# OTDS as SAML service Provider

# **Contents**

Contents

[OTDS as SAML service Provider 1](#_Toc38149559)

[**Contents** 2](#_Toc38149560)

[1. Overview 4](#_Toc38149561)

[2. Revision History 5](#_Toc38149562)

[3. Terminology 6](#_Toc38149563)

[4. Prerequisites 7](#_Toc38149564)

[5. ADFS Configuration 8](#_Toc38149565)

[5.1 Creating a self-signed SSL certificate 8](#_Toc38149566)

[5.2 Installing AD DS 8](#_Toc38149567)

[5.3 Creating accounts 9](#_Toc38149568)

[5.4 Importing adfs certificate to server 10](#_Toc38149569)

[5.5 Configuring IIS 10](#_Toc38149570)

[5.6 Installing AD FS 11](#_Toc38149571)

[5.8 Adding Relying party rules 12](#_Toc38149572)

[5.7 Post configuration steps 13](#_Toc38149573)

[6. OTDS Configuration 14](#_Toc38149574)

[6.1 Create ADFS Partition 14](#_Toc38149575)

[6.2 Create SAML Authentication Handler 17](#_Toc38149576)

[6.3 Create OAuth Client 19](#_Toc38149577)

[7. Test OAuth Client 20](#_Toc38149578)

[7.1 OAuth URL 20](#_Toc38149579)

## Overview

This document provides the configuration steps for Documentum client to leverage OTDS functionality and use it as service provider for SAML authentication for the client with SAML identity provider(IdP).

## Revision History

|  |  |  |
| --- | --- | --- |
| Rev | Date | Comments Added |
| 01 | April 16,2020 | Initial Draft version |

## Terminology

OTDS Open Text Directory Services

IdP Identity Provider

SAML Security Assertion Markup Language

ADFS Active Directory Federation Service

OAuth Open Source Standard for Authorization

SSO Single Sign On

SP Service Provider

ADDS Active Directory Domain Service

IIS Internet Inforamtion Service Manager

## Prerequisites

* + OTDS should be up and running in both native and secure mode.
  + Windows Server 2019 should be installed.

## ADFS Configuration

### 5.1 Creating a self-signed SSL certificate

SSL is an essential requirement of AD FS. In a production environment, certificates are obtained from a certification authority (CA). For the purposes of lab deployment in this guide, self-signed certificates are used

Below commands can be created using openssl on a Linux machine like Ubuntu/Centos or can use java keytool for the same.

* + **Generate a private key:**

openssl genrsa -out adfs.key 2048

* + **Generate a CSR (Certificate Signing Request):**

openssl req -new -key adfs.key -out adfs.csr

**NOTE:** Hostname should match with ADFS domain name.

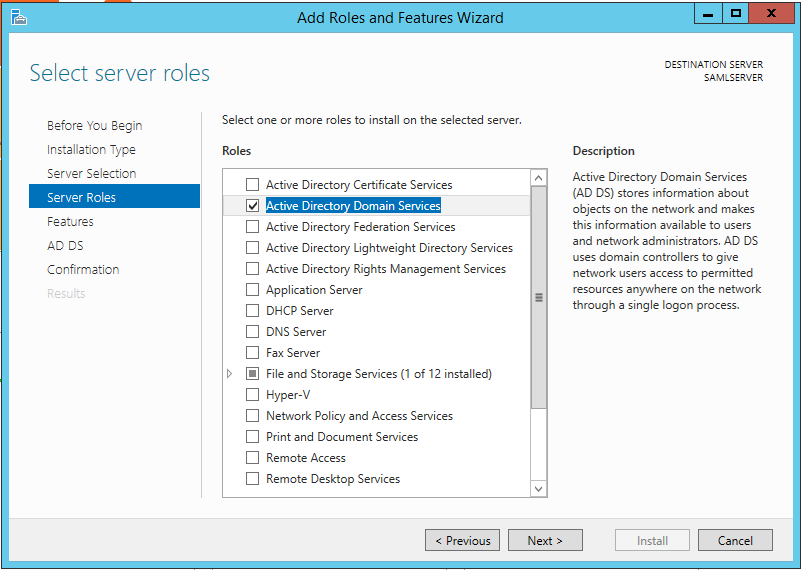
* + **Generate a self-signed certificate:**

openssl x509 -req -days 3650 -in adfs.csr -signkey adfs.key -out adfs.cert

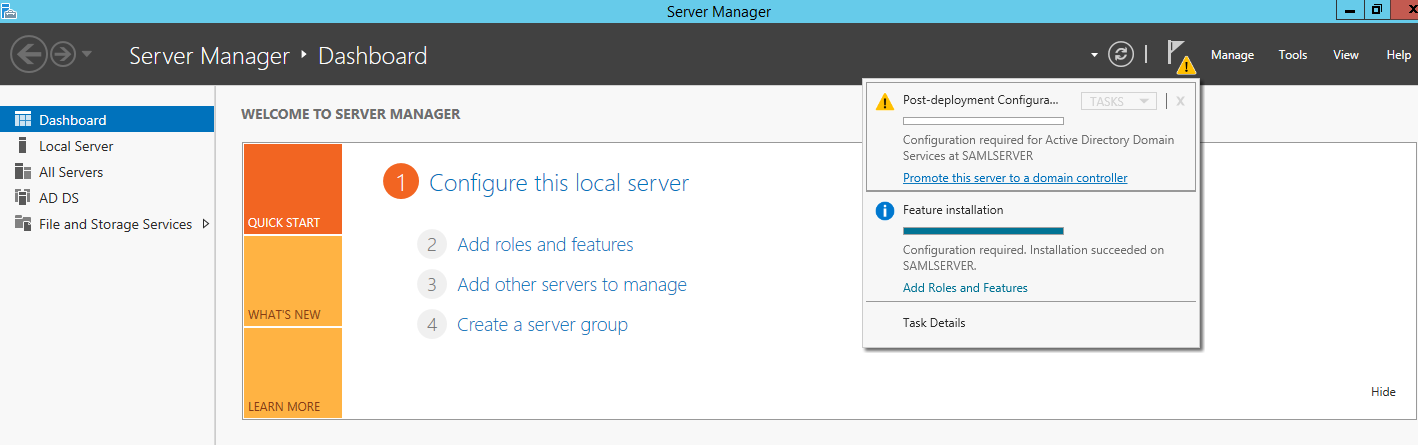
openssl pkcs12 -export -in adfs.cert -inkey adfs.key -out adfs.p12 -passout pass:password

5.2 Installing AD DS

* + Open **'Server Manager'**
  + Click on **'Add Roles or Features'**
  + On the **'Server Roles'** Page, select **'Active Directory Domain Services'** and Install



* + Once installation is completed, click on notification for **‘Post-Deployment Configuration’**. Select **‘Promote this server to a domain controller’**



