



FORUM SYSTEMS SENTRY™ VERSION 8.11
MICROSERVICES AND DOCKER
BEST PRACTICES GUIDE



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 © 2002-2019 Forum Systems, Inc. – All Rights Reserved.

Forum Systems Sentry™ Version 8.11 Microservices and Docker Best Practices Guide, published June 2019.







D-ASF-SE-602323

Table of Contents

Forum Sentry Virtual Form Factors.....	4
Elastic Licenses	4
Microservices Gateway	4
Automated Sentry Deployments using Docker	5
Pre-Provisioning a Sentry Docker Instance for Deployment	5
Custom Configuration for Baseline Policy Auto-Configuring	6
Using the REST API to modify Sentry Docker Instance Policy Settings	7
Using the Forum License Server	8
Reviewing Docker Deployment with Forum Support Team.....	9

Forum Sentry Virtual Form Factors

Forum Sentry is provided in various virtual form factors that facilitate microservice deployments where the computing environments are often virtual or cloud-based.

 HARDWARE	Hardware	ForumOS™. FIPS 140-2 Level II purpose-built chassis with FIPS 140-2 Level III HSM. NIAP NDPP Certified.
 vmware OVA IMAGE	VMWare	Fully encapsulated virtualized rendition of Hardware system in a deployable OVA VMWare image
 amazon web services AMI IMAGE	Amazon	Fully encapsulated virtualized rendition of Hardware system in a deployable Amazon AMI
 Microsoft Azure 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
 WINDOWS LINUX	Software	Windows or Linux software provided via single-package install with no dependencies.

Elastic Licenses

For microservice deployments, often the instances of Forum Sentry are mutable and are spun up and down on-demand. This is considered an elastic deployment model commonly used in cloud-based deployment environments. The Forum Sentry License Server is used for these deployments to enable any virtual variants of Sentry to share licenses to enabled on-demand elasticity and movable Sentry instances.

Microservices Gateway

Forum Sentry can operate as a standard enterprise-class API Security Gateway at the data boundary perimeter, or as a microservice gateway at the dev/ops application tier. The purposes of the 2 deployment paradigms are similar, but have some different aspects. Generally, at the microservices level, the expected benefits of using Forum Sentry as a Microservice Gateway include:

- 1) Monitoring of internal business communications
- 2) Developer level latency, volume, and errors
- 3) Automated deployments via scripting, or orchestration platforms such as Kubernetes
- 4) API response caching

Automated Sentry Deployments using Docker

Using Docker containers on a Linux OS is a common mechanism to use for Forum Sentry virtual deployments in cloud environments such as Amazon and Azure. Docker instances allow for automated Forum Sentry deployment capabilities such as pre-provisioning, cloning, and using REST API commands for environment updates. Instructions on how to set up Forum Sentry on Docker can be found on our Help Desk FAQ: [Creating a Docker Image for a Forum Sentry Linux Software Instance](#)

