FORUMSYSTEMS™

MANAGING & ACCELERATING XML WEB SERVICES SECURITY

FORUM SYSTEMS HANDS-ON TRAINING

LAB 15. IDENTITY – FORM POST SSO WITH FSSESSION COOKIES

Published: September 2014
Forum Systems Hands-on Training – Lab 15. Identity – Form Post SSO with FSSESSION Cookies
D-ASF-SE-010029

Contents

Introduction

Lab 15. Identity – Form Post SSO with FSSESSION Cookies

Skill Level

This lab is Intermediate Skill Level. Some existing experience with Forum Sentry and SOAPSonar, or completion of the Beginner Level labs, is assumed.

Prerequisites

This lab requires the Forum Sentry Training Image, with a licensed copy of Forum Sentry.

Refer to the "FS_Training_Labs_v8-1_Introduction" document for information on the Forum Sentry Training Image and licensing SOAPSonar Enterprise Edition.

This lab utilizes the Sentry LDAP Policies built in Lab 13. If these do not exist, follow the instructions in Lab 13 to build the Runtime User LDAP Policy.

This lab utilizes the User ACL built in Lab 14. If this User ACL does not exist, follow the instruction in Lab 14 to generate a User ACL that includes the runtime user LDAP policy built in Lab 13.

This lab utilizes the .NET WebMatrix web server installed on the Forum Sentry Training Image. Review Lab 1 to familiarize yourself with the .NET WebMatrix web server.

Lab Overview

Forum Sentry enables many types of Single Sign-On (SSO). HTTP Form Post authentication is a common option for SSO with web sites, web apps, and mobile apps.

HTTP Form Post authentication is a type of Password Authentication, with the username and password provided to the service via HTTP form post (credentials within the message body). Contrast this to HTTP Basic Authentication where the credentials are provided to the service within an HTTP Authorization Header.

Providing SSO capabilities is essential in locking down access to resources without inundating users with the need to provide credentials repeatedly.

In this lab, we will use Forum Sentry to enable SSO for resources available on the .NET WebMatrix web server. The .NET WebMatrix server is behaving as a typical web server in this scenario.

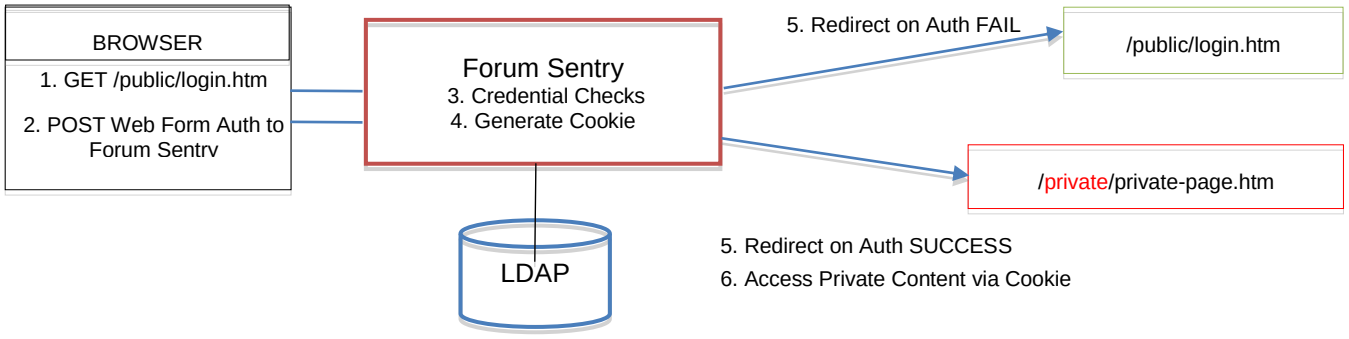
To provide centralized access control and protection, all public and private content is brokered through the Forum Sentry API Gateway.

