Security Checklist

How to Protect WSM from Attacks

1 Purpose

When you install WSM, it is ready for development. This means that developers and administrators can comfortably access it for configuration and development.

We strongly recommend that you use this guide to close all of the potential security holes after installation. If you do leave a potential security hole open for development, make sure that you close it before outside users have access to the system.

Note: Some of the properties mentioned here may not be installed on your system depending on the installer option you selected.

Because WSM stores all of its internal files in the ContentBus repository, you can seal off all sensitive areas by setting restrictive access rights on the ContentBus.

Note: If a recommendation includes modifying or deleting files, and if you are not sure whether you can do so safely, create a backup of the ContentBus or of the files. You can do so using WSM's package tool.

2 Change the Superuser Password

This applies to all author and publish instances in a live environment. If your development instances run in an environment where outsiders can access it, change the password there as well.

Setting the Password During Installation

If you install WSM using the **Custom Installation**, the installer asks you to type the superuser password for each instance you install.

Changing the Password on Author Instances

If you did not change the superuser password during installation, then changing it on an author instance is straightforward:

1. Log in on the author instance with **superuser/superuser**
2. Click the **User Properties** button (top right).
3. Change the superuser password.
4. After you submit, log in with the new password.

Changing the Password on Publishing Instances

On a publishing instance, you typically do not have an administration environment. To change the password, you need to replicate the modified superuser account from the authoring environment. For this, you use WSM's package tool. Proceed as follows:

1. Log in to WSM's authoring and administration environment.
2. Click the **Miscellaneous** tab, click the **Packages** folder, and then click the **New** icon (blank page). The Create Page window opens.
3. Type a title (for example, "**superuser**"). Click **WSM Package Definition Template**, and then click **OK**. WSM creates a new package page.
4. Click the new package. The package window opens. In the Rules field, type **/access/users/superuser**. In the Type list, click **Allow**. Click the **Add/Modify** button to add the rule, and then click the **Recreate Package** button to create the package.

5. In the Delivery Agents group, check the delivery agent for your publishing environment. In the default installation, check **author**. Click the **Deploy Package** button to transfer the user account to the publish instance.

6. Log in to the publish instance with the new password to make sure that the transfer has worked. You may have to log out and close all browser windows before you can successfully do so.

Note: If you use the superuser account for replication, make sure that you change the replication password to the new password.

---

3 Change the JMX MBean Server Password

WSM has an internal JMX MBean server. This server has its own port, administration screen, user name and password. By default, you can connect to port 8090 of a Computer that runs WSM, and log on using the user name “superuser” and the password “superuser”.

Change the password in the configuration file **/config/manager.xml**, as follows:

```
<management domain="Communique4"
mBeanServerType="private">
    <http port="8090">
        <user name="superuser" password="myNewPassword"
/>
    </http>
</management>
```

Also, make sure that users cannot access port 8090 of a productive WSM instance.

Note: Do not remove the user element. If you do not specify a user, anyone can log in without specifying a user name or password.

4 Default Users and Groups

Depending on your selected installation options, the WSM Installer installs a number of default user and group accounts. The following table lists each user and group with a short description and FileNet's recommendation about what to do with it. If you do not delete the accounts listed here, **do change the default password**. Note that some of these accounts have full read and write access – do not keep them open to outside access.

Account	Description	Recommendation
Webmaster	An example Webmaster account.	Delete or adapt to your needs.
System Users/pre	Defines the default rights for all user accounts.	Do not modify or delete. Modifying this account has additional security implications.
System Users/post	Defines the mandatory access rights for all users.	Do not modify or delete. Modifying this account has additional security implications.
System Users/ anonymous	The default rights for unauthenticated access. By default, no rights.	Do not delete. Modifying this account has additional security implications.
System Users/nobody	The account used for unauthenticated access to a publish instance. By default, read rights to the /content section.	Do not delete. Modify if your Web site has restricted sections.
Replication Users/author	This is an example delivery agent to replicate content to a publish instance. A delivery agent replicates all content that it has read access to. By default, it has read access to the entire ContentBus.	Delete or adapt for your needs. If you want to replicate user accounts to the publish instance, you must set the superuser account as the transport user.
Replication	This is an example	Modify if you use the

Users/ dispatcher	delivery agent to send cache flush requests to a dispatcher. By default, it has read access on the entire ContentBus.	dispatcher, or delete if you do not.
Replication Users/publish	An example receiver agent for publish instances. Has full access to the section it updates.	Delete or adapt it to your needs. You cannot use this account to replicate user accounts, because only the superuser account can do so.
Personalisation Users /surfer	An example account to demonstrate the personalization features of the example project.	Delete.
Collaboration Users/forum	An example account to demonstrate the use of the forum.	Delete if you do not use the forum module. If you use the module, restrict the access to where the forum is located.
Development Users/ jspdebugger	The user account that is used by default by the WSM JSP Debugger.	Delete it if you do not use the JSP Debugger.

Account	Description	Recommendation
Content Author	Users in this group have full access rights to the content and miscellaneous sections.	Keep it if you can use it. If not, delete.
Site Administrator	Users in this group see the Site, Inbox and Search tab in the CMS. Rights to the content pages itself are not included.	Useful to control which functions of the CMS an author has available. Delete if you do not use it.