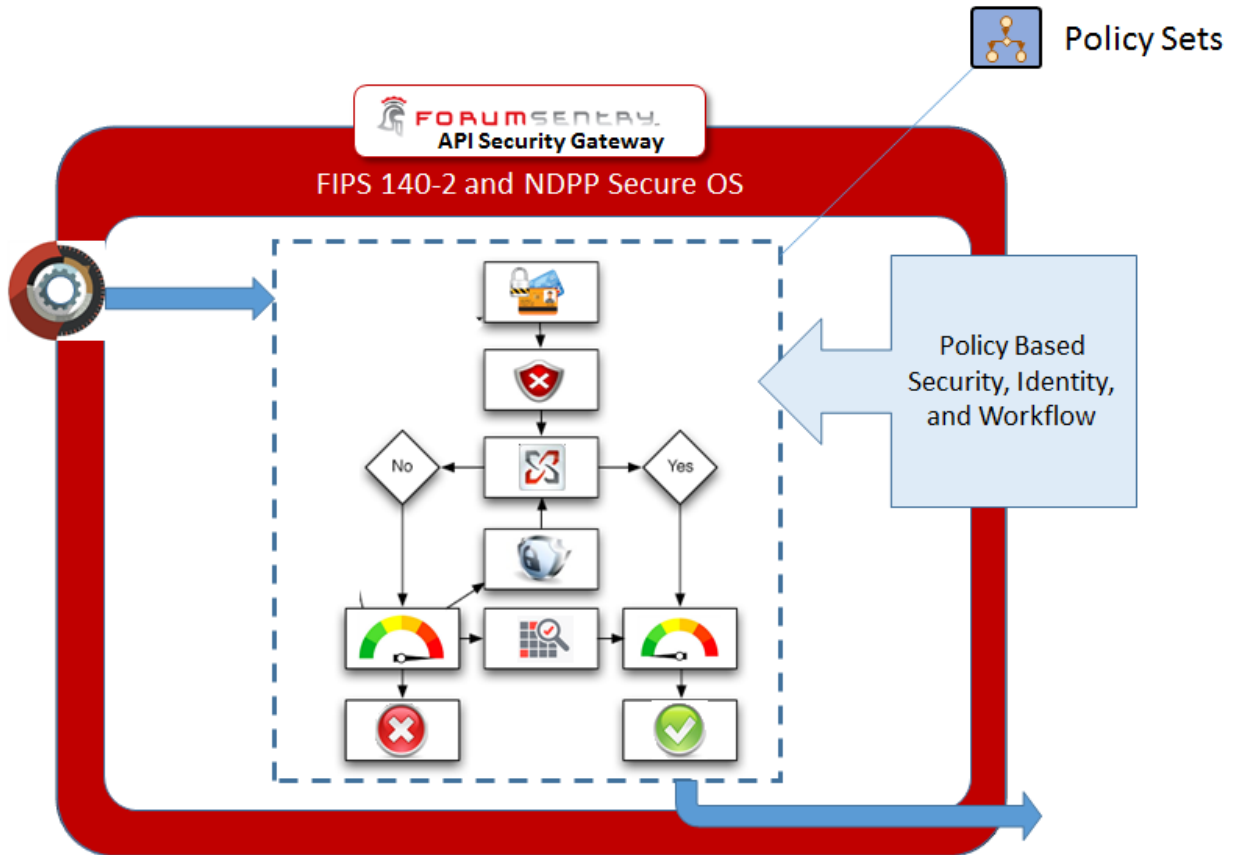
Pre-Provisioning a Sentry Docker Instance for Deployment

Establishing a baseline policy set to apply to an installed Sentry instance allows the policies to be staged for pre-determined workflows to be deployed and activated during the deployment of new Docker images.

A baseline policy set is simply an FSX configuration file which represents an exported set of policies that have already been established to provision this instance of Sentry with a default policy set. Using the graphical WebAdmin interface to build the base policy sets allows these policies to then be used for auto-deployment and provisioning of new Docker-based Sentry instances. You can use any virtual variant of a Sentry instances to pre-provision policies that can then be exported as FSX (full configuration) and FSG (partial configuration) files that can be applied to newly launched Docker images to establish a set of baseline policies and behavior for the Sentry instances.

For more information about FSX policies, please see the **FS_Sentry_V8.11_System_Management_Guide** “Global Device Management” section.

Note that it is recommended when provisioning the policies this way that the “Use Device IP” option is enabled for any listener policies created. This ensures that the system will come up and bind to the IP address of the target system rather than binding to a specific IP address, which would cause conflicts when trying to deploy multiple instances.



Custom Configuration for Baseline Policy Auto-Configuring

The config.properties file contains various startup and system properties used by Forum Sentry. This file resides in the **xmlserver** installation root subdirectory. For example:

```
/root/ForumSystems/xmlserver/config/config.properties
```

In order to automate the baseline policy for Sentry to import, you will need 2 variations of the config.properties file. The 1st variation will have the import flag and a reference to your base FSX configuration file. The 2nd variation will be the same config.properties with this flag and reference removed. You will use the 2nd file once the provisioning has taken place to prevent Sentry from continually overwriting the configuration each time it starts up.

Flags for Loading FSX:

- loadFsx: References the full path to the FSX to import
- fsxPassword: Password of the FSX

For example:

```
-loadFsx=/home/fsx_exports/my-core-policy-set.fsx -fsxPassword={FSXPASSWORD}
```

The process to perform the base policy provisioning is similar to this:

- 1) Stop the Sentry service

- 2) Copy the config.properties **with** the FSX import information. i.e.

cp config.properties.install_policy /root/ForumSystems/xmlserver/config/config.properties

- 3) Start the Sentry service

(This step processes the config.properties file command to import the referenced FSX on startup and apply it as the baseline configuration.)

