

**Service Provider**

Version 1.0

***Important:*** *This document has been prepared specifically for you and contains confidential, trade secret and proprietary information to Activants. Neither this document nor the information contained within this document may be disclosed to any person outside of your organization without Activants’ expressed written permission. By accepting or reading this document, you affirm that you will comply with these expectations.*

**Prepared by Activants Pte Ltd**



24 Sin Ming Lane

#08-105 Midview City

Singapore 573970

Tel +65 6684 7044

Fax +65 6684 7042

Email [info@activants.com](mailto:info@activants.comhttp://www.activants.com)

Contents

[1. SAML 3](#_Toc29544019)

[a. About SAML 3](#_Toc29544020)

[b. SAML diagram 3](#_Toc29544021)

[c. SAML Sequence diagram 4](#_Toc29544022)

[d. Activants SAML Single-Sign-On Process 4](#_Toc29544023)

[e. Activants SAML Single-Sign-On Activity diagram 5](#_Toc29544024)

[2. ACTIVANTS SAML SIGNING CERTIFICATES 6](#_Toc29544025)

[a. SAML Certificates diagram 6](#_Toc29544026)

[b. X509 Certificates 6](#_Toc29544027)

[c. Identity Provider Certificates 6](#_Toc29544028)

[d. Activants Service Provider Certificate 7](#_Toc29544029)

[e. Generate X509 Certificate (.CER and .PFX) 7](#_Toc29544030)

[f. Adding Certificate to Microsoft Management Console (MMC) 8](#_Toc29544031)

[g. Adding Certificate (.PFX) to IIS Server 8](#_Toc29544032)

[3. ACTIVANTS SERVICE PROVIDER SAML METADATA 9](#_Toc29544033)

[a. SAML Metadata 9](#_Toc29544034)

[b. Generate Activants Service provider SAML Metadata 9](#_Toc29544035)

[c. Import Activants Service Provider metadata into Identity provider 10](#_Toc29544036)

[4. IDENTITY PROVIDER SAML METADATA 12](#_Toc29544037)

[a. Identity provider saml metadata 12](#_Toc29544038)

[b. Import Identity Provider metadata into Activants Service provider 12](#_Toc29544039)

[c. Import Identity Provider SAML Certificates into Service Provider 13](#_Toc29544040)

[5. SAML LOGGING 14](#_Toc29544041)

[6. MSSQL DATABASE 14](#_Toc29544042)

[a. Database tables 14](#_Toc29544043)

[b. Table and its uses 15](#_Toc29544044)

[c. Database and connections 15](#_Toc29544045)

[7. SPCP based SAML Process FLOW (HTTP-Artifact) 15](#_Toc29544046)

[a. Login Process Flow (HTTP-Artifact) 15](#_Toc29544047)

# SAML

## About SAML

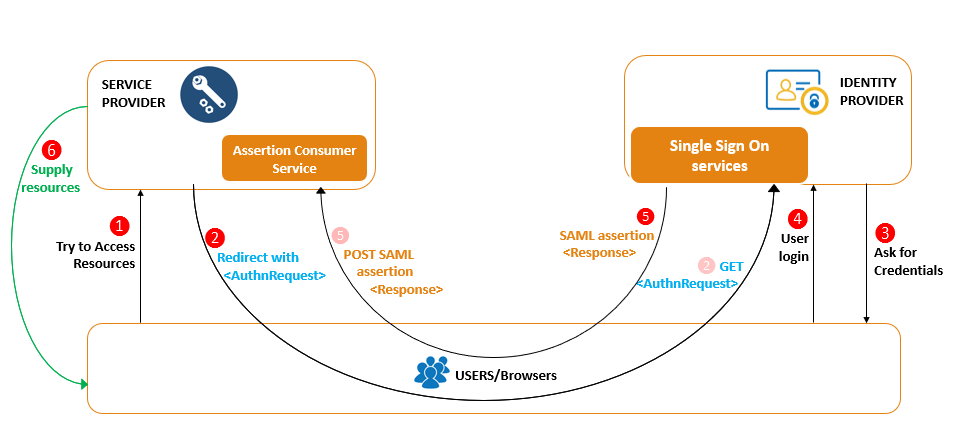
Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between Identity Providers and Service Providers to support Single-Sign-On (SSO) capability. SAML uses:

* **Identity Providers**: Manage User Identities and provide interfaces allowing Users to log in to SAML sessions.
* **Service Providers**: Acts as Relying Parties for SAML identity information.

