



FORUM SYSTEMS HANDS-ON TRAINING

LAB 4. THE FORUM SENTRY WEBADMIN INTERFACE



FORUM SYSTEMS

A Crosscheck Networks Company

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.

FORUMOST™ 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 © 2002-2014 Forum Systems, Inc. – All Rights Reserved.

Published: September 2014

Forum Systems Hands-on Training – Lab 4. The Forum Sentry WebAdmin Interface D-ASF-SE-010029

Contents

Introduction.....	4
<i>Skill Level</i>	4
<i>Prerequisites</i>	4
<i>Lab Overview</i>	4
The Forum Sentry WebAdmin Interface	5
<i>SSL Warning</i>	5
<i>Navigation</i>	5
Admininstrator Access and Role Based Access Control	8
<i>Creating a Restricted User</i>	8
Sentry Log Files	10
<i>Log Types</i>	10
<i>System Log Layout</i>	10
<i>Logging Settings</i>	11
System Settings	12
BACK IT UP!	13
<i>Additional Information</i>	13
About Forum Systems.....	14

Introduction

Lab 4. The Forum Sentry WebAdmin Interface – Navigation, Logging, Logs, Admin Users, Role Based Access Control, System Settings

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 of SOAPSonar Enterprise Edition.

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

This Lab introduces the Forum Sentry WebAdmin interface. The WebAdmin interface is accessed via browser using HTTPS on port 5050. If on the local machine, you can access the WebAdmin via:

<https://127.0.0.1:5050>

For developers, all Sentry policy configurations for deploying and securing APIs, enabling SSO, etc... are built in the WebAdmin interface.

For administrators, most of the diagnostics information (logs, monitoring, etc..) will be found in the WebAdmin interface. All administrator accounts, whether full access or partial, are setup in the WebAdmin interface.

This lab will provide an introduction to the WebAdmin interface. Topics will include:

1. Navigation
2. Help Options
3. Role Based Access Control
4. Sentry Log Files
5. Reviewing System Settings

The Forum Sentry WebAdmin Interface

The Sentry WebAdmin interface is where all Sentry runtime and admin access policies are built.

SSL Warning

When you first access the Sentry WebAdmin interface, using a browser, you may receive an SSL warning in your browser. This warning indicates that the WebAdmin cert is not trusted by your browser. While the cert can and should be changed, for now you can simply ignore this warning and click through the warnings/prompts to get to the login page.

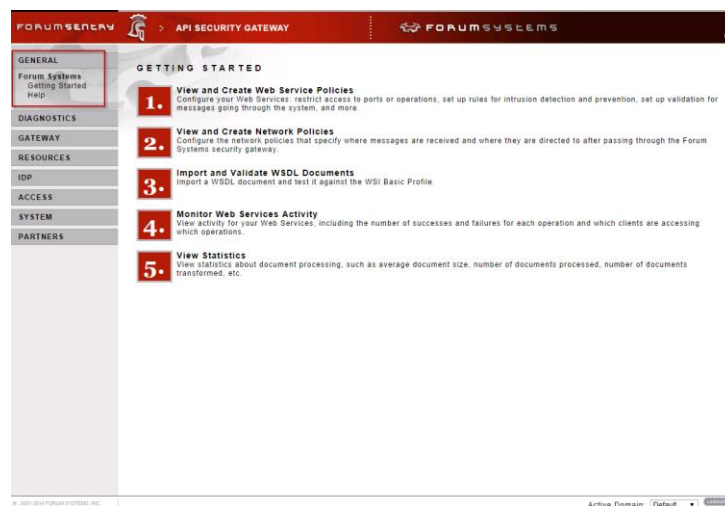
Navigation

After you've logged into the WebAdmin interface, you will be shown the Getting Started page. This page includes 5 shortcuts to commonly used screens.

You'll notice there are 8 main menus on the left pane, these are the 8 main categories detailed below.

Each menu has submenus for specific features. Navigation in the WebAdmin is simple, you simply click the menu/submenu on the left for the settings you need to access.

1. General – To access the Help pages (PDF documentation) and the Getting Started shortcuts.



2. Diagnostics – To access logs, set log thresholds, see version information, enabling monitoring, check system resources, etc. These are menus that are commonly used by Sentry Administrators who will monitor the devices, pull logs, and troubleshoot issues.



3. Gateway – To build and manage Runtime Policies that will process the traffic being processed by Sentry. This includes network policies, content policies (REST, JSON, HTML, etc.), WSDL policies, and Task Lists. These are screens commonly used by Sentry developers who build the runtime policies.



4. Resources – To build the “reusable policy objects” that will be associated to and used by the runtime policies defined under the Gateway menu. This includes keys, security policies, error templates, etc.



