FORUM SYSTEMS™

MANAGING & ACCELERATING XML WEB SERVICES SECURITY

FORUM SYSTEMS HANDS-ON TRAINING

LAB 17. SENTRY CONFIGURATION STORAGE

FORUMSYSTEMS

A Crosscheck Networks Company

Legal Marks

Published: September 2014
Forum Systems Hands-on Training – Lab 17. Sentry Configuration Storage
D-ASF-SE-010029

Contents

Introduction

Lab 17. Sentry Configuration Storage

Skill Level

This lab is beginner skill level. Little to no prior experience with Forum Sentry or SOAPSonar is required.

Prerequisites

This lab requires the Forum Sentry Training Image, with a licensed copy Sentry and SOAPSonar.

Refer to the “FS_Training_Labs_v8-1_Introduction” document for information on the Forum Sentry Training Image and licensing SOAPSonar Enterprise Edition.

Lab Overview

All of the policies built in Sentry can be exported as files. This is useful for backup, policy propagation, and versioning of Sentry policies.

Full Sentry configurations (all policies) are saved as FSX files. Partial Sentry configurations (e.g. REST policy, a key pair, a Task List, etc..) are saved as FSG files. Both file types are password encrypted files that can only be read by Sentry. These cannot be edited or modified manually.

In addition to exporting configuration files to disk, Sentry administrators can also export directly to a database. Using a central database as a repository for Sentry configurations across several Sentry instances is recommended.

The Sentry configurations stored in the database can be viewed and compared to each other through the Sentry WebAdmin interface. These configurations can also be imported from the database.

In addition to manually exporting a configuration file, Sentry can be configured to automatically export the full configuration (FSX) to a database daily.

In this lab you will enable centralized storage of the Sentry configuration files and configure the automatic daily backup to the database.

This lab will provide instructions for centralized configuration storage in Forum Sentry. Topics will include:

1. Data Sources
2. Exporting Sentry Policies
3. Importing Sentry Policies
4. Automated Configuration Backup

Data Source Configuration

Data Sources in Sentry define how to access an external database. Sentry supports MySQL, Oracle, DB2, and SQL Server databases. The schema files required to build the correct database tables are available through the Sentry WebAdmin interface on the Data Sources screen.

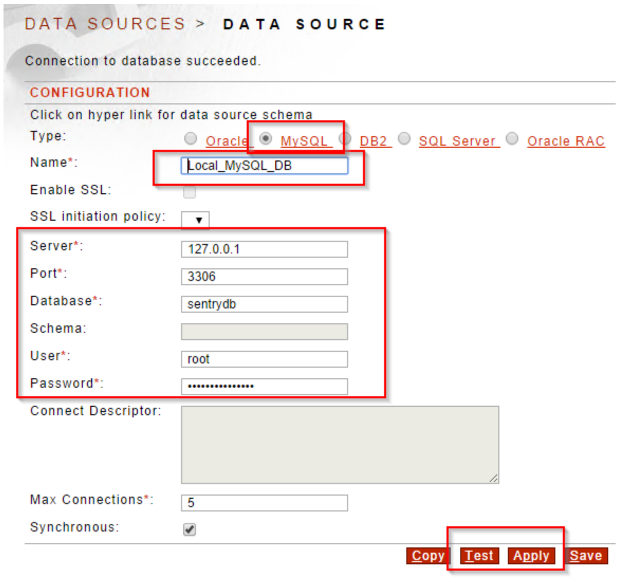
The Sentry Training Lab has MySQL pre-installed, with the Sentry schema already applied. We will build a Data Source to connect to this local database.

In this step you'll build a Data Source in Sentry.

Building a Data Source

Follow the steps below to build a Data Source in Sentry

1. Navigate to the Diagnostics→Logging→Data Sources page in Sentry.
2. Click New to create a new Data Source. Configure the Data Source with the following criteria:
    a. Type: MySQL
    b. Name: Local_MySQL_DB
    c. Server: 127.0.0.1
    d. Port: 3306
    e. Database: sentrydb
    f. User: root
    g. Password: P@ssw0rd!
    h. Leave all other defaults
    i. Click Apply
    j. Click Test – you should receive a "Connection to database succeeded" message at the top of the page – if not, check the settings and ensure the MySQL service is running



DATA SOURCES > DATA SOURCE

Connection to database succeeded.

