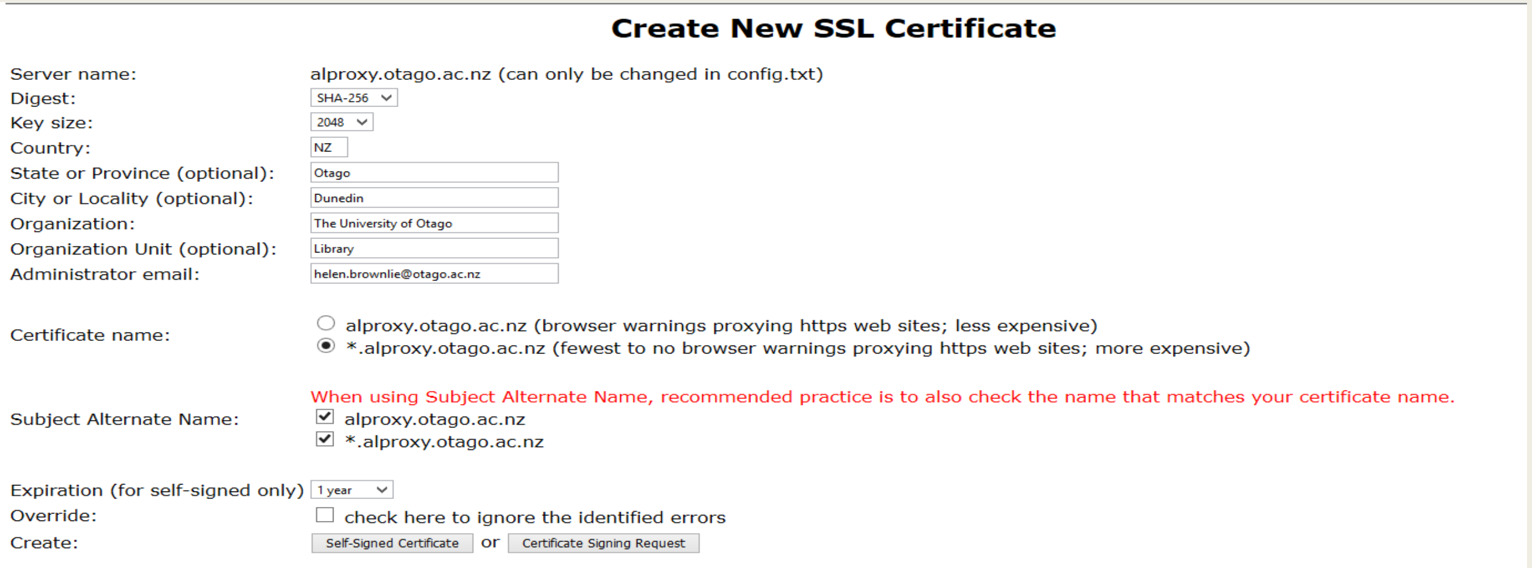
DigLib-SIG

Digital Library Special Interest Group LIANZA

Ezproxy Security

Security Certificates

- Self signed certificate
- Certificate purchased from a Certificate Signing Authority
- Wildcard certificate
  - *Not required if you are using Proxy by Port*



Create New SSL Certificate

Server name:	alproxy.otago.ac.nz (can only be changed in config.txt)
Digest:	SHA-256
Key size:	2048
Country:	NZ
State or Province (optional):	Otago
City or Locality (optional):	Dunedin
Organization:	The University of Otago
Organization Unit (optional):	Library
Administrator email:	helen.brownlie@otago.ac.nz
Certificate name:	○ alproxy.otago.ac.nz (browser warnings proxying https web sites; less expensive) ● *.alproxy.otago.ac.nz (fewest to no browser warnings proxying https web sites; more expensive)
Subject Alternate Name:	When using Subject Alternate Name, recommended practice is to also check the name that matches your certificate name. ☑ alproxy.otago.ac.nz ☑ *.alproxy.otago.ac.nz
Expiration (for self-signed only)	1 year
Override:	□ check here to ignore the identified errors
Create:	Self-Signed Certificate or Certificate Signing Request

