Syniti Solutions psaAuthenticate

Installation, Configuration & User Guide

BackOffice Associates, LLC, d/b/a Syniti
www.syniti.com
info@syniti.com

Contents

Overview

psaAuthenticate will allow users to authenticate to the Stewardship Tier Single Sign On. It uses any one of the following methods: SAML , OAuth and Active Directory.

Key Features:

- Single place of authentication

Install psaAuthenticate

The application can be installed on Syniti Solutions DSP versions 7.0.1 and above

Download the Application & License

The psaAuthenticate application and/or license are obtained by opening a support ticket at support.syniti.com.

Perform the following steps to retrieve the necessary information for a license request:

1. On the DSP application server, locate the Hardware Identifier program (called **"HardwareIdentifier.exe"**) included in a zip file along with the DSP installation software and documentation previously downloaded from Syniti.
2. Open the program.
3. Click **Generate**.
4. Copy the automatically generated ID and collect the following additional information. All information below pertains to the application server running DSP; no information is needed regarding the database server:
    a. Hardware ID (as mentioned above)
    b. Windows computer name
    c. Number of processor cores (as shown in the Task Manager CPU tab)
    d. Usage of the DSP instance, as in, DEV, TEST (or QA) or PROD
5. Syniti Licensing will deliver the license file via the support ticket.

Install the License

Perform the following steps to install the license:

1. Log in to the DSP site as an Administrator.
2. Select **Admin > Configuration > Product Licenses** in the Navigation pane.
3. Click the Upload a file icon in the **FILE NAME** column next to the Upload a New Product License link.
4. Locate the license file that was provided by Syniti Licensing.

5. Click **Open**.
6. Verify the license is uploaded.
    a. **NOTE**: If the Navigation pane does not display all the licensed components as expected, use the browser refresh button or the F5 key to refresh the screen. At this point the full vertical menu will appear.

Install the Application

Perform the following steps to install the application:

1) Obtain the public certificate from the Identity Provider
2) Right click on **psaAuthenticates.zip** and go to **Properties**. Ensure to unblock the file if it is blocked.
3) Unzip the file
4) Navigate to the DSP Installation folder (e.g. D:\BOA\DSP or C:\Program Files (x86)\BOA\DSP)
5) Back up the DSP Install\BOA\DSP folder to a compressed zip file
6) Back up all Syniti-supplied SQL Server databases or verify that a complete recent backup already exists
    a) Supplied databases: AutoGen, cMap, cMap_Data, cMass, cMass_Data, Console, CranPort, CranSoft, DataConstructionServer, DataDialysis, DataGarage, DBMoto_Client, DGE, DGE_Data, dgReports, dgSAP, dspAddOn, DSPCommon, dspMonitor_AccPak, dspMonitorConfig, DSW, IGC, Integrate, IntegrateStaging, InterfaceServer, MC, & RADToolkit
7) Stop IIS

    This process disconnects all active DSP users, so it is highly recommended to perform the install when no users are on the system. This process stops IIS on the web server.

    a) Open Windows *Start* Menu.
    b) Open the **Command Prompt** (run as an administrator).
    c) Type: **IISReset –stop**.
    d) Press the **Enter** key.
    e) Leave the Command Prompt window open for later use.
8) Stop all services that start with “Cransoft Service …”

    This process stops all DSP background jobs, so it is highly recommended to perform the install when no scheduled operations are running on the system.

    a) Open Windows *Start* Menu.
    b) Select **Administrative Tools**.
    c) Run **Services**.
    d) Right-click the DSP service.

e) Select **Stop**.

f) Repeat the previous two steps for any additional DSP services.

