Insurance

Oracle Insurance

Insbridge Enterprise Rating

Security Guide

Release 5.6

November 2018

Oracle Insurance Insbridge Enterprise Rating Security Guide

Release 05.06.00

Part # E96984-01

Library # E96993-01

November 2018

Primary Authors: Mary Elizabeth Wiger

CONTENTS

OVERVIEW 5

Definitions *6*

USERS AND PRIVILEGES 7

INSTALLER PERMISSIONS 7

ADMINISTRATIVE USER ACCOUNTS 7

FILE PERMISSIONS 7

Extended Permission Required by the Insbridge User *7*

Insbridge User Password *8*

DATABASE USER ROLES AND PERMISSIONS 8

Database File Location *9*

Microsoft SQL Server *10*

Oracle *10*

IBM DB2 .... *11*

APPLICATION SERVER 12

Deployment Permissions *12*

Application User Permissions *12*

SSL *12*

USER AUTHENTICATION 13

IBFA 13

Protocols *13*

Types of Authentication *14*

LOGS 15

Event Log Events *17*

Audit Log *18*

RATEMANAGER 19

USER SECURITY 19

USER PRIVILEGES AND GROUP-BASED ACCESS CONTROL 19

Group Rights *20*

Session Management *22*

AUDITING 23

AUDIT REPORT 24

IBSS 25

Auditing *25*

SECURITY 26

Security Enabled *26*

LOGS 27

WEB SERVICES SECURITY 30

USING COOKIES IN INSBRIDGE APPLICATION 31

ENCRYPTION ALGORITHMS 32

SECURITY BEST PRACTICES 33
ADDITIONAL SOURCES OF SECURITY INFORMATION.. 36

OVERVIEW

Security planning is a critical step in protecting your company's valuable data and ensuring that information is not compromised. Established security policies must work with and meet your company's security standards.

The Oracle Insurance Insbridge Enterprise Rating (Insbridge) system stores sensitive data and requires security measures to be taken. Security policies should align with those already established at your organization, or new ones should be established if they are not already defined.

This document provides guidelines for securing an Insbridge installation, including the configuration and installation steps needed to meet security goals. Details on the on the types of security features and services that are available are provided. This encompasses secure system deployment, protection of sensitive data, reliability and availability of the application, authentication and authorization mechanisms.

You may use this document to develop your organization's security policies and practices in the context of Insbridge. It is critical that an organization set security standards and properly implement them. The development and review of security documentation, an evaluation of business requirements, and the configuration and validation of available security measures and services should all be performed.

Definitions

Some commonly used terms when installing or using the Oracle Insurance Insbridge Enterprise Rating system:

- **IBER:** Insbridge Enterprise Rating System. (Insbridge) This is the entire system.
- **IBRU:** Previous name for Insbridge Enterprise Rating; Insbridge Rating and Underwriting. The acronym may still be in use in certain areas.
- **IBFA:** Insbridge Framework Administrator. IBFA is an administrative tool used to configure Insbridge applications and setup RateManager database connections. IBFA will be located on a Windows Server machine. IBFA/SR-WIN is an Insbridge Framework Administrator/SoftRater for Windows.
- **IBSS:** Insbridge SoftRater Server. IBSS is the administrative tool for the SoftRater engine. The SoftRater engine is a multi-platform component within Insbridge that executes the rules, rating and underwriting instructions as defined by the user in RateManager. IBSS is usually located on a Java machine. IBSS/SR-JAVA is an Insbridge SoftRater Server/SoftRater for Java.
- **SoftRater Node:** A SoftRater node is either an IBFA (without RateManager) or IBSS instance on a physical environment.
- **RM:** RateManager. RateManager is a component within Insbridge that enables users to manage the product definition and modification process, including rating and underwriting logic.
- **SR:** SoftRater. The engine that executes the rating, rules and underwriting instructions defined within RateManager. The rating environment for runtime execution and processing of business content. SoftRater can be further defined by the operating system where it has been loaded.
- **SR-WIN:** SoftRater for Windows. This is also another name for IBFA.
- **SR-JAVA:** SoftRater for Java. This is also another name for IBSS.
- **SRP:** SoftRater Packages. A package that holds all the RateManager logic for a specific program and version.

USERS AND PRIVILEGES

The Insbridge application requires certain users roles and permissions depending upon the action to be performed.

INSTALLER PERMISSIONS

The installation program requires that the installer have administrator rights on the machine where the install is occurring. The install must be run as administrator.

ADMINISTRATIVE USER ACCOUNTS

No administrative account is created when Insbridge is installed. An administrative user account must be created on the server where the Insbridge system is going to be installed. This required account is the Insbridge Local User Account.

The Insbridge Local User needs to be a member of the User group and requires certain privileges in order to fully control the entire Insbridge environment. For ease of installation and if the server is dedicated to the Insbridge Enterprise Rating System, this user can be added to the local machine Administrators group.

FILE PERMISSIONS

The Insbridge User requires read/write permissions on:

- The Windows Temp Folder. This is necessary for MSMQ.
- The Insbridge Application Pool Identity
- The Insbridge Folder

The Insbridge user must also be given **full control** over the following registry key:

- HKEY_LOCAL_MACHINE/SOFTWARE/Insbridge

Extended Permission Required by the Insbridge User

In order to start the Insbridge services from IBFA, the Insbridge user must be given full access to both the Insbridge Message Service and the Insbridge Task Manager Service. If the Insbridge user account will not have full administrative permissions on the server where the Insbridge Framework is installed, then certain operations from IBFA will not be available. A system administrator may be required to start the Insbridge services from the server.

Insbridge User Password

The password can be set to any password that meets your company standards. The Insbridge administrator must make note of the password for future configuration.

For ease of maintenance, the Insbridge user should not have to change the password and the password should never expire.

The installation automatically applies the Insbridge user name and password to the necessary libraries, virtual directories and, if used, Internet Proxy settings in IBFA. If you change the Insbridge user password, you will have to change the password in all three of the Insbridge Com+ libraries, all three of the Insbridge virtual directories and, if you are using it, the Internet Proxy settings in IBFA.

NOTE: Please note that if your company requires passwords to be re-set, you will have to make changes to the COM+ Application libraries, virtual directories and if you are using it, the Internet Proxy settings in IBFA after you change your password. You also may re-install the application. This recreates the COM+ applications, virtual directories and IBFA instance with the updated Insbridge user password. Be aware that re-installing the application may reset security settings in IBFA as well.

***NOTE**: If the Installer has permissions, an Insbridge User account can be created from within the install. If you create an Insbridge user from the install, you may not be able to set the permissions you need. Please be sure to verify the proper permissions are in place before continuing.*

Database User Roles and Permissions

If a more granular approach is required for management of security of the Insbridge databases, then the following guidelines can be used to set permissions.

NOTE: *These are only guidelines. If not properly configured, certain processes within the Insbridge Enterprise Rating System will fail. An experienced database administrator's expertise is highly recommended before making any security changes.*

A separate ibru account must be created for the Insbridge application. This account allows for Insbridge database errors to be easily distinguished.

Recommended RateManager Permissions:

It is recommended that the IBRM and IB_CLIENT database user have:

- **A database owner (db_owner) role.** db_owner access is needed to execute the Insbridge stored procedures and have full access to the Insbridge schema.
- **Disk Admin permissions** are also recommended in order to create backups within RateManager.

Recommended SoftRater Permissions:

The recommended permissions are required for new tables to be created in the SoftRater (IBSR) database dynamically when or if a new line of business SRP (SoftRater Package) is loaded to the SoftRater system. If the recommended permissions are not possible, manual steps will need to be performed that will allow for packages to be loaded.

SoftRater can utilize three database types, SQL Server, DB2 and Oracle.

- **Insbridge SoftRater SQL Server Database**.

  It is recommended that the Insbridge login be granted permission to connect to the database engine and be enabled. It is also recommended that the Insbridge login be mapped to the Insbridge database with the db_owner role checked.

- **Insbridge SoftRater Oracle Database**.

  It is recommended that the Insbridge user be granted, as defaults, the “CONNECT” and “RESOURCE” Roles.

- **Insbridge SoftRater DB2 Database**.

  It is recommended that the Insbridge user be granted, as defaults, the “Connect to database”, “Create Tables”, and “Create packages” authorities.

It is recommended that the databases be on separate machines from the applications due to performance and security issues. The Insbridge applications and databases can be tenants in a larger setup.

It is recommended that db_owner permissions be given to the Insbridge user. This will allow scripts to be run automatically when a new package is loaded for a new line of business. If this is not possible, DT scripts for each new line will have to be run manually before the package can be loaded.

Database File Location

For the IBRM and IB_CLIENT databases, if db_owner permissions are not possible, the database will need to be updated manually. If disk admin permissions are not allowed, backups will have to be done outside of RateManager.

The IBRM database may also have a reports reader user created to allow for Insbridge Runtime Reports to be run against the IBRM database using a reporting tool such as Microsoft Excel.

NEW IB_CLIENT and IBRM Databases – Files are located in the download file available on Oracle Software Delivery Cloud. Template files are current.

UPDATING IB_CLIENT and IBRM Databases – The preferred method of updating the IBRM, and IB_CLIENT databases is to run them through RateManager. If the RM administrator has DB User privileges and is the DB Owner of the database as well as the disk administrator, database updates can be done on the Tools→Database→Updates tab. If these privileges are not in place, an error message is displayed.

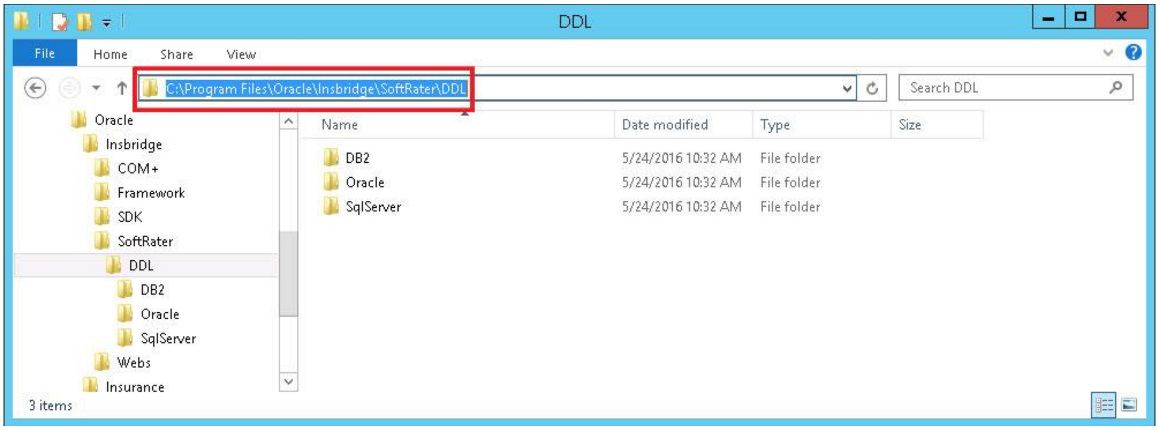
These databases can be updated manually by downloading the scripts and running directly in SQL Server. Scripts must be run in sequential order. You must have SQL SERVER permissions.

New IB_CLIENT and IBRM database updates are usually not required.

For SoftRater databases, in the event that db_owner permissions are not possible, scripts will have to be run to create the necessary tables. Tables are required for each Project and or Product. If the tables are not created, the packages cannot be loaded.

DDL scripts can be found on the server where Insbridge was installed in the …//Oracle/Insbridge/SoftRater folder.

For example: C:\Program Files\Oracle\Insbridge\SoftRater\DDL



C:\Program Files\Oracle\Insbridge\SoftRater\DDL

Name	Date modified	Type	Size
DB2	5/24/2016 10:32 AM	File folder	
Oracle	5/24/2016 10:32 AM	File folder	
SqlServer	5/24/2016 10:32 AM	File folder	

For SQL Server, backup files are included in the Insbridge-Windows folder under databases.

Microsoft SQL Server

JDBC Driver Class

“com.microsoft.jdbc.sqlserver.SQLServerDriver”

Versions – 2012, 2016 SP1

User Account Requirements

Create Table
Create Index
Execute on the SoftRater User Defined Stored Procedures

Oracle

SoftRater database schema is support by all available ORACLE database platforms.

