



FORUM SENTRY API SECURITY GATEWAY
QUICK START GUIDE
V9.1

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 © 2002-2020 Forum Systems, Inc. – All Rights Reserved.

Forum Systems Quick Start Guide, published July 2020.

D-ASF-SE-015457

Table of Contents

I.	Introduction	4
II.	Requirements and Installation	4
1.	Minimum Requirements	4
2.	Forum Sentry Software Installation Procedures	4
3.	Forum Sentry Virtual Appliance Installation Procedures.....	5
4.	Forum Sentry Hardware Appliance Installation Procedures	6
5.	Forum Sentry AMI Installation Procedures	7
6.	Licensing Forum Sentry	8
III.	Deploying a SOAP API - Creating a WSDL Policy	9
1.	Importing a WSDL	9
2.	Creating the WSDL Policy.....	10
3.	Reviewing the WSDL Policy and Enable WSDL Access	11
4.	Review the Associated Network Policies	12
IV.	Testing the Sentry WSDL Policy.....	13
1.	Obtaining SOAPSonar from Crosscheck Networks	13
2.	Loading the WSDL into SOAPSonar.....	13
3.	Sending a Request to the Sentry WSDL Policy	15
4.	Reviewing Transactions in the Sentry System Log.....	16
V.	Deploying a REST API – Building a REST Policy	18
1.	Creating the REST Policy.....	18
2.	Reviewing the REST Policy and Building Additional Virtual Directories	18
3.	Review the Associated Network Policies	19
VI.	Configuration Next Steps and Additional Information	20
1.	Configuration Next Steps	20
2.	Contacting Forum Systems Support	20
3.	Forum Sentry Documentation	20

I. Introduction

The Forum Sentry Quick Start Guide will provide an introduction to the Forum Sentry API Security Gateway product from Forum Systems. The guide will cover initial requirements and installation procedures for all four form factors: Hardware Appliance, Virtual Appliance, AWS AMI, and Sentry Software packages.

This guide will detail how to deploy SOAP and REST APIs through Sentry, send transactions for these policies and review the details of the transactions within the Sentry logs.

Links to the full Sentry documentation are included in the last chapter, as is the full contact information for Forum Systems Support.

II. Requirements and Installation

1. Minimum Requirements

Please visit the link below to see the minimum requirements for the various Forum Sentry form factors, including software, Virtual, and Cloud formats.

[Forum Sentry Minimum Requirements](#)

2. Forum Sentry Software Installation Procedures

The Sentry software installation is a wizard based install package with steps for installing on the target machine. When the installation is completed per the steps below, the Web Administration interface (WebAdmin) will be able to be accessible from a web browser on that machine using the address: <https://127.0.0.1:5050>.

If you have not yet obtained a license key for Sentry, the initial login page at the link above will provide instructions for obtaining and applying a Sentry license.

****IMPORTANT NOTES****

- If you will be using the on-board ClamAV virus detection with a Sentry software instance, you will need to install and maintain ClamAV separately. For more information please contact support@forumsys.com.
- If you will be using Tivoli Access Manager with a Sentry software instance, there is a separate process you will need to run on the host OS before this feature will work in Sentry. For more information please contact support@forumsys.com.

The instructions for installing the software instances can also be used for upgrading the software instances.

Installing on Windows:

1. Navigate your file system and click on the downloaded installation package.
2. The installation package Introduction screen will appear. Click **Next**.
3. The License Agreement screen appears.
4. Read the product License Agreement terms and conditions. To accept the License Agreement, check the **I accept the terms of the license agreement** radio button, and then click **Next**.
5. The Choose Install Set screen appears. Click **Next**.

6. The Choose Install Folder screen appears. Use the default location or enter a new location to install the software and click **Next**.
7. The Pre-Installation Summary screen displays a summary of install options. Click **Install** to begin the installation.
8. Once installation is complete, the Install Complete screen appears. Click **Done** to configure and start the Forum service. Your default web browser will be launched to access the Web Administration interface at <https://127.0.0.1:5050>.
9. A Security Alert screen appears for the default SSL Certificate used by the Forum service. Accept this Certificate to access the Web Administration interface.

NOTE: These instructions also pertain to upgrading the Sentry Windows software instances. To upgrade, stop the "Forum Sentry" service and then install on top of the existing version. It is recommended that you back-up the full Sentry configuration file (.FSX) from the Import/Export screen before upgrading.

Full upgrade instructions are available at <https://helpdesk.forumsys.com>.