In our environment, Activants Service Provider (ASP) acts as a service provider and has been tested with the following identity providers:

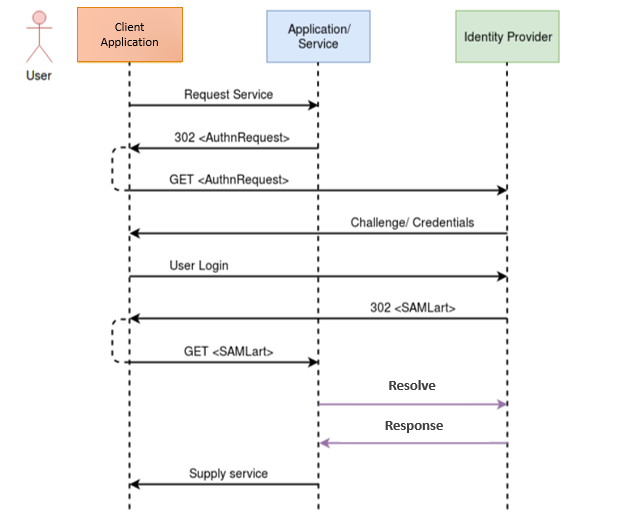
* Xecurify - Secure It Right – Identity Provider

## SAML diagram



* Users try to access resources
* Service Provider redirects users to Identity providers.
* Identity providers authenticates users and provides SAML Assertions/response to service providers.
* Service Providers supply requested resources to the authenticated user.

