Cache-Control

no-cache, no-store, must-revalidate, pre-check=0, post-check=0, max-age=0, s-maxage=0

Expires

0

PHPSESSID

no-cache

Pragma

no-cache

X-Content-Security-Policy-Report-Only

default-src 'self'; script-src 'self';

X-Content-Type-Options

nosniff

X-Frame-Options

DENY

X-XSS-Protection

1; mode=block

Strict-Transport-Security

Max-age=31536000

X-Frame-Options

SAMEORIGIN

2. "right click on my computer" go to "advance menu" then go to "environment variables" then

3. NOW CONFIGURE ON IIS SETTING.

4. NOW GO TO "HANDLER MAPPINGS" THEN GO TO "ADD MODULE MAPPING" then "see" the screenshot ppt file for setup.

5. IF CGI IS NOT CONFIGURE THEN GO TO "CONTROL PANEL" THEN GO TO "PROGRAMS AND FEATURE" THEN GO TO "TURN WINDOWS FEATURES ON OR OFF" THEN GO TO "INTERNET INFORMATION SERVICES" THEN GO TO "WORLD WIDE WEB SERVICES" THEN GO TO "APPLICATION DEVELOPMENT FEATURES" THEN "(TICK)" ON "CGI" THEN CLICK ON "OK".

To disable 3DES encryption on Windows Server 2019, you can follow these steps:

1. Open the Registry Editor: Press Windows + R, type in "regedit" and press Enter.
2. Navigate to the following key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168
3. Right-click on the key, select "Export," and save the key to a .reg file. This will serve as a backup of the registry in case you need to restore the settings later.
4. Right-click on the "Enabled" value, select "Modify," and change the value data to 0. This will disable 3DES encryption.
5. Restart the computer.

Note: Changing registry values can have serious consequences, and it's always recommended to back up your registry before making any changes.

3DES Disable steps :-

(a) Run the IIS Crypto 3.2 software & select the required TLS.

(b) After run the IIS software goto HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\ciphers only AES 256 & AES 128 folder to need. Other folder all are deleted in ciphers folder.

(c) After run the IIS software goto HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Security Providers\SCHANNEL\Hashes only SHA512 folder to need. Other folder all are deleted in hashes folder.

(d) After run the IIS software goto HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Security Providers\SCHANNEL\Keyexchange only PKC folder to need. Other folder all are deleted in keyexchange folder.

(e) After run the IIS software goto HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Security Providers\SCHANNEL\Protocols only SSL2.0, SSL3.0, TLS 1.0, TLS1.1, TLS1.2 folder. Other folder all are deleted in protocols folder.