Installing on Linux or Solaris:

1. Navigate your file system and set the downloaded package to be executable (**chmod +x**).
2. Run the installation file (./<install-file>.bin). The Introduction screen will appear. Verify you have the appropriate minimum system requirements and are logged in as root. Press <ENTER> to continue.
3. Read the license agreement and choose whether to accept it.
4. Press <ENTER> to accept the default Install Set.
5. Press <ENTER> to accept the default location, or specify the install location.
6. Review the Pre-Installation Summary and press <ENTER> to continue.
7. Press <ENTER> again to install to the location specified.
8. Press <ENTER> to complete the install.
9. To start the daemon, type: **/etc/init.d/xmlserver start**.
10. To stop the daemon, type: **/etc/init.d/xmlserver stop**.
Note that on Linux you can use the "service xmlserver start/stop/restart" commands.
11. Once the daemon has started, access the Web Administration interface through a web browser at <https://127.0.0.1:5050>.
12. A Security Alert screen appears for the default SSL Certificate used by the Forum service. Accept this Certificate to access the Web Administration interface.

NOTE: These instructions also pertain to upgrading the Sentry Linux and Solaris software instances. To upgrade, stop the "xmlserver" daemon and then install on top of the existing version. It is recommended that you back-up the full Sentry configuration file (.FSX) from the Import/Export screen before upgrading.

Full upgrade instructions are available at <https://helpdesk.forumsys.com>.

3. Forum Sentry Virtual Appliance Installation Procedures

The Forum Sentry virtual appliances run the FIPS certified ForumOS™ operating system. Sentry virtual appliances run within VMware infrastructure. An OVA file from Forum Systems is required to install and run the Sentry virtual appliance.

Some general instructions are included below. For detailed installation steps please refer to the "FS **Sentry VMware Virtual OS Installation Guide**" available from Forum Systems Support.

- The OVA file is run on VMware server technology and has the same "look and feel" as the Sentry hardware appliances.
- Once booted up, you'll be prompted with our command line interface (CLI) wizard to apply the network settings, set the CLI enable mode password, and create the admin account.

- For more information on the network topology options and initial CLI wizard see the hardware installation procedures in section 4 of this chapter.
- For evaluations Forum Systems typically recommends One Port topology mode which uses two IPs total - one for MGMT (web administration and SSH to CLI) and one for WAN (runtime traffic).
- If both IPs will be in the same subnet, you'll need to disable the MGMT filter using the CLI command: "network config mgmt-filter" run from Enable Mode.
- Once you have completed the CLI installation wizard, you will need to assure that the virtual WAN, LAN and MGMT interfaces are mapped to the desired virtual networks within your host environment (see the "**FS Sentry VMware Virtual OS Installation Guide**").
- The CLI has two modes, Command Mode (ForumOS>) and Enable Mode (ForumOS#). Command mode is the default and doesn't allow modifications. Enter Enable Mode by typing "Enable" and then the enable mode password, which is set up during the initial configuration wizard.
- Once the device is provisioned, access the WebAdmin interface via browser using https://mgmt_IP:5050. The page will prompt for a license. Send all of that information to licenses@forumsys.com to receive a license.
- The WebAdmin interface is where you will build all runtime policies in Forum Sentry.

4. Forum Sentry Hardware Appliance Installation Procedures

The Forum Sentry appliances run the FIPS certified ForumOS™ operating system. Each appliance will need to be racked and configured for network access. The user interfaces to the Sentry appliances are the CLI (command line interface) accessible via SSH (network) or Serial console (physical) and the WebAdmin interface available via HTTPS. There is no monitor, keyboard, or mouse access.

Each appliance has 3 network interfaces:

- MGMT for management traffic
- WAN for external traffic
- LAN for bridging to the internal network.

These interfaces can have IP addresses and Ports bound to them for various functions. Routing across the interfaces is based on standard routing rules. The interfaces do not operate as a Network Switch, but rather the interfaces will always consult the routing table to determine how to route packets. Be sure to plan your IP addresses, netmask definitions, and static routes accordingly.

It is also important to determine how the network interfaces are to be used. The management port can be set to any of the 3 interfaces, but is bound to the physical MGMT interface by default. If you choose to use the dedicated MGMT interface for the management port, be sure that the MGMT network is properly segmented and that no machines that can access the MGMT network can access the WAN or LAN networks, otherwise you will be creating a network loop and can experience network issues.

The steps below provide a quick outline of installation procedure. For detailed instructions and for more details on the networking options, please see the **Sentry Hardware Installation Guide**, and if you have a Sentry HSM enabled appliance, please review the **Sentry HSM Quick Start Guide**.

1. Unpack and install the Sentry appliance into a rack unit.
2. Power on device and connect to the Serial port using the supplied null modem Serial cable.
3. Access the CLI via Serial console. The configuration wizard will appear.
4. If you are using an HSM enabled Sentry system, the configuration wizard will first request initialization of the HSM Security World. Otherwise, skip to step 5. Connect the admin card reader and prepare the Admin card set to initialize to the security world (or you can use an already initialized admin card). It is recommended that you use at least 5 admin cards to initialize a security world to ensure redundancy. The wizard will request passwords for each of

the admin cards. The admin card is only required when creating the security world. Each new Sentry HSM hardware device can be initialized into an existing Security World to allow secure storage of keying information only within the defined Security World.

