit zone template workflow. <b>Does not imply creation and deletion of Zones.</b>
<b>Enterprise Any Zone Agents</b>	n/a	Permits the creation, deletion and modification of zone agents.
<b>Zone &lt;zoneId&gt;</b>	Similar to “Any Zone View” permission except that it only applies to a specific zone referenced by <zoneId>. Dynamically created and deleted.	Similar to “Any Zone Modify” permission except that it only applies to a specific zone referenced by <zoneId>. Includes permission to edit zone workflow. Dynamically created and deleted.
<b>Zone &lt;zoneId&gt; Agents</b>	n/a	Similar to “Enterprise Any Zone Agents Modify” Permission except that it only applies to a specific zone referenced by <zoneId>. Permits modification of agent settings and queues, but not adding or deleting zone agents. Dynamically created and deleted.

## Security (User) Groups

An administrator creates a security group by selecting one or more permissions, and providing a unique Group name. A description may also be added to a group to document the purpose of the group.

Four default security groups are created and maintained by the ZIS: “Server Administrator,” “Server Operator,” “Zone Administrator,” and “Zone Operator.” The permissions included in each default security group are listed below.

Group	Permissions
Server Administrator	Server Settings Modify Server Certificates Modify Enterprise Users Reset Passwords Enterprise Users Modify Enterprise User Groups Modify Enterprise Workflow Modify Enterprise Zones Modify Enterprise Any Zone Modify Enterprise Any Zone Agents Modify
Server Operator	Server Settings View Enterprise Users View Enterprise User Groups View Enterprise Workflow Modify Enterprise Zones Modify Enterprise Any Zone Modify Enterprise Any Zone Agents Modify
Zone Administrator	Server Settings View Enterprise Workflow View Enterprise Zones Modify Enterprise Any Zone Modify Enterprise Any Zone Agents Modify
Zone Operator	Server Settings View Enterprise Workflow View Enterprise Any Zone View Enterprise Any Zone Agents Modify

Groups operate the same for “Local File” mode and “External LDAP” mode with the exception that a user may not be directly assigned to a group in “External LDAP” mode. In “External LDAP” mode an administrator must use the “Attribute to Group Mapping” and “Group to Group Mapping” in the ZIS administration console to create an association between some feature of LDAP and a local ZIS group. Group Mapping will be described in detail in the “External LDAP” section.

## Users

An administrator creates a User by providing the following information:

- Login Name (required)
- Password (required)
- Name
- Phone
- Email
- Groups (selected from a list)

Users may be assigned one or more groups, but any assigned Groups must exist before the user is created.

When user management is configured for “External LDAP” mode, Users may not be created or deleted. When viewing User settings in “External LDAP” mode, no modification may be made; presented Group membership is based on Group Mappings.

