# Table of Contents

Overview .......................................................................................................................... 3

Security Assertion Markup Language (SAML) ........................................................................ 3

  SAML SSO Flow .................................................................................................................. 4

  Exterro Requirements .......................................................................................................... 4

Prerequisites ....................................................................................................................... 5

Redis Installation ................................................................................................................. 5

SAML Service Provider Configuration .................................................................................. 5

  i. saml-config.properties .................................................................................................... 6

  ii. saml-redis.properties .................................................................................................... 8

  iii. config.properties ......................................................................................................... 9

  iv. application.properties ................................................................................................... 11

Starting the SAML Service Provider .................................................................................... 12

App.config ......................................................................................................................... 19

Contact Exterro .................................................................................................................. 20
Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Legal GRC platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world’s largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

Security Assertion Markup Language (SAML)

Exterro provides a Single Sign-on solution using end user provided identity federation Services for FTK Central. A brief introduction to SAML (Security Assertion Markup Language) is provided below.

The Security Assertion Markup Language (SAML) is an XML based open standard used to pass a user’s authentication identity information between the following entities:

- **Identity Provider (IdP)** – The application that the user logged into using the user’s identity authentication.
- **Service Provider (SP)** – The external service/application which can be accessed using the identity authentication provided by the Identity Provider (IdP)
SAML SSO Flow

The diagram below illustrates the single sign-on flow for service provider-initiated SSO, i.e. when an application triggers SSO.

Identity provider initiated SSO is similar and consists of only the bottom half of the flow.

Exterro Requirements

IDP metadata is required for SSO within FTK Central. This metadata is used to configure our Service Provider (SP) website for the Identity Provider (IDP) that is used by the client. As mentioned previously, any SAML 2.0 compatible IDP will work with FTK Central. Moreover, the external access to the IDP is not required, but it does enhance the usability.

Users must agree on an Authentication Value (GUID) that the IDP will return to the SP for authenticating the users. This value must be unique per user and the client should not be able to reuse it. SamAccountname, Employee IDs, etc. are commonly used unique values. Some firms choose email, but this value in some firms are re-used which would in turn disqualify it in order to maintain the unique identification of users.
Prerequisites

To authenticate into FTK Central, you have to install Redis and SAML Service Provider.

Redis Installation

Follow the below instructions to do so:

1. Download and execute the Redis installation package.
2. Execute the `install.bat` to install Redis.

   **Note:** Redis must have the read/write access on the machine and should be accessible by SAML SSO Service Provider (SP).

   - A new Windows service, “exterroredis” will be created.

3. Start the Redis service from the Windows services.

   **Note:** Redis must be started before starting SAML Service Provider.

SAML Service Provider Configuration

Follow the below instructions to do so:

1. Install Java 8 (x64) v1.8.0_342 or higher versions on the Windows instance.
2. Set the home path in Windows environment variables.
3. Download the installation package from the Google Drive location provided by the Exterro team.
4. Extract the downloaded installation package.
5. Open the **config** folder to find the configuration files.

6. Configure the properties below:

   i. **saml-config.properties**

<table>
<thead>
<tr>
<th>Property name</th>
<th>Property Value Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTH_ALGORITHM_TYPE</td>
<td>SHA-256</td>
<td>The SAML signature algorithm is an SML security signature algorithm URI or suitable abbreviation (e.g., rsa-sha256).</td>
</tr>
<tr>
<td>METADATA_ENTITY_ID</td>
<td>http://&lt;saml_instance_dns_name&gt;/exterrosso/saml/login</td>
<td>DNS name provided to the SAML SSO configured windows instance.</td>
</tr>
<tr>
<td>PROTOCOL</td>
<td>https</td>
<td>For the Platform support services such as discovery, transactions, security, authentication, other communication and protocols.</td>
</tr>
<tr>
<td>S3_CONFIG_LOCATION</td>
<td>config</td>
<td>Configuration files folder name.</td>
</tr>
<tr>
<td>SAML_HOME_PATH</td>
<td><strong>Example:</strong> E:\ExterroSAML_Service_pakage</td>
<td>Service packages extracted location.</td>
</tr>
<tr>
<td>SERVER_CONTEXTPATH</td>
<td>/exterrosso</td>
<td>End point URL path.</td>
</tr>
<tr>
<td>SERVER_DNS_NAME</td>
<td><strong>Example:</strong> accdatasso.accessdatagroup.net</td>
<td>Server DNS name.</td>
</tr>
<tr>
<td>SERVER_PORT</td>
<td>443</td>
<td>Port number to execute the services.</td>
</tr>
</tbody>
</table>
# SAML Configuration for FTK Central