## SAML Sequence diagram

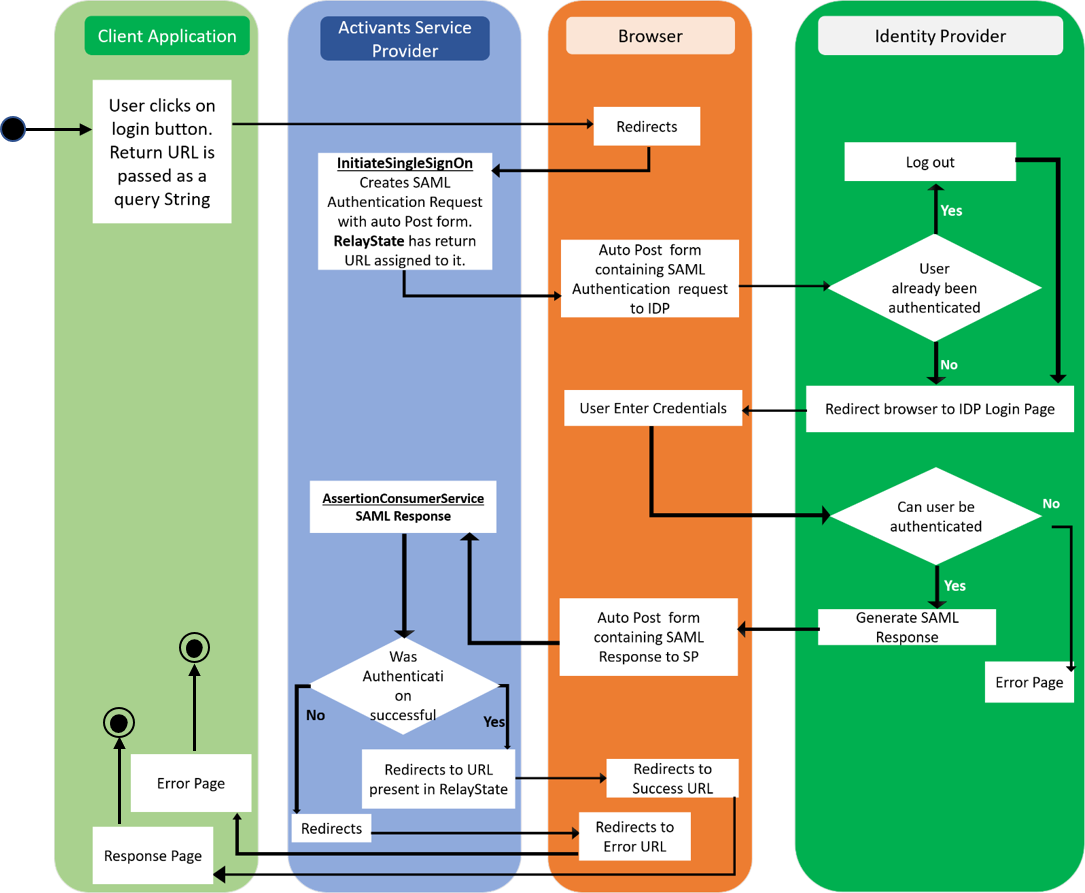


## Activants SAML Single-Sign-On Process

When users click login in any Activants web applications, Activants Service Provider (ASP) sends an authentication request to the Identity provider. The identity provider displays a login window where the User can enter his credentials. If the authentication is successful, the identity provider passes a response containing one or more assertion statements to the Activants Service Provider.

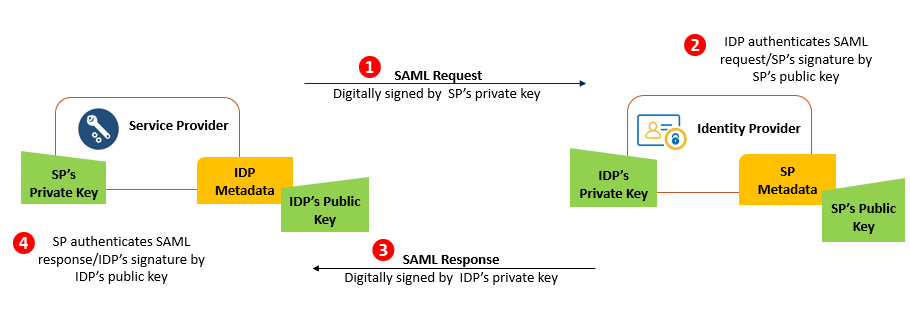
An assertion indicates that the Identity Provider has successfully authenticated the User and includes a **user id** (ex: e-mail address) and possibly additional optional attributes about the User (ex: Name, department, etc.). The Activants Service Provider uses the assertions and then logs the authenticated user into the Activant’s web Applications.

## Activants SAML Single-Sign-On Activity diagram



# ACTIVANTS SAML SIGNING CERTIFICATES

## SAML Certificates diagram



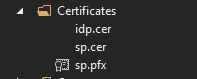
## X509 Certificates

Security is one of the most important to ensure that messages are coming from the expected identity and service provider rather than a malicious third-party. These certificates are stored in both the identity and service providers at the time of configuration.

A ***self-signed certificate can be used temporarily during initial testing***. For production, we use a publicly trusted X.509 certificate from a public third-party certification authority (CA).

## Identity Provider Certificates

The identity provider’s public certificate needs to be imported into Activants Service Provider. The easiest approach is to import the metadata provided by the identity provider. The metadata includes configuration information as well as certificates. If configuring the identity provider manually, copy and paste its public certificate manually into **idp.cer** file under Certificates folder.



## Activants Service Provider Certificate

Two certificates (typically with a ".cer" file extension) and matching private key certificate (typically with a ".pfx" file extension) must be created. These can then be imported into the Activants Service Provider using the SAML settings. The public certificate needs to import into the identity provider. The easiest way to do this is to export the Activants Service Provider settings as metadata, and then import the metadata (which includes the certificate) into the identity provider.