Versions – 11g, and 12c

JDBC Driver Class

"oracle.jdbc.driver.OracleDriver"
Using prefix jdbc:oracle:thin:

User Account Requirements

Create Table
Create Index
Query access to "SYS.OBJ$"

IBM DB2

SoftRater database schema is supported on version 11.1.

Version – 11.1

JDBC Driver Class

"com.ibm.db2.jcc.DB2Driver"
For Native AS400 – "com.ibm.as400.access.AS400JDBCDriver"

User Account Requirements

Connect to database
Create Table
Create Packages
Query access to "SYSIBM.SYSTABLES"

Configuration Settings

- **Required**
  The query dynamics of the SoftRater system requires some modification to Configuration settings. The following Performance Configurations parameters required to the target SoftRater database.
  Instance Level – ASLHEAPSZ >= 1024
  Instance Level – QUERY_HEAP_SZ => 10240
  Database Level – APPLHEAPSZ >= 1024

Recommended

The query dynamics of the SoftRater system will benefit from the following modification to Configuration settings.

Instance Level – INTRA_PARRALLEL (Yes) – For Symmetrical Processing Machines (CPU >=2)

Database Level – DFT_DEGREE (-1) – For Symmetrical Processing Machines (CPU >=2). Allow the optimizer to determine the degree of intra-partition parallelism based on the number of processors and the type of query.

APPLICATION SERVER

The Insbridge application JAVA engine called SoftRater Server (IBSS) can be deployed in three application servers: WebLogic, WebSphere, and JBoss.

Deployment Permissions

Deployment requires admin permissions on the server to create holding folders for file placement. On a Linux machine, non-root users must used.

Application User Permissions

The SoftRater Server (IBSS) application servers WebLogic, WebSphere, and JBoss require read/write permissions on the Insbridge.net.softraterconfig.xml that resides in the shared directory for all nodes. Also required is full control on the SoftRater node instance directory creates the config files and log files for that JVM.

SSL

IBSS supports HTTPS (ssl). Functionality is the same as an HTTP connection. HTTPS has to be configured at the server level and no additional configuration is needed in IBSS.

Enable IBSS over HTTPS to secure the application. It is advised to completely disable HTTP when HTTPS(ssl) is enabled.

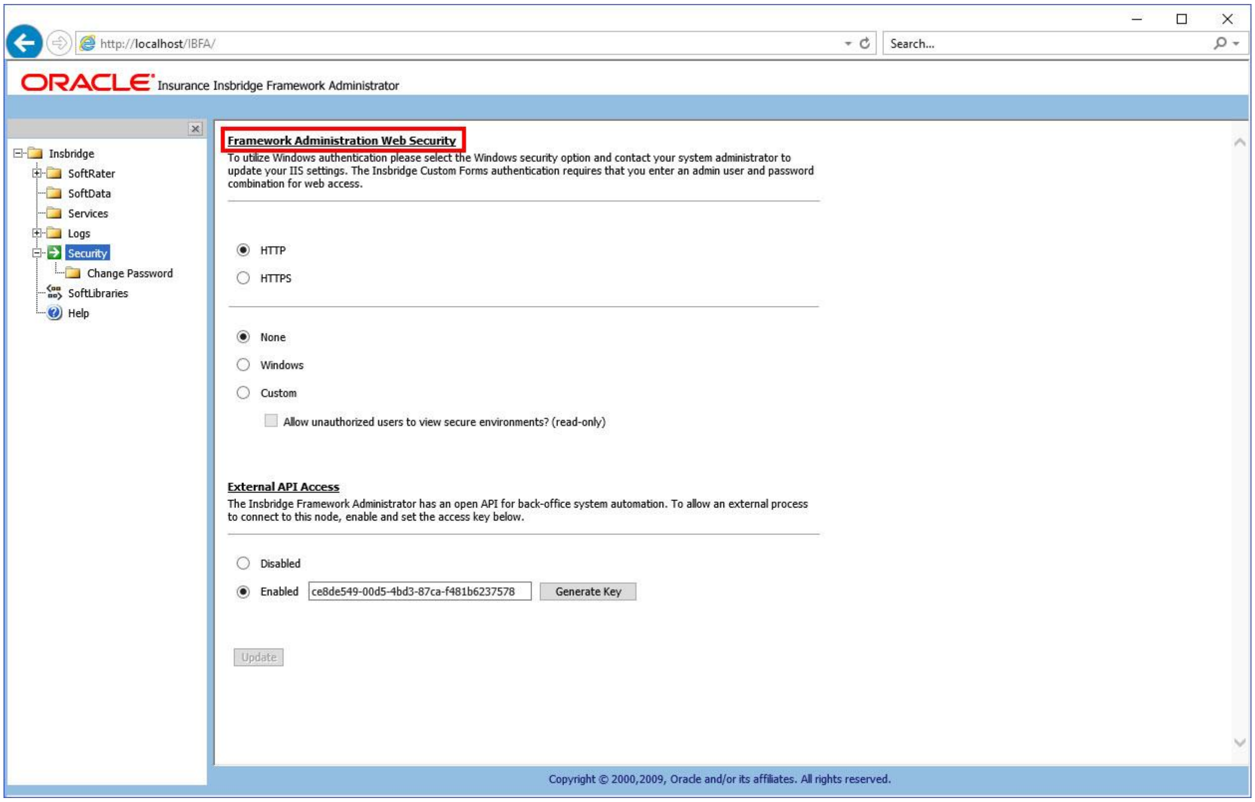
Check Secure when creating a node instance. This indicates that the connection at the server level is secured. A secure node can be added only in a HTTPS enabled IBSS.

USER AUTHENTICATION

The Insbridge application provides an out-of-the box user authentication mechanism as well as an ability to implement alternative authentication models like a Windows Authentication. Each application with the Insbridge system has security measures in place.

IBFA

The security section of the Framework Administrator allows an administrator to set the type of protocol used and the authentication that will be used to certify users and allow them to access to all sections of the Framework Administrator. If a user does not have full access, they will be allowed to see only the **Packages** subtab of the SoftRater Explorer. Within the SoftRater Explorer, the user will only be able to manipulate packages that are not located in a secure environment.



Framework Administration Web Security

To utilize Windows authentication please select the Windows security option and contact your system administrator to update your IIS settings. The Insbridge Custom Forms authentication requires that you enter an admin user and password combination for web access.

● HTTP
○ HTTPS

● None
○ Windows
○ Custom
□ Allow unauthorized users to view secure environments? (read-only)

External API Access

The Insbridge Framework Administrator has an open API for back-office system automation. To allow an external process to connect to this node, enable and set the access key below.

○ Disabled
● Enabled ce8de549-00d5-4bd3-87ca-f481b6237578

Copyright © 2000,2009, Oracle and/or its affiliates. All rights reserved.

Figure 1 IBFA Security

Protocols

The protocol is how IBFA is exposed. The Framework Administrator allows you to set the type of protocol used. The available options are:

- **HTTP:** Hyper Text Transfer Protocol.
- **HTTPS:** Hyper Text Transfer Protocol Secure. A secure version of HTTP.

The default protocol is HTTP.

Types of Authentication

The Framework Administrator allows you to set the type of authentication used. The available options are:

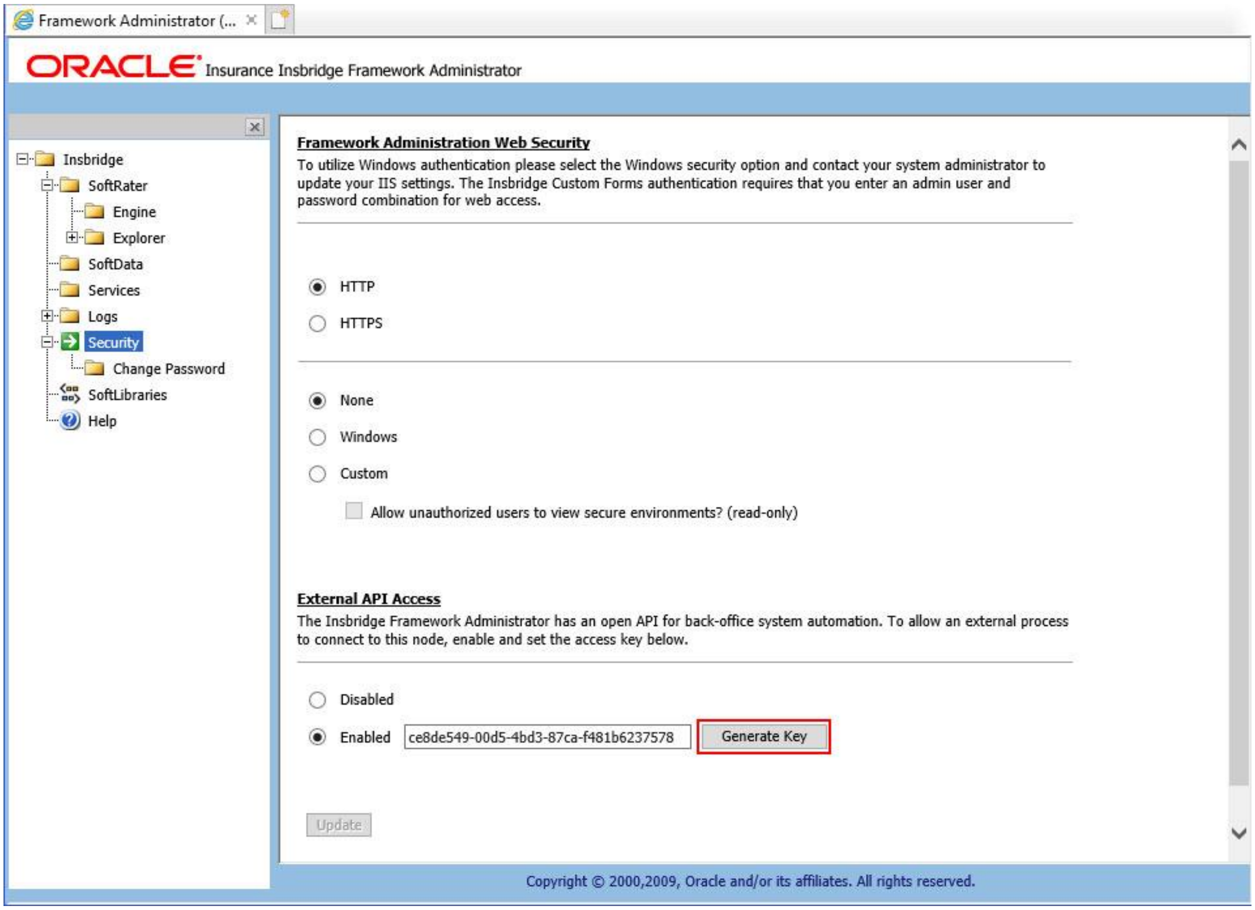
- **None:** All users will have access to all portions of the Framework Administrator. This is not recommended for security reasons.

- **Windows:** Users, and the areas of the Framework Administrator they can access, are validated by IIS. This option relies on Microsoft Internet Information Services (IIS) to provide authenticated users. All methods supported by IIS are permitted. When using IIS, the provider module uses the authenticated identity passed in from IIS. IIS authenticates the identity using basic, digest, integrated Windows authentication or some combination of these. You can use impersonation and NTFS ACL permissions to restrict or allow access to protected resources. Intranet Credentials can be entered anonymous website to website access is denied.

- **Custom: DEFAULT OPTION** Users can log in through an HTML form. Users that are not logged in can only access non-secure environments. This option collects a user's credentials through a login window. The user enters a user ID and password and then submits the HTML form. If the application authenticates the request, the system issues a cookie that contains the credentials, key, for reacquiring the identity. Subsequent requests are issued with the cookie in the request headers. The requests are authenticated and authorized by an ASP.NET event handler, using whatever validation method the application specifies. The system also allows the administrator to change or reset the password that is encrypted on disk.

OBI Credentials

OBI Publisher is required to generate reports. The credentials in IBFA must match the credentials in OBI Publisher in order for reports to be generated.