The figure below outlines the transaction flow for this scenario. The steps are listed here:

1. The browser retrieves a login page through Sentry from a public location on the web server.
2. The user enters credentials on the login screen and submits. These credentials are sent to Sentry.
3. Sentry does the credential check using an LDAP Policy.
4. If the credentials are valid, Sentry generates a cookie (FSSESSION cookie).
5. If the credential check succeeds, the browser is redirected to another virtual directory in Sentry

that consumes the cookie and allows access to the private data on the web server. If the credential check fails, the browser is redirected to the login page.

6. On SUCCESS, the user can browse private content. Any subsequent calls to obtain private content utilize the cookie generated by Sentry. This enables users to have access to protected information without having to re-send credentials.



In the Samples folder on the Desktop of the Forum Sentry Training Image, there are two folders: public and private. Review the content of both folders. These folders will be used for setting up the SSO scenario.

In this lab we'll build a new HTML Policy in Sentry to broker traffic for the .NET WebMatrix web server. We will apply authentication requirements and enable SSO.

This lab will provide instructions for enabling HTTP Form Post SSO in Forum Sentry. Topics will include:

1. HTML Policies
2. HTTP Cookies
3. HTTP Redirects

Sentry Redirect Policies

Sentry Redirect Policies will be used to redirect the browser upon different authentication events. These redirects will improve the user experience, ensuring the user lands on either the correct page upon successful authentication or the login page upon failed auth.

Building the Redirect Policies

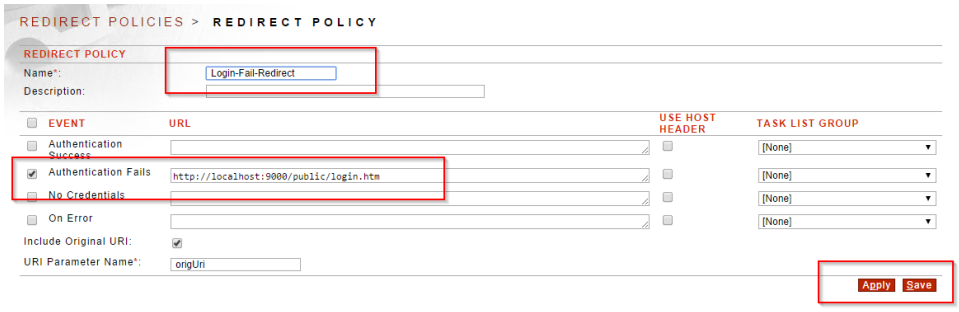
In this step we will create two Sentry Redirect Policies required for this SSO scenario.

Follow the steps below to create the Redirect Policy for successful authentication in Sentry

1. Navigate to the Gateway→Redirect Policies→Redirect Policies page.
2. Click new to create a new Redirect Policy. Configure the policy with the following criteria:
    a. Name: Login-Redirect
    b. Authentication Success: http://localhost:9000/private/private-page.htm
    c. Authentication Fails: http://localhost:9000/public/login.htm
    d. Click Apply and Save

Follow the steps below to create the Redirect Policy for failed authentication in Sentry

1. Navigate to the Gateway→Redirect Policies→Redirect Policies page.
2. Click new to create a new Redirect Policy. Configure the policy with the following criteria:
    a. Name: Login-Fail-Redirect
    b. Authentication Fails: http://localhost:9000/public/login.htm
    c. Click Apply and Save



Sentry HTML Policy

Sentry HTML Policies are used to broker HTML traffic typical for web sites and web portals. HTML Policies are very similar to REST Policies, and are configured in the same manner. The difference between an HTML Policy and a REST Policy is just the types of traffic each will process. Typically REST Policies broker REST CRUD calls for an API while HTML Policies broker HTML and other typical web site and web portal traffic.

