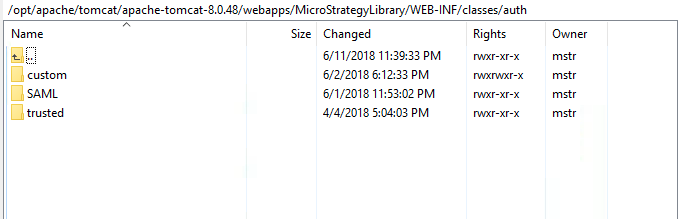
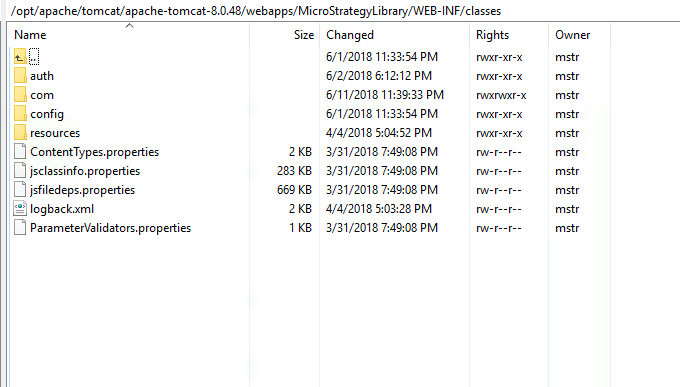
# JWT Integration Sample Deployment Instructions

## Extend the trusted authentication workflow

In order to consume a JWT Token for single sign-on, a customization must be added to the process in charge of handing the Trusted Authentication process.

1. Within the MicroStrategyLibrary web application directory, navigate to **WEB-INF/auth**
2. Add the included **custom** folder package to this directory

Note – This custom folder contains an XML file that instructions MicroStrategyLibrary to leverage a custom class to handle the authentication process for trusted authentication. This class file will be deployed in the next steps.

1. Within the MicroStrategyLibrary web application directory, navigate to **WEB-INF/classes**
2. Add the included **com** folder package to this directory

Note – This com folder contains a sample custom class which was built to parse a JWT token provided as a body parameter to the API request and submit a trusted authentication request using the **sub** parameter within the JWT Token. The source of this class has been provided within the included **src** folder.

## Enable cross domain communication (optional)

If the web application that will be embedding MicroStrategy content lives on a separate domain, the below steps must be performed to enable this communication