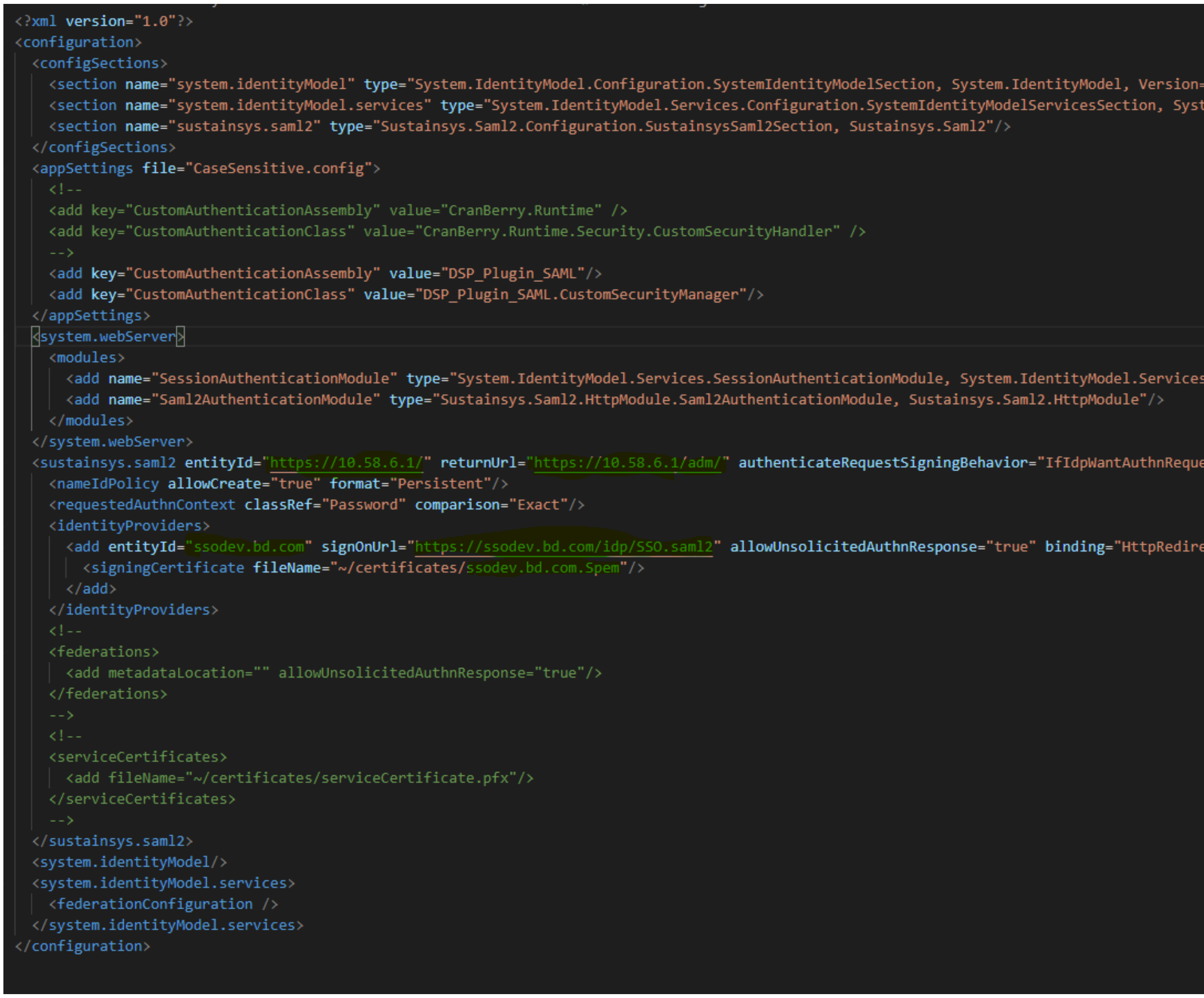
9) Copy the **Web** folder from the zip file to your existing DSP install\Web folder. If prompted, replace the files in the destination.

a) Note: this install comes with 2 additional files: Virtual.SAML.aspx and web.SAML.config.

i) You should backup your original Virtual.aspx file and then rename Virtual.SAML.aspx to Virtual.aspx.

ii) You will have to merge the web.SAML.config with your web.config file. Add the additional XML tags and update any existing ones so your web.config file incorporates the ones from web.SAML.config. You will update the green highlighted sections for your specific installation.

