

Smart IDENTITY Management

Information security is a complex system requiring the integration of many technologies such as Firewalls, Intrusion Detection and Prevention, Antivirus, Antispam, Content Filtering and others. With security and network devices bombarding administrators with log events and email alerts, keeping track of actual attacks versus false positives is a constant challenge. Unfortunately, all network and security alerts are typically unaware of “user identity” – simply giving a MAC or IP address as the originating source. Without identity information, administrators must manually resolve unknown addresses to host names and then to user identity. With dynamic addressing and mobile users, this may be very difficult to do.

To be proactive, security and network devices must work with Identity & Access Management (IAM) systems to bridge the gap and speed forensic, tracking, and auditing activities. With government regulations and corporate compliance demanding better controls and record keeping, identity becomes an integral part of modern information security & networking architecture.

A10 Networks’ IDSentrie™ 1000 provides a complete Identity and Access Management solution with the most useful IAM features to help administrators gain control of identity resources and simplify the convergence of network, security, and identity management. IDSentrie’s unified IAM solution can be implemented quickly and cost effectively, and customers can enable IDSentrie components individually or in any combination to fulfill their authentication and identity management needs.

IDSentrie 1000 Components

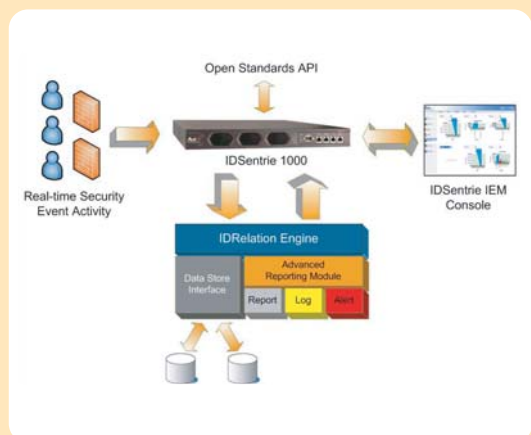
- Hardened RADIUS Server
- RADIUS & LDAP Authentication Proxy
- Unified IDENTITY Manager
- User Self-Help Service
- IDENTITY Event Manager
- Advanced Reporting
- DHCP Server
- Open Standards API

Correlated Identity Management

IDSentrie’s IDENTITY Event Manager (IEM) creates a new paradigm for forensic activity and is the industry’s first true identity-based correlation engine for security and networking devices. By forwarding critical event logs from security and networking devices to IDSentrie, administrators can resolve uninformative MAC & IP addresses to user identity information in real-time or through historical logs and reports.

IEM’s IDRelations Engine correlates MAC & IP addresses with user identity information to make easy work of identity forensics. Without the need to manually resolve user information, security & network monitoring, troubleshooting, and forensics becomes much more efficient.

Firewall Log Analyzer



In-Depth Visibility

Identity Event Manager supports the industry’s most popular security devices – such as firewalls from Check Point, Cisco, NetScreen (Juniper), Fortinet and others using the WebTrends Enhanced Log Format (WELF). To simplify reporting, IDSentrie’s Advanced Reporting module provides comprehensive identity-based reporting, logging and alerting with over 140 supplied reports. With the IEM Dashboard, administrators and operation centers can obtain high-level consolidated views of user activity for troubleshooting and trend analysis. The IEM Dashboard identifies top bandwidth users, web users, telnet users, FTP users, SSH users, and top applications.

Powerful Reporting

IDSentrie’s Custom Reports allows administrators to create reports with user defined queries, device groups, and filter groups. Reports can be generated instantly or scheduled, emailed to a specific individual or group, and formatted as HTML, text or XML. IDSentrie’s Advanced Reporting provides over 140 report templates covering a wide range of reporting categories including:

- Device Activity, User Activity, Event Activity
- Recent Event Types, Connection Events
- Bandwidth Usage, Activity Utilization
- Protocol Breakdown, Traffic Violations
- System Reports, Account Usage, Activity Auditing

In addition to powerful identity-based reporting, IEM also monitors all incoming events and allows administrators to create policies & thresholds for critical event alerting and notification.