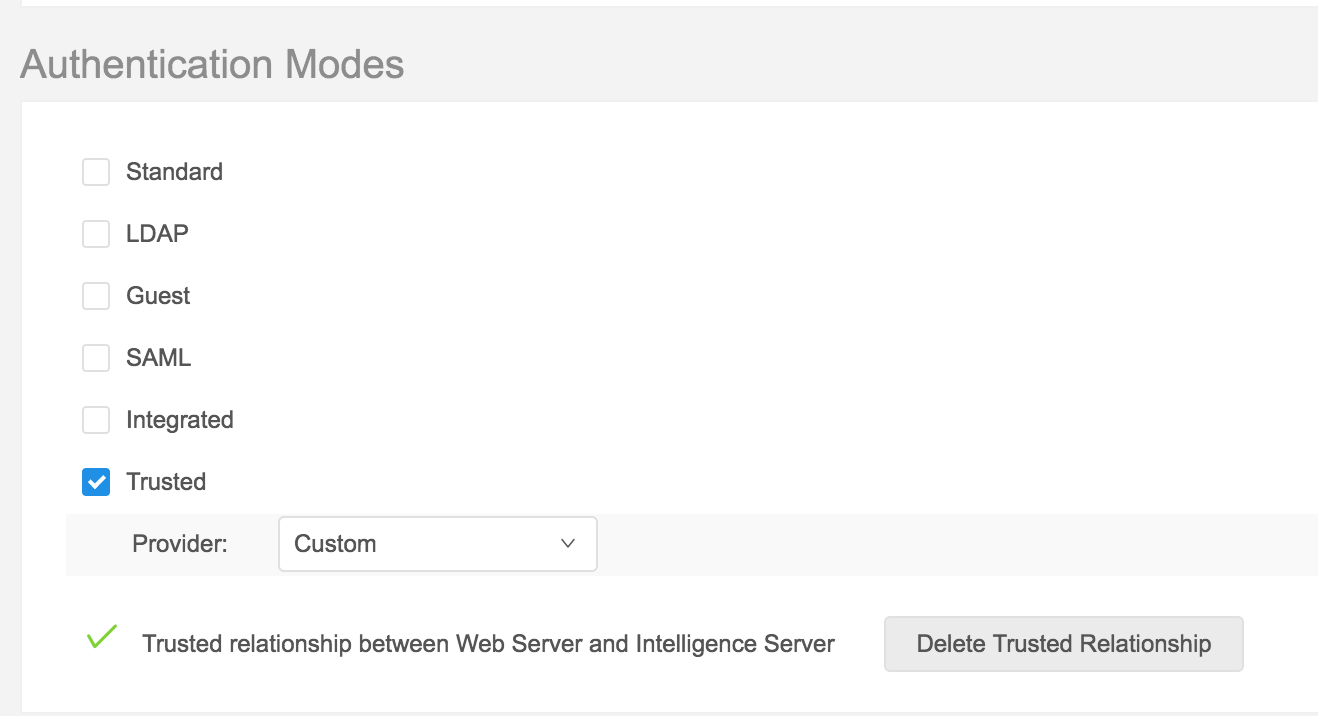
1. Within the MicroStrategyLibrary web application directory, navigate to **WEB-INF/classes/config**
2. Open the file **configOverride.properties**
3. Add the following line to the end of the file:
   1. auth.cors.origins = \*

Note – The \* will allow all domains to attempt to access MicroStrategy Library content – you may restrict this by listing specific domains.

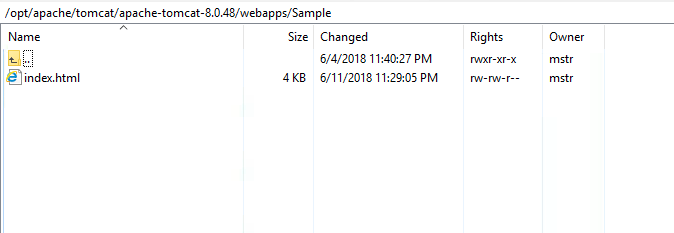
1. Within the MicroStrategyLibrary web application directory, navigate to **WEB-INF/classes/config**
2. Open the file **security\_headers-index.properties**
3. Clear the entire contents of this file and save.