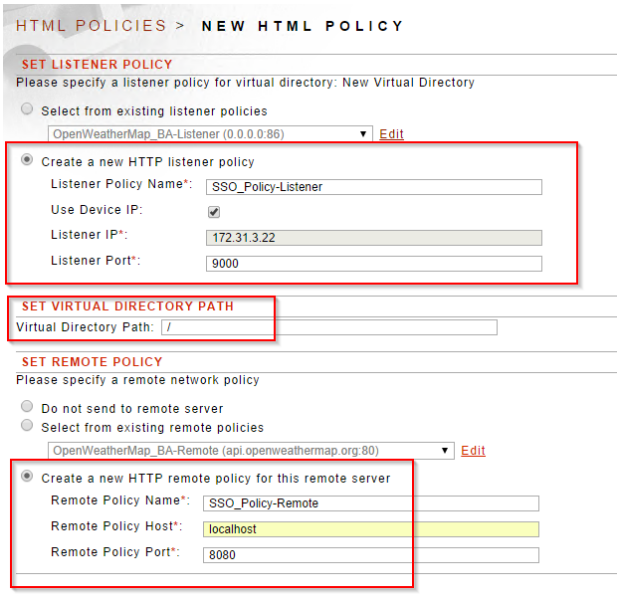
Building the HTML Policy

In this step we will create an HTML Policy in Sentry with three virtual directories, which is required for this SSO scenario. We will create new HTTP Listener and Remote policies, rather than use existing policies.

We will enable session cookies on this HTML Policy. This will generate an FSSESSION cookie upon successful form post authentication.

Follow the steps below to create the HTML Policy in Sentry.

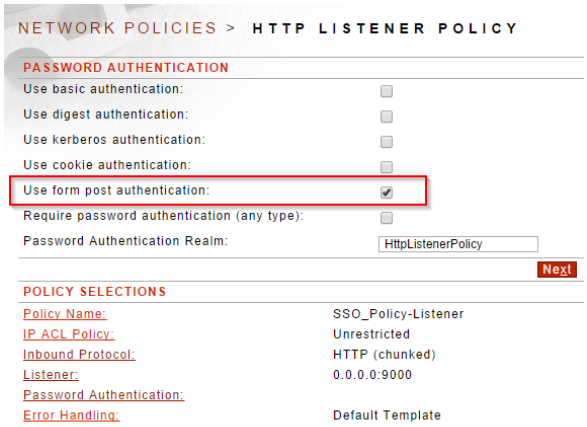
1. Navigate to the Gateway→Content Policies→HTML Policies page.
2. Click New to create a new HTML Policy. Configure the policy with the following criteria:
    a. Name: SSO_Policy
    b. Label: SSO
    c. Click Next
        i. Create a new HTTP Listener
    d. Listener Policy Name: SSO_Policy-Listener
    e. Use Device IP: Enabled
    f. Listener Port: 9000
    g. Virtual Directory Path: /
    h. Create a new HTTP Remote
    i. Remote Policy Name: SSO_Policy-Remote
    j. Remote Policy Host: localhost
    k. Remote Policy Port: 8080



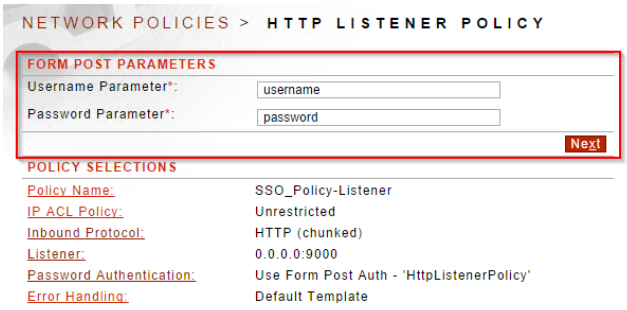
3. Modify the new “SSO_Policy-Listener” network listener policy. Navigate to the

