



**NETENG Assignment 2**  
**ENGR3821**  
**Network Engineering**  
**Website LDAP Authentication**

**15/06/2019**

## Consent

I, the author, give consent to ENGR3821 Topic Staff to distribute this document for the purposes of peer marking and assessment.

## Table of Contents

Consent .....	i
Table of Contents.....	i
List of Tables .....	ii
Table of Figures .....	ii
Definitions.....	ii
0 Introduction.....	1
0.0 Revision History.....	1
0.1 Purpose.....	1
0.2 Scope .....	1
1 Required Software .....	1
1.0 Overview .....	1
1.1 LDAP System.....	2
1.2 Software Dependencies .....	3
1.3 Licences.....	3
2 Deployment Procedure.....	4
2.0 Preliminaries.....	4
2.1 LDAP Server.....	4
2.1.1 slapd installation .....	4
2.1.2 LDIF Modifications and import.....	5
2.2 Authentication Configuration.....	5
2.2.1 Administrator Portal.....	5
2.2.2 tcpdump Testing.....	8
2.3 Encryption Implementation.....	10
2.3.1 Creating the Cryptographic Keys.....	10
2.3.2 Configuring SSL and Apache .....	10
2.3.3 Redirect Port 80 to 443 .....	12
2.3.4 Enabling Changes .....	13
2.3.5 Testing Encryption.....	14
3 Bibliography .....	15
4 Appendices.....	15
Appendix A – Sample Dokuwiki Configuration File.....	15

## List of Tables

Table 1 - Author and Revision History.....	1
Table 2 - LDAP server alternatives [1-5] .....	2
Table 3 - Packages required for web server and wiki installation .....	3
Table 4 - New licences required .....	3

## Table of Figures

Figure 1 - Initial admin password request.....	4
Figure 2 - Positive systemctl status on slapd .....	4
Figure 3 - Access the admin controls on the top right of the page .....	6
Figure 4 - Administrator portal .....	6
Figure 5 - Extension manager page .....	6
Figure 6 - Plugin Authentication block.....	7
Figure 7 - Configure the plugin to point to the LDAP server .....	7
Figure 8 - Do not use the in-built TLS option .....	8
Figure 9 - An example successful login display .....	9
Figure 10 - Example 1 of default-ssl.conf .....	11
Figure 11 - Example 2 of default-ssl.conf .....	11
Figure 12 - Redirect traffic over SSL .....	12
Figure 13 - Apache Full profiles active .....	12
Figure 14 - Components enables and apache2ctl test returning positive.....	13
Figure 15 - Self-signed certificate warning .....	14
Figure 16 - Inspection of Certificate .....	14

## Definitions

Term	Definition
CDDL	Common Development and Distribution Licence
HSTS	(Header) Strict Transport Security
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over S[SL]
IP	Internet Protocol
IPA	Identity, Policy, Audit
LDAP	Lightweight Directory Access Protocol
MSAD	MicroSoft Active Directory
RHEL	Red Hat Enterprise Linux
RSA	Rivest–Shamir–Adleman [Algorithm]
SSL	Secure Socket Layer
TLS	Transport Layer Security
UCS	Univention Corporate Server
UFW	Uncomplicated FireWall
VM	Virtual Machine

## 0 Introduction

### 0.0 Revision History

*Table 1 - Author and Revision History*

Revision No.	Author	Date	Details
0	<REDACTED1>	15/06/19	Initial Documentation
1	<REDACTED1>	24/06/19	Formatting

### 0.1 Purpose

This document is intended to be a guide on the process to set up LDAP authentication on an Apache2 Web Server running Dokuwiki wiki software on an Ubuntu 18.04 VM which had installation documentation detailed in Assignment 1. Furthermore, this document will outline the steps required to encrypt the authentication process over TLS/SSL and ensure unencrypted access is not available.

### 0.2 Scope

The setup of the LDAP authentication mechanism and the TLS/SSL encryption and other features are to be extended onto an installation detailed by Assignment 1.

## 1 Required Software

### 1.0 Overview

On top of the wiki and web server installation, the authentication mechanism requires an LDAP backend, and interface between the LDAP server and the wiki, and the software that will implement SSL/TLS.

## 1.1 LDAP System

It is required that the backend software that will be used is OpenLDAP. However, this section will identify and list other alternatives that may be applicable for other use-cases.