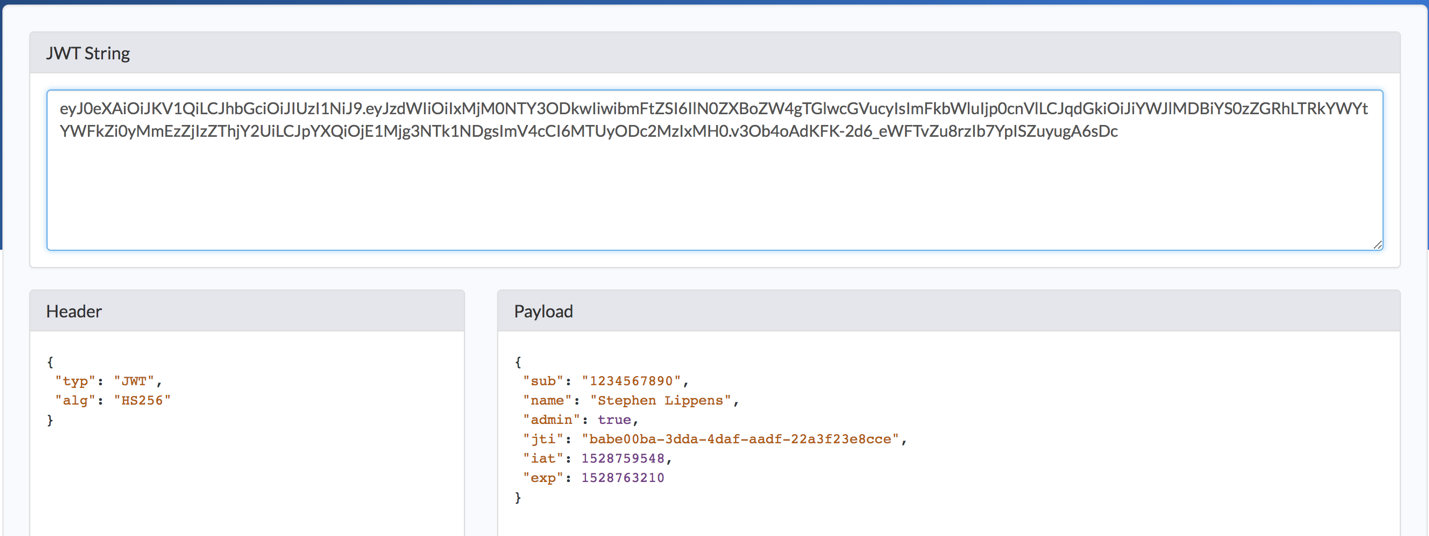
Note – This is required to allow the JSEmbedding api to embed the dossier content across domains.

## Enable Trusted Authentication for MicroStrategy Library

1. Launch the MicroStrategy Library admin page
   1. <https://WEBSERVERNAME/MicroStrategyLibrary/admin/webserver>
2. Check the option for **Trusted** and click **save.** 

## Deploy sample application

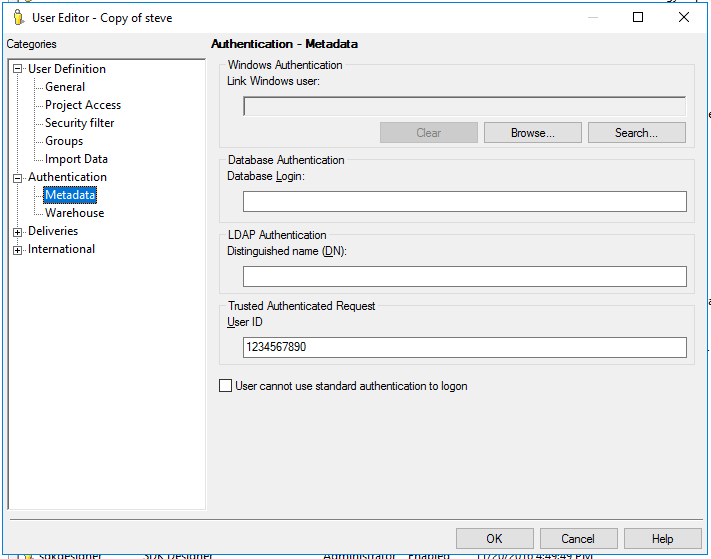
1. Navigate to your webserver and deploy the provided index.html file 
2. Edit the index.html file
3. Alter the configuration parameters on lines 16-25, namely:
   1. Line 16 – Path to the embeddinglib.js in your environment (this is included in the MicroStrategy Library deployment)
   2. Line 19 – URL path to MicroStrategyLibrary
   3. Line 20 – The projectID the user should connect to
   4. Line 21 – The dossierID that should be rendered
   5. Line 25 – The JWT Token that will be used for SSO. A Sample JWT token is provided in the sample with the following definition:



Note – The **sub** value is what the sample expects to be mapped to a MicroStrategy user, which will be done in the next steps.

## Configure MicroStrategy user for Trusted Authentication

1. Open MicroStrategy Developer
2. Edit a user and go to the **Authentication** tab
3. Set the **User ID** that matches the **sub** parameter from the JWT token. The sample value is 1234567890



## Restart the webserver for all changes to take place

1. Restart Webserver

## Run sample index.html file to see the embedded content.