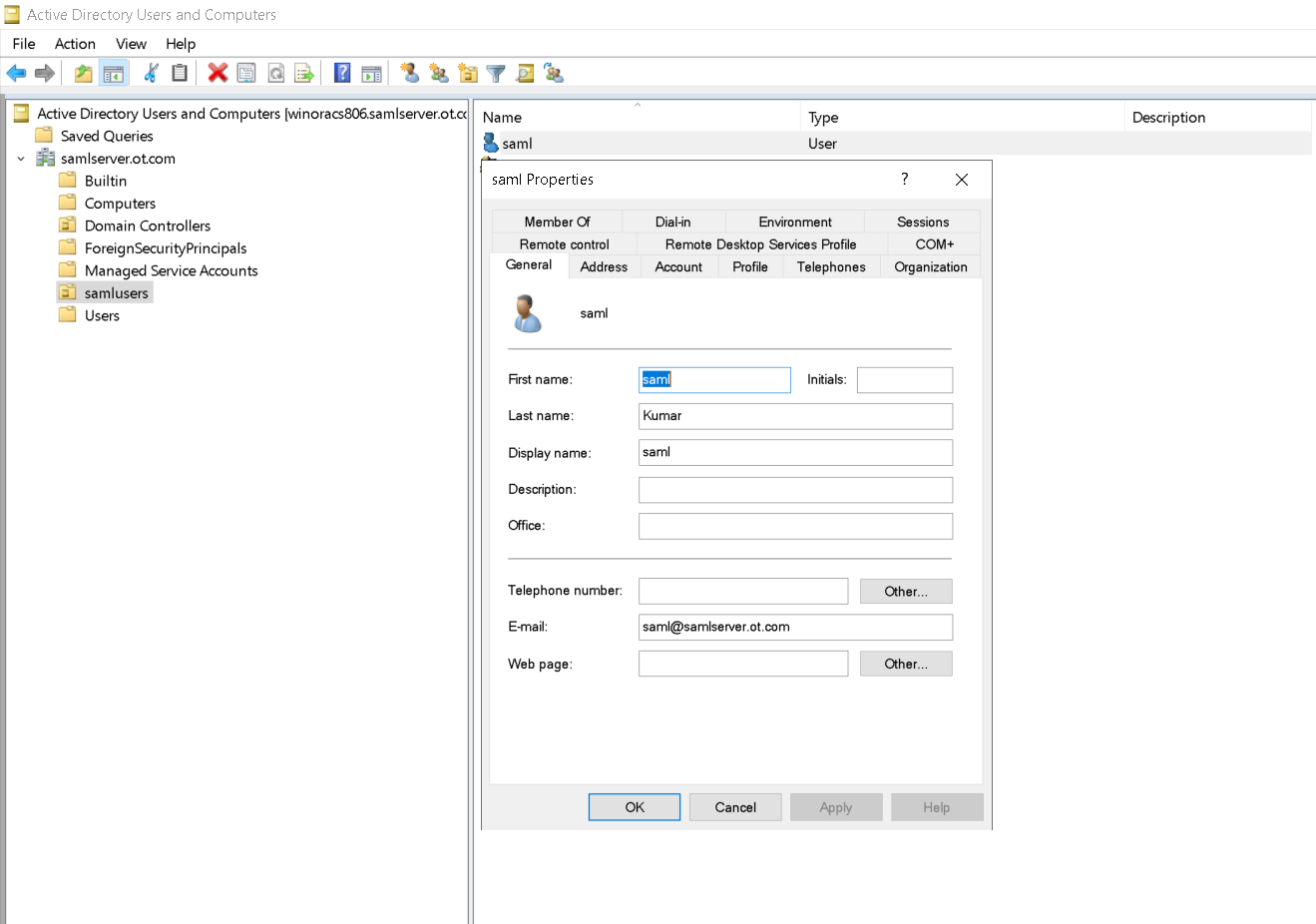
**Active Directory Domain Services Configuration Wizard:**

* + Deployment Configuration:
    - Add a new forest
    - Root Domain Name: samlserver.ot.com
  + Domain Controller Options:
    - Password: Password@123
  + Additional Options:
    - NetBIOS Domain name: SAMLSERVER0
  + Next->Next->Next->Install

### 5.3 Creating accounts

Restart the machine and login as Domain user

* + Open **‘Server Manager’**
  + Click on **Tools** -> **Active Directory Users and Computers**
  + Create new **‘Organizational Unit’** under domain named samlusers, and create new user ‘saml’ and group ‘samlgroup’ and configure First Name, Last Name, Display Name and email id as mentioned below:



* + Add the ‘saml’ user to the group ‘samlgroup’

### 5.4 Importing adfs certificate to server

* + Click **Start** -> **Run** -> **certmgr.msc**
  + Double-click the **Trusted Root Certification Authorities** folder, right-click **Certificates** -> **All Tasks** -> **Import**.
  + On the **Welcome to the Certificate Import Wizard** page, click **Next**.
  + On the **File to Import** page, select **adfs.cert** and import it to **Trusted Root Certification Authorities**
  + Repeat same steps to import **adfs.p12**.

### 5.5 Configuring IIS

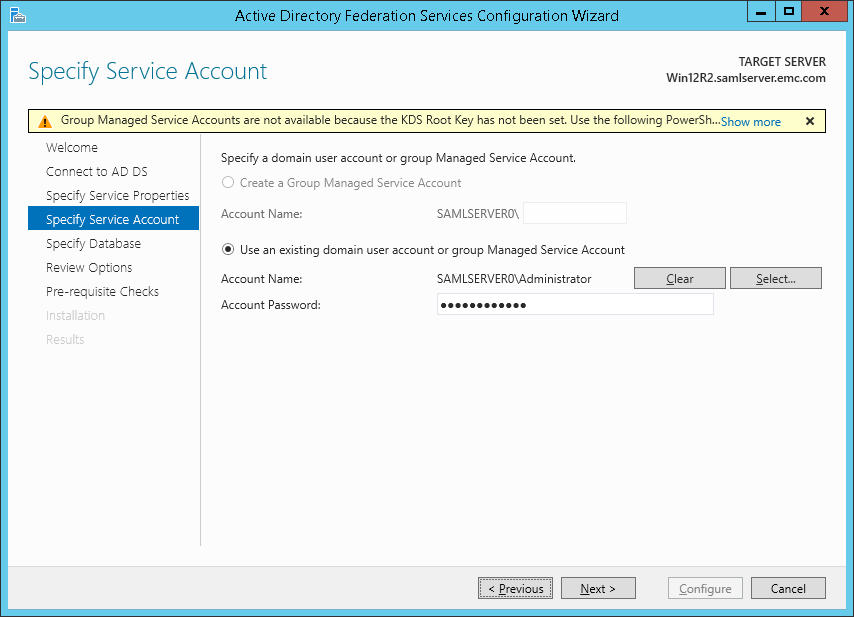
* + Open **'Server Manager'**
  + Click on **'Add Roles or Features' and install ‘Web Server (IIS)’** Once installation is completed, open IIS Manager
  + Click on **Tools** -> **Internet Information Services (IIS) Manager**
  + Click the root node that contains the name of the computer, and then, in the details pane, double-click the icon named **Server Certificates** in the **IIS grouping**
  + In the **Actions** pane, click **Import** and import **adfs.p12**
  + In the console tree, select **Sites** -> **Default Web Site**
  + In the **Actions** pane, click **Bindings**
  + In the **Site Bindings** dialog box, click **Add**
  + In the **Add Site Binding** dialog box, select **https** in the **Type** drop-down list, select the **(host/IP)** certificate in the **SSL certificate** drop-down list, click **OK**
  + Close the **Internet Information Services (IIS) Manager** console.

### 5.6 Installing AD FS

* + Open **'Server Manager'**
  + Click on **'Add Roles or Features'** and install **'Active Directory Federation Services'**
  + Once installation is completed, click on notification for **‘Post-Deployment Configuration’**. Select **‘Configure the federation service on this server’**

**Active Directory Federation Services Configuration Wizard:**

* + Welcome
    - Create the first federation server in a federation server farm
  + Connect to AD DS
  + Specify Service Properties
    - SSL Certificate:samlserver.ot.com (from drop down)
    - Federation Service name: samlserver.ot.com
    - Federation service Display name: samlserver
  + Specify Service Account
    - Use an existing domain user account and provide user details



* + Specify database
    - Create a database on this server using Windows Internal Database
  + Next->Next->Configure