Miscellaneous Administrator	Users in this group see the Miscellaneous tab in the CMS. Rights to the miscellaneous pages are not included.	Useful to control which functions of the CMS an author has available. Delete if you do not use it.
User Administrator	Users in this group see the Users tab in the CMS. Users can edit their own account and all sub accounts.	Useful to control which functions of the CMS an author has available. Delete if you do not use it.
Group Administrator	Users in this group see the Groups tab in the CMS. Includes full access rights to edit the groups.	Useful to control which functions of the CMS an author has available. Delete if you do not use it.
Roles Administrator	Users in this group see the Roles tab in the CMS. Includes full access rights to edit the roles.	Useful to control which functions of the CMS an author has available. Delete if you do not use it.
Developer	Users in this group can connect to the WSM instance using the WSM Development Environment (CQDE).	Use only on development instances. On all other instances, delete.

Note: Again, make sure that you have **changed the passwords** of all the users and groups that you have not deleted.

5 Restrict CQDE Access

When you perform a default installation, or if you check **Enable Development** during the custom installation process, the WSM installer installs the CQDE library. This library allows you to connect to the ContentBus using the WSM Development Environment (CQDE).

This library is located in the following folder in the ContentBus:

```
/system/cqde
```

Make sure that this library is not available on a live system if you do not absolutely need it. Using CQDE, users have read access to the entire ContentBus repository, which may pose a serious security threat, even if they are not allowed to modify any content.

If you want to keep the option of logging on with CQDE at a later time, create a package of the system/cqde folder, and then delete it. If you require CQDE access, you can re-install the package.

Note: If you need to connect to a live instance using CQDE (for example to debug features that only work in the live environment), give the connecting user explicit rights to connect to this library. Access to it is explicitly denied in the **pre**, **anonymous** and **nobody** account.

---

6 Disable WebDAV

Using WebDAV, you can connect to the ContentBus using a Web folder. This allows you to use file-based development environments on the ContentBus repository.

WSM has two default WebDAV pages located in the folder **/etc/webdav.** You can see the pages in the **Miscellaneous** tab in section **WebDAV**:

- The **Content View** is an example that shows how you can edit content from the example projects as RTF files. Delete this page, at least on a production environment.
- The **Resource View** shows all resource files as text files, similar to the resource view in CQDE. This view is mainly used for development purposes. Delete it when on non-development instances.

7 Deny Access with Dispatcher Configuration

You can use the Dispatcher to seal off sensitive areas. If a dispatcher is in front of a publish instance, you can define a filter that refuses all requests to sensitive areas. A request to a sensitive area results in a 404 error code (page not found).

For example, the following filter configuration in the file dispatcher.any shuts off the administration screen from outside access:

```
...
/filter
  {
  /0001
    {
    /glob "*"
    /type "allow"
    }
  /0002
    {
    /glob "* /system*"
    /type "deny"
    }
  /0003
    {
    # restrict access to CMS administration
    /glob "* /libs/CFC/content/admin*"
    /type "deny"
    }
  }
...
```

If your publish instance uses a Web application context, for example “publish”, specify the context as follows:

```
...
/filter
  {
  /0001
    {
    /glob "*"
    /type "allow"
    }
  /0002
    {
    /glob "* publish/system*"
    /type "deny"
    }
  /0003
    {
    # restrict access to CMS administration
    /glob "* publish/libs/CFC/content/admin*"
    /type "deny"
    }
  }
```

```
...
```

If you still want to access single pages in the restricted area, such as the status window, you can allow access to them. The status window is located at the following address:

```
/libs/CFC/content/admin/status.html?CFC_technique=iFrame
```

To allow access to this address, add the following section to the configuration file:

```
...
/0004
{
/glob "* /libs/CFC/content/admin/status*"
/type "allow"
}
...
```

Again, if you have a Web application context prefix, add it as well.

With this setting, a user still has to log in as superuser to see the status screen. As said before, **do change the superuser password** on the publish instance.

Note: Some libraries contain images that WSM uses. If you block too much of a library, you may lose access to these.

---

8 Restrict the Servlet Engine Administrator

If you installed the WSM Servlet Engine, you have a Servlet Engine administration application available under the /admin folder of your Web site.

When you have installed the WSM Servlet Engine, the installer has asked you to type the password for the **Servlet Engine Administrator** account named **admin**. If you did not alter the password, it is set to **admin**. So:

CHANGE THE SERVLET ENGINE ADMIN USER PASSWORD!

To do this, go to the servlet engine administration page, for example:

```
http://localhost:4302/admin/
```

Log in with admin/admin, click **Change Password**, and type the new password.

We also recommended to disable access to the /admin folder completely from outside. To do so, add the following section to your Dispatcher configuration file:

```
...
/0005
  {
  /glob "* /admin*"
  /type "deny"
  }
...
```

9 Check for Cross-Site Scripting (XSS)

Cross-site scripting, or XSS, allows an attacker to execute JavaScript code in the Web browser. The attacker types the JavaScript code into a text field, such as a search field, and the targeted application executes it when it displays the results along with the content of the search field.

WSM's authoring and administration environment is protected against this type of attack. If you have made changes to the authoring environment, make sure that they are protected as well.

Note: In general, WSM's example code is not protected against attacks. Example code illustrates a basic concept, and is as simple as possible. If you want to use example code in a productive environment, you may have to add protection from XSS attacks.