FORUM SYSTEMS™
MANAGING & ACCELERATING XML WEB SERVICES SECURITY

FORUM SENTRY BEST PRACTICES

USING DATABASES WITH FORUM SENTRY

FORUM SYSTEMS

A Crosscheck Networks Company

Forum Systems Sentry™ Using Databases with Forum Sentry

D-ASF-SE-010029

Contents

INTRODUCTION

Scope of this Document

This document is intended to provide an outline of the various features of Forum Sentry that make use of an external database, which Sentry connects to using Data Source Policies.

Additional Documentation

For more details on using databases with Forum Sentry, review the “FS Sentry v8 Logging Guide” and the “FS Sentry v8 Task Management Guide”.

Much of the information in this Best Practices Guide is taken from these documents.

Platforms

The use case can be implemented using any of the following available Forum Sentry form factors:

 FIPS 140-2 Hardware	Powered By GNU/Linux	solaris	Microsoft Windows xp	vm	CLOUD COMPUTING
✓	✓	✓	✓	✓	✓

Data Source Policies in Forum Sentry

In previous releases the Data Sources screen was titled Archiving. The Data Sources screen allows users to set up multiple JDBC connections (data sources) for archiving. Users may create, enable or disable a data source policy, edit data source settings, upgrade database drivers and view sample data for their data sources.

Supported Databases

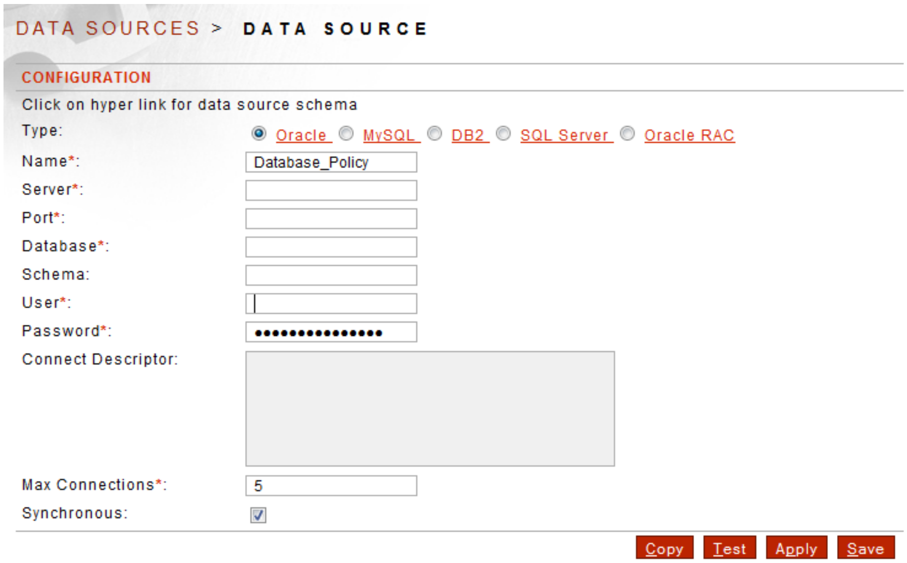
The system supports Oracle 9i, 10g, 11g, and 10g Real Application Cluster (RAC), MySQL, 4 and 5, DB2 7.2 and Microsoft SQL Server 2005/2008 databases. Support for the DB2 8.1 databases is available as a patch upgrade. It is possible that Sentry will work with newer versions of these databases, contact Forum Systems support for the latest information.

Forum Systems provides SQL scripts to create Oracle, MySQL, DB2 or SQL Server database tables and users for archiving, available by selecting the linked database name. These SQL scripts, accessible by selecting the database name link, are intended to be run by a user with enough privileges to create users, tables and sequences.

Creating Data Sources in Sentry

Before creating your Data Source, confirm that you have:

- Database name
- Database port
- Created a database schema (for DB2 and Oracle databases only)
- Database schema name (for DB2 and Oracle databases only)
- Database user name and password



DATA SOURCES > DATA SOURCE

CONFIGURATION

Click on hyper link for data source schema

Type:	● Oracle ○ MySQL ○ DB2 ○ SQL Server ○ Oracle RAC
Name*:	Database_Policy
Server*:	
Port*:	
Database*:	
Schema:	
User*:	
Password*:	•••••••••••••••
Connect Descriptor:	
Max Connections*:	5
Synchronous:	☑

Sentry Features Utilizing Data Source Policies

WS Reports

Forum Sentry can store statistical information in an external database, using a Data Source policy for the purpose of generating WS Reports.

The types of reports available include:

- Number of Hits
- Throughput
- Request Size
- Response Size
- Response Time
- Number of Faults

Archiving Request and Response Documents Globally

As part of the WS Reporting functionality in Sentry, administrators can set a global option (for all policies) to archive all request and response messages that come through the system. The same Data Source policy that is used for WS Reports is used for this global request/response archiving option.

Archive Document Task

Administrators can configure the Archive Document task to archive entire XML documents or select elements of an XML document to an external database, using a Data Source policy. The tasks can be applied on individual policies, making this a more granular approach to simply archiving all request/response documents with the WS Reports option.

Log Archiving

The logging information that is kept locally on the Sentry machine (appliance or host OS) can also be written off of the system via Remote Syslog policies or to an external database using a Data Source policy.

Query Database Task

The Query Data Source task is used to run queries against target databases and use the results for mapping to other locations or to build XML documents automatically. The Query Database Task was previously named “Query Data Source” and requires a Data Source Policy to connect to the database.

Sentry Policy and Configuration Management

As part of Sentry’s Global Device Management (GDM) functionality, administrators can export and import Sentry configurations to/from an external database using a Data Source Policy. This functionality supports both partial and full Sentry configurations files (FSX and FSG). There is also an automated routine with the Forum Sentry Appliances for backing up the full (FSX) configuration nightly to a database. Configurations that are stored in the database can easily be retrieved from any Sentry instance that has access to the database and diffs can be run on the various policies stored in the database.

IDP Quarantining

With Custom IDP Actions there are some Auditing options, including the ability to quarantine a document to a database, using a Data Source Policy.

Session Management

Forum Sentry has the ability to set and consume session headers (cookies). When using multiple Sentry instances behind a load balancer, this session validation needs to be stateful as the client request can go through multiple Sentry instances. Sentry stores the session information in a database, using a Data Source policy.

Conclusion

There are many features of Forum Sentry that utilize external databases. Sentry uses Data Source Policies to connect to these external databases.

Databases are used to store statistical information for reporting purposes and they are used for archiving/storing messages passed through Sentry. Custom work flows and message processing tasks can be achieved by making a database call while processing a message in Sentry. Configuration management is greatly improved with the ability to store and retrieve Sentry policies in a database. Setting and validating session cookies using multiple Sentry instances calls for a stateful approach where a database is required to store the session information.

The vast majority of the mature SOA environments that utilize the Forum Sentry products use at least some of the features requiring access to an external database.

About Forum Systems

Forum Systems, a wholly owned subsidiary of Crosscheck Networks, Inc., is a leader in Service Oriented Architecture (SOA) and secure service mediation. Through comprehensive Threat mitigation and Trust enablement, Forum's family of hardware, software, and cloud-based instances provides enterprises and government organizations with the foundation for achieving secure service mediation. Processing more than one billion transactions per day worldwide, the FIPS- and DoD-certified Forum products offer the industry's most comprehensive protection against XML- and SOAP-based vulnerabilities. Forum Sentry has been issued an industry-first patent (7,516,333) for XML security functions such as XML Encryption, XML Decryption, and XML Signatures using a network appliance. For more information, please visit www.forumsys.com.