### 5.8 Adding Relying party rules

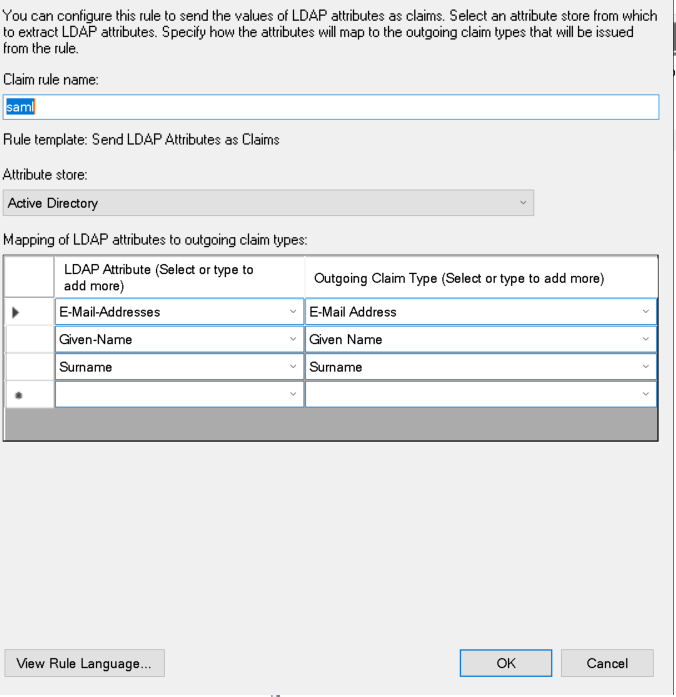
* + Open **‘Server Manager’**
  + Click on **Tools** -> **ADFS Management**
  + Under **ADFS** -> **Trust Relationships**, right-click the **Relying Party Trusts**, and then click **Add Relying Party Trust**.
  + Click the **Start** button to start the Add **Relying Party Trust Wizard**.
    - Welcome
      * Select ‘Claims aware’
    - Select Data Source
      * Select **Import data about the relying party from a file**

**NOTE:** Make sure you had already created authentication handler on OTDS and exported the metadata and saved it to xml file.

* + - Specify Display Name
      * OTDS
    - Click Next-> Next->Next and then Close.

**Configure Claim Rules:**

* + Click ‘**Edit Claim Issuance Policy’**
  + Click **‘Add Rule’**
  + Select **Send LDAP Attributes as Claims**
  + Enter **Claim rule name**
  + Select **Active Directory** as **Attribute store** and **add mappings** as shown in snapshot below:



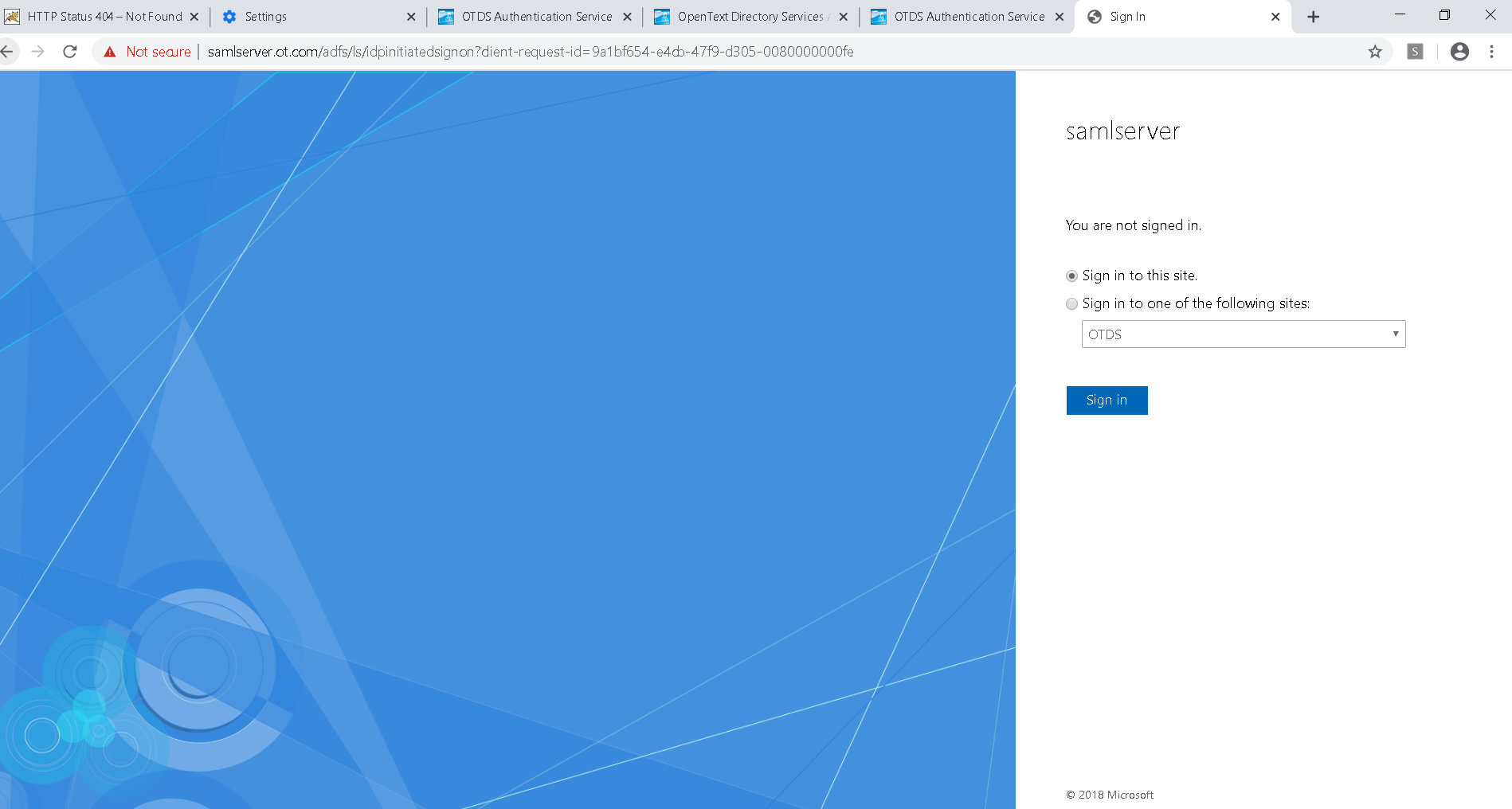
* + Click **Finish**

### 5.7 Post configuration steps

* + Go to PowerShell and run the below command:
    - **set-ADFSRelyingPartyTrust –TargetName “OTDS” –EncryptClaims $False**

