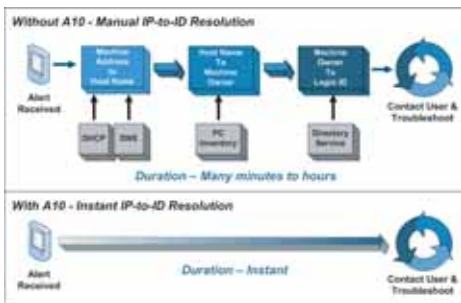


Resolve Critical Problems Faster

Resolving user identity information has always been a critical part of managing corporate networks and securing data resources. As security concerns increase and regulations drive demand for better logging and internal controls, companies are searching for more efficient ways of tracking and recording user activity across the organization.

Traditional methods of correlating network activity to individuals have always been difficult and time consuming. The task of manually researching MAC and IP addresses requires correlation of entries from multiple logs stored on different systems which are often times owned by a variety of teams. Manual backtracking often takes hours allowing for the further spread of security breaches and infections while IT teams work to track down the individual responsible for an event alert.

A10 Networks' IP-to-ID Service within the IDsentry appliance is a revolutionary technology designed to automate identity resolution by seamlessly integrating with existing networking and security devices as well as logging and reporting systems. The IP-to-ID Service minimizes troubleshooting and forensic efforts and helps to ease compliance and internal control requirements.



IP-to-ID Service Solutions and Benefits

► Identify Users Instantly

Solutions:

The IDsentry IP-to-ID Service provides a variety of ways to instantly identify a user behind an alert for critical events such as a security breach, network anomaly or traffic spike.

Benefits:

The source of critical issues can be identified with minimal effort allowing IT teams to address problems quickly and reduce the time threats have to spread and affect other areas of the organization. Time and money is saved by minimizing employee downtime, forensics efforts and post incident clean-up.

► Stop Malicious User Access

Solutions:

IT staff can immediately disable user access to multiple resources and applications with the click of a button through the IDsentry provisioning GUI.

Benefits:

Minimize the spread and damage of an issue by limiting a user's access to the network and resources. User access can be temporarily disabled while an incident is being addressed and then re-enabled after it has been resolved.

► Enhance Logs and Reporting

Solutions:

Integrates with current logging infrastructure to add user identity into log files and reports. The IDsentry provides over 140 different reports using information from a variety of network and security devices.

Benefits:

Logs become much more useful and meaningful when events are associated with a real user. The IDsentry Identity Event Manager (IEM) provides the ability to look at trends and events in the network based on user and not just IP address.

► Simplify Compliance Requirements

Solutions:

Integrate identity directly into log files that are stored for compliance purposes.

Benefits:

Eliminate the need for manual correlation of user names to events. Respond to auditor requests much faster to help lower compliance costs as well as overhead on supporting teams. Eliminate the complexity of identifying users months or years after an event.

IP-to-ID Service Details

Integration with IDsentrie GUI

Customers can leverage the IP-to-ID Service right out of the box with the IDsentrie management interface. User names can be resolved and associated with events instantly, reducing the time required to troubleshoot network issues and track down users causing security problems.

► Instant User Identification

Perform ad-hoc searches using an IP or MAC address to find an associated user name. Query using a single point in time for a specific event or with a date/time range to see all users associated with an IP or MAC in a defined period.

IP Address:	Start Time:	End Time:
192.168.12.20	2006-12-01 12:16	2006-12-12 12:16
User Name	Start Time	End Time
abourdain	Sat Dec 2 09:13:00 2006	Sat Dec 2 09:40:00 2006
abourdain	Sun Dec 3 08:25:00 2006	Sun Dec 3 08:30:00 2006
abourdain	Mon Dec 4 08:19:00 2006	Mon Dec 4 07:30:00 2006

► Track Activity By User

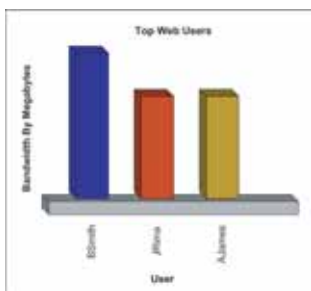
Perform a query with a user name to see all logon and logoff activity along with associated IP addresses for a given user for a defined period of time.

► Logon Activity Reporting

The IP-to-ID Service allows for the query of all login activity within a given period of time to easily identify who logged in, when they logged in and the IP address that they were assigned at that time.

