

# FAQ: How to improve security of connection to AhsayCBS (Strong Cipher, TLS protocol and PFS)

**Article ID:** 8116

**Reviewed:** 30/04/2021

**Product Version:**

AhsayCBS: 8.1 or above

OS: All platforms

## Description

This article outlines how to improve security of connection to AhsayCBS by:

- Usage of strong cipher and TLS protocol
- Support of perfect forward secrecy (PFS)

**Important:** Only perform the following steps if you have no version 6 AhsayOBM / ACB client connecting to your AhsayCBS server.

## Steps

Refer to the following steps for detail:

- To change the HTTPS connection to TLSv1.2 only:
  1. Browse to the following path on the AhsayCBS server:  
  
%CBS\_Installation\_Home%/conf
  2. Open the server.xml file with a text editor:

server.xml

```
...
...
    <Connector maxKeepAliveRequests="9999"
keepAliveTimeout="30000" address="0.0.0.0" scheme="https"
enableLookups="false" socket.txBufSize="43800"
    connectionUploadTimeout="900000" acceptCount="200"
secure="true" URIEncoding="utf-8" sendReasonPhrase="true"
protocol="org.apache.
    maxHttpHeaderSize="8192" redirectPort="443"
executor="tomcatThreadPool-https-0.0.0.0-443"
disableUploadTimeout="false" coyote.
    http11.Http11NioProtocol" SSLEnabled="true" port="443"
socket.rxBufSize="25188" connectionTimeout="10000"
maxConnections="500">
    <SSLHostConfig disableCompression="true"
caCertificateFile="${catalina.base}/conf/ca.crt"
insecureRenegotiation="false"
    honorCipherOrder="false" ciphers="HIGH:!aNULL:!MD5"
disableSessionTickets="false"
protocols="+TLSv1+TLSv1.1+TLSv1.2"
    certificateVerification="false"
certificateVerificationDepth="10">
```

3. Edit the line from `protocols="+TLSv1+TLSv1.1+TLSv1.2"` to `protocols="TLSv1.2"`:

server.xml

```
...
...
    <Connector maxKeepAliveRequests="9999"
keepAliveTimeout="30000" address="0.0.0.0" scheme="https"
enableLookups="false" socket.txBufSize="43800"
    connectionUploadTimeout="900000" acceptCount="200"
secure="true" URIEncoding="utf-8" sendReasonPhrase="true"
protocol="org.apache.
    maxHttpHeaderSize="8192" redirectPort="443"
executor="tomcatThreadPool-https-0.0.0.0-443"
disableUploadTimeout="false" coyote.
    http11.Http11NioProtocol" SSLEnabled="true" port="443"
socket.rxBufSize="25188" connectionTimeout="10000"
maxConnections="500">
    <SSLHostConfig disableCompression="true"
caCertificateFile="${catalina.base}/conf/ca.crt"
insecureRenegotiation="false"
    honorCipherOrder="false" ciphers="HIGH:!aNULL:!MD5"
disableSessionTickets="false" protocols="TLSv1.2"
    certificateVerification="false"
certificateVerificationDepth="10">
```

## Keywords

seedload, import, local, cloud, network, removable, export, win

From:  
<https://wiki.ahsay.com/> - **Ahsay Wiki**

Permanent link:  
[https://wiki.ahsay.com/doku.php?id=public:8116\\_faq:how\\_to\\_improve\\_security\\_of\\_connection\\_to\\_cbs&rev=1619774766](https://wiki.ahsay.com/doku.php?id=public:8116_faq:how_to_improve_security_of_connection_to_cbs&rev=1619774766)

Last update: **2021/04/30 17:26**