**NOTE:** TargetName should match to ReplyingPartyTrust name as earlier created.

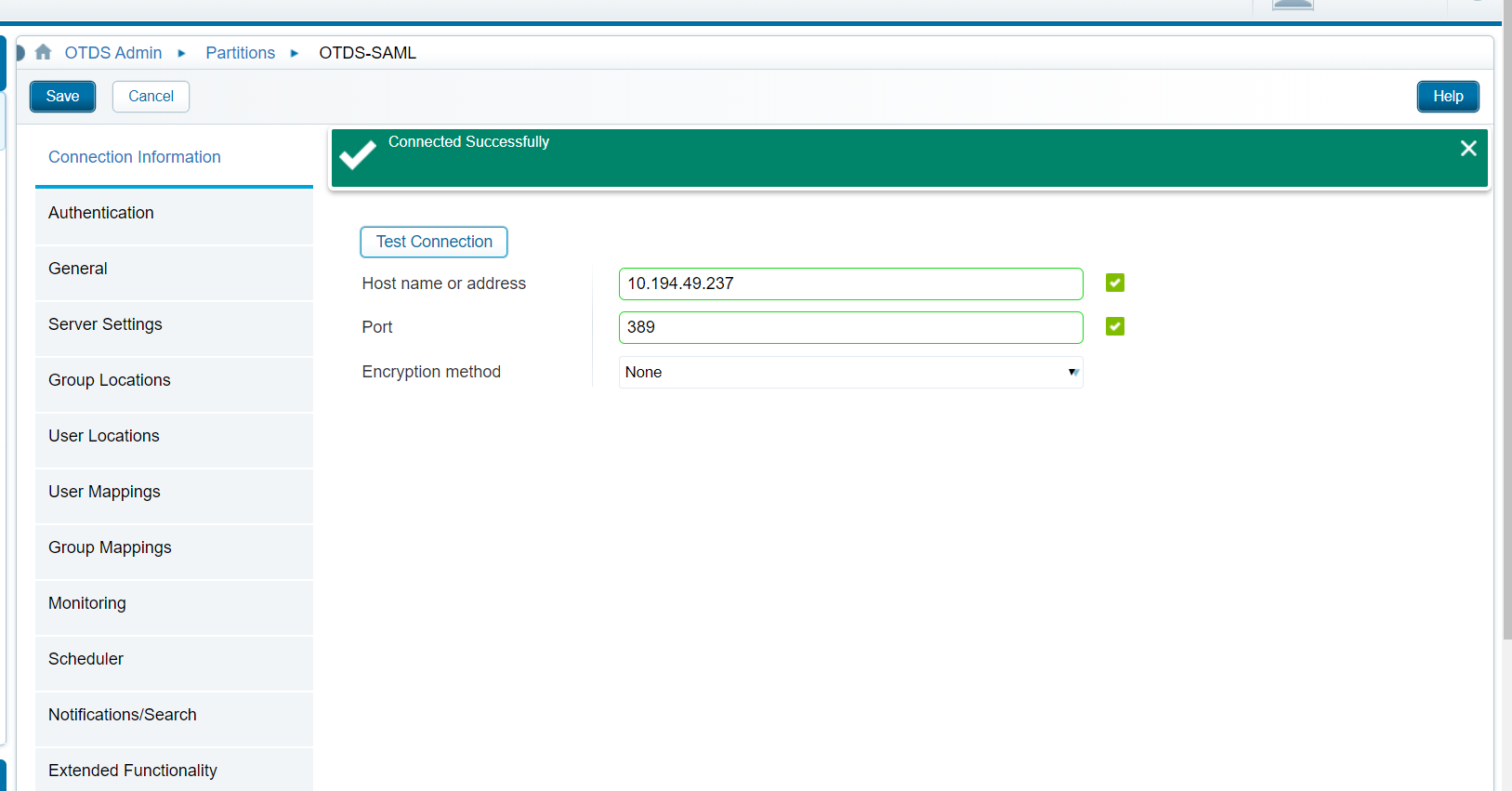
* + Enable **EnableIdpInitiatedSignonPage** 
    - **set-ADFSProperties -EnableIdpInitiatedSignonPage $True**
  + **Sanity check:** Access the below URL in browser and check if authentication succeeds or not. Also can use HTTP network monitoring tools to capture sample SAML request and response
  + **https://<FQDN>/adfs/ls/idpinitiatedsignon.aspx**



