-

NSE Clearing

Circular

NSE Clearing Limited
(Formerly known as National Securities Clearing Corporation Limited)

Department : Cyber and Information Security	
Download Ref No: NCL/CMPT/41830	Date : 07 AUGUST 2019
Circular Ref. No: 128/2019	

All Members,

Subject – Decommissioning of support for TLS 1.0 and TLS 1.1

To enhance the security of data and communications to and from NSE Clearing's systems, we intend to decommission the support for TLS 1.0 and TLS 1.1 protocols.

TLS (Transport Layer Security) is the protocol which secures HTTPS. TLS provides secure communication between web browsers and servers. TLS 1.2 was published ten years ago to address weaknesses in TLS 1.0 and 1.1 and has enjoyed wide adoption since then.

Accordingly, the leading browsers have decided to drop the support for the earlier versions of the protocol i.e. TLS 1.0 and TLS 1.1.

1. Microsoft will disable Transport Layer Security (TLS) 1.0 and 1.1 by default in supported versions of Microsoft Edge and Internet Explorer 11 in the first half of 2020.
2. Firefox will disable support for TLS 1.0 and TLS 1.1 in March 2020
3. Google Chrome will disable support for TLS 1.0 and TLS 1.1 in Chrome 72. TLS 1.0 and 1.1 will be disabled altogether in Chrome 81. This will affect users on early release channels starting January 2020.

With this background, and considering the implications, all members are requested to implement **one** of the following:

1. Upgrade the browsers to the latest versions.
    a. Google's Chrome - https://www.google.com/chrome/
    b. Mozilla's Firefox - https://www.mozilla.org/en-US/firefox/new/
    c. Microsoft's Internet Explorer - http://windows.microsoft.com/en-us/internet-explorer/download-ie
    d. Microsoft's Edge – https://www.microsoft.com/en-us/download/details.aspx?id=48126
2. Update the settings as per the steps outlined in Annexure – 1.

Beginning of October 1, 2019, NSE Clearing's web facing applications/websites shall only accept connections over TLS 1.2 version.

Reference Links:

1. https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/#Qt07jVdqb5lj99jy.97
2. https://security.googleblog.com/2018/10/modernizing-transport-security.html
3. https://www.ssl.com/article/tls-1-3-is-here-to-stay/
4. https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
5. https://kinsta.com/blog/tls-1-3/

Disclaimer:

1. The information contained in this notice has been extracted from the reference links as above
2. Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment. Please test all the settings in a test environment before being deployed on production.

For and on behalf of
NSE Clearing Limited
(Formerly known as National Securities Clearing Corporation Limited)

Huzefa Mahuvawala
Vice President

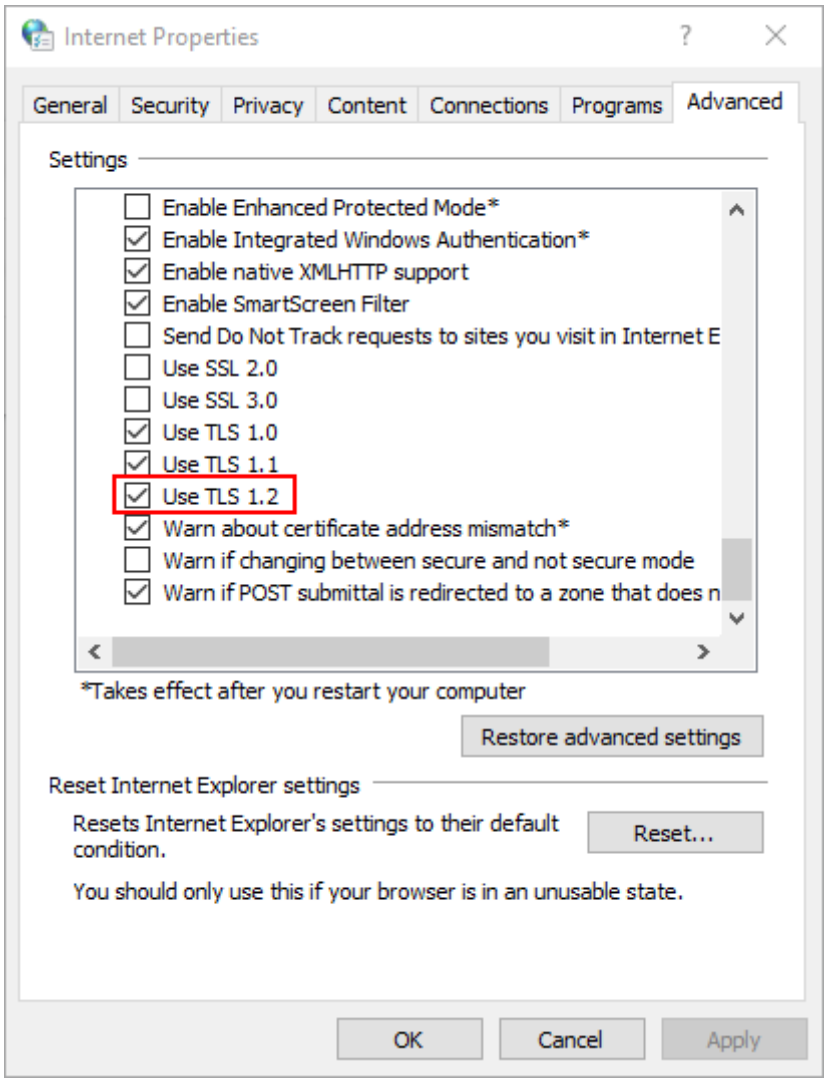
Toll Free No	Telephone	Email id
1800 266 0057	022-2659 8100	fao_clearing_ops@nsccl.co.in

Annexure – 1.

A) <u>Settings to be done on Internet Explorer (IE) browser at client end.</u>

1) Go to Tools → Internet Options → Advanced→Security
2) Following options should be checked
    a. Use TLS 1.2
3) Kindly apply and save the changes and restart the browser

In case 'Use TLS1.2' option is not available, kindly upgrade IE browser to the latest version



B) <u>Settings to be done on Chrome browser at client end</u>

No changes required.