

Smart Identity Management

Today's modern computing and business applications are driving enterprises to expand beyond the borders of their traditional networks, pushing applications and business processes to be more open and available while adhering to tough regulatory requirements. However, as each new business application is brought online, authentication and access control management becomes more complex and increases vulnerability and security risks for unauthorized access.

A10 Networks' IDSentrie™ 1000 provides a complete Identity and Access Management (IAM) solution with the most useful features to strengthen authentication through a wide range of standardized authentication protocols and popular 3rd party data stores. 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.

Next Generation Authentication

With today's security conscious business environments and tough regulatory requirements demanding better authentication, authorization, accountability, and internal controls, enterprises are demanding stronger Identity Management systems that do more than just authenticate users. A10 Networks' Smart Identity Management solution provides customers with a secure robust authentication system that provides rich tracking and reporting for their entire authentication, authorization, and accounting 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

A Need for Tough Authentication

IDSentrie's standard-based AAA RADIUS authentication services support all of the latest strong authentication protocols and popular 3rd party data stores. IDSentrie provides strong authentication service for all types of access: wireless LAN, wired LAN, VPN, Dial-up, applications, and more. Authentication activities are controlled by flexible and granular policies to strictly control access and detailed logging and reporting tracks all user access and authentication activity for auditing compliance.

* Please see the IDSentrie 1000 Datasheet for more information on supported authentication protocols and 3rd party data stores.



Universal Authentication Support

With universal support for all popular authentication protocols and IDSentrie's Authentication Proxy service providing pass-through authentication to popular standards-based data stores, customers can build flexible centrally managed authentication solutions without having to convert or migrate from their existing data stores. Authentication Proxy allows enterprises to quickly adopt the latest authentication technologies such as 802.1x and EAP without "ripping out" their existing systems.

Customers who need to consolidate identity information from multiple legacy data stores can leverage IDSentrie's Unified Identity Manager and Authentication Proxy service to create a smooth and uninterrupted migration path.

With IDSentrie bridging the new environment to legacy data stores, administrators can migrate user resources at their own pace without jeopardizing usability for end users.

Granular Authentication Control

IDSentrie RADIUS provides granular control based on Realms, Groups, and individual Users with the ability to assign multiple authentication policies and passwords to each user. Policies can be scheduled to provide unparalleled flexibility and control.

Customers can quickly build sophisticated profiles and policies using IDSentrie's intuitive Web interface to grant and restrict authentication access to users and groups. Vendor specific attribute support for more than 50 vendors along with the ability to add custom attributes provide fast in-depth policy creation, provisioning and enforcement.

ACCELERATED Authentication Management

Authentication Simplicity

To alleviate the pressures of traditional authentication systems, IDSentrie customers can enable advanced features such as User Self-Help Services to offload simple IT requests. User Self-Help empowers users with the ability to make their own changes to authorized fields – such as cell phone number, surname, home address and password. Lost passwords and locked accounts can also be recovered after proper validation.

Customers can also tailor their provisioning forms and screens with IDSentrie's Custom Forms to ensure that only relevant identity information is collected and displayed – reducing complexity, inconsistencies, and mistakes. With IDSentrie's DHCP server enabled, dynamic IP addressing is accurately tied to the authenticating user's identity to improve troubleshooting, forensics, and compliance reporting.

Application Authentication Tracking

IDSentrie's LDAP Proxy Service tracks user application usage by keeping track of when users authenticate to their business applications. IDSentrie's detailed reports of both physical network and application use provide administrators with the tools to boost their regulatory compliance and internal control tracking capabilities.

A10 Networks' IDSentrie 1000 leads the industry in price/performance. Its Smart Identity Management solutions greatly simplify identity management tasks, improve security, and reduce overall costs.

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.

Simplifying Regulatory Compliance

With the latest government regulations around the world demanding better accountability and access control, identity management is more important than ever. IDSentrie's Smart Identity Management solutions provide the identity management features to attain compliance and improve internal controls.

Secure and Robust Authentication

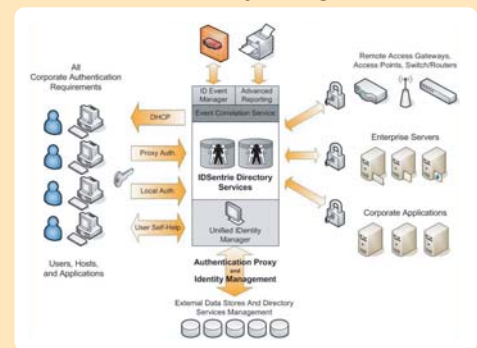
To secure against unauthorized access and attacks, IDSentrie employs purpose-built hardware and operating system software. Limited application ports on user-facing interfaces permit only authorized authentication protocols. A dedicated management interface provides "out-of-band" administration for maximum security and remote administration can be performed securely with HTTPS and SSH. To ensure that identity information is properly secured on the hard disk drives, all critical identity information is encrypted to prevent theft and unauthorized use.

For mission critical applications, a pair of IDSentrie units can be clustered in Active-Standby mode to form a High-Availability (HA) solution – providing seamless failover and uninterrupted service.

Comprehensive Identity Management

By enabling multiple IDSentrie components, customers can create sophisticated IAM solutions to centrally control all aspects of authentication and identity activities throughout the enterprise. IDSentrie's Authentication component can be combined with any of the following IDSentrie modules - included in the system free of charge.

Smart Identity Management



Unified Identity Manager (UIM) - UIM provides customers with the ability to consolidate identity information from separate and dissimilar data stores for centralized provisioning, management and policy enforcement.

User Self-Help Service – Empowers users with the ability to select new passwords, recover from lost passwords or locked accounts, and change account profile information.

Identity Event Manager (IEM) – IEM tracks activity events from popular security & network devices to correlate with identity information. Violations and suspicious traffic is quickly and accurately identified back to the true user with full logging and auditing. IEM can greatly accelerate security investigation and forensic efforts to identify access violations and unauthorized activity. The Advanced Reporting Module provides over 140 reports to simplify reporting.

Open Standards API – IDSentrie's API provides customers with an easy way to fully tap the identity information managed by IDSentrie. With API services, IDSentrie can be added to any existing security and network system to provide user information.