

### Create practical, comprehensible and accessible information

UTM FAST360 equipment provides fantastic control points for operators (Web and Messaging Traffic, Mobile Traffic via VPNs, User Authentication, Intrusion Detection, Viral Infection, etc).

This equipment produces very high volumes of log data every day. Ordinary tools very often don't make full use of this data, which is indispensable for diagnosis, audits and measurements. This is because of weaknesses in query formulation and poor presentation of results.

It is therefore essential that the various players in the company (from the operator administrator to the management controller) be provided with a log management platform that enables:

- Security requirements to be met in a way that is measurable and understandable by everyone,
- Past and current events on the network to be understood in detail,
- Risks to be minimised and availability improved whilst reducing investigation times.

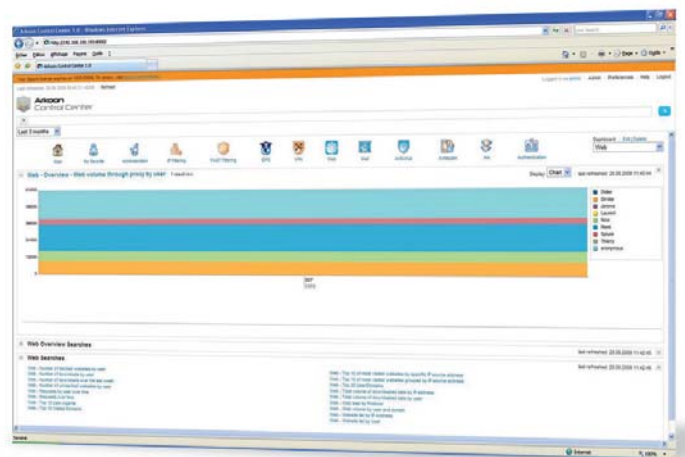
## Arkoon Control Center



The Arkoon Control Center (ACC) is the storage, query and log analysis platform dedicated to Arkoon's FAST360 appliances. This user-friendly and easy-to-implement tool is accessible from a Web interface and meets the requirements of technical operators and management controllers: production and sharing of audit and decision aid reports, generation of alerts and event correlation. The ACC is a true operator's 'Wiki', built around a very powerful search engine, and offers precise reports

and extremely quick search capability. The ACC comes with over 50 pre-defined reports (graphs, tables) and has a high-level query language that enables real-time customisation of all query types.

The ACC is available in a multi-user version and is intended for both end



users and managed security service providers (MSSP) who want to enhance their offer.

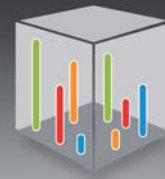
### Key points



- Storage and real time log indexing without data volume limits
- Optimised search engine
- Over 50 pre-defined reports, classified by subject area
- High-level, multi-criteria query language
- Highly user-friendly interface
- Multi-user, multi-client platform



# Technical specifications



## Storage – Indexing

- Storage and indexing of FAST360 logs sent via Syslog or from archive files.
- Extremely high performance levels: processing of up to 150,000 events per second.
- 12 to 48% compression rate.
- Processing scalability (several Terabytes / day with distributed architecture).
- Configurable archiving and recovery policy.

## Search, selection and report

- High-level query language enabling instantaneous and interactive sorting and selection in all fields and date ranges.

- Operators for statistical analysis and event correlation.
- Creation and backup of customised queries and reports that may be re-used and shared.
- Graphical representation (line graph, histogram, pie chart, etc) and/or tables.
- Over 50 pre-defined reports filed in customisable Dashboards (Administration, Network, IP Filtering, FAST Filtering, IDPS, VPN, Web, Mail, Antivirus, Antispam, Cluster, OS, Authentication).
- Planning of queries and reports for transmission via e-mail or RSS feed.
- Configurable report<sup>(1)</sup> printing modules.
- Alerts (via e-mail, RSS, SNMP or

customised scripts) based on query results.

## User authentication

- User authentication based on AD or LDAP.
- Granular role management for discretionary access control to source data, queries and reports (multi-user and/or MSS mode).

## Interface

- Web interface to access search/report modules.
- Interface customisation for use in MSS mode.

## System platform

- Distribution Linux Red Hat 32 and 64 bits
- Distribution Linux Debian 32 and 64 bits
- Windows XP, Windows Server 2000, 2003 and 2008 (32 bits)<sup>(2)</sup>

Note: virtual environments (VMWare, Xen, HyperV, etc) are supported.

<sup>(1)</sup> Available in V2.0

<sup>(2)</sup> US version in V1.0

## Client / Browser operating system

- AIX, BSD and Linux: Firefox 1.5 or 2.0; Adobe Flash 9 or higher
- Mac OS X: Firefox 1.5 or 2.0; Adobe Flash 9 or higher
- Windows: Internet Explorer 6 or 7 or Firefox 1.5 or 2.0; Adobe Flash 9 or higher

## Minimum and recommended hardware platform

### System

Non-Windows

Windows

### Recommended hardware platform

2x3.4 GHz CPU, 4 GB RAM

Multi-core Xeon or equivalent at 3GHz, 4GB RAM

### Minimum hardware platform

1x1.4 GHz CPU, 1 GB RAM

Pentium 4 or equivalent at 2GHz, 2GB RAM

## Product references

Reference	Description
020-ACC-ACC200	Licence ACC 200 Mbs / day
020-ACC-ACC500	Licence ACC 500 Mbs / day
020-ACC-ACC1000	Licence ACC 1 Gb / day
020-ACC-ACC2000	Licence ACC 2 Gb / day
020-ACC-ACC5000	Licence ACC 5 Gbs / day
020-ACC-ACC10000	Licence ACC 10 Gbs / day
032-ALS-ACC200	Contrat Serenium ACC 200 Mbs / day - 3 years
032-ALS-ACC500	Contrat Serenium ACC 500 Mbs / day - 3 years
032-ALS-ACC1000	Contrat Serenium ACC 1 Gb / day - 3 years
032-ALS-ACC2000	Contrat Serenium ACC 2 Gb / day - 3 years
032-ALS-ACC5000	Contrat Serenium ACC 5 Gbs / day - 3 years
032-ALS-ACC10000	Contrat Serenium ACC 10 Gbs / day - 3 years

# ARKOON

1, Place Verrazzano  
69009 Lyon - France  
Tél. : +33 (0)4 72 53 01 01  
Fax : +33 (0)4 72 53 12 60  
[www.arkoon.com](http://www.arkoon.com)



Arkoon  
Control Center