5. IDP – To build and manage the IDP Rules (Intrusion Detection and Prevention) in Sentry. These are firewall type rules that filter/block transactions based on a variety of criteria, including but not limited to: size, frequency, content, virus scanning, authentication/authorization failures, etc.

IDP
IDP Blocking IDP Blocking
IDP Policies IDP Rules IDP Groups IDP Actions IDP Schedules IDP Clustering

6. Access – To build and manage both runtime and Sentry administrator access control policies. This is where admin accounts can be built and managed, where runtime User ACLs are set, where policies to connect to an LDAP server are built, etc.

ACCESS
Runtime Access User ACLs IP ACLs XACML
Admin Access Domains Roles
User Policies Users Cache User Groups Active Users LDAP RSA SecurID Kerberos SiteMinder TAM WebSeal Oracle Access Mana ClearTrust HP SelectAccess WS-Trust OpenAM REST Sentry Custom

7. System – To manage system settings, configure backups, manage the Sentry configurations, control the Sentry service/appliance and upgrade (hardware only).

SYSTEM
Settings System Control Preferences
Configuration Import/Export Backup Agents Agent Groups WSDL API

8. Partners – To enable integrations with other products including enabling on-board AV scanning.

PARTNERS
Partners Clam AV ICAP AV Oracle WSM Unicenter WSDM HP OpenView SOA Mar Embedded SOA MP

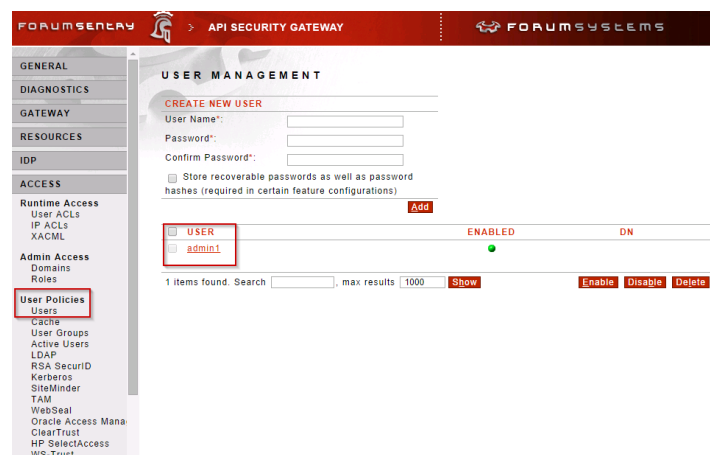
Administrator Access and Role Based Access Control

Sentry allows for different admin users to have different access rights (read/write permissions) when they log into Sentry. Admin accounts can be stored locally, or Sentry can be configured to communicate with an existing identity store (e.g.: ldap, Siteminder, TAM) for admin access. Even when Sentry is integrated with an external identity store for admin access, there will always be at least one local user with full rights (privileged access).

A local “privileged access” user is generated upon initial configuration. With a Sentry appliance, this is at the end of the network configuration wizard. With a Sentry software instance, this is after licensing.

There are no default accounts and no way for Forum Systems to reset the user password.

To view the local users in Sentry go to the **Access→User Policies→Users** page.



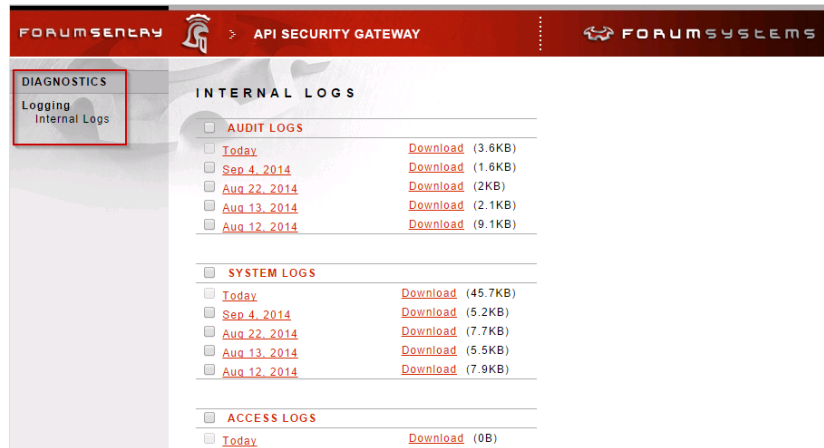
Users who will have access to certain screens, but not all, either to read or write, will not be privileged access users.

Creating a Restricted User

Follow the steps below to create a user who only has access to view the Log files in the WebAdmin interface.

