



FORUM SENTRY™ VERSION 9

DOCKER 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.

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

Forum Sentry™ Version 9 Docker Guide, published May 2024.

D-ASF-SE-61350

Table of Contents

Sentry Deployments using Docker.....	4
1. Build the Dockerfile	4
2. Build the docker image	5
3. Launch the docker image	5
4. Commit the docker image	6
4. Attach the docker image	6
5. License the Forum Sentry docker image.....	7
6. Provision the baseline configuration Sentry Policies	7
7. Commit Configuration	7
7. Deploy Sentry Docker Image.....	7
Provisioning a Sentry Docker Instance for Deployment	8
Baseline Policy Auto-Configuring	8
Using REST API to modify Sentry Docker Instance Policy Settings	9
Using the Forum License Server	11
Reviewing Docker Deployment with Forum Support Team.....	11

Sentry Deployments using Docker

Using Docker containers on a Linux OS is a common mechanism to use for Forum Sentry virtual deployments on 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.

1. Build the Dockerfile

Below is a sample Dockerfile which creates a Centos v8 image with supporting utilities and Forum Sentry version 9.10. Edit the sample to make changes to fit your environment such as:

- package_version (i.e. '9')
- package_build (i.e. '280')
- package_ftp_base_path (location to the install file)

For example, the binary name for Sentry version 9.10 is **fs-sentry-9.10-x86_64-linux.bin**.

Place your Dockerfile in the local directory.

```
# Base image for a publicly available Sentry
FROM forumsys/sentry_public:base
MAINTAINER support@forumsys.com

EXPOSE 5050 5060 5070 5080

ARG package_version
ARG package_build

ENV container docker
ENV package_ftp_base_path=ftp://aaa.bbb.com/Sentry
ENV package_name fs-sentry-${package_version}.${package_build}-x86_64-linux.bin

SHELL ["/bin/bash", "-c"]

RUN (cd /lib/systemd/system/sysinit.target.wants/; for i in ; \
do [ $i == systemd-tmpfiles-setup.service ] || rm -f $i; done); \
rm -f /lib/systemd/system/multi-user.target.wants/*; \
rm -f /etc/systemd/system/.wants/*; \
rm -f /lib/systemd/system/local-fs.target.wants/*; \
rm -f /lib/systemd/system/sockets.target.wants/*udev*; \
rm -f /lib/systemd/system/sockets.target.wants/*initctl*; \
rm -f /lib/systemd/system/basic.target.wants/*; \
rm -f /lib/systemd/system/anaconda.target.wants/*;

CMD ["/usr/sbin/init"]
```

```
RUN rm -f /etc/localtime
RUN cp /usr/share/zoneinfo/UTC /etc/localtime

RUN wget -q -O /root/${package_name} ${package_ftp_base_path}/${package_version}/${package_name};
RUN chmod +x /root/${package_name}

RUN /root/${package_name} -i silent; exit 0
RUN rm /root/${package_name}

COPY runSentry.sh /root
RUN chmod +x /root/runSentry.sh

ENTRYPOINT /root/runSentry.sh
```

2. Build the docker image

```
# docker build -t <Tag> .
```

For this exercise the following command is creating the Sentry Docker Image with the Tag sentry_9.10 under the repository forumsys/services

```
# docker build -t forumsys/services:sentry_9.10 .
```

Once finished you should see that the new Docker Image has been created via the command:

```
# docker images
```

Or more specifically

```
# docker images <repository>:<Tag>
```

Example:

```
# docker images forumsys/services:sentry_9.10
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
forumsys/services	sentry_9.10	fdd4d234086f	2 hours ago	1.69GB

3. Launch the docker image

The following two commands launch the Docker Image and start Forum Sentry. The first command shows CPU and Memory allocation as well as mapping of the default Web Admin port (5050) inside the Docker Container to the desired and available port on the host. The second command starts Forum sentry.

Note: in the example below the port on the host is 50501 which is mapped to the web admin port (5050) in the container running Forum Sentry

```
# docker run --cpus 2 -m 12GB --rm -itd -p 50501:5050 - --name sentry_9.10 forumsys/services:Sentry_9.10
```

