SecureAuth IdP

Two-Factor GFIPM Configuration guide

SecureAuth IdP can be configured to provide attributes required from within the GFIPM framework. When configuring SecureAuth IdP to provide the proper assertions you will first configure the type of user authentication you would like the user to be faced with. Many time companies will provide SSO based access if a user is inside the protected network and then set the authentication up to 2 factor authentication if the user is outside of the protected network.

**Summary /Overview**

This document describes the steps to setup a SAML integration for providing assertions that work with the GFIPM Framework

**SecureAuth Version**

7.4

**Description / Definitions**

**SP Init (Service Provider Initiated):**Service provider initiates the login process by providing a SAML assertion.

**GFIPM:  The Global Federated Identity and Privilege Management (GFIPM) program is funded jointly by the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS), and is under the direction of the**[**Global Justice Information Sharing Initiative**](http://www.it.ojp.gov/default.aspx?area=globalJustice)**. The goal of GFIPM is to enable information sharing for state and local agencies through a federated model that is secure, scalable, and cost-effective. One of the guiding principles of GFIPM is to seek to understand and meet the needs of state and local agencies through a collaborative, consensus-based process that incorporates the input of all major stakeholders, including state and local agencies as well as the federal government.**

**Configuration Steps**

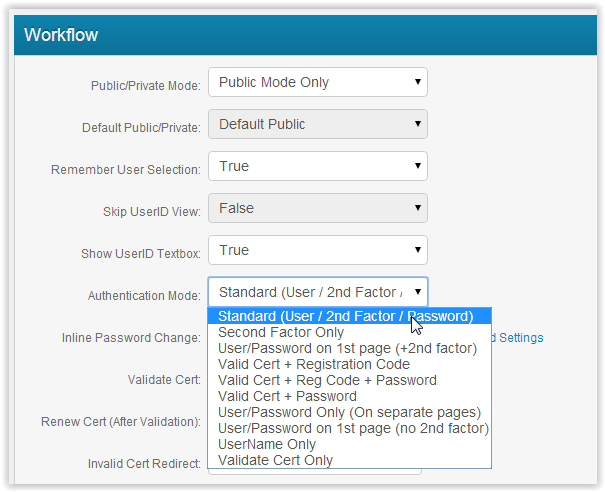
1) Configuring 2-Factor/SSO

2) Configuring SAML Datasources

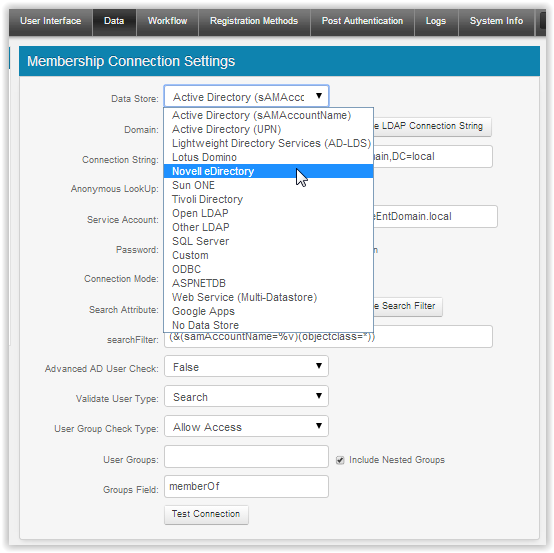
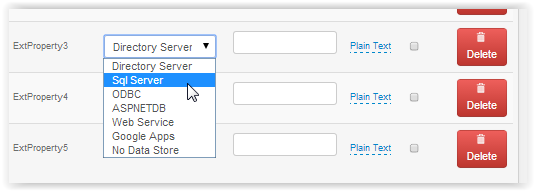
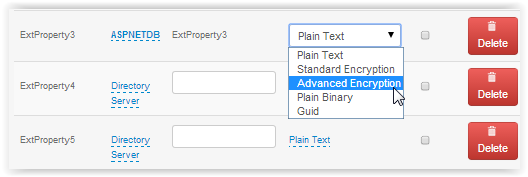
3) Configure SAML Assertion

**Configure 2-Factor/SSO access to assertion**

1. Go to the SecureAuth realm and configure the workflow section to require 2-factor authentication or SSO.  This is where you can specify that the end user has to use such items as a CAC/PIV card, push notification, SMS, email etc...