To generate/create Activants Service Provider **metadata**, we can simply refer to <https://www.samltool.com/sp_metadata.php>

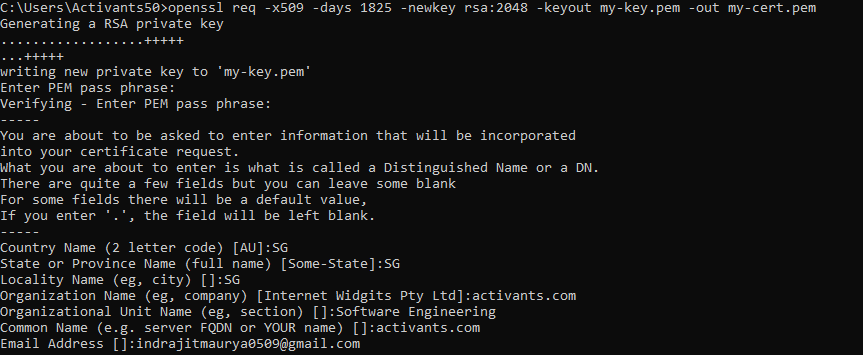
## Generate X509 Certificate (.CER and .PFX)

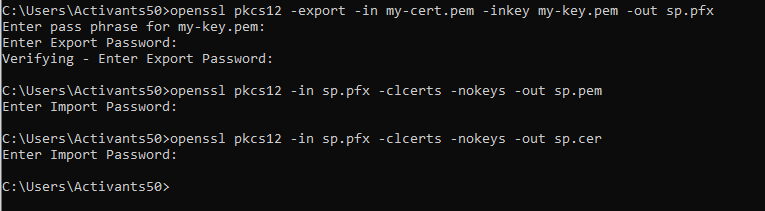
A ***self-signed certificate can be used temporarily during initial testing***.

For generating Self-signed certificate, we use OpenSSL. Steps to download and install OpenSSL is as follows:

* Download the Software : <http://openssl.cs.utah.edu/related/binaries.html>
* Click on Open SSL for Windows
* Download [Win64 OpenSSL v1.1.0L](http://slproweb.com/download/Win64OpenSSL-1_1_0L.exe) (37MB) and install it.
* Please select The OpenSSL binaries (/bin) directory while installing the application.
* Generate .PFX and .CER files
* Open Command Prompt and paste the following command.

***openssl req -x509 -days 1825 -newkey rsa:2048 -keyout my-key.pem -out my-cert.pem***or refer to the following image.





## Adding Certificate to Microsoft Management Console (MMC)

* Steps to follow:
* Open MMC
* Click on File – Add or Remove Snap-ins
* Click on Certificates
* Click on Add – Computer Account – Local Computer – Finish
* Right click on Trusted Root Certificates – All Tasks – import.
* Browse the .PFX file – import the file.

## Adding Certificate (.PFX) to IIS Server

* Open Server Certificates and click on import.
* Browse the file and import it.

# ACTIVANTS SERVICE PROVIDER SAML METADATA

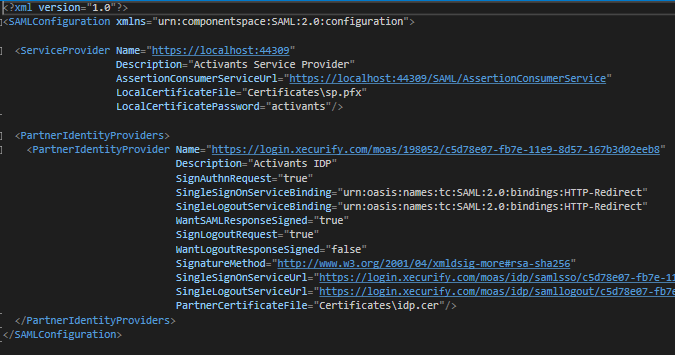
## SAML Metadata

SAML also defines a format for metadata, which is provided in the form of an XML document that describes what is supported and required by an identity or service provider.

## Generate Activants Service provider SAML Metadata

Steps to generate saml metadata:

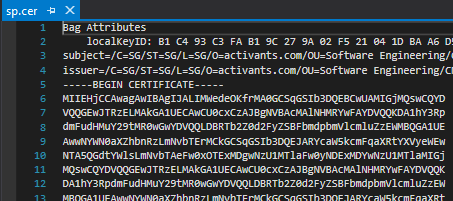
1. Open **saml.config** file from ActivantsSP web application.



