



CONFIGURATION GUIDE

CONFIGURING SSL FOR THE LEPIDE WEB CONSOLE

Table of Contents

- 1 Introduction..... 3
- 2 Using LDSP Web Console with SSL 3
- 3 Using LDSP Web Console without SSL 12
- 4 Support 14
- 5 Trademarks 14

1 Introduction

This guide explains how to use Lepide Data Security Platform (LDSP) Web Console with and without applying an SSL certificate.

2 Using LDSP Web Console with SSL

Please follow the steps below to configure SSL with LDSP Web Console:

1. Assign a Public IP (**Example -102.50.55.12**) to Lepide Application Server If the access is to be allowed from the external network. If it is to be accessed internally, it can be on a private IP as well.
2. Go to purchased domain vendor portal (www.mytestcompany.com) and update 'A' Records to the IP of the Lepide Application Server (**102.50.55.12**)
3. Ping the domain name and verify that the IP is same as we provided in 'A' Records.
4. Generate CSR from any online CSR generator tool. (Example - www.csrgenerator.com)
5. Upload CSR to SSL vendor portal and request for SSL certificate for Apache server.
6. This SSL certificate must consist of a .CRT and .KEY file which will be used in our solution.
7. Open the File '**httpd.conf**' from the following path:

Lepide installation directory\LDSP Web Console\apache\conf

By Default, the solution is installed in the following location, unless changed by the administrator:

C:\Program Files (x86) \Lepide Data Security Platform

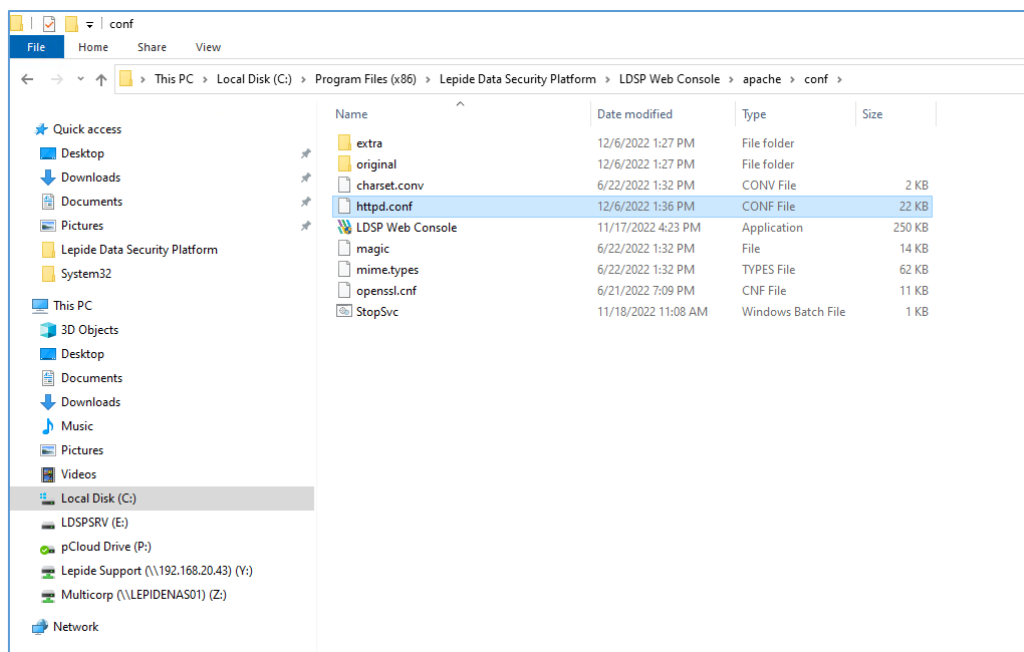
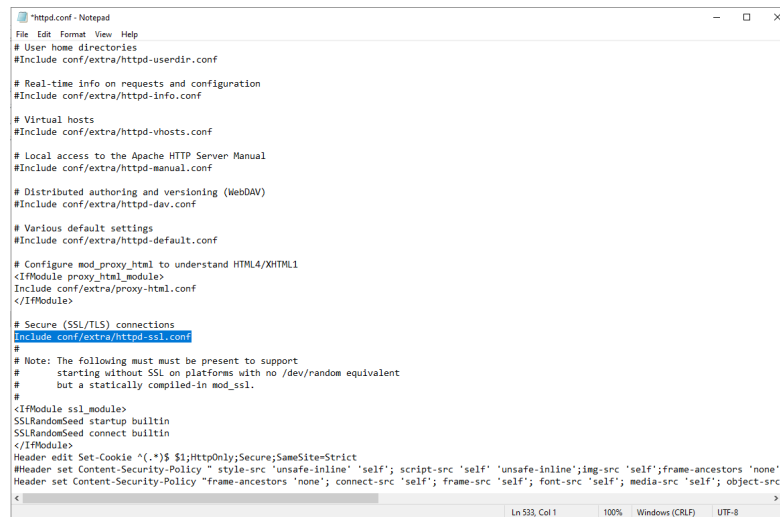


