Setup Windows Integrated Security With Waffle

This document describes how to connect the Waffle valve in DigDash Enterprise to active Windows Integrated Security (NTLM...).

This add-on is located in **<DDE install>/add-ons/singlesignon/Waffle**.

The current Waffle version is 1.8.1.

This document describes all folders and files to modifiy to activate this valve.

I. APACHE-TOMCAT / LIB

Cleanup previous waffle version

In case of a DigDash upgrade, you may have a previous version of waffle deployed on the tomcat. You must first clean the corresponding jar files from **<DDE install>/apache-tomcat/lib**. Please refer to the waffle deployment guide from the previous version of DigDash to delete the old waffle library files from **<DDE install>/apache-tomcat/lib**, and only these ones.

Tomcat 8

Add the waffle libraries from the folder **<DDE install>/add-ons/singlesignon/Waffle/Tomcat8** to the folder **<DDE install>/apache-tomcat/lib**:

- guava-19.0.jar
- jna-4.2.1.jar
- jna-platform-4.2.1.jar
- slf4j-api-1.7.21.jar
- slf4j-log4j12-1.7.21.jar
- log4j-1.2.15.jar
- waffle-jna-1.8.1.jar
- waffle-tomcat8-1.8.1.jar
- waffle_digdash_extension_tomcat8.jar
- log4j.properties

Tomcat 7

Add the waffle libraries from the folder **<DDE install>/add-ons/singlesignon/Waffle/Tomcat7** to the folder **<DDE install>/apache-tomcat/lib**:

- guava-19.0.jar
- jna-4.2.1.jar
- jna-platform-4.2.1.jar
- slf4j-api-1.7.21.jar
- slf4j-log4j12-1.7.21.jar
- log4j-1.2.15.jar
- waffle-jna-1.8.1.jar
- waffle-tomcat7-1.8.1.jar
- waffle_digdash_extension_tomcat7.jar
- log4j.properties

II. APACHE-TOMCAT / CONF / CONTEXT.XML

Add the following security valve XML:

```
<Valve className="waffle.apache.SharedNegotiateAuthenticator"
principalFormat="fqn" roleFormat="both"
sharedPasswd="SecretPwdToChange" allowAddr="localhost,127.0.0.*"/>
<Realm className="waffle.apache.WindowsRealm"/>
```

It is important to change the shared password (**sharedPasswd**). This password must be identical to the one specified in file **<DDE install>/apache-tomcat/digdash_dashboard/WEB-INF/web.xml** (see chapter IV).

You can also add allowed remote host addresses (**allowAddr**) to let other applications (digdash_dashboard) to connect to DigDash Enterprise server. In **allowAddr** attribute, you should add your server's IP address.

III. APACHE-TOMCAT / CONF / WEB.XML

Add the XML content for the security constraint:

```
<security-role>
      <role-name>Everyone</role-name>
</security-role>

<security-constraint>
      <display-name>Waffle Security Constraint</display-name>
      <web-resource-collection>
            <web-resource-name>Protected Area</web-resource-name>
            <url-pattern>/*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
            <role-name>Everyone</role-name>
      </auth-constraint>
</security-constraint>

<security-constraint>
      <display-name>vjdbc Security Constraint</display-name>
      <web-resource-collection>
            <web-resource-name>UnProtected Area</web-resource-name>
            <url-pattern>/vjdbc/*</url-pattern>
      </web-resource-collection>
</security-constraint>
```

Important

Security role name (role-name) MUST match the actual role you have in your AD (localized). Example : BUILTIN\Users

If your are not sure about the role names in your Active Directory, you can activate the debug log for waffle by using the provided log4j.properties. You just need to copy this file into **<DDE install>/apache-tomcat/lib**

IV. APACHE-TOMCAT / WEBAPPS / DIGDASH_DASHBOARD / WEB-INF / WEB.XML

Search for the definition of the parameter **sharedPasswd** in this file, un-comment the corresponding XML and change the password value (**bold underline**):

```
<init-param>
      <param-name>sharedPasswd</param-name>
      <param-value>SecretPwdToChange</param-value>
</init-param>
```

Important

> The specified password must be identical to the one set in file **<DDE install>/apache-tomcat/conf/context.xml** (chapter II).