Framework Administration Web Security

To utilize Windows authentication please select the Windows security option and contact your system administrator to update your IIS settings. The Insbridge Custom Forms authentication requires that you enter an admin user and password combination for web access.

● HTTP

○ HTTPS

● None

○ Windows

○ Custom

□ Allow unauthorized users to view secure environments? (read-only)

External API Access

The Insbridge Framework Administrator has an open API for back-office system automation. To allow an external process to connect to this node, enable and set the access key below.

○ Disabled

● Enabled ce8de549-00d5-4bd3-87ca-f481b6237578

Copyright © 2000,2009, Oracle and/or its affiliates. All rights reserved.

Figure 2 ESI Key

ESI Access

Oracle Insurance Insbridge Enterprise Rating Extended Services Interface (ESI) is a library module designed to provide remote services to the Insbridge Enterprise Rating (INSBRIDGE) business services without directly utilizing the system User Interfaces (UI).

ESI allows users to pass information between a user's source policy or business admin system and the RateManager system or the Insbridge Framework Administrator (IBFA) without using either the RateManager or IBFA UI. Information is passed through a custom built interface that resides on a source policy or business admin system on the client side to the ESI web service that resides on the Insbridge side. The information is processed and results returned from the ESI web service back to the custom built interface into the client's source policy or business admin system.

For security purpose, you may want to change the key periodically. Every key generated will be unique.

Logs

Logs are records of selected events or activities that happen in IBFA. These are separated into two types.

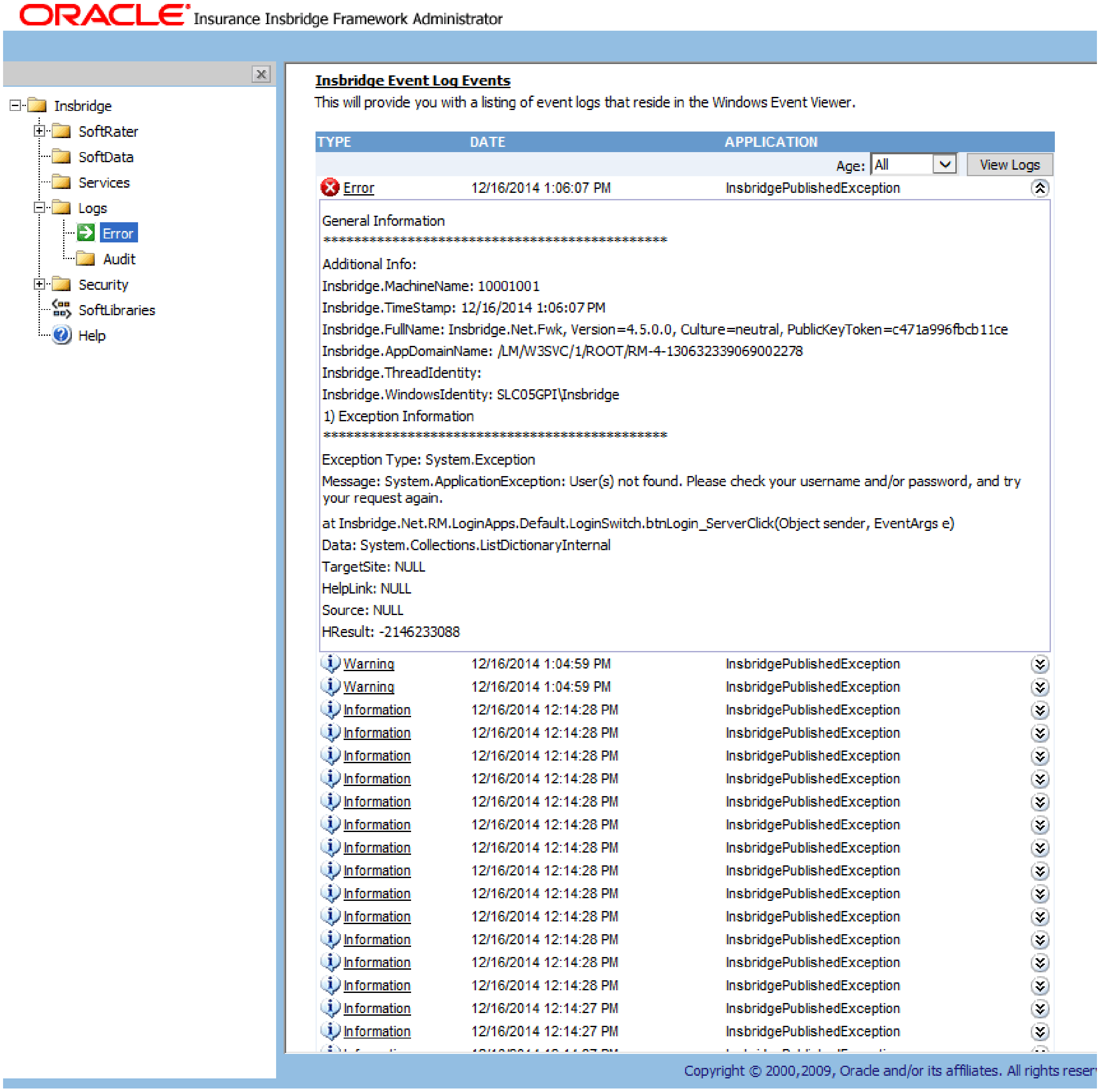
- **Event Log Events** are triggered when an Insbridge application either fails to do what has been requested or successfully completes an operation.

- **Audit Log Activities** are triggered when there is SoftRater package activity.

Event Log Events

When an Insbridge application generates an error, it logs the event in the server's event viewer. Error events occur when an Insbridge application fails to do what it is supposed to. For example, if the Insbridge Message Service fails to start, an error event will be logged.

In addition to error events, information events are also logged in the event viewer. An information event describes the successful completion of an operation by an Insbridge application. For example, when the Insbridge Message Service starts successfully, an information event is logged.


ORACLE Insurance Insbridge Framework Administrator
Insbridge
SoftRater
SoftData
Services
Logs
Error
Audit
Security
SoftLibraries
Help
Age: All
View Logs
Copyright © 2000,2009, Oracle and/or its affiliates. All rights reser

Insbridge Event Log Events

This will provide you with a listing of event logs that reside in the Windows Event Viewer.

TYPE	DATE	APPLICATION
Error	12/16/2014 1:06:07 PM	InsbridgePublishedException

```
General Information
**************************************************
Additional Info:
Insbridge.MachineName: 10001001
Insbridge.TimeStamp: 12/16/2014 1:06:07 PM
Insbridge.FullName: Insbridge.Net.Fwk, Version=4.5.0.0, Culture=neutral, PublicKeyToken=c471a996fbcb11ce
Insbridge.AppDomainName: /LM/W3SVC/1/ROOT/RM-4-130632339069002278
Insbridge.ThreadIdentity:
Insbridge.WindowsIdentity: SLC05GPI\Insbridge
1) Exception Information
**************************************************
Exception Type: System.Exception
Message: System.ApplicationException: User(s) not found. Please check your username and/or password, and try
your request again.
at Insbridge.Net.RM.LoginApps.Default.LoginSwitch.btnLogin_ServerClick(Object sender, EventArgs e)
Data: System.Collections.ListDictionaryInternal
TargetSite: NULL
HelpLink: NULL
Source: NULL
HResult: -2146233088
```

Warning	12/16/2014 1:04:59 PM	InsbridgePublishedException
Warning	12/16/2014 1:04:59 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:28 PM	InsbridgePublishedException
Information	12/16/2014 12:14:27 PM	InsbridgePublishedException
Information	12/16/2014 12:14:27 PM	InsbridgePublishedException

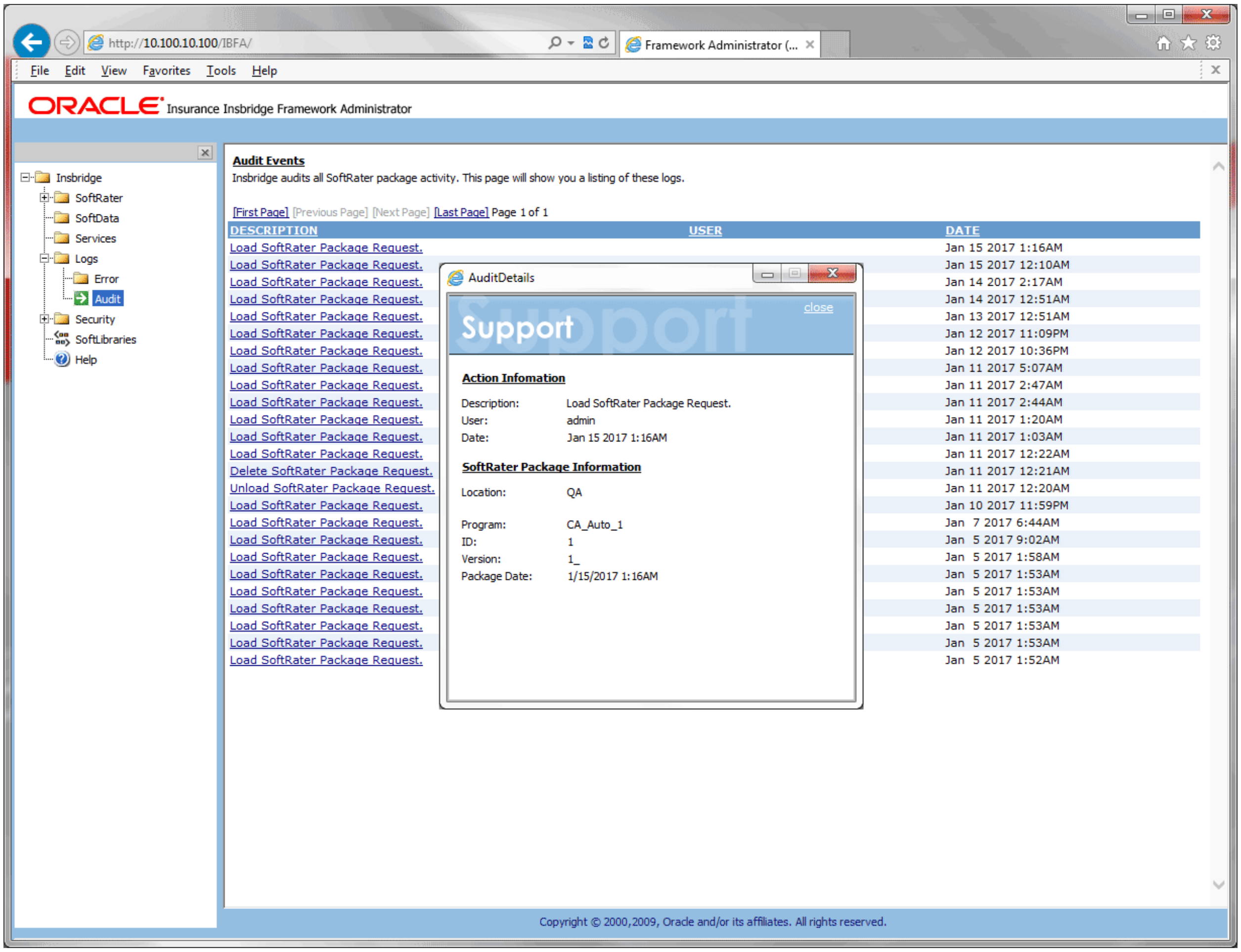
Figure 3 Insbridge Event Log Event

IBFA will display 80 events. If you require more than that, you need to return to the server's event log.

Audit Log

The Audit Log keeps track of all SoftRater package activity, known as audit events. The types of audit events recorded are:

- **Download:** An event that records the downloading of a package.
- **Load:** An event that records the loading of a package.
- **Unload:** An event that records the unloading of a package.
- **Delete:** An event that records the deletion of a package.
- **Copy:** An event that records the copying of a package.
- **Move:** An event that records the moving of a package.
- **Backup:** An event that records the creation of a SoftRater Native backup.



Audit Events

Insbridge audits all SoftRater package activity. This page will show you a listing of these logs.

