

Smart Identity Management

With the number of business applications increasing, each requiring their own methods of authentication and access control, IT professionals are busier than ever setting up and managing separate systems and data stores. Managing separate data stores and directory services complicate identity management and increase not only the work load, but the chances that mistakes will be made. In addition, network and data security is compromised as each new data store, authentication method, and control policies are brought online. The more identity information is scattered across dissimilar systems, the higher the probability of duplicate, unknown, and unauthorized accounts granting illegitimate access.

A10 Networks' IDSentrie™ 1000 provides a complete Identity and Access Management (IAM) solution with the most useful features to help administrators gain control of user accounts and to simplify users' account and password experiences to improve productivity. 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.

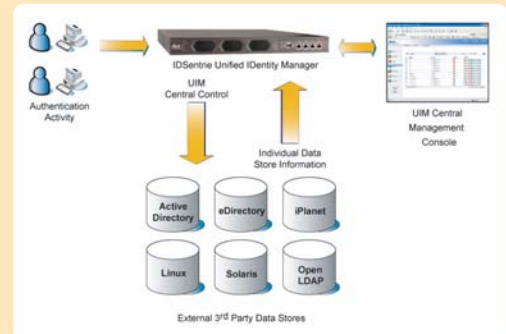
Unified Identity Manager

IDSentrie's Unified Identity Manager (UIM) solves the complexities and security concerns of managing multiple data stores throughout the enterprise. UIM provides the ability to fully consolidate all user account information from multiple disparate data stores and directory services into one corporate-wide Virtual Directory service that can be centrally managed.

To provide fast deployment and immediate benefits, UIM's Virtual Directory service automatically inventories user account information from all managed data stores without requiring migration of account information. Administrators can provision and manage user accounts immediately after the connection is made between IDSentrie and the data store.

Information provisioned with UIM is automatically synchronized between data stores to simplify account creation, deletion, and modifications – decreasing IT overhead significantly and eliminating data entry mistakes.

IDSentrie Unified Identity Manager



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

The Need to Consolidate

Enterprises use multiple data stores to support application authentication and to secure network and resource access. Many small and medium enterprises support a minimum of three data store types and larger installations often have five or more.

Managing too many data stores such as Active Directory, LDAP, Sun Directory Server, Novell eDirectory, Linux, Kerberos, SecurID, and so forth can only mean one thing. Administrators and users are saddled with management overhead in administrating and remembering multiple accounts and passwords for each application and access method - increasing security risks, operational overhead, and making compliance and internal controls much more difficult to achieve.

Management Issues with Multiple Data Stores

- Additional management overhead to provision and maintain user account information
- Scattered views of corporate-wide authentication and identity information with no easy

correlation

- Inconsistent password and authentication policies increases user complexity and non-productivity
- Higher volumes of support calls
- Steeper learning curve for system administrators
- Higher cost, unnecessary complexity, slower response times

Security Issues with Multiple Data Stores

- Unauthorized entry points exist and are hard to detect without a unified view of all identity information
- User credential theft resulting from insecure servers hosting critical authentication information
- Security risks resulting from left-over accounts that are not completely removed after terminated relationships with employees, partners or customers
- Inconsistent access policies weaken security stance
- Security issues decrease customer confidence, create negative corporate PR, and can lead to costly lawsuits

A10 Networks' IDSentrie 1000 leads the industry in price/performance - greatly simplifying identity management tasks, improving security, and reducing overall costs. With IDSentrie, corporations can enhance their ability to meet tough regulatory standards such as the Sarbanes-Oxley, Health Insurance Portability and Accountability, and Gramm-Leach Bliley acts.

Identity Aware Network Solutions

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

Uncompromising Control

IDSentrie provides support for the most popular data store types to make integration fast and simple.

- Internal and external RADIUS
- LDAP, Novell eDirectory, Sun Directory Server
- Microsoft Active Directory, Windows NT Domain
- Kerberos v5, Solaris, Linux
- RSA SecurID

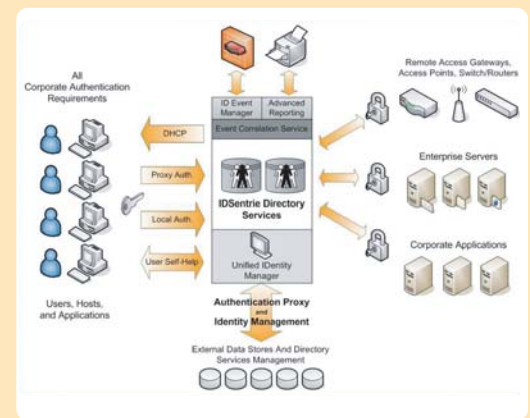
With all identity information centralized, administrators can gain complete control over all user account information and retrieve critical statistics and status information for each user. Reports on user authentication activity, user statistics and user activity give a complete picture of the individual and their account activity - and audit trails provide a chronological history of account management activity to meet regulatory requirements.

Comprehensive Identity Management

By enabling one or multiple IDSentrie components, customers can create sophisticated IAM solutions to centrally control all aspects of authentication and identity activities throughout the enterprise.

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

Smart IDentify Management



Elevated Security

Unified IDentify Manager enhances security for existing data stores in several ways. With centralized account management, companies can limit management access to all of their 3rd party data stores, allowing changes to be made only through IDSentrie. IDSentrie logs all administrative functions to track all account management activity - reducing the chances of unauthorized changes, theft of identity information, and improving internal controls for compliance purposes.

Additional security is also possible with IDSentrie's Authentication Proxy service. Authentication Proxy can perform all RADIUS authentication requests using existing 3rd party data stores. Administrators can restrict direct client access to data store servers and limit access to only IDSentrie. With LDAP Proxy Service, businesses can fully track user access to critical applications requiring LDAP authentication.

UIM provides a consolidated view of all identity information across the enterprise allowing administrators to quickly see invalid and unauthorized accounts. Once identified, UIM allows rapid disablement or deletion of unnecessary accounts from one central location regardless of where the accounts are stored - eliminating security risks quickly and efficiently.

Improved Operational Efficiency

Improved operational efficiency is attained by centrally managing identity information where it natively resides, without disruption to existing data store systems.

Data store synchronization ensures accurate information changes and eliminates the need to manage each data store separately to reduce management overhead.

To help administrators customize IDSentrie for their environments, Custom Forms and Attribute Field Mapping are available to fully control data store schema information. To ensure compatibility, IDSentrie's data import module accepts user information from all Human Resource systems and applications supporting the comma delimited file format.

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 IDentify Management solutions provide the identity management features to attain compliance and improve internal controls.