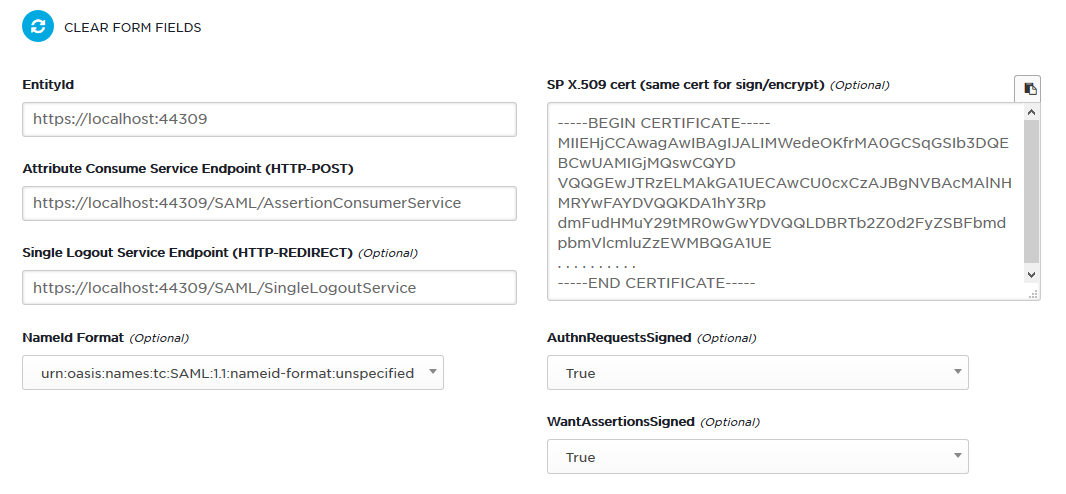
**Key factors:**

* **Service Provider name:** The ID (EntityId) of service provider. It can be the domain name. This ID will be shared with the Identity provider.
* **AssertionConsumerServiceUrl:** URL to receive SAML Response from IDP.
* **Local Certificate File**: Path of the local certificate (typically .pfx) to sign the SAML request before sending to the IDP. IDP validates the SAML request with the shared public key of service provider.
* **Local Certificate password**: password for the .PFX file.

1. Open sp.cer file under Certificates folder. Include **all** including *----BEGIN CERTIFICATE---- (key) ------END CERTIFICATE-----* while generating metadata.



1. Open <https://www.samltool.com/sp_metadata.php>
2. Fill the fields as in the picture below. Please refer to the saml.config above to fill all the required fields.



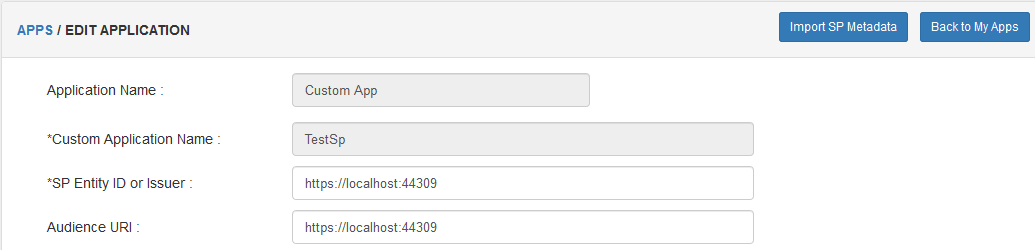
Click on generate SP metadata. This will generate an XML document that describes what is supported and required by an identity provider.

1. Copy the Service Provider Metadata and save it to a file.

## Import Activants Service Provider metadata into Identity provider

We can configure Service Provider metadata into identity providers either manually ***or*** directly using a saml configured text file (XML document). The sample identity provider used here is [*www.xecurify.com*](http://www.xecurify.com)

