Enabling stronger cipher/protocol security with Enterprise Manager

If your exacqVision Enterprise Manager is already using HTTPS as described in our Knowledge Base Article ‘How to Enable HTTPS for ESM’ you can make sure you are using strong ciphers and the most current ssl protocol using this document.

Locate and make the indicated changes to the file httpd-ssl.conf

Windows

```
C:\Program Files\exacqVision\EnterpriseManager\apache_solr\apache2\conf\extra\httpd-ssl.conf
```

Linux

```
/usr/local/exacq/esm/apache_solr/apache2/conf/ httpd-ssl.conf
```

Find SSLCipherSuite and SSLProxyCipherSuite and make sure they match the following.

```
SSLCipherSuite "HIGH:!aNULL:!MD5:!3DES:!CAMELLIA:!AES128"
SSLProxyCipherSuite "HIGH:!aNULL:!MD5:!3DES:!CAMELLIA:!AES128"
```

Find the SSL Protocol Support section and make sure the following is set as follows. Note, it may be possible to user TLSv1.3 but it has not been tested yet.

```
SSLProtocol TLSv1.2
SSLProxyProtocol TLSv1.2
```

Verifying

To verify the endpoint is running as expected for your Enterprise Manager HTTPS site.

Run the following command from a Linux machine with openssl installed.

```
openssl s_client -connect YOUR_EM_URL:443
```

Note the output under SSL-Session.

```
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

Created On: 1st February 2021
KB Number: KB-00018-18-210201

tyco | Exacq