- 4) Stop the Sentry service

- 5) Copy the config.properites **without** the FSX import information. I.e.

cp config.properties.nofsx /root/ForumSystems/xmlserver/config/config.properties

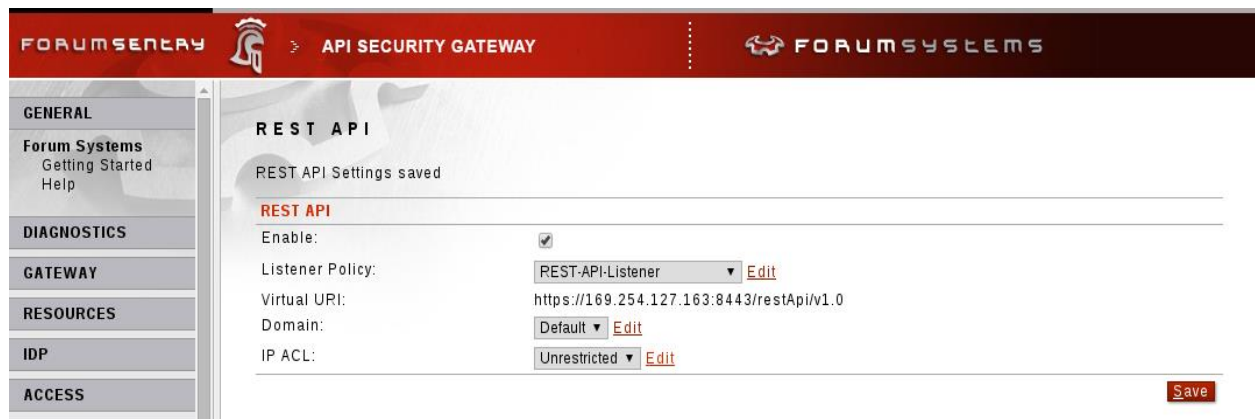
(This step ensures that the FSX does not get continually overwritten on each startup)

- 6) Start the Sentry service

Using the REST API to modify Sentry Docker Instance Policy Settings

The Forum Sentry REST API is enabled via the System->Configuration->REST API menu within the Web Admin Screen. Ensure that this option is enabled in the baseline FSX such that once deployed you can use the API to modify policy settings.

Once enabled, you can open a web browser and navigate to the Virtual URI as shown on the screen. You will be prompted to enter administrator credentials in order to access the REST API. This will load the self-documenting REST API screen which will expose and show all methods and means of invoking the methods supported by the Forum Sentry REST API.



The screenshot shows the Forum Sentry REST API configuration interface. The top navigation bar includes the Forum Sentry logo, 'API SECURITY GATEWAY', and the Forum Systems logo. A left sidebar contains menu items: GENERAL, Forum Systems (with sub-items Getting Started and Help), DIAGNOSTICS, GATEWAY, RESOURCES, IDP, and ACCESS. The main content area is titled 'REST API' and displays 'REST API Settings saved'. Below this, the 'REST API' settings are shown with the following values:

Enable:	<input checked="" type="checkbox"/>
Listener Policy:	REST-API-Listener Edit
Virtual URI:	https://169.254.127.163:8443/restApi/v1.0
Domain:	Default Edit
IP ACL:	Unrestricted Edit

A [Save](#) button is located at the bottom right of the settings area.