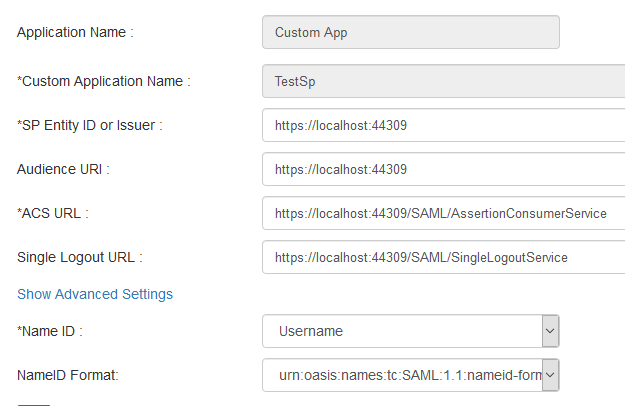
**Importing using saml metadata file.**

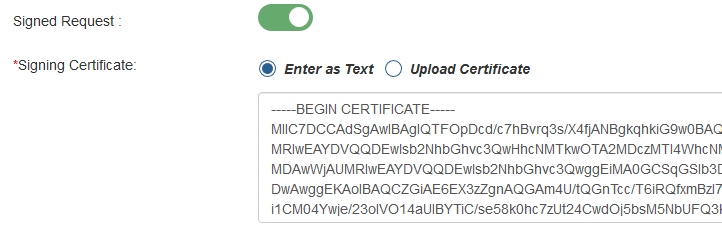


We can import and configure Service provider metadata by clicking the **import SP metadata** button.

**Manually configuring SAML metadata**

If absent of SAML Configured text file, one can manually configure Service Provider SAML metadata into Identity provider.

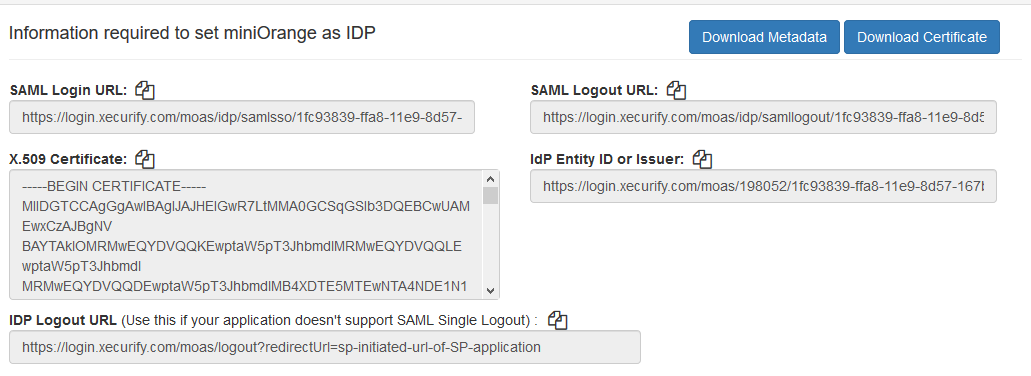




# IDENTITY PROVIDER SAML METADATA

## Identity provider saml metadata

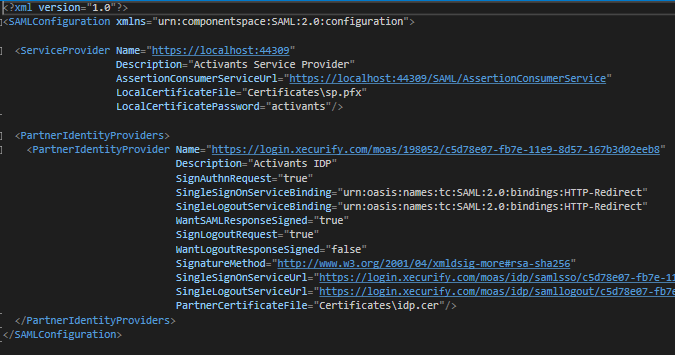
Identity providers provides SAML metadata in the form of an XML document that describes what is supported and required by Service providers.



One can either download Identity Provider’s metadata (XML document) directly or configure Identity provider metadata into Service provider manually with the required fields.

## Import Identity Provider metadata into Activants Service provider

Service Provider uses **saml.config** file to configure itself with the Identity Provider metadata. By the URLs provided in Identity Provider metadata we can configure **saml.config** file to connect to its IDP.

