

Communication issues with Management Console 3.3.2 and Blancco 5 erasure software

Since Java 8 update 60 (1.8.0_60) "RC4" cipher suites have been disabled. This caused issues with the communication between Management Console and Blancco 5 erasure software clients. The issue have been fixed in the Blancco Management Console 3.5.0 release.

Disabled "RC4" cipher suite may cause communication issues if Management Console version 3.3.2 is used with the Blancco 5 (5.9.0 or newer) erasure software.

To fix the issue Management Console cipher set needs to be updated manually into the Management Console's server.xml file.

1. Stop Blancco Management Console 3 service.
2. Go to the Management Console 3 installation folder: {MC_3_installation_folder}\apache-tomcat\conf\
3. Locate server.xml file.
4. Make a backup copy of the file.
5. Edit the server.xml file with a text editor software (for example Notepad) according to the example further below.
6. After editing the file, save it and restart the Blancco Management Console 3 service.

Locate line 14 (looks like this):

```
<Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="500" ciphers="SSL_RSA_WITH_RC4_128_SHA" clientAuth="false" compression="on" connectionTimeout="30000" enableLookups="false" executor="tomcatThreadPool" keystoreFile="conf/keystore.jks" keystorePass="mchammer" port="8443" protocol="org.apache.coyote.http11.Http11Protocol" scheme="https" secure="true" sslEnabledProtocols="SSLv3,TLSv1,TLSv1.1,TLSv1.2"/>
```

Change it to this (replace the black bold string with the red bold string):

```
<Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="500" ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256" clientAuth="false" compression="on" connectionTimeout="30000" enableLookups="false" executor="tomcatThreadPool" keystoreFile="conf/keystore.jks" keystorePass="mchammer" port="8443" protocol="org.apache.coyote.http11.Http11Protocol" scheme="https" secure="true" sslEnabledProtocols="SSLv3,TLSv1,TLSv1.1,TLSv1.2"/>
```