Gateway→Network Policies→Network Policies page. Click on “SSO_Policy-Listener” policy and configure as follows:

a. Click on the Password Authentication link
b. Enable Form Post Authentication

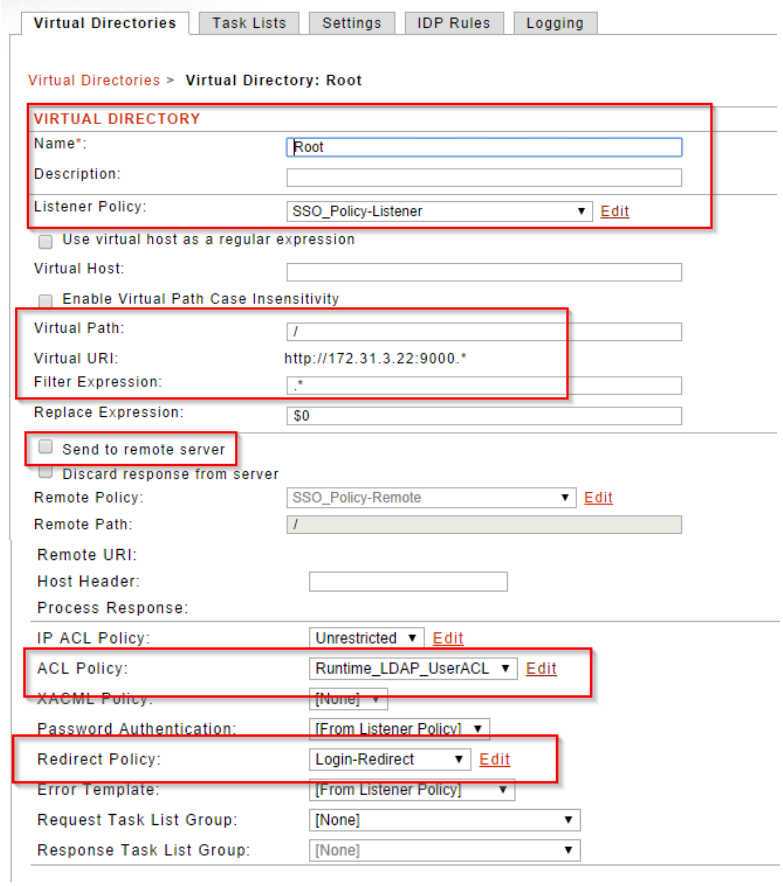


c. Click Next
d. Enter the Form Post Parameters as follows:
    i. Username Parameter: username
    ii. Password Parameter: password

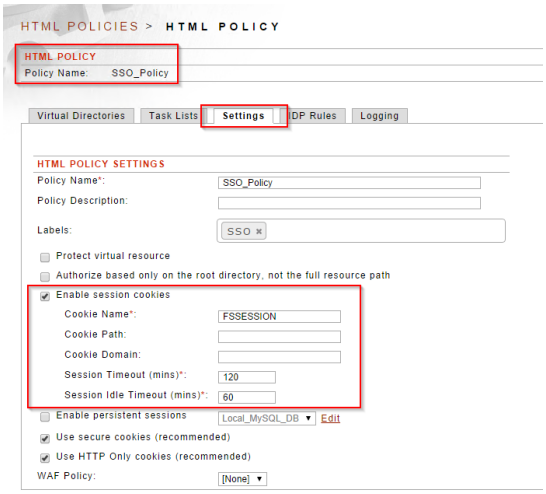


e. Click Next and Click Finish to save the policy
f. Leave all other default options

4. Navigate to the Gateway→Content Policies→HTML Policies page. Open the “SSO_Policy” HTML Policy and access the Virtual Directory by clicking the link “New Virtual Directory”. Configure the virtual directory with the following criteria:
    a. Name: Root
    b. Virtual Path: /
    c. Filter Expression: .*
    d. Send to remote server: UNCHECK
    e. ACL Policy: Runtime_LDAP_UserACL
    f. Redirect Policy: Login-Redirect
    g. Leave all other default values
    h. Click Save



5. While still in the HTML Policy, click the Settings tab to enable session cookies. Configure the Settings tab with the following criteria:
    a. Enable session cookies: CHECK
    b. Cookie Name: FSSESSION
    c. Leave all other defaults
    d. Click Save



