

# Identity Management ROI Calculation Case Study

March 2006



*Think IDentity*

## Table of Contents

INTRODUCTION.....	3
IDENTITY & ACCESS MANAGEMENT COMPONENTS.....	4
THE BENEFITS OF IDENTITY & ACCESS MANAGEMENT.....	4
INCREASED SECURITY, IN-DEPTH VISIBILITY AND COMPLIANCE.....	4
CALCULATING RETURN-ON-INVESTMENT.....	5
CALCULATING ACCOUNT & PASSWORD MANAGEMENT COSTS.....	5
SOLVING THE PROBLEM USING A10'S IDSENTRIE 1000.....	9
WHAT INDUSTRY EXPERTS ARE SAYING.....	12
SUMMARY.....	12

## Disclaimer

Although A10 Networks has attempted to provide accurate information in these materials, A10 Networks assumes no legal responsibility for the accuracy or completeness of the information. More specific information is available on request from A10 Networks. Please note that A10 Networks' product information does not constitute or contain any guarantee, warranty or legally binding representation, unless expressly identified as such in a duly signed writing. A10 Networks and IDSentrie are registered trademarks of A10 Networks, Inc.

## Obtaining More Information

For more information on A10 Networks' Smart IDentity Management solution and its IDSentrie product family, please visit A10's web site at [www.a10networks.com](http://www.a10networks.com).

## Corporate Headquarters

A10 Networks, Inc.  
2125 Oakland Road  
San Jose, CA 95131-1578  
USA

+1 (408) 325-8668 (main)  
+1 (408) 325-8666 (fax)

## Introduction

Identity and Access Management (IAM) is a critical technology for properly managing identity resources. With a well implemented IAM system, businesses achieve stronger management control of their identity resources, robust mechanisms to control network access, and enhanced tools to meet tough compliance reporting, logging, and record retention. Many Fortune 1000 enterprises have implemented IAM solutions to improve IT operational efficiency, boost user productivity, mitigate security risks, and improve authentication and access control.

But traditional IAM solutions have always been tough to justify for non-global 1000 companies with smaller IT budgets. Some of the reasons why traditional IAM solutions have been so difficult to justify and implement include:

- Most IAM solutions are software-based and require multiple components to be functional.
- Software solutions require additional servers and operating systems, raising costs and overhead.
- Expensive, per-user annual licensing fees that must be budgeted year after year.
- Long deployment cycles that require many hours of professional consulting services, raising deployment costs significantly.
- Can be intrusive to existing applications, requiring customization and making it difficult to integrate.
- Often requires the migration of user accounts from departmentally or geographically separate data stores into one centrally managed Meta Directory, causing difficulties with existing organizational and management structures.
- Many traditional IAM solutions are point-play solutions that do not offer a full IAM suite. For example, some offer account provisioning, but not authentication, others offer User Self-Help but not user account management, etc.
- Many require steep learning curves and the complete re-education of IT resources.

What many companies fail to realize is that the benefits of IAM can be achieved without the headaches and long deployment cycles associated with traditional full suite IAM solutions. By carefully selecting just a few of the most popular identity management solutions, businesses can recover valuable IT resources and improve operational efficiency.

This whitepaper highlights two popular IAM features that are part of IDSentrie's unified IAM solution and illustrates how IAM projects can be justified for quick return-on-investment (ROI).

## Identity & Access Management Components

Identity management is a system of integrated components that enable organizations to properly authenticate, provision, manage, synchronize, and track user and application activity across the enterprise. There are many different types of Identity and Access Management solutions that range greatly in price, deployment difficulty, and functionality. The major IAM categories include the following:

**Full Suite Solutions** - provide complete solutions with directory services, provisioning, self-help, single sign-on, secure access and Federated identity elements. These solutions are complex and expensive to deploy.

**Provisioning Solutions** – provide account life cycle management with account, workflow, and role-based provisioning. Many provisioning solutions provide user self-service and single sign-on extensions and are less complex than full suite solutions, but are still too expensive for most companies.

**Secure Access Solutions** – provide strong multi-factor authentication with hardware tokens, smart cards, biometrics, certificates, and single sign-on. Does not provide any account life cycle management and are typically high in management overhead.

**Federated Identity Solutions** – provide access and trust policies based on virtual communities. Single sign-on for partner, vendor, and application access and requires modification and upgrading of most applications and systems. Standards are being defined and there is very little Federated technology implemented in production environments.