*Table 2 - LDAP server alternatives [1-5]*

Software	Licence	Developer
Active Directory	Proprietary	Microsoft
OpenLDAP	OpenLDAP Public Licence <a href="http://www.openldap.org/software/release/license.html">http://www.openldap.org/software/release/license.html</a>	Kurt Zeilenga + (slapd developers)
Apache Directory Server	Apache Licence 2.0	Apache Software Foundation
389 Directory Server	GPLv3	Red Hat
OpenDJ	CDDL	OpenDJ Community

The following list shows community-tested LDAP software successfully integrated into Dokuwiki[6]:

- OpenLDAP
- MSAD
- Lotus Domino
- Open Directory (Mac OSX Server)
- UCS
- Oracle Internet Directory
- Novell eDirectory
- TinyLDAP
- Apache Directory
- FreeIPA
- RHEL Enterprise IPA

As stated in the Assignment specification, the required software to be used is an OpenLDAP distribution.

## 1.2 Software Dependencies

The following table shows the dependencies inherited from the previous installation in Assignment 1[7]:

*Table 3 - Packages required for web server and wiki installation*

Package	Version	Source
Oracle VirtualBox	6.0.4	<a href="https://www.virtualbox.org/">https://www.virtualbox.org/</a>
Linux Ubuntu	18.04	<a href="https://www.ubuntu.com/download/desktop">https://www.ubuntu.com/download/desktop</a>
Apache	2.4.29	sudo apt-get install apache2
PHP	7.2.15-0ubuntu0.18.04.2	sudo apt-get php
libapache2-mod-php	-	sudo apt-get libapache2-mod-php
php-xml	-	sudo apt-get php-xml
DokuWiki	2018-04-22b "Greebo"	<a href="https://download.dokuwiki.org/">https://download.dokuwiki.org/</a>
Web Browser	Recent	Any recent web browser
Plugins	Optional	DokuWiki Distr. Page or Apache Distr. Page

Additional Dependencies necessary for this installation are tabulated below.

*Table 4 - New licences required*

Package	Version	Source
slapd (OpenLDAP)	Apr 10 2019 12:53:11	sudo apt-get slapd

## 1.3 Licences

Inherited from the previous installation of the web server and the wiki, the required licences are:

1. GPL2
2. Apache Licence v2

OpenLDAP is the only software that extends from the previous installation as the SSL/TLS encryption setup is contained entirely within the Apache2 Licence.

3. OpenLDAP Public License 2.8

This describes all the licences required to complete the installation.

## 2 Deployment Procedure

### 2.0 Preliminaries

Ensure that the Apache2 server, Dokuwiki and any other previous dependencies and configurations are installed as per Assignment 1 and Table 3 before continuing. The user should have sudo privileges and be non-root. Also, to be safe, first update the apt database.

```
sudo apt-get update
```

### 2.1 LDAP Server

#### 2.1.1 slapd installation

The OpenLDAP distribution can be installed from the `slapd` package using `apt-get`. The `-y` eliminates the need for operator confirmation .

```
sudo apt-get -y slapd
```

The installation of `slapd` will ask for an initial LDAP administrator password.



Figure 1 - Initial admin password request

Next, allow the LDAP daemon through the firewall `ufw` and check the correct status of the `slapd` installation and the firewall.

```
sudo ufw allow ldap
sudo systemctl status ufw
sudo systemctl status slapd
```

A positive result on `systemctl` status checks should resemble the following figure.

```
student@neteng:/var/www/html/dokuwiki/conf$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Mon 2019-06-10 18:49:38 ACST; 27s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 3 (limit: 2319)
   CGroup: /system.slice/slapd.service
            └─2335 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap

Jun 10 18:49:38 neteng systemd[1]: Starting LSB: OpenLDAP standalone server (Lig
Jun 10 18:49:38 neteng slapd[2328]: * Starting OpenLDAP slapd
Jun 10 18:49:38 neteng slapd[2334]: @(#) $OpenLDAP: slapd (Ubuntu) (Apr 10 2019
                Debian OpenLDAP Maintainers <pkg-ope
Jun 10 18:49:38 neteng slapd[2335]: slapd starting
Jun 10 18:49:38 neteng slapd[2328]: ...done.
Jun 10 18:49:38 neteng systemd[1]: Started LSB: OpenLDAP standalone server (Ligh
```

Figure 2 - Positive systemctl status on slapd

If the status check for `slapd` returns negative, simply enable the service.

```
sudo systemctl start slapd
sudo systemctl enable slapd
sudo systemctl status slapd
```

### 2.1.2 LDIF Modifications and import

Using the LDIF file created in ENGR3821 Workshop Unit 2[8], the modified version should be inserted into the newly created LDAP database.