5. Complete the initial configuration wizard by providing the administration user, the enable mode password, and the topology mode. The most common topology mode used is **INLINE / 2 IP**

INLINE / 2 IP

- a) Connect the WAN port to your data network.
- b) Connect the LAN port the other side of your data network.
- c) Connect the MGMT port to your private management network

or

- d) From the CLI, enter 'enable' and type the enable mode password
- e) type '**network config mgmt-iface**' and choose either **LAN** or **WAN** as the physical interface to bind the management port to.

6. Provide the IP addresses for the interfaces as requested by the CLI wizard.
7. Provide the default gateway IP address as requested by the CLI wizard.
8. Provide the DNS server(s) as requested by the CLI wizard.
9. Once the wizard has completed for the first time, the system will reboot and the Web Administration interface will be available from a web browser.

5. Forum Sentry AMI Installation Procedures

The Forum Sentry AMI for Amazon Web Services (AWS) is a virtual instantiation of the FIPS certified ForumOS™ operating system running within AWS EC2.

Some general instructions are included below. For detailed installation steps please review the [Forum Sentry AMI Installation Guide](#)

- Find the Forum Sentry AMI in the AWS Marketplace or under "public images" on the AMI page in the EC2 console
- Launch an instance specifying the appropriate Instance Type (see [Forum Sentry Minimum Requirements](#))
- Ensure that the Inbound Security Group for the instance allows access on port 22 (SSH) and TCP port 5050 (for WebAdmin interface via Browser)
- Access the Sentry WebAdmin interface via browser using the syntax: https://ip_or_dns_name:5050
- You will be prompted for a license, see section 6 below
- After applying a license, you are prompted to create a new Admin account
- After creating the Admin account, you are logged into the WebAdmin
- SSH into the instance using the same IP or DNS name used to access the WebAdmin interface, using the Admin account created in the previous step
- Upon first SSH access, you are prompted to enter an Enable Mode password – which is machine specific and not related to the Admin account
- The setup is now complete

Notes:

- While it is possible to run instances in other AWS regions, the AMI is only in N. Virginia – to run in another region, you'll need to first launch in N. Virginia then create your own AMI from that instance, then copy that new AMI to whatever region you want.

6. Licensing Forum Sentry

This section applies to the Sentry software, virtual, and AMI instances only - Sentry hardware appliances are licensed at the factory before shipping.

When the Sentry installation completes, you will be required to import a license before logging into the WebAdmin interface. The information required to obtain an evaluation license includes your Contact Name, Company Name, email address of Primary Contact and the displayed unique server ID.

If you do not already have a license, send this information to licenses@forumsys.com to obtain a license.

For more information on using the Forum Sentry Floating License Model with v9.1 and later, please see the [Forum Sentry License Server User Guide](#).

LICENSE WARNING

A license for the server was not detected.

To request a floating license, please fill in the form below.

If a permanent license has already been obtained, upload the license in the form below.

To obtain a permanent license, please email licenses@forumsys.com or contact Forum Systems Customer Service at (888) 811-0060 and provide the following information:

- Name
- Company Name
- Purchase Order
- Email Address
- Server ID — EC290346-9CBB-235E-2D58-C26FC850B4E9
- Product — Sentry
- Product Version — 8.11.39
- Operating System — ForumOS
- Cores — 2

LICENSE REQUEST

Licensing Model: Floating Permanent

License File*:

When you receive the license.xml file from Forum Systems, browse to the license and click Import to apply it.

If the licensing is successful, you will be prompted to create a new Administrator user for the Sentry WebAdmin interface.



Notes: For software instances (Windows and Linux), if you are unable to access the WebAdmin interface using the address: <https://127.0.0.1:5050>, ensure the Sentry service is running (“Forum Sentry” on Windows and “xmlserver” on Linux).

If the service is running but you still cannot access the page, ensure there are no local firewalls preventing this communication. You may also need to adjust your browser’s proxy settings and verify that port 5050 is bound and active using ‘netstat’.

After you have created the new administrator user you are logged into the WebAdmin interface. The default page is the Getting Started page.

III. Deploying a SOAP API - Creating a WSDL Policy

A WSDL policy in Sentry is a set of rules that provide a policy for processing of Web Service SOAP messages flowing through the system WSDLs can be imported from a file, URL or UDDI search. This Quick Start Guide assumes the user has a SOAP Web Service with a WSDL that they want to protect with Forum Sentry.

The steps below provide an outline for building a Sentry WSDL Policy. For more information and detailed instructions please review the **WSDL Policies Guide** available through the Help menu in the WebAdmin interface.

1. Importing a WSDL

1. Log into the WebAdmin interface and navigate to the Gateway>>Gateway Policies>>WSDL Policies page.
2. Click **New** to create a new WSDL Policy. A WSDL can be loaded via File, URL, from a UDDI or from an existing WSDL Library.

