THE LEADER IN API SECURITY MANAGEMENT

FORUM SYSTEMS SENTRY™ VERSION 8.7
SHAREPOINT 2013 SSO
CONFIGURATION GUIDE

Legal Marks

Forum Systems Sentry™ Version 8.7 SharePoint 2013 SSO Configuration Guide, Published July 2016

D-ASF-SE-051021

Contents

Introduction to the Forum Sentry SharePoint 2013 SSO Configuration Guide

Audience

The *Forum Systems Sentry™ Version 8.7 SharePoint 2013 SSO Configuration Guide* is for Sentry Administrators who will configure Forum Sentry as an Identity Provider (IdP) for SharePoint 2013 On Premise.

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 API Security Gateway™ 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 the following are not shown:

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

For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 8.7 Web-based Administration Guide*.

Assumptions

This document assumes that the reader will review all chapters before performing the configuration operations listed in this document. It is highly recommended that the user read the full document prior to starting the configurations.

This document also assumes that the reader is familiar with SharePoint 2013 administration, including the power shell commands and the Central Administration setup necessary to define a trusted Identity Provider.

Not all steps in the configuration tutorial are listed out in detail. Visit https://helpdesk.forumsys.com and/or contact Forum Systems Support for assistance as necessary.

Forum Sentry Support for SharePoint 2013 SSO

Introduction

There are multiple ways to integrate Sentry with Sharepoint 2013. This guide describes a solution for integrating SSO with Sharepoint 2013 on premise without using ADFS.
Forum Sentry functions as the Identity Provider (IdP) for SharePoint 2013. Versions of SharePoint other than 2013 have not been tested and are unsupported. For Sharepoint 2013 deployments that are cloud-based or involve ADFS, please contact Forum Systems for appropriate solutions.

This guide will provide the following information:

1. General overview of the SSO flow
2. Sample configuration steps for SharePoint 2013
3. Sample configuration steps for Forum Sentry
4. Outline of testing procedures

Sentry as the Identity Provider (IdP)

For the SharePoint 2013 SSO use case, Forum Sentry serves as the Identity Provider. Sentry STS policies function as the IdP policies. An STS policy is used to consume an optional request and generate SAML responses. The STS policies support both SP initiated and IdP initiated SAML SSO.

SP Initiated – the user accesses the service provider (in this case SharePoint 2013) without valid credentials, and the SP redirects the browser to the STS policy with a SAML request. The user is then redirected to the SP with a SAML response.

IdP Initiated – the user accesses the STS policy (IdP) directly and is then redirected to the SP with a SAML response.

While it is possible to configure either SP or IdP initiated flows with Forum Sentry and SharePoint 2013, the sample configurations in this guide are for the SP Initiated flow (user accesses SharePoint 2013 and is redirected to Sentry to provide credentials).

Overview of the SharePoint 2013 SSO flow with Forum Sentry as the Identity Provider (IdP)

Forum Sentry supports a wide range of customer use cases as they pertain to SAML SSO. The procedures outlined in this document cover a specific SharePoint 2013 centric approach to SAML SSO. Further specific customization of these policies will be required for each customer use case.

The SSO flow discussed in this configuration guide involves both SAML 1.1 and WS-Federation, with Forum Sentry as the IdP and SharePoint 2013 as the SP.

1. User accesses SharePoint 2013 site
2. User is redirected to Sentry STS policy
3. User is prompted for basic auth credentials
4. User enters credentials, which are validated against the local Sentry user store
5. User is redirected back to SharePoint 2013 with a SAML 1.1 token containing the correct claims necessary for the SharePoint 2013 configuration

6. SharePoint 2013 validates the SAML. The user is logged in, and the SharePoint FedAuth cookie is set

SharePoint 2013 SSO Configuration

There are two parts to the SharePoint 2013 configuration. The first involves running a series of SharePoint 2013 Management Shell commands. This will create the trusted identity provider that will later be selected in the Central Administration. The second part involves enabling the federated authentication via the SharePoint 2013 Central Administration.

Note that the specific SharePoint 2013 configuration for each environment will likely differ. The settings provided below are for sample purposes only.

SharePoint 2013 Management Shell Commands

For more information on each command, refer to the Microsoft documentation.