CONFIGURATION

Click on hyper link for data source schema

Type: ○ Oracle ● MySQL ○ DB2 ○ SQL Server ○ Oracle RAC

Name*: Local_MySQL_DB

Enable SSL: □

SSL initiation policy: ▾

Server*: 127.0.0.1

Port*: 3306

Database*: sentrydb

Schema:

User*: root

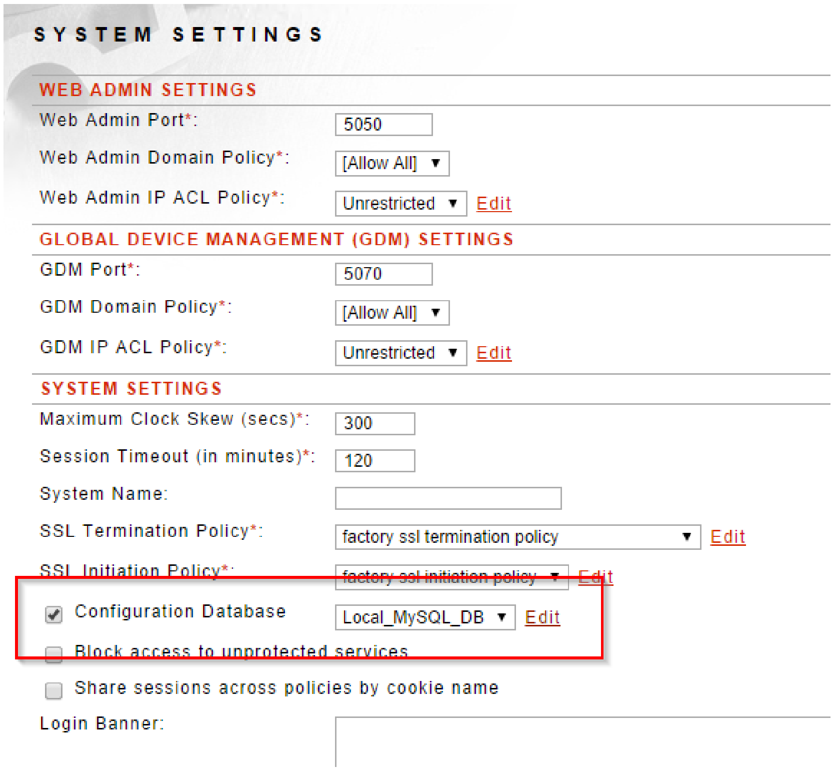
Password*: •••••••••••••••

Connect Descriptor:

Max Connections*: 5

Synchronous: ☑

3. Set the Configuration Database. Sentry needs to be configured with a “configuration database” before you can export to the database. Navigate to the System→Settings→System screen.
   a. Set the Configuration Database to: Local_MySQL_DB
   b. Scroll down and Click Save



SYSTEM SETTINGS

WEB ADMIN SETTINGS

Web Admin Port*: 5050

Web Admin Domain Policy*: [Allow All] ▼

Web Admin IP ACL Policy*: Unrestricted ▼ Edit

GLOBAL DEVICE MANAGEMENT (GDM) SETTINGS

GDM Port*: 5070

GDM Domain Policy*: [Allow All] ▼

GDM IP ACL Policy*: Unrestricted ▼ Edit

SYSTEM SETTINGS

Maximum Clock Skew (secs)*: 300

Session Timeout (in minutes)*: 120

System Name:

SSL Termination Policy*: factory ssl termination policy ▼ Edit

SSL Initiation Policy*: factory ssl initiation policy ▼ Edit

☑ Configuration Database Local_MySQL_DB ▼ Edit

☐ Block access to unprotected services

☐ Share sessions across policies by cookie name

Login Banner:

Exporting a Sentry Configuration to a Database

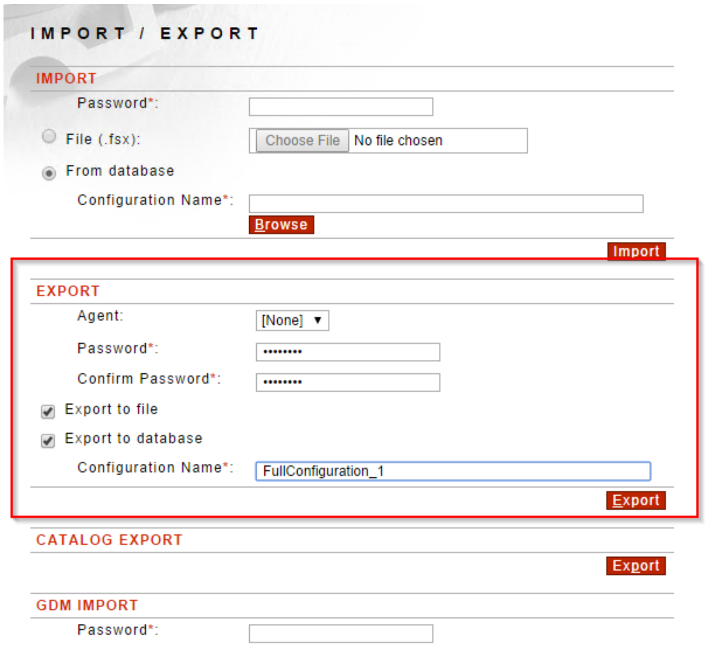
Both full (FSX) and partial (FSG) Sentry configurations can be exported to a database.

In this step we'll export the full Sentry configuration to a database and then view the store configuration through the WebAdmin interface.

Export the Sentry Configuration File

Follow the steps below to export the Sentry configuration file

1. Navigate to the System→Configuration→Import/Export Screen.
2. In the Export section, use the following criteria:
   a. Agent: None
   b. Password/Confirm Password: password
   c. Export to file: CHECKED
   d. Export to database: CHECKED (if this is greyed out, you have to set the configuration database on the System Settings screen)
   e. Configuration Name: FullConfiguration_1



IMPORT / EXPORT

IMPORT

Password*:

○ File (.fsx): Choose File No file chosen

● From database

Configuration Name*:

EXPORT

Agent: [None]

Password*: ••••••••

Confirm Password*: ••••••••

☑ Export to file

☑ Export to database

Configuration Name*: FullConfiguration_1

CATALOG EXPORT

GDM IMPORT

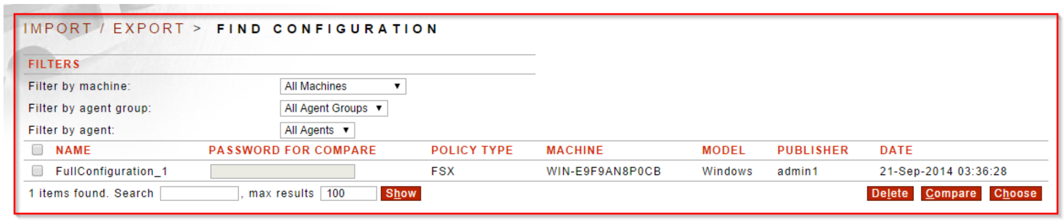
Password*:

   f. Click Export
   g. You should be prompted to save the FSX file to disk -or it is saved automatically depending on your browser settings
   h. The configuration is exported to the database

View the Sentry Configuration File in the Database

Follow the steps below to view the Sentry configuration file in the database through the WebAmin interface

1. Navigate to the System→Configuration→Import/Export Screen.
2. Under the Import section:
    a. Select: from database
    b. Click Browse
    c. Notice the configuration recently exported is available to import
    d. If there are multiple configurations you can select multiple and Compare them
    e. The screen can be filtered for specific Sentry instances



