FORUM SYSTEMS

THE LEADER IN API SECURITY & ZERO TRUST

FORUM SYSTEMS SENTRY™ VERSION 9.1

MICROSERVICES AND DOCKER

BEST PRACTICES GUIDE

Legal Marks

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.

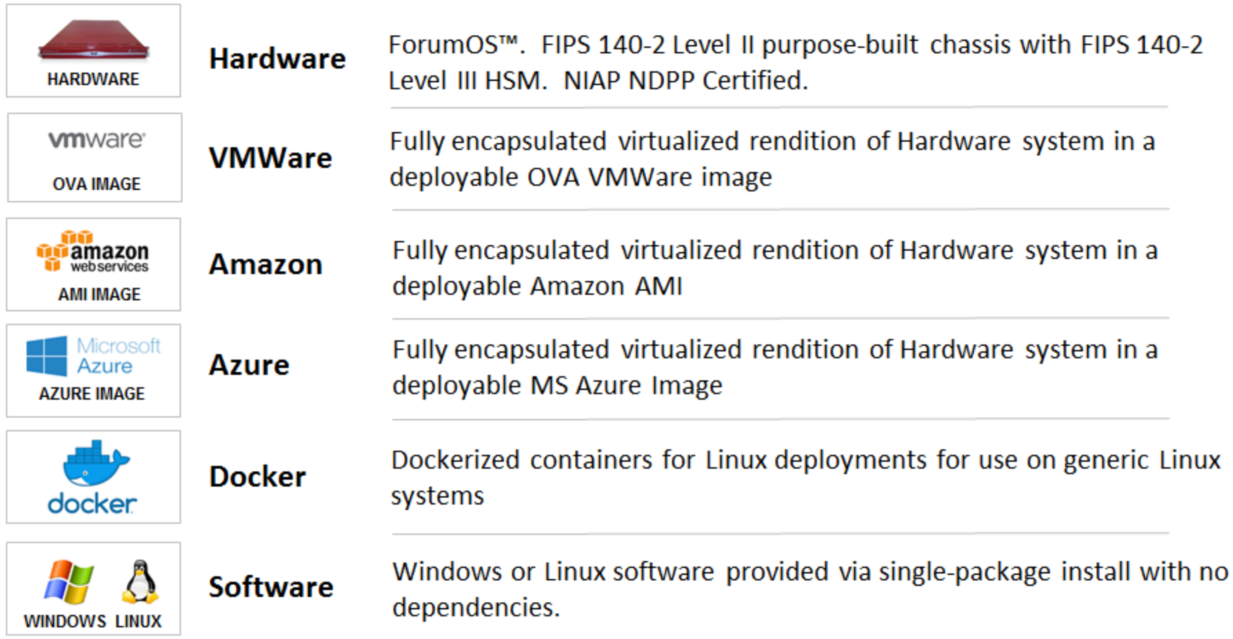
Forum Systems Sentry™ Version 9.1 Microservices and Docker Best Practices Guide, published June 2020.

D-ASF-SE-602324

Table of Contents

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.

Automated Software Deployments on 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.

Pre-Provisioning a Sentry Docker Instance for Deployment

Staging the policy sets enables a pre-determined list of policies to be deployed and activated during the automated installation. 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.

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.

Automated Software Deployment and Provisioning Procedure

Automated Software Deployment and Provisioning of Sentry include the ability to automate the installation of Sentry and to provision the policies on Sentry. Forum Sentry software comes in a fully encapsulated InstallIAnywhere package. The installation package can be installed using the "-i silent" command line option to eliminate prompts and provide for automated installations.

Automated Silent Install

Sentry is available in software form for Linux or Windows and is packaged into a single binary distributable with no external dependencies. This allows a silent installation of Sentry via scripting. The Sentry installer accepts a silent flag to that indicates the installation should be performed in silent mode, without requiring any user intervention.

The format of this is:

```
/opt/installers/forumsentry/${FSGBINARY} -i silent
```

Where **${FSGBINARY}** represents the name of the Sentry installation package.