► Enhanced Syslog Reporting

The integrated Identity Event Manager (IEM) integrates with the IP-to-ID Service to add identity into syslog events from a variety of networking and security devices. The IEM reporting capabilities provide the tools to see exactly who is doing what and when on the network.



Easy To Use Tools for Identity Resolution

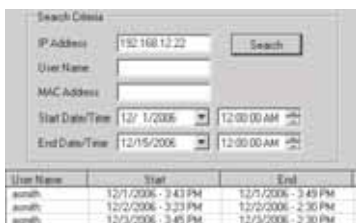
A10 Networks offers bundled tools to integrate with the IDsentrie IP-to-ID Service giving IT staff flexible options to perform identity resolution.

► Universal Identity Resolver (UIR)

Open any text-based file (e.g. syslog, event log, application log, etc...) and instantly resolve an IP address to a user identity. Simply highlight an IP address in question, select query and the IDsentrie sends back the user ID in less than a second. The UIR can also be used to resolve all IP addresses to user IDs in a given file.

► Universal Identity Resolver (UIR) Toolbar

A lightweight tool targeted at those who need to resolve problems quickly. The UIR toolbar sits in the Windows system tray and is quickly launched to resolve user identities. Enter an IP or MAC address, specify a date/time range, click search and user identity is returned in less than a second. Search with user name returns associated IP addresses.



Integration with 3rd Party Tools and Devices

The A10 Networks IP-to-ID Service easily integrates with security and networking devices and applications such as firewalls, intrusion detection and prevention systems (IDS/IPS), and network analyzers to extend the reach of instant identity resolution.

► WildPackets UIR Plug-In

This free of charge plug-in integrates with the WildPackets Omni Peek and OmniPeek Personal platforms to deliver the first identity-based network analyzer. User identity is integrated in real time as packets are captured to add more meaning to the analysis of activity. Identity is also integrated into the peer map to see the resources that users are interacting with.

Packet	Source	Destination	Flags	Size
3202	cmurphy	IP-209.62.186.9		64
3203	IP-209.62.186.9	cmurphy		1518
3204	cmurphy	IP-209.62.186.9		64
3205	IP-209.62.186.9	cmurphy		1518

► Batched Syslog Processing

Customizable tools are available to turn any log file into an identity-based log file in a matter of seconds making them more readable, meaningful and usable. Identity-based logs can be used to simplify compliance requirements by eliminating the need to manually correlate logged events to the associated end user.

► Snort Intrusion Prevention (IPS) Integration

With the IP-to-ID Service integration example, Snort IPS events can be associated with a user identity as they are logged. This integration allows Snort alerts to be sent to an e-mail address, pager or other alerting device with integrated identity in addition to other user contact information to simplify the process of identifying and contacting the user in question.

```
Mar 18 16:23:06 localhost snort: [1:0:0] ALERT {UDP} 192.168.1.89 (humlser):137 -> 192.168.1.255 ():137
Mar 18 16:23:48 localhost snort: [1:0:0] ALERT {UDP} 192.168.1.89 (humlser):137 -> 192.168.1.255 ():137
Mar 18 16:24:20 localhost snort: [1:0:0] ALERT {UDP} 192.168.1.110 (krivera):138 -> 192.168.1.255 ():138
```

Secure Access

Access to IDsentrie's IP-to-ID Service is secure to protect sensitive data and to ensure that only authorized individuals have access.

► GUI Authentication

The IDsentrie interface requires administrative authentication with a user name/password and optional authentication token so that only authorized users can access the management interface and IP-to-ID Service tools.

► External Communication

Communication with external devices and applications is done using an encrypted connection to ensure privacy of data as it travels across the network. In addition devices using the IP-to-ID Service must authenticate with the IDsentrie before making an IP-to-ID translation request to ensure that only those that are authorized have access to this information.

Network Identity Management Solutions

IDsentrie is the industry's only appliance delivering integrated features that resolve IP addresses to identity (IP-to-ID) instantly, improve help desk efficiency, simplify user account management, and enhance network authentication and access control. For more information, visit A10 Networks at <http://www.a10networks.com>.

© 2005, 2006, 2007 A10 Networks, Inc. All rights reserved. A10 Networks and IDsentrie are registered trademarks of A10 Networks, Inc. All other trademarks are the property of their respective owners.