iii)



```
<?xml version="1.0"?>
<configuration>
  <configSections>
    <section name="system.identityModel" type="System.IdentityModel.Configuration.SystemIdentityModelSection, System.IdentityModel, Version=
    <section name="system.identityModel.services" type="System.IdentityModel.Services.Configuration.SystemIdentityModelServicesSection, Syst
    <section name="sustainsys.saml2" type="Sustainsys.Saml2.Configuration.SustainsysSaml2Section, Sustainsys.Saml2"/>
  </configSections>
  <appSettings file="CaseSensitive.config">
    <!--
    <add key="CustomAuthenticationAssembly" value="CranBerry.Runtime" />
    <add key="CustomAuthenticationClass" value="CranBerry.Runtime.Security.CustomSecurityHandler" />
    -->
    <add key="CustomAuthenticationAssembly" value="DSP_Plugin_SAML"/>
    <add key="CustomAuthenticationClass" value="DSP_Plugin_SAML.CustomSecurityManager"/>
  </appSettings>
  <system.webServer>
    <modules>
      <add name="SessionAuthenticationModule" type="System.IdentityModel.Services.SessionAuthenticationModule, System.IdentityModel.Services
      <add name="Saml2AuthenticationModule" type="Sustainsys.Saml2.HttpModule.Saml2AuthenticationModule, Sustainsys.Saml2.HttpModule"/>
    </modules>
  </system.webServer>
  <sustainsys.saml2 entityId="https://10.58.6.1/" returnUrl="https://10.58.6.1/adm/" authenticateRequestSigningBehavior="IfIdpWantAuthnReque
    <nameIdPolicy allowCreate="true" format="Persistent"/>
    <requestedAuthnContext classRef="Password" comparison="Exact"/>
    <identityProviders>
      <add entityId="ssodev.bd.com" signOnUrl="https://ssodev.bd.com/idp/SSO.saml2" allowUnsolicitedAuthnResponse="true" binding="HttpRedire
        <signingCertificate fileName="~/certificates/ssodev.bd.com.Spem"/>
      </add>
    </identityProviders>
    <!--
    <federations>
      <add metadataLocation="" allowUnsolicitedAuthnResponse="true"/>
    </federations>
    -->
    <!--
    <serviceCertificates>
      <add fileName="~/certificates/serviceCertificate.pfx"/>
    </serviceCertificates>
    -->
  </sustainsys.saml2>
  <system.identityModel/>
  <system.identityModel.services>
    <federationConfiguration />
  </system.identityModel.services>
</configuration>
```

10) Copy the **Databases** folder from the zip file to your existing DSP install\Databases folder. If prompted, replace the files in the destination.

11) Navigate to DSP install\Databases and execute file **psaAuthenticate_Install.bat** (run as an administrator)

12) Start all services that start with "Cransoft Service …"

    a) Open Windows *Start* Menu.

    b) Select **Administrative Tools**.

    c) Run **Services**.

    d) Locate the DSP service(s).

    e) Right-click the DSP service.

    f) Select **Start**.

    g) Repeat the previous two steps for any additional DSP services.

13) Start IIS

    a) Open Windows *Start* Menu.

    b) Open the **Command Prompt** (run as an administrator).

    c) Type: **IISReset –start**.

    d) Press the **Enter** key.