The screenshot shows the 'NEW WSDL POLICY' configuration page in the Forum Sentry Web Services Security Gateway. The page layout includes a top navigation bar with the Forum Sentry logo and 'WEB SERVICES SECURITY GATEWAY' text, and the Forum Systems logo. A left sidebar provides navigation for various system components. The main form area is titled 'NEW WSDL POLICY' and contains the following fields and controls:

- Name*:** A text input field.
- Description:** A text input field.
- WSDL Source:** Three radio button options:
 - File:** Selected. Includes a text input field and a 'Browse...' button.
 - URL:** Includes a text input field and a 'Browse UDDI' button.
 - WSDL Library:** Includes a dropdown menu.
- HTTP Basic Authentication:** Includes 'Username' and 'Password' text input fields.
- Automatically load imported files:** A checkbox.
- Next:** A red button to proceed to the next step.

The footer of the page displays '©2002-2010 FORUMSYSTEMS', 'FIPS MODE: OFF', 'Active Domain: Default', and a 'LOGOUT' button.

3. The WSDL Policy name will be auto-generated based on the URI or Filename fields. Once you have chosen your method of importing the WSDL click **Next**.

2. Creating the WSDL Policy

1. On the next screen you will create (or select) the network Listener Policy, the Virtual Directory Path, and the network Remote Policy.

The screenshot shows the 'NEW WSDL POLICY' configuration page in the Forum Sentry Web Services Security Gateway. The interface is divided into a left-hand navigation menu and a main configuration area.

Navigation Menu (Left):

- GENERAL
- Forum Systems
 - Getting Started
 - Help
- DIAGNOSTICS
- GATEWAY
 - Gateway Policies
 - Network Policies
 - Proxy Policies
 - WSDL Libraries
 - WSDL Policies
 - XML Policies
 - Task List Groups
 - Task Lists
 - Documents
- RESOURCES
- IDP
- ACCESS
- SYSTEM
- PARTNERS

Main Configuration Area:

WSDL POLICIES > NEW WSDL POLICY

SET LISTENER POLICY

Please specify a listener policy for service: QAServices, port: QAServicesSoap

Create a new HTTP listener policy

Listener Policy Name*:

Use Device IP:

Listener IP*:

Listener Port*:

SET VIRTUAL DIRECTORY PATH

Virtual Directory Path:

SET REMOTE POLICIES

Send to remote server

Please specify a remote network policy for the URL: http://10.5.1.17/qaservice/qaservice.asmx

Create a new HTTP remote policy for this remote server

Remote Policy Name*:

Remote Policy Host*:

Remote Policy Port*:

Next

©2002-2010 FORUMSYSTEMS FIPS MODE: OFF Active Domain: Default LOGOUT

- The listener policy is the IP and Port that Sentry will listen on for incoming traffic for this WSDL policy.
- The “Use Device IP” option selects the WAN IP address (the device IP) as the listening IP address.
- The Virtual Directory Path is the path for this WSDL policy (for the listener URI, this is everything after the port number).
- The remote policy is the actual endpoint for the service as defined in the imported WSDL. This is where Sentry will send the processed request - after receiving the incoming request and performing the IDP scan, schema validation, and any task processing defined in Sentry.
- The “Send to remote server” option should be enabled if you want to use this policy in proxy mode (send the processed request to a back-end service). Disable this option if you want to use this policy in service mode (the processed request is sent immediately back to the client – nothing is sent to a back-end service).

2. After entering the appropriate values, click **Next** to create the WSDL policy.

3. Reviewing the WSDL Policy and Enable WSDL Access

1. When the WSDL Policy has been successfully created, the status, the Virtual URI, the Physical URI, and each operation will be listed on the screen.

The screenshot shows the 'WSDL POLICY' configuration page for the 'qaservice' policy. It includes a table of services and a detailed view of the 'QAServices' service port 'QAServicesSoap'. The service is currently disabled. The detailed view shows several operations with their respective statuses (all green), ACLs (all '[Allow All]'), and associated input/output message links. The 'Echo' and 'SevrallInputs' operations are highlighted in red. There are 'Enable' and 'Disable' buttons for both the service and the detailed view.

2. Click on the hyperlinked PORT link to access the Virtual Directory settings page. On this screen you can make several changes to the WSDL policy, including selecting the Listener and Remote policies to associate, changing the virtual directory path, and enabling WSDL access.

By default, the WSDL generation and access is disabled. If you want your clients to be able to access the WSDL from the Sentry WSDL policy, enable this option by checking the checkbox.

3. For the purposes of this tutorial, ensure that the “Enable WSDL access” option is checked. The WSDL for this service can then be retrieved using the full Virtual URI with the ?WSDL syntax added at the end.

For instance, if the virtual URI is: <http://192.168.0.14:80/qaservice/qaservice.asmx>

Use this URI to retrieve the WSDL: <http://192.168.0.14:80/qaservice/qaservice.asmx?WSDL>

Enter this link into a web browser and verify that the WSDL document is shown. This is the newly generated WSDL document from Forum Sentry and will have the Sentry listener policy endpoints as the service port locations, such that clients will communicate directly with Sentry as the service provider.

Note: to publish the WSDL on a public IP or NAT IP, simply check the “Publish a different location in exported WSDL” option and enter the appropriate IP and Port information.