1. Create the Read-Only User by going to:
ACCESS→USER POLICIES→USERS and create a user
2. Create a User Group by going to:
ACCESS→USER POLICIES→USER GROUPS and create a group
3. Click on the newly created GROUP and add the new USER to it.
4. Create a new Domain by going to:
Access→ADMIN ACCESS→DOMAINS and create a new Domain
5. Click on the new Domain and check READ for the new group created in step 2, then SAVE
6. Create a new role for the Read-Only Internal Logs as follows:
 - a. Go to Access→ADMIN ACCESS→ROLES
 - b. Create a new role

- c. Click on the new role and SELECT/CHECK the menus this role will have access to - in this case, select Internal Logs then SAVE
7. Finally add a Restriction to the new Domain via the new Role as follows:
 - a. Go to ADMIN ACCESS→DOMAINS and click on the newly created Domain
 - b. SELECT/CHECK the Restrict Menus option
 - c. Select the new Role created in step 6, then SAVE
8. Test by logging out of the WebAdmin (logout button at bottom right) and then login with the new user account. Notice the only menu available is the Diagnostics→Logging→Internal Logs page.



Sentry Log Files

This chapter will discuss the different logs in Sentry and the logging settings. The Sentry logs are always stored locally, but can also be sent to a remote syslog daemon. The logs can be downloaded – both a full log download as well as a partial (per transaction).

Log Types

There are three types of Logs in Sentry.

1. Audit Logs – Tracks all administrator access and policy modifications
2. System Logs – Detail the runtime traffic and processing done in Sentry
3. Access Logs – Shows a single line for each runtime transactions with basic details and hyperlinks to System log for more detail on a particular transaction.

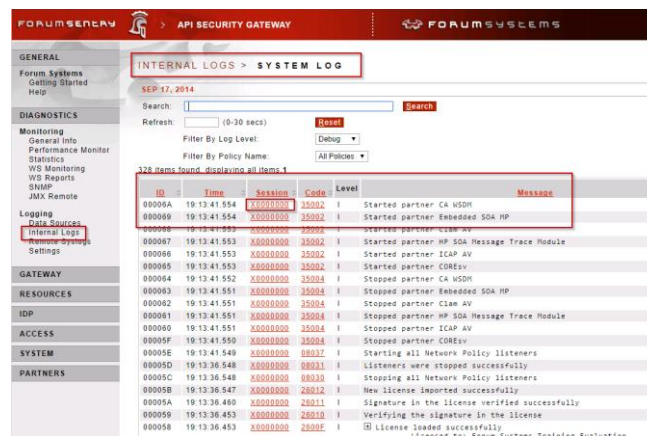
System Log Layout

The System log is where most Sentry developers and administrators will spend the majority of the time reviewing logs. This log records runtime traffic.

The log can be searched, filtered, reset (cleared), and refreshed.

There are 6 columns of logging information in the System log. The logs can be sorted by these columns.

1. ID – The unique log id for this message
2. Time – The timestamp for the log message
3. Session – The sortable Session ID assigned to all log messages for a particular transaction. Click this to sort only show log messages for that particular transaction.
4. Code – Each type of log message has a code, so you can choose to always or never log a certain code regardless of levels set.
5. Level – The log level this log message is written at. The four log levels are:
 - a. Error – only logs errors
 - b. Warning – logs errors and warning conditions
 - c. Info – logs errors, warnings, and info level events
 - d. Debug – logs everything about the transaction, this is the most verbose log



The screenshot shows the Sentry web interface. On the left is a sidebar with navigation links: GENERAL, DIAGNOSTICS, LOGGING, GATEWAY, RESOURCES, IDP, ACCESS, SYSTEM, and PARTNERS. The main area is titled 'INTERNAL LOGS > SYSTEM LOG' and shows a table of log entries. The table has columns: ID, Time, Session, Code, Level, and Message. The log entries are filtered by date (SEP 17, 2014) and show 328 items found, displaying all items. The log levels are set to Debug. The messages include various system events like 'Started partner: CA USDM', 'Started partner: Embedded SOA HP', 'Started partner: HP SOA Message Trace Module', 'Started partner: ICAP AV', 'Started partner: COREV', 'Stopped partner: CA USDM', 'Stopped partner: Embedded SOA HP', 'Stopped partner: ICAP AV', 'Stopped partner: HP SOA Message Trace Module', 'Starting all Network Policy listeners', 'Listeners were stopped successfully', 'Stopping all Network Policy listeners', 'New license imported successfully', 'Signature in the license verified successfully', 'Verifying the signature in the license', and 'License loaded successfully'.