Configure psaAuthenticate

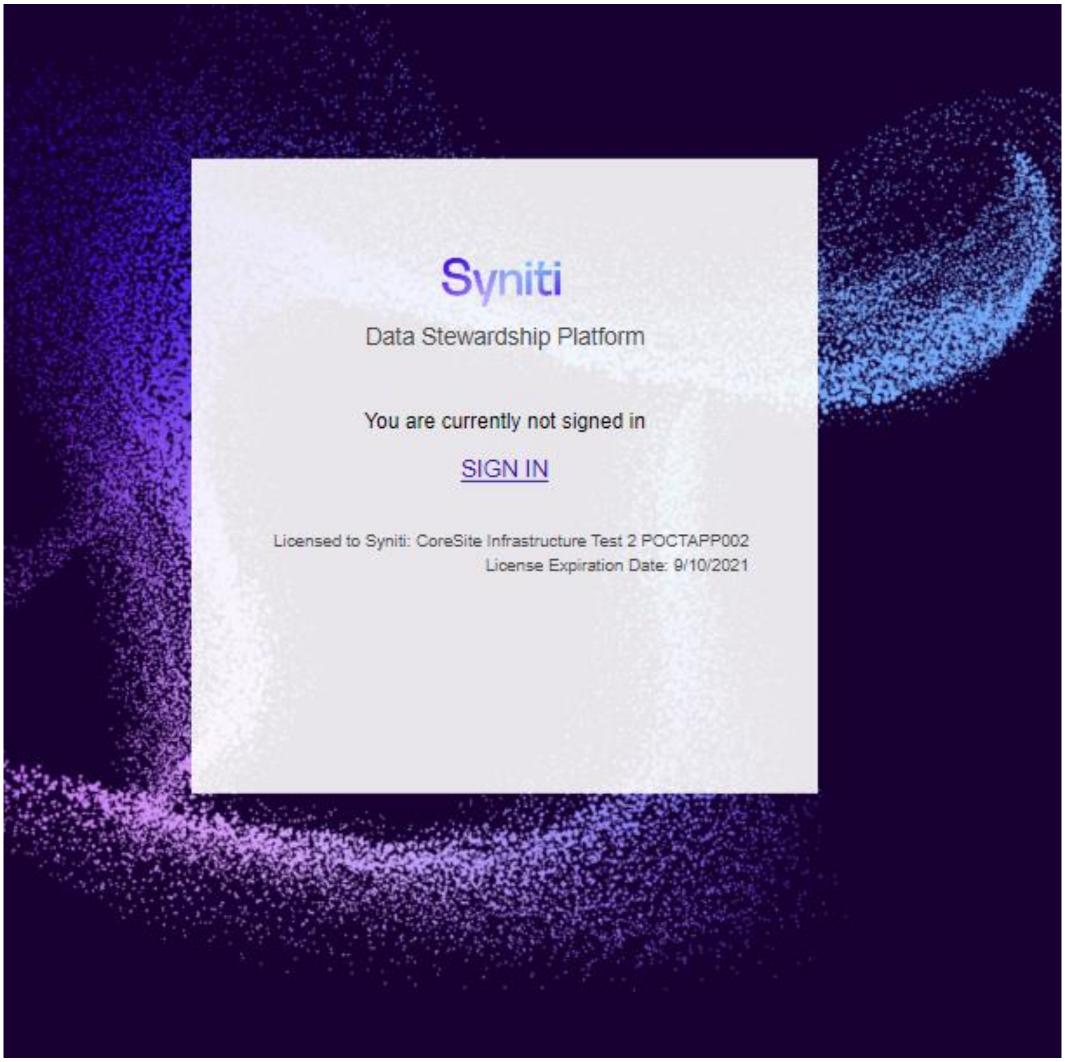
psaAuthenticate comes pre-configured to read from the system it's being installed on. No manual configuration is needed.

If the Navigation pane in DSP doesn't show psaAuthenticate, then try these steps:

1. Log in to the DSP site as an Administrator.
2. Select **Admin > Configuration > Product License** in the Navigation pane.
    a. Ensure that psaAuthenticate appears here.

Login Page

psaAuthenticate allows you to leverage your existing Identity Provider so you can leverage Single Sign On. The traditional Username and Password fields have been removed. To being your session, click “Sign In”. That will redirect you to your Identity Provider login page.