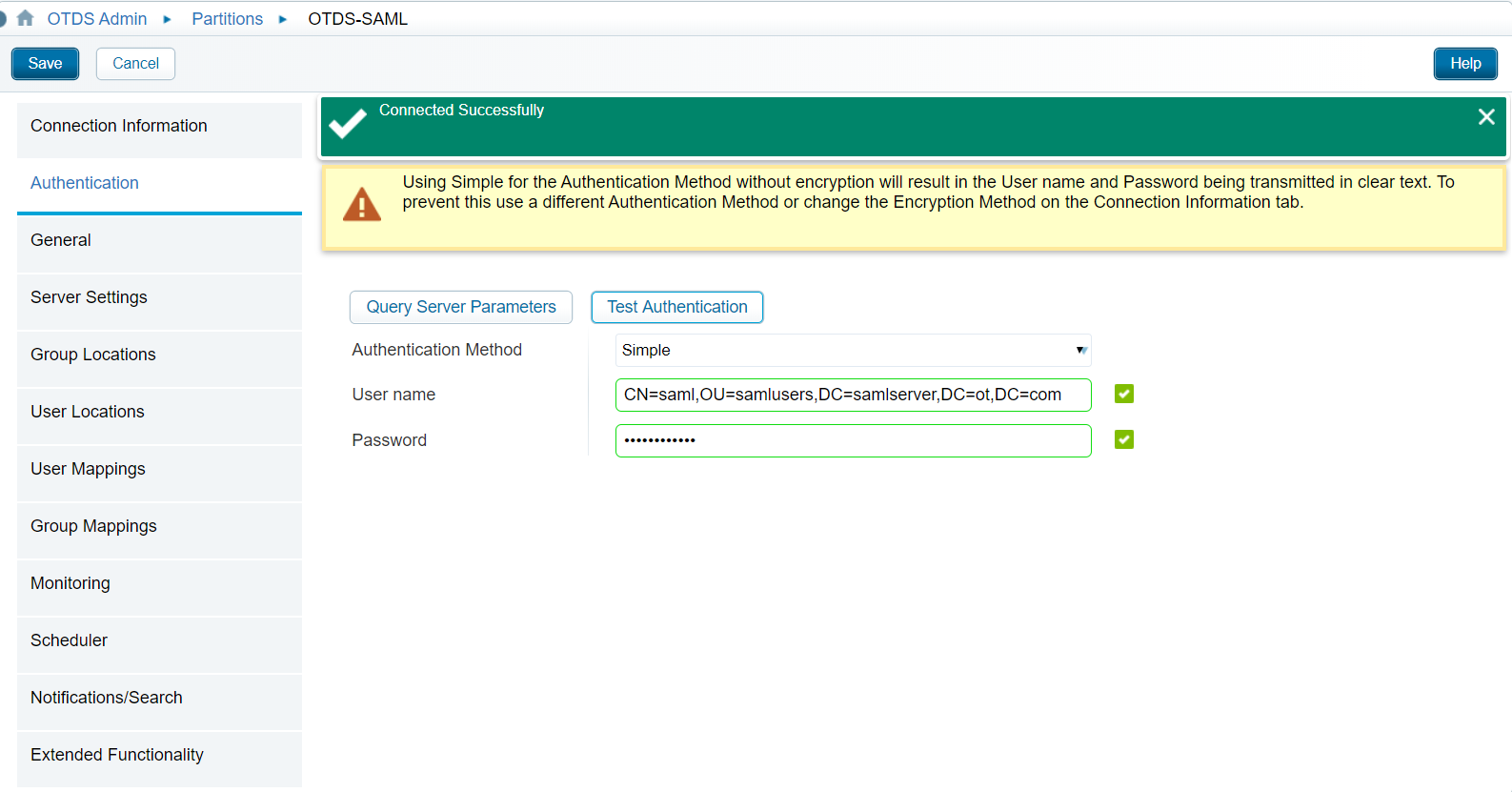
## OTDS Configuration

### 6.1 Create ADFS Partition

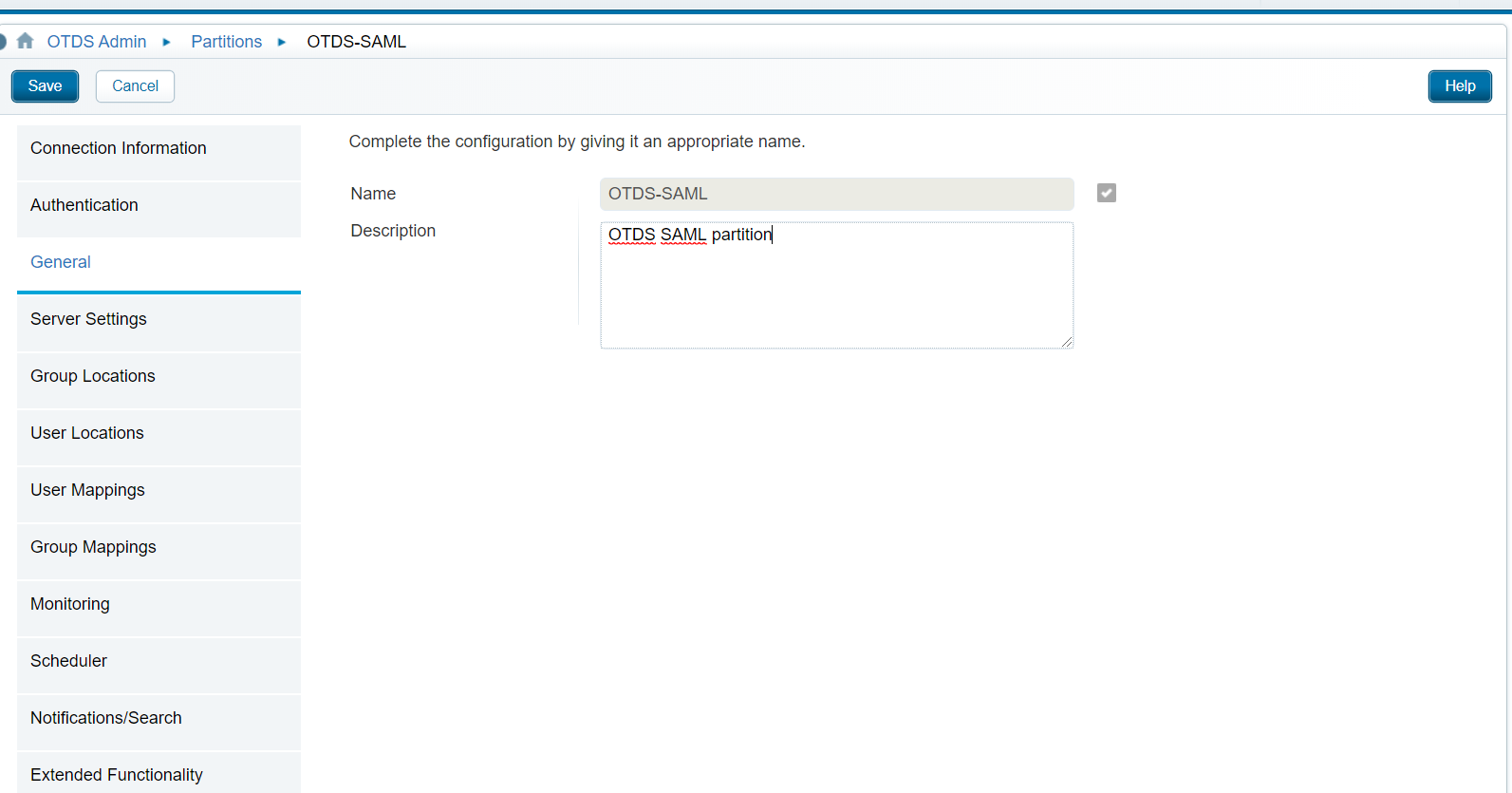
* + Browse OTDS web-client administrator URL
    - http://<*fully\_qualified\_domain\_name\_of\_server*>:<*web\_application\_server\_port\_number*>/otds-admin/
  + Enter login Credentials
  + Click on **Partition** tab and then Click **Add-> New Synchronized User Partition**
  + Enter ADFS **HostName** and select **Encryption method** as **None**
  + Click on **Test Connection** and verify



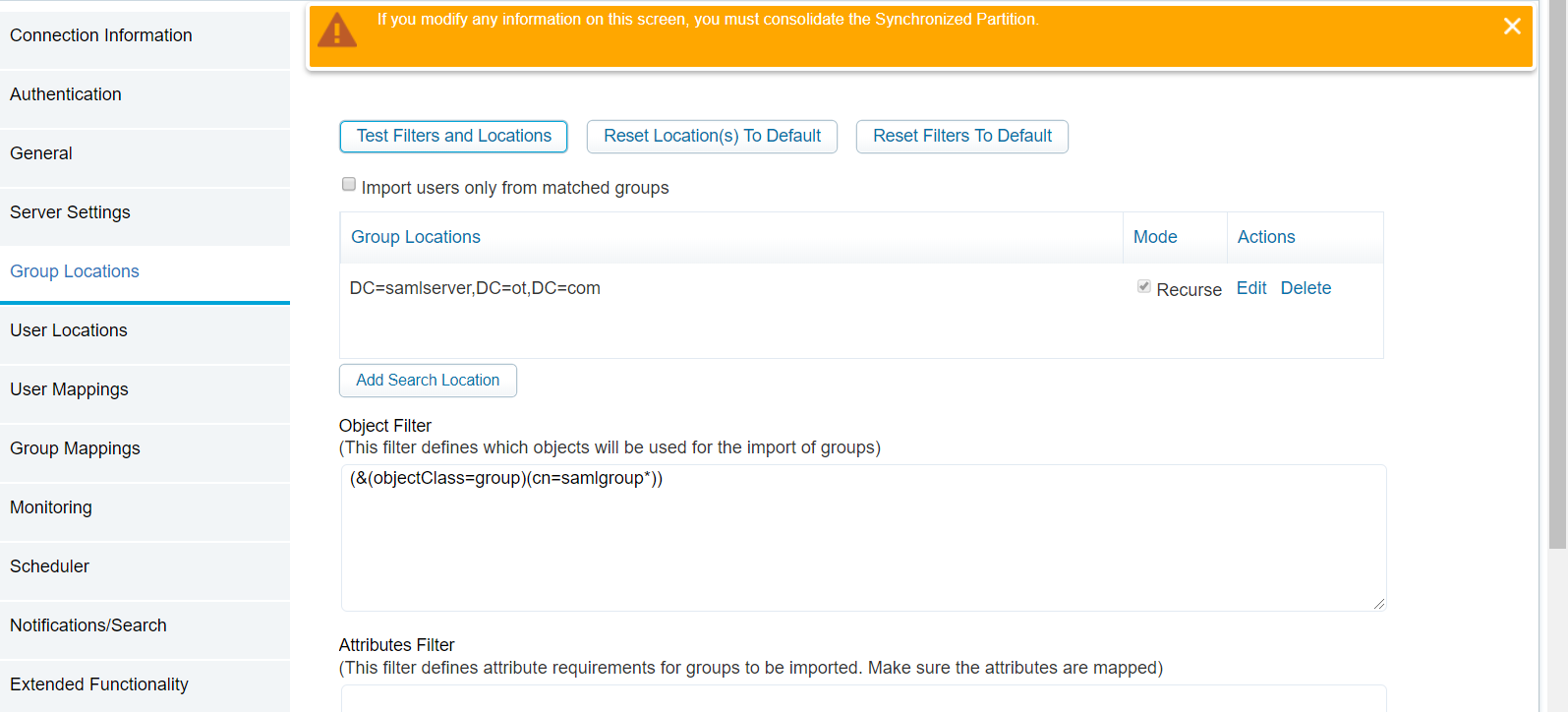
* + Click **Next**
  + Select **Authentication Method** and enter **User Name** and **password** and **Test Authentication**