[First Page] [Previous Page] [Next Page] [Last Page] Page 1 of 1

DESCRIPTION	USER	DATE
Load SoftRater Package Request.		Jan 15 2017 1:16AM
Load SoftRater Package Request.		Jan 15 2017 12:10AM
Load SoftRater Package Request.		Jan 14 2017 2:17AM
Load SoftRater Package Request.		Jan 14 2017 12:51AM
Load SoftRater Package Request.		Jan 13 2017 12:51AM
Load SoftRater Package Request.		Jan 12 2017 11:09PM
Load SoftRater Package Request.		Jan 12 2017 10:36PM
Load SoftRater Package Request.		Jan 11 2017 5:07AM
Load SoftRater Package Request.		Jan 11 2017 2:47AM
Load SoftRater Package Request.		Jan 11 2017 2:44AM
Load SoftRater Package Request.		Jan 11 2017 1:20AM
Load SoftRater Package Request.		Jan 11 2017 1:03AM
Load SoftRater Package Request.		Jan 11 2017 12:22AM
Delete SoftRater Package Request.		Jan 11 2017 12:21AM
Unload SoftRater Package Request.		Jan 11 2017 12:20AM
Load SoftRater Package Request.		Jan 10 2017 11:59PM
Load SoftRater Package Request.		Jan 7 2017 6:44AM
Load SoftRater Package Request.		Jan 5 2017 9:02AM
Load SoftRater Package Request.		Jan 5 2017 1:58AM
Load SoftRater Package Request.		Jan 5 2017 1:53AM
Load SoftRater Package Request.		Jan 5 2017 1:53AM
Load SoftRater Package Request.		Jan 5 2017 1:53AM
Load SoftRater Package Request.		Jan 5 2017 1:53AM
Load SoftRater Package Request.		Jan 5 2017 1:53AM
Load SoftRater Package Request.		Jan 5 2017 1:52AM

Action Infomation

Description:	Load SoftRater Package Request.
User:	admin
Date:	Jan 15 2017 1:16AM

SoftRater Package Information

Location:	QA
Program:	CA_Auto_1
ID:	1
Version:	1_
Package Date:	1/15/2017 1:16AM

Figure 4 Audit Log

RateManager

Access to the RateManager application is granted through login/password. Only a RateManager administrator may configure RateManager security settings. Usernames and groups are created and system rights assigned. Groups can be created to grant users access to specific lines of business and specific screens within that line of business (variables, algorithms, etc.), with or without write access. Groups also can be given access to specific modules, Testing or Impact Analysis.

User Security

A user must have an existing RateManager user account identified by username and password to log into the RateManager application. When creating a new user account, an administrator enters or selects the following information:

- User login name and password
- Basic information about user – first and last name, department, email, and phone
- User’s company
- Security groups that user belongs to
- If the User is a Network User: If set to **True**, network user’s credentials (username and password) are validated using Windows Authentication Tokens. The username in RateManager must match the network user ID. Users can access RateManager using the Insbridge Portal. Users will need the Insbridge URL to access RateManager via the portal. They will not be required to enter login information at the RateManager login screen.

This information is persisted in the IB_Client database, with the encrypted password digest stored as discussed in the User Authentication section of this document.

There is one pre-existing or default user account and security group in the Insbridge application. This user account cannot be deleted. Users are advised to change the password to prevent unauthorized access.

User Privileges and Group-Based Access Control

The Insbridge user privileges and access restrictions implementation are based on the role-based access control (RBAC) model. According to the model, user permissions are assigned to specific groups or roles that are created for various job functions. A user who is assigned to particular groups gains permissions through those groups to perform particular system functions. If a user is assigned to multiple groups, the user will have access to all resources authorized for all of those groups.

By default, a newly created user account does not have authorizations to access any of the application restricted resources. Authorizations have to be explicitly granted by a RateManager administrator. In setting up the user groups, an administrator needs to be careful to include only the minimum set of permissions that allow users of a particular group to perform their job functions.

Group Rights

Group Rights are broken into areas and lines of business. You can allow users access to the entire system or just certain modules. You also can restrict users from performing certain actions, such as packaging or creating folders.

User Actions	VIEW	WRITE	PACKAGE	LOCK
Permissions to Grant				
RateManager Scenario Manager Admin				
Scenario Management – Allows users full access to Scenario Management.	X	X		
RateManager Table Job Admin				
Export Management – Allows users full access to the Table Job Management tab.	X	X		
RateManager Domain Admin				
Product Management – Allows users full access to manage products.	X	X		
Project Management – Allows users full access to manage projects.	X	X		
Setup Options – Allows users to create, edit, and delete elements in Setup Options. Users with any Domain Admin rights can perform Setup Options. Users without Domains Admin rights can view only.	X	X		
RateManager Universals				
Variables –	X			
Write Access –		X		
Algorithms –	X			
Write Access –		X		
Fields –	X			
Write Access –		X		
Categories –	X			
Write Access –		X		
Valid Values Management –	X	X		
Scenarios –	X			
Write Access –		X		
RateManager Testing				
Testing Module – Allows users full access to the testing module.	X	X		
RateManager Package Admin				
Program Export – Allows users to export programs in the Library.	X	X		
Program Import – Allows users to import programs in the Library.	X	X		
Release Management – Allows users to access the Releases Module. **NOTE**: Product rights are required as well.	X	X		
Database Support				
Backups – Allows users to create database backups within RateManager.	X	X		

Restores – Allows users to restore databases within RateManager.	**X**	**X**		
Product				
Variables –	**X**			
Write Access –		**X**		
Algorithms –	**X**			
Write Access –		**X**		
Driver Assignment – AUTO Product ONLY	**X**			
Write Access –		**X**		
Sequencing –	**X**			
Write Access –		**X**		
Output Mapping –	**X**			
Write Access –		**X**		
Fields –	**X**			
Write Access –		**X**		
Categories –	**X**			
Write Access –		**X**		
Program Management –	**X**			
Write Access –		**X**	**X**	
Lock Admin –				**X**
Valid Values Revision Selection –		X		
Scenarios –	X			
Write Access –		X		

Permission to Grant Definitions

Available areas include:

1. **RateManager Scenario Manager Admin** – Allows users to create scenarios, add program versions, add tables, and publish.
    a. Scenario Administration
2. **RateManager Table Job Admin** – Allows users access to the Table Job management tab. Here users can create, edit, delete and start table export jobs.
    a. Export Management
3. **RateManager Domain Access** – Allows users to manage products and projects.
    a. **Product Management** – Users will be able to create, edit, activate, deactivate, disable, and delete products.
    b. **Project Management** – Users will be able to create, edit and delete Other domain types. Create, edit, clear, and delete domains. Create, edit, clear, and delete projects.
    c. **Select Products** – Users can select products in a project only if both Product Management rights and Project Management rights are granted.
    d. **Setup Options** – Setup options can be viewed by all users. Permissions are required to create, edit, and delete Setup Options. Any Domain Access permission grants permissions to work in Setup Options. The permission may be needed by users who set naming standards, create variable messages, or manage system level constants.

4. **RateManager Universals** – Allows users to work in the domain type universal elements.
    a. Read permissions are granted to all areas within the product by checking any element.
    b. Write permissions are granted per element. Checking a write permission will also grant read permission to all areas in the product.
    c. Valid Values Management permissions to create, edit, and delete validations in any domain are assigned here.
    d. Scenario permissions to manage and edit universal level tables in a scenario.

5. **RateManager Testing** – Allows users to work in the Testing Module. Users are granted full access when the element is checked.

6. **RateManager Package Admin** – Allows users to work with packages in the system and allows user to input mappings. Users are granted full access when the element is checked.
   a. **Program Export** – Allows users to create export programs on the Library tab. The permission may be needed by users who work with templates.
   b. **Program Import** – Allows users to apply exported programs and templates on the Library tab. The permission is needed by users who work with templates.
   c. **Release Management** – Allows users to work in the Releases Module. Users are granted full access when the element is checked. Users with releases rights now require product rights as well. Programs cannot be selected for a release unless the user has rights to the product where the program resides.

7. **Database Support** – Allows users to work on Database Backups and Database Restores. Users are granted full access when the element is checked.

8. **Product** – Each product will have rights separate from the other products.
   a. Read permissions are granted to all areas within the product by checking any element.
   b. Write permissions are granted per element. Checking a write permission will also grant read permission to all areas in the product.
   c. Package permissions are in the Program Management section. Checking a write permission grants package permissions as well as grant read permission to all areas in the product. Package permissions also allows for users to manage folders, move, copy, and create revisions.
   d. Valid Values Revision Selection allows users to set revisions at the global level.
   e. Scenarios permission allow users to add, edit and delete content from a scenario,

User Actions Definitions

Write Access allows users to create and edit entries. Users who do not have write access have Read-Only access unless access to the entire module has not been granted.

- **View:** Allows users to view the elements that have been created.

- **Write:** Allows users to create, edit, copy, and delete elements.

- **Package:** Allows users to create RateManager, SoftRater and Global Versioning packages.

- **Lock:** Allows users to lock programs.

Session Management

Session Management allows an administrator to view users who currently have a RateManager session open and disconnect them to free up a session.

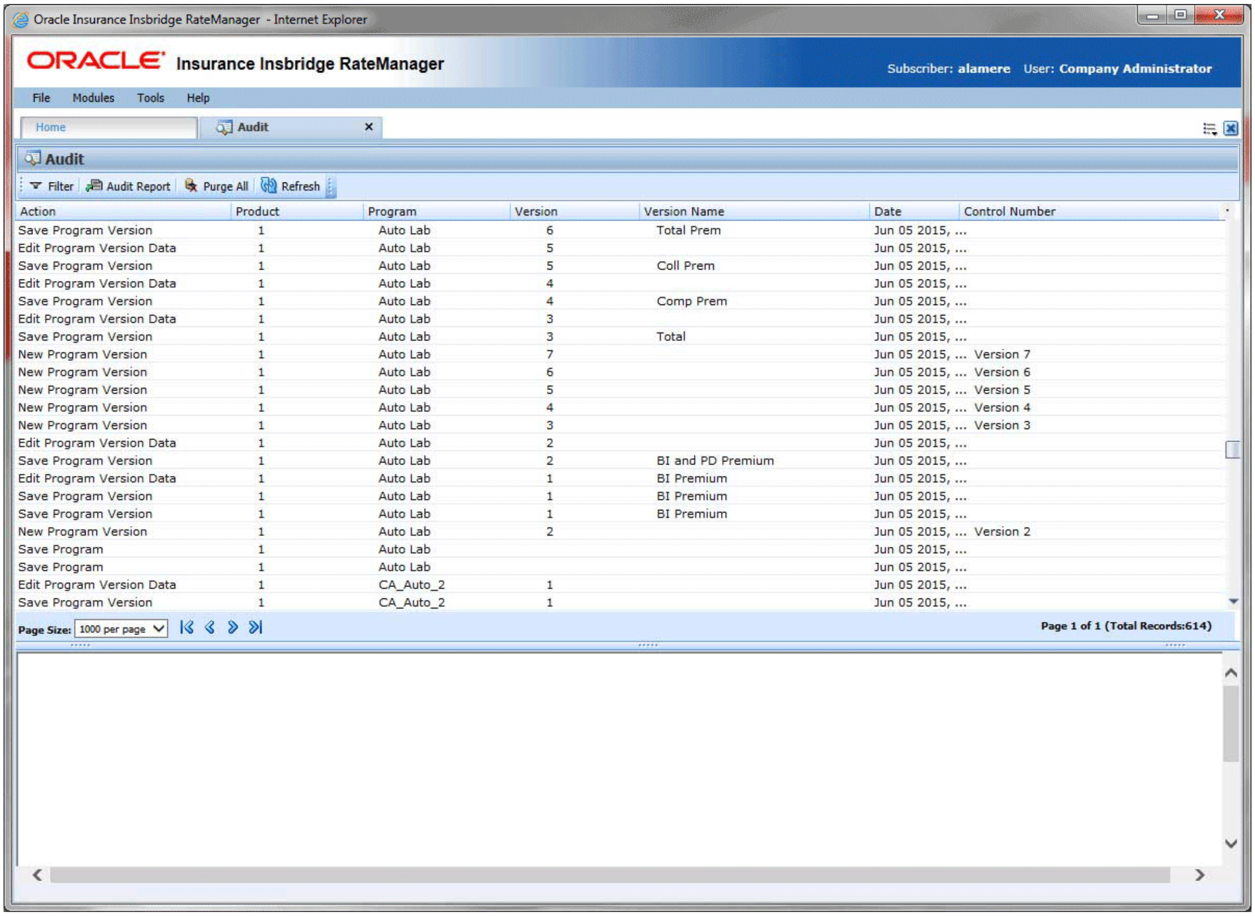
AUDITING

RateManager can keep an audit log of user activity. Audit logs contain information such as action performed, user ID, date and time stamp. Audits set to high will also track adding a user, editing a user and deleting a user. Audit logs also can include program information such as program ID, program version and line of business as well as element information.