Figure 1: httpd.conf

8. Find the following lines and remove the '#' from the beginning:

- **Include conf/extra/httpd-ssl.conf**
- **LoadModule socache_dbm_module modules/mod_socache_dbm.so**
- **LoadModule ssl_module modules/mod_ssl.so**



```
*httpd.conf - Notepad
File Edit Format View Help
# User home directories
#Include conf/extra/httpd-userdir.conf

# Real-time info on requests and configuration
#Include conf/extra/httpd-info.conf

# Virtual hosts
#Include conf/extra/httpd-vhosts.conf

# Local access to the Apache HTTP Server Manual
#Include conf/extra/httpd-manual.conf

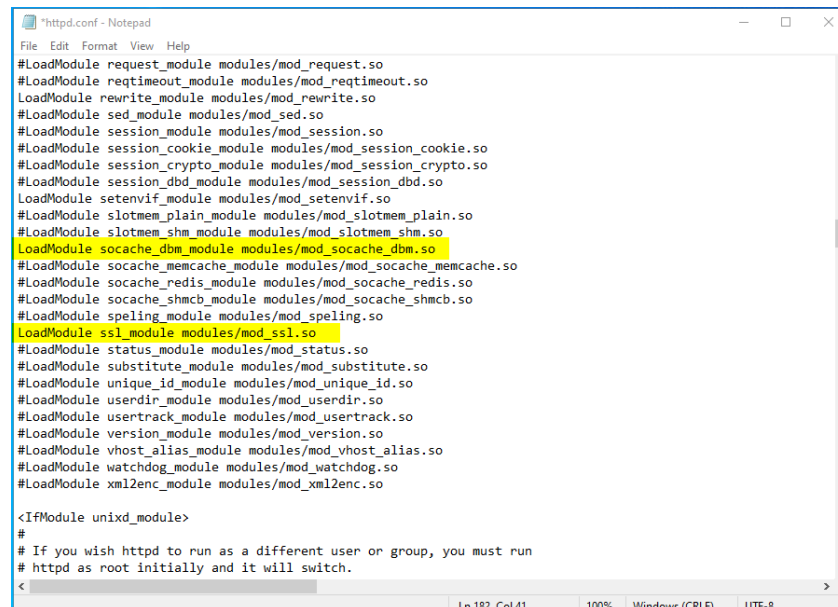
# Distributed authoring and versioning (WebDAV)
#Include conf/extra/httpd-dav.conf

# Various default settings
#Include conf/extra/httpd-default.conf

# Configure mod_proxy_html to understand HTML4/XHTML
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
</IfModule>

# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
Header edit Set-Cookie ^(.*)$ $1HttpOnly;Secure;SameSite=Strict
#Header set Content-Security-Policy " style-src 'unsafe-inline' 'self'; script-src 'self' 'unsafe-inline'; img-src 'self'; frame-ancestors 'none'
Header set Content-Security-Policy "frame-ancestors 'none'; connect-src 'self'; font-src 'self'; frame-src 'self'; media-src 'self'; object-src 'self'"
<
Ln 533, Col 1    100%    Windows (CRLF)    UTF-8
```

Figure 2: Include conf/extra/httpd-ssl.conf



```
*httpd.conf - Notepad
File Edit Format View Help
#LoadModule request_module modules/mod_request.so
#LoadModule reqtimeout_module modules/mod_reqtimeout.so
LoadModule rewrite_module modules/mod_rewrite.so
#LoadModule sed_module modules/mod_sed.so
#LoadModule session_module modules/mod_session.so
#LoadModule session_cookie_module modules/mod_session_cookie.so
#LoadModule session_crypto_module modules/mod_session_crypto.so
#LoadModule session_dbd_module modules/mod_session_dbd.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule socache_dbm_module modules/mod_socache_dbm.so
#LoadModule socache_memcache_module modules/mod_socache_memcache.so
#LoadModule socache_redis_module modules/mod_socache_redis.so
#LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule spelling_module modules/mod_spelling.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
#LoadModule unique_id_module modules/mod_unique_id.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule watchdog_module modules/mod_watchdog.so
LoadModule xml2enc_module modules/mod_xml2enc.so

<IfModule unixd_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
<
Ln 182, Col 41    100%    Windows (CRLF)    UTF-8
```

Figure 3: mod_socache_dbm.so and mod_ssl.so

- Save the file with the changes and close it.