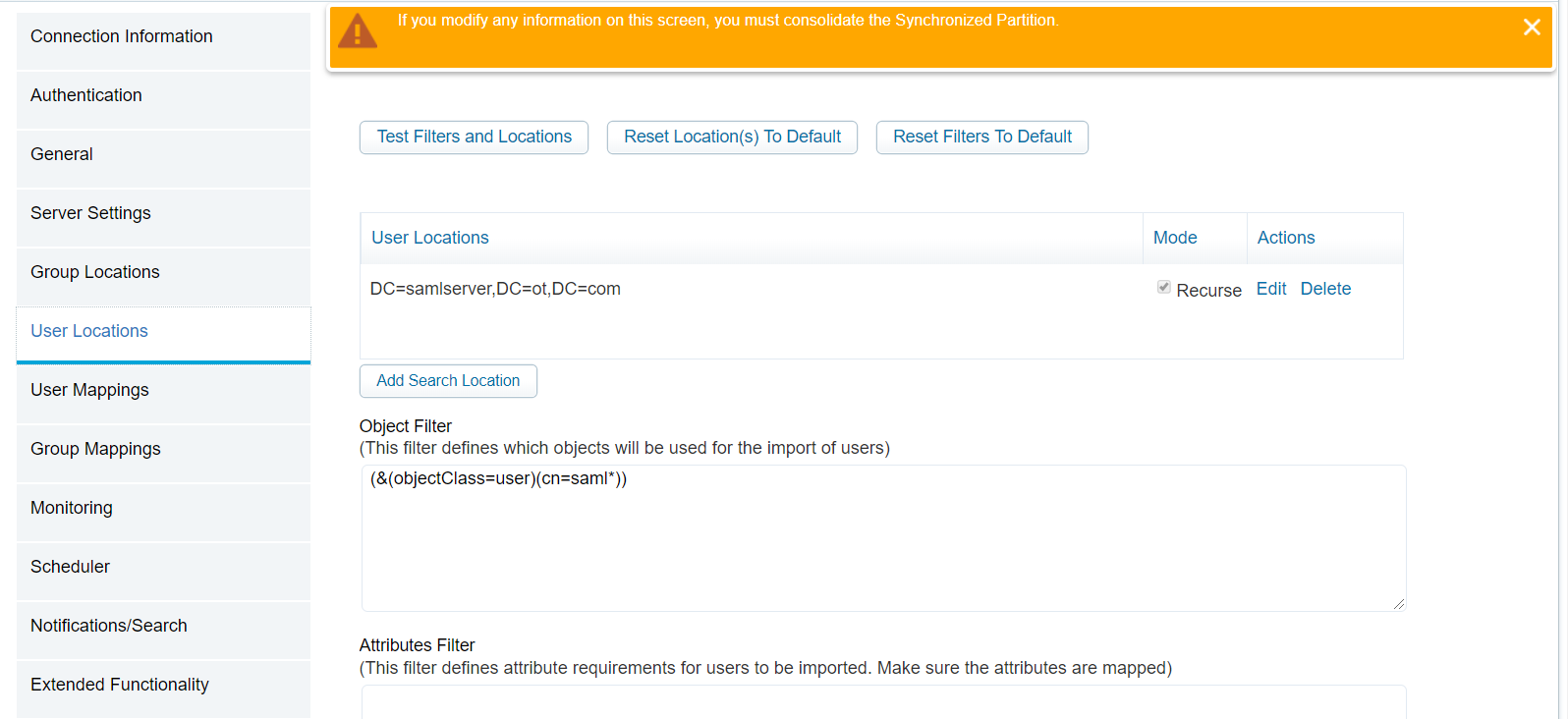
* + Click **Next** and Enter **Name** and **Description** of the partition.



* + Click **Next -> Next** and Enter **Object Filter** in **Group Location**



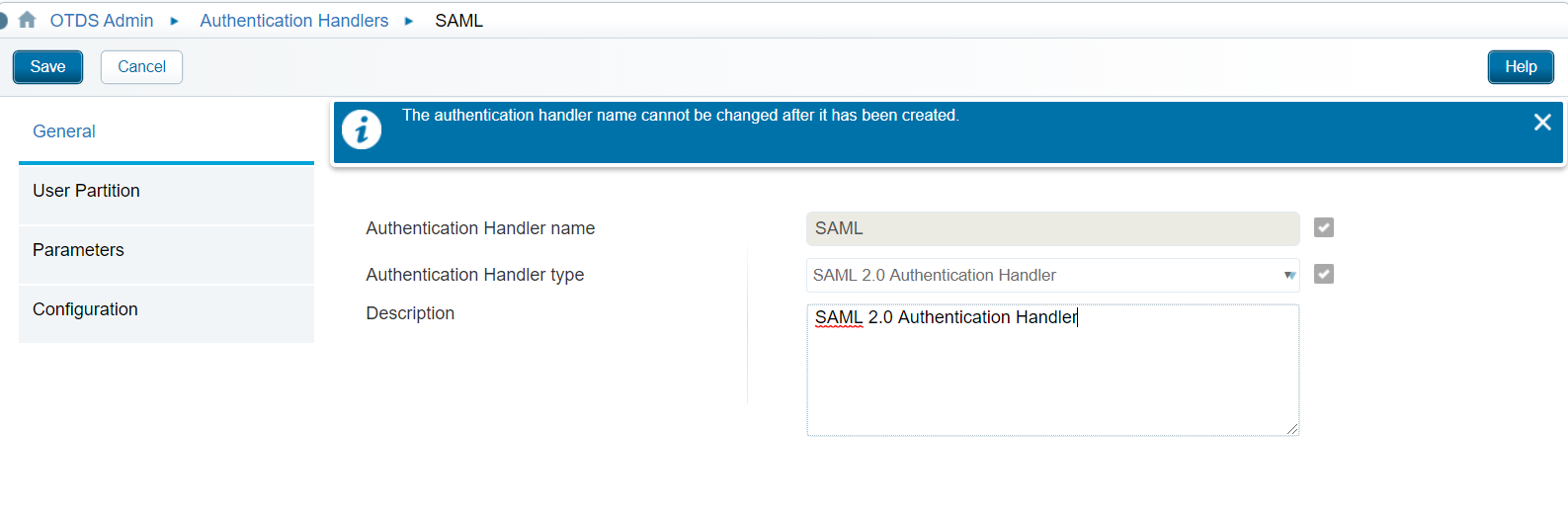
* + Click **Next** and Enter **Object Filter** in **User Location**



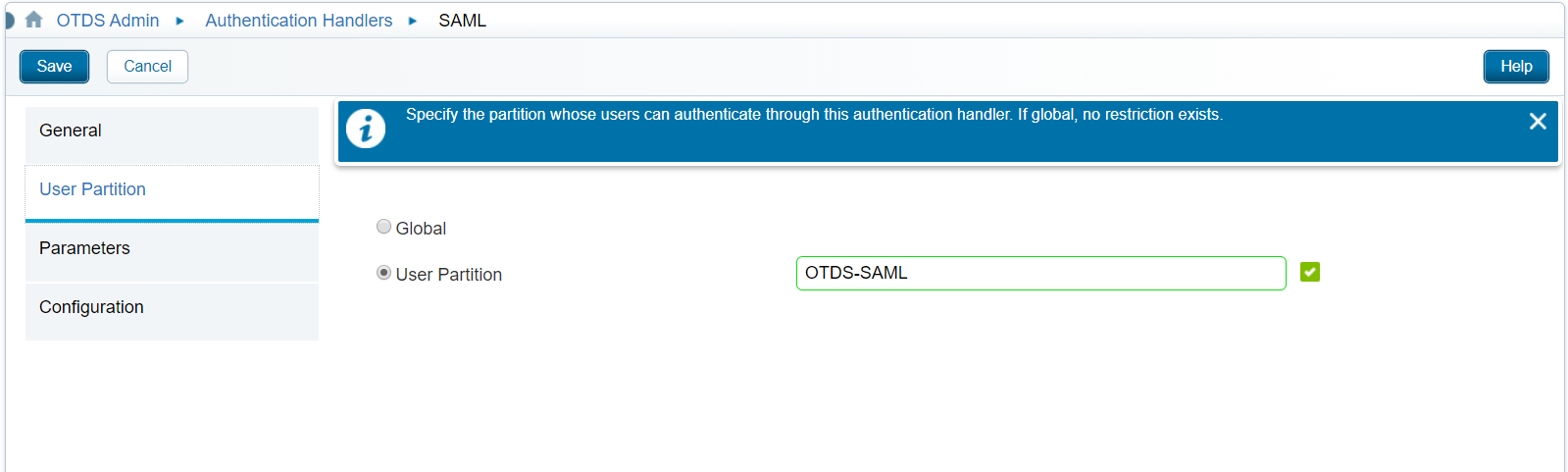
* + Click **Next** and Leave rest as default and then **Save** the partition.