Automated Licensing

Sentry requires a license in order to run. The license file is a digitally signed XML file with the name **license.xml** and this file resides in the subdirectory "**xmlserver/config"** in the installation directory. For example:

/root/ForumSystems/xmlserver/config/license.xml

Thus, in order to automate the installation of Sentry, you will also need to automate the provisioning of the license file. This is a simple process of copying the desired license to overwrite the existing license.xml.

For example:

```
cp – p /opt/installers/forumsentry/${FSGLICENSE}  /root/ForumSystems/xmlserver/config/license.xml
```

where **${FSGLICENSE}** is the name of the license file to copy.

Starting and Stopping the Forum Sentry Service

Forum Sentry runs as a service. Depending on the target OS you are running Sentry on (i.e. different distributions of Linux or Windows) the format of the command below may be slightly different.

Start the Sentry service:

```
/etc/init.d/xmlserver start
```

Stop the Sentry service:

```
/etc/init.d/xmlserver stop
```

Custom Configuration for Baseline Policy Auto-Configuring

Another key aspect in auto-provisioning is establishing a baseline policy set to apply to an installed Sentry instance. 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 (Note: For more information about FSX policies, please see the System Management Guide “Global Device Management” section).

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.properites ***with*** the FSX import information. I.e.

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

3) Start the Sentry service in order to process the config.properties file.
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

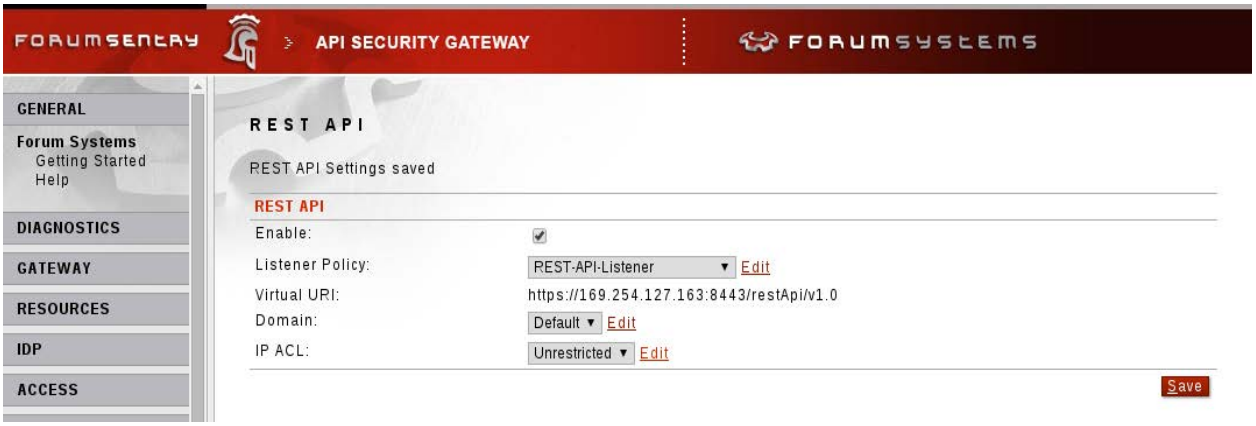
6) Start the Sentry service .

REST API Automation

Sentry supports adding, modifying, and deleting policies via a REST API automation interface. 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 the REST API automation and features, please refer to the Sentry REST API Guide.

Provisioning Sentry via REST API

The Forum Sentry REST API is enabled via the System->Configuration->REST API menu. 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.