The modifications include:

- 1 Populating the user entries with `userPasswords`. For this installation example, every user will have the password `12345`. Administrators should consider enforcing stronger passwords.
- 2 Change the domain and corresponding `dn` entries to the desired domain name. For this example, the domain will remain at `dc=nodomain`.

In the directory containing the ldif file to be inserted, use the following command with an optional `-v` argument, assuming the administrator `cn` is `cn=admin`.

```
sudo ldapadd -x -W -v -c -D cn=admin,dc=nodomain -f ldiffile.ldif
```

Verify that the `ldapadd` worked by using `ldapsearch`. For example:

```
ldapsearch -o ldif-wrap=no -x -LLL -H -v ldap:/// -b dc=nodomain \* >
ldapentities.log
```

## 2.2 Authentication Configuration

### 2.2.1 Administrator Portal

Dokuwiki supports LDAP authentication backends through installing plugins. If the setup instructions were followed correctly from Assignment 1, the plugin should already be installed. If not, the following steps will detail it.

Firstly, log in using the administrator account and navigate to the Admin settings when connected to the wiki at `aaa.bbb.ccc.ddd` (the web server's IP address).



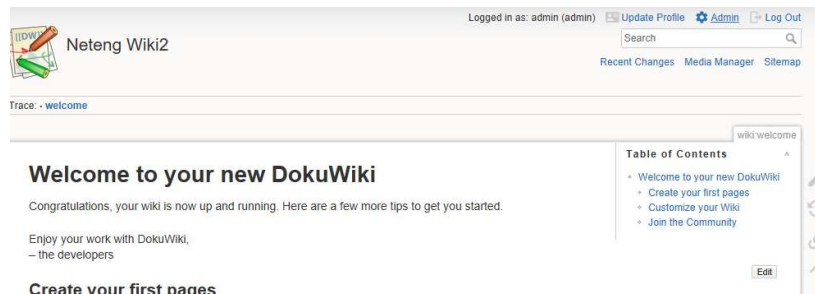


Figure 3 - Access the admin controls on the top right of the page

Next, access the extension manager and enable the “LDAP Auth Plugin” plugin. Ensure the correct permissions were set as per Assignment 1. If they were set up correctly, the “Extension directory is not writable” message can be safely ignored.

