

Save Hours While Resolving Security Issues

The A10 Networks IDSentrie® is the industry's only network identity management appliance with instant user identity resolution, which helps organizations save hours everyday and minimize risk by resolving security issues faster. The IDSentrie is built on a flexible, virtual directory model for rapid integration with existing network infrastructure and support for a variety of popular data stores to help simplify today's complex identity resource management, authentication and security issues.



The A10 Networks IDSentrie
– Network Identity Management

IDSentrie Main Components

- Appliance based solution to simplify Identity and Access Management (IAM) infrastructure
- Account data synchronization for simplified sign on and enhanced compliance
- User Self-Help Service to reduce costs associated with password resets and account updates
- Integrated authentication mechanisms to enhance and simplify security
- Instant IP-to-ID correlation to eliminate manual forensics and provide quicker resolution for critical network events
- Identity-based reporting & logging to help address network issues and meet regulatory requirements
- Full featured RADIUS with enterprise grade performance

► **Central Account Management with Unified Identity Manager (UIM)** – Simplifying user account management through the consolidation of user information from multiple data stores into a single, manageable virtual directory. IDSentrie's UIM component provides provisioning, management and de-provisioning of user accounts from one central interface allowing for quick changes, which can be synchronized across all data stores to help improve accuracy, usability and security while lowering overhead.

► **User Self-Help Web Portal for Password Resets and Account Updates** – Allowing end users to reset passwords and update account information without the need to involve help desk or IT personnel. The Self-Help Service not only reduces support overhead and costs but also simplifies account infrastructure with the synchronization of passwords and other account details. The Self-Help Service also integrates with password policy and password expiration notifications to simplify management and compliance requirements.

► **Centralized RADIUS Authentication for Simplified Sign-on** – Providing a consolidated solution to help simplify user authentication. The IDSentrie can easily integrate with existing account infrastructure to help simplify the authentication process for users and strengthen authentication mechanisms

for devices such as VPNs, wireless access points, switches, routers and security devices. The IDSentrie is a fully featured RADIUS server with powerful extensions allowing RADIUS requests to be fulfilled by non-RADIUS servers such as Active Directory, LDAP, UNIX, SQL and many more, removing the need for RADIUS specific usernames and passwords.

► **IP-to-ID or MAC-to-IP Service for Instant Identity Resolution** – Find out who is on your network with the unique ability to correlate an IP, ID or MAC address to a user identity, instantly. IDSentrie's IP-to-ID Service eliminates the need to manually correlate IP, ID or MAC addresses to user identity and allows IT engineers to take corrective action immediately to lower security risks and potential damage. IP-to-ID Services provide multiple access methods to obtain user identity information for truly seamless integration with existing security, network and software applications.

► **Authenticated DHCP and Guest Access Services** – The IDSentrie DHCP server can be enhanced by enabling Authenticated DHCP, which provides the ability to quarantine non-authenticated users and prevent unauthorized network access. A Guest Access web portal and web administration portal are also included.

With IDSentrie, companies can improve their security and compliance requirements while lowering operational costs and reducing management overhead. System Administrators are more productive with UIM's ability to centrally provision and manage user accounts from multiple data stores simultaneously. Employees are more productive with the User Self-Help Web Portal eliminating the need to have help desk engineers reset passwords. Security is enhanced with Network Authentication and Access Control Services preventing unauthorized network access. Busy IT departments can quickly reduce overhead and speed troubleshooting with IP-to-ID Services pin-pointing issues directly to the users responsible. IDSentrie's rich reporting and auditing features provide full visibility to allow IT departments to work more effectively.

» Data Store Support

- Internal RADIUS
- RADIUS Proxy Authentication
- LDAP v2, v3 / OpenLDAP
- Microsoft Active Directory
- Apple Open Directory
- Windows NT
- Kerberos v5
- Lotus Domino
- Novell eDirectory
- Sun ONE, iPlanet Directory Server
- Solaris
- SCO Open Server
- Fedora Core, Red Hat, FreeBSD, NetBSD Linux
- MS SQL, Oracle, mySQL, PostgreSQL, Sybase
- RSA SecurID

» Identity Provisioning Features

- Management for 3rd Party Data Stores
- Centralized Account & Group Provisioning & Management
- Central Password Policy Enforcement
- Identity Attribute Synchronization
- Account Password & Data Synchronization
- Customizable Provisioning Views
- Customizable Attribute Mapping
- Batch and Scheduled Provisioning
- Account Migration & Alias User Support
- Central User Auditing

