

Activeworx Log Center (ALC)

a unified security information and log management platform

ACTIVWORX ENTERPRISE

- LOG CENTER
- Security Center
- Event Manager
- Snort Management Center



Activeworx Log Center™ (ALC) ist die neueste Erweiterung der Security-Lösungen der Activeworx Produkte. Basierend auf der preisgekrönten Activeworx Plattform, kombiniert Activeworx Log Center ein leistungsfähiges Raw-Logging-Werkzeug, einer umfangreichen forensischen Analyse, mit einem skalierbaren Reporting-Funktion. Activeworx Log Center erfasst alle Raw-Netzwerk-Events, verschlüsselt diese und gewährleistet die Integrität der Daten. Indizes werden verwendet um Daten in einer leistungsfähige Such-Funktion zu visualisieren und in einen Out-of-the-box-Compliance Reporting zur Verfügung zu stellen.

Das Activeworx Log Center bietet darüber hinaus die Möglichkeit, Software-Plug-Ins für eine einfache und kostengünstige Skalierung in verteilten und heterogenen Netzwerk-Umgebungen und die vollständige Integration in die Activeworx Security-Center über die Activeworx Plattform.

Appliance Options:

Entry Level 1U Appliance

This appliance has the basic features

Mid range 1U Appliance

This adds to the entry level appliance with hot swappable drives, more memory and an additional Power Supply.

High end 2U appliance

This appliance adds to the midrange by adding more CPU, memory and faster disks along with a high-end NIC.

Compliance

Activeworx Log Center™ (ALC) is a compliance ready solution that can be used as demonstrable evidence for regulatory compliance regulations

Historical Understanding

Activeworx Log Center™ (ALC) gives users the ability to generate complex lists, groups, and sorts, including detailing the most frequent occurrences, from historical, raw data.

Log Visualization

Activeworx Log Center™ (ALC) offers customizable viewing formats. The Activeworx diagram engine offers flexible and interactive graphing capabilities for a better strategic understanding of compliance posture and more effective forensic diagnosis of security breaches.

Total Integration with Activeworx™ Product Line

No cross-functionality concerns. The Activeworx family of products can be used as standalone products, or as part of a truly integrated security and log management suite.

Features and Benefits

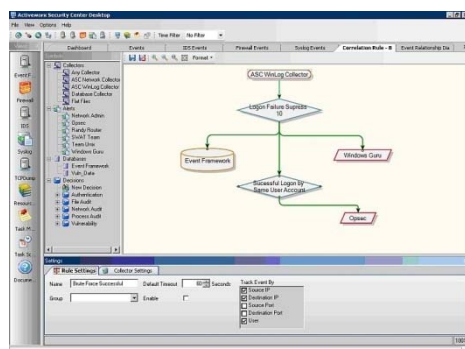
TECHNICAL SUPPORT

24 Stunden technischer Support durch Knowledgebase des Herstellers.

Telefonischer technischer Support während der Geschäftszeiten oder per E-Mail an:
support@activesphere.net

ZERO DOWNTIME

Ständige Verfügbarkeit des Supports durch ein weltweites Partnernetzwerk in über 40 verschiedenen Ländern geben telefonisch und per E-Mail Unterstützung in der Landessprache



ActiveWorx Log Center Features - Raw Audit Logging

Raw audit logging and log management of ALL events generated by virtually any computer or device on your network. The high performance logging engine is capable of logging over 50,000 EPS sustained and logs directly to flat files with indexing and search capabilities as well as SIEM integration. ActiveWorx Log Center provides full data retention capabilities for statutory compliance acts like HIPAA and GLBA among others, as well as requirements for Payment Card Industry regulations.

Flexible Active Platform

The ActiveWorx Log Center is based on the ActiveWorx platform and can be easily integrated with the ActiveWorx Security Center to add powerful forensic capabilities to an already robust log solution.

Comprehensive Reporting

ActiveWorx Log Center includes a built-in Report Center to provide intelligence on incidents of interest along with compliance reports.

Powerful Correlation Capabilities

ActiveWorx Log Center includes a Correlation Engine that is designed to handle events at a higher rate and hold more events in the state engine without degrading performance. This allows you to quickly perform root cause analysis and perform an intelligent diagnosis without having to stumble around to find events of interest. ALC correlation engine can correlate based on references, vulnerability information, host information and application information. No matter where you are within ALC, you have the power to correlate information from within your current view to other events from different data types or databases, and display them in a variety of useful output formats.

Detailed Alerting

Knowing when an event has occurred is imperative to security administrators. ALC provides rules-based alerting through several standardized protocols, such as e-mail and Syslog.

Visualize Events

The ALC event dashboards are completely customizable. Users have the ability to choose from over 50 different panels to display information and save multiple layouts. The event dashboards provide many different charts and graphs to visualize information. Each interactive view has the ability to drill down and see the events, perform search correlations, run custom commands on context sensitive values, copy charts into a report and customize charts to better view your data.

Event Relationship Diagramming

ALC has a powerful diagram engine that displays events and the relationship between them. Once these events are displayed, you can replay the order in which they occurred, color code the events to highlight different characteristics, perform different types of auto layouts to change the way in which the events are being displayed, or drill down into the events to gather more details.

Interactive Graphing

Interactive graphs are one of the many ways to drill down into data to obtain a better forensic understanding of information collected. All graphs can be drilled into to view the events making up the graph, as well as performing correlation searches to create customized views based on the portion of the graph selected.