



# **FORUM SENTRY™ VERSION 9**

## **SAML WEB BROWSER SSO PROFILE**

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

Forum Sentry™ Version 9 SAML Web Browser SSO Profile Configuration Guide, Published May 2024

D-ASF-SE-051027

## Contents

Introduction to the Forum Sentry SAML Web Browser SSO Profile Guide .....	4
<i>Audience</i> .....	4
<i>Conventions Used</i> .....	4
<i>Assumptions</i> .....	4
Forum Sentry Support for SAML 2.0 Web Browser SSO Profile .....	5
<i>Introduction</i> .....	5
<i>Sentry as the Service Provider (SP)</i> .....	5
<i>Sentry as the Identity Provider (IdP)</i> .....	5
<i>Sentry as both the Service Provider (SP) and the Identity Provider (IdP)</i> .....	5
Forum Sentry SAML SSO Policy Configuration .....	6
<i>Configuring Sentry as the Service Provider (SP)</i> .....	6
Create a Redirect Policy .....	6
Create a Request Filter Policy .....	7
Create the User Identity and Access Control Task List Group .....	7
Create an HTML Policy .....	9
<i>Configuring Sentry as the Identity Provider (IdP)</i> .....	10
Create the STS Policy .....	10
<i>Testing the Forum Sentry SAML SSO Configuration</i> .....	11
Testing the SAML SSO Flow .....	11
More Information .....	11

# Introduction to the Forum Sentry SAML Web Browser SSO Profile Guide

## Audience

The *Forum Sentry™ SAML Web Browser SSO Profile Guide* is for Sentry Administrators who will configure Forum Sentry for SAML SSO Web Browser Profile as either an Identity Provider (IdP) or Service Provider (SP) or both.

## Conventions Used

A red asterisk ( \* ) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**  
Password: **\*\*\*\*\***

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

## Assumptions

This document assumes that the reader will review the appropriate chapter before performing the operations listed in this document.

This document also assumes that the reader is at least generally familiar with SAML SSO Web Browser Profile concepts, creating Forum Sentry Content Policies, and creating Forum Sentry Task Lists.

Not all steps in the configuration tutorial are listed out in detail.

# Forum Sentry Support for SAML 2.0 Web Browser SSO Profile

## Introduction

Forum Sentry supports SAML 2.0 Web Browser SSO Profile both as a Service Provider (SP) and an Identity Provider (IdP).

Forum Sentry supports both Service Provider initiated and Identity Provider initiated SAML 2.0 SSO.

The same Sentry instance can behave as either an SP or IdP or both, though typically the SP and IdP responsibilities are separated and each handled by a dedicated Sentry tier.

The SAML 2.0 SSO Web Browser profile utilizes automatic redirects to make the login process (which requires multiple hops) seamless to the end user.

This guide will outline how Sentry behaves as an SP through Content Policies as well as an IdP through STS Policies.

## Sentry as the Service Provider (SP)

As an SP, Sentry functions as a reverse proxy for an API or web site enforcing various security requirements, including enforcing access control and enabling single sign-on.

As an SP, Sentry will redirect unauthenticated requests sent to the protected API or web site to a configured service provider authentication URL (to an IdP).

At the SP authentication URL (the Sentry Virtual Directory) a task list containing a User Identity & Access Control task configured for SAML SSO redirects the client browser to an STS URL with a SAML POST authentication request. That STS can be a Sentry STS policy or another SAML 2.0 IdP.

## Sentry as the Identity Provider (IdP)

Sentry STS policies function as the IdP policies. An STS policy is used to consume a request and generate SAML responses. The STS policies support either SP initiated or IdP initiated SAML SSO.

SP Initiated – the user accesses the service (Sentry Content Policy) without valid credentials and the SP redirects the browser to the STS policy with a SAML request.