Recommended parameters for automatic login in dashboard

It is recommended to configure the following parameters in file **<DDE install>/apache-tomcat/webapps/digdash_dashboard/WEB-INF/web.xml** when deploying for using Windows Integrated Security (Waffle).

Specify (and force) DigDash Enterprise domain:

```
<init-param>
      <param-name>DOMAIN</param-name>
      <param-value>ddenterpriseapi</param-value>
</init-param>
<init-param>
      <param-name>FORCEDOMAIN</param-name>
      <param-value>true</param-value>
</init-param>
```

Specify (and force) DigDash Enterprise domain URL. Use *localhost* address when ddenterpriseapi web application is installed on the same Tomcat than digdash_dashboard web application. Adapt port if needed:

```
<init-param>
      <param-name>SERVERURL</param-name>
      <param-value>http://localhost:8080</param-value>
</init-param>
<init-param>
      <param-name>FORCESERVERURL</param-name>
      <param-value>true</param-value>
</init-param>
```

Specify a logout URL to allow the user to disconnect properly from DigDash

Enterprise and, for example, return to an Intranet page:

```
<init-param>
      <param-name>urlLogout</param-name>
      <param-value>/adminconsole</param-value>
</init-param>
```

Important

> By default, loging out the dashboard returns to its login page. This page is bypassed in a SSO context, so it automatically logs in the user again. It is important to specify a logout page to create a nice user experience.

See the document **digdash_enterprise_advanced_system_guide_en.pdf** for more details on these parameters.

V. APACHE-TOMCAT / WEBAPPS / DDENTERPRISEAPI / WEB-INF / WEB.XML

Search for definition of the **authMethod** parameter in this file and change its value into **NTUser**:

```
<init-param>
      <param-name>authMethod</param-name>
      <!-- possible values: LDAP, PassThru, NTUser, NTUserOrLDAP -->
      <param-value>NTUser</param-value>
</init-param>
```

Note

The mode « **NTUserOrLDAP** » let the user authenticate on the DigDash server through Windows Integrated Security, with a fallback authentication through DigDash LDAP.
For instance, a user from the NT domain could automatically pass the Waffle valve with his Windows credentials, but would fail loging in DigDash if he does not exist in DigDash LDAP. In that mode, he would get a login form to specify a DigDash login/password.
Also in this mode is an optional parameter « **loginForm** » used in some URLs which allows the login page to be always displayed. This way the Windows credentials are only used to pass the Waffle valve. A typical use case is to allow a Windows user to connect as “admin” in DigDash settings pages.

VI. APACHE-TOMCAT / WEBAPPS / ADMINCONSOLE / DIGDASH.JNLP

By default, when the DigDash server is configured to use the Windows Integrated Security, the user must enter its Windows login (NT domain\user) and password in the Studio login dialog box. For instance:

User: NT_DOMAIN\user1

Password: ******

There is a way to allow the Studio to automatically authenticate the current logged Windows user. The following conditions are required:

- Studio is launched on a Windows computer, from a Windows session authenticated in the concerned Windows security domain
- The URL of the DigDash server, the DigDash enterprise domain name, and the authentication mode of the Studio (NTUser, NTUserOrLDAP…) are specified and forced in the JNLP file

Proceed with the following configuration in the **<DDE install>/apache-tomcat/webapps/adminconsole/digdash.jnlp** file if you want to activate the automatic login with Windows Integrated Security in DigDash Enterprise Studio.

At the end of this file you will find the XML for the parameter of the Studio. Replace the value of some of the parameters as shown below (see values in **bold underline**):

```
<application-desc main-class="commandline.CommandLineMain">
      <argument>http://server_digdash:8080</argument>
      <argument>ddenterpriseapi</argument>
      <argument><%=lang%></argument>
      <argument><%=dashboard%></argument>
      <argument>true</argument>
      <argument>NTUser</argument>
</application-desc>
```

Description of the modified parameters:

- 1st parameter: DigDash serveur URL accessed by the Studio.
- 2nd parameter: DigDash Enterprise domain name.
- 5th parameter: Force specified URL and domaine name: they are read-only in Studio's login dialog box (true).
- 6th parameter: Forced authentication mode for the Studio (see chapter V for more details). Only the « **NTUser** », « **NTUserOrLDAP** » or « **NTUserOrLDAP,loginForm** » allow the automatic login with Windows Integrated Security.