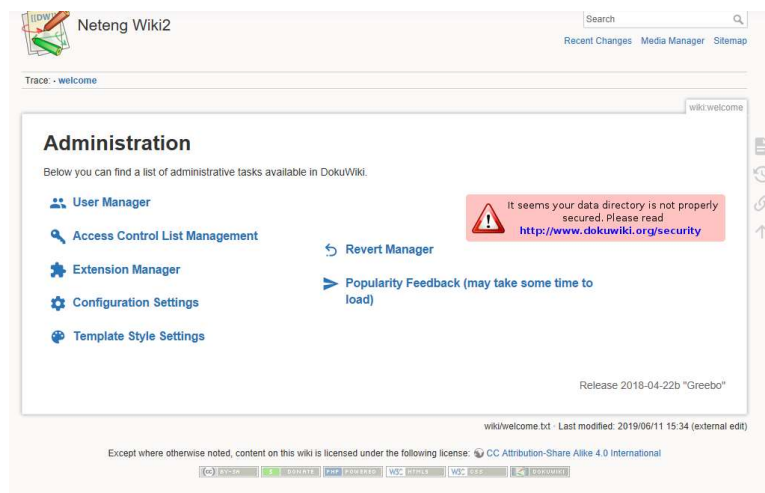


Figure 4 - Administrator portal

## Extension Manager

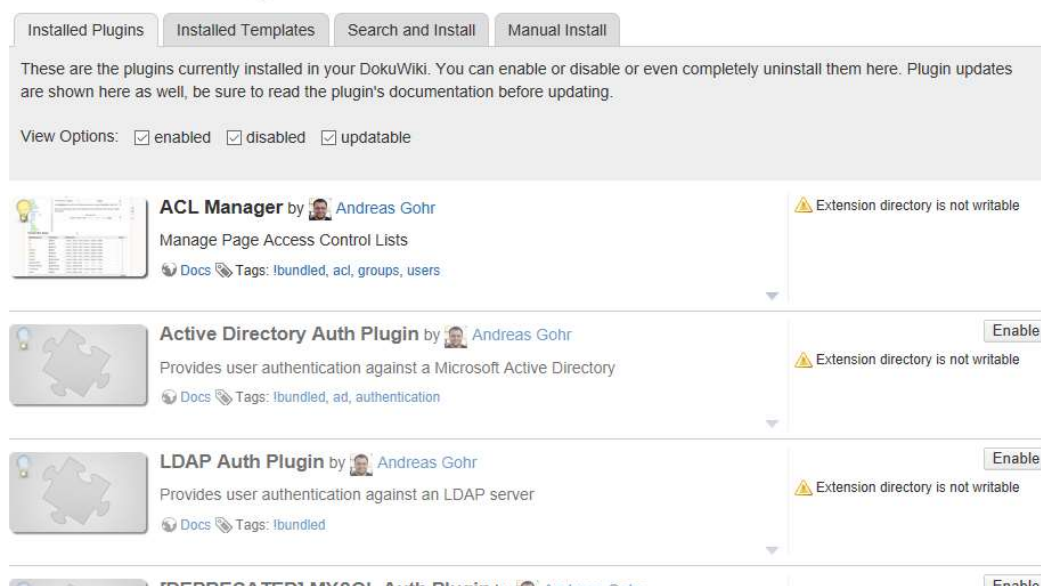
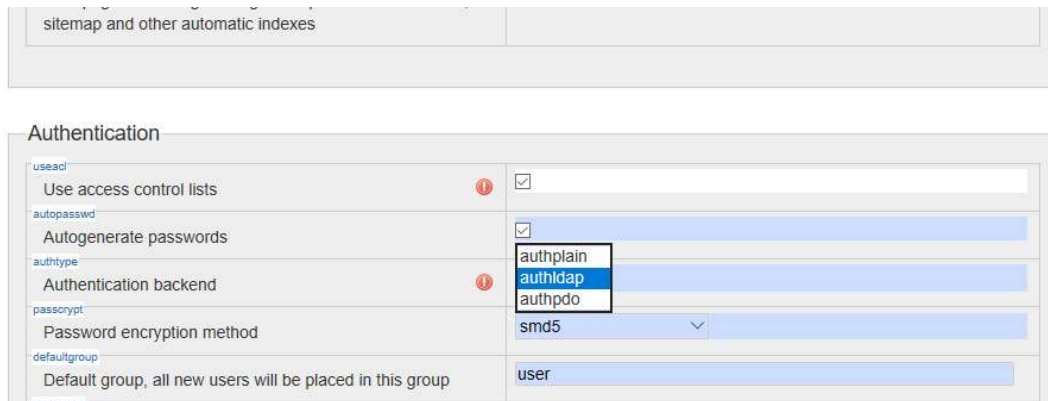


Figure 5 - Extension manager page

Navigate back to the administrator portal after enabling the extension and access the “Configuration Settings” menu. Under the Authentication Block, change the Authentication Backend to `authldap`.



The screenshot shows the 'Authentication' configuration block. The 'Authentication backend' dropdown is open, with 'authldap' selected. Other settings include 'Use access control lists' (checked), 'Autogenerate passwords' (checked), 'Password encryption method' (smd5), and 'Default group' (user).

Figure 6 - Plugin Authentication block

Ensure that the authentication plugin points to port 389 on the LDAP server’s IP address and that the user tree and group trees are set up accordingly. Ensure that your schema in the LDIF file has groups implemented if a non-top level group filter is specified. Ensure that LDAPv3 is set.

## Plugin



The screenshot shows the 'Authldap' configuration block. It contains several settings with red error icons indicating issues:

- `plugin=authldap=server`: Your LDAP server. Either hostname (localhost) or full qualified URL (ldap://server.tld:389). Error icon.
- `plugin=authldap=port`: LDAP server port if no full URL was given above. Error icon.
- `plugin=authldap=usertree`: Where to find the user accounts. Eg. ou=People, dc=server, dc=tld. Error icon.
- `plugin=authldap=grouptree`: Where to find the user groups. Eg. ou=Group, dc=server, dc=tld. Error icon.
- `plugin=authldap=userfilter`: LDAP filter to search for user accounts. Eg. (&(uid={user})(objectClass=posixAccount)). Error icon.
- `plugin=authldap=groupfilter`: LDAP filter to search for groups. Eg. (&(objectClass=posixGroup)(|(gidNumber={gid})(memberUID={user}))). Error icon.
- `plugin=authldap=version`: The protocol version to use. You may need to set this to 3. Error icon.