NOTE: If the permissions are not sufficient, please save it in a different location, for example desktop, etc. and replace it here in the original location.

- Open file **httpd-ssl.conf** from the following path:

Lepide installation directory\LDSP Web Console\apache\conf\extra

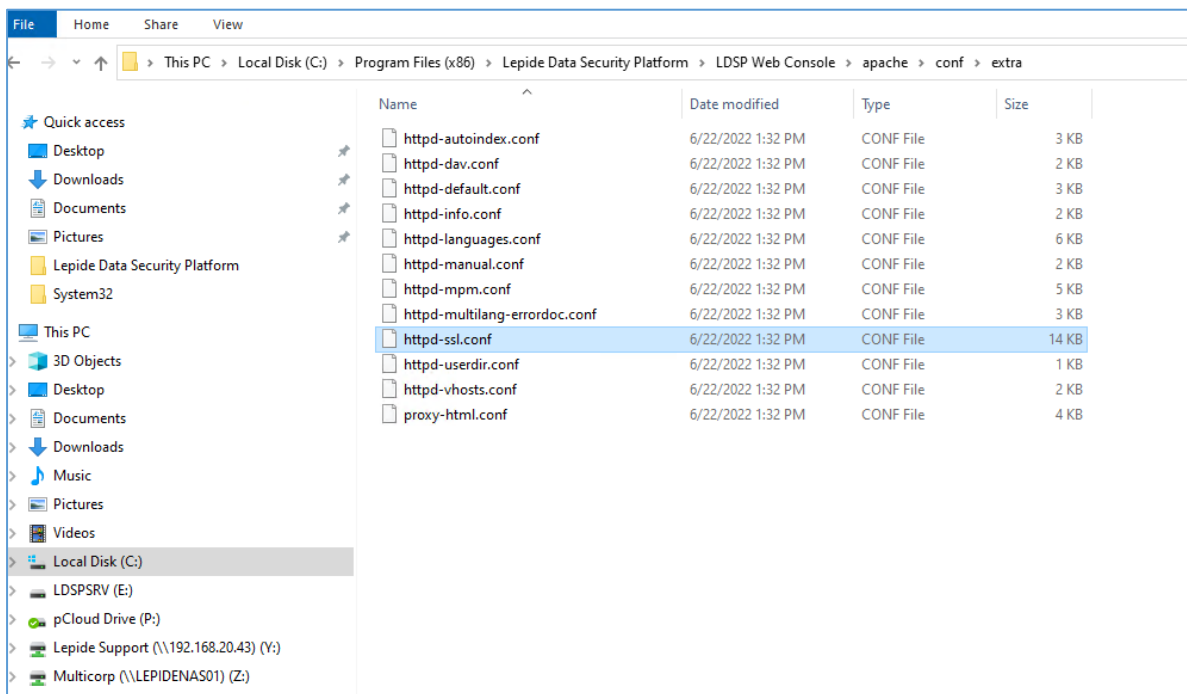


Figure 4: httpd-ssl.conf

- Update the Lepide Installation Directory path in the following lines and uncomment them by removing the # from beginning:

Previous Value:

```
#SSLSessionCache "dbm:${SRVROOT}\logs\ssl_cache"
```

```
SSLSessionCache "shmcb:${SRVROOT}\apache\logs\ssl_cache(512000)"
```

New Value:

```
SSLSessionCache "dbm:Lepide Installation directory\LDSP Web Console \logs\ssl_cache"
```

```
SSLSessionCache "shmcb:Lepide Installation directory\LDSP Web Console\apache\logs \ssl_cache  
(512000)"
```

```

File Edit Format View Help
# Disable SSLv3 by default (cf. RFC 7525 3.1.1). TLSv1 (1.0) should be
# disabled as quickly as practical. By the end of 2016, only the TLSv1.2
# protocol or later should remain in use.
SSLProtocol all -SSLv3
SSLProxyProtocol all -SSLv3

# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is an internal
# terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog builtin

# Inter-Process Session Cache:
# Configure the SSL Session Cache: First the mechanism
# to use and second the expiring timeout (in seconds).
SSLSessionCache "dbm:C:\Program Files(86)\Lepide Data Security Platform\LDSP Web Console\logs\ssl_scache"
SSLSessionCache "shmcb:C:\Program Files(86)\Lepide Data Security Platform\LDSP Web Console\logs\ssl_scache(512000)"
SSLSessionCacheTimeout 300

# OCSP Stapling (requires OpenSSL 0.9.8h or later)
#
# This feature is disabled by default and requires at least
# the two directives SSLUseStapling and SSLStaplingCache.
# Refer to the documentation on OCSP Stapling in the SSL/TLS
# How-To for more information.
#
# Enable stapling for all SSL-enabled servers:
#SSLUseStapling On

# Define a relatively small cache for OCSP Stapling using
# the same mechanism that is used for the SSL session cache
# above. If stapling is used with more than a few certificates,
# the size may need to be increased. (AH01929 will be logged.)
#SSLStaplingCache "shmcb:${SRVROOT}/logs/ssl_stapling(32768)"

# Seconds before valid OCSP responses are expired from the cache
#SSLStaplingStandardCacheTimeout 3600

# Seconds before invalid OCSP responses are expired from the cache
#SSLStaplingErrorCacheTimeout 600