4. Review the Associated Network Policies

1. Navigate to the Gateway>>Gateway Policies>>Network Policies page of the WebAdmin interface. Here you will see the HTTP Listener and HTTP Remote policies generated while creating the WSDL Policy.

A Listener Policy can be of many different protocol types including HTTP, FTP, MQ, EMS, sFTP, and more. A listener policy does the following:

- Defines the IP and Port and the Protocol (HTTP, HTTPS, etc.)
- Defines Get Queue to listen for inbound messages (MQ, EMS, JMS, etc)
- Provides Policy level IP filtering
- Provides Credential based Access Control

A Remote Policy can be of many different protocol types including HTTP, FTP, MQ, EMS, sFTP, and more. A remote policy does the following:

- Defines the remote IP and Port that Sentry will communicate with (HTTP, HTTPs, etc)
- Defines Send Queue to publish processed messages (MQ, EMS, JMS, etc)
- Defines Failover and Load-Balancing for Back-End services (Group Remote Policies)
- Provides back-end protocol authentication
- Provides optional response processing (applying policies to the response document)

IV. Testing the Sentry WSDL Policy

After creating a WSDL Policy on Sentry, administrators will want to test the policy. We recommend using the free edition of the SOAPSonar Service Testing tool from Crosscheck Networks to generate the SOAP messages to test the Sentry policies.

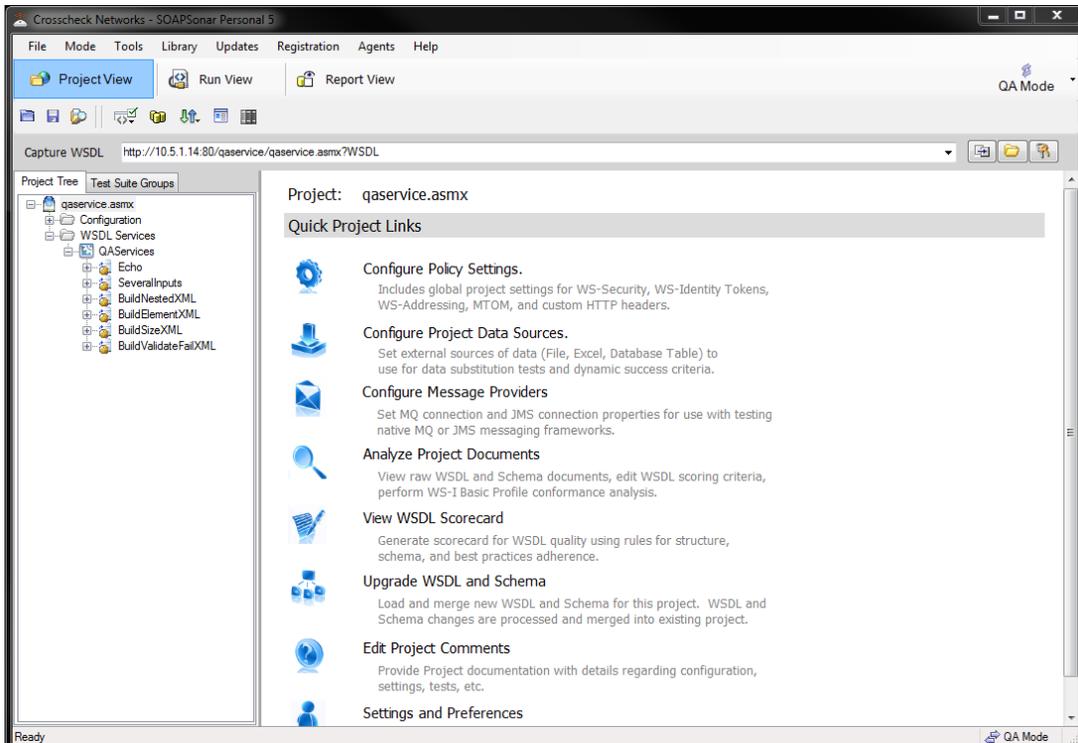
For assistance with SOAPSonar, please contact support@crosschecknet.com.

