# ID SERIES

## Network Identity Management

### Supported Platforms

ID Series
physical appliance

### Overview

Using a modular, agent-less approach, ID Series connects into multiple user directories, operating systems and networking devices, enabling a series of advanced identity management functionality. The ID Series approach has drawn praise for providing multiple identity services on a single appliance, vastly reducing operational complexity and installation time.

## Save Hours While Resolving Security Issues

The ID Series is a network identity management appliance with instant user identity resolution, which helps organizations save hours everyday and minimize risk by resolving security issues faster. The ID Series 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.

## ID Series Main Components

### 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. ID Series' 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 ID Series 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 ID Series 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. ID'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 ID Series 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 ID, 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. ID's rich reporting and auditing features provide full visibility to allow IT departments to work more effectively.

## ID Series Features

### 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 and Group Provisioning and Management
- Central Password Policy Enforcement
- Identity Attribute Synchronization
- Account Password and Data Synchronization
- Customizable Provisioning Views
- Customizable Attribute Mapping
- Batch and Scheduled Provisioning
- Account Migration and 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 AccountsLayer 2 and Layer 3 Support

### 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

### Management Access

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

### ID 1100 Capacity

- UIM Devices: 400
- UIM Users: 10,000
- RADIUS Users: 10,000
- IP to ID Events: 10 million
- IP to ID Estimated Retention: 30 days*
- Log Events: 500K

*Version 2.3 and up


**ID 1100**

## ID Series Hardware Summary

| ID 1100 | |
|---|---|
| Processor | • Single Quad Core |
| Interface | • 4 x 1000BaseT (Gigabit Over Copper<br>• Management Through Ethernet Port<br>• 1 x RS-232 Serial Console Port |
| Dimensions | • 1.75 in (H), 17.3 in (W), 16.7 in (D)<br>• 4.4 cm (H), 43.9 cm (W), 42.4 cm (D)<br>• Weight 16 lbs (7.3 kg), 1 U Rack Mountable |
| Power Supply | • AC Input Voltage 100 to 240 VAC<br>• Frequency 50 to 60 Hz<br>• Single Power Supply 250 W |
| Fan | • Single Fan |
| Flash Memory | • 1 GB |
| Hard Drives | • 250 GB |
| Regulatory Certification | • FCC Class A, UL, CE, TUV, CB, VCCI |
| Warranty | • 90-day Hardware and Software Standard |

## About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**


### Corporate Headquarters

**A10 Networks, Inc**
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

### Worldwide Offices

**North America**
sales@a10networks.com
**Europe**
emea_sales@a10networks.com
**South America**
brazil@a10networks.com
**Japan**
jinfo@a10networks.com
**China**
china_sales@a10networks.com
**Taiwan**
taiwan@a10networks.com
**Korea**
korea@a10networks.com
**Hong Kong**
HongKong@a10networks.com
**South Asia**
SouthAsia@a10networks.com
**Australia/New Zealand**
anz_sales@a10networks.com


To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.

Part Number: 15107-EN-03 Feb 2014