```

Figure 5: ssl_scache and ssl_scache (512000)

NOTE: Please put the relevant path if the Solution is installed in any other directory/location. For example if the Solution is installed on the E drive then the path will begin with E:\

- In the same file, locate the following section and update the path of the installation directory and the values as below in the following lines:

```
<VirtualHost _default_:443>
```

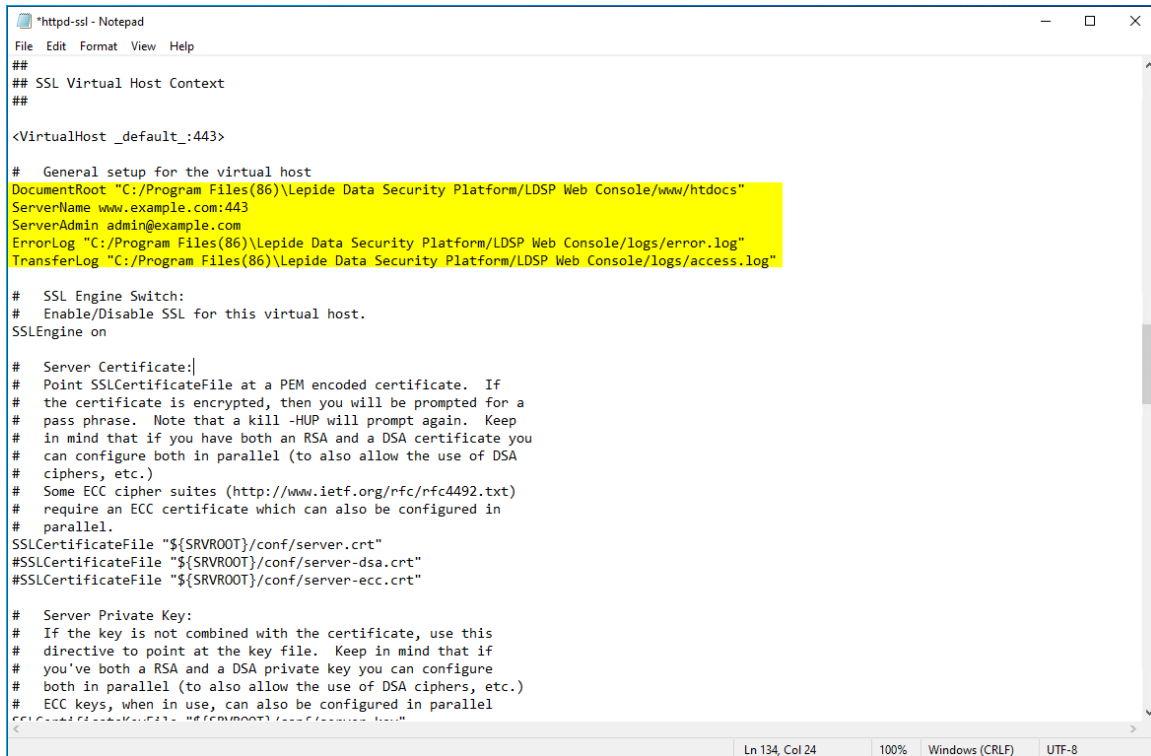
```
DocumentRoot "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console\www"
```

```
ServerName localhost:443
```

```
ServerAdmin admin@localhost
```

```
ErrorLog "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console \apache\logs\error.log"
```

```
TransferLog "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console \apache\logs\access.log"
```



```

httpd-ssl - Notepad
File Edit Format View Help
##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>

# General setup for the virtual host
DocumentRoot "C:/Program Files(86)\Lepide Data Security Platform/LDSP Web Console/www/htdocs"
ServerName www.example.com:443
ServerAdmin admin@example.com
ErrorLog "C:/Program Files(86)\Lepide Data Security Platform/LDSP Web Console/logs/error.log"
TransferLog "C:/Program Files(86)\Lepide Data Security Platform/LDSP Web Console/logs/access.log"

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "${SRVROOT}/conf/server.crt"
#SSLCertificateFile "${SRVROOT}/conf/server-dsa.crt"
#SSLCertificateFile "${SRVROOT}/conf/server-ecc.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
# with RSA keys.
SSLPrivateKeyFile "${SRVROOT}/conf/server.key"