1. Obtaining SOAPSonar from Crosscheck Networks

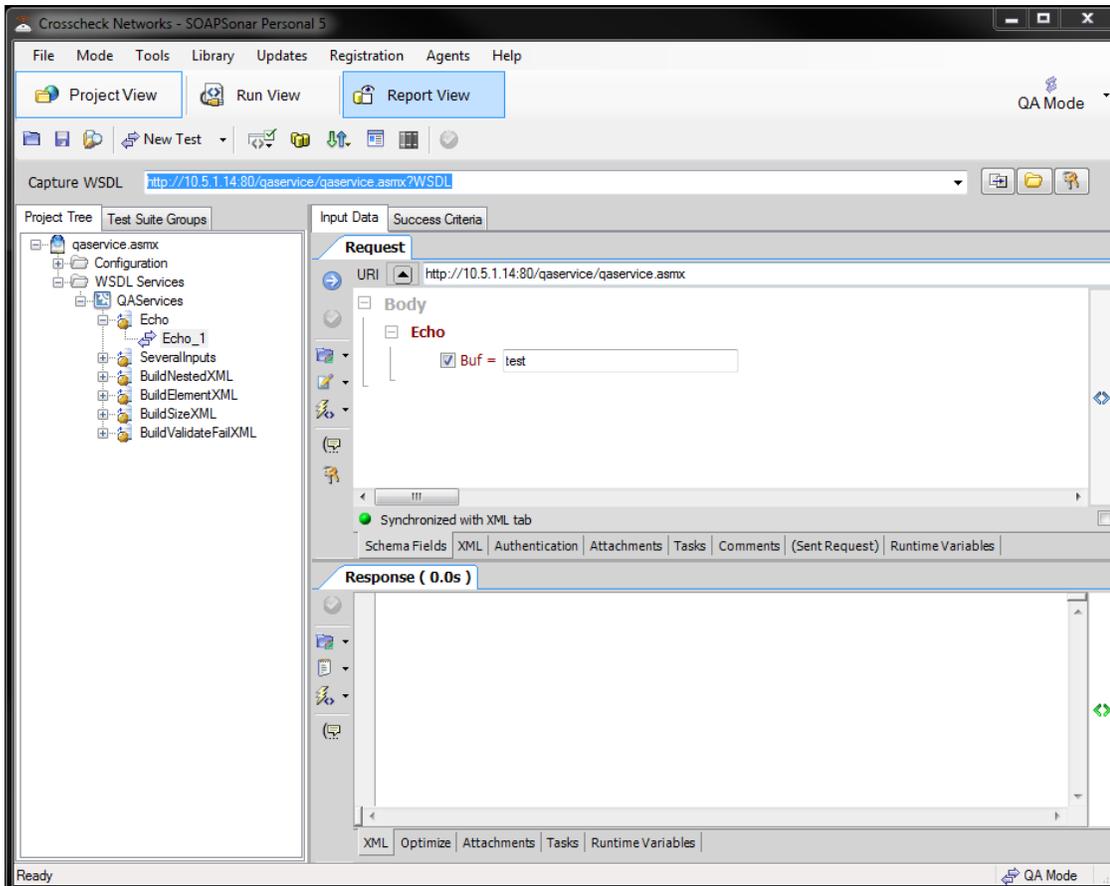
1. You can obtain the free SOAPSonar Personal Edition from: <http://www.crosschecknet.com/download/soapsonarpersonal.php>
2. SOAPSonar runs on Windows only and requires the .NET 2.0 (or later) Framework.
3. Installation is straight forward. Install with full admin rights and activate online or via email.

2. Loading the WSDL into SOAPSonar

1. Launch SOAPSonar and enter the link to the generated WSDL on Sentry within the “Capture WSDL” field. Click the capture button to the right of this field to retrieve the WSDL from Sentry.



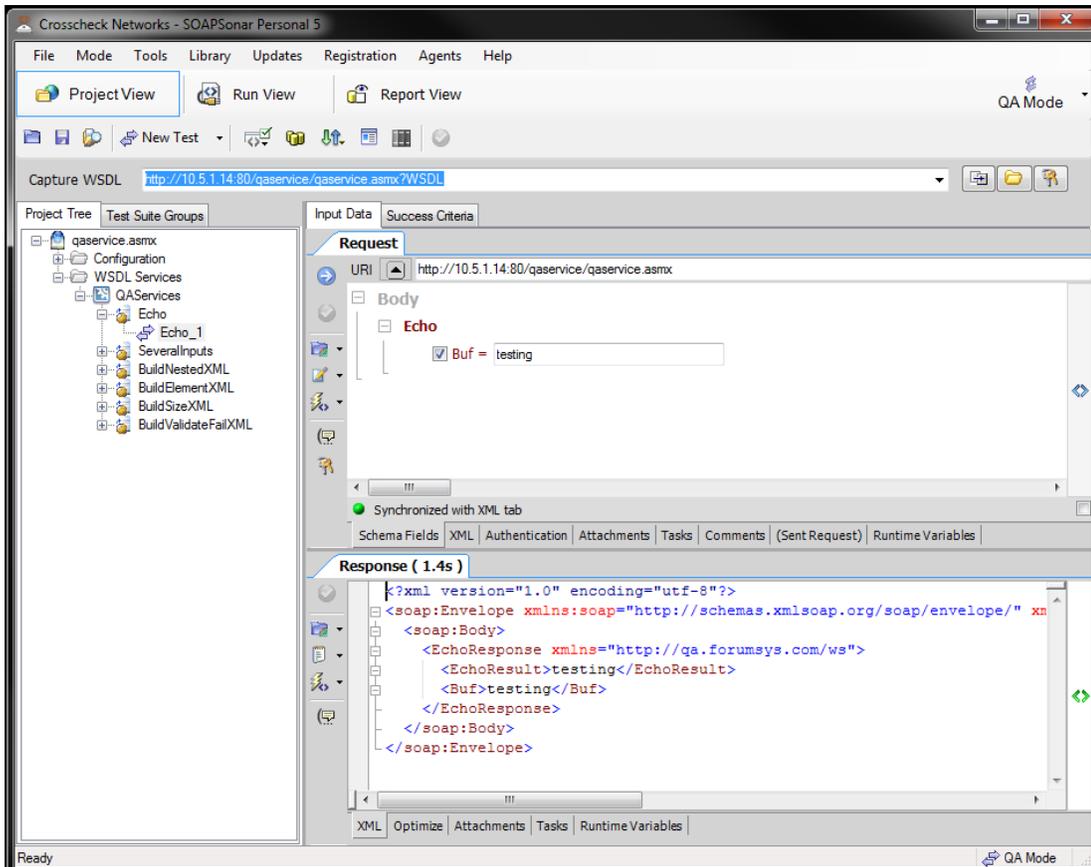
2. The WSDL interfaces will be automatically parsed and test cases automatically generated under each WSDL operation. Click on an Operation to open the default test case that was generated.
3. Under Project Tree on the left, expand out to see a test case. You'll see the Request window open showing the Schema Fields view. This allows you to easily enter data for each element of the SOAP request being generated. Click on the XML tab to see the auto-generated SOAP message from the schema field values provided.



