Title: Web Connectors 2.0.1 and users' management

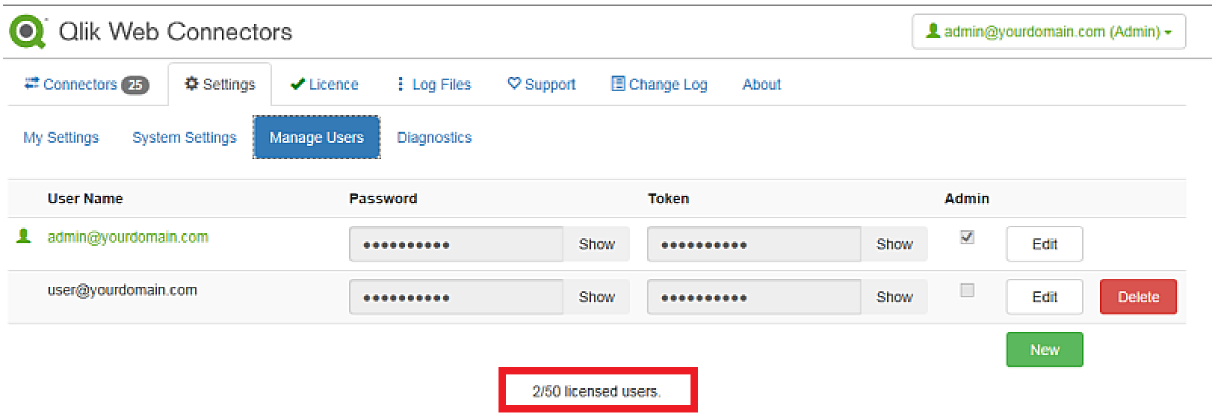
IT or server admins can use the Web Connectors 2.0.1 web interface to manage who can use this application. Hence selected users in Qlik Web Connectors 2.0.1 can log in after they are granted permissions to work with such Connectors and generate QlikView or Qlik Sense load scripts.

Description:

In some scenarios, the IT or server Admins want to manage or restrict the usage of Web Connectors by allowing only a number of users to access the Web Connectors, generate the load scripts and be able to use them in their Qlik Sense or Qlik View applications for pulling data from different data-sources.

Managing users in the Web Connectors enables us to manage the licenses designation per users. At the bottom of the Web Connectors interface, we can see how many users the current Web Connectors license permits and how many of these have been used so far (see image below).

If you did the Web Connectors configuration correctly, then you should be able to see "Manage Users" option under Settings next time you start it.



User Name	Password	Token	Admin		
admin@yourdomain.com	●●●●●●●●●● Show	●●●●●●●●●● Show	☑	Edit	
user@yourdomain.com	●●●●●●●●●● Show	●●●●●●●●●● Show	□	Edit	Delete

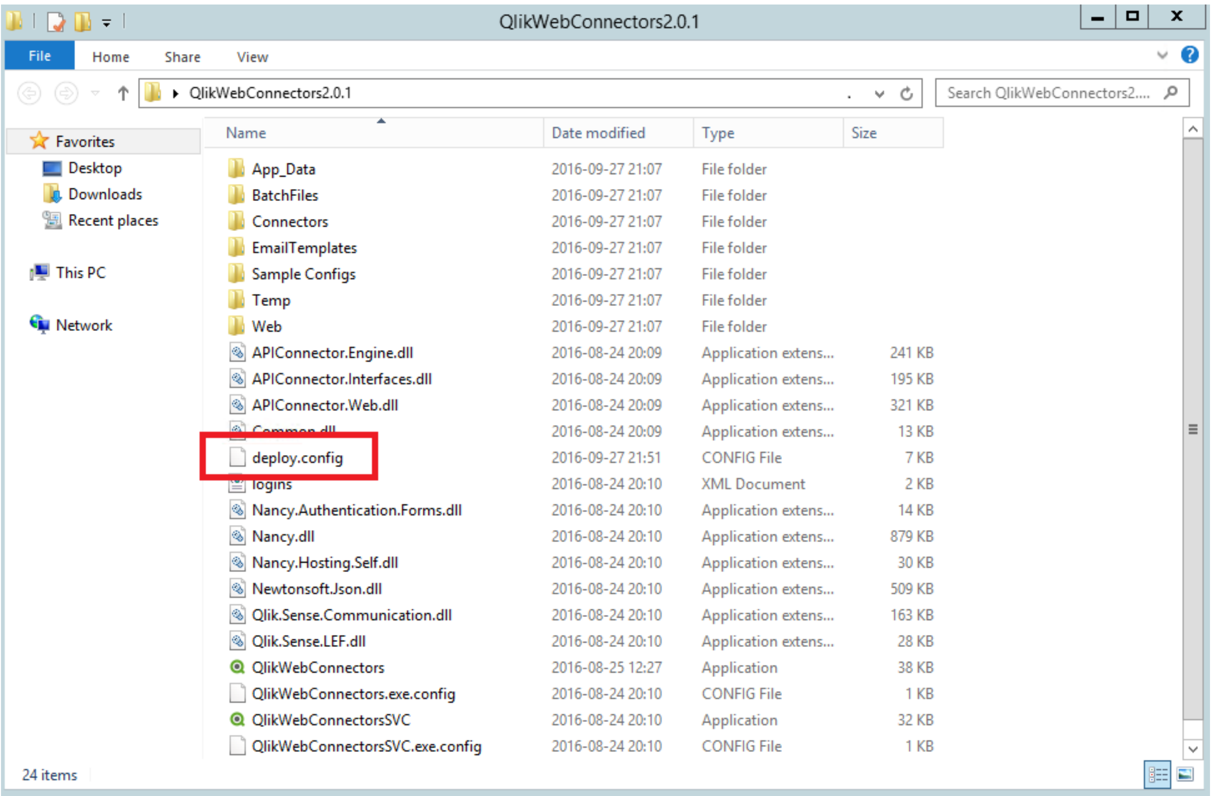
2/50 licensed users.