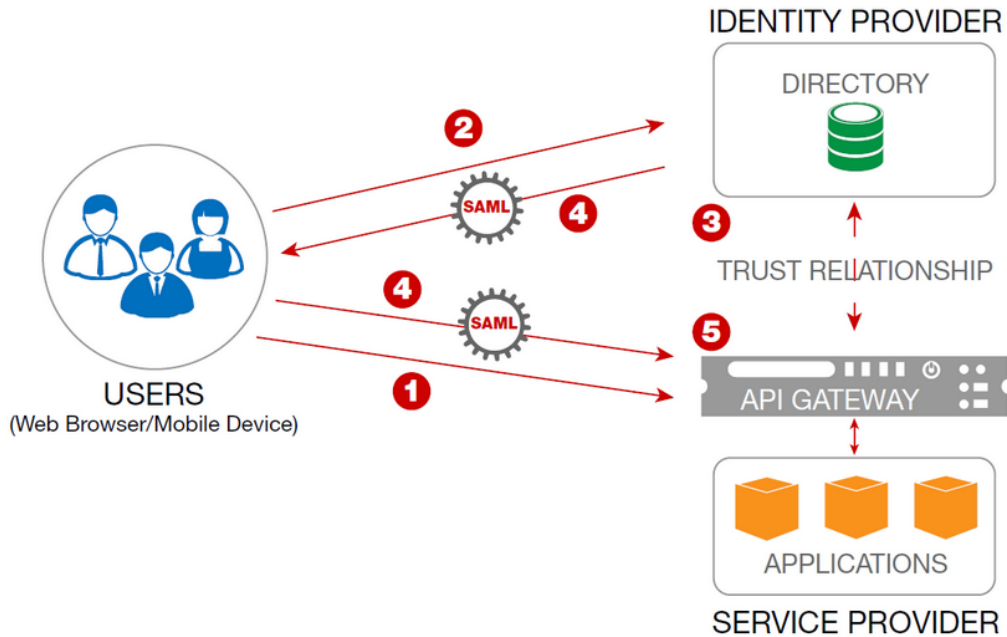
IdP Initiated – the user accesses the STS policy (IdP) directly with some authentication credential and is then redirected to the SP with a SAML to be validated.

## Sentry as both the Service Provider (SP) and the Identity Provider (IdP)

The following outlines a standard SP initiated flow with Sentry as both the SP and IdP.

1. The unauthenticated user (browser, mobile app, etc...) accesses the service at the Sentry Content policy virtual URI.
2. The Sentry Content policy redirects the user to the STS policy with a SAML request via a User Identity & Access Control task configured for SAML SSO.
3. The Sentry STS policy authenticates the client browser, e.g. with basic authentication.
4. The STS policy redirects the client browser back to the service provider authentication URL (the Content policy) with a SAML response.

5. The SAML SSO task at the service provider authentication URL (the Content policy) verifies the SAML assertion and redirects the client browser back to the original target URL with a session cookie to authenticate the user.



## Forum Sentry SAML SSO Policy Configuration

Forum Sentry supports a wide range of customer use cases as they pertain to SAML SSO. The procedures outlined in this document cover a general, standards based, approach to SAML SSO. It is likely that further specific customization of these policies will be required for each customer user case.

### Configuring Sentry as the Service Provider (SP)

#### Create a Redirect Policy

Create a Sentry redirect policy which will later be applied to the HTML Policy that handles the traffic for the protected service.

1. Specify the SP authentication URL, e.g. "http://192.168.82.203/login", as the URL for both "Authentication Fails" and "No Credentials". This will be one of the virtual directories of the HTML Policy used to handle the secured data flow.
2. Include the original URI and specify the parameter name, e.g. "orgUri".

REDIRECT POLICIES > REDIRECT POLICY

**REDIRECT POLICY**

Name\*:

Description:

Labels:

<input type="checkbox"/> EVENT	URL	USE HOST HEADER	TASK LIST GROUP
<input type="checkbox"/> Authentication Success	<input type="text"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Authentication Failure	<input type="text" value="http://192.168.82.203/login"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/> No Credentials	<input type="text" value="http://192.168.82.203/login"/>	<input type="checkbox"/>	
<input type="checkbox"/> On Error	<input type="text"/>	<input type="checkbox"/>	

Include Original URI: ☒

URI Parameter Name\*:

**Apply Save**

## Create a Request Filter Policy

Create a Sentry Request Filter Policy to use on the HTML policy built later. This Request Filter will allow HTTP GETs and POSTs.