6. We will now add a second virtual directory to this same HTML Policy. Navigate to the Virtual

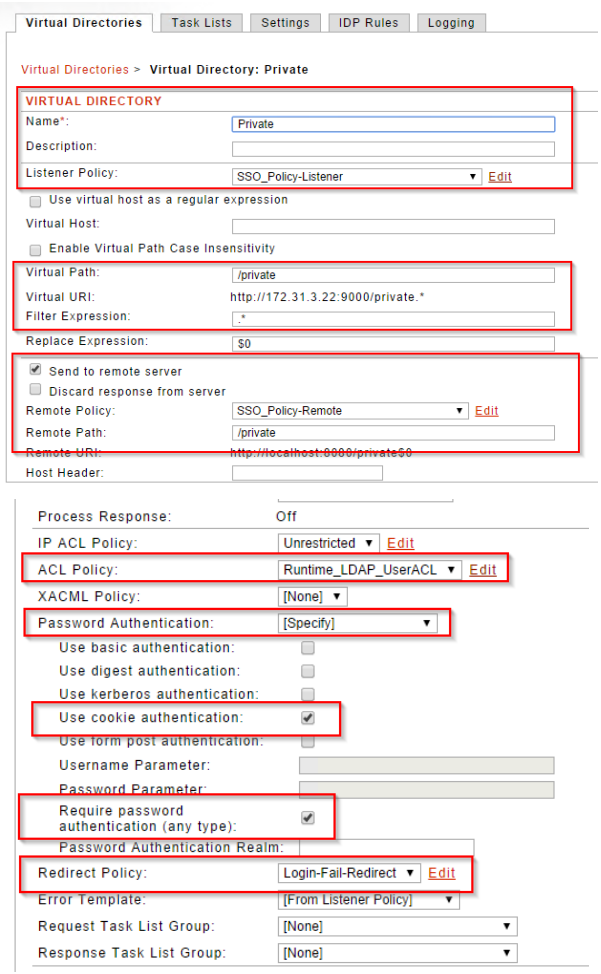
Directories tab of the HTML policy. Click New to create a new virtual directory. Configure the new virtual directory with the following criteria:

a. Name: Public
b. Listener Policy: SSO_Listener-Policy
c. Virtual Path: /public
d. Filter Expression: .*
e. Send to Remote Server: CHECKED
f. Remote Policy: SSO_Remote-Policy
g. Remote Path: /public
h. ACL Policy: Allow All
i. Leave all other defaults
j. Click Save

7. We will now add a third virtual directory to this same HTML Policy. Navigate to the Virtual Directories tab of the HTML policy. Click New to create a new virtual directory. Configure the new virtual directory with the following criteria:

a. Name: Private
b. Listener Policy: SSO_Listener-Policy
c. Virtual Path: /private
d. Filter Expression: .*
e. Send to Remote Server: CHECKED
f. Remote Policy: SSO_Remote-Policy
g. Remote Path: /private
h. ACL Policy: Runtime_LDAP_UserACL (created in Lab 13)
i. Password Authentication: SPECIFY

j. Use Cookie Authentication: CHECKED
k. Require Password Authentication (any type): CHECKED
l. Redirect Policy: Login-Fail-Redirect
m. Leave all other defaults
n. Click Save



Test the SSO Setup

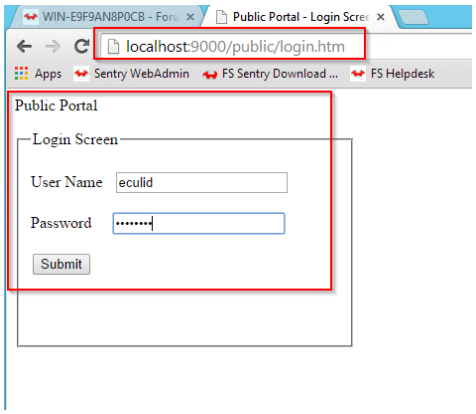
We are now ready to test the Form Post SSO configuration in Sentry.