Login Encryption

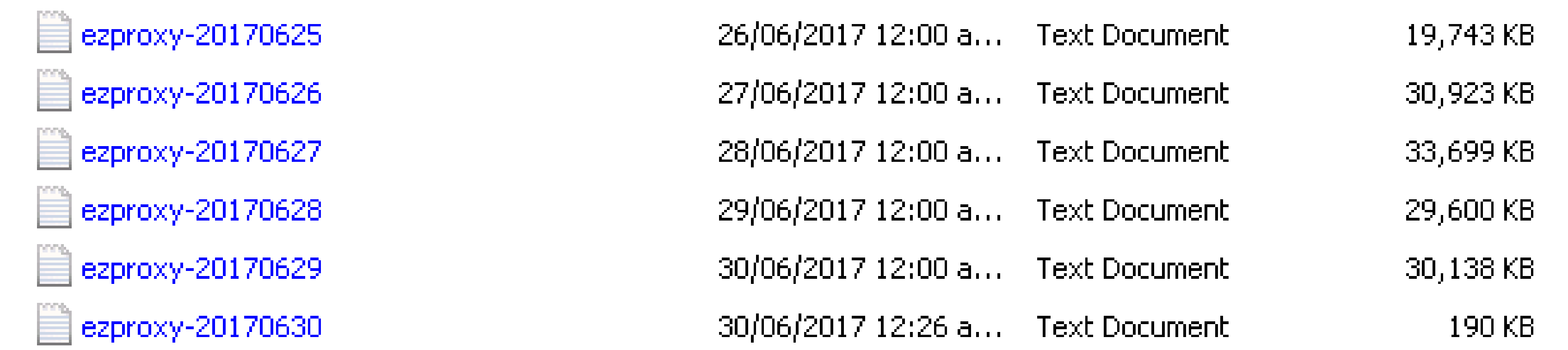
- LoginPortHTTPS
  - *Specifies the port on which EZproxy should listen for incoming login, menu, and administration requests using https. It is necessary if you want to require your users to login using https as defined by the Option ForceHTTPSLogin directive.*
- Option ForceHTTPSLogin
  - *Users will be redirected to a secure login page whenever they try to access EZproxy resources. This helps to keep your server and users' credentials secure.*

Limits

- MaxLifeTime
  - *Closes sessions that remain inactive for longer than a given period of time. This can help minimise the likelihood that a valid session left open on a public computer be taken over by an illegitimate user.*
  - *Issue with some vendors who use “heartbeat” or similar to keep sessions active*
- MaxSessions
  - *Limits the maximum number of EZproxy sessions that can exist at one time. This helps protect against denial of service.*
- Option BlockCountryChange
  - *Disconnects any user whose IP address changes from one country to another during a session.*

Logging

- Create and keep logs
- Audit MOST
- AuditPurge
- OPTION LogUser
- OPTION StatusUser
- LogFormat %h %{client-ip}i %l %u %{ezproxy-session}i %t "%r" %s %b
- LogFile -strftime C:\ezproxy\ezproxy\logs\ezproxy-%Y%m%d.log