4. Notice that the Request also has a URI field. This is auto populated based on the endpoint defined in the WSDL. As this WSDL was retrieved from the Sentry WSDL Policy, the URI should be the Virtual URI for the Sentry WSDL Policy.

3. Sending a Request to the Sentry WSDL Policy

1. Enter some request data and click the  icon to commit the settings. Then click the  icon to send the request to the Sentry WSDL Policy.
2. The response message should show up on the Response tab (either below the request window or next to it). This is the response message that is coming back from Sentry. If the processing is successful on Sentry, the request will go from Sentry to the remote server and the response will be proxied back through Sentry to the client.



3. You have now sent a request transaction through the Sentry WSDL policy. Try sending an invalid request by modifying the request XML (on the XML tab) and notice that Sentry will block the message and return a SOAP fault error message.

4. Reviewing Transactions in the Sentry System Log

To review or troubleshoot transactions processed by Sentry, you will review the Sentry System Log.

1. In the WebAdmin interface, go to the Diagnostics>>Logging>>Settings page.
2. Set the System Log Logging Level to DEBUG (for testing purposes only).
3. Send another request from SOAPSonar to Sentry.
4. Access the Sentry System log on the Diagnostics>>Logging>>Internal Logs page. Select the Today log to view the most recent transactions.
5. The System log has 6 columns:
 - ID: A unique ID for each log message

- Time: The timestamp for each log message
- Session: Each log message for a specific transaction has the same session ID. This allows for easy filtering of the log to only show log messages for a specific transaction.
- Code: Each type of event is logged with its own logging code. You can configure Sentry to only allow certain codes.
- Level: Each log level has an associated log level; you can configure Sentry to only log certain levels.
- Message: The log message.

INTERNAL LOGS > SYSTEM LOG

DEC 29, 2010

Filter By: Debug Search Refresh: (11-30 secs) Reset

Filter By Policy Name:

51 items found, displaying all items.1

ID	Time	Session	Code	Level	Message
0004C1	17:11:21.992	X0296A5	08402	D	Document left Communications Layer
0004C0	17:11:21.991	X0296A5	0840C	D	Sending client a raw response: Status Code: 200 Header Info: ...
0004BF	17:11:21.990	X0296A5	09334	D	Adding Via header to response
0004BE	17:11:21.989	X0296A5	09330	D	Stored header suppressed from proxying - content-length: 359
0004BD	17:11:21.988	X0296A5	0914D	D	Request filter encode: document was generated locally; encoding with 'simple' format
0004BC	17:11:21.987	X0296A5	08408	D	Response document: <?xml version="1.0" encoding="utf-8"?><soap:Envelop...
0004BB	17:11:21.987	X0296A5	09604	D	Simple decode succeeded
0004BA	17:11:21.985	X0296A5	09607	D	Decoding a document of 359 bytes
0004B9	17:11:21.984	X0296A5	09211	D	Received an HTTP response: Protocol: HTTP/1.1 Response Code: 200 ...
0004B8	17:11:21.160	X0296A5	0840B	D	Sending remote server a processed request: Remote Path: /qaservice/qaservice.asmx ...

- The latest log messages are listed at the top of the page. After you send a request, click the Session ID to show only the log messages for that transaction. Then scroll to the bottom to see the first log message: "Document entered communications layer".
- Going up from there, you'll see the incoming request headers, the actual request itself, and all processing Sentry performs on the request.
- When you see the "Sending remote server a processed request" message, this indicates that the request processing was successful and Sentry is now proxying the request to the remote server.
- Processing errors will show up highlighted in yellow.
- The last log message for a transaction will be "Document left communications layer". This indicates that the response has been sent to the client and processing in Sentry is complete.