Figure 7 - Configure the plugin to point to the LDAP server

There are errors in Figure 7. The groupFilter and userGroupTree should be `dc=nodomain` in the example case as the directory tree does not have groups defined in the schema. Your implementation may choose to implement something like `posixGroup`. A sample configuration file can be found in the Appendices detailing the expected contents of `/var/www/html/dokuwiki/conf/info.php`.

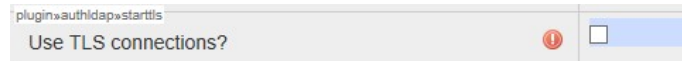


Figure 8 - Do not use the in-built TLS option

Ensure that the Dokuwiki implementation of TLS is not enabled. Logout of the admin account.

### 2.2.2 tcpdump Testing

Test the login functionality by using one of the populated users and passwords. e.g.

Username: `mw3@explosiveinvestments.com.au`

Password: `12345`

Optionally, use tcpdump to analyse the network traffic.

```
sudo tcpdump -i enp0s8 -nn -s0 -vv > tcpd.txt
```

Where `enp0s8` is the name of the network interface that the web server is facing.

Searching the output for the authentication inputs should return text similar to the following:

```
sectok=&id=wiki%3Awelcome&do=login&u=mw3%40explosiveinvestments.com.au&p=12345[!http]
13:34:08.983129 IP (tos 0x0, ttl 64, id 45729, offset 0, flags [DF], proto TCP (6), length 40)
  192.168.1.111.80 > 192.168.1.115.51526: Flags [.], cksum 0x844d (incorrect -> 0x2325), seq
  1, ack 725, win 240, length 0
13:34:09.022783 IP (tos 0x0, ttl 64, id 45730, offset 0, flags [DF], proto TCP (6), length 617)
  192.168.1.111.80 > 192.168.1.115.51526: Flags [P.], cksum 0x868e (incorrect -> 0xff35), seq
  1:578, ack 725, win 240, length 577: HTTP, length: 577
  HTTP/1.1 302 Found
  Date: Tue, 11 Jun 2019 04:04:08 GMT
  Server: Apache/2.4.29 (Ubuntu)
  Vary: Cookie
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Set-Cookie:
  DW84669e0b736a85c6eeda0cf5b0a2b382=bXczQGv4cGxvc2l2ZWludmVzdG1lbnRzLmNvbS5hdQ%3D%3D%7C0%7Cs%2F
  lAK161C4Q3pj9nJmXG7nke9fTzkdsPn1UNFG%2FfSwQ%3D; path=/dokuwiki/; HttpOnly
  Location: http://192.168.1.111/dokuwiki/doku.php?id=wiki:welcome
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8
```

Alternatively, an unsuccessful login attempt should result in a HTTP:403 Login Failed.

```
sectok=&id=wiki%3Awelcome&do=login&u=mw3%40explosiveinvestments.com.au&p=12346[!http]
13:43:55.049518 IP (tos 0x0, ttl 64, id 53525, offset 0, flags [DF], proto TCP (6), length 40)
  192.168.1.111.80 > 192.168.1.115.51698: Flags [.], cksum 0x844d (incorrect -> 0x218c), seq
1, ack 725, win 240, length 0
13:43:55.152305 IP (tos 0x0, ttl 64, id 53526, offset 0, flags [DF], proto TCP (6), length
6437)
  192.168.1.111.80 > 192.168.1.115.51698: Flags [P.], cksum 0x9d4a (incorrect -> 0x38b3),
seq 1:6398, ack 725, win 240, length 6397: HTTP, length: 6397
  HTTP/1.1 403 Login failed
  Date: Tue, 11 Jun 2019 04:13:55 GMT
  Server: Apache/2.4.29 (Ubuntu)
  Vary: Cookie
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Set-Cookie: DW84669e0b736a85c6eeda0cf5b0a2b382=deleted; expires=Thu, 01-Jan-1970
00:00:01 GMT; Max-Age=0; path=/dokuwiki/; HttpOnly
  X-UA-Compatible: IE=edge,chrome=1
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=utf-8
```

A successfully logged in user should have their email address displayed on the top right of the screen. For example:



Figure 9 - An example successful login display

---

## 2.3 Encryption Implementation

To implement SSL over HTTP (HTTPS) the web server must distribute a digital certificate to the client. This certificate can be purchased or self-signed[9]. The process of creating a self-signed digital certificate and redirecting all http traffic to port 443 will be detailed below.