Note also in the above added users, those accounts have User name, Passwords and Tokens. The question that may also raise how all this fit together in the "Manage Users" section of the Web Connectors?

Resolution:

To enable the "Manage Users" option under Settings in the Web Connectors, you need to follow these steps:

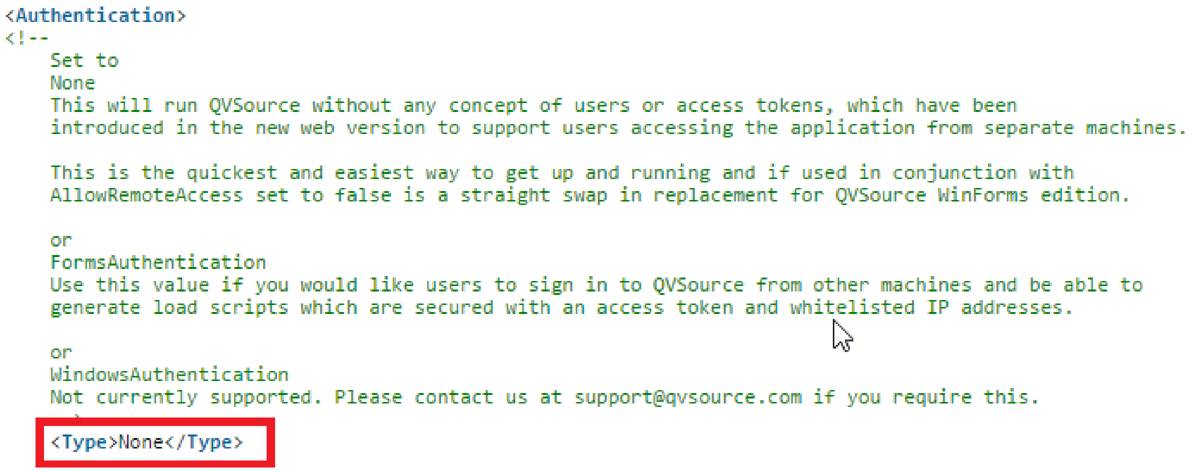
- You have the Web Connectors 2.0.1 zip file downloaded from qlik.com, extract it and test first with the exe file. You can start the web interface for using the Web Connectors – double click on QlikWebConnectors.exe.
- Close the Web Connectors interface and the associated running process (the web interface and the QlikWebConnectors.exe started from the previous step).
- Go to the folder where you extracted the zip file and allocate deploy.config.