```

Figure 6: VirtualHost Settings

- Put the .CRT and .KEY file in root of the LDSP Web Console folder and update the path of the .CRT and .KEY file in the following lines in the same file httpd-ssl.conf:

Previous Value:

SSLCertificateFile "\${SRVROOT}/conf/server.crt"

SSLCertificateKeyFile "\${SRVROOT}/conf/server.key"

New Value:

SSLCertificateFile "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console\certificate.crt"

SSLCertificateKeyFile "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console\Private.key"

NOTE: These lines are uncommented by default. Please do not modify any commented line with a similar name. Please see the screenshot below:

```
<VirtualHost _default_:443>

# General setup for the virtual host
DocumentRoot "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/www/htdocs"
ServerName www.example.com:443
ServerAdmin admin@example.com
ErrorLog "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/logs/error.log"
TransferLog "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/logs/access.log"

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/Certificate.crt"
#SSLCertificateFile "${SRVROOT}/conf/server-dsa.crt"
#SSLCertificateFile "${SRVROOT}/conf/server-ecc.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/Private.key"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-dsa.key"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-ecc.key"

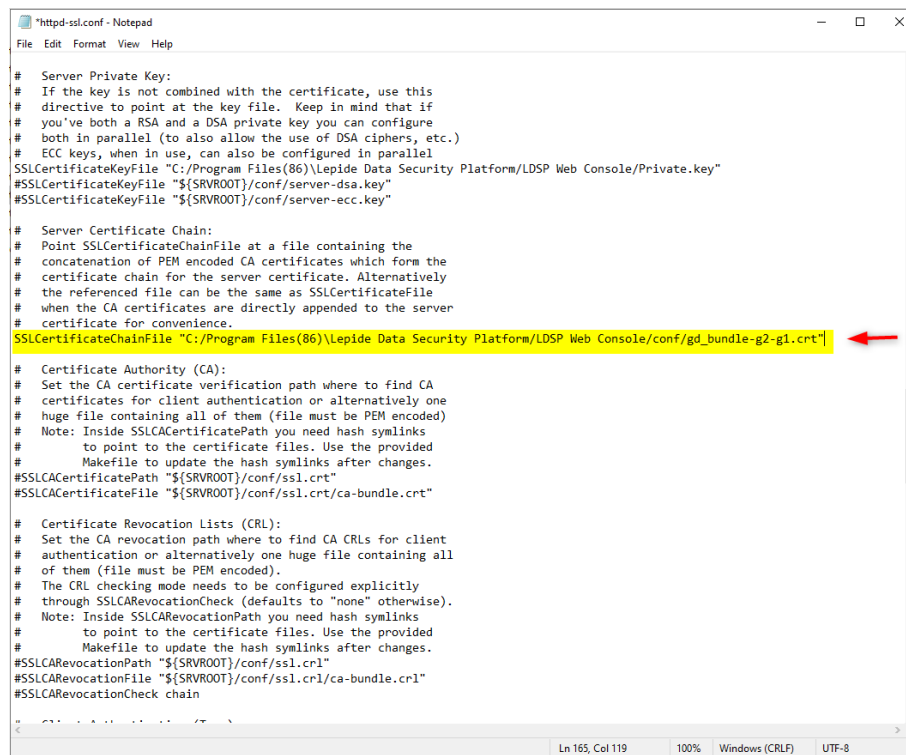
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
```

Figure 7: SSLCertificate Settings

14. Some vendors like Godaddy and Digicert might provide a **Server Certificate Chain** file as well, which must be kept in the same location as the .CRT and .KEY file. Please locate the section **Server Certification Chain** and update the path in the following line to the Certificate Chain file:

```
SSLCertificateChainFile "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console
\certificate_gd_bundle-g2-g1.crt"
```