Command 1
Set the X.509 certificate to use for SAML signature verification. This public certificate should align with the private key (key pair) used in the Sentry to sign the SAML.

```
$cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("C:\Users\Administrator\User1-
CP.02.01.crt")
```

Note: Adjust the path to point to the specific certificate you want to use.

Command 2
Create the SP Trusted Root Authority.

```
New-SPTrustedRootAuthority -Name "Token Signing Cert" -Certificate $cert
```

Note: Adjust the name if an existing SP trusted root authority with the same name already exists.

Command 3
Set EmailAddress as a claim type.

```
$emailClaimMap = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName
"EmailAddress" –SameAsIncoming
```

Command 4
Set the Realm.

```
$realm = "urn:forumsys:sharepoint"
```

Command 5
Set the Sign In URL.

```
$signInURL = "https://sts.fssupport.com/wsf"
```

Note: This needs to match the Sentry STS Policy URL, which will be created later in this tutorial.

Command 6
Create the SP Trusted Identity Token Issuer.

$ap = New-SPTrustedIdentityTokenIssuer -Name "Sentry" -Description "Sentry" -realm $realm -ImportTrustCertificate $cert -ClaimsMappings $emailClaimMap -SignInUrl $signInURL -IdentifierClaim $emailClaimMap.InputClaimType

Note: This creates a new Trusted Identity Provider that will be selected in the SharePoint 2013 Central Administration, using the settings from the previously entered commands.

SharePoint 2013 Central Administration Configuration

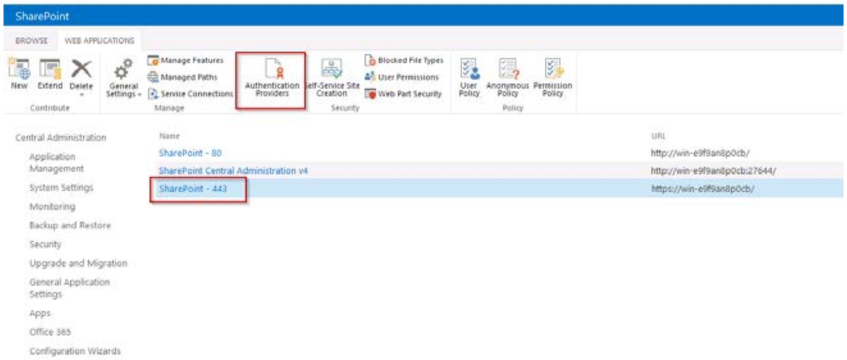
After running all of the management shell commands successfully, log into the SharePoint 2013 Central Administration and run through the following steps.

Step 1 – Access the Web Application

1. Go to **Manage Web Applications** and select <Your SharePoint App>

Step 2 – Enable the Trusted Identity Provider

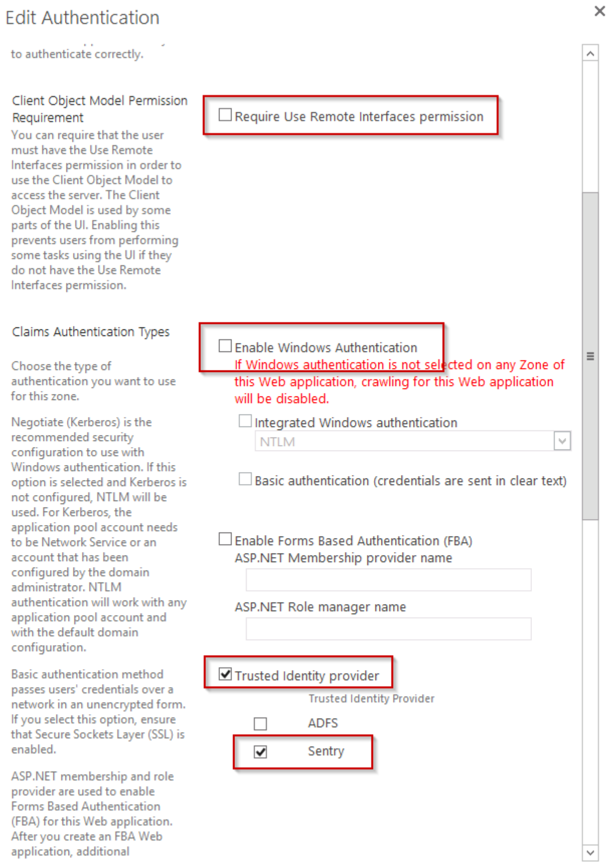
1. With your Web Application highlighted, select Authentication Providers



