FileNet P8 Workplace XT, **Version 1.1.5** Application server: **WebSphere Application Server**

Configuring WebSphere Application Server to support user tokens and WebDAV connections for Workplace XT

Some applications that work with Workplace XT, such as Application Integration, eForms, and Records Manager, require that you enable the generation and acceptance of user tokens on the Workplace XT server. This configuration is also required to enable WebDAV connections.

To configure WebSphere® Application Server to support user tokens and WebDAV connections:

1. Stop WebSphere Application Server, if it is running.
2. (For installations with Content Engine at 4.5.0 or 4.5.1) Copy the authentication-websphere.jar file from here:

   install_path/IBM/FileNet/WebClient/WorkplaceXT/authenticationFiles

   to here:

   WAS_home/AppServer/lib/ext

3. (For installations with Content Engine at 4.0.) Copy the authentication-websphere-1.1.2.jar file from here:

   install_path/IBM/FileNet/WebClient/WorkplaceXT/authenticationFiles/1.1.2

   to here:

   WAS_home/AppServer/lib/ext

4. Copy the log4j-1.2.13.jar file from here:

   install_path/IBM/FileNet/WebClient/WorkplaceXT/WEB-INF/lib

   to here:

   WAS_home/AppServer/lib/ext

5. Enable JAAS.
   a. Navigate to the Java™ Virtual Machine.

      WebSphere Application Server 6.1
      Servers > Application Servers > *server_name* > Java & Process Management > Process Definition > Java Virtual Machine
      WebSphere Application Server 7.0

Servers > Server Types > WebSphere application servers > server_name > Java & Process Management > Process Definition > Java Virtual Machine

b. If there is an entry in the Generic JVM arguments, add a space after it, then add the following entry and apply your changes.

   If there is no entry, do not add the space.

   UNIX

   ```
   -Djava.security.auth.login.config=install_path/CE_API/config/jaas.co
   ```

   Windows

   ```
   -Djava.security.auth.login.config=install_path\CE_API\config\jaas.co
   ```

   where *install_path* is the installation path of Workplace XT.

   Your path might be slightly different depending on the version of your client installations, or whether you have chosen a custom path for installation. For example, if your Content Engine Client is at 4.0, this path might include a samples directory under the config directory. Verify the location of the file before you enter the path.

   Do not copy and paste the text from this guide because hidden formatting can cause problems with the entry. Instead, type the entry into the field.

   On WebSphere Application Server for Windows, the path cannot contain a space. You must use 8.3 notation for the install path portion of the djava argument.

   If *install_path* is:

   ```
   C:\Program Files\IBM\FileNet\WebClient
   ```

   use:

   ```
   C:\Progra~1\IBM\FileNet\WebClient
   ```

   Example of full argument for Windows:

   ```
   -Djava.security.auth.login.config=C:\Progra~1\IBM\FileNet\WebClient\CE_AP
    config\jaas.conf.WebSphere
   ```

   Example of full argument for UNIX:

   ```
   -Djava.security.auth.login.config=/opt/IBM/FileNet/WebClient/CE_API/
    config/jaas.conf.WebSphere
   ```

   Note that for 64-bit machines with Workplace XT installed in the Program Files (x86) directory, the JVM argument is:

   ```
   -Djava.security.auth.login.config=C:\Progra~2\IBM\FileNet\WebClient\CE_AP
    config\jaas.conf.WebSphere
   ```

c. (For components not using SSO only) Create a custom module.
   Important: Do not create a custom module if you are enabling JAAS for any component using SSO. Creating the custom module makes SSO unusable.

i. Navigate to the JAAS login module settings in the Security area of the administration console.

WebSphere Application Server 6.1
Navigate to Security > Secure administration, applications, and infrastructure > JAVA Authentication and Authorization Service > System logins > WEB_INBOUND > JAAS login modules.
WebSphere Application Server 7.0
Navigate to Security > Global security > JAVA Authentication and Authorization Service > System logins > WEB_INBOUND.

ii. Click New to create a new custom login module.
iii. Enter the following with no spaces for the Module class name setting:

```
com.filenet.ae.authentication.
  loginmodule.UserTokenWSLoginModule
```

iv. Apply and save your changes to the master configuration.

6. Enable trust association and specify the interceptor setting.
   a. Navigate to the trust association settings in the Security area of the administration console.

   WebSphere Application Server 6.1
   Navigate to Security > Secure administration, applications, and infrastructure > Web security > Trust association.
   WebSphere Application Server 7.0
   Navigate to Security > Global security > Web and SIP security > Trust association.

   b. In the Trust associations settings, set Enable trust association.
   c. Under Additional Properties, click Interceptors.
   d. Add a new Interceptor, and enter the following for the Interceptor class name:
   `com.filenet.ae.authentication.tai.UserTokenInterceptor`
   e. Apply and save your changes to the master configuration.
7. Restart WebSphere Application Server.

Parent topic: Configuring Workplace XT on WebSphere Application Server

---

Last updated: March 2013
wxtip018.htm