Testing the HTML Policy

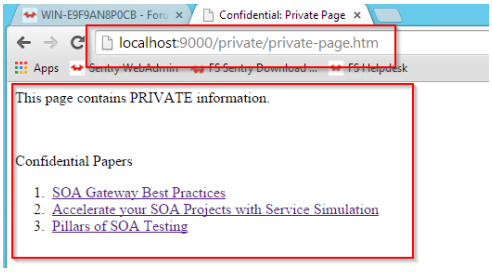
In this step we will use a browser to test the HTML Policy built in this lab. Upon the first call the user will be provided with a login page. After providing the correct LDAP credentials the user will be allowed to access the resources in the private directory on the web server.

Follow the steps below to test the HTML Policy in Sentry.

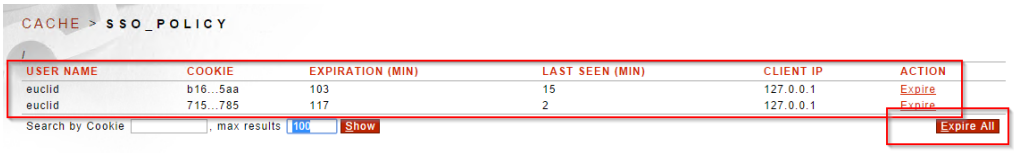
1. Using a new browser instance or tab, go to the following URL: http://localhost:9000/public/login.htm
2. This will retrieve the Login Page.
3. Enter the following credentials:
    a. Username: euclid
    b. Password: password
4. Click Submit.



5. With successful login, the private page will be presented. You can click on the links in the private page to download the confidential information. This download is authenticated with session cookies.



6. Back in the WebAdmin interface, navigate to Access→ User Policies → Cache → SSO Policy. A list of cookies and related information is displayed as shown below. Click *Expire All*.



7. Try to access one of the Confidential Papers on the private web site again. Since the session cookie is no longer valid, the request for confidential information will be redirected to the login screen.

END

Additional Testing and More Reading

BACK IT UP!

It is recommended that you export your HTML Policy and/or your full Sentry configuration after completing this lab.

To export the HTML policy, navigate to the HTML Policies page, select the HTML policy and use the GDM Export option to export the policy (and all dependencies) as a password encrypted FSG file. This can later be imported on the System→Configuration→Import/Export screen.

To export your full Sentry configuration, navigate to the System→Configuration→Import/Export screen and use the Export option in the center of the page to export the full Sentry configuration file as a password encrypted FSX file. This can later be imported on the same screen.

Backup your SOAPSonar project file by using the File→Save As option. All of your test cases will be saved in an .SSP file.

We recommend including the lab number in the name of the export files.

Additional Tests and Discussion Topics

1. Be sure to review the Sentry Access and System logs to review the processing done in Sentry. Start with the Access Log to easily identify each of the transactions happening in Sentry.
2. Password Authentication should not be used without SSL as the credentials are not encrypted in any way. Add SSL to the policy and test again.
3. What happens if you use the wrong URL?

Additional Information

Details of the online LDAP Server from Forum Systems:
http://www.forumsys.com/tutorials/integration-how-to/ldap/online-ldap-test-server/

For more information, review the following Forum Sentry Admin Guide:

1. Access Control Guide
2. Network Policies Guide

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified, patented, and proven products deployed in the most rigorous and demanding customer environments worldwide. Forum Systems has been an industry leader for over 12 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Forum Systems security-first mindset enables trusted, network edge deployments of its technology for protecting critical enterprise transactions.

Our product technology is purpose-built and designed for mission-critical, enterprise-class scalable solutions where business solutions require the modern day security and identity enforcement protection, while enabling a scalable architecture and low-latency, high-volume throughput.

Forum Systems supports global enterprise customers across industries in commercial, government, and military sectors. Forum Systems technology provides the leading-edge of modern-day cyber-security innovation with integrated identity and SSO features that enable out-of-the box business solutions with point-and-click technology.

Forum's patented; FIPS 140-2 and NDPP certified hardware and virtual products make modern-day business communications secure by actively protecting and accelerating data exchange and API service access across networks and business boundaries. For more information, please visit www.forumsys.com.