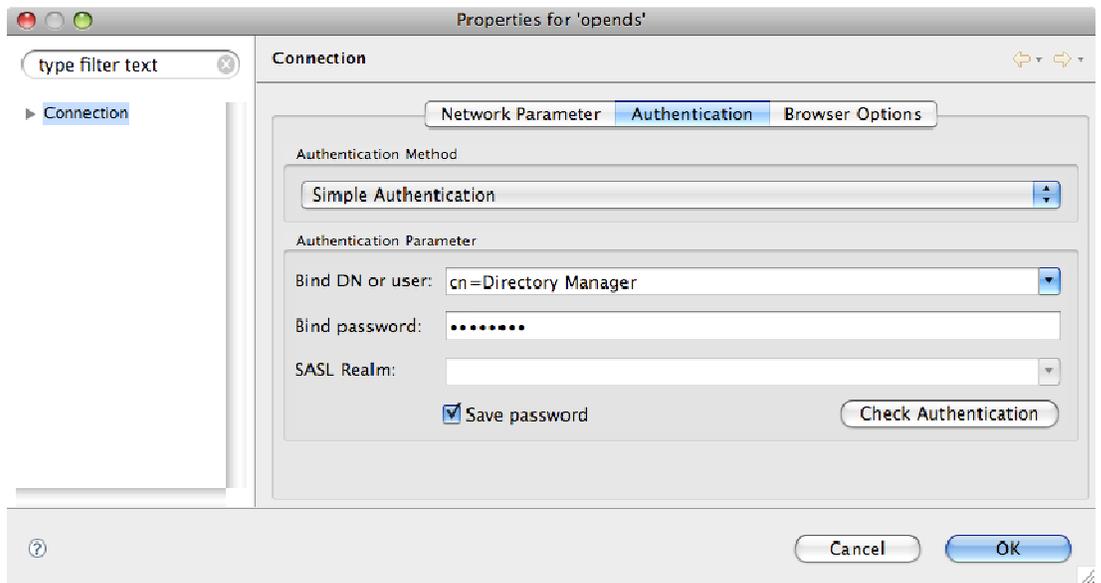
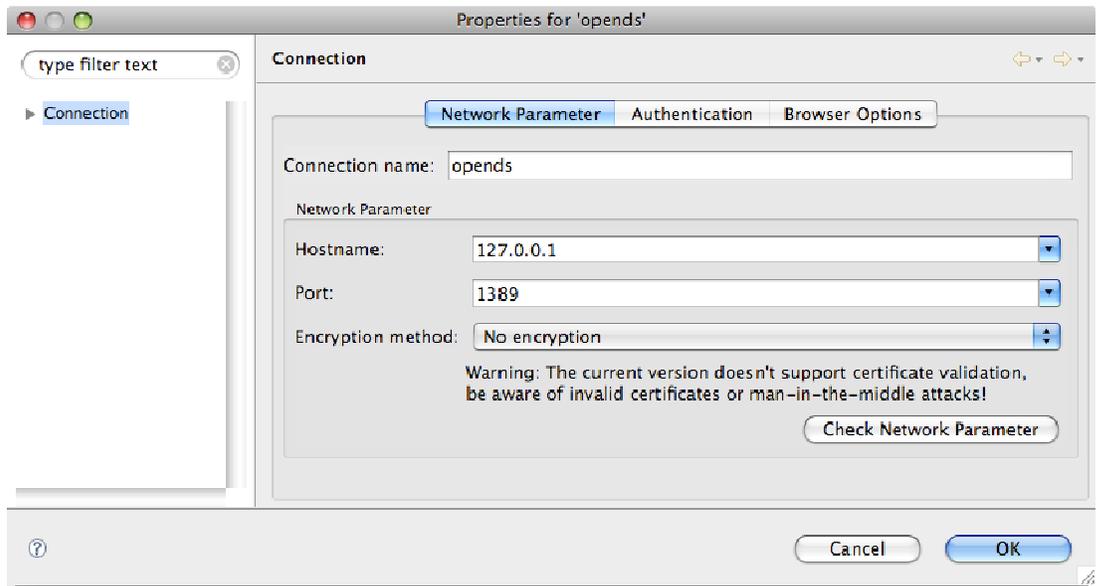
# 8. External LDAP Mode

“External LDAP” mode requires an LDAP directory service to perform authentication and mapping to local Groups. The following tool may be used to evaluate the behavior of LDAP-based authentication, and the steps required for o setup are provided below.

- <http://directory.apache.org/studio/>

## Apache Directory Studio Setup

Apache Directory Studio provides platform specific installers. Download the appropriate version for your ZIS server, and follow the instructions provided on the download page. Launch Apache Directory Studio and use the following dialogs to enter the connection and authentication information.



After using "Check Network Parameter" and "Check Authentication," click "OK." Double-click the connection to open it.

## Directory Service Configuration

To add a new User, right-click on "ou=People" and select "New Entry...". Select "Use existing entry as template" and click "Browse...". Select an existing User ("uid=user.0") and click "OK." Click "Next," and click "Next" again. Change the RDN to the login name of the new user (e.g. "jdoe") and click "Next." Double-click the "userPassword" attribute and enter a new plaintext password. Also change the CN (common name) and SN (surname) fields. Click "Finish."

Before creating Groups you should create a "Groups" organizational unit. Right-click on "dc=example,dc=com" and select "New Entry...". Select "Create entry from scratch" and click "Next". Select "organizationalUnit" from the available object classes and click "Add" and "Next". Select "ou" from the RDN drop-down , enter "Groups" and click "Next". Click "Finish."