REST API

REST API Settings saved

REST API

Enable: ☑

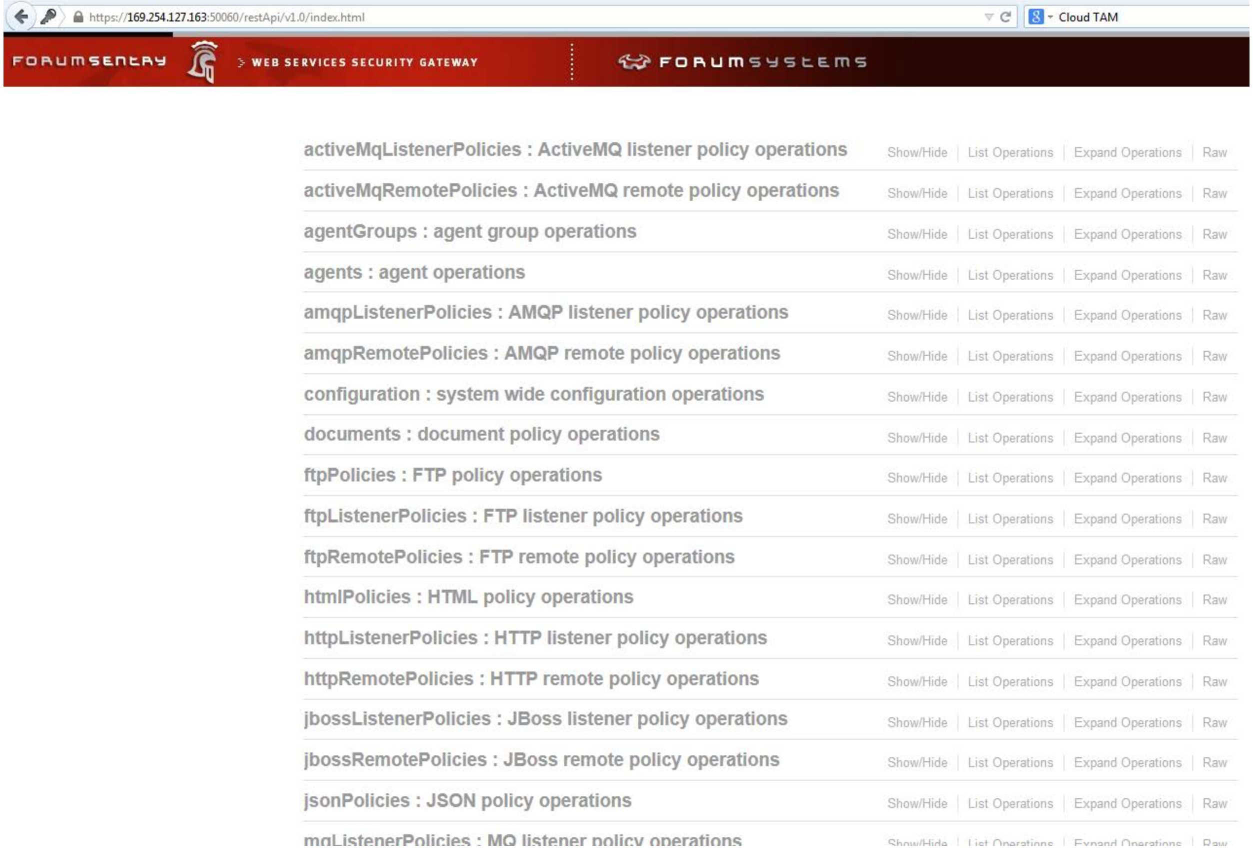
Listener Policy: REST-API-Listener ▾ Edit

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

Domain: Default ▾ Edit

IP ACL: Unrestricted ▾ Edit

Figure 1: REST API Enablement


https://169.254.127.163:50060/restApi/v1.0/index.html
Cloud TAM
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

Figure 1: Forum Sentry REST API Self-Documenting Interface

Sample Scripts

The Sentry support helpdesk has access to sample scripts which provide examples on the various topics above. The helpdesk article is:

The samples include the following example script files:

config.properties.core_policy	Example of a config.properties with an FSX import
config.properties.nofsx_policy	Example of a standard config.properties
install.inc	Example of an include file with variable references
install_forum.sh	Example of a script which performs all the automation functions
start.sh	Example of a script to start Forum Sentry service
stop.sh	Example of a script to stop Forum Sentry service
uninstall_core_config.sh	Example of using an FSX to reset/revert policies
uninstall_forum.sh	Example of uninstalling Forum Sentry