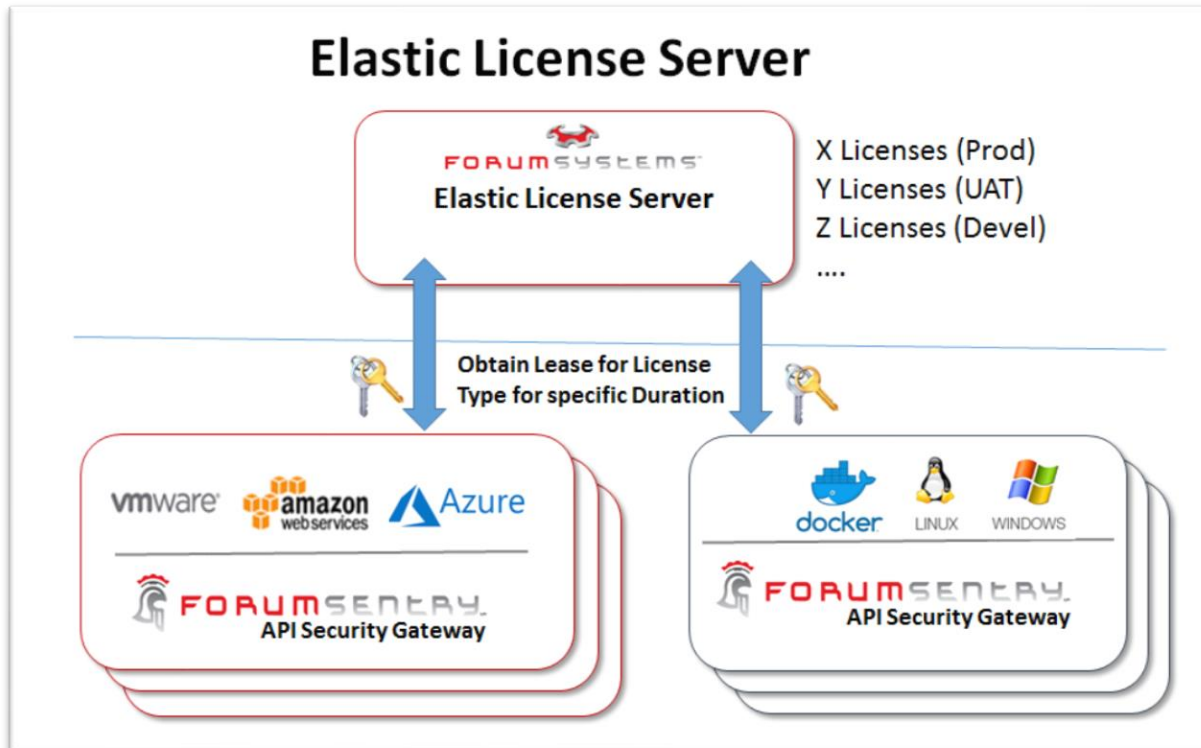
FORUMSENTRY > WEB SERVICES SECURITY GATEWAY		FORUMSYSTEMS	
activeMqListenerPolicies : ActiveMQ listener policy operations	Show/Hide	List Operations	Expand Operations Raw
activeMqRemotePolicies : ActiveMQ remote policy operations	Show/Hide	List Operations	Expand Operations Raw
agentGroups : agent group operations	Show/Hide	List Operations	Expand Operations Raw
agents : agent operations	Show/Hide	List Operations	Expand Operations Raw
amqpListenerPolicies : AMQP listener policy operations	Show/Hide	List Operations	Expand Operations Raw
amqpRemotePolicies : AMQP remote policy operations	Show/Hide	List Operations	Expand Operations Raw
configuration : system wide configuration operations	Show/Hide	List Operations	Expand Operations Raw
documents : document policy operations	Show/Hide	List Operations	Expand Operations Raw
ftpPolicies : FTP policy operations	Show/Hide	List Operations	Expand Operations Raw
ftpListenerPolicies : FTP listener policy operations	Show/Hide	List Operations	Expand Operations Raw
ftpRemotePolicies : FTP remote policy operations	Show/Hide	List Operations	Expand Operations Raw
htmlPolicies : HTML policy operations	Show/Hide	List Operations	Expand Operations Raw
httpListenerPolicies : HTTP listener policy operations	Show/Hide	List Operations	Expand Operations Raw
httpRemotePolicies : HTTP remote policy operations	Show/Hide	List Operations	Expand Operations Raw
jbossListenerPolicies : JBoss listener policy operations	Show/Hide	List Operations	Expand Operations Raw
jbossRemotePolicies : JBoss remote policy operations	Show/Hide	List Operations	Expand Operations Raw
jsonPolicies : JSON policy operations	Show/Hide	List Operations	Expand Operations Raw
mqListenerPolicies : MQ listener policy operations	Show/Hide	List Operations	Expand Operations Raw

Sentry supports adding, modifying, and deleting policies via a REST API automation interface using any REST based tool. This can be used for full policy provisioning and deployment, or for modifying environment properties of policies that have been loaded on the Sentry instance.

For more information about Forum Sentry REST API automation and features, please refer to the **FS_Sentry_V8.11_REST_API** Guide and our Help Desk FAQ: [How To: Use the Sentry REST API for Policy Configuration and Management](#)

Using the Forum License Server

The Forum License Server enables floating elastic license usage across any virtual variant of Forum Sentry. It is the recommended licensing mechanism for Docker deployments as it provides the flexibility of on-demand computing and movable instances. The Forum License Server itself is available at no cost for any Forum Sentry customer.



To install and deploy the Forum License Server, please review the instructions provided at the following Help Desk FAQ: [Forum Sentry License Server User Guide](#)

Reviewing Docker Deployment with Forum Support Team

Please contact us to assist with reviewing your deployment and assisting with configuration and best practices. The best way to do this is to schedule a session via the [Help Desk](#), or via emailing support@forumsys.com.