IMPORT / EXPORT > FIND CONFIGURATION

FILTERS

Filter by machine: All Machines

Filter by agent group: All Agent Groups

Filter by agent: All Agents

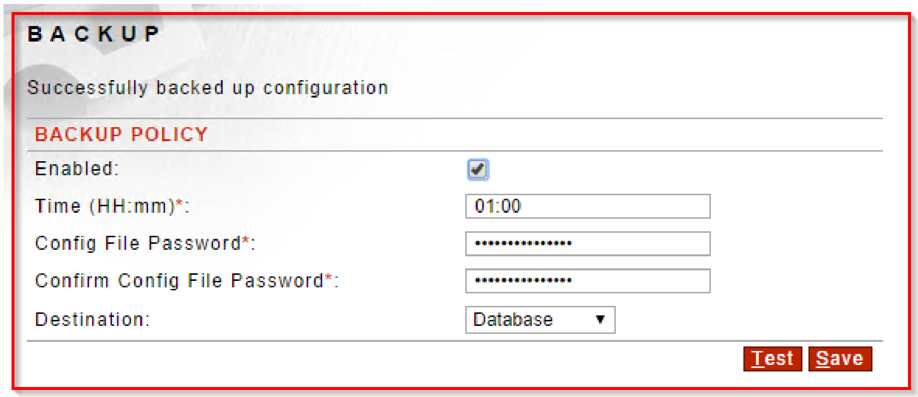
□	NAME	PASSWORD FOR COMPARE	POLICY TYPE	MACHINE	MODEL	PUBLISHER	DATE
□	FullConfiguration_1		FSX	WIN-E9F9AN8P0CB	Windows	admin1	21-Sep-2014 03:36:28

1 items found. Search , max results 100

Enable the Automated Configuration Backup

Follow the steps below to configure an automated configuration backup to a database.

1. Navigate to the System→Configuration→Backup page.
2. Configure the automated backup with the following criteria:
    - **a.** Enabled: CHECKED
    - **b.** Time: 01:00
    - **c.** Config File Password / Confirm Password: password
    - **d.** Destination: Database (Sentry also supports exporting to FTP and SFTP servers)
    - **e.** Click Save
    - **f.** Click Test to test the configuration (makes a backup)
    - **g.** Go back to the Import/Export screen and browse the database again, the config from the test should exist



BACKUP

Successfully backed up configuration

BACKUP POLICY

Enabled:	☑
Time (HH:mm)*:	01:00
Config File Password*:	•••••••••••••••
Confirm Config File Password*:	•••••••••••••••
Destination:	Database ▼

END

Additional Testing and More Reading

BACK IT UP!

Set up the automated backup on ALL Sentry instances. Ensure this feature is enabled as part of any “baseline” Sentry configuration file.

Before any system upgrades or policy modifications, make a backup of the full config and the specific policy being modified so you can roll back.

Additional Tests and Discussion Topics

1. Export a partial configuration file (FSG). You can export Content Policies, Task Lists, Keys, etc.
2. Change the configuration, then import your backup.
3. What happens when importing on top of an existing policy with the same name?
4. The automatic configuration export can also be configured from the ForumOS CLI with the Sentry appliances.

Additional Information

For more information, review the following Forum Sentry Admin Guide:

1. System Management Guide
2. How to Guide:

   https://helpdesk.forumsys.com/entries/39409268-How-To-Automatically-Back-Up-the-Forum-Sentry-Configuration-FSX-Files

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified, patented, and proven products deployed in the most rigorous and demanding customer environments worldwide. Forum Systems has been an industry leader for over 12 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Forum Systems security-first mindset enables trusted, network edge deployments of its technology for protecting critical enterprise transactions.

Our product technology is purpose-built and designed for mission-critical, enterprise-class scalable solutions where business solutions require the modern day security and identity enforcement protection, while enabling a scalable architecture and low-latency, high-volume throughput.

Forum Systems supports global enterprise customers across industries in commercial, government, and military sectors. Forum Systems technology provides the leading-edge of modern-day cyber-security innovation with integrated identity and SSO features that enable out-of-the box business solutions with point-and-click technology.

Forum’s patented; FIPS 140-2 and NDPP certified hardware and virtual products make modern-day business communications secure by actively protecting and accelerating data exchange and API service access across networks and business boundaries. For more information, please visit www.forumsys.com.