### 2.3.1 Creating the Cryptographic Keys

Install openssl with apt-get.

```
sudo apt-get -y openssl
```

Generate a new X.509 certificate and a 2048 bit RSA key and save it to the directories as shown by the following command[9]. The cert will be valid for 365 days.

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout  
/etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
```

Enter the information required to be on the cert when prompted.

### 2.3.2 Configuring SSL and Apache

A file called ssl-params.conf must be created to specify the SSL configuration settings such as disabling HSTS and preloading functionality. A suggested configuration is adapted from Elst[10]. Create a file with the following contents and save it as: /etc/apache2/conf-available/ssl-params.conf

```
SSLCipherSuite ECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH  
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1  
SSLHonorCipherOrder On  
# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"  
Header always set X-Frame-Options DENY  
Header always set X-Content-Type-Options nosniff  
# Requires Apache >= 2.4  
SSLCompression off  
SSLUseStapling on  
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"  
# Requires Apache >= 2.4.11  
SSLSessionTickets Off
```

Use a text editor to modify `/etc/apache2/sites-available/default-ssl.conf` such that the following lines exist between the `<VirtualHost _default_:443>` and `</VirtualHost>` elements where `admin@neteng.com` is the administrator email address and `aaa.bbb.ccc.ddd` is the address of the web server:

```
ServerAdmin admin@neteng.com
ServerName aaa.bbb.ccc.ddd

SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile   /etc/ssl/private/apache-selfsigned.key
```

```
GNU nano 2.9.3 /etc/apache2/sites-available/default-ssl.conf Modified
IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin admin@neteng.com
    ServerName 192.168.1.111

    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notices
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For examS
G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Figure 10 - Example 1 of default-ssl.conf

```
GNU nano 2.9.3 /etc/apache2/sites-available/default-ssl.conf Modified

# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

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

# A self-signed (snakeoil) certificate can be created by instS
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, onS
# SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile   /etc/ssl/private/apache-selfsigned.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
File Name to Write: /etc/apache2/sites-available/default-ssl.conf
^G Get Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend ^T To Files
```

Figure 11 - Example 2 of default-ssl.conf



### 2.3.3 Redirect Port 80 to 443

Modify the file `/etc/apache2/sites-available/000-default.conf` and add a redirect directive in the `<VirtualHost>` element to redirect HTTP traffic to HTTPS. Add a permanent modifier when testing is complete. For example: `Redirect permanent "/" "https://* "`.

```
GNU nano 2.9.3 /etc/apache2/sites-available/000-default.conf Modified

CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

Redirect "/" "https://192.168.1.111"

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Figure 12 - Redirect traffic over SSL

Change the `ufw` settings to allow the “Full” Apache profiles through and thus, allow HTTPS.

```
sudo ufw allow 'Apache Full'
sudo ufw delete allow 'Apache'
```

A `ufw status` check should return the following output.

```
student@neteng:~/work$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
  OpenLDAP LDAP
  OpenLDAP LDAPS
student@neteng:~/work$ sudo ufw allow 'Apache Full'
Rule added
Rule added (v6)
student@neteng:~/work$ sudo ufw status
Status: active