The **Audit** tab contains a list of audits logs. The audit log feature has to be enabled at the group level. On the Group Management tab, Tools→Security→Group Management, select the group where you want to apply auditing. There are three options for auditing the group:

- **None:** No auditing is done.
- **Normal:** All saves and deletes are logged.
- **High:** All new, creates, changes, saves, and deletes for the group are logged.

If the group(s) has high auditing, more audit logs are created and you will have more types of actions you can filter on.


Oracle Insurance Insbridge RateManager - Internet Explorer
ORACLE Insurance Insbridge RateManager
Subscriber: alamere User: Company Administrator
File
Modules
Tools
Help
Home
Audit
Audit
Filter
Audit Report
Purge All
Refresh
Page Size: 1000 per page

Action	Product	Program	Version	Version Name	Date	Control Number
Save Program Version	1	Auto Lab	6	Total Prem	Jun 05 2015, ...	
Edit Program Version Data	1	Auto Lab	5		Jun 05 2015, ...	
Save Program Version	1	Auto Lab	5	Coll Prem	Jun 05 2015, ...	
Edit Program Version Data	1	Auto Lab	4		Jun 05 2015, ...	
Save Program Version	1	Auto Lab	4	Comp Prem	Jun 05 2015, ...	
Edit Program Version Data	1	Auto Lab	3		Jun 05 2015, ...	
Save Program Version	1	Auto Lab	3	Total	Jun 05 2015, ...	
New Program Version	1	Auto Lab	7		Jun 05 2015, ...	Version 7
New Program Version	1	Auto Lab	6		Jun 05 2015, ...	Version 6
New Program Version	1	Auto Lab	5		Jun 05 2015, ...	Version 5
New Program Version	1	Auto Lab	4		Jun 05 2015, ...	Version 4
New Program Version	1	Auto Lab	3		Jun 05 2015, ...	Version 3
Edit Program Version Data	1	Auto Lab	2		Jun 05 2015, ...	
Save Program Version	1	Auto Lab	2	BI and PD Premium	Jun 05 2015, ...	
Edit Program Version Data	1	Auto Lab	1	BI Premium	Jun 05 2015, ...	
Save Program Version	1	Auto Lab	1	BI Premium	Jun 05 2015, ...	
Save Program Version	1	Auto Lab	1	BI Premium	Jun 05 2015, ...	
New Program Version	1	Auto Lab	2		Jun 05 2015, ...	Version 2
Save Program	1	Auto Lab			Jun 05 2015, ...	
Save Program	1	Auto Lab			Jun 05 2015, ...	
Edit Program Version Data	1	CA_Auto_2	1		Jun 05 2015, ...	
Save Program Version	1	CA_Auto_2	1		Jun 05 2015, ...	

Page 1 of 1 (Total Records:614)

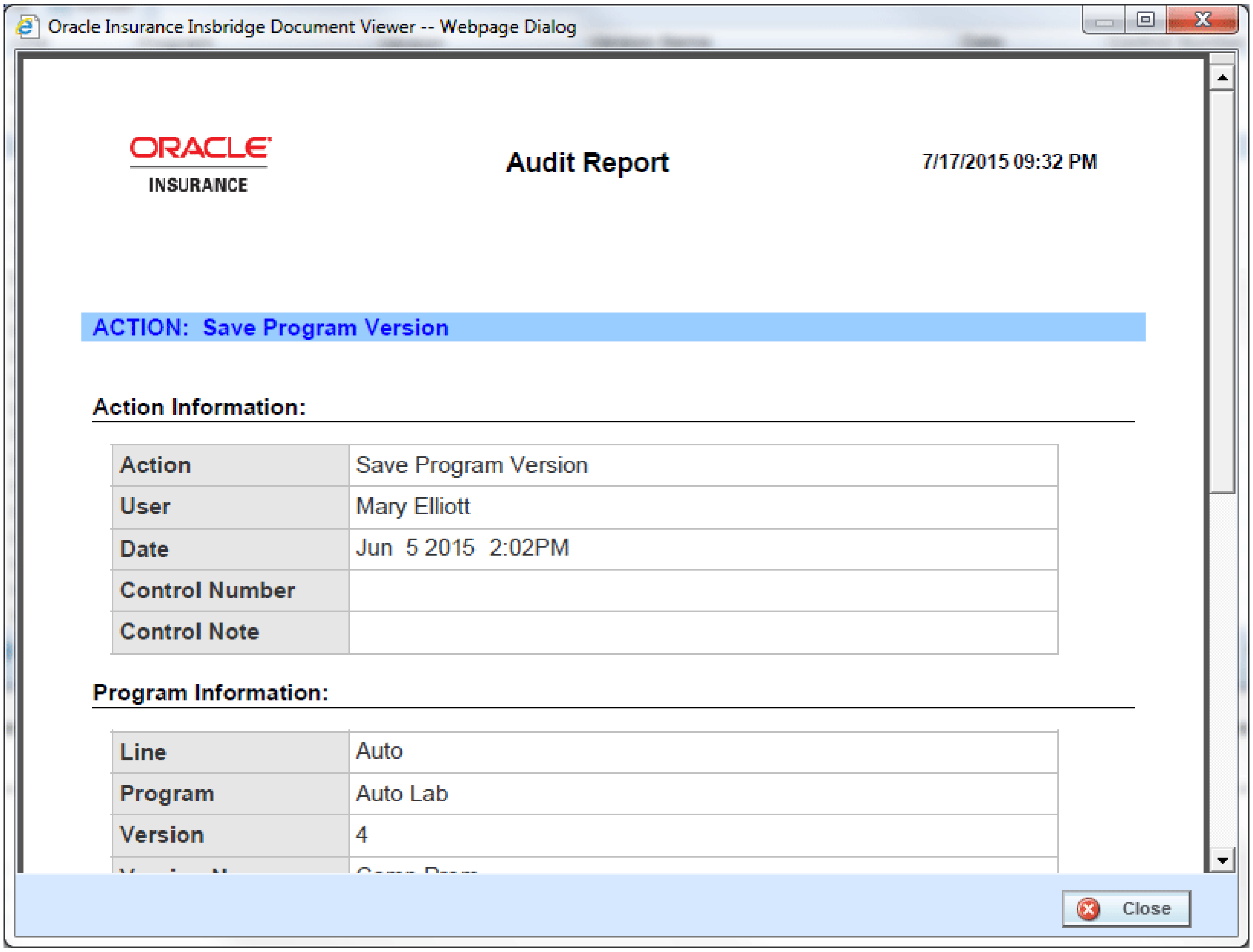
Figure 5 Audit Tab

AUDIT REPORT

An audit report for all audit logs currently displayed on all pages by filter criteria can be produced. If you want an Audit Report for all audit logs, make sure the filter has been cleared. If you want an audit report for a specific type of audit log, make sure to filter by those criteria. For Example, if you want the audit logs from a particular day forward, then enter that day in the From Date on the Filter. All the audits from that day and forward will be listed. The audit report is a maximum of 15 pages.

Report Details

The report contains details for each of the audit logs included, starting with the newest. Each log has action information, defining the action taken, the user, and the date. Program information, such as LOB, program, program version, and program ID, may be included. If applicable, element/item information including description, revision and ID may be included.


Oracle Insurance Insbridge Document Viewer -- Webpage Dialog
ORACLE
INSURANCE
Close

Audit Report

7/17/2015 09:32 PM

ACTION: Save Program Version

Action Information:

Action	Save Program Version
User	Mary Elliott
Date	Jun 5 2015 2:02PM
Control Number	
Control Note	

Program Information:

Line	Auto
Program	Auto Lab
Version	4

Figure 6 Audit Report

IBSS

Access to IBSS requires a username and password combination. Administrators can set options to get the level of auditing and logs desired.

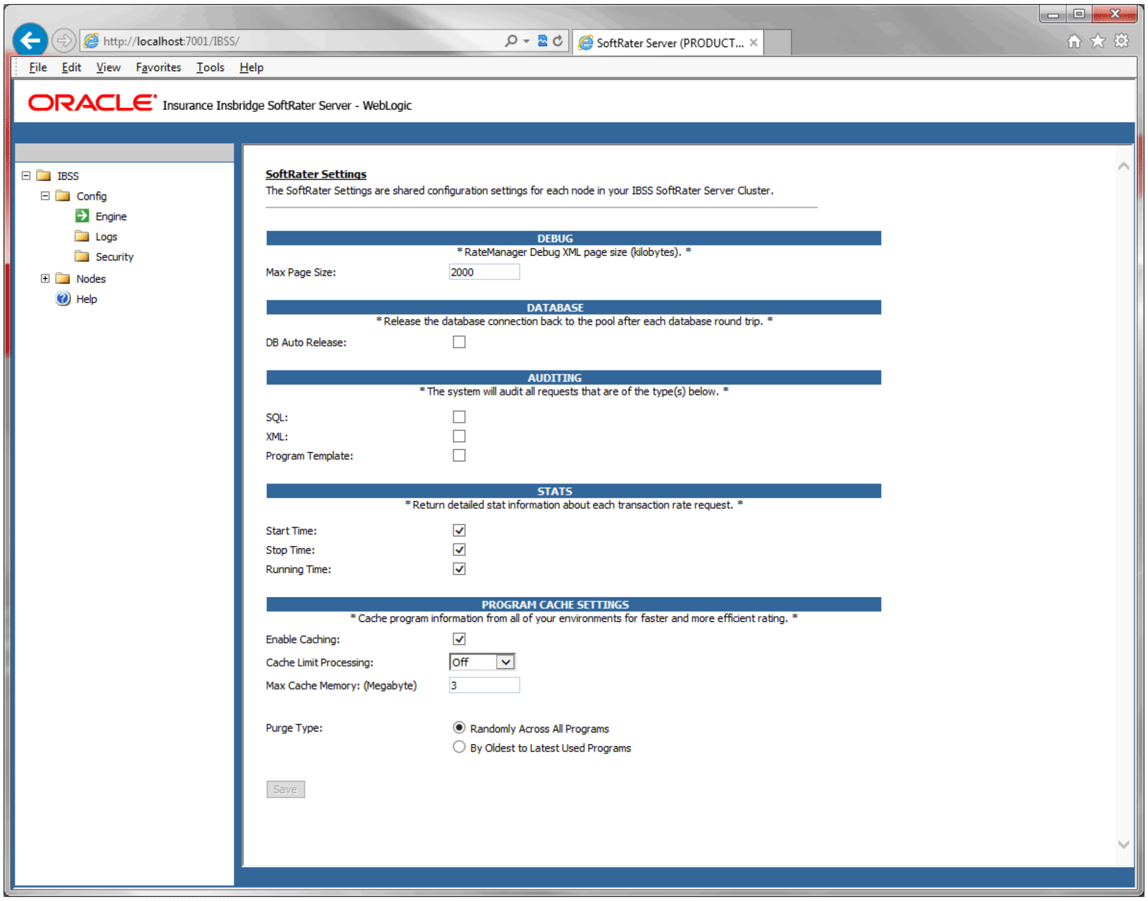
Auditing

Allows you to select what information should be logged for each transaction. These options should typically be left unchecked, unless directed to check them by a member of the Oracle Insurance Support team. Leaving auditing on may result in exceptionally large log files.

SQL: The SQL script that was executed. If this option is not selected, this information will still be logged if an error occurs.

XML: The XML that was used. If this option is not selected, this information will still be logged if an error occurs.