<table>
<thead>
<tr>
<th>Property name</th>
<th>Property Value Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER_SSL_JKS_NAME</td>
<td>&lt;file_name&gt;.JKS</td>
<td>JKS file to store certificate files.</td>
</tr>
<tr>
<td>SERVER_SSL_JKS_PASSWORD</td>
<td>password</td>
<td>Certificate file password</td>
</tr>
<tr>
<td>SERVER_SSL_KEYALIAS</td>
<td>Imported certificate file Alias name</td>
<td>Alias name added in JKS file.</td>
</tr>
<tr>
<td>SERVER_SSL_KEYSTORETYPE</td>
<td>JKS</td>
<td>Keystore file type.</td>
</tr>
<tr>
<td>EXTERRO_CERT_ISSUED_TO</td>
<td>.&lt;domain_name&gt;</td>
<td>Domain name.</td>
</tr>
<tr>
<td>APP_BASE_URL_PATH</td>
<td>/</td>
<td>Application URL end path.</td>
</tr>
<tr>
<td>IS_ONPERM</td>
<td>true</td>
<td>To start the application on a cloud or local mode.</td>
</tr>
<tr>
<td>TENANT_ID</td>
<td>&lt;TFKC tenant id&gt;</td>
<td>Tenant id (get it from the FTKC application) (ADG.selfhost) URL DNS name.</td>
</tr>
</tbody>
</table>

**Example:** accdata.accessdatataroup.net > here tenant id is "accdata" and followed by domain name (.accessdatataroup.net)

**Syntax:**

```plaintext
AUTH_ALGORITHM_TYPE=SHA-256
METADATA_ENTITY_ID=http://<replace_with_dns_name>/exterrosso
PROTOCOL=https
S3_CONFIG_LOCATION=config
SAML_HOME_PATH=<replace_with_saml_home_path>
SERVER_CTXEPATH=/exterrosso
SERVER_DNS_NAME=<replace_with_dns>
SERVER_PORT=443
SERVER_SSL_JKS_NAME=<replace_with_jks>
SERVER_SSL_JKS_PASSWORD=<replace_with_jks_password>
SERVER_SSL_KEYALIAS=<replace_with_jks_alias_name>
SERVER_SSL_KEYSTORETYPE=JKS
EXTERRO_CERT_ISSUED_TO=<replace_with_domain_name>
APP_BASE_URL_PATH=/
IS_ONPERM=true
TENANT_ID=<replace with tenant ID>
```
**Example Configuration:**

```
AUTH_ALGORITHM_TYPE=SHA-256
METADATA_ENTITY_ID=http://accdata.accessdatagroup.net/exterroso/saml/login
PROTOCOL=https
S3_CONFIG_LOCATION=config
SAML_HOME_PATH=E:\ExterroSAML_Service_pakages
SERVER_CONTEXTPATH=/exterroso
SERVER_DNS_NAME=accdata.accessdatagroup.net
SERVER_PORT=443
SERVER_SSL_JKS_NAME=exterrocloudinfo.jks
SERVER_SSL_JKS_PASSWORD=************
SERVER_SSL_KEYALIAS=exterrokey
SERVER_SSL_KEYSTORETYPE=JKS
EXTERRO_CERT_ISSUED_TO=accessdatagroup.net
APP_BASE_URL_PATH=/
IS_ONPERM=true
TENANT_ID=exterro
```

ii. **saml-redis.properties**

<table>
<thead>
<tr>
<th>Property name</th>
<th>Property Value Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redis.hosts</td>
<td>&lt;replace with Redis host IP address&gt;:6379</td>
<td>IP address of Redis installed location.</td>
</tr>
</tbody>
</table>

```
redis.hosts=<replace with redis host IP address>:6379
```
iii. config.properties