To add a new Group, right-click on "ou=Groups" and select "New Entry...". Select "Create entry from scratch" and click "Next." Select "groupOfUniqueNames" from the available object classes and click "Add" and "Next." Select "cn" from the RDN drop-down, enter "ServerAdministrator" and click "Next." Click "Finish." Create additional Groups by replacing "ServerAdministrator" with your desired Group name.

To add a User to a Group, click on "cn=ServerAdministrator", right-click on the "Entry Editor" window and select "New Attribute...". Select "uniqueMember" from the drop-down box and click "Finish". In the "uniqueMember" attribute value field enter "uid=jdoe,ou=People,dc=example,dc=com" and press the Enter/Return key.

To use the copy/paste method of entering DNs first right-click on the node you wish to copy and select "Copy Entry / DN." Then, after adding a new "uniqueMember" attribute, right click on the attribute row and select "Edit Value With >> Text Editor" and paste the DN and click "OK."

To add users to a group, uncheck the "Hide existing attributes" box before selecting "uniqueMember." You will likely have to close the connection and re-open it to see group membership changes. (This appears to be a defect in Apache Directory Studio.)

After creating a User, Group and the association between the two, the directory service is ready for a simple "External LDAP" test.

## ZIS "External LDAP" Configuration

Configuring the ZIS user management for "External LDAP" will require the ZIS to be restarted one or more times. You may wish to start the ZIS from the console rather than run it as a service for this test. Also, the following configuration must initially be performed as the super-user "sifworks".

Click "My Enterprise >> Enterprise Settings >> Users & Groups >> Setup" to see the users setup page. Click the red "Settings" link under the "User & Group

Setup” title. Use the following screen capture for “External LDAP” configuration values.

The screenshot displays a configuration interface for External LDAP. It is organized into four sections:

- Account Source:** A dropdown menu is set to "External LDAP".
- LDAP Connection:** Fields include Address (127.0.0.1), Port (1389), Search User DN (cn=Directory Manager), and Search User Password (masked with asterisks). There is an unchecked checkbox for "Encrypted (StartTLS)".
- LDAP Configuration:** Fields include Profile (a dropdown menu with "<USE ONLY FOR INITIAL CONFIGURATION>" selected), Base DN (dc=example,dc=com), User Object (inetOrgPerson), User Identifier Attribute Name (uid), and Group Attribute Name (isMemberOf).
- Other Configuration:** A field for Local Correlation Attribute Name is set to entryUUID.

Click “Save,” and then click the red “Group to Group Mappings” link. Click “Add Mapping” and then copy the “ServerAdministrator” Group DN from Apache Directory Studio and paste it into the “LDAP Group DN” field in the ZIS administration console. Select “Server Administrator” from the “Local Group Name” drop-down box and click “Save.” The “ServerAdministrator” Group DN should look like “cn=ServerAdministrator,ou=Groups,dc=example,dc=com”.

Restart the ZIS. Any changes to account management configuration and Group Mappings require a ZIS restart.

If everything is functioning, you should be able to login as “sifworks” and find the new name in the Users list. Viewing the user account will show that the new user is a member of the “Server Administrator” Group.

## External LDAP Configuration Fields

Field Name	Description
<b>Address</b>	Host name or IP address of directory service server.
<b>Port</b>	Port number on which the directory service listens.
<b>Search User DN / Password</b>	Distinguished Name (DN) and password of the account that the ZIS will use to access the directory service. This search user only needs read permissions to the directory service as all changes to users and groups must be performed through an LDAP browser / editor.
<b>Encrypted (StartTLS)</b>	When checked, the ZIS will encrypt the directory service connection using the StartTLS method.
<b>Profile</b>	Profile options should only be used during initial configuration. Selecting one of the directory services listed will fill in many of the remaining fields with typical values for that directory service.
<b>Base DN</b>	Base Distinguished Name (DN) is where the user and group search begins in the directory tree. This must be the closest ancestor that the user's node and group's node share. This value will look like "dc=example,dc=com".
<b>User Object</b>	Class name that identifies a record as a user – typically "inetOrgPerson".
<b>User Identifier Attribute Name</b>	User identifier attribute name is the attribute used to get the login name of the user from the user's record.
<b>Group Operational Attribute Name</b>	Group operational attribute name is the attribute in the user's record that is used to find group membership. The value of the group operational attribute name is the DN of the group, and the user's record may contain zero or more of this operational attribute.

