FAQ: How to provide a higher level of SSL security for AhsayCBS

Article ID: 5116
Reviewed: 13/11/2017

Product Version:
AhsayCBS: All
OS: All platforms

Description

This article provides instruction on how to provide a higher level of SSL security for AhsayCBS.

Steps

To disable all weak cipher suite on AhsayCBS:

1. Edit the server.xml file found under ${Install-Home}\conf
    - Open 'server.xml' with a text editor:

server.xml

```
...
<Service name="Catalina">
        <Connector port="80" protocol="HTTP/1.1" maxKeepAliveRequests="1000" disableUploadTimeout="true" ...
           redirectPort="443" minSpareThreads="50" maxThreads="2000" acceptCount="200" ...
           connectionTimeout="120000" address="0.0.0.0" socketBuffer="16384" />
        <Connector port="443" SSLCipherSuite="HIGH:!aNULL:!MD5" protocol="HTTP/1.1" ...
...
...
```

    - Update the SSLCipherSuite parameter with:

SSLCipherSuite="ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:EDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK"

server.xml

```
...
<Service name="Catalina">
        <Connector port="80" protocol="HTTP/1.1" maxKeepAliveRequests="1000" disableUploadTimeout="true" ...
        redirectPort="443" minSpareThreads="50" maxThreads="2000" acceptCount="200" ...
           connectionTimeout="120000" address="0.0.0.0" socketBuffer="16384" />
```

```
        <Connector port="443" SSLCipherSuite="ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-
        GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:
        DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:EDH+AESGCM:ECDHE-
        RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
        ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-
        RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-
        AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:
        DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK" protocol="HTTP/1.1" ...
...
...
```

- Save and exit from the text editor.

2. Restart the AhsayCBS service.

Keywords

improve, security, cert, ssl, freak, weak, cipher, ciphersuite, suite, key

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

Permanent link:
https://wiki.ahsay.com/doku.php?id=public:5116_faq:how_to_provide_a_higher_level_of_ssl_security_for_ahsaycbs&rev=1529979337

Last update: **2021/04/30 16:22**