Name	URL
SharePoint - 80	http://win-e9f9an8p0cb/
SharePoint Central Administration v4	http://win-e9f9an8p0cb:27644/
SharePoint - 443	https://win-e9f9an8p0cb/

2. Select Default
3. Uncheck the “Require Use Remote Interfaces permission” option
4. Uncheck the “Enable Windows Authentication” option
5. Check the “Trusted Identity Provider” option

6. Select Sentry



Edit Authentication

to authenticate correctly.

Client Object Model Permission Requirement

You can require that the user must have the Use Remote Interfaces permission in order to use the Client Object Model to access the server. The Client Object Model is used by some parts of the UI. Enabling this prevents users from performing some tasks using the UI if they do not have the Use Remote Interfaces permission.

☐ Require Use Remote Interfaces permission

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional

☐ Enable Windows Authentication

If Windows authentication is not selected on any Zone of this Web application, crawling for this Web application will be disabled.

☐ Integrated Windows authentication

NTLM

☐ Basic authentication (credentials are sent in clear text)

☐ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

ASP.NET Role manager name

☑ Trusted Identity provider

Trusted Identity Provider

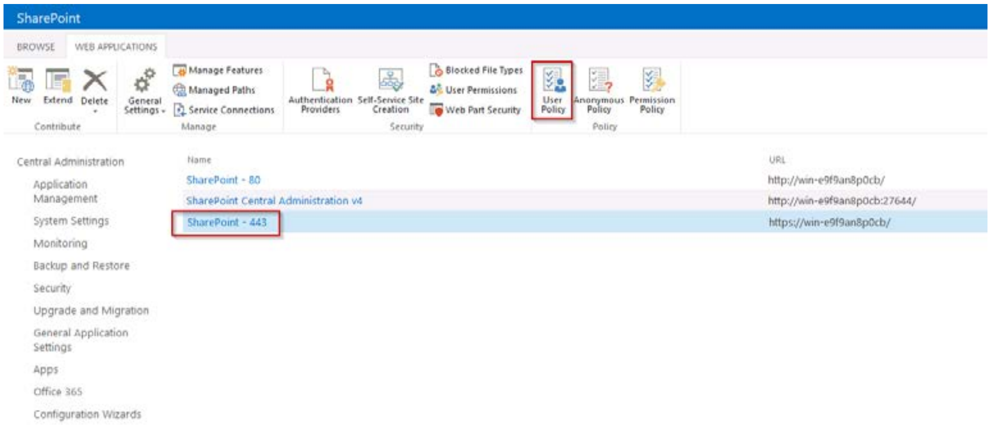
☐ ADFS

☑ Sentry

7. Click Save

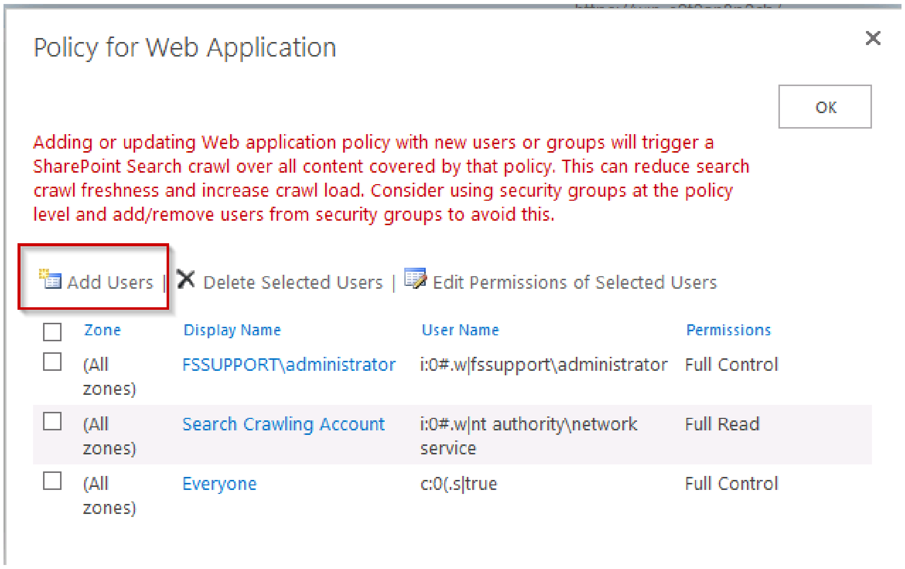
Step 3 – Set the User Policy