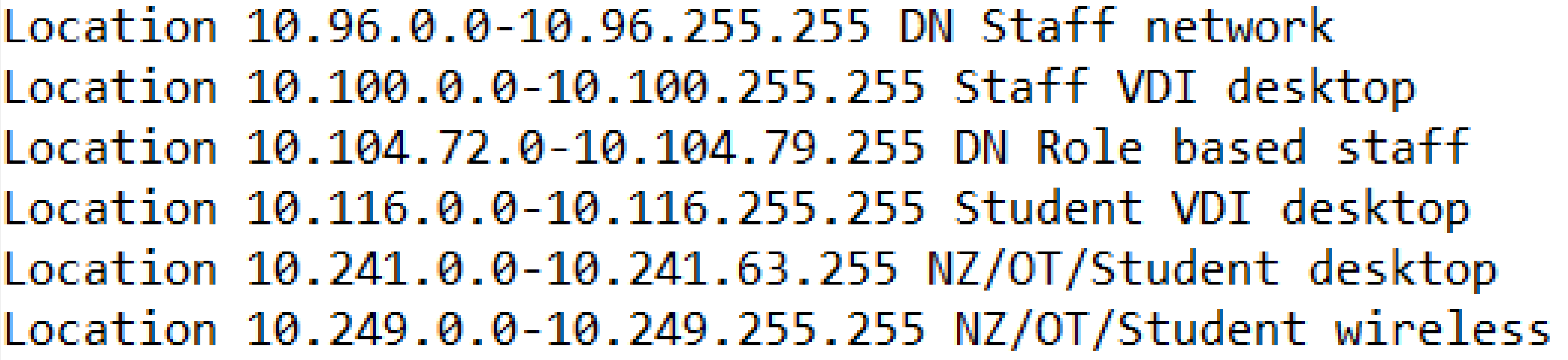
ezproxy-20170625	26/06/2017 12:00 a...	Text Document	19,743 KB
ezproxy-20170626	27/06/2017 12:00 a...	Text Document	30,923 KB
ezproxy-20170627	28/06/2017 12:00 a...	Text Document	33,699 KB
ezproxy-20170628	29/06/2017 12:00 a...	Text Document	29,600 KB
ezproxy-20170629	30/06/2017 12:00 a...	Text Document	30,138 KB
ezproxy-20170630	30/06/2017 12:26 a...	Text Document	190 KB

Monitoring

- IntruderIPAttempts
  - *Allows you to identify and automatically block users who repeatedly attempt to access your EZproxy server from a specific IP address with invalid credentials*
  - *IntruderIPAttempts -interval=5 -expires=15 20*
- IntruderUserAttempts
  - *Allows you to identify and automatically block users who repeatedly attempt to access your EZproxy server with an invalid password for a given username.*
  - *IntruderUserAttempts -interval=5 -expires=15 10*
- UsageLimit
  - *Provides options for monitoring and then enforcing limits on usage.*
  - *UsageLimit -enforce -interval=15 -expires=360 -MB=150 Global*

Location

- **Location**
  - *Allows you to identify where your patrons are located when they access EZproxy. Can be used to determine if a particular user's use of EZproxy is legitimate or if that person's account credentials have been compromised.*
  - *Uses GeoLiteCity.dat.gz to break down an IP address into town/city/region/country*
- Can also setup your own locations



```
Location 10.96.0.0-10.96.255.255 DN Staff network
Location 10.100.0.0-10.100.255.255 Staff VDI desktop
Location 10.104.72.0-10.104.79.255 DN Role based staff
Location 10.116.0.0-10.116.255.255 Student VDI desktop
Location 10.241.0.0-10.241.63.255 NZ/OT/Student desktop
Location 10.249.0.0-10.249.255.255 NZ/OT/Student wireless
```

Managing IPs

- ExcludeIP
- IncludeIP
- RejectIP
  - *Paul Butler's list https://github.com/prbutler/EZProxy_IP_Blacklist/blob/master/EZProxy_IP_Blacklist_RejectIP.txt*
  - *Current list has 9539 IPs!!*
- AutoLoginIP

Monitoring tasks at Otago

Let me show you ….

Resources

- Securing your Ezproxy server –

  http://www.oclc.org/support/services/ezproxy/documentation/example/securing.en.html

  https://github.com/upenn-libraries/ezproxy-security-issues

- Identifying compromised credential

  http://www.oclc.org/support/services/ezproxy/documentation/manage/security-breach.en.html

  Paul Butler, Brian Helstein, Jenny Rosenfeld (2016) EZproxy Forensics: Guarding Against and Identifying Compromised User . View Recording

  Paul Butler – Suggested tools including use of grep command and the black list http://lianzaitsig.pbworks.com/w/file/118895955/Paul_Butler.pdf

  Albert Ball, Christine Davidian, Jonathan Jiras, Scott Vieira & Peseng Yu (2016) Responding Proactively to the Problem of Compromised User Accounts, Serials Review, 42:3, 259-265, DOI: 10.1080/00987913.2016.1212315 http://dx.doi.org/10.1080/00987913.2016.1212315