<b>Use Group Operational Attribute Name</b>	When this checkbox is checked, the Group Operational Attribute Name is used to identify a user's membership in a group. When unchecked, a less efficient simple search is performed to identify group membership.
<b>Local Correlation Attribute Name</b>	Local correlation attribute name used to get the identifier value with which local (non-LDAP) attributes are associated. Local attributes are application-specific, and never sent to or received from the directory service. This attribute name should be the unique identifier of the record, not the attribute used for the user's login name.
<b>First Name, Last Name, Full Name</b>	The attribute names used to get the user's name. If full name is not empty, it is used directly. Otherwise, first name and last name are used to get the user's full name for presentation.
<b>Phone</b>	The attribute name used to get the user's phone number for presentation.
<b>Email</b>	The attribute name used to get the user's email address for presentation.

# Part V

## 9. SIF Messaging Version Translation

SIF Message Version Translation is supported in all Enterprise or Hosting licenses of SIFWorks ZIS. SIF message version translation enables a SIF zone to support agents that have different major versions. The built-in translation mappings support translation between SIF version 1.x and 2.x (e.g. SIF 1.5r1 to SIF 2.1, and SIF 2.1 to SIF 1.5r1) for the following SIF data objects.

- Authentication
- EmployeePersonal
- LEAInfo
- SchoolCourseInfo
- SchoolInfo
- SectionInfo
- StaffAssignment
- StaffPersonal
- StudentPersonal
- StudentSchoolEnrollment
- StudentSectionEnrollment
- TermInfo

The version translation for these objects is driven by the same technology that enables Data Solutions' agents to support multiple SIF versions. This translation technology ensures that translated SIF data objects are valid for the target SIF version. The built-in translation mappings handle the standard SIF data object elements and value sets. However, if agents are built to expect non-standard SIF data object elements, the translation mappings must be modified to support the non-standard changes.

The remainder of this section introduces the information necessary to make changes to the default translation mappings that reside in the "conf/mappings.xml" file. Before any changes are made to the default mappings file a backup copy should be created, or the mappings override

mechanism provided in the zone template section of the ZIS administration console should be used.

## Translation Engine

A translation engine that automatically handles most structural changes in a SIF message drives the SIFWorks ZIS message version translation feature. Minor structural changes and valueset (code table) translations use the translation mappings file to complete the translation process.

A ZIS administrator may modify the “conf/mappings.xml” file to support custom data object elements and code tables that may be required by a non-SIF-standard agent. The mappings file is an XML file that contains code tables and element/attribute level rules for translating the codes.

## Valueset Tables

The “valueset” tables contain the necessary information to translate a specific code from one SIF version to another. A consistent naming convention used in the “id” attribute value to identify the direction of the translation for a specific table. Two tables, for the address type attribute, are shown below.

```
<valueset id="AddressType_1.5_to_2.0">
  <!-- Permanent home address (physical location) -->
  <value name="01">0765</value>
  <!-- Other home address -->
  <value name="02">1073</value>
  <!-- Mailing address (other address or P.O. Box address) -->
  <value name="03">0123</value>
  <!-- Campus address -->
  <value name="04">0123</value>
  <!-- Employer's address -->
  <value name="05">1074</value>
  <!-- Employment address -->
  <value name="06">1075</value>
  <!-- Organization's address -->
  <value name="07">2382</value>
</valueset>
<valueset id="AddressType_2.0_to_1.5">
  <!-- Mailing address (other address or P.O. Box address) -->
  <value name="0123">03</value>
  <!-- Shipping address -->
  <value name="0124">03</value>
  <!-- Permanent home address (physical location) -->
  <value name="0765">01</value>
  <!-- Other home address -->
  <value name="1073">02</value>
  <!-- Employer's address -->
  <value name="1074">05</value>
  <!-- Employment address -->
  <value name="1075">06</value>
  <!-- Organization's address -->
  <value name="2382">07</value>
</valueset>
```

The valueset mappings shown are symmetrical; for each value in SIF 1.5 there is a matching value in SIF 2.0. Some valuesets may be asymmetric where one or more values do not exist in the target SIF version. When this condition occurs,

the most common solution is to use the “other” value, or pick a satisfactory default value from the set of valid values.