Name	Date modified	Type	Size
App_Data	2016-09-27 21:07	File folder	
BatchFiles	2016-09-27 21:07	File folder	
Connectors	2016-09-27 21:07	File folder	
EmailTemplates	2016-09-27 21:07	File folder	
Sample Configs	2016-09-27 21:07	File folder	
Temp	2016-09-27 21:07	File folder	
Web	2016-09-27 21:07	File folder	
APIConnector.Engine.dll	2016-08-24 20:09	Application extens...	241 KB
APIConnector.Interfaces.dll	2016-08-24 20:09	Application extens...	195 KB
APIConnector.Web.dll	2016-08-24 20:09	Application extens...	321 KB
Common.dll	2016-08-24 20:09	Application extens...	13 KB
deploy.config	2016-09-27 21:51	CONFIG File	7 KB
logins	2016-08-24 20:10	XML Document	2 KB
Nancy.Authentication.Forms.dll	2016-08-24 20:10	Application extens...	14 KB
Nancy.dll	2016-08-24 20:10	Application extens...	879 KB
Nancy.Hosting.Self.dll	2016-08-24 20:10	Application extens...	30 KB
Newtonsoft.Json.dll	2016-08-24 20:10	Application extens...	509 KB
Qlik.Sense.Communication.dll	2016-08-24 20:10	Application extens...	163 KB
Qlik.Sense.LEF.dll	2016-08-24 20:10	Application extens...	28 KB
QlikWebConnectors	2016-08-25 12:27	Application	38 KB
QlikWebConnectors.exe.config	2016-08-24 20:10	CONFIG File	1 KB
QlikWebConnectorsSVC	2016-08-24 20:10	Application	32 KB
QlikWebConnectorsSVC.exe.config	2016-08-24 20:10	CONFIG File	1 KB

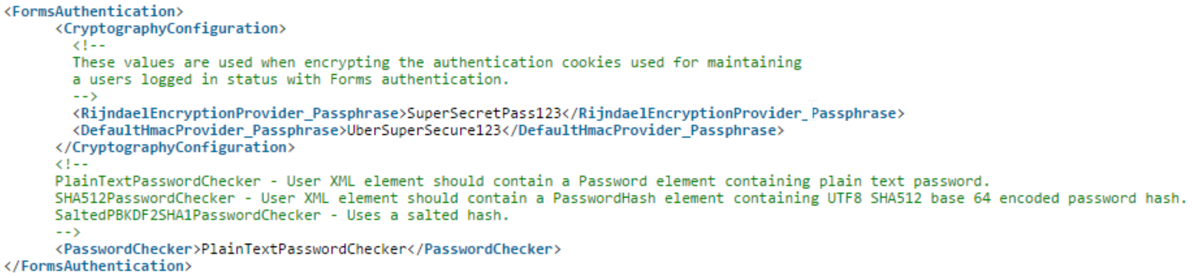
24 items

- Open deploy.config in a text editor and allocate the following section:



```
<Authentication>
<!--
    Set to
    None
    This will run QVSource without any concept of users or access tokens, which have been
    introduced in the new web version to support users accessing the application from separate machines.

    This is the quickest and easiest way to get up and running and if used in conjunction with
    AllowRemoteAccess set to false is a straight swap in replacement for QVSource WinForms edition.

    or
    FormsAuthentication
    Use this value if you would like users to sign in to QVSource from other machines and be able to
    generate load scripts which are secured with an access token and whitelisted IP addresses.

    or
    WindowsAuthentication
    Not currently supported. Please contact us at support@qvsource.com if you require this.

    <Type>None</Type>
```

- Change <Type>None</Type> to <Type> FormsAuthentication</Type>
- Note that according to the former QvSource documents “None” and “FormsAuthentication” are the only supported modes at the moment. While “WindowsAuthentication” is not supported.
- By setting the value of “FormsAuthentication” the following sections become relevant:



```
<FormsAuthentication>
      <CryptographyConfiguration>
        <!--
        These values are used when encrypting the authentication cookies used for maintaining
        a users logged in status with Forms authentication.
        -->
        <RijndaelEncryptionProvider_Passphrase>SuperSecretPass123</RijndaelEncryptionProvider_Passphrase>
        <DefaultHmacProvider_Passphrase>UberSuperSecure123</DefaultHmacProvider_Passphrase>
      </CryptographyConfiguration>
      <!--
      PlainTextPasswordChecker - User XML element should contain a Password element containing plain text password.
      SHA512PasswordChecker - User XML element should contain a PasswordHash element containing UTF8 SHA512 base 64 encoded password hash.
      SaltedPBKDF2SHA1PasswordChecker - Uses a salted hash.
      -->
      <PasswordChecker>PlainTextPasswordChecker</PasswordChecker>
</FormsAuthentication>
```

And

```
<FormsUsers provider="FileBasedFormsUsersProvider" config="{app_root}/logins.xml"></FormsUsers>
```

- You can also enable “Manage Users” by copying the deploy.config and logins.xml files from the “Sample Configs\Forms Auth and Remote Access” directory. This sets Web Connectors up with two users.
- Once you have copied these into the QVSource root directory you should be able to log-in with either:
  - admin@yourdomain.com
  - password01
  - Or: user@yourdomain.com
  - password01
- The first user has admin privileges. You can also edit the element in logins.xml first to be your own username or email address.
- Once logged in as Admin, you can go to the user management screen to add or edit users.
- For local network access (a user accessing the server locally for example), it is enough to start the QlikWebConnectors.exe on the server, then from the other machine the user type in the browser the full **HTTP** URL containing the host machine name, the port number, by default it is 5555, can be changed to something else if needed in the deploy.config.