## The Benefits of Identity & Access Management

By implementing a well-planned IAM solution, corporations can reap many benefits that can help improve operational efficiency, reduce security risks, improve visibility, and enhance compliance and internal controls. The benefits of A10's IDSentrie 1000 solution include:

### **Improved Efficiency and Minimized Management Overhead**

- Centralized account management simplifies account provisioning and termination, and reduces the management overhead associated with manually provisioning multiple data stores.
- Synchronized identity information reduces errors, improves security and user experience.
- Centralized authentication policies consolidate authentication and access control services.
- Authentication Proxy services decrease deployment times and eliminate the need for additional user accounts and passwords.
- User Self-Help services increases user productivity and reduce IT and help desk involvement.

### **Increased Security, In-depth Visibility and Compliance**

- Centralized account management identifies unauthorized & stale accounts.
- Identity-based reporting & logging correlates user activity with identity information to take the mystery out of network troubleshooting and forensics.
- Compliance and internal controls are enhanced with identity-based logging and reporting and the ability to archive activity and identity logs for long durations.

**Reduced Complexity and Lower Cost**

- Simplifying password management reduces complexity and reduces the number of help desk issues related to password resets and account provisioning.
- Centralized management reduces learning times associated with managing many dissimilar data stores.
- Appliance model simplifies deployment and reduces cost of entry.
- Chassis licensing model eliminates costly year-over-year subscription costs.
- Rapid deployment (within a few hours to days) allows businesses to quickly see the benefits of IAM.

**Calculating Return-on-Investment**

Calculating the actual IAM costs and return-on-investment for an IAM project will depend on two main factors - the IAM features deployed and the salary and operational expenses for the company. The two IAM features that are easiest to justify and calculate ROI for are Centralize User Account Provisioning and User Self-Help Services.

What many small and medium-sized businesses don't realize is that the benefits of identity management can be obtained without the complete installation of a Full Suite IAM Solution or an expensive Provisioning System. By carefully analyzing their needs and strategically selecting a few well-placed IAM functions, all companies can quickly reap the rewards of identity management and reduce their security exposure and operational costs.

**Calculating Account & Password Management Costs**

IDSentrie's Unified IDentity Manager (UIM) provides a powerful management platform to completely centralize account provisioning and management by aggregating identity information from dissimilar and separate data stores into one manageable Virtual Directory Service. UIM gives IT managers a complete picture of all identity information spread across their business.

New account additions, changes, and deletions are automatically reflected in all managed data stores to reduce provisioning overhead. By centrally enforcing password policies and synchronizing user information across all corporate data stores, mistakes caused by data entry errors are virtually eliminated - reducing potentially costly and dangerous errors.

To help demonstrate the process of analyzing the need for identity management and creating the justification, A10 Networks created an ROI calculator to help automate the calculations. The A10 Unified IDentity Manager (UIM) ROI Calculator was developed with industry data gathered from its customers and Technical Advisor Board to simulate actual IT and help desk experiences.

To see how much IDSentrie can save your company, please download A10's UIM ROI Calculator from A10 Networks' web site and follow along with your company's statistics and usage guidelines. A10's UIM ROI Calculator can be found at: <http://www.a10networks.com/resources>

## ROI Calculation for ABC Company

This example illustrates the justification process for a medium sized company and shows the procedures taken to gather information for each of the calculation steps.

### **Step 1: Understanding the Project Scope**

ABC Company employs **1500 employees** in three different locations - California, Boston, and the United Kingdom. ABC Company uses **five separate data store** types (LDAP, Active Directory, Linux, Solaris NIS, and SecurID) to control access to their network and business applications. Each employee uses a separate account to access each application and to gain access to the network. The number of accounts assigned to each employee is dependent on their application and access needs.

- For email service, users authenticate to the corporate LDAP server.
- For file and print services, users authenticate to the corporate Active Directory service and/or to Solaris NIS.
- For business applications, users are assigned multiple accounts that are either managed by the application's data store natively or on the corporate LDAP data store.
- 70% of the user base has both Unix and Windows access.
- For remote access, all users must be issued a SecurID hardware token (2 factor authentication)

Most of the commercial business applications are authenticating to the corporate LDAP server, but many of the home grown applications developed by the various departmental MIS groups require users to login to local Linux data stores that are servicing the application. ABC Company's users have a minimum of 3 accounts with an **average of 5 user accounts** being the norm for most employees.

