



IKARUS
wifi.security

Security on open WiFi network

Protect your WiFi hotspots while simultaneously meeting possible legal requirements for wireless network operators: **IKARUS wifi.security** checks all instances of access via your wireless network and efficiently protects that network against malware and misuse.

Additional features, such as personalised landing and block response pages, provide further space to promote your service. Define different network areas and access options, block unwanted content and limit download options.

Protection for operators and users

IKARUS wifi.security is compatible with all firewalls. Many settings not only offer optimal security, but they also provide interesting options when it comes to network configuration: Block unwanted content by URLs and categories, add to this with blacklists and whitelists, set up different network areas, define different administrative authorisation levels, create access profiles and time-based access controls, limit downloads per session and use landing and block pages for informational and advertising purposes.

Thanks to its multi-client capability, **IKARUS wifi.security** is also perfectly suited to companies with several locations or business areas: Each instance can be customised and branded on an individual basis. Design and configure your landing pages and use the integrated data collection tool to register users in your wireless network. The tool can also be used for reporting or newsletter campaigns. The block response page, which informs users if their web request contains malware or violates your usage guidelines, can also be designed by you yourself.

Comprehensive log information and automatic reports round off the feature set.



Product highlights

Protection against viruses, SPAM and malware

- » Anti-virus and Anti-SPAM features for HTTP, FTP and FTP over http
- » Activities monitor
- » Time-based access controls
- » Download limits per user session
- » Regular updates for real-time protection against the latest threats
- » Personalised landing pages
- » Personalised block response pages
- » Diverse landing pages (different brandings and content)

Configuration options

- » Create access profiles with ease using URLs, file names and file types
- » User-defined setup of administrative authorisation level
- » Differentiation of different networks through GRE/WCCP

Reporting and statistics

- » Detailed logging for all functions
- » Automated reporting and statistics