» Web Based User Self-Help Portal Features

- Password Policy Enforcement
- Automatic Password Expiration E-mail Notification
- Password Management & Recovery
- User Profile Management

- Tiered Security Challenge
- Self-Help Activity Logged for Auditing
- Detailed Activity and Status Reports
- User Reset Can Update Multiple Accounts

» Identity Services

- IP-to-ID, MAC-IP and Host Name
- Universal Identity Resolver (UIR)
- 3rd Party Integration Through XML API
- Monitor Events from Internal RADIUS or DHCP Services
- Monitor Events From Most 3rd Party Devices (VPN, Firewall, Switch/Router, DHCP Server, Application Server, etc.)
- Built In Support for Check Point, Cisco, Netscreen/Juniper, Fortinet, SonicWALL.
- Parse any Text Based Event Using the Generic Parser
- Retrieve Events from Syslog or Log File
- Advanced Reporting with Identity
- Login Activity
- Threshold Alerts
- Scheduled Reports with Off Device Archive

» RADIUS Authentication Protocol Support

- PAP, CHAP, MS-CHAP Versions 1 and 2
- EAP 802.1X Methods:
MD5, LEAP, PEAP, MS-CHAPv2, SIM, TLS, TTLS, GTC, OTP
- EAP Certificate Management

» RADIUS Features

- Realm Alias Support
- Realm-Based Access Control
- Multiple Policies per User
- NAS-Based Policy per User
- Group-Policy Configuration
- Group-Default Profile Configuration

- Group-Level Access Control
- Group-Device Access Control
- Concurrent Session Control
- Inactivity Timed Policy Control
- Scheduled Group Policy Control
- Time Based Usage Quota
- Multiple Accounting Formats:
Cisco TACACS, Free RADIUS, Livingston, MERIT v2

» DHCP Features

- Authenticated DHCP
- High Performance DHCP Server
- Microsoft Network Access Protection (NAP) Enforcement Point*
- Web Based Guest Access Portal
- Detailed Lease Reports
- Integrated with ID Correlative
- Blacklist Notification

» Management Features

- Secure Web GUI (HTTP and HTTPS)
- SSH and RS-232 Serial Console
- SecurID and RADIUS Support for Management Access
- Advanced Command Line Interface (CLI)
- SNMPv1, v2
- Encrypted Passwords
- Secured Updates, Backup & Restore
- Multiple Language Support
 - ♦ English, Japanese, Simplified and Traditional Chinese

» Capacity

	IDsentrie 1000	IDsentrie 2000
• UIM Devices	400	800
• UIM Users	10000	30000
• RADIUS Users	10000	20000
• IP to ID Events	10 Million	30 Million
• IP to ID Estimated Retention	30 Days	90 Days*
• Log Events	500K	1000K

*Version 2.3 and Up

» Hardware Specifications

	IDsentrie 2000	IDsentrie 1000
Processors	Dual Processor, Dual Core	Single Processor
Interfaces	8 x 10/100/1000 BaseT (Gigabit Over Copper) + 2 SFP Fiber Ports 12 x 1000BaseT (Gigabit Over Copper) Management Through Ethernet Port 1 x RS-232 Serial Console Port	4 x 1000BaseT (Gigabit Over Copper) Management Through Ethernet Port 1 x RS-232 Serial Console Port
Dimensions	3.5 in (H), 17.0 in (W), 24.0 in (D) 8.89 cm (H), 43.18 cm (W), 60.96 cm (D) Weight 35 lbs (17.0 kg), 2 U Rack Mountable	1.75 in (H), 17.0 in (W), 19.5 in (D) 4.45 cm (H), 43.18 cm (W), 49.53 cm (D) Weight 17.6 lbs (8.0 kg), 1 U Rack Mountable
Power Supply	Redundant Power Supply with Smart Fan AC Input Voltage 100 to 240 VAC Frequency 50 to 60 Hz 460 W DC Each Removable	AC input voltage 100 to 240 VAC Frequency 50 to 60 Hz Single Power Supply 300W Max
Fan	3 Removable Smart Fans	Single Fan
Flash Memory	128M	128M
Hard Drives	Removable Dual 160G, RAID 1	160G
Regulatory Certification	FCC Class A, UL, CE, TUV, CB, VCCI	FCC Class A, UL, CE, TUV, CB, VCCI
Warranty	90-day Hardware and Software Standard	90-day Hardware and Software Standard