NOTE: This line is commented by default, so please uncomment it by removing the '#' from the beginning



```

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/Private.key"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-dsa.key"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-ecc.key"

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
SSLCertificateChainFile "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/conf/gd_bundle-g2-g1.crt"

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
# Note: Inside SSLCACertificatePath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
#SSLCACertificatePath "${SRVROOT}/conf/ssl.crt"
#SSLCACertificateFile "${SRVROOT}/conf/ssl.crt/ca-bundle.crt"

# Certificate Revocation Lists (CRL):
# Set the CA revocation path where to find CA CRLs for client
# authentication or alternatively one huge file containing all
# of them (file must be PEM encoded).
# The CRL checking mode needs to be configured explicitly
# through SSLCAREvocationCheck (defaults to "none" otherwise).
# Note: Inside SSLCAREvocationPath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
#SSLCAREvocationPath "${SRVROOT}/conf/ssl.crl"
#SSLCAREvocationFile "${SRVROOT}/conf/ssl.crl/ca-bundle.crl"
#SSLCAREvocationCheck chain

```

Figure 8: SSLCertificate Settings

15. Scroll to the bottom of the file now and find the section **SSL Engine Options**. Now update the LDSP Web Console path in the following lines:

```

<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
<\FilesMatch>
<Directory "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console \apache\cgi-bin">
    SSLOptions +StdEnvVars
<\Directory>

```

```

# SSL Engine Options:
# Set various options for the SSL engine.
# o FakeBasicAuth:
#   Translate the client X.509 into a Basic Authorisation. This means that
#   the standard Auth/DBMAuth methods can be used for access control. The
#   user name is the 'one line' version of the client's X.509 certificate.
#   Note that no password is obtained from the user. Every entry in the user
#   file needs this password: 'xxj31ZMTZzkVA'.
# o ExportCertData:
#   This exports two additional environment variables: SSL_CLIENT_CERT and
#   SSL_SERVER_CERT. These contain the PEM-encoded certificates of the
#   server (always existing) and the client (only existing when client
#   authentication is used). This can be used to import the certificates
#   into CGI scripts.
# o StdEnvVars:
#   This exports the standard SSL/TLS related 'SSL_*' environment variables.
#   Per default this exportation is switched off for performance reasons,
#   because the extraction step is an expensive operation and is usually
#   useless for serving static content. So one usually enables the
#   exportation for CGI and SSI requests only.
# o StrictRequire:
#   This denies access when "SSLRequireSSL" or "SSLRequire" applied even
#   under a "Satisfy any" situation, i.e. when it applies access is denied
#   and no other module can change it.
# o OptRenegotiate:
#   This enables optimized SSL connection renegotiation handling when SSL
#   directives are used in per-directory context.
#SSLOptions +FakeBasicAuth+ExportCertData+StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory "C:/Program Files(86)/Lepide Data Security Platform/LDSP Web Console/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>

# SSL Protocol Adjustments:
# The safe and default but still SSL/TLS standard compliant shutdown
# approach is that mod_ssl sends the close notify alert but doesn't wait for

```

Figure 9: SSL Engine Options

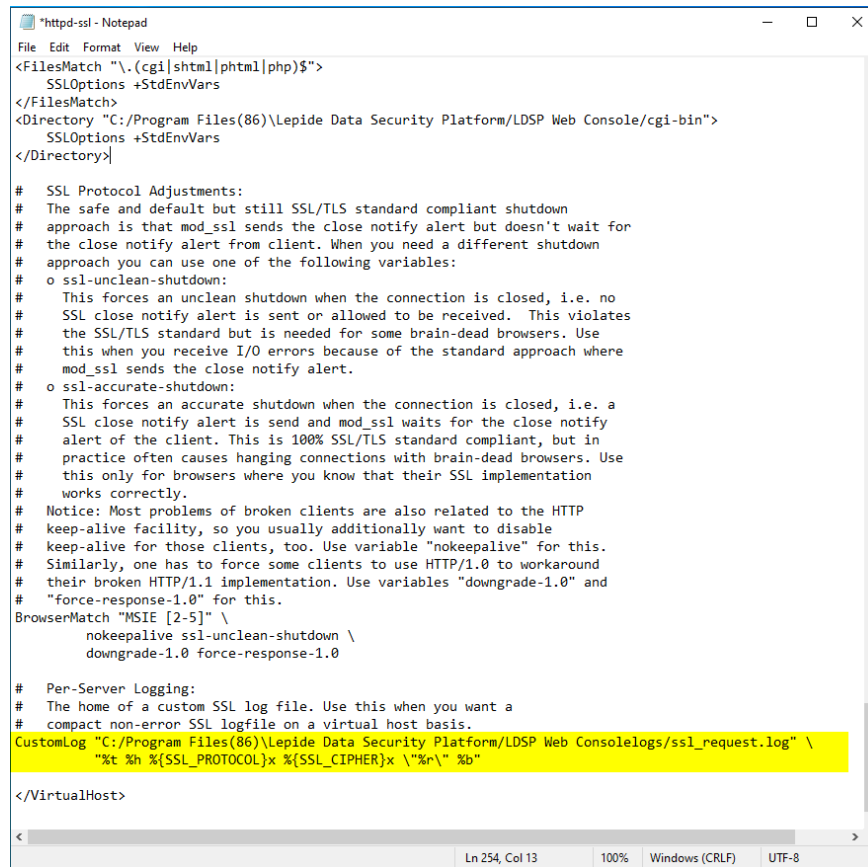
16. Similarly, update the LDSP Web Console folder path in the following Custom Log line as well:

CustomLog "C:\Program Files (x86)\Lepide Data Security Platform\LDSP Web Console
 \apache\logs\ssl_request.log"

```

"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
<\VirtualHost>

```



```

*httpd-ssl - Notepad
File Edit Format View Help
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory "C:/Program Files(86)\Lepide Data Security Platform/LDSP Web Console/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>

# SSL Protocol Adjustments:
# The safe and default but still SSL/TLS standard compliant shutdown
# approach is that mod_ssl sends the close notify alert but doesn't wait for
# the close notify alert from client. When you need a different shutdown
# approach you can use one of the following variables:
# o ssl-unclean-shutdown:
# This forces an unclean shutdown when the connection is closed, i.e. no
# SSL close notify alert is sent or allowed to be received. This violates
# the SSL/TLS standard but is needed for some brain-dead browsers. Use
# this when you receive I/O errors because of the standard approach where
# mod_ssl sends the close notify alert.
# o ssl-accurate-shutdown:
# This forces an accurate shutdown when the connection is closed, i.e. a
# SSL close notify alert is sent and mod_ssl waits for the close notify
# alert of the client. This is 100% SSL/TLS standard compliant, but in
# practice often causes hanging connections with brain-dead browsers. Use
# this only for browsers where you know that their SSL implementation
# works correctly.
# Notice: Most problems of broken clients are also related to the HTTP
# keep-alive facility, so you usually additionally want to disable
# keep-alive for those clients, too. Use variable "nokeepalive" for this.
# Similarly, one has to force some clients to use HTTP/1.0 to workaround
# their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
# "force-response-1.0" for this.
BrowserMatch "MSIE [2-5]" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0

# Per-Server Logging:
# The home of a custom SSL log file. Use this when you want a
# compact non-error SSL logfile on a virtual host basis.
CustomLog "C:/Program Files(86)\Lepide Data Security Platform/LDSP Web Console/logs/ssl_request.log" \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

</VirtualHost>

