LCOS 10.92

LANCOM Security Essentials Option

Network security from the cloud

The LANCOM Security Essentials Option provides an efficient and reliable solution to protect networks against threats such as ransomware, phishing, malware, and credential theft. The integrated Content Filter effectively blocks unwanted and illegal internet content – preserving corporate integrity and significantly reducing liability risks. At the same time, the BPjM module of the German Federal Review Board for Media Harmful to Minors (BzKJ) reliably shields minors from harmful content. The underlying database used to verify website content is hosted in a GDPR-compliant cloud provided by European security specialist Bitdefender. For maximum scalability, use of the option is not limited to a specific number of users – making it ideal for growing networks.

→ Category-based filtering rules for web content (Content Filter)
→ Time- and profile-based configuration
→ Comprehensive usage statistics
→ Configurable category-based website overrides
→ Unlimited number of users
→ Blocking of harmful content for minors using the website list provided by the German Federal Review Board for Media Harmful to Minors (BzK
→ Simple software upgrade for LANCOM SD-WAN Gateways, SD-WAN Central Site Gateways, and WLAN controllers

LANCOM Security Essentials Option

The security upgrade for business networks

With the LANCOM Security Essentials Option, your network bandwidth is fully reserved for business operations. Websites containing spyware, phishing, viruses, and other threats are reliably blocked using a powerful, database-driven web filtering technology. The requested web content is checked online via a trusted rating server operated by the European security specialist Bitdefender. Administrators can freely define which thematic categories are blocked or allowed. Four preconfigured security profiles enable quick and efficient implementation.

Flexible Content Filter rules and custom configuration

The LANCOM Security Essentials Option allows for granular control of Internet access. Category-based filtering rules can be defined for various types of content such as criminal, pornographic, or violent websites. These rules are fully customizable and can be selectively overridden using the integrated override function.

Comprehensive protection against harmful content for minors

The integrated BPjM module from the German Federal Review Board for Media Harmful to Minors (BzKJ) ensures that harmful media is reliably blocked. This is based on an official and continuously updated website list issued by the BzKJ, providing maximum protection for minors in schools, youth centers, or at home.

Individual, time- and profile-based configuration

Internet access rights can be flexibly configured with the LANCOM Security Essentials Option. For instance, specific content may be made accessible during lunch breaks while being restricted during core business hours. User-dependent profiles can also be set up to selectively permit access to business-relevant websites.

Comprehensive statistics for full control

The LANCOM Security Essentials Option delivers detailed statistics on Internet usage, including category-based analysis. For example, top-10 lists of blocked and allowed website access can be generated for a configurable time frame. All statistics are anonymized to comply with data protection regulations.

Flexible override function

Where justified, the override button allows for temporary access to blocked websites without needing to adjust existing configurations. Overrides can be activated based on categories and monitored via email, SYSLOG, or SNMP to ensure controlled and secure use.