1. On the Request Filters page, click New
2. Name the Request Filter SAML\_SSO
3. Click Create to create a custom request filter identification expression
4. Select the GET and POST methods, leave all other defaults, click Apply
5. Ensure the new filter is the only enabled filter in the Request Filter Policy

REQUEST FILTER POLICIES > REQUEST FILTER POLICY

**REQUEST FILTER POLICY**

Policy Name\*:

#	MESSAGE TYPE FILTER	FORMAT	DESCRIPTION	STATUS
1	XML Default	Simple	Plain XML	●
2	HTTP GET	Simple	HTTP GET	●
3	Multipart	Multipart	WSDL 1.1 MIME Filter	●
4	DIME	DIME	WS-Attachments	●
5	Streaming	Streaming	Generic	●
6	MTOM	MTOM	SOAP Message Transmission Optimization Mechanism	●
7	SMTP Text	Simple	HTML or Plain Text Email	●
8	SMTP MIME	Multipart	Email with Attachments	●
9	SAML_SSO_GET_and_POST	Simple		●

**Enable Disable New Delete Update Save**

## Create the User Identity and Access Control Task List Group

Create a Task List Group and Task List with a User Identity & Access Control task. This same task list will handle two important processing functions in this flow:

1. Initiate the SAML SSO flow - redirect the browser to the STS with a SAML request upon unauthenticated request
2. Consume the SAML response generated by the STS policy, which is provided by the browser upon being redirected by the STS policy

TASK NAME	
Task Name*:	<input type="text" value="User Identity &amp; Access Control"/>
<b>Next</b>	
USER IDENTITY & ACCESS CONTROL	
Task Type:	User Identity & Access Control
<u>Task Name:</u>	User Identity & Access Control
<u>ACL Policy:</u>	No user mapping
<u>User Identity Mechanism:</u>	Validate SAML SSO assertion & establish identity
<u>Identity Provider URL:</u>	<a href="http://192.168.82.203/sts">http://192.168.82.203/sts</a>
<u>Public Proxy URL:</u>	
<u>Redirect Parameter:</u>	origUri
<u>Request Issuer:</u>	<a href="http://www.forumsys.com/sentry">http://www.forumsys.com/sentry</a>
<u>Force authentication:</u>	No
<u>Request subject:</u>	[None]
<u>Sign request:</u>	Yes
<u>Signature Policy:</u>	Signature_Policy_US_DoD
<u>Include certificates:</u>	Yes
<u>Issuer(s):</u>	<a href="http://www.forumsys.com/sentry">http://www.forumsys.com/sentry</a>
<u>Audience:</u>	
<u>Require signature:</u>	Yes
<u>Verification Policy:</u>	Verification_Policy
<u>Require encryption:</u>	Yes
<u>Decryption Policy:</u>	Decryption_Policy
<u>SAML Identity Mechanism:</u>	Custom
<u>Custom:</u>	[Username]
<u>Error Template:</u>	[From Policy]

Build the Task List and Task List Groups following the steps below.

*If the task option is not documented, leave the default setting.*

*If Signatures and Encryption are required (recommended), be sure to build the Signature, Verification, and Encryption policies before proceeding.*