### 6.2 Create SAML Authentication Handler

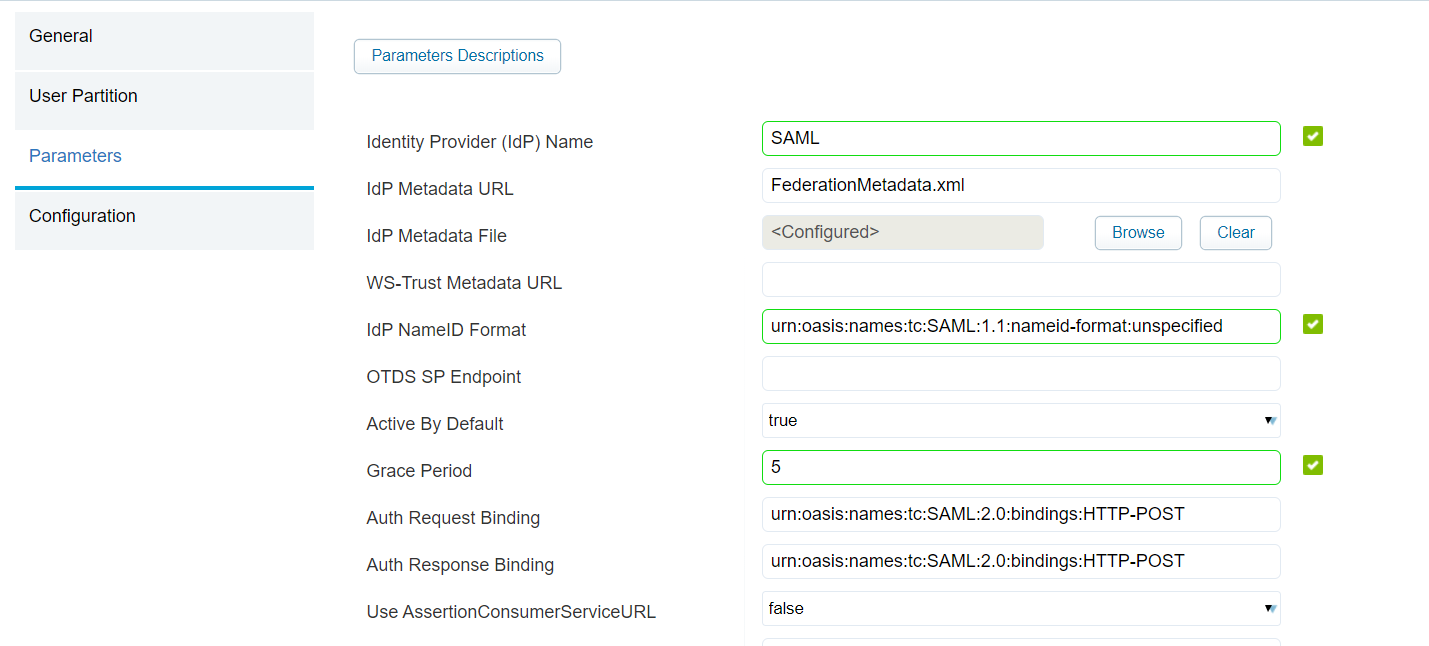
* + Click on **Authentication Handler** tab and Click **Add**
  + Choose **SAML 2.0 Authentication Hander** in **Authentication Handler type**
  + Enter **Authentication Handler name**



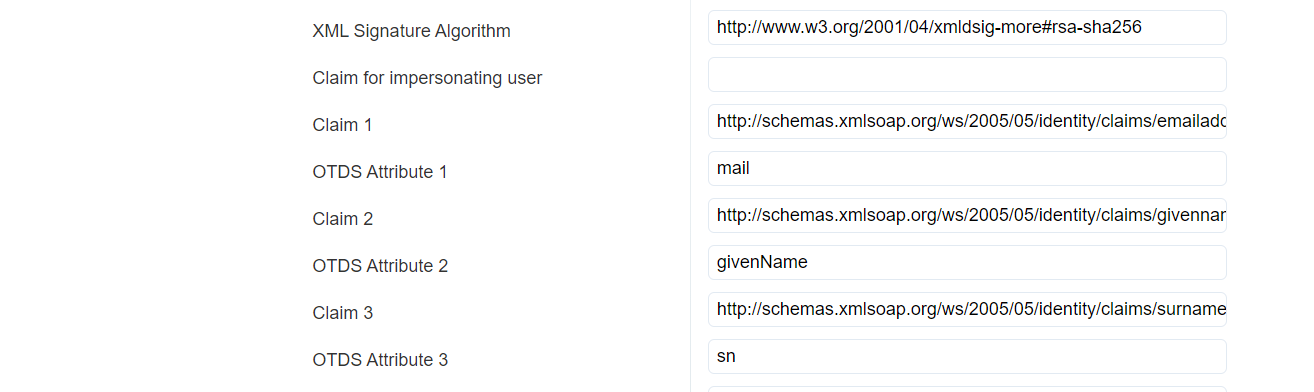
* + Click **Next** and Select ADFS-Partition created earlier as in **User Partition**



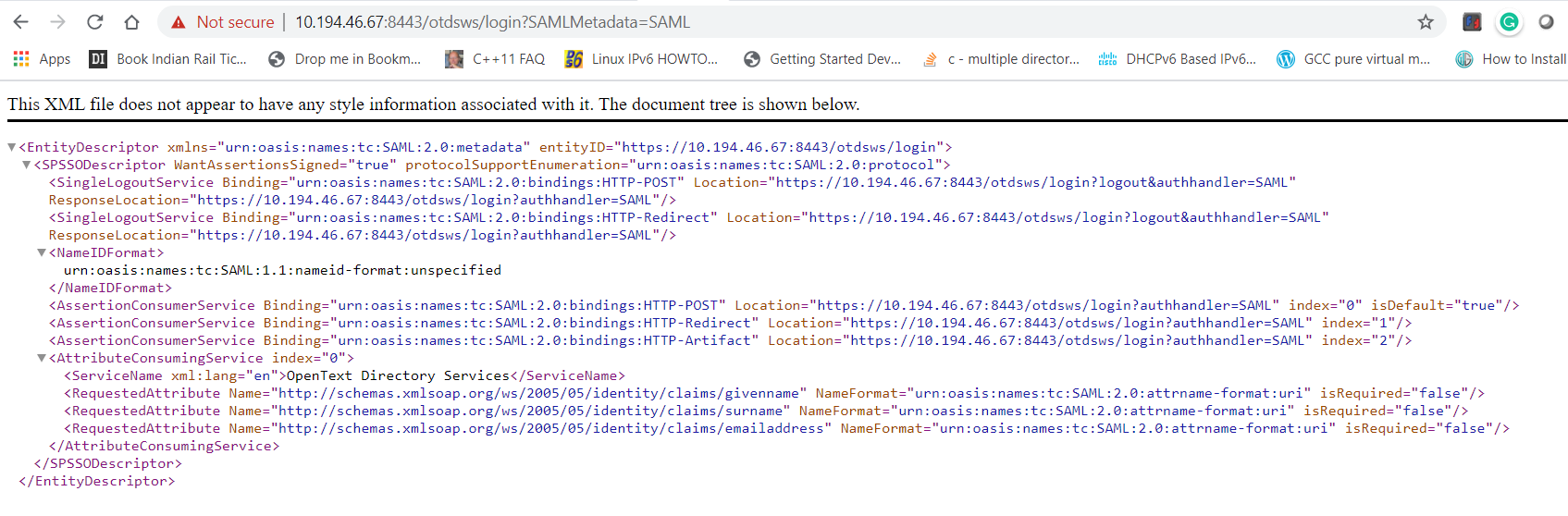
* + Click **Next** and Enter **Parameters** Details
    - Enter **Identity Provider (IdP) Name**
      * Best Practice is to have the Identity Provider (IdP) Name set to the same value as the Authentication Handler name
    - Upload the metadata.xml obtained from the ADFS configuration as the **IdP Metadata File**
      * https://<ADFS\_FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
    - Set **IdP NameID Format** to unspecified as mentioned below:
      * urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    - **OTDS SP Endpoint** is not required for this setup and is typically used for proxy configurations
    - **Active By Default** is true (default) which prevents the user from landing on the OTDS Login page and selecting the Authentication Handler icon.



