



FORUM SENTRY BEST PRACTICES

USING DATABASES WITH FORUM SENTRY

Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Using Databases with Forum Sentry

D-ASF-SE-310684



Contents

INTRODUCTION.....	4
<i>Scope of this Document</i>	4
<i>Additional Documentation</i>	4
Data Source Policies in Forum Sentry	5
<i>Supported Databases</i>	5
<i>Creating Data Sources in Sentry</i>	5
Sentry Features Utilizing Data Source Policies	6
<i>Custom Identity Policy</i>	6
<i>Query Database</i>	6
<i>Archiving Request and Response Documents Globally</i>	6
<i>Archive Document Task</i>	6
<i>Log Archiving</i>	6
<i>Query Database Task</i>	6
<i>Sentry Policy and Configuration Management</i>	6
<i>IDP Quarantining</i>	7
<i>Session Management</i>	7
<i>WS Reports</i>	7
Conclusion.....	7
About Forum Systems.....	8



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 v8.5 Logging Guide” and the “FS Sentry v8.5 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:

 HARDWARE	Hardware	ForumOS™. FIPS 140-2 Level II purpose-built chassis. NIAP NDPP Certified. Patented cryptographic acceleration
 OVA IMAGE	VMware	Fully encapsulated virtualized rendition of Hardware system in a deployable OVA VMware image
 AMI IMAGE	Amazon	Fully encapsulated virtualized rendition of Hardware system in a deployable Amazon AMI
 AZURE IMAGE	Azure	Fully encapsulated virtualized rendition of Hardware system in a deployable MS Azure Image
 docker	Docker	Dockerized containers for Linux deployments for use on generic Linux systems or the hardened Forum Systems Linux Kernel
 WINDOWS LINUX	Software	Windows or Linux software provided via single-package install with no dependencies.

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*:

Enable SSL: ☐

SSL initiation policy:

Server*:

Port*:

Database*:

Schema:

User*:

Password*:

Connect Descriptor:

Max Connections*:

Synchronous: ☒

[Test](#) [Apply](#) [Save](#)

Sentry Features Utilizing Data Source Policies

Custom Identity Policy

The Custom identity policy enables the use of a Task List Group to define the credential authentication type. This fully extensible authentication adapter is commonly used to access user credential information stored in database tables. The “Query Database Task” is subsequently used in the associated Task List Group which defines the SQL queries and attribute mappings that occur to authenticate users via a database.

Query Database

The Query Database task allow you to use database queries to store or retrieve information from a database in order to map to attributes, use for runtime decisions, add role information for a user, lookup a value based on a dynamic session variable, and many other use cases. The Query Database task references a Data Source policy as the means to communicate with the applicable database.

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.

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

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 is the global leader in API and Cloud Security technology with industry-certified and patented products that secure enterprise infrastructure. Forum Systems has been an industry leader since 2002 and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Our security-first mindset enables trusted, network edge deployments for protecting critical enterprise transactions.

Forum Systems supports enterprise customers across commercial, government, and military sectors. Forum Systems technology provides leading-edge security with identity and SSO features that enable out-of-the box business solutions with code-free configuration. For more information, please visit www.forumsys.com.