Program Template: Provides an XML view of the entire program that was executed. This information is used to help Oracle Insurance determine why a program is not rating correctly.


http://localhost:7001/IBSS/
SoftRater Server (PRODUCT...
File
Edit
View
Favorites
Tools
Help
ORACLE
Insurance Insbridge SoftRater Server - WebLogic
IBSS
Config
Engine
Logs
Security
Nodes
Help
Save

SoftRater Settings

The SoftRater Settings are shared configuration settings for each node in your IBSS SoftRater Server Cluster.

DEBUG

* RateManager Debug XML page size (kilobytes). *

Max Page Size: 2000

DATABASE

* Release the database connection back to the pool after each database round trip. *

DB Auto Release: □

AUDITING

* The system will audit all requests that are of the type(s) below. *

SQL: □
XML: □
Program Template: □

STATS

* Return detailed stat information about each transaction rate request. *

Start Time: ☑
Stop Time: ☑
Running Time: ☑

PROGRAM CACHE SETTINGS

* Cache program information from all of your environments for faster and more efficient rating. *

Enable Caching: ☑
Cache Limit Processing: Off
Max Cache Memory: (Megabyte) 3

Purge Type: ● Randomly Across All Programs
○ By Oldest to Latest Used Programs

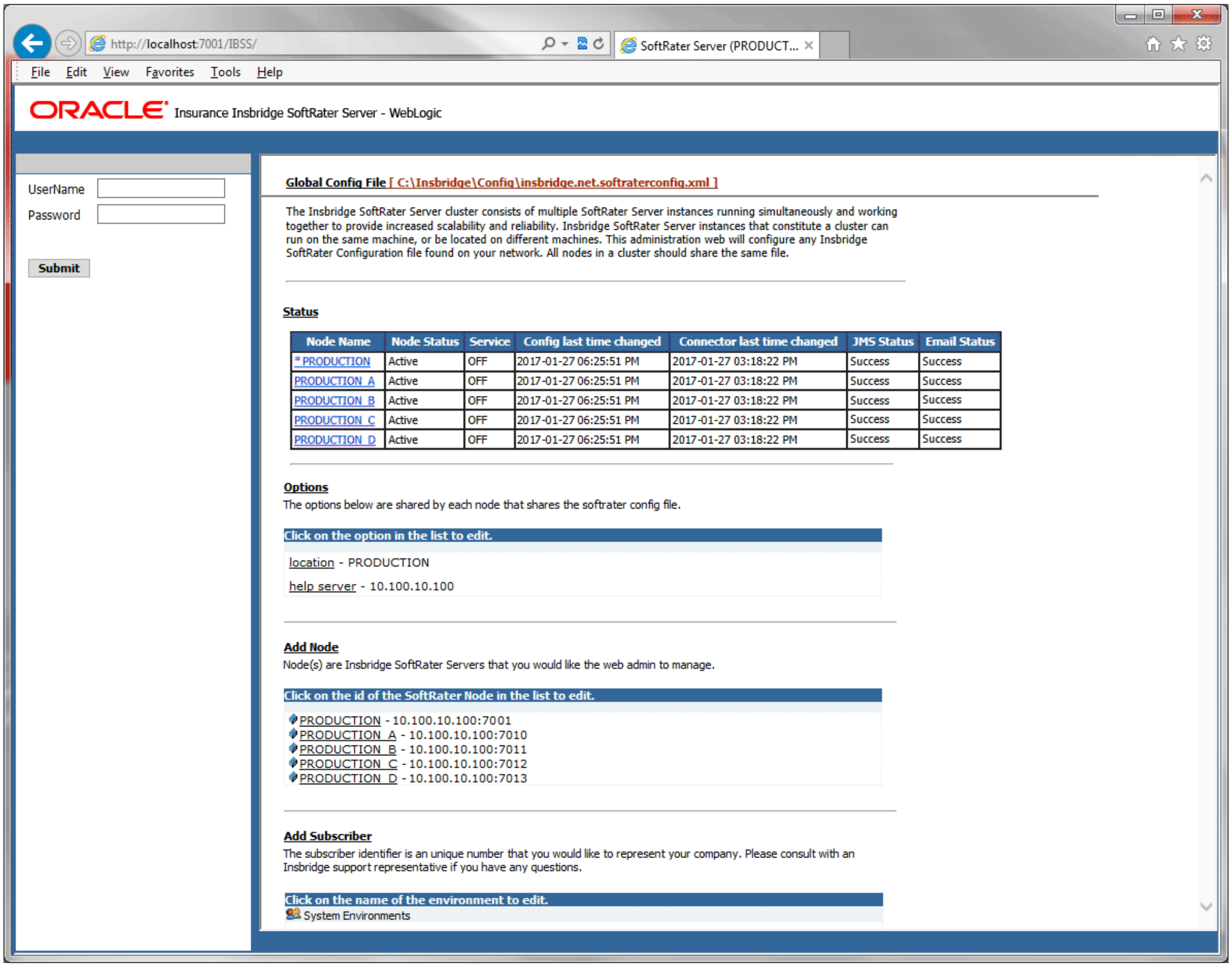
Figure 7 IBSS Engine Page

SECURITY

The security page is where the administrator can turn on or turn off authentication for IBSS. The default is for security to be on. Security is enabled at installation but can be disabled at a later time. When security is enabled, a login and password will be required. If users do not have a login and password, no section of IBSS will be available to them. If security is disabled, at the next instance of IBSS, no login screen is presented.

Security Enabled

Security is enabled by default; users are presented with a login screen. A user name and password must be entered to gain access. Information regarding the status of the system is presented but will not be accessible. The default is for security to be enabled.



http://localhost:7001/IBSS/
SoftRater Server (PRODUCT...
File Edit View Favorites Tools Help
ORACLE Insurance Insbridge SoftRater Server - WebLogic
UserName
Password
Submit

Global Config File [C:\Insbridge\Config\insbridge.net.softraterconfig.xml]

The Insbridge SoftRater Server cluster consists of multiple SoftRater Server instances running simultaneously and working together to provide increased scalability and reliability. Insbridge SoftRater Server instances that constitute a cluster can run on the same machine, or be located on different machines. This administration web will configure any Insbridge SoftRater Configuration file found on your network. All nodes in a cluster should share the same file.

Status

Node Name	Node Status	Service	Config last time changed	Connector last time changed	JMS Status	Email Status
* PRODUCTION	Active	OFF	2017-01-27 06:25:51 PM	2017-01-27 03:18:22 PM	Success	Success
PRODUCTION_A	Active	OFF	2017-01-27 06:25:51 PM	2017-01-27 03:18:22 PM	Success	Success
PRODUCTION_B	Active	OFF	2017-01-27 06:25:51 PM	2017-01-27 03:18:22 PM	Success	Success
PRODUCTION_C	Active	OFF	2017-01-27 06:25:51 PM	2017-01-27 03:18:22 PM	Success	Success
PRODUCTION_D	Active	OFF	2017-01-27 06:25:51 PM	2017-01-27 03:18:22 PM	Success	Success

Options

The options below are shared by each node that shares the softrater config file.

Click on the option in the list to edit.

location - PRODUCTION

help server - 10.100.10.100

Add Node

Node(s) are Insbridge SoftRater Servers that you would like the web admin to manage.

Click on the id of the SoftRater Node in the list to edit.

PRODUCTION - 10.100.10.100:7001
PRODUCTION_A - 10.100.10.100:7010
PRODUCTION_B - 10.100.10.100:7011
PRODUCTION_C - 10.100.10.100:7012
PRODUCTION_D - 10.100.10.100:7013

Add Subscriber

The subscriber identifier is an unique number that you would like to represent your company. Please consult with an Insbridge support representative if you have any questions.

Click on the name of the environment to edit.

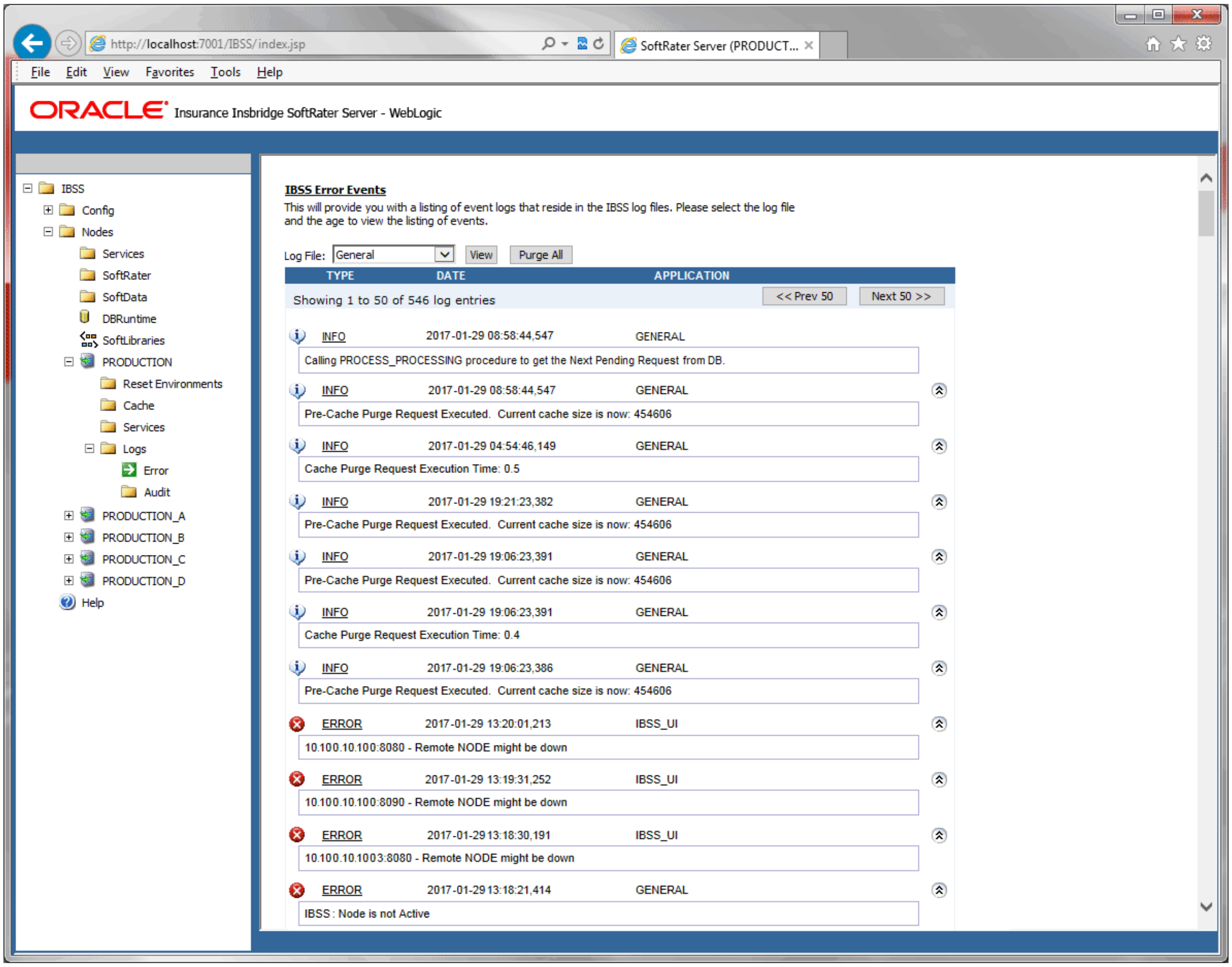
System Environments

Figure 8 Security Enabled in IBSS

When Security is enabled, a default user “admin” with a default password of “insbridge” is assigned. This is the user name and password to be used the first time you enter IBSS. It is strongly recommended that the password be updated at the first log in.

Logs

There are two Logs pages. One is for errors and one is for audits. Both pages show a listing of the logs available. By default, information is only logged when an error occurs. Audit logs must be enabled. This can be done on the Config->Engine page.



IBSS Error Events

This will provide you with a listing of event logs that reside in the IBSS log files. Please select the log file and the age to view the listing of events.