<table>
<thead>
<tr>
<th>Property name</th>
<th>Property Value Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>basePath</td>
<td>Configuration folder path</td>
<td>Configuration folder path</td>
</tr>
<tr>
<td></td>
<td>Example: \E:\ExterroSAML_Service_packages\config\metadata\</td>
<td></td>
</tr>
<tr>
<td>tenants</td>
<td>&lt;FTKC tenant id&gt;</td>
<td>Tenant ID (can get it from the FTKC application) (ADG.selfhost) URL DNS name. Example: accdata.accessdatataroup.net &gt; here tenant id is “accdata” and followed by domain name (.accessdatataroup.net).</td>
</tr>
<tr>
<td>&lt;FTKC tenant id&gt;.idpMetadata</td>
<td>&lt;file_name&gt;.xml</td>
<td>The XML file (provided by the client) should be added in &lt;HOME&gt;/config/SSL/ folder.</td>
</tr>
<tr>
<td>&lt;FTKC tenant id&gt;.idpEntity</td>
<td>&lt;replace with IDP entity ID&gt; (Will be provided by client)</td>
<td>An Entity ID is globally unique name for a SAML entity i.e., your Identity Provider (IdP) or Service Provider (SP). It is how other services identify your entity.</td>
</tr>
<tr>
<td>&lt;FTKC tenant id&gt;.metaType</td>
<td>F</td>
<td>To mention file or URL.</td>
</tr>
<tr>
<td>&lt;FTKC tenant id&gt;.idpDiscoveryEnabled</td>
<td>False or true</td>
<td>To enable multiple IDP support.</td>
</tr>
<tr>
<td>&lt;FTKC tenant id&gt;.isWantAssertionSigned</td>
<td>True</td>
<td>To encrypt SAML Assertion between SP and IDP</td>
</tr>
<tr>
<td>&lt;FTKC tenant id&gt;.isRequiredSigned</td>
<td>True</td>
<td>Only signed request will be accepted by SMAL SP.</td>
</tr>
</tbody>
</table>
### SAML Configuration for FTK Central

<table>
<thead>
<tr>
<th>Property name</th>
<th>Property Value Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;FTKC tenant id&gt;.additionalIdpToken</td>
<td>nameid</td>
<td>Mapping attribute name to get authentication field value from client FTK IDP. ('nameid' mapping field is mandatory and multiple mapping attributes can be added with a comma (,) as a separator.)</td>
</tr>
</tbody>
</table>

**Syntax:**

```java
basePath=<replace with SAML homepath>\|config\|metadata\|
tenants=<replace with tenant ID>
<replace with tenant ID>.idpMetadata = <metadata file name.xml>
<replace with tenant ID>.idpEntity = <replace with IDP entity ID>
<replace with tenant ID>.metaType = F
<replace with tenant ID>.httpURL =
<replace with tenant ID>.idpDiscoveryEnabled= false
<replace with tenant ID>.isdsarEnabled = false
<replace with tenant ID>.isWantAssertionSigned = true
<replace with tenant ID>.isRequiredSigned = true
<replace with tenant ID>.userIdpToken = nameid
<replace with tenant ID>.custodianIdpToken = nameid
<replace with tenant ID>.additionalIdpToken= <replace with IDP attributes>
```

**Example Configuration:**

```java
basePath=D:\SMALWorkspace\spring-boot-security-saml-sample-master\|config\|metadata\|
tenants=exterro
exterro.idpMetadata = adfs.xml
exterro.idpEntity = http://adfs.exterro.info/adfs/services/trust
exterro.metaType = F
exterro.httpURL =
exterro.idpDiscoveryEnabled= false
exterro.isdsarEnabled = false
exterro.isWantAssertionSigned = true
exterro.isRequiredSigned = true
exterro.userIdpToken = nameid
exterro.custodianIdpToken = nameid
exterro.additionalIdpToken= nameid,http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
```

**Note:** The `nameid` attribute is mandatory while configuring the attribute names on IDP.
iv. application.properties

In `application.properties` add below properties

<table>
<thead>
<tr>
<th>Property name</th>
<th>Property Value Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server.contextPath</td>
<td>/exterrosso</td>
<td>Provide the application context path for startup.</td>
</tr>
<tr>
<td>server.port</td>
<td>443</td>
<td>Provide the application service port details.</td>
</tr>
<tr>
<td>server.ssl.key-store</td>
<td>&lt;jks_file-name&gt;.jks</td>
<td>Provide the JKS file details.</td>
</tr>
<tr>
<td>server.ssl.key-store-password</td>
<td>password</td>
<td>Provide the JKS file password.</td>
</tr>
<tr>
<td>server.ssl.keyStoreType</td>
<td>File type (JKS)</td>
<td>Provide the Key store file type (JKS).</td>
</tr>
<tr>
<td>server.ssl.keyAlias</td>
<td>Alias name for certificate stored in JKS file</td>
<td>Provide the Alias name for certificate stored in JKS file</td>
</tr>
</tbody>
</table>