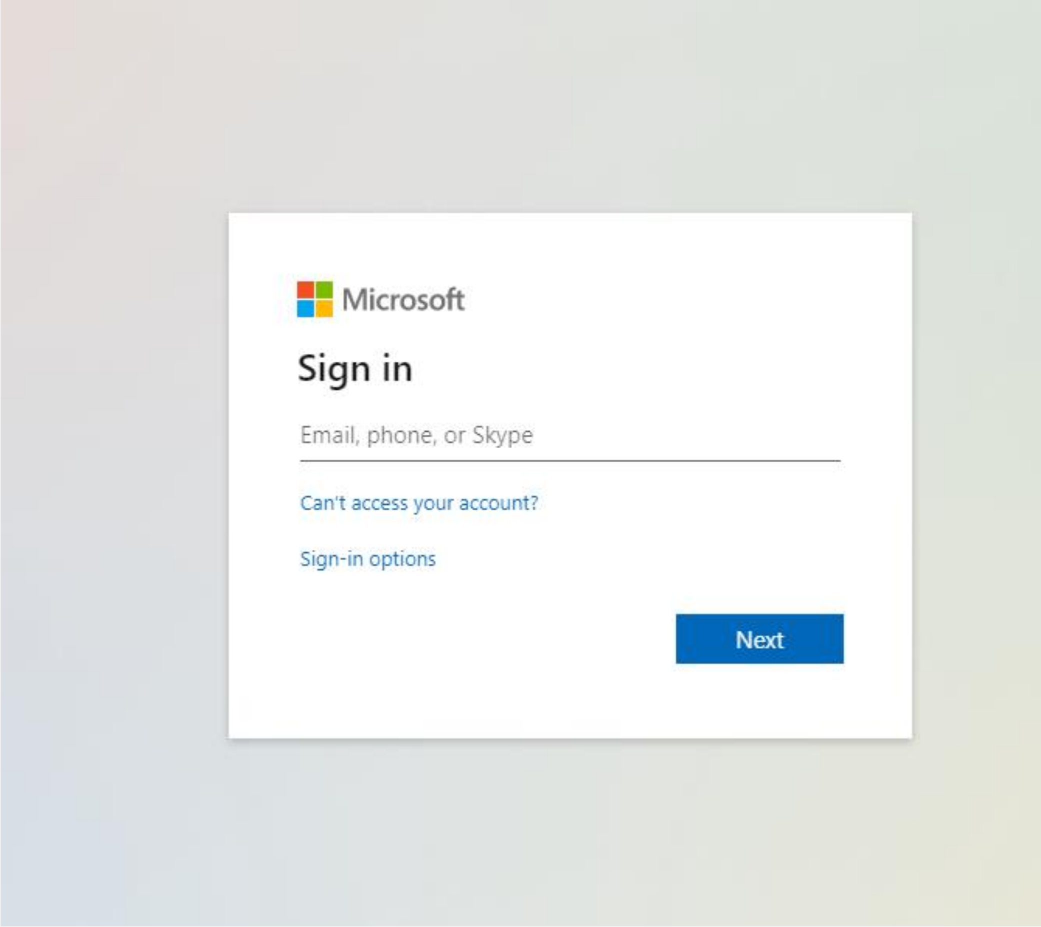

Syniti

Data Stewardship Platform

You are currently not signed in

Licensed to Syniti: CoreSite Infrastructure Test 2 POCTAPP002
License Expiration Date: 9/10/2021

For Azure, the page may look like the following. Your Identity Provider may provide a different page for authenticating.



Microsoft

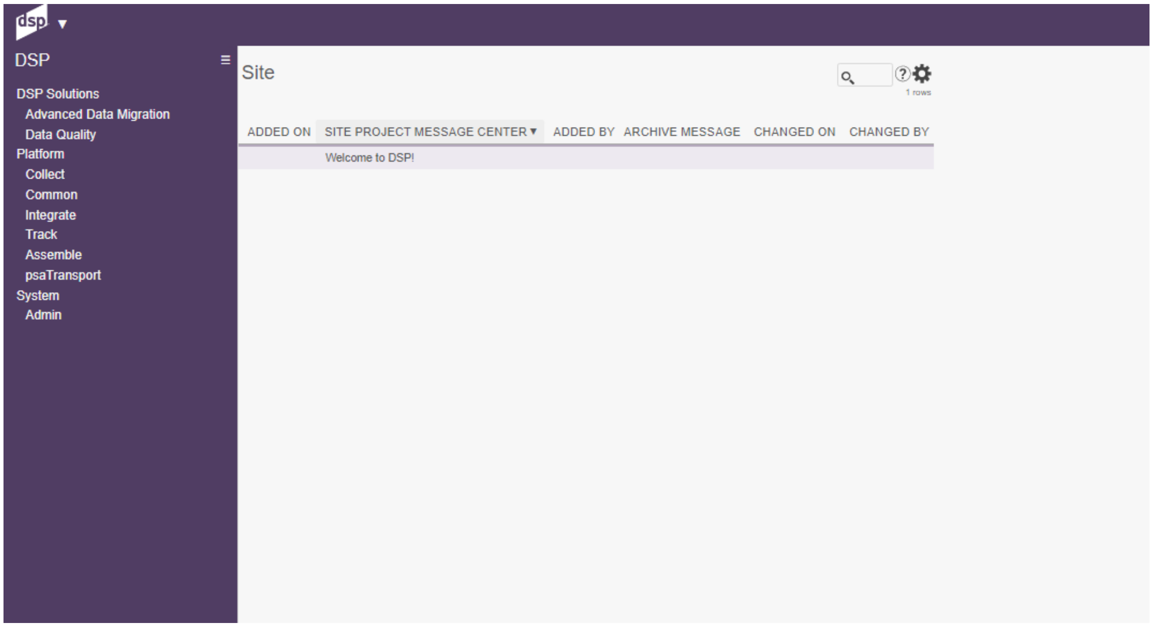
Sign in

Email, phone, or Skype

Can't access your account?

