



XchangeCore TechNote – Tomcat Cross Origin Resource Sharing (CORS)

XCORE-CORS-R1C01

November 23, 2014

The XchangeCore Community

www.XchangeCore.com



1.0 Tomcat Cross Origin Resource Sharing (CORS)

The XchangeCore Connector for ArcGIS Online requires enabling the XchangeCore’s Tomcat component’s Cross Origin Resource Sharing (CORS) filter. Apache Tomcat includes the support of CORS from Tomcat version 7.0.41 and after. XchangeCore Version 1.3.3 and 2.0 both use this or a later version of Tomcat.

2.0 Procedure to Enable Tomcat CORS Filters

The procedures to enable the CORS filters are as follows:

1. Open the Windows Command Prompt “as Administrator.”
2. Change directory to C:\Core.
3. At the C:\Core> prompt, execute “core stop tomcat”. This will stop the tomcat service.
4. Open C:\Core\Server\Tomcat\conf\web.xml file with an editor
5. Locate the line
`<!-- ===== Built In Filter Definitions ===== -->`
6. Add the following xml segment BEFORE the line

```
<filter>
<filter-name>CorsFilter</filter-name>
<filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
<init-param>
<param-name>cors.allowed.origins</param-name>
<param-value>*</param-value>
</init-param>
<init-param>
<param-name>cors.allowed.methods</param-name>
<param-value>GET,POST,HEAD,OPTIONS,PUT</param-value>
</init-param>
<init-param>
<param-name>cors.allowed.headers</param-name>
<param-value>Content-Type,X-Requested-With,accept,Origin,Access-Control-Request-
Method,Access-Control-Request-Headers</param-value>
</init-param>
<init-param>
<param-name>cors.exposed.headers</param-name>
<param-value>Access-Control-Allow-Origin,Access-Control-Allow-Credentials</param-value>
</init-param>
<init-param>
<param-name>cors.support.credentials</param-name>
<param-value>>true</param-value>
</init-param>
<init-param>
<param-name>cors.preflight.maxage</param-name>
```



```
<param-value>10</param-value>
</init-param>
</filter>
<filter-mapping>
  <filter-name>CorsFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

7. Save the file.
8. Open C:\Core\ServerApps\uicds\WEB-INF\web.xml file with an editor
9. Locate the following security constraint section and add the highlighted lines

```
<!-- Define a Security Constraint on this Application -->
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>UICDS Web Services</web-resource-name>
      <url-pattern>/core/ws/services/*</url-pattern>
      <url-pattern>/pub/*</url-pattern>
      <url-pattern>/query/*</url-pattern>
      <url-pattern>/Console.html</url-pattern>
    <!--CORS here -->
      <http-method>GET</http-method>
      <http-method>POST</http-method>
      <http-method>PUT</http-method>
      <http-method>DELETE</http-method>
    </web-resource-collection>
    <auth-constraint>
      <role-name>uicds-users</role-name>
    </auth-constraint>
  </security-constraint>
```

10. Save the file
11. At the C:\Core> prompt, execute “core start tomcat”. This will start the Tomcat service with CORS filter enabled.