**Syntax:**

```properties
server.contextPath=/exterrosso
server.port:443
server.ssl.key-store: \config\SSL\<jks_file-name>.jks
server.ssl.key-store-password:<password>
server.ssl.keyStoreType:JKS
server.ssl.keyAlias:<alias-name>
```

**Example Configuration:**

```properties
server.contextPath=/exterrosso
server.port:443
server.ssl.key-store: \config\SSL\exterrocloudinfo.jks
server.ssl.key-store-password:ExtRRo123
server.ssl.keyStoreType:JKS
server.ssl.keyAlias:exterrokey
```
Starting the SAML Service Provider

Follow the below steps to start SAML Service Provider:

1. Open Task Scheduler on the Windows instance.
2. Click Create Task.
3. Enter Task Name as ExterroSAML.

4. Navigate to Triggers tab.
5. Click **New**.
   - The **New Trigger** pop-up is displayed.

6. Change the **Begin the task** as **At startup**.
7. Click **OK**.
8. Navigate to **Actions** tab.
9. Click **New...**
   - The **New Action** pop-up is displayed.

![New Action pop-up](image)

10. Update the **Program/script** to select **start.bat**.

11. Enter the home path for the **start.bat** in **Start in** field.
12. Navigate to Conditions tab.

13. Deselect the option under Power section.
14. Navigate to **Settings** tab.

15. Enable **Run task as soon as possible after a scheduled start is missed**.

16. Uncheck the **Stop the task if it runs longer than** and **If the running task does not end when requested, force it to stop** options.
17. Click OK.
   - The Task Schedule window is displayed.

18. Click on Task schedule Library.
19. Find ExterroSAML.
20. Click Run option to start the service.
SAML CONFIGURATION FOR FTK CENTRAL

App.config

Location: <installed location>\AccessData\Forensic Tools\7.6\bin

Users must update their WeblabSelfHost.exe.config file as shown below:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseAD</td>
<td>0 (Default)</td>
<td>Provide the value as ‘5’ for SAML authentication.</td>
</tr>
<tr>
<td>MultipleIDP</td>
<td>False (Default)</td>
<td>Set the value as ‘False’ to configure single IDP.</td>
</tr>
<tr>
<td></td>
<td>True</td>
<td>Set the value as ‘True’ to configure multiple IDP.</td>
</tr>
<tr>
<td>ServiceProviderUrl</td>
<td>&lt;URL of SAML Exterro Service&gt;</td>
<td>This URL is referred as the Exterro SAML service URL to which the IDP will send the SAML response or SAML assertion after successful authentication.</td>
</tr>
<tr>
<td>IdpEntityUrl</td>
<td>&lt;entityID&gt;</td>
<td>Enter the value of the ‘entityID’ key (present in the IDP metadata file) provided by the client while configuring SAML. Example:  &lt;EntityDescriptor ID=&quot;_8dee9f22-29f7-44fa-a32b-8179963a865&quot; entityID=&quot;http://adfs.exterro.info/adfs/services/trust&quot; xmlns=&quot;urn:oasis:names:tc:SAML:2.0:metadata&quot;&gt;</td>
</tr>
<tr>
<td>IdentifierAttributeEmailId</td>
<td>&lt;nameID&gt;</td>
<td>The ‘Email Id’ value has to be set against the ‘nameid’ and should be configured as below:  &lt;add key=&quot;IdentifierAttributeEmailId&quot; value=&quot;nameid&quot; /&gt; Example: In below IDP configuration the ‘Email address’ attribute is passed against ‘nameid’ attribute:</td>
</tr>
</tbody>
</table>
Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization’s internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:

Exterro, Inc.

4145 SW Watson Ave., Suite 400

Beaverton, OR 97005.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail: info@exterro.com

Website: wwwexterro.com

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exterro, Inc. The trademarks, service marks, logos or other intellectual property rights of Exterro, Inc and others used in this documentation (“Trademarks”) are the property of Exterro, Inc and their respective owners. The furnishing of this document does not give you license to these patents, trademarks, copyrights or other intellectual property except as expressly provided in any written agreement from Exterro, Inc.

The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.

You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc’s prior written consent. In addition, you may not use the