V. Deploying a REST API – Building a REST Policy

A REST policy in Sentry is a set of rules that provide a policy for processing of RESTful Web Service requests and responses flowing through the system.

Unlike a SOAP API, there is no WSDL to import into Sentry. Building a REST policy in Sentry is very similar to building an XML, JSON, or HTML policy. The steps are essentially the same for all of them.

The steps below provide an outline for building a Sentry REST Policy. For more information and detailed instructions please review the **XML Policies Guide** available through the Help menu in the WebAdmin interface.

1. Creating the REST Policy

1. Under the Gateway >> Content Policies menu, click on REST Policies. Click new to start the wizard to build the REST policy. Provide a Name, Description (optional), and Label (optional) for the REST policy, click **Next**.
 - Select or build the Listener policy - The listener policy is the IP and Port that Sentry will listen on for incoming traffic for this REST policy.
 - The “Use Device IP” option selects the WAN IP address (the device IP / host OS machine IP address) as the listening IP address.
 - The Virtual Directory Path is the path for this REST policy (for the listener URI, this is everything after the port number).
 - The remote policy is the actual endpoint for the service. This is where Sentry will send the processed request - after receiving the incoming request and performing the Access Control, IDP scan, schema validation, and any task processing defined in Sentry.
 - The “Send to remote server” option should be enabled if you want to use this policy in proxy mode (send the processed request to a back-end service). Disable this option if you want to use this policy in service mode (the processed request is sent immediately back to the client – nothing is sent to a back-end service).
2. After entering the appropriate values, click **Next** to create the REST policy.

2. Reviewing the REST Policy and Building Additional Virtual Directories

1. When the REST Policy has been successfully created, the status, the Virtual URI, and the Physical URI are listed on the screen. You can add multiple virtual directories to the same REST policy and many use cases will require this.

For instance, many SSO use cases will have a “service mode” **/login** virtual directory that simply consumes user credentials then sets a cookie and redirects the client to the **/service_path** virtual directory - which requires cookie authentication. In this case the **/login** directory never proxies to a remote server.

When a request comes into Sentry, if it does not match a defined virtual directory it will be rejected (404 virtual directory not found). Using a root virtual directory (/) will catch all traffic.



2. Click on the name of the Virtual Directory (“New Virtual Directory” by default) to access the Virtual Directory settings page. On this screen you can make several changes to the REST policy, including selecting the Listener and Remote policies to associate, changing the virtual directory path, and enabling adding Access Control.

IMPORTANT for REST and HTML policies, it is recommended to change the default Filter Expression on the Virtual Directory page to simply .* (that’s, dot star) which is a wildcard value that allows all characters after the virtual path. Without this change, requests with query parameters in the URI will be rejected by Sentry.

3. Review the Associated Network Policies

1. Navigate to the Gateway>>Gateway Policies>>Network Policies page of the WebAdmin interface. Here you will see the HTTP Listener and HTTP Remote policies generated while creating the REST Policy.

A Listener Policy can be of many different protocol types including HTTP, FTP, MQ, EMS, sFTP, and more. A listener policy does the following:

- Defines the IP and Port and the Protocol (HTTP, HTTPS, etc.)
- Defines Get Queue to listen for inbound messages (MQ, EMS, JMS, etc)
- Provides Policy level IP filtering
- Provides Credential Based Access Control

A Remote Policy can be of many different protocol types including HTTP, FTP, MQ, EMS, sFTP, and more. A remote policy does the following:

- Defines the remote IP and Port that Sentry will communicate with (HTTP, HTTPS, etc)
- Defines Send Queue to publish processed messages (MQ, EMS, JMS, etc)
- Defines Failover and Load-Balancing for Back-End services (Group Remote Policies)
- Provides back-end protocol authentication
- Provides optional response processing (applying policies to the response document)

VI. Configuration Next Steps and Additional Information

1. Configuration Next Steps

After completing this Quick Start Guide, Sentry administrators may now want to further customize the Sentry policies. Some immediate considerations should be:

1. Configuring SSL/TLS – **Security Policies and PKI Guide**
2. User Identity and Access Control - **Access Control Guide**
3. Importing and Creating Keys – **Security Policies and PKI Guide**
4. Creating Task Lists – **Task Management Guide**

2. Contacting Forum Systems Support

Online Helpdesk - create support tickets, access forums, docs, FAQs: <https://helpdesk.forumsys.com>

Email Support: support@forumsys.com

Phone Support: + 1.781.791.7510 option 2

3. Forum Sentry Documentation

Full Sentry Documentation (also available through the WebAdmin interface):
http://www.forumsys.com/downloads/doc/FS_Sentry_V9.1_Docs.zip

Technical Papers
<https://www.forumsys.com/resources/white-papers/>

Sentry Data Sheet:
<https://www.forumsys.com/wp-content/uploads/ForumSentry-DataSheet-2020.pdf>