```

Figure 10: Custom Log Path

17. Save the file with the changes in the same location
18. Restart LDSPapache Service as shown below:

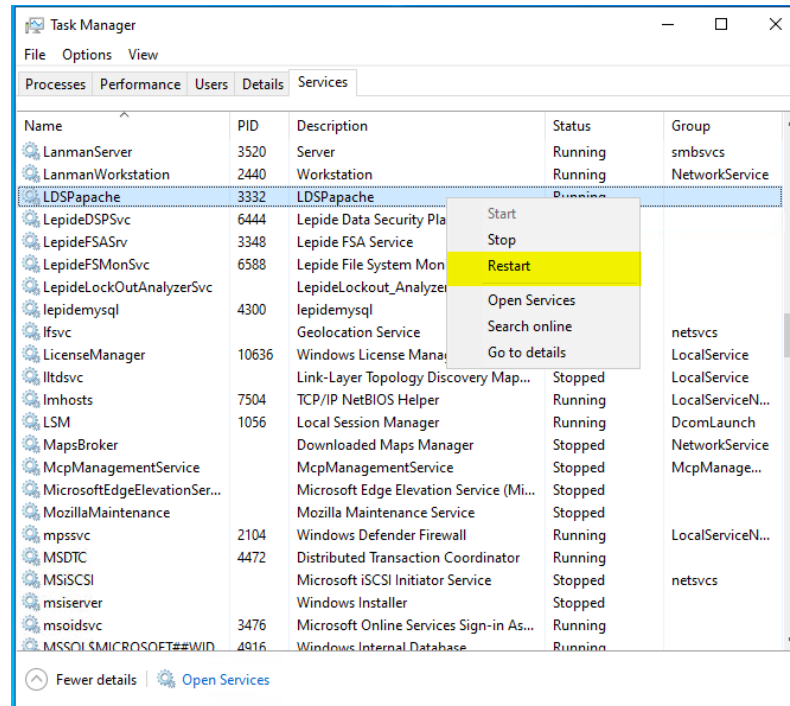
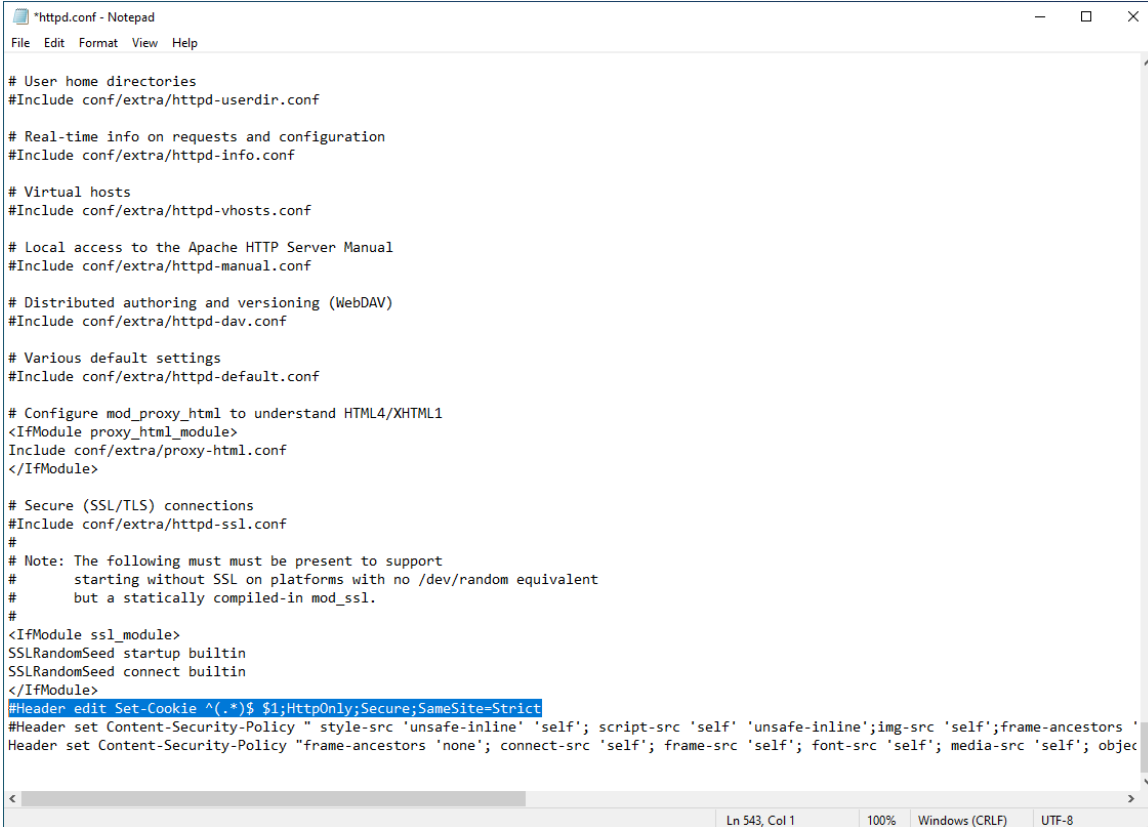


Figure 11: LDSPapache Service Restart

3 Using LDSP Web Console without SSL

1. Open the File '**httpd.conf**' from the path '**Lepide installation directory folder\LDSP Web Console\apache\conf**'
2. Go to the bottom of the file, find the following line, and add a '#' at the beginning:

#Header edit Set-Cookie ^(.*)\$ \$1;HttpOnly;Secure;SameSite=Strict



```
*httpd.conf - Notepad
File Edit Format View Help

# User home directories
#Include conf/extra/httpd-userdir.conf

# Real-time info on requests and configuration
#Include conf/extra/httpd-info.conf

# Virtual hosts
#Include conf/extra/httpd-vhosts.conf

# Local access to the Apache HTTP Server Manual
#Include conf/extra/httpd-manual.conf

# Distributed authoring and versioning (WebDAV)
#Include conf/extra/httpd-dav.conf

# Various default settings
#Include conf/extra/httpd-default.conf

# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
</IfModule>

# Secure (SSL/TLS) connections
#Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
#Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure;SameSite=Strict
#Header set Content-Security-Policy " style-src 'unsafe-inline' 'self'; script-src 'self' 'unsafe-inline';img-src 'self';frame-ancestors '
Header set Content-Security-Policy "frame-ancestors 'none'; connect-src 'self'; frame-src 'self'; font-src 'self'; media-src 'self'; objec

Ln 543, Col 1    100%    Windows (CRLF)    UTF-8
```

Figure 12: #Header edit Set-Cookie

3. Save the file with the changes in the same location.
4. Restart the **LDSPapache** service.

4 Support

If you are facing any issues whilst installing, configuring, or using the solution, you can connect with our team using the contact information below.

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit <https://www.lepide.com/contactus.html> to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit <https://www.lepide.com/data-security-platform/>.

5 Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.