To comply with the company's Computer Usage Policy, administrators require tough password selection and rotation on **four of the five** data stores **every 90 days**, once per quarter, and SecurID users are not affected. ABC users cannot select previously used passwords, as a history of the last 10 passwords is enforced. Various tough password syntax enforcement filters have been implemented on each data store type to ensure users select strong passwords.

Currently, ABC Company does not use any IAM productivity tools and performs manual account provisioning to each of the five data stores. Interviews with the Help Desk Manager and a sampling of the user population show that users are unhappy with the current setup. They are required to remember and manage too many accounts and passwords and are mandated to change their passwords at different times. With four data stores enforcing password rotations in an **unsynchronized fashion**, users are complaining that they are constantly changing passwords - and having to remember which password goes with which application has been a **big challenge** for many. Both users and help desk technicians cringe whenever the next password change interval is due – as the volume of help desk tickets and frustrated users rise.

To simplify this problem, many users have created their own solutions. They have been writing down their passwords and saving them by their desks or have been storing them on their cell phones, PDAs and notebook computers in unsecured text files. This has ABC's Security Manager extremely worried as many of his users are not following the company's Computer Usage Policy and **exposing the firm** to unnecessary risk.

ABC Company is located in San Jose, California – the heart of Silicon Valley where salaries and operational costs tend to be higher than the national average. ABC Company is an engineering firm and a majority of their end user population are highly skilled employees. HR has supplied the average wage scale for calculating the ROI, and to keep the calculations simple, average wage figures **do not include** company benefits or other incentive programs offered by ABC.

- Senior System Administrator = **\$85,000** USD per year
- Help Desk Engineer = **\$68,000** USD per year
- End User Population = **\$75,000** USD per year

ABC projects that its current **growth rate is 7% year-over-year** for the next two years and HR has described the company's employee **termination rate as 10%**. ABC Company has grown rapidly the last few years and proper project planning has not always been done. Most identity management tasks are still performed manually, but ABC now realizes the need for structured and automated identity and access management as complaints and mistakes are rising with each new employee added.

## Step 2: Calculating the Salary Costs

Taking the information supplied by the project scope analysis, calculate the cost of doing business using the A10 UIM ROI Calculator.

Deployment Size Calculation Parameters		Customer Supplied Values	Comments
Total number of users in your company		1500	
Average number of accounts per employee		5	Assumes one password per account

  

Personnel Calculation Parameters	Annual Salary Rate	Calculated Hourly Rate	Comments
Average Salary of System Administrators	\$85,000	\$41	Account adds, changes, deletes for each account in various data stores managed
Average Salary of Help Desk Personnel	\$68,000	\$33	Password maintenance, account provisioning, password resets, unlocking accounts
Average Salary of End User Personnel	\$75,000	\$36	Authentication, password entry, account modifications, non-productivity time

Figure 1: Breakdown of salary and hourly rates for various employee types

Figure 1 shows the annual and hourly salary rates for the System Administrators, Help Desk Technicians, and average wages for the user population at ABC Company. The hourly rates are used to calculate the cost for account provisioning, password resets, account changes, account deletions, and so forth.

## Step 3: Calculating the Cost of HR Generated Account Provisioning

When gathering the project scope information it was also noted that there were **two types of account provisioning** tasks performed by system administrators and help desk technicians. System administrators were primarily responsible for servicing the company's HR account provisioning requests - creating accounts for new employees, assigning access rights, and disabling or deleting accounts when employees left the company. Help desk staff were primarily responsible for existing users' account and password provisioning requests.

Lists for new hires and terminations are supplied by Human Resources and are emailed to **12 system administrators** in the security, networking and system administration groups for the 3 locations. One of the serious downsides of this manual procedure is the time zone difference between the three offices. Frequently, **accounts are not deleted** as fast as the company would like - with some accounts for terminated employees existing for several days afterwards.

From the information gathered, we can estimate the number of account provisioning tasks performed by the System Administration team for the year.

