Disabling Outdated Versions of SSL/TLS

Article Number: 870 | Rating: Unrated | Last Updated: Thu, Aug 6, 2020 at 10:54 AM

How to disable outdated versions of SSL/TLS in Apache

In order to provide the most robust security possible, old versions of SSL/TLS should be disabled. Most modern browsers support the newer and more secure versions of SSL/TLS so disabling the less secure and older versions of SSL/TLS should not hinder user experience.

To disable outdated versions of SSL/TLS in Apache:

1. On your server, edit ssl.conf (usually located in /etc/httpd/conf.d).
2. Find the line that begins with the following in the file: *SSLProtocol all -SSLv2*
3. Comment out the line by adding a # before the line. This will disable TLS 1.0/1.1 and SSL 2.0/3.0.
4. Add the following line underneath the line you have just commented out: *SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1*
5. Next, find the line that begins with the following in the file: *SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA*
6. Comment out the line by adding a # before the line.
7. Add the following line underneath the line you have just commented out: *SSLCipherSuite HIGH:!aNULL:!MD5:!3DES*
    - This ensures the use of SSL encryption only with a high degree of protection.
8. Add the following line underneath the line you just added: *SSLHonorCipherOrder on*
    - This ensures that server cipher preferences are used and not the client preferences.
9. Save and close the file.
10. Restart the Apache service with the following command: *service httpd restart*
    - **NOTE:** This command will differ depending on your OS.

Be sure to test all applications that interact with your server. If you experience any problems, you can remove the comments (#) and added lines to return to the previous version of the file.

Posted by: **rspielman** - Thu, Aug 6, 2020 at 10:06 AM. This article has been viewed 2327 times.

Online URL: https://support.nagios.com/kb/article/disabling-outdated-versions-of-ssl-tls-870.html