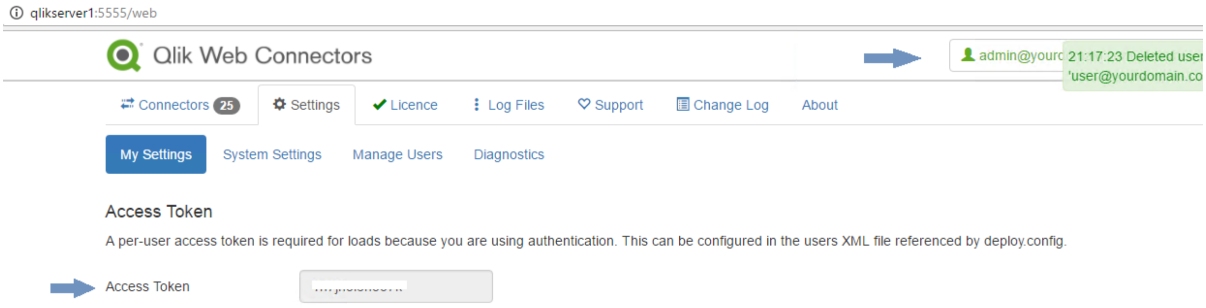
  Example of a working URL tested on my machine:

  http://qlikserver1:5555/web

  Where qlikserver1 is the name of the host machine.
- For more information on this topic especially for people wanting to enable out of the local network access using SSL, then you are welcome to have a look on this page http://wiki.qvsource.com/Running-Over-SSL.ashx
- The Qlik online help documents with more details on the topic: https://help.qlik.com/en-US/connectors/Subsystems/Web_Connectors_help/Content/2.0/Configuration/Advanced-configuration.htm#Authentication

Web connectors and tokens

When “FormsAuthentication” is enabled in the deploy.config file, users will be able to sign-in to the Web Connectors from other machines and create load scripts which are secured with an access token. This token is generated automatically the first time for the Admin user.



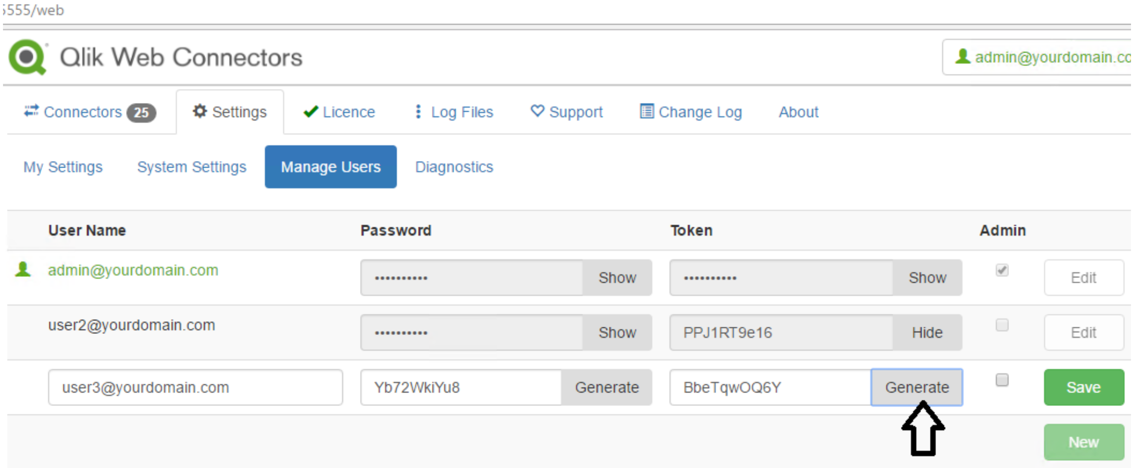
21:17:23 Deleted user 'user@yourdomain.co

Access Token

A per-user access token is required for loads because you are using authentication. This can be configured in the users XML file referenced by deploy.config.

Access Token [redacted]

Then it is manually generated by the Admin for any new added user. Most of the time users are in this case developers working with the load scripts within a given organization or company.