LCOS 10.92

LANCOM Security Essentials Option

Security Essentials

Cloud-based security engine	Globally distributed and highly available Bitdefender servers for real-time URL classification queries. Database with over 200 million URLs and 45 million domains across more than 70 content categories. Daily analysis of over 1 billion web requests, with more than 50 million blocked. Automated classification using heuristic content analysis, text evaluation, detection of NSFW content via skin tone concentration in images, structural and link analysis, URL reputation assessment based on telemetry from over 500 million endpoints, honeypots, and email traps. Malware detection through analysis of web content, downloads, and embedded objects. Response time under 100 milliseconds.
URL check*	Database based online check of web sites (HTTP/HTTPS). HTTPS websites are checked based on DNS names of HTTPS server certificates or based on "Reverse DNS lookup" of IP addresses.
Categories/category profiles*	Filter rules can be defined in each profile by collecting category profiles from 72 categories, for example to restrict Internet access to business purposes only (limiting private use) or by providing protection from content that is harmful to minors or hazardous content (e.g. malware sites). Clearly structured selection due to the grouping of similar categories. Content for each category can be allowed, blocked, or released by override
Override**	Each category can be given an optional manual override that allows the user to access blocked content on a case-by-case basis. The override operates for a limited time period by allowing the category or domain, or a combination of both. Optional notification of the administrator in case of overrides
Black-/whitelist	Lists that are manually configured to explicitly allow (whitelist) or block (blacklist) web sites for each profile, independent of the rating server. Wildcards can be used when defining groups of pages or for filtering sub pages
Profiles	Timeframes, blacklists, whitelists and categories are collected into profiles that can be activated separately for filter actions. A default profile with standard settings blocks pornographic, criminal, and extremist content as well as anonymous proxies, drugs, SPAM and malware
Time frames	Timeframes can be flexibly defined for control over filtering depending on the time of day or weekday, e.g. to relax controls during break times for private surfing
Flexible firewall action	Activation of the content filter by selecting the required firewall profile that contains content-filter actions. Firewall rules enable the flexible use of your own profiles for different clients, networks or connections to certain servers
Individual display pages (for blocked, error, override)	Response pages displayed by the content filter in case of blocked sites, errors or overrides can be custom designed. Variables enable the inclusion of current information such as the category, URL, and rating-server categorization. Response pages can be issued in any language depending on the language set in the user's web browser
Redirection to external pages	As an alternative to displaying the device's own internal response pages to blockings, errors or overrides, you can redirect to external web servers
License management	Automatic notification of license expiry by e-mail, LANmonitor, SYSLOG or SNMP trap. Activation of license renewal at any time before expiry of the current license (the new licensing period starts immediately after expiry of the current license)
Statistics	Display of the number of checked and blocked web pages by category in LANmonitor. Logging of all content-filter events in LANmonitor; log file created daily, weekly or monthly. Hit list of the most frequently called pages and rating results. Analysis of the connection properties; minimum, maximum and average rating-server response time
Notifications	Messaging in case of content-filter events optionally by e-mail, SNMP, SYSLOG or LANmonitor
Wizard for typical configurations	Wizard sets up the content filters for a range of typical scenarios in a few simple steps, including the creation of the necessary firewall rules with the corresponding action

LCOS 10.92

LANCOM Security Essentials Option

Security Essentials

Prerequisite	The prerequisite for using the Security Essentials option is LCOS 10.92 or higher
*) Note	Categorization is maintained by Bitdefender. Neither Bitdefender or LANCOM can guarantee full accuracy of the categorization.
**) Note	The Override function is only available for HTTP websites.

Item numbers

62168	LANCOM Security Essentials B Option 1-Year (for LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller LANCOM WLC-60)
62169	LANCOM Security Essentials B Option 3-Years (for LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller LANCOM WLC-60)
62170	LANCOM Security Essentials B Option 5-Years (for LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller LANCOM WLC-60)
62171	LANCOM Security Essentials C Option 1-Year (for LANCOM SD-WAN gateways of the 1900 series and LANCOM 2100EF)
62172	LANCOM Security Essentials C Option 3-Years (for LANCOM SD-WAN gateways of the 1900 series and LANCOM 2100EF)
62173	LANCOM Security Essentials C Option 5-Years (for LANCOM SD-WAN gateways of the 1900 series and LANCOM 2100EF)
62174	LANCOM Security Essentials D Option 1-Year (for LANCOM SD-WAN central site gateways ISG-5000 and ISG-8000 as well as WLAN controller LANCOM WLC-2000)
62175	LANCOM Security Essentials D Option 3-Years (for LANCOM SD-WAN central site gateways ISG-5000 and ISG-8000 as well as WLAN controller LANCOM WLC-2000)
62176	LANCOM Security Essentials D Option 5-Years (for LANCOM SD-WAN central site gateways ISG-5000 and ISG-8000 as well as WLAN controller LANCOM WLC-2000)

lancom-systems.com