Terminations: 1500 employees X 10% attrition rate = **150 terminations** per year

Back Fill Hires: **150 back fill hires** per year

New Growth Hires: 1500 employees X 7% growth rate = **105 new hires** per year

Total Provisioning: (150 terminations + 150 back fills + 105 new hires) X an average of 5 accounts / user = 2025 tasks

With a 7% growth rate estimated over the next two years, the amount of provisioning will increase for system administrators. The increased volumes for HR generated provisioning requests are:

Current Year: 2025 provisioning tasks

Second Year: 2167 provisioning tasks

Third Year: 2319 provisioning tasks

Personnel Expense Calculation Parameters			Annual Salary Rate	Calculated Hourly Rate	Comments
Average Salary of System Administrators			\$85,000	\$40.87	Account adds, changes, deletes for each account in various data stores managed
Average Salary of Help Desk Personnel			\$68,000	\$32.69	Password maintenance, account provisioning, password resets, unlocking accounts
Average Salary of End User Personnel			\$75,000	\$36.06	Authentication, password entry, account modifications, non-productivity time
HR Generated Provisioning Cost Parameters			Customer Supplied Values	Calculated Values	Comments
Employee Termination or Attrition Rate			10.00%	150	Employees terminated annually
Company Growth Rate			7.00%	105	New employees hired annually
Backfill Hires			150		Backfilled employees to retain growth rate
<b>Total HR Employee Provisioning Tasks</b>				<b>2,025</b>	Total HR provisioning accounts times the average number of accounts per user
<b>Administrative Provisioning Cost</b>				<b>\$4,138</b>	Administration calculation uses .05 hours average provisioning time per employee per data store multiplied by the System Admin hourly rate

Figure 2: HR Generated Provisioning Cost Calculation for Current Year

#### Step 4: Calculating the Cost of User Generated Account & Password Support

The majority of manual identity management costs can be associated with provisioning and issues rising from the existing user base. To gain an understanding of the overall provisioning and password management workloads, the following assumptions can be made from the information provided by ABC Company:

- 1500 users X 5 average accounts each = 7500 user accounts requiring management
- 4 mandated password changes per year X 7500 user accounts = 30,000 mandatory password changes / year
- 30,000 password changes / 1500 users = minimum of 20 password changes / year for each user
- All help desk and account provisioning requests are logged and controlled with ABC's Help Desk Ticketing System and the cost per incident takes the following into account:
  - Time user takes to log a trouble-ticket with the help desk dispatch center
  - Time taken to dispatch the ticket to a technician
  - Technician's time to resolve the problem
  - Technician's time to close the trouble-ticket in the help desk system
  - Non-productivity time experienced by the user when their account is locked out

To fully understand the frequency of user generated account provisioning and password related help desk issues, research was conducted by interviewing system administrators, help desk personnel, and a sampling of end users. The study also included the analysis of ABC's help desk ticketing system reports for the previous 6 months to gain an accurate picture of ABC's help desk ticket trends.

From the study, the following information was obtained for the last 6 months and extrapolated to an annual basis:

- The average number of times a user requires a password reset is 6 times a year
- The average number of times a user requires account provisioning is 4 times a year
- 40% of the user population has placed a password reset request in the last year
- 33% of the user population has placed an account provisioning request in the last year
- Average time to reset a locked account or lost/stolen password is 1 hour
- 20% of user requests are solved by system administrators when help desk personnel is unavailable

Figure 3 illustrates how the Total Employee Generated Account & Password Cost is generated using the information provided by ABC Company.

Employee Generated Provisioning Cost Parameters	Customer Supplied Values	Calculated Values	Comments
Number of times per year user forgets a password	6		
Number of times per year user requests provisioning	4		
Percentage of users with password problems	40%		
Percentage of users with provisioning requests	33%		
Percentage of employee requests services by System Administrators	20%		
Percentage of employee requests services by Help Desk Technicians		80%	
<b>System Administrator Provisioning Cost:</b>		\$38,081	Administration calculation uses an average of 10 minutes per employee per data store. Includes trouble ticket generation, ticket dispatch, resolution and closure.
<b>Help Desk Provisioning Cost:</b>		\$121,859	Help desk calculation uses an average of 10 minutes per password and account issue. Includes trouble ticket generation, ticket dispatch, resolution and closure.
<b>Employee Non-Productivity Cost:</b>		\$129,808	Calculation uses a 1.0 hour non-productivity time average per password incident caused by locked out accounts.
<b>Total Employee Generated Cost:</b>		\$289,747	
<b>Total Provisioning &amp; Management Costs:</b>		\$293,885	Adds HR and Employee generated costs

Figure 3: Employee Generated Provisioning Cost Calculation for Current Year

### Step 5: Calculating the Annual Cost & IT Resources

From the A10 UIM ROI Calculator, the total cost for ABC Company's account provisioning and user account support is approximately **\$294K USD** for the current year. Based on the 7% growth projection, the cost will rise to \$315K for the 2<sup>nd</sup> year and \$337K for the 3<sup>rd</sup> year. Based on the average annual IT salary, ABC employs **4 full-time IT head counts** just for account and password management.