Sign-in options

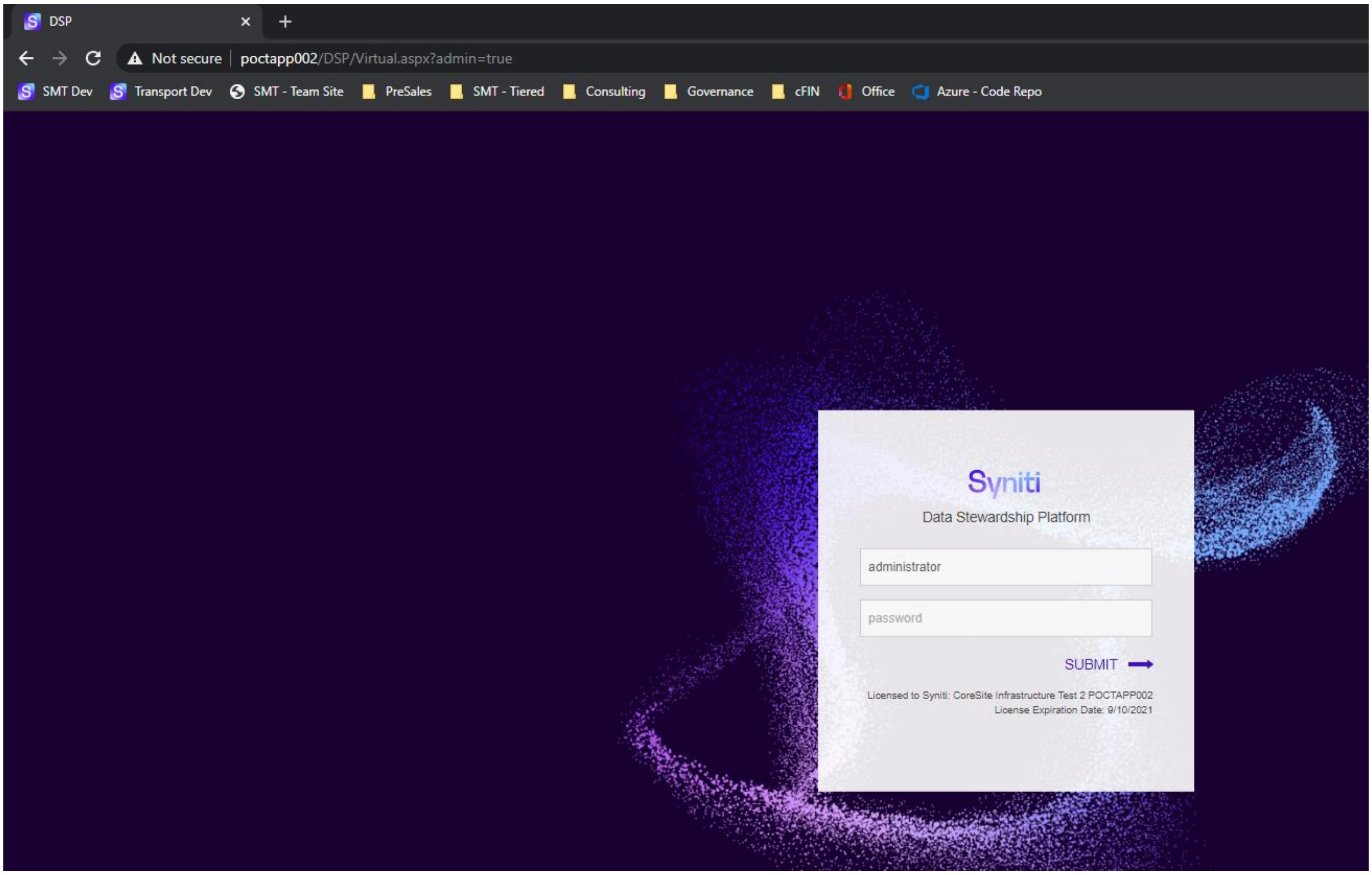
After that – you will be successfully logged into the Stewardship Tier:



ADDED ON	SITE PROJECT MESSAGE CENTER ▾	ADDED BY	ARCHIVE MESSAGE	CHANGED ON	CHANGED BY
	Welcome to DSP!				

Administration Login

If you need to login as the administrator, you can append the url to include ***?admin=true***. That will allow you enter the administration user and password.



Data Stewardship Platform

administrator

password

Licensed to Syniti: CoreSite Infrastructure Test 2 POCTAPP002
License Expiration Date: 9/10/2021

Authentication Error

If you get a message that you are authenticated successfully but are not automatically logged into the Stewardship Tier, you can verify the following:

- Your user has been created successfully in the Stewardship Tier
- The email address in the Stewardship Tier matches the email address provided from the Identity Provider
- The Identity Provider is sending an assertion that contains “email”