ID	Time	Session	Code	Level	Message
00006A	19:13:41:554	X0000000	35002	I	Started partner: CA USDM
000069	19:13:41:554	X0000000	35002	I	Started partner: Embedded SOA HP
000068	19:13:41:553	X0000000	35002	I	Started partner: HP SOA Message Trace Module
000066	19:13:41:553	X0000000	35002	I	Started partner: ICAP AV
000065	19:13:41:553	X0000000	35002	I	Started partner: COREV
000064	19:13:41:552	X0000000	35004	I	Stopped partner: CA USDM
000063	19:13:41:551	X0000000	35004	I	Stopped partner: Embedded SOA HP
000062	19:13:41:551	X0000000	35004	I	Stopped partner: ICAP AV
000061	19:13:41:551	X0000000	35004	I	Stopped partner: HP SOA Message Trace Module
000060	19:13:41:551	X0000000	35004	I	Stopped partner: COREV
00005F	19:13:41:550	X0000000	35004	I	Stopped partner: CA USDM
00005E	19:13:41:549	X0000000	08037	I	Starting all Network Policy listeners
00005D	19:13:36:548	X0000000	08037	I	Listeners were stopped successfully
00005C	19:13:36:548	X0000000	08030	I	Stopping all Network Policy listeners
00005B	19:13:36:547	X0000000	28012	I	New license imported successfully
00005A	19:13:36:480	X0000000	28011	I	Signature in the license verified successfully
000059	19:13:36:453	X0000000	28010	I	Verifying the signature in the license
000058	19:13:36:453	X0000000	28007	I	License loaded successfully

Logging Settings

The logging settings are set on the Diagnostics→Logging→Settings page. Important options include:

1. Log File Size (in MB) – 1 GB by default, after this value is reached the logs is rolled over (deleted) and all information is lost.
2. Logging Levels – Set for each log type, INFO is recommended though DEBUG will be used throughout the training process.
3. Include/Exclude Codes – The ability to always or never log a message based on code. This can be used to always see a DEBUG level message even with the level at INFO. Alternatively, this can be used to prevent proprietary transactional data from being logged at DEBUG level.

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS

GENERAL

DIAGNOSTICS

Monitoring

General Info

Performance Monitor

Statistics

WS Monitoring

WS Reports

SNMP

JMX Remote

Logging

Data Sources

Internal Logs

Remote Syslogs

Settings

GATEWAY

RESOURCES

IDP

ACCESS

SYSTEM

PARTNERS

LOG CONFIGURATION SETTINGS

CONFIGURATION

Sign Logs with Key Pair: DEFAULT Edit

Download Format: Plain Text

Compression Mode: Zip GNU Zip

Log File Size (in MB): 1024

Default Display Length: 100

Global Logging Level: Info

AUDIT LOG

Logging Level: Info

Log Lifespan (in days): 15

SYSTEM LOG

Logging Level: Info

Log Lifespan (in days): 15

☐ Override log level for the following codes

☒ Include these codes

☐ Exclude these codes

Comma delimited list of codes:

Partial codes will include any codes starting with the partial code

Pattern Match Policy: [None]

ACCESS LOG

Logging Level: Info

Log Lifespan (in days): 15

Save

© 2021-2024 FORUM SYSTEMS, INC.

System Settings

The System Settings for each Sentry instance can be set on the System→Settings→System page. Important settings on this page include:

1. WebAdmin Domain – The Domains that are allowed to access the WebAdmin
2. WebAdmin IP ACL – To set IP restrictions for WebAdmin access
3. Session Timeout – The WebAdmin and CLI interface timeout values – default is 8, we recommend you modify this to 120 for the training instance of Sentry
4. SSL Termination Policy – The SSL policy used for WebAdmin access
5. SSL Initiation Policy – The SSL policy used when Sentry connects to certain remote locations for admin features
6. Configuration Database – The Database used to store Sentry policies
7. Login Banner – The banner displayed on the WebAdmin login page and during the CLI login
8. SMTP Settings – The SMTP server settings Sentry uses to send email alerts and reports

FORUMSENTRY > API SECURITY GATEWAY FORUMSYSTEMS

GENERAL
DIAGNOSTICS
GATEWAY
RESOURCES
IDP
ACCESS
SYSTEM
Settings System
Control
Preferences
Configuration
Import/Export
Backup
Agents
Agent Groups
WSDL API
PARTNERS

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)*: 8

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:

END

BACK IT UP!

It is recommended that you export your full Sentry configuration after completing this lab.

To export your full Sentry configuration, navigate to the System→Configuration→Import/Export screen and use the Export option in the center of the page to export the full Sentry configuration file as a password encrypted FSX file. This can later be imported on the same screen.

We recommend including the lab number in the name of the export files.

Additional Information

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

1. [Logging Guide](#)
2. [Web Based Administration Guide](#)
3. [Access Control Guide](#)

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.