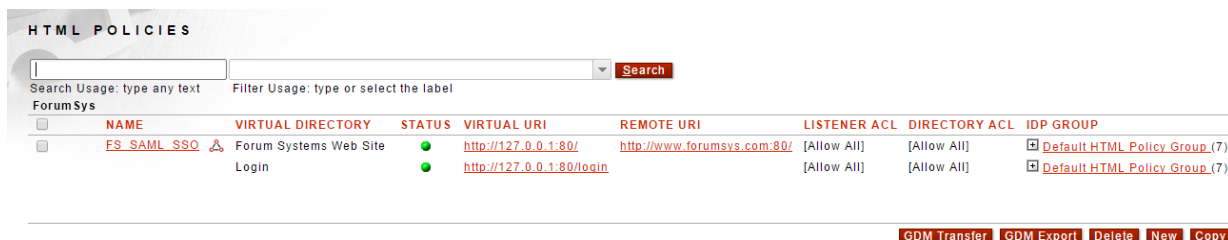
1. Create a new Task List
2. Create a new User Identity and Access Control Task
3. Uncheck "Map identified user to a known user"
4. Specify "Validate SAML SSO assertion & establish identity" as the User Identity Mechanism
5. Specify the STS URL as the identity provider URL – the STS policy has not yet been built – for this tutorial we'll use <http://192.168.82.203/sts>
6. For the redirect parameter, specify the same parameter used in the redirect policy, e.g. "origUri"
7. Specify the "Request Issuer" and "Issuer" fields to match the STS policy – for this tutorial we'll use <http://www.forumsys.com/sentry> for both
8. Specify Custom for the SAML identity mechanism
9. Specify Username as the Custom Value Type
10. Create a Task List Group from the Task List



## Create an HTML Policy

Create a Sentry HTML policy with two virtual directories:

1. Target directory to be protected – this is a proxy mode directory that will handle the runtime API or web site traffic
2. Login directory – this is a service mode (not a proxy) directory that is used for the SAML SSO flow



	NAME	VIRTUAL DIRECTORY	STATUS	VIRTUAL URI	REMOTE URI	LISTENER ACL	DIRECTORY ACL	IDP GROUP
<input type="checkbox"/>	FS_SAML_SSO	Forum Systems Web Site	●	<a href="http://127.0.0.1:80/">http://127.0.0.1:80/</a>	<a href="http://www.forumsys.com:80/">http://www.forumsys.com:80/</a>	[Allow All]	[Allow All]	Default HTML Policy Group (7)
<input type="checkbox"/>		Login	●	<a href="http://127.0.0.1:80/login">http://127.0.0.1:80/login</a>		[Allow All]	[Allow All]	Default HTML Policy Group (7)

Build the HTML Policy following the steps below.

*If the option is not documented, leave the default setting.*

*If SSL is required (recommended), be sure to build the HTTPS Listener and Remote policies before proceeding.*

1. Create a new HTML Policy and with it the first virtual directory “Service”
2. Set the HTTP Listener policy
3. Set the Virtual path as /
4. Set the HTTP Remote policy to point to the backend API or web site that Sentry will proxy the runtime traffic to, in our tutorial we are using [www.forumsys.com](http://www.forumsys.com)
5. After clicking Save to build the HTML policy, open the new Virtual Directory
6. Rename to “Service” or something descriptive of your API / web site
7. Set Password Authentication to “Specify”
8. Select “Use cookie authentication”
9. Select “Require password authentication”
10. Set the Redirect Policy to the policy created earlier in this tutorial
11. Save the virtual directory
12. Click New to create a second “Login” virtual directory
13. Name the virtual directory “Login”
14. Use the same HTTP Listener policy
15. Set the Virtual Path to /login
16. Set the Filter Expression to .\*
17. Set the Request Filter Policy to the “SAML\_SSO” Request Filter Policy built earlier in this tutorial
18. Set the Request Task List Group to the Task List Group created earlier in this tutorial
19. Uncheck “Send to remote server” – this will be a service mode policy
20. Save the second virtual directory
21. On the settings tab, enable Session Cookies, specify / as the path

## Configuring Sentry as the Identity Provider (IdP)

### Create the STS Policy

In this step you will create an STS policy that will do the following:

1. Validates an HTTP Basic Authentication credentials using a local runtime User ACL
2. Generate a SAML Responses for the user
3. Redirect the client with the SAML response to a target URL

NAME	VIRTUAL DIRECTORY	STATUS	URI	LISTENER ACL	DIRECTORY ACL	IDP GROUP
<a href="#">Sentry_STS_Policy</a>	STS	●	<a href="http://127.0.0.1:80/sts">http://127.0.0.1:80/sts</a>	[Allow All]	<a href="#">OnlineLDAP</a>	<a href="#">Default XML Policy Group (9)</a>

Build the STS Policy following the steps below.

