

Log File Retention Guidelines

Institute for Advanced Study

February 24, 2020 (revision 297)

Contents

1 Log File Retention Times	1
2 Finding Log Files	1
3 Log File Destruction Procedure	2
4 Related Documents	2

1 Log File Retention Times

The default log retention time is *100 days*, except as shown in Table 1.

Table 1: Log File Retention Times

Log File Type	Retention Time
Web Proxy Campus ^a	168 hours
Web Proxy Resnet ^b	168 hours
Urchin Web Analytics ^c	Indefinitely
Virtual Machine backups ^d	465 days
Logs stored in Databases ^e	13 months
Logs related to Eduroam Radius Servers ^f	6 months

^aAs ratified by SPC on 2010-02-02

^bAs ratified by SPC on 2010-01-14

^cContains logs and reports of visits to ias.edu web pages.

^dVMs may hold 100 days of logs and are backed up for 365 days, so 465 days total. As ratified by SPC 2010-12-03

^eAs ratified by SPC on 2011-07-14

^fper https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf
As ratified by SPC on 2013-10-17

2 Finding Log Files

The EFF provides *logfinder*¹, a python script which is helpful in identifying log files. See `logfinder.py --help` and the included README file for usage. *logfinder* can be run in one of two ways:

- `logfinder.py` – Scans open files system-wide.
- `logfinder.py /some/path` – Statically analyzes files in `/some/path` for log-like characteristics.

3 Log File Destruction Procedure

The three-pass DoD 5220.22-M method is suitable. Here are some sample commands to destroy log files on various operations systems² to this standard:

- Linux: `shred -ufn3`
- Windows³: `sdelete -p 3`
- Mac OS X: `srm -fm`

In general, log files should be selected for deletion according to last modification time. The following command would destroy log files in `/var/log` older than 100 days:

```
find /var/log -type f -mtime +100 -exec shred -ufn3 {} \;
```

4 Related Documents

All Institute Computing policies can be referenced here: <https://security.ias.edu/policies>

- Institute for Advanced Study. *Log File Retention Policy*

¹<http://www.eff.org/osp/logfinder-0.1.tar.gz>

²Other devices or operating systems may not have such a utility. In these cases destruction via the best and most economical method available is required.

³*sdelete* is part of SysInternals.