To Action From
--
389 ALLOW Anywhere
Apache Full ALLOW Anywhere
389 (v6) ALLOW Anywhere (v6)
Apache Full (v6) ALLOW Anywhere (v6)
student@neteng:~/work$
```

Figure 13 - Apache Full profiles active

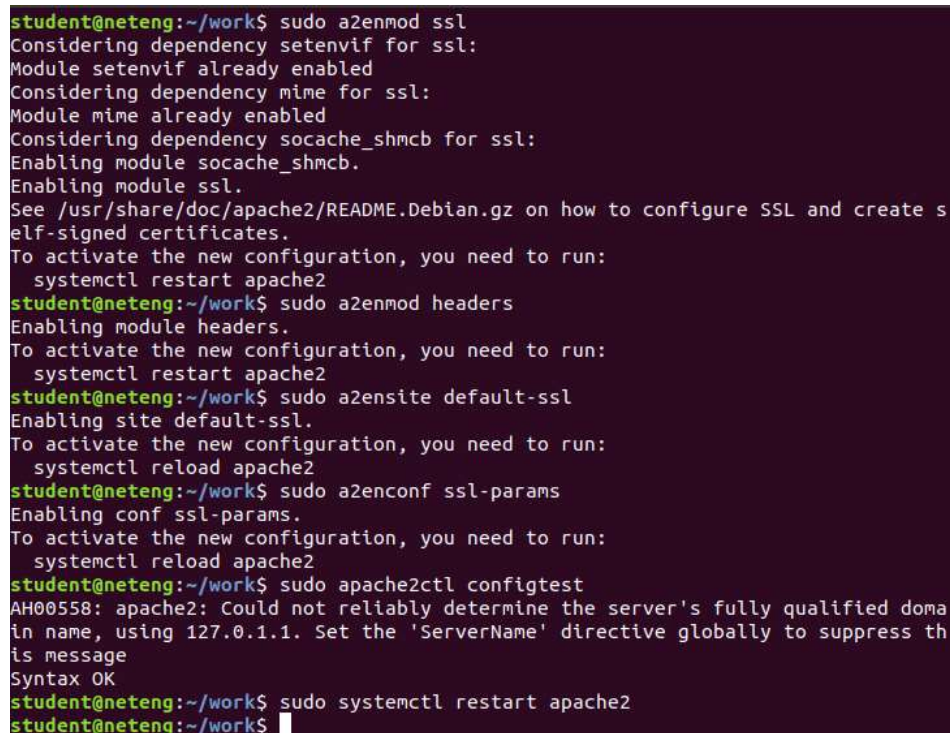
### 2.3.4 Enabling Changes

The configuration requires the following components to be enabled using the following commands.

```
sudo a2enmod ssl
sudo a2enmod headers
sudo a2ensite default-ssl
sudo a2enconf ssl-params
```

Check the config files for syntax errors using:

```
sudo apache2ctl configtest
```



```
student@neteng:~/work$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
student@neteng:~/work$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  systemctl restart apache2
student@neteng:~/work$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
student@neteng:~/work$ sudo a2enconf ssl-params
Enabling conf ssl-params.
To activate the new configuration, you need to run:
  systemctl reload apache2
student@neteng:~/work$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified doma
in name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress th
is message
Syntax OK
student@neteng:~/work$ sudo systemctl restart apache2
student@neteng:~/work$
```

Figure 14 - Components enables and apache2ctl test returning positive

If the configtest returns negative, return to Step 2.3.1 and check the syntax and placement of config entries.

Restart the web server using:

```
sudo systemctl restart apache2
```



### 2.3.5 Testing Encryption

Upon accessing the website through a browser, the following page should appear (or similar depending on your browser).

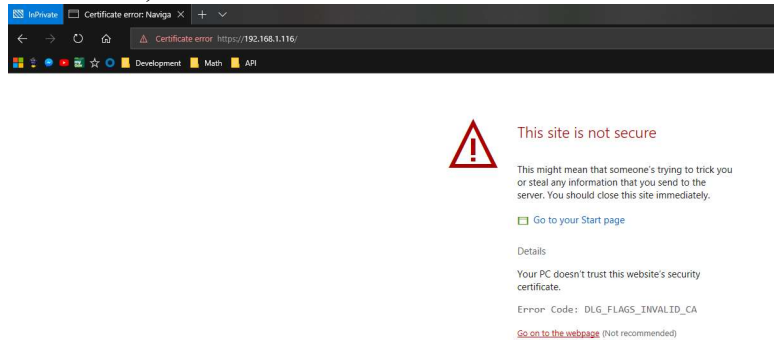


Figure 15 - Self-signed certificate warning

This is normal given that the certificate is self-signed. Attempt to access the browser using HTTP. The browser should be redirected to a HTTPS connection on port 443. Continue to the web page and log in using credentials from the populated LDAP server while using tcpdump. The output should not contain the credentials or any identifying information. Inspect the certificate using your browser. The information provided in Step 2.3.1 should be visible.

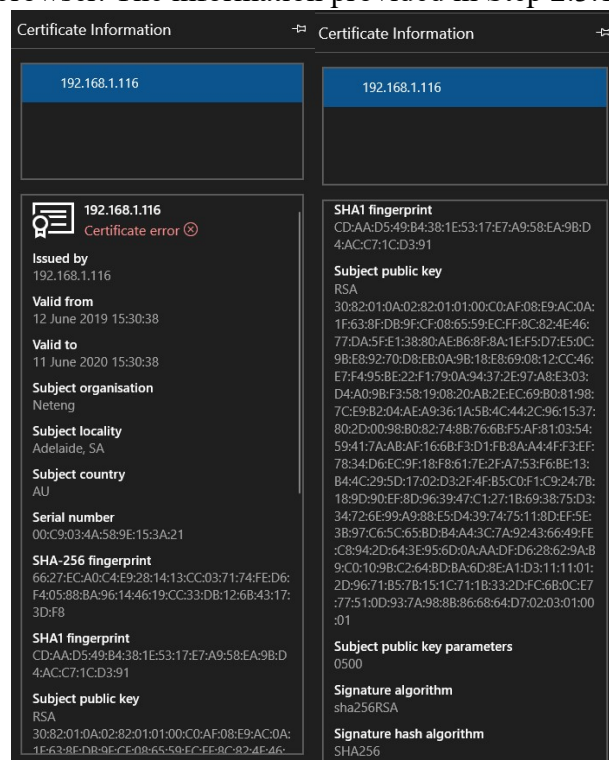


Figure 16 - Inspection of Certificate

This confirms the successful implementation of the LDAP authentication and SSL Encryption over the installation of the wiki and web server detailed in Assignment 1.

END OF INSTALLATION PROCEDURE

### 3 Bibliography

- [1] Microsoft. (2018). *Whats new in Active Directory Domain Services for Windows Server 2016*. Available: <https://docs.microsoft.com/en-us/windows-server/identity/whats-new-active-directory-domain-services>
- [2] OpenDJ. (2018, 15/06/19). *OpenIdentityPlatform/OpenDJ*. Available: <https://github.com/OpenIdentityPlatform/OpenDJ>
- [3] symas. (2018). *OpenLDAP*. Available: <https://www.openldap.org/>
- [4] RedHat. (2019). *389 Directory Server*. Available: <https://www.port389.org/>
- [5] Apache. (2018). *The Apache Directory™ Project*. Available: <https://directory.apache.org/>
- [6] DokuWikiCommunity. (2019). *LDAP Authentication Plugin*. Available: <https://www.dokuwiki.org/plugin:authldap>
- [7] B. Lu, "Wiki and Dynamic Web Server Selection, Deployment and Documentation " 2019.
- [8] B. Lu, "unit2-solution-a2mod.ldif," 2019.
- [9] B. Boucheron. (2018, 15/06/2019). *How To Create a Self-Signed SSL Certificate for Apache in Ubuntu 18.04* Available: <https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-18-04>
- [10] R. v. Elst. (n.d., 15/06/19). *Cipherli.st Strong Ciphers for Apache, nginx and Lighttpd*. Available: <https://cipherli.st/>

### 4 Appendices

#### Appendix A – Sample Dokuwiki Configuration File

```
<?php
/*
 * Dokuwiki's Main Configuration File - Local Settings
 * Auto-generated by config plugin
 * Run for user:
 * Date: Tue, 11 Jun 2019 16:14:54 +0930
 */

$conf['title'] = 'Neteng Wiki2';
$conf['license'] = 'cc-by-sa';
$conf['useacl'] = 1;
$conf['authtype'] = 'authldap';
$conf['superuser'] = '@admin';
$conf['disableactions'] = 'register';
$conf['plugin']['authldap']['server'] = 'localhost';
$conf['plugin']['authldap']['usertree'] = 'dc=nodomain';
$conf['plugin']['authldap']['grouptree'] = 'dc=nodomain';
$conf['plugin']['authldap']['userfilter'] = '(&(mail=%{user})(objectClass=inetOrgPerson)(objectClass=organizationalPerson))';
$conf['plugin']['authldap']['groupfilter'] = 'dc=nodomain';
$conf['plugin']['authldap']['version'] = 3;
$conf['plugin']['authldap']['starttls'] = 0;

// end auto-generated content
```