Log entry metadata

# Log entry metadata

Any security log data collected must comply with these metadata standards to ensure we are able to consistently interpret log data using other systems.

## Time/date

* a: all log events must be time stamped in the common log timestamping format as defined by [ISO8601](https://en.wikipedia.org/wiki/ISO_8601) [dd/MM/yyyy:hh:mm:ss +-hhmm] where the fields are defined as follows:
  + 1: dd is the day of the month
  + 2: MMM is the month
  + 3: yyyy is the year
  + 4: :hh is the hour
  + 5: :mm is the minute
  + 6: :ss is the seconds
  + 7: +-hhmm is the time zone
* b: systems must use an automated time syncing protocol (such as NTP) with an external time source to ensure it is not subject to 'time drift' that may impact the accuracy of time stamping.

## Formats

Only the following log file formats should be used:

* a: Apache Common Log Format
* b: NCSA (Common or Access, Combined, and Separate or 3-Log)
* c: Windows Event Log
* d: W3C Extended Log File Format
* e: W3C Extended (used by Microsoft IIS 4.0 and 5.0)
* f: SunTM ONE Web Server (iPlanet)
* g: IBM Tivoli Access Manager WebSEAL
* h: WebSphere Application Server Logs