***A Signature Policy is required to build an STS Policy as the Sentry generated SAML is required to be signed. Build the Signature Policy prior to building the STS Policy.***

***An Access Control policy is required to test this setup. Create a local runtime user, add the user to a User Group, and add the group to a User ACL.***

*If the option is not documented, leave the default setting.*

*If SSL is required (recommended), be sure to build the HTTPS Listener and Remote policies before proceeding.*

1. On the Gateway>>Content Policies>>STS Policies page click New to create a new STS policy
2. Name the STS policy
3. Under “SAML TOKEN CONFIGURATION”, select the SAML v2.0 Token Type and expand.
4. Make the following changes under “TOKEN CONFIGURATION”
  - a. Confirmation Method = Bearer
  - b. Issuer = <http://www.forumsys.com/sentry>
  - c. Audience = <http://www.forumsys.com/sentry>
  - d. Identification Format = Custom
  - e. Value Type = Username
  - f. Include Certificates = Enabled
5. Under “SAML REQUEST PROCESSING” you can optionally choose to verify the signature on the incoming SAML request and select the appropriate verification policy. Leave the Task Lists options as [None]
6. Make the following configuration changes under “SAML RESPONSE PROCESSING”
  - a. The optional target URI, if specified, should match the login virtual directory configured earlier on the HTML policy (the service provider authentication URL). For this tutorial the value should be: <http://192.168.82.203/login>
  - b. Token Lifetime (in seconds) = 60 (or whatever value you want)
  - c. Signature Policy = the Signature Policy to use to sign the SAML response
  - d. Sign Key Info = Unchecked
  - e. Encrypt token = Unchecked
  - f. Leave the task list options as [None]
7. Click Next
8. Set the HTTP/S Listener Policy

9. Set the Virtual Directory Path – Note that the virtual directory (comprised of the listener and path) has to match what is defined in the SAML SSO User Identity and Access Control task on the HTML policy as the Identity Provider URL. In this tutorial we are using <http://192.168.82.203/sts> and set the path to /sts.
10. Click Finish
11. On the Virtual Directories tab, click on the new virtual directory.
12. Set the “ACL Policy” to the correct User ACL
13. Set “Password Authentication” to [Specify]
14. Select “Use Basic Authentication”
15. Select “Require password authentication”
16. Click Save

## Testing the Forum Sentry SAML SSO Configuration

Use a browser to test the HTML and STS policies built from this tutorial. Using the browser developer tools and reviewing the Sentry Access and System logs at DEBUG level are highly recommended to see and understand the flow.

### Testing the SAML SSO Flow

1. Using a web browser, make a request to the “Service” virtual directory of the HTML Policy. This should result in your browser being redirected to the /login directory.
2. When the browser hits the /login directory, the SAML SSO flow begins via the SAML SSO task list.
3. The browser is again redirected, this time with a SAML request to the STS policy.
4. The STS policy prompts for basic auth credentials – enter the user credentials.
5. The STS policy validates the credentials, generates a SAML response, and redirects the browser back to the /login directory.
6. The /login directory validates the SAML response using the same SAML SSO task list.
7. Upon success, an FSSESSSION cookie is set and the browser is again redirected, this time to the “Service” directory.
8. If the request to the “Service” directory includes the cookie, the request is proxied to the remote server.
9. All subsequent calls to the “Service” directory will require the cookie. If it is not present, or if it is expired, Sentry will redirect back to the /login directory and the process will begin again.

## More Information

Forum Systems Support Knowledgebase – Sample Sentry policies for SAML SSO, both SP and IdP scenarios are available for download at <https://helpdesk.forumsys.com>.

Forum Systems Whitepapers and Blogs – Forum Systems has posted multiple blogs and whitepapers related to solving enterprise SAML SSO with Forum Sentry. Please visit <http://www.forumsys.com> for more information.