Log File: General

```
TYPE        DATE                        APPLICATION
Showing 1 to 50 of 546 log entries

INFO        2017-01-29 08:58:44,547     GENERAL
Calling PROCESS_PROCESSING procedure to get the Next Pending Request from DB.
INFO        2017-01-29 08:58:44,547     GENERAL
Pre-Cache Purge Request Executed.  Current cache size is now: 454606
INFO        2017-01-29 04:54:46,149     GENERAL
Cache Purge Request Execution Time: 0.5
INFO        2017-01-29 19:21:23,382     GENERAL
Pre-Cache Purge Request Executed.  Current cache size is now: 454606
INFO        2017-01-29 19:06:23,391     GENERAL
Pre-Cache Purge Request Executed.  Current cache size is now: 454606
INFO        2017-01-29 19:06:23,391     GENERAL
Cache Purge Request Execution Time: 0.4
INFO        2017-01-29 19:06:23,386     GENERAL
Pre-Cache Purge Request Executed.  Current cache size is now: 454606
ERROR       2017-01-29 13:20:01,213     IBSS_UI
10.100.10.100:8080 - Remote NODE might be down
ERROR       2017-01-29 13:19:31,252     IBSS_UI
10.100.10.100:8090 - Remote NODE might be down
ERROR       2017-01-29 13:18:30,191     IBSS_UI
10.100.10.1003:8080 - Remote NODE might be down
ERROR       2017-01-29 13:18:21,414     GENERAL
IBSS : Node is not Active
```

Figure 9 Error Logs Page

Error Logs

Errors get logged whenever the application encounters an exception. The exception can be with the request execution, the request itself, or with the properties configuration. Details regarding the exception can be found in the error logs.

General: General error message logs.

Batch: Error logs for batch files.

Impact Analysis: Error logs for Impact Analysis.

Batch Import/Export: Error logs for batch imports and exports.

Audit Logs

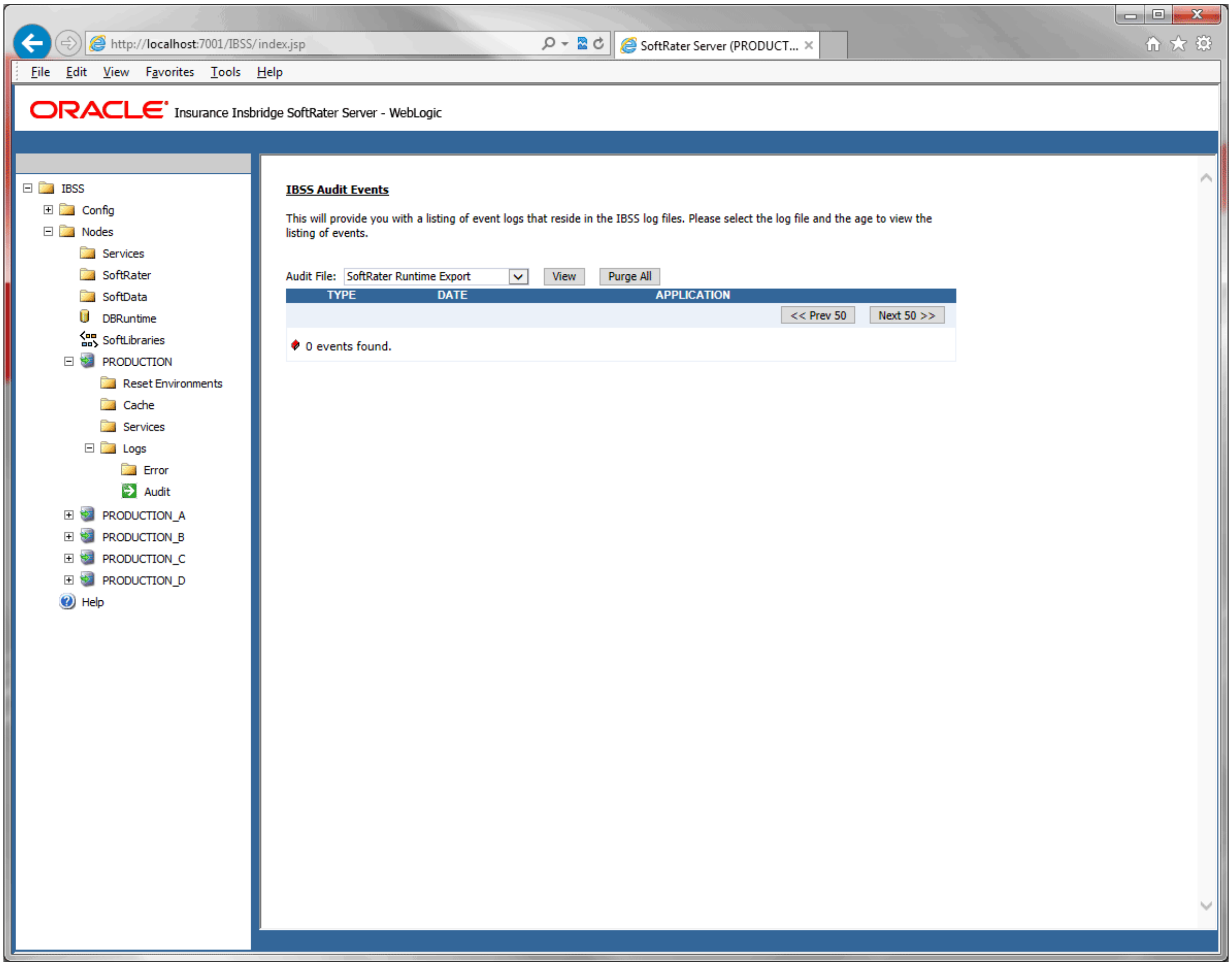
Audit logs are used for tracking the SoftRater engine operations. The Audit logs contain information about the Engine categorized into three different operations, XML, SQL, and SoftRater Runtime Export.

XML: Operational XML that triggered some exception processing.

SQL: SQL text that has generated some exception processing.

SoftRater Runtime Export: Provides an XML view of the entire program that was executed.

To view an error log, click the hyperlink. The log will be returned in the text area at the bottom of the screen. If auditing has not been turned on, there will not be any audit logs displayed. To turn audit logging on, please go to the Config->Engine page.



IBSS Audit Events

This will provide you with a listing of event logs that reside in the IBSS log files. Please select the log file and the age to view the listing of events.

Audit File: SoftRater Runtime Export

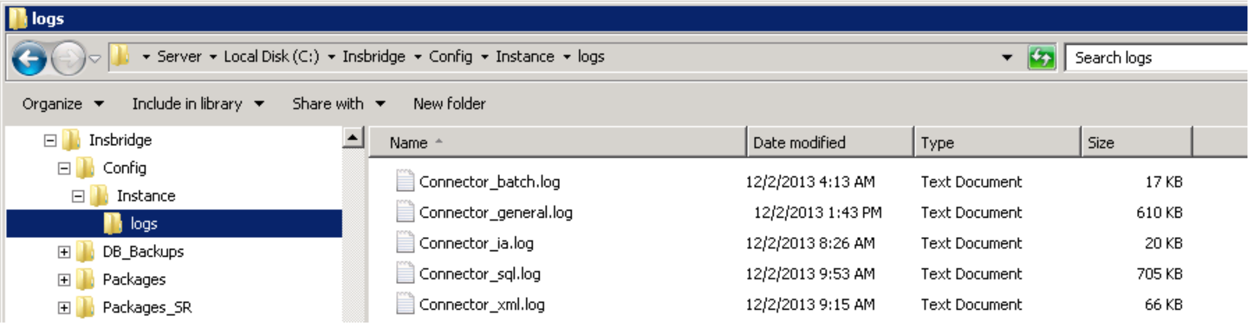
TYPE	DATE	APPLICATION

0 events found.

Figure 10 Audit Logs

Viewing Logs on the Server

If you have access to the server where IBSS was deployed, you can view log files in the Instance folder of the node. Each node has an instance folder where logs are stored. The location of the Instance folder was determined at installation time.



Name	Date modified	Type	Size
Connector_batch.log	12/2/2013 4:13 AM	Text Document	17 KB
Connector_general.log	12/2/2013 1:43 PM	Text Document	610 KB
Connector_ia.log	12/2/2013 8:26 AM	Text Document	20 KB
Connector_sql.log	12/2/2013 9:53 AM	Text Document	705 KB
Connector_xml.log	12/2/2013 9:15 AM	Text Document	66 KB

Figure 11 Logs stored on the Server

These are the logging options available and a description of what is being logged in the Instance file.

- **Connector_batch.log:** This is the error plus information log for batches.
- **Connector_general.log:** This is the error plus information log. All errors, warnings, requests, results, and such are logged here. Any SoftRater exceptions are logged here also.
- **Connector_ia.log:** This is the error plus information log for Impact Analysis.
- **Connector_sql.log:** This log records all database queries sent by SoftRater, including table variable lookup, and global versioning selection.
- **Connector_xml.log:** This log records all the rating request and result XMLs. The SoftRater.xml log only logs the rating request XML submitted to a SoftRater instance for both synchronous and batch rating requests. At the point a rating request makes it to SoftRater, the request does not distinguish between the two, since the IBFA Spindle web service is what handles the threading of the requests and the aggregation of the results

If XML Audit Logging option is enabled, it contains both <rate> and <result> nodes, so it logs both the request XML and the result XML.

WEB SERVICES SECURITY

Securing IBFA Web Services

Locking down IBFA web services is done by locking down the web. This relies on Microsoft Internet Information Services (IIS) to provide authenticated users. All methods supported by IIS are permitted.

When using IIS, the provider module uses the authenticated identity passed in from IIS. IIS authenticates the identity using basic, digest, integrated Windows authentication or some combination of these. You can use impersonation and NTFS ACL permissions to restrict or allow access to protected resources.

If you select to use Windows authentication:

1. Go to IIS and disable anonymous access for IBFA.
2. Turn Windows authentication on.
3. Enter the SoftRater Explorer and change the Intranet Credentials to the windows account that is to be used.

Securing IBSS Web Services Using SOAP

Insbridge uses JAS-WS for implementing Web Services. For securing web services, WS-Security standards are used to perform authentication and authorization against Insbridge user accounts. The SOAP header contains the appropriate Security credentials. The password can be sent as a Digest or as a Text.