## Solving the Problem Using A10's IDSentrie 1000

ABC Company purchased A10's IDSentrie appliance to help solve two of their most pressing identity resource management issues – account provisioning and password management. With IDSentrie's drop-in appliance, installation, training and rollout was completed in under a week for ABC's three locations. After using the system for 3 months, ABC Company noticed a significant reduction in the number of help desk calls and the amount of time system administrators spent provisioning and managing user accounts on the various disparate data stores.

### Operational Analysis with IDSentrie Deployed

- With IDSentrie's Unified IDentity Manager (UIM) component, the number of provisioning tasks performed by system administrators was dramatically reduced. Central provisioning allowed system administrators to reset passwords and create, change, and delete accounts from the IDSentrie console instead of provisioning account information to each data store and business application separately. From ABC's experience, this had the **virtual effect of reducing** the average number of accounts per user **from 5 to 1** - as administrators only had to log into one system to provision account information using IDSentrie.
- With UIM's Password Synchronization service, administrators and users no longer had to manually change passwords for each data store. Synchronized passwords lowered the number of password

incidents significantly as users no longer had to remember different passwords for each data store. The number of times ABC users forgot their password was reduced **from an average of 6 to just 2 times** per year.

- With Self-Help Service's Password Expiry Notification, users are **automatically sent** a password change reminder from IDSentrie 5 days before their passwords expire. Using the hyperlink to access the Self-Help portal, **users can now change and reset passwords** without calling the IT help desk. The service has also significantly **reduced the number of locked-out accounts** that were normally experienced with the manual system.
- Enforcing 4 mandated and **unsynchronized** password changes per year caused many users to forget which password was associated with each account and application – causing help desk volumes to rise sharply after each mandated password change cycle. This problem has been greatly reduced.
- With IDSentrie's User Self-Help service, the number of account resets, password changes, and password recoveries that were once handled by the help desk and system administrators has been significantly reduced. After 3 months, ABC found that **60% of their user population** used IDSentrie's Self-Help service to make their own changes. This reduced the percentage of password related issues that had to be resolved by the help desk to an average of **16%**.
- With 60% of the user population using the Self-Help portal, the remaining percentage of account provisioning requests that had to be resolved by the help desk was reduced to an average of **13%**.

Some of the harder benefits to monetarily measure included the security benefits offered by central provisioning and password management. For ABC Company, these included the following:

- By reducing the number of passwords users must now remember, ABC has also learned that users are now less likely to write down their passwords or store them in insecure devices – such as cell phones, PDAs and notebook computers – mitigating security risks that were caused by the old manual system.
- With UIM's Central Password Policy, ABC can now enforce tough password selection across all of their data stores to ensure that the corporate security policies were being adhered to. This helped to reduce the level of risk caused by weak password selection.
- User productivity and satisfaction were improved significantly as the frustration and complexity of managing their passwords were solved with IDSentrie's services.

### Step 6: Calculating the Post IDSentrie Costs

To calculate the cost savings, we can use the ROI calculator to calculate the operational costs with the new parameters obtained after IDSentrie was installed and deployed. The average number of accounts/passwords per user has been effectively reduced to 1 with IDSentrie's ability to centrally manage accounts and passwords.

Deployment Size Calculation Parameters		Customer Supplied Values	Comments
Total number of users		1500	
Average number of accounts/passwords per user		1	

  

Personnel Expense Calculation Parameters		Annual Salary Rate	Calculated Hourly Rate	Comments
Average Salary of System Administrators		\$85,000	\$40.87	Account adds, changes, deletes for each account in various data stores managed
Average Salary of Help Desk Personnel		\$68,000	\$32.69	Password maintenance, account provisioning, password resets, unlocking accounts
Average Salary of End User Personnel		\$75,000	\$36.06	Authentication, password entry, account modifications, non-productivity time

Figure 4: Post IDSentrie Account Volume Calculation

With the average number of accounts and passwords per user reduced to 1, we can see that provisioning and terminating accounts as directed by ABC's HR department is dramatically simplified. With IDSentrie's UIM component, system administrators are no longer manually provisioning to 5 separate data stores for each user – reducing the HR provisioning costs by approximately 80% (from \$4138 to \$828).