```
# docker exec sentry_9.10 ./root/ForumSystems/xmlserver.nonroot restart
```

The above two commands can go into a single script and executed as a shell script.

Note: again, there are many ways to accomplish these steps and further simplify. This is but one of these methods.

After running the above commands, you should be able to view the newly created container using:

```
# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
38137c33e867	forumsys/services:sentry_9.10	"/usr/sbin/init"	9 minutes ago	Up 9 minutes	0.0.0.0:50501->5050/tcp	sentry_9.10

4. Commit the docker image

It is recommended that a Docker Image is saved apart from any you intend to deploy. These base images can be used as part of a new Dockerfile to create more specialized Docker Images. For example, the above steps have led to the creation of a base Forum Sentry Linux Docker Image which can be used to further create newer Test/Dev and Production images.

To create a base image, you will need to specify a name tag as follows:

```
# docker commit 38137c33e867 forumsys/services:Sentry_9.10_base
```

4. Attach the docker image

The following command places you inside the container in execute mode:

```
# docker exec -it <container_name> bash
```

Example:

```
# docker exec -it sentry_9.10 bash
```

The above command should place you right inside the container:

5. License the Forum Sentry docker image

This step can be done by obtaining a license file in XML format and writing it directly to the subdirectory where Forum Sentry is installed (i.e. /root/ForumSystems/xmlserver/config/) or you can launch a web browser and go to your host's IP at the mapped web admin port (i.e. https://[Docker_Image_IP]:50505) and the license screen that will be the first screen that appears. You can apply an instance license, or an elastic floating license from a Forum License Server. \

6. Provision the baseline configuration Sentry Policies

Once licensed you should be prompted to create an initial Web Admin Account. Login and proceed to create a new configuration by adding new policies, etc. You can also import a pre-existing configuration via Import of FSX (full configuration file) or FSG (policy-based granular configuration file). Please note that at this point the newly created Policies will not be exposed until you commit changes.

7. Commit Configuration

As it was recommended above, the **Commit** is again used to create a pre-configured Docker ready to deploy.

```
# docker commit acadd734d92e forumsys/services:Sentry_9.10_prod
```

7. Deploy Sentry Docker Image

At this point you would have at least a couple of Docker Images where the first, base image, can be used in a Dockerfile to create new Docker Images and the second, pre-configured Forum Sentry Images, ready to be deployed.

In order to deploy Forum Sentry Docker Images, all of the listener ports used in all policies that will be exposed need to be mapped during the deployment. For example, the command below shows the web Admin port 5050 is mapped to 50505 on the host and policy ports 8080 and 443 are mapped respectively to 8088 and 443 on the host.

```
# docker run --cpus 2 -m 12GB --rm -itd -p 50505:5050 -p 8088:8080 -p 443:443 --name sentry_9.10_prod1 forumsys/services:sentry_9.10_prod
```

```
# docker exec sentry_9.10_prod1 ./root/ForumSystems/xmlserver.nonroot restart
```

```
# docker ps | grep prod1
```

```
137c12b26edc    forumsys/services:sentry_9.10_prod  "/usr/sbin/init"    2 minutes ago    Up 2
minutes       0.0.0.0:443->443/tcp, 0.0.0.0:50505->5050/tcp, 0.0.0.0:8088->8080/tcp  sentry_9.10_prod1
```

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 and exported set of policies that have already been established to provision this instance of Sentry to use as the default policy set. Using the graphical Web Admin 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_V9_System_Management_Guide** “Global Device Management” section.

Note that it is recommended when provisioning the policies this way that the “Use Device IP” option 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.

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 .

Example extended from [Build the Dockerfile](#) section above

```
...
RUN /root/$package_name -i silent; exit 0

RUN rm /root/$package_name

RUN sed -i "s/APP_ARGS=\\(.\\*\\)/APP_ARGS=\\1
-loadFsx=\\root\\ForumSystems\\xmlserver\\config\\$base_config
-fsxPassword=$base_config_password
-license=server=license-server.forumsys.com,dr_server=license-server-dr.forumsys.com,type=
devel,time=30,auto=true/" /root/ForumSystems/xmlserver/config/config.properties

COPY runSentry.sh /root

RUN chmod +x /root/runSentry.sh

COPY $base_config /root/ForumSystems/xmlserver/config/$base_config

ENTRYPOINT /root/runSentry.sh
```

Using 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 for the baseline FSX you create to baseline the policy set that this feature is enabled 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.

