API Authentication

Contents:

- *Required Permissions*
- *Basic Authentication*
- *SSO Authentication*
- *Kerberos Authentication*
- *Logout*

The Trifacta REST APIs support the following methods of authentication.

> **NOTE:** You must submit authentication credentials with each request to the platform.

Required Permissions

Authenticating user must be a valid user of the deployed instance of the Designer Cloud powered by Trifacta platform .

Basic Authentication

As request parameters, you can submit username/password under Basic Auth to any REST API endpoint.

> **NOTE:** The user must have permissions to execute the endpoint action.

Example:

This example submits authentication requirements over HTTP, including the username and password (`me@example.com:me_pwd`):

```
$ curl  -u me@example.com:me_pwd \
    -b ~/cookies.txt -c ~/cookies.txt \
    http://<platform_host>:<platform_port_number>/v3/<endpoint>
```

where:

Parameter	Description
`-u me@example.com:me_pwd`	Required username and password.
`-b` and `-c`	Required paths and filenames for storage of send and receive HTTP cookies.
`<platform_host>`	Fully qualified name of the host of the Designer Cloud powered by Trifacta platform
`<platform_port_number>`	Port number through which to access the Designer Cloud powered by Trifacta platform . Default is `3005`.

SSO Authentication

In a single-sign on environment, you can use basic authentication to interact with the APIs.

> **NOTE:** Enabling SSO integration with the Designer Cloud powered by Trifacta platform requires additional configuration. See *Configure SSO for AD-LDAP*.

However, some changes are required:

- Basic authentication to the gateway must be enabled as part of the configuration for the reverse proxy. This feature is enabled by default, but please verify that it has not been explicitly disabled in your environment. For more information, see *Configure SSO for AD-LDAP*.
- You must authenticate using the SSO principal as the username and the LDAP or AD password associated with that user.
- You must authenticate to the SSO gateway. In the Designer Cloud powered by Trifacta platform , this value corresponds to the `<platform_host>:<platform_port_number>` value.

Example:

```
$ curl  -u myUser@example.com:foobar -x http://<platform_host>:<platform_port_number> \
    -b ~/cookies.txt -c ~/cookies.txt \
    http://<platform_host>:<platform_port_number>/v3/<endpoint>
```

> **NOTE:** For the protocol identifier, you can also use `https` if SSL is enabled. See *Install SSL Certificate*.

Parameter	Description
`myUser@example.com:foobar`	LDAP principal and password associated with that username.

For more information, see *Configure SSO for AD-LDAP*.

Kerberos Authentication

In a Kerberos environment, credentials must be submitted with each request using the SPNEGO Auth method.

- Kerberos is a network authentication protocol for client/server applications.
- SPNEGO provides a mechanism for extending Kerberos to Web applications through HTTP.
- For more information on the differences, see *https://msdn.microsoft.com/en-us/library/ms995330.aspx#http-sso-2_topic2*.

Credentials are authenticated by the KDC for each request.

> **NOTE:** SPNEGO must be enabled and configured for your REST client or programming library.

Example 1 - Embedded in Java:

SPNEGO requires a custom client. The following SPNEGO client enables submission of URL-based authentication parameters from within Java:
http://docs.oracle.com/javase/6/docs/technotes/guides/security/jgss/lab/part5.html

Example 2 - Using cURL:

To use cURL:

1. Verify that your version of cURL supports GSS:

```
$ curl -V
curl 7.51.0 (x86_64-apple-darwin16.0) libcurl/7.51.0 SecureTransport zlib/1.2.8
Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtsp smb smbs smtp
smtps telnet tftp
Features: AsynchDNS IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz UnixSockets
```

2. Verify that `GSS-API` and `SPNEGO` are in the output.
3. Run `kinit` and authenticate using the hadoop principal:

```
$ kinit
Please enter the password for [hadoop.user.principal]@localhost:
$
```

4. Access using cURL:

```
$ curl --negotiate -u anything \
    -b ~/cookies.txt -c ~/cookies.txt \
    http://<platform_host>:<platform_port_number>/v3/<endpoint>
```

   where:

Parameter	Description
`--negotiate`	Enables SPNEGO use in cURL. This option requires a library built with GSS-API or SSPI support. If this option is used several times, only the first one is used. Use `--proxy-negotiate` to enable Negotiate (SPNEGO) for proxy authentication.
`-u anything`	Required username. However, this username is ignored. Instead, the principal used in `kinit` is applied.

For more information:

- *https://hadoop.apache.org/docs/r2.7.3/hadoop-auth/Examples.html*
- *https://msdn.microsoft.com/en-us/library/ms995329.aspx*

Logout

Since each request requires credentials, logging out is not required.