User Name	Password	Token	Admin	
admin@yourdomain.com	•••••••••• Show	•••••••••• Show	☑	Edit
user2@yourdomain.com	•••••••••• Show	PPJ1RT9e16 Hide	□	Edit
user3@yourdomain.com	Yb72WkiYu8 Generate	BbeTqwOQ6Y Generate	□	Save
				New

Each user added to the Web Connectors will have his/her own specific token, you may call it also a key which in turn will be embedded in the generated load script “specifically the URL of the HTTP request”, as in the following example where we tried to connect to JIRA REST API.

```
http://qlikserver1:5555/data?connectorID=WebConnector&table=JsonToXmlRaw&ur
l=https%3a%2f%2fjira.qlikdev.com%2frest%2fapi%2f2%2fsearch%3fjql%3dproject%
2520in%2520(%2522NPrinting%252016%2522%252C%2520%2522Qlik%2520NPrinting%252
2%252C%2520%2522Qlik%2520for%2520iOS%2522%252C%2520%2522Qlik%2520Sense%2520
Cloud%2522%252C%2520QlikView%252C%2520%2522QlikView%252011.20%2522%252C%252
0%2522QVX%2520Configurable%2520Rest%2520Connector%2522%252C%2520Sense)%2520
AND%2520issuetype%2520%253D%2520Bug%2520and%2520status%2520%253D%2520New&Us
erName=yha&PasswordEncrypted=sSNw%2bObuikFZAto1KMuqMQ%3d%3d&appID=&loadAcce
ssToken=0b8jh3i6h9o7x
```

If this token is removed from the HTTP request, then the load script will fail and throw the following error message if tested for example in Chrome and the expected result was a JSON response from the REST API.

```
Error Code 2. Please contact the Qlik Web Connectors deployment
administrator with this message, your IP Address (172.17.17.101) and
details of your request (including your request URL).
```

The load access tokens allow the Web Connectors to map the request to particular user and look up settings associated with that user (e.g. access tokens to a particular API) as well as associate API call logs and error logs to that user.

Since Tokens are embedded in the QlikView and Qlik Sense load script, thus it is important to guard and deliver them in a secure way. If others put their hands on the tokens, then they will be able to use them in their own API requests / load scripts and retrieve data using the Web Connectors installed on your machine.

Enabling access with Tokens

1. From the “Settings” tab you may add a new user by filling the input fields for username@domain.com and Password. You can key-in the password or click on the generate button to assign one.
2. Then you may key-in the token or click on “Generate” to have the application creates the Token automatically.
3. Passwords and tokens are at least 10 characters.
4. Click on “Save”, the Password and Token become hidden now. You may click on “Show” to view them again.
5. You will only be able to edit the passwords easily in the logins.xml file if the “PasswordChecker” element in deploy.config is set to:

```
<PasswordChecker>PlainTextPasswordChecker</PasswordChecker>
```

Otherwise the passwords will be hashed and not easy to set manually without going through the Web UI.

Web connectors licensing and how many users can be setup

After installing the Web Connectors the first time, you will need to insert your license information in case you want to use the "Premium connectors". If you don't need the premium connectors, then you may use the standard ones.

For licensing your Web Connectors, you need the following information, provided by Qlik:

- The serial number and control number.
- Otherwise the Lef.txt file (if the machine on which you are installing the license has no internet connection)

As it is the case with new users and Tokens allocation, the Web Connectors will always allow a maximum number of 50 users to be added, this is regardless if the license is provided or not. Once "FormsAuthentication" is enabled then by default you will get 50 users as a maximum number of users to be managed.

Steps for licensing the Web Connectors:

- Run the Web Connectors and then click on the "License" tab at the top of the page.
- Enter the Owner name and the Owner organization.
- Enter the Serial number and Control number.
- If you do not have internet access on the machine you are licensing, open the Lef.txt file in an appropriate application, like Notepad. Select all the text in the file and copy/paste it into the Enter LEF text box.
- Click on Apply new LEF.

Once this is done, the "License" tab is updated to reflect the installed license. Click on the Connectors tab to return to the list of connectors. The connectors included in your license will now show true in the Licensed column.

Note, the installed LEF license text can be found in the LicenceSettings.xml file, in the App_Data folder of the Web Connectors folder on the root drive, see the example below.

```
C:\Users\{some user}\Desktop\Qlik\QlikWebConnectors2.0.1\App_Data
```

Tags: Web Connectors, user management, deploy.config, FormsAuthentication

By: Youness Ghanim