## Field Rules

Field rules instruct the translation engine how to use the valueset tables. The mapping process occurs in two steps, 1) perform inbound matching on existing values in the SIF message and 2) perform outbound translation using a valueset table.

Most mappings rules will occur in pairs. An example for address type is shown below, and may be read as, “when the inbound message is SIF version 1.5r1 or earlier match the address type attribute, and perform outbound translation using the AdresType\_1.5\_to\_2.0 table when the target SIF version is 2.0 or higher.”

```
<field name="ADDRTYPE_1.5_?" sifVersion="-1.5r1" direction="inbound"
valueset="AddressType_1.5_to_2.0">Address[@Type=?]/@Type</field>

<field name="ADDRTYPE_1.5_?" sifVersion="+2.0" direction="outbound"
valueset="AddressType_1.5_to_2.0">AddressList/Address[@Type=?]/@Type<
/field>
```

The rule pair shown translates the address type attribute from a SIF 1.x to SIF 2.x value. The combination of the “direction” and “sifVersion” attributes control how the translation is performed. The “?” character in the “name” attribute of the rules is used internally by the translation engine to do value matching. Each rule also contains an XPath expression that is used to match against one or more elements (or attributes) in the SIF message.

Two variations of field rules exist – one to add element or attributes, and one to delete element or attributes. The following example, using address type field rules, shows both cases.

```
<field name="ADDRTYPE_2.0_?" sifVersion="+2.0" direction="inbound"
valueset="AddressType_2.0_to_1.5">AddressList/Address[@Type=?]/@Type</field>

<field name="ADDRTYPE_2.0_?" sifVersion="-1.5r1" direction="outbound"
valueset="AddressType_2.0_to_1.5">StudentAddress/Address[@Type=?]/@Type</field>

<field alias="ADDRTYPE_2.0_?" name="SP_POD_2.0_?" sifVersion="-1.5r1" direction="outbound"
valueset="AddressType_2.0_to_1.5">StudentAddress/@PickupOrDropoff=NA</field>

<field alias="ADDRTYPE_2.0_?" name="SP_DOW_2.0_?" sifVersion="-1.5r1" direction="outbound"
valueset="AddressType_2.0_to_1.5">StudentAddress/@DayOfWeek=NA</field>

<field name="ADDRTYPE_2.0_DELETE" sifVersion="-1.5r1"
direction="outbound">StudentAddress/Address[@Type!='03']</field>
```

When an element or attribute is being inserted into a SIF message, an additional rule must be added. The rule must have an “alias” attribute that matches the

“name” attribute of an existing rule, have a unique “name” attribute and be an outbound rule. In the example, there are two attributes that are being added to the “StudentAddress” element of a SIF version 1.5r1 (or lower) message.

One or more elements may be deleted using a single rule. The rule must have a unique “name” attribute and have the string “\_DELETE” appended to the name. The translation engine will delete all elements that match the XPath expression.

## 10. Contacting Data Solutions

### **Support for SIFWorks ZIS**

Our well-qualified support team is available to help get the Data Solutions SIFWorks ZIS configured and running correctly, provided that a current support contract is in place .

#### **Telephone Support**

Customers can reach Technical Support at 1-877-790-1261 during our regular business hours from 7:00 AM (07:00) to 6:00 PM (18:00) Mountain Standard Time. Such support will include technical assistance of product installation, technical configuration of the installed components, technical issue resolution, and reporting of bugs and enhancement requests. If support is required outside of these hours, it may be arranged through the Director of Implementation Services.

#### **On-Line Customer Support Center**

Customers with an active Support Agreement are eligible to access the Customer Support Center at <http://www.pearsondatasolutions.com/support> to view or log issues, and to access the Data Solutions knowledge base. A Customer Support representative can grant access to a customer by activating "self-service" on the contact screen in Salesforce.

#### **Remote Access**

Customer Support is accomplished primarily via telephone and/or remote access. For remote access, Data Solutions uses GoToMeeting, WebEx, and VPN technology to visually inspect and access a customer's server environment.

#### **On-Site Support Service**

Customer Support Services may be requested for product installation or other support reasons. If on-site support is requested, it may be arranged through the Director of Implementation Services.