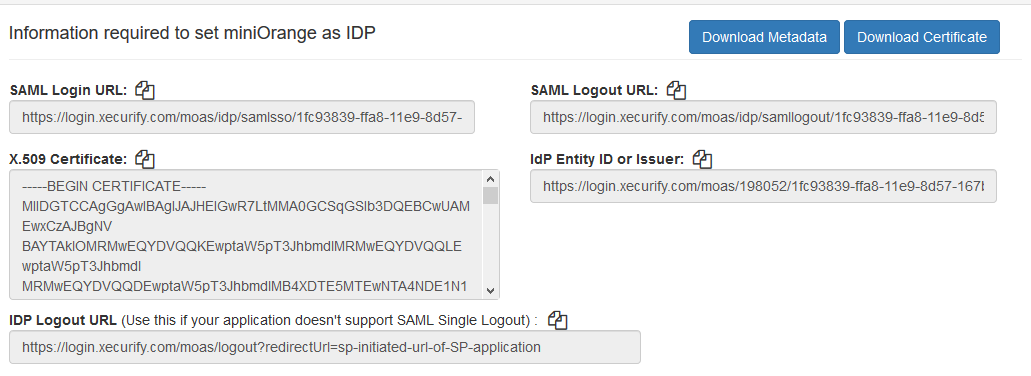


**Key Factors:**

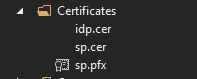
* **PartnerIdentityProvider**: The ID of Identity provider.
* **SingleSignOnServiceUrl**: The login page URL of Identity Provider
* **SingleLogotServiceUrl:** The logout URL of Identity Provider
* **PartnerCertificateFile:** The local path of the shared public key of IDP used to validate and decrypt the Signed SAMLresponse sent from IDP.

## Import Identity Provider SAML Certificates into Service Provider

The identity provider’s public certificate needs to be imported into Activants Service Provider. The easiest approach is to import the metadata provided by the identity provider. The metadata includes configuration information as well as certificates.



If configuring the identity provider manually, copy and paste its public certificate manually into **idp.cer** file under Certificates folder.



# SAML LOGGING

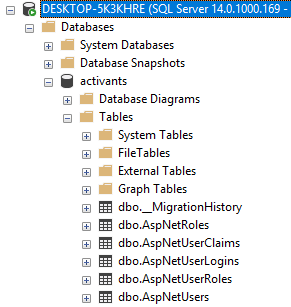
SAML provides logging features where it stores all the debug logs to identity issues. The log files are stored under **ActivantsSP\_MVC/logs** directory.

# MSSQL DATABASE

## Database tables

Activants Service Provider is an ASP.NET C# MVC projects with Individual User Authentication as its authentication type.

Individual User authentication has by default the following tables as shown in the picture below. These tables and its columns are generated automatically once the application starts running.



**dbo.AspNetUsers** : This table is used to the id of an individual along with its security stamp.

**dbo**.**AspNetUserClaims**: This table is used to store other related additional optional attributes about the User (ex: Name, department, etc.) which comes along with SAML assertions/ response.

***Note****: The claims table is optional. One can opt to delete the data of a user once he/she logout of the system.*

## Table and its uses

**dbo.AspNetUsers** table is used to store an id of an individual user along with its security stamp. This table can be used to **count** the total number of authenticated users using the service.

## Database and connections

We configure database in web.config file present in ActivantsSP web application.



# SPCP based SAML Process FLOW (HTTP-Artifact)

## a. Login Process Flow (HTTP-Artifact)

|  |  |  |
| --- | --- | --- |
| **Client** | **Service Provider** | **Identity Provider** |
| Sign (URL) |  |  |
|  |  | LoginPage   * Credentials * Redirect |
|  |  | SSOService   * Page\_Load * CreateSAMLResponse * SendSAMLResponse |
|  | AssertionConsumerService   * ProcessSAMLResponse * ReceiveSAMLResponse |  |
|  |  | ArtifactResponder   * Page\_Load * ProcessArtifactResolver |
|  | AssertionConsumerService   * ReceiveSAMLResponse * ProcessSAMLResponse * ProcessSuccessSAMLResponse |  |
| Logged in page |  |  |

## b. Log out Process Flow (HTTP-Artifact)

|  |  |  |
| --- | --- | --- |
|  | Service Provider | Identity Provider |
| Logout (URL) |  |  |
|  | Logout page   * Logout\_function |  |
|  |  | SLOService   * Page\_Load * ProcessLogoutRequest * CreateLogoutResponse * SendLogoutResponse |
|  | SLOService   * Page\_Load * ProcessLogoutResponse |  |
| Default Page |  |  |