CORRELATED IDENTITY MANAGEMENT

Identity Proxy Service

A10 understands the need to simplify the convergence of identity, network and security functions. With IDSentrie's Open Standards API, administrators can now create identity-based network solutions by leveraging identity resources managed by IDSentrie. The secure thin-client API can be integrated quickly with virtually any 3rd party security or networking application to empower it with user identity information.

With IDSentrie's API providing user information, critical security & network alerts are demystified - allowing administrators to quickly zero in on individuals causing the problems. For customers without integration capabilities, IDSentrie also provides a Windows client that can perform the same query functions - giving administrators the power to resolve mysterious MAC & IP addresses to user identities in real-time.

A10 Networks' IDSentrie 1000 leads the industry in price/performance - greatly simplifying identity management tasks, improving security, and reducing overall costs.

A10 Networks' Smart IDentity Management surpasses traditional authentication and gives corporations the power to regain control of their identity resources.

Identity Aware Network Solutions

A10 Networks provides the industry's first Smart IDentity Management solution to empower enterprise, government, and institutions with the ultimate control, flexibility, and visibility in designing secure identity-based networks.

Comprehensive Identity Management

The IDSentrie solution is modular. Customers can enable any or all of IDSentrie's components to create sophisticated identity & access management solutions with identity-based reporting and logging.

Customers can enable IDentity Event Manager with other IDSentrie components such as the RADIUS Authentication Module, Unified IDentity Manager, User Self-Help, LDAP Proxy and Advanced Reporting. All software modules are included in IDSentrie's price for a complete and cost effective solution.

With IDSentrie, businesses can quickly see the benefits of Identity & Access Management without the long implementation times normally associated with traditional IAM solutions. By combining the most useful IAM features in a unified appliance, A10 customers can implement IAM features at a pace they desire, without the high costs of user licenses and ongoing costs.

Auditing , Retention and Compliance

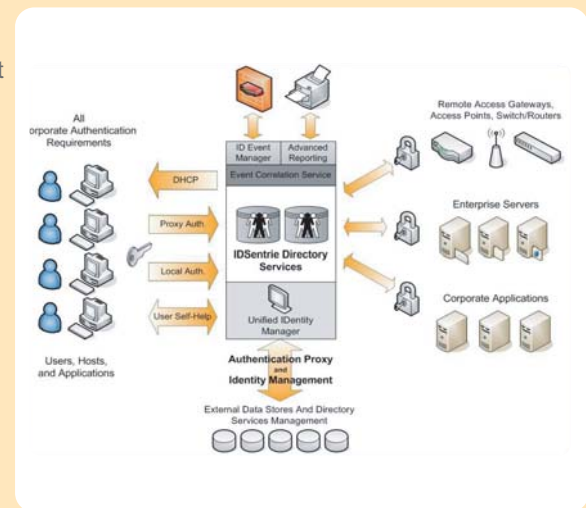
Along with a powerful identity-based reporting and alerting engine, IEM can chronologically store all critical events and system activity - capturing all critical RADIUS and LDAP authentication activity, user account activity, firewall, and system related activity within a single system.

IDSentrie provides advanced filtering capabilities to speed searching of event and system logs to aide compliance auditing and reporting. Administrators can create policies to automatically rotate and achieve logs to external systems for retention purposes. With identity-based logging & reporting, attaining compliance is much simpler as users are automatically identified without manual correlation efforts.

Improved Operational Efficiency

IDSentrie provides functionality that goes well beyond traditional authentication or user account management systems and greatly improves the ability to see individuals and applications using network resources. IDentity Event Manager

Smart IDentity Management



improves operational efficiency by quickly integrating into existing network environments and leveraging log information from security and network devices. With IDSentrie's purpose built hardware and hardened operating system, enterprises can be up and running with IDSentrie in hours, not days or weeks like other complex and expensive identity management systems.

Working in conjunction with other IDSentrie components, IEM can reduce or eliminate many manual and tedious IT tasks. Valuable time administrators spend resolving IP and MAC address information to user names are a thing of the past with IEM. Meeting compliance auditing is greatly simplified with user information fully integrated into IDSentrie logs and reports - improving accuracy, saving time and unnecessary manual correlation.

Having accurate and timely information is critical for network & security forensics. Obtaining identity information quickly can make the difference between apprehending the culprit or coming to a dead end.