FORUMSENTRY

API SECURITY GATEWAY

FORUMSYSTEMS

GENERAL

Forum Systems
Getting Started
Help

DIAGNOSTICS

GATEWAY

RESOURCES

IDP

ACCESS

REST API

REST API Settings saved

REST API

Enable:

☒

Listener Policy:

REST-API-Listener

Edit

Virtual URI:

https://169.254.127.163:8443/restApi/v1.0

Domain:

Default

Edit

IP ACL:

Unrestricted

Edit

Save

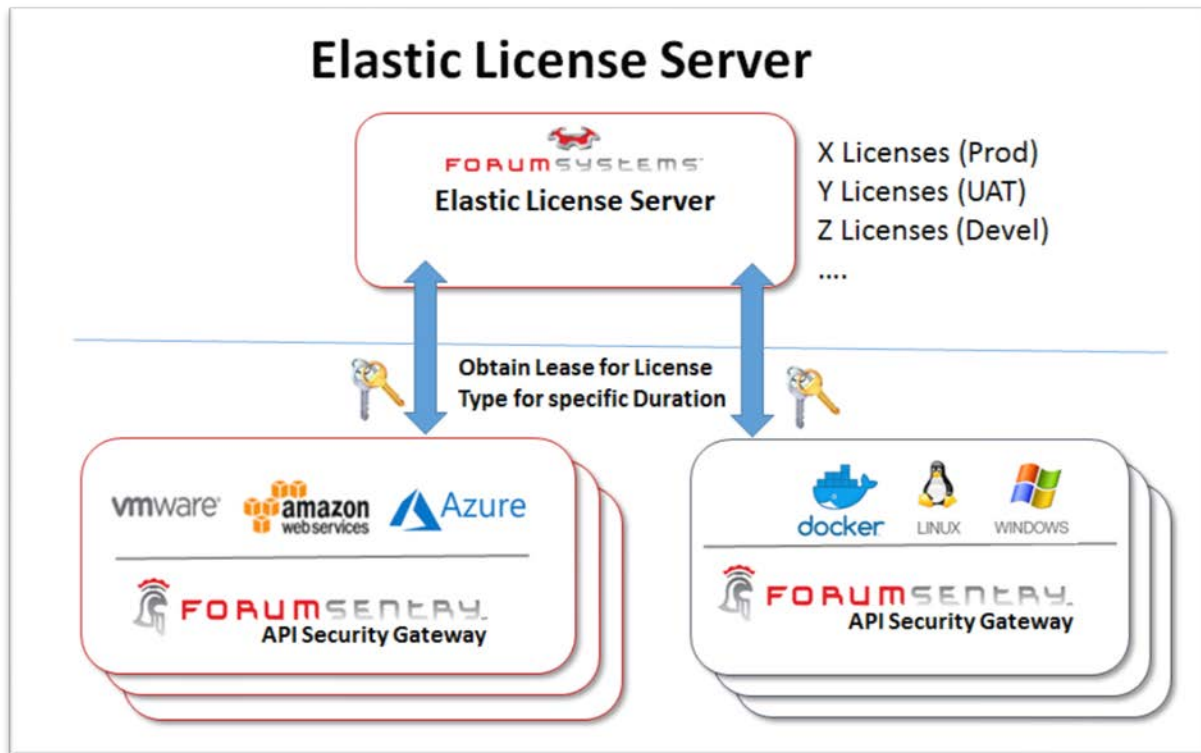
activeMqListenerPolicies : ActiveMQ listener policy operations	Show/Hide	List Operations	Expand Operations	Raw
activeMqRemotePolicies : ActiveMQ remote policy operations	Show/Hide	List Operations	Expand Operations	Raw
agentGroups : agent group operations	Show/Hide	List Operations	Expand Operations	Raw
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_V9_REST_API** Guide.

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 Helpdesk FAQ (note a valid Forum Systems support account is required to access this page):

<https://helpdesk.forumsys.com/hc/en-us/articles/360021088073-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 Helpdesk at helpdesk.forumsys.com, or via emailing support@forumsys.com.