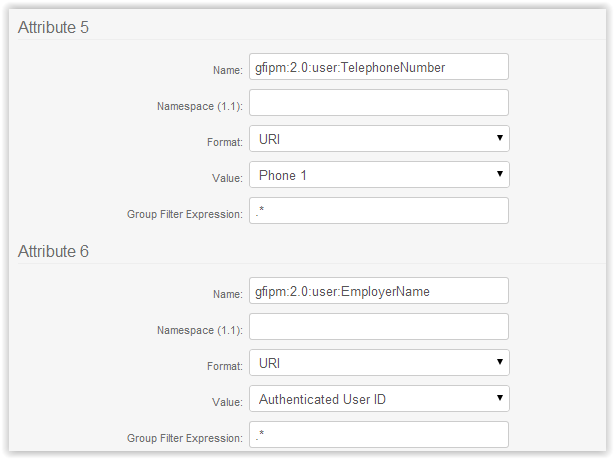


**Configure SAML Datasources**

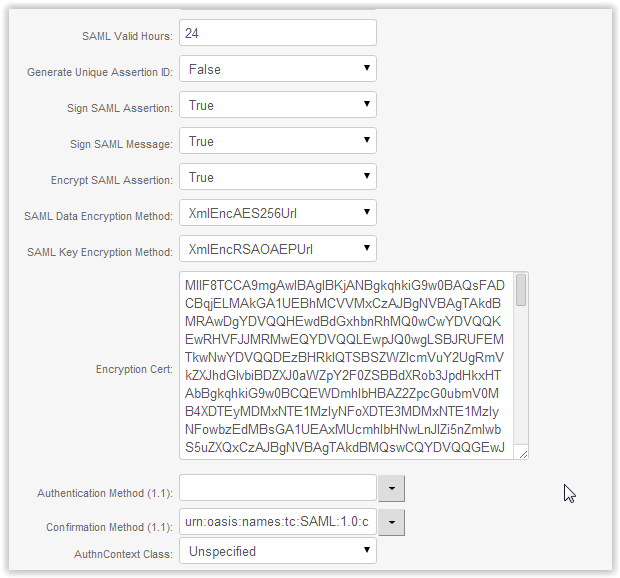
1. In the Data section you can select the datasources you will be connecting too  
   
2. Now you can select the specific datasources for each attribute you will want to include in the SAML assertion  
   
3. You can also select plain text/ecryption, etc.  
   

**Configure SAML Assertion**

1. In the post authentication section you can easily map the required attributes.



2. You can also choose to encrypt the assertion and set any other attributes.



**You are now ready to test**

1. Click [HERE](https://demoportal.gosecureauth.com/SecureAuth26/SecureAuth.aspx?SAMLRequest=fZJLb4MwEIT%2fCvI9PEwaEisg0eTQSGmLCu2hl8qQJVgyNvWaPv59CfSRXnJc7Xhm55PXyFvZsbS3jXqA1x7QOh%2btVMjGRUx6o5jmKJAp3gIyW7E8vd0z6vqsM9rqSkvipIhgrNBqoxX2LZgczJuo4PFhH5PG2g6Z55kGJHaugdo91qJrXQXWyxtRllqCbVxE7Z28qZfd5wVxtsMxQvGT7Z%2fJAVrdaWO5dI8aoeoN8OF4t9Ktl4%2fjqQtdEGe3jclLsFyF85pHURCu5pSGUAZLuIpgGfmLQ8nrQYbYw06h5crGhPrBfOaHM7oqgpDRBaP%2bM3Gy76LXQh2EOl6mUk4iZDdFkc2mKk9gcKwxCEiyPrFlY7A5o33Zlv8gJslFoPgLdO2d5UyhHbsbjHfbTEtRfTqplPp9MxC0EJOAeMn05P9%2fSL4A&RelayState=ss%3amem%3aaccccbaf7fffe6823f77dcf3b56b010fb77c7e47cdaf5125c193062a387d8eb5) and use your SecureAuth provided test username/2nd factor/Password