* + - **XML Signature Algorithm** must set to SHA-256 as mentioned below:
      * <http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>
    - Set Claim 1 through 3 must be set to match the format of the attributes within ADFS claim rule(Refer Image)



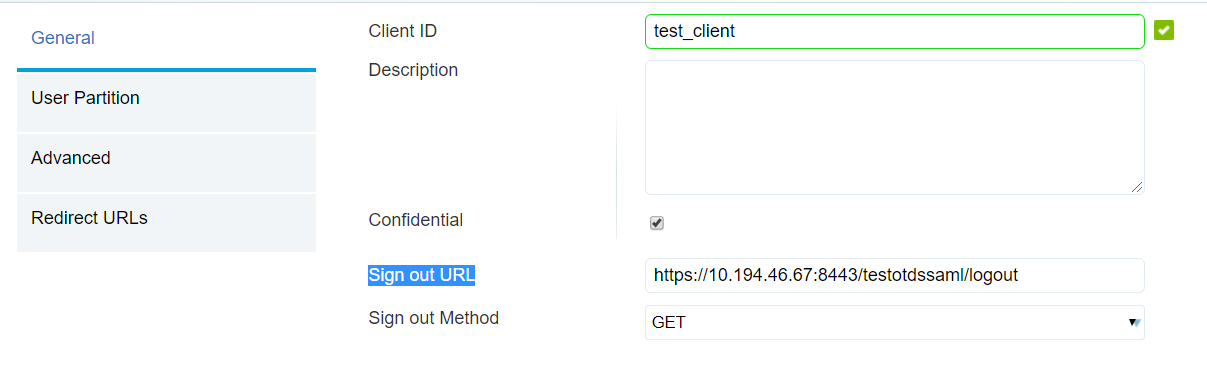
* + Click **Next** and Enter **Configuration** details
    - Add **Authentication principal attribute** is set to **mail**
  + **Save** the Authentication Handler
  + Validate Authentication Handler was successfully created
    - Access the following URL that exports the SP (Service Provider) Metadata
    - https://<otds\_ip>:<otds\_port>/otdsws/login?SAMLMetadata=<saml\_handler\_name>



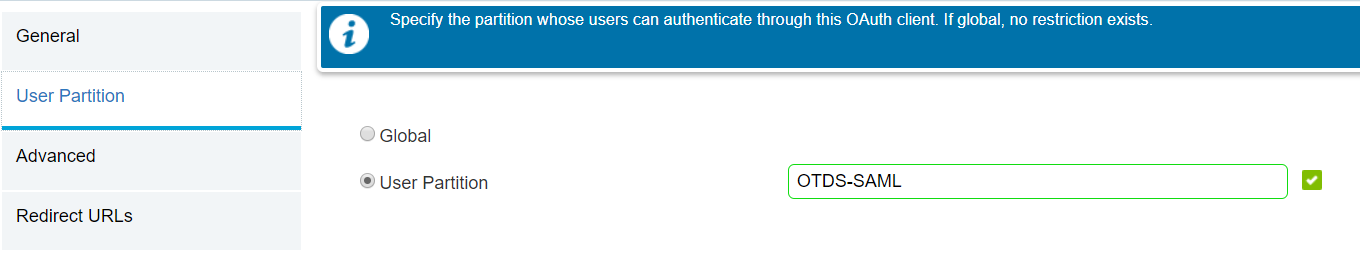
* + - If this URL is blank this means there’s an issue with the configuration of the Authentication Handler
    - Set OTDS logging to DEBUG, attempt to access the URL again and review the otds.log file for errors

### 6.3 Create OAuth Client

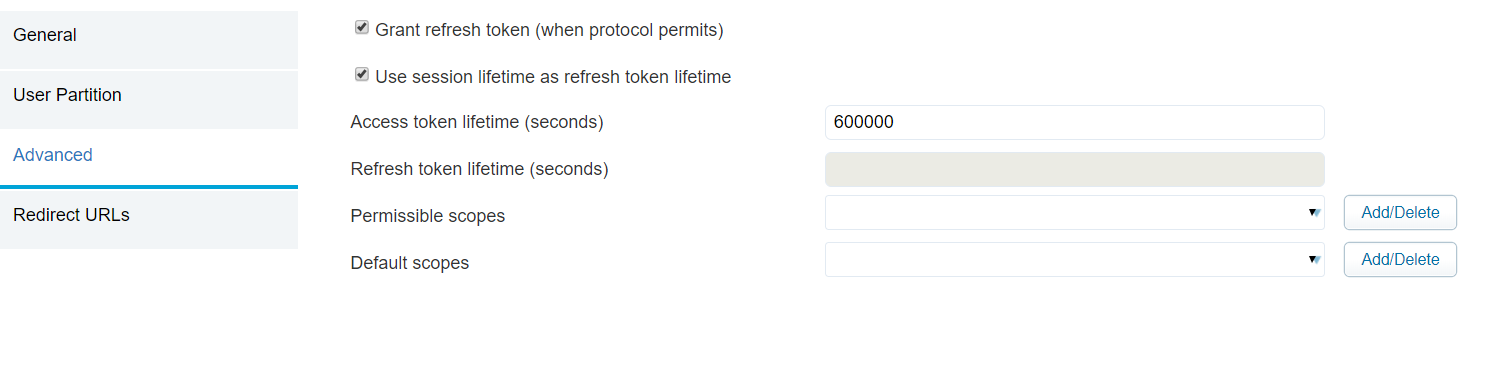
* + Click **OAuth Clients** tab and Click **Add**
  + **General**
    - Enter **Client ID**
    - Enter **Description**
    - Tick mark **Confidential**
    - Enter **Sign out URL**
    - Select **Sign Out Method**



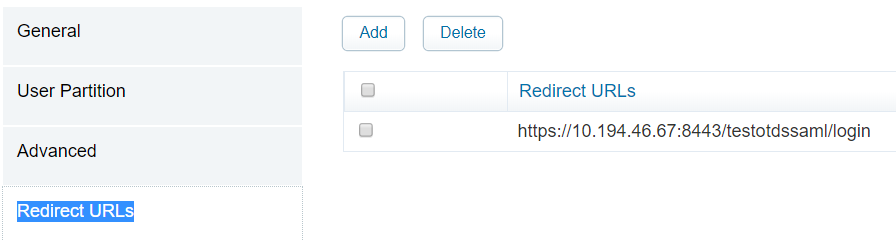
* + **User Partition**
    - Select **User Partition**



* + **Advanced**
    - Enter **Access token lifetime (seconds)**



* + **Redirect URLs**
    - **Add URL**



* + **Save** OAuth Client and note down the client secret.

## Test OAuth Client

### 7.1 OAuth URL

Prepare an URL similar to below

https://<otds\_ip>:<otds\_secure\_port>/otdsws/oauth2/auth?response\_type=token&client\_id=<OAuth\_client\_name>&client\_secret=<OAuth\_client\_secret>&redirect\_uri=<OAuth\_client\_login\_uri>

Eg:

<https://10.194.46.67:8443/otdsws/oauth2/auth?response_type=token&client_id=test_client&client_secret=Gl01RpVb3TTcgmLKMJLuSqUfpJmbG1M5&redirect_uri=https://10.194.46.67:8443/testotdssaml/login>

Browse the URL and see if it’s responded back with access token and login URI in browser address bar.

Eg:

<https://10.194.46.67:8443/testotdssaml/login#access_token=eyJraWQiOiIzZGIwM2E4NTJjMzQ5MDNmMTBjYjEyZGNjYzQ1ZWJkNzFhYWYxYzMzIiwidHlwIjoiSldUIiwiYWxnIjoiUlMyNTYifQ..NJ4JAiu-ZTYLLkgvlxS6u5dIL8zfnzbATve6SNf-_2Xd0kOwOsady5JwhHUL0eq6M8Bz03QBHmuaDjpvlNLFkiDa3rkHsEbN7P6iV353-MHufqIcQCgUAbOg2upuBg2a5tlU1ArrcbaIOGlfVLkCGaYvVyHIha5kKBLiLq9LL7-fp8tLj3uSGi48SI2pEwzZW23kw0jFqrpSwlKi9Y0UEibtzJBnzuZpn7Z5FQ9HnovwjjgMSV-tJX-qE8u8VRYHVLSJMAJOOeWoT6tTDybjaospsxYucAhLZ-pa1jaUKwxn1NIeKUQ-dSYoLz-cBaskmQfr7mnblh8QCBD7Cv5iMw&expires_in=600000>