The SOAP header with WS-Security would look like the following when the Password Digest is used:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Header>
      <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <wsse:UsernameToken wsu:Id="UsernameToken-1" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
            <wsse:Username>username</wsse:Username>
            <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordDigest">passwordencrypted</wsse:Password>
            <wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary">kC5eI6iq8x17/qA3mzs6/g==</wsse:Nonce>
            <wsu:Created>2010-03-22T14:12:34.223Z</wsu:Created>
         </wsse:UsernameToken>
      </wsse:Security>
   </soapenv:Header>
```

For more information on the WS Security standard please refer to the website: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

By default web services should be secure.

USING COOKIES IN INSBRIDGE APPLICATION

The Insbridge application is accessed by users through Internet Explorer. Because Insbridge uses session cookies to manage user sessions, cookies must be enabled in the Internet Explorer browser. To allow using cookies in Internet Explorer, open the Privacy tab of the Internet Options dialog, then choose the Sites popup dialog and add the Insbridge server address to the list of Allowed sites.

The *JSESSIONID* session cookie contains session ID generated for a user to manage data associated with the user's session. A unique session ID is generated when a user successfully logs into the Insbridge application. The session ID is generated by the J2EE web server and passed to a browser as a non-persistent cookie. The browser retains it for the duration of the session, and deletes it when the user logs out or the session times out. During a session, when a browser issues a request back to the application server, it sends the session cookie in the HTTP header of the request. Requests that do not contain valid session IDs are not processed by the server.

The *ice.sessions* cookie is generated by the IceFaces library used by Insbridge to implement the user interface. The cookie is a session-scope cookie and used by IceFaces to maintain IceFaces user session.

Cookie Names for RateManager user sessions are:

- RM4CUSER
- Insbridge.NET.RM4
- rm4roles_550_9

ENCRYPTION ALGORITHMS

Insbridge allows configurable algorithms by allowing new keys per subscriber, using the following:

1. Symmetric (IBFA)
    a. DES (The best known algorithm is the U.S. Department of Defense's Data Encryption Standard (DES))

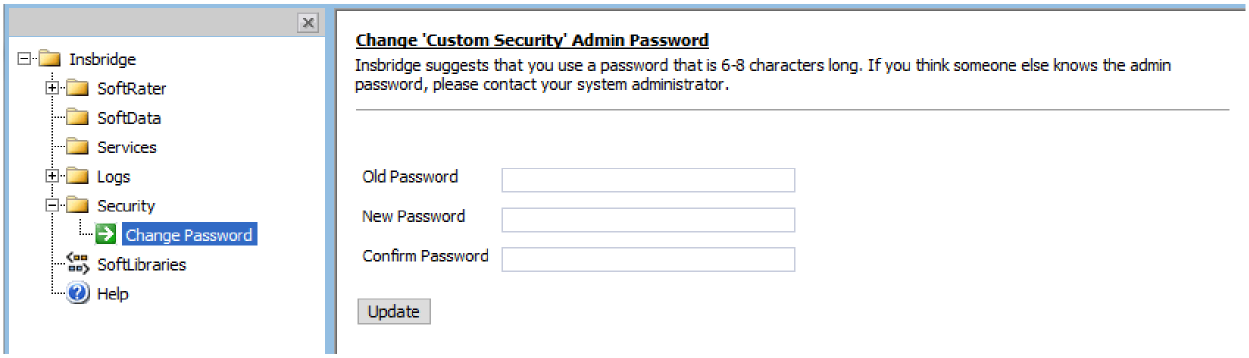
2. Asymmetric (IBFA)
    a. This is the public/private key usage for packaging. We use AES with DPAPI.

3. Hashing (IBSS)

Security Best Practices

Insbridge has recommended best practices for installing and running the Insbridge system.

- It is recommended that the databases be on separate machines from the applications due to performance and security issues.
- It is recommended that you download and read the Installation and user guides.
- It is recommended that you change your password periodically
- It is strongly recommended that any database modification be performed by a qualified database administrator (DBA).
- For IBFA, it is recommended that you change the password immediately.



Change 'Custom Security' Admin Password

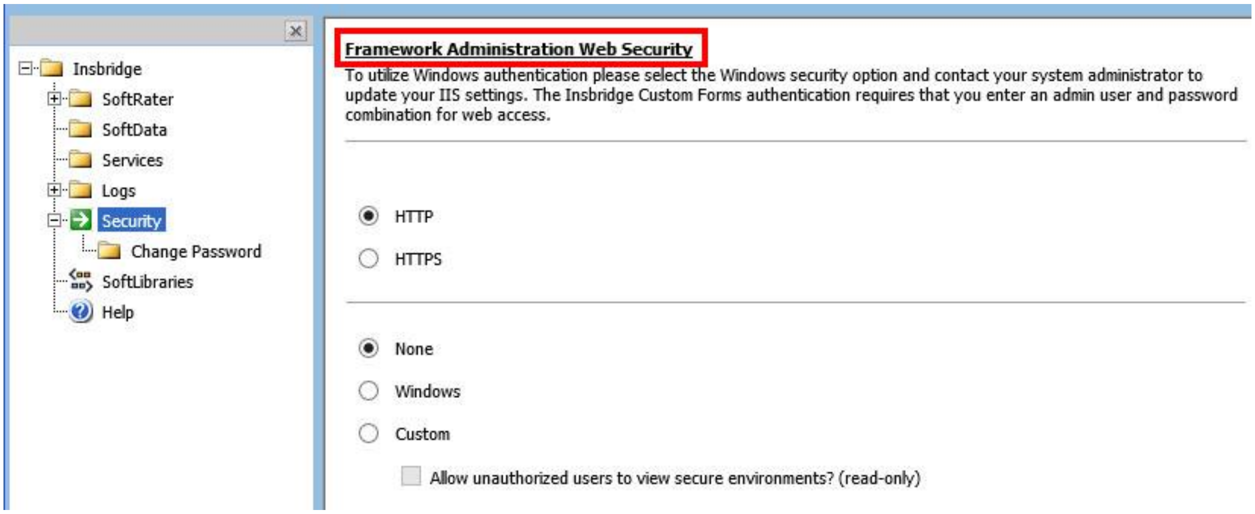
Insbridge suggests that you use a password that is 6-8 characters long. If you think someone else knows the admin password, please contact your system administrator.

Old Password

New Password

Confirm Password

- It is recommended that you have security enabled on IBFA. You can choose from None, Windows and Custom security.
- If using HTTPS, select the HTTPS protocol.



Framework Administration Web Security

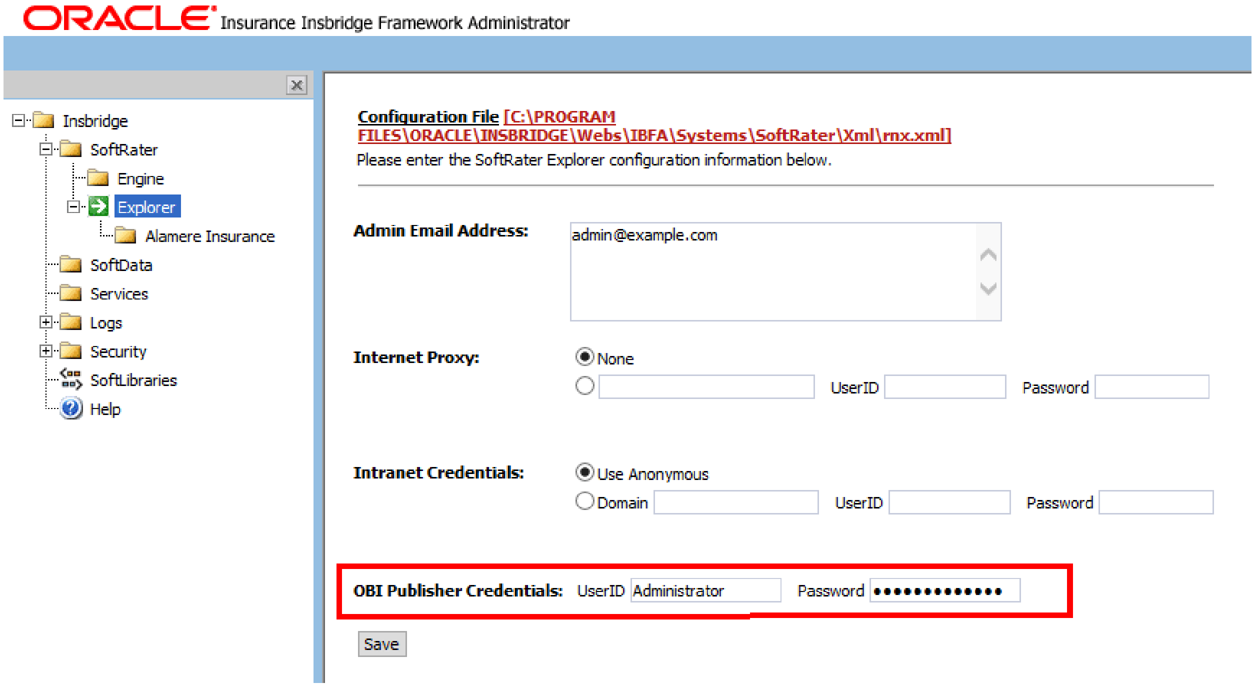
To utilize Windows authentication please select the Windows security option and contact your system administrator to update your IIS settings. The Insbridge Custom Forms authentication requires that you enter an admin user and password combination for web access.

● HTTP
○ HTTPS

● None
○ Windows
○ Custom

□ Allow unauthorized users to view secure environments? (read-only)

- The OBI Publisher requires a User ID and password to be entered in IBFA. OBI is required to create certain reports in RateManager. The username and password must match the entry in OBI.



Configuration File [C:\PROGRAM FILES\ORACLE\INSBRIDGE\Webs\IBFA\Systems\SoftRater\Xml\rnx.xml]

Please enter the SoftRater Explorer configuration information below.

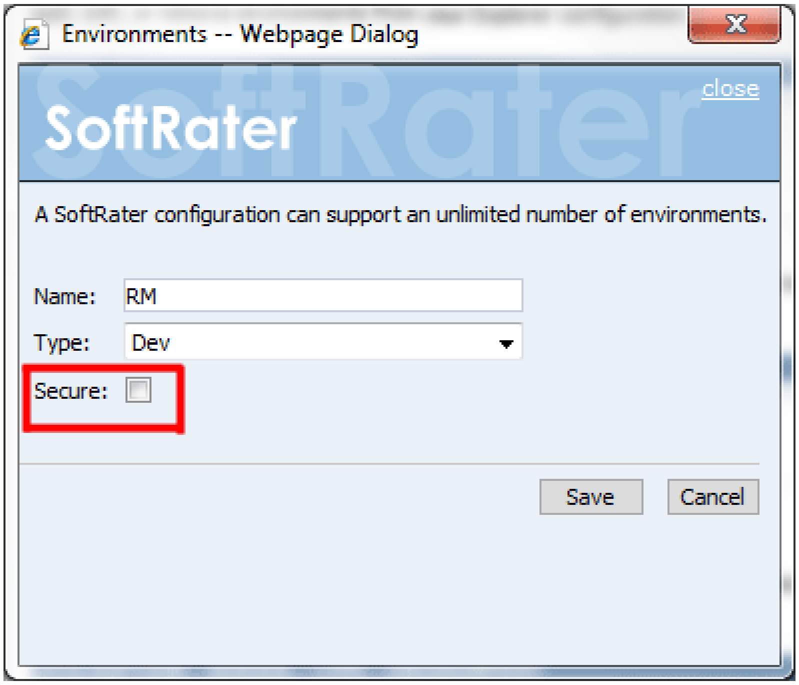
Admin Email Address: admin@example.com

Internet Proxy: ● None ○ UserID Password

Intranet Credentials: ● Use Anonymous ○ Domain UserID Password

OBI Publisher Credentials: UserID Administrator Password ••••••••••••••

- In IBFA if you want to make the new environment secure, check the box next to Secure. A secure environment will be available to users who are logged into the Framework Administrator only.



A SoftRater configuration can support an unlimited number of environments.

Name: RM

Type: Dev

Secure: □

- The recommended way to update a database is directly from RateManager. This is also more secure as the script files are not accessible and less prone to being modified.

- Prior to users accessing RateManager for the first time, it is recommended that Preferences be set. Only administrators can edit system settings from the Preferences option in RateManager. Tools → Preferences

- Remember to set the ‘Minimum Login User ID’ Length field. This is the minimum number of characters required for a user ID.

- Remember to set the User must change password field. This where you set the number of days before a user is required to change his/her password.

- To safeguard against unwarranted revisions of elements being created, and to have an audit of such revisions, change control can be switched on. If change control is on, it is mandatory for users to enter a change control entry and justification to any element or program when it is revisioned.

ADDITIONAL SOURCES OF SECURITY INFORMATION

In addition to securing the Insbridge application, all infrastructure resources – Linux/Windows servers, J2EE application and database servers – that comprise an Insbridge environment must be secured. The following list of links should be helpful while planning how to lockdown the Insbridge environment.

Oracle 11g Database

http://download.oracle.com/docs/cd/E11882_01/network.112/e16543/toc.htm
http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/toc.htm
http://download.oracle.com/docs/cd/E11882_01/network.112/e10744/toc.htm

Oracle 12 c Database

https://docs.oracle.com/database/121/DBSEG/title.htm

Microsoft SQL Server 2012 and 2016 Database

https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server

IBM DB2 11.1 Database

ftp://ftp.software.ibm.com/ps/products/db2/info/vr95/pdf/en_US/db2sece950.pdf

Microsoft Windows 2008 Server

http://www.microsoft.com/download/en/details.aspx?id=17606

Oracle WebLogic 12.1.3 J2EE Application Server

http://docs.oracle.com/middleware/1213/wls/wls-secure.htm

Oracle WebLogic 12.2.1 J2EE Application Server

https://docs.oracle.com/middleware/1221/wls/SECMG/toc.htm

JBoss EAP 7.0 FINAL Application Server

https://access.redhat.com/documentation/en-us/red_hat_jboss_enterprise_application_platform/7.0/html-single/how_to_configure_server_security/

IBM WebSphere 11.1 Application Server

https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.admin.sec.doc/doc/c0021804.html