

_include_wsc55x_server_configure_selinux

Security-Enhanced Linux (SELinux) defines the access and transition rights of every user, application, process, and file on the system. SELinux manages the interactions of these entities using a security policy that specifies how strict or lenient a given Red Hat Enterprise/CentOS Linux installation should be.

The default installation of the WebSpellChecker Server package is not intended for such a secured environment. It requires additional configuration steps from your side. Once the default installation has been performed, you can proceed with the SELinux configuration as described in this section.

2.1. Define security context for WebSpellChecker Server. To do so, specify the appropriate security context for all the files inside the installation directory using the following command:

```
sudo /sbin/restorecon -R -v /<WebSpellChecker_Installation_Dir>/WSC
```



restorecon command sets files security context. Read more about [SELinux/restorecon](#).

-R option changes files and directory file labels recursively.

-v option defines where the changes will take place, e.g. all the files under /<WebSpellChecker_Installation_Dir>/WSC will be changed.

2.2. Allow network connection. To do so, allow Apache HTTP Server scripts and modules to connect to the network by setting a SELinux boolean to a given value.

```
sudo /usr/sbin/setsebool -P httpd_can_network_connect=1
```



setsebool command allows setting a SELinux boolean value. Read more about [SELinux/setsebool](#).

httpd_can_network_connect allows HTTPD scripts and modules to connect to the network.

-P option saves all pending values on the disk. Without **-P** option, only the current boolean value would be affected. After the reboot, it will be reverted.



Step below is required only if you have selected the installation of **WSC Dialog Plugin for CKEditor** (Option 4) or **All products** (Option 5) before.

3.3. Define Security Context for SSRV Script. Separately you need to set the appropriate security context for the SSRV.FGCI script. By default, SSRV.FGCI script has the **default_t** context type. This is incorrect security context for SELinux. If you try to view page, SELinux will deny access and log the error.

Run the following command to set a proper security context type of **httpd_sys_content_t** for SSRV.FGCI:

```
sudo chcon -t httpd_sys_content_t /opt/WSC/WebComponents/WebInterface/script/ssrv.fcgi
```