HR Generated Provisioning Cost Parameters		Customer Supplied Values	Calculated Values	Comments
Employee Termination or Attrition Rate		10.00%	150	Employees terminated annually
Company Growth Rate		7.00%	105	New employees hired annually
Backfill Hires		150		Backfilled employees to retain growth rate
<b>Total HR Employee Provisioning Tasks:</b>			<b>405</b>	Total HR provisioning accounts times the average number of accounts per user
<b>Total System Administrative Cost:</b>			<b>\$828</b>	Administration calculation uses an average of 3 minutes provisioning time per account per data store.

Figure 5: Post IDSentrie HR Generated Provisioning Costs

With users being able to resolve their own password issues and account provisioning needs, the volume of support calls to the help desk is reduced significantly. Users are much happier as they only receive one email reminder per quarter for mandated password changes. Their newly selected passwords are now automatically synchronized between all of their data store accounts, simplifying password management and improving productivity.

Employee Generated Provisioning Cost Parameters		Customer Supplied Values	Calculated Values	Comments
Number of times per year user forgets a password		2		
Number of times per year user requests account provisioning		4		
Percentage of users with password problems		16%		
Percentage of users with account provisioning requests		13%		
Percentage of employee requests services by System Administrators		20%		
Percentage of employee requests services by Help Desk Technicians			80%	
<b>System Administrator Provisioning Cost:</b>			<b>\$1,720</b>	Administration calculation uses an average of 10 minutes per employee per data store. Includes trouble ticket generation, ticket dispatch, resolution and closure.
<b>Help Desk Provisioning Cost:</b>			<b>\$5,503</b>	Help desk calculation uses an average of 10 minutes per password and account issue. Includes trouble ticket generation, ticket dispatch, resolution and closure.
<b>Employee Non-Productivity Cost:</b>			<b>\$17,308</b>	Calculation uses a 1.0 hour non-productivity time average per password incident caused by locked out accounts.
<b>Total Employee Generated Cost:</b>			<b>\$24,531</b>	
<b>Total Provisioning &amp; Management Costs:</b>			<b>\$25,358</b>	Adds HR and Employee generated costs

Figure 6: Post IDSentrie Employee Generated Provisioning Costs

Figure 6 illustrates the post IDSentrie operational costs as calculated by the A10 UIM ROI Calculator. By implementing centralized account provisioning and password management, ABC's operation cost for these two functions has been reduced to approximately **\$25K USD** per year.

### ABC's Annual Savings

ABC Company's identity management savings for the current year was **\$269K USD**.

## What Industry Experts are Saying

The benefits of IAM solutions are well known amongst industry analysts and journalists. The following quotes from 3<sup>rd</sup> party experts help validate the cost savings shown in the ABC Company Identity Management example.

*“A well implemented identity management solution can reduce administrative costs up to 78% and reduce user lost productivity by 53%”*

*- The Radicati Group, Inc. 2005*

*“The self-service password management feature alone can cut corporate costs by thousands in a matter of days – according to various studies, it reduces IT help desk calls by 40% - 60%.”*

*- The Radicati Group, Inc: Identity Management Market 2005 - 2009*

*“It turns out that helpdesk employees often spend more than half their time resetting passwords for users. An identity management system that can automatically reset passwords for users without helpdesk intervention is easy to justify.”*

*- The 451 Group: Identity Management Becomes an Essential IT Function, August 2005*

## Summary

Traditional IAM solutions have proven the benefits of identity management, but have been too expensive and hard to deploy for the masses. A10 Networks has changed the IAM market space with a unified Identity & Access Management solution called IDSentrie. IDSentrie empowers customers with the ability to quickly deploy some of the most beneficial features of identity management to quickly recover IT resources and improve user productivity.

Businesses that overlooked IAM solutions due to high costs and long deployment times can now experience the benefits of identity management with just a few of IDSentrie's IAM features. To see how much your company can save using IDSentrie, download A10's UIM ROI Calculator and run through the numbers yourself. <http://www.a10networks.com/resources>

## Contacting A10 Networks

For more information on A10 Networks' IDSentrie products, please call A10 Networks or visit A10's web site at: [www.a10networks.com](http://www.a10networks.