1. With your Web Application highlighted, click on User Policy



Name	URL
SharePoint - 80	http://win-e9f9an8p0cb/
SharePoint Central Administration v4	http://win-e9f9an8p0cb:27644/
SharePoint - 443	https://win-e9f9an8p0cb/

2. Click Add Users



Policy for Web Application

×

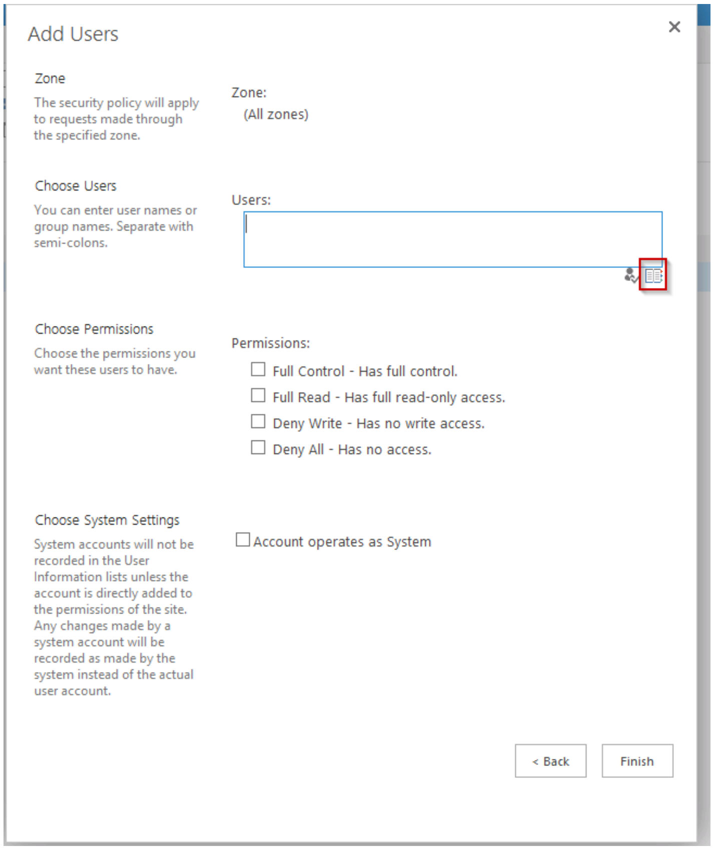
OK

Adding or updating Web application policy with new users or groups will trigger a SharePoint Search crawl over all content covered by that policy. This can reduce search crawl freshness and increase crawl load. Consider using security groups at the policy level and add/remove users from security groups to avoid this.

Add Users | Delete Selected Users | Edit Permissions of Selected Users

□	Zone	Display Name	User Name	Permissions
□	(All zones)	FSSUPPORT\administrator	i:0#.w|fssupport\administrator	Full Control
□	(All zones)	Search Crawling Account	i:0#.w|nt authority\network service	Full Read
□	(All zones)	Everyone	c:0(.s|true	Full Control

3. Click Next on the Zones screen
4. Click the Browse icon under Choose Users



Add Users

×

Zone

The security policy will apply to requests made through the specified zone.

Zone:
(All zones)

Choose Users

You can enter user names or group names. Separate with semi-colons.

Users:

Choose Permissions

Choose the permissions you want these users to have.

Permissions:

- □ Full Control - Has full control.
- □ Full Read - Has full read-only access.
- □ Deny Write - Has no write access.
- □ Deny All - Has no access.

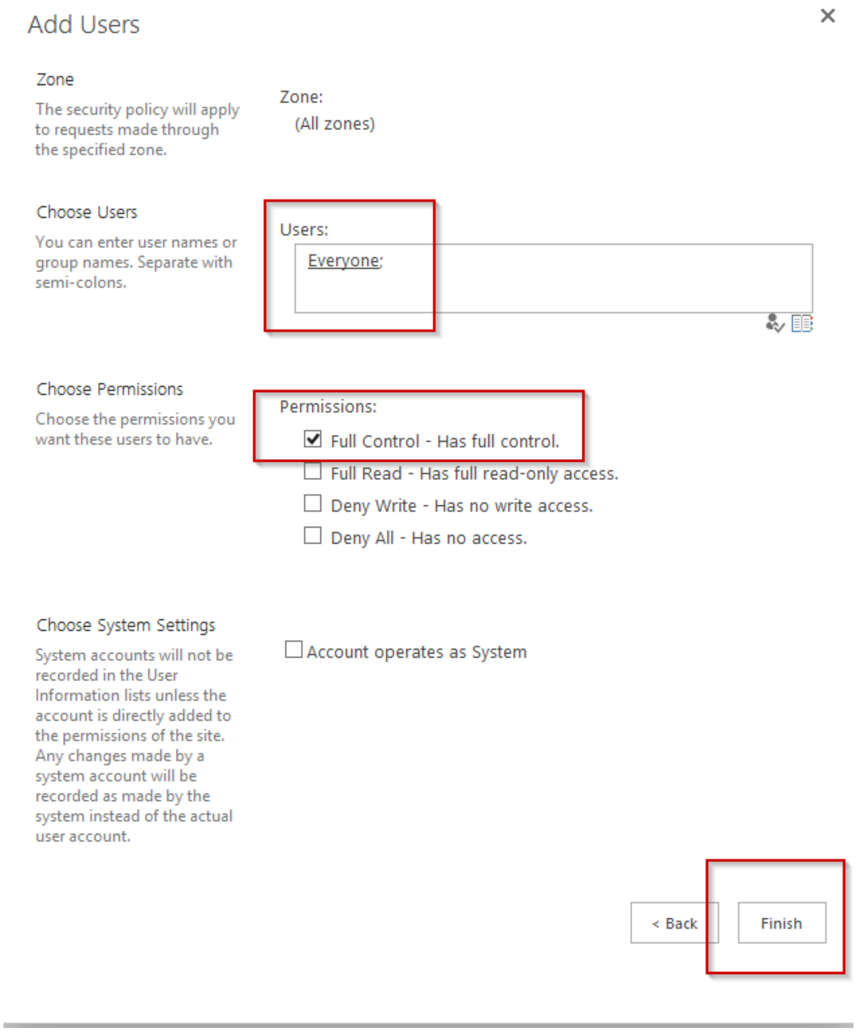
Choose System Settings

System accounts will not be recorded in the User Information lists unless the account is directly added to the permissions of the site. Any changes made by a system account will be recorded as made by the system instead of the actual user account.

□ Account operates as System

< Back | Finish

5. Select the appropriate users. In this sample we selected Everyone
6. Give the proper permissions (we used Full Control) and click Finish



Add Users

Zone

The security policy will apply to requests made through the specified zone.

Zone:
(All zones)

Choose Users

You can enter user names or group names. Separate with semi-colons.

Users:
Everyone;

Choose Permissions

Choose the permissions you want these users to have.

Permissions:
☑ Full Control - Has full control.
□ Full Read - Has full read-only access.
□ Deny Write - Has no write access.
□ Deny All - Has no access.

Choose System Settings

System accounts will not be recorded in the User Information lists unless the account is directly added to the permissions of the site. Any changes made by a system account will be recorded as made by the system instead of the actual user account.

□ Account operates as System

A Note on Claims

The emailAddress claim is arbitrary. In this example we configure the emailAddress claim to be used as the display name in SharePoint 2013.

There are several uses for claims other than as the display name. SharePoint 2013 can be configured to authorize access based on any arbitrary value of any arbitrary claim/attribute.

For example, a multi-value "role" attribute is sometimes used to authorize users based on whether they have membership in a prerequisite group, e.g. role=support. Custom code can also be written in SharePoint 2013 to populate fields in the user profile from arbitrary claims, such as given name and surname.

Refer to Microsoft’s SharePoint 2013 document for more information on claims.

Configuring Forum Sentry as the Identity Provider (IdP)

The procedures below detail how to configure Forum Sentry as the Identity Provider for SharePoint 2013. There are three parts: creating the local user for testing, creating the Signature Policy to sign the SAML, and creating an STS policy.

Create a Local User, User Group, and User ACL for Testing

In this step you will create a local user in Sentry for testing through the WebAdmin interface.

Typically in a live environment the ACL specified on the STS policy would reference an external identity management system, such as an LDAP server.

1. Access >> User Policies >> Users and create a new user
2. Open the new user and provide an email address
3. Access >> User Policies >> User Groups create a new User Group
4. Open the User Group and add the user from step 1 to the group
5. Access >> Runtime Access >> User ACLs create a new User ACL
6. Open the User ACL and add the User Group from step 3 to the User ACL

Create a Signature Policy

In this step you will create a Signature Policy in Sentry through the WebAdmin interface.

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

IMPORTANT- Use the key pair that corresponds to the certificate configured on SharePoint 2013.

1. Resources >> PKI >> Keys (if the key pair does not already exist, import your key pair or create a new one)
2. Resources >> Security Policies >> Signature Policies and click New
3. Select the correct key pair
4. Set the Signature and Digest Algorithms, e.g. RSA-SHA256 and SHA-256 respectively
5. Click Save

Create the STS Policy

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

1. Validate an HTTP Basic Authentication credentials using a local runtime User ACL
2. Generate a signed SAML 1.1 token for the user with the correct claims included
3. Redirect the client (browser) with the SAML response to a target URL (the SharePoint 2013 site)

Build the STS 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 policy 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 v1.1 Token Type and expand

4. Make the following changes under "TOKEN CONFIGURATION"
    a. Confirmation Method = Bearer
    b. Issuer = http://www.forumsys.com/sentry (you can use whatever value you want)
    c. Audience = urn:forumsys:sharepoint (IMPORTANT: This must match the realm defined in SharePoint 2013 set via the management shell commands)
    d. Identification Format = Email
    e. Include Certificates = Enabled
    f. Include Attribute = Enabled
    g. Namespace = http://schemas.xmlsoap.org/ws/2005/05/identity/claims
    h. Name(s) = emailaddress
    i. Value Type = Email
5. Under "SAML REQUEST PROCESSING" leave all options default (nothing selected)
6. Make the following configuration changes under "SAML RESPONSE PROCESSING"
    a. The Target URL should match the SharePoint 2013 web app URL with the _trust appended to the end. For example we used: https://sp.fssupport.com/_trust
    b. Token Lifetime (in seconds) = 3600
    c. Signature Policy = the Signature Policy created earlier 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 – IMPORTANT: The Sentry URL must match the Sign In URL entered in the SharePoint 2013 Management shell commands.
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 for the local test user
13. Set "Password Authentication" to [Specify]
14. Select "Use Basic Authentication"
15. Select "Require password authentication"
16. Click Save

Testing the SharePoint 2013 and Forum Sentry Configuration

Use a browser to test the SharePoint 2013 SSO flow 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 SharePoint 2013 web app URL
2. SharePoint 2013 will redirect to the Sentry STS policy
3. The Sentry STS policy prompts for basic auth credentials – enter the user credentials
4. The STS policy validates the credentials, generates a SAML 1.1 token, and redirects the browser back to the SharePoint 2013 web app URL (with _trust appended o the URL)
5. SharePoint 2013 validates the SAML 1.1 token, sets the FedAuth cookie, and logs the user in

Reviewing the Sentry Logs

Ensure the System log is at DEBUG level.

Check the Sentry Access log first, you'll see 2 transactions. Click the Session ID on a transaction to jump to the System log and see the Debug logging for that transaction.

1. The first transaction is the 401 auth failure upon initial redirection into the STS Policy which results in the pop-up box for credentials.
2. The second transaction is the consumption of the basic auth credentials, generation of the SAML 1.1 token, and finally the redirect back to SharePoint 2013.

Note that the redirect is not an HTTP 300 level redirect, but rather Sentry returns a form to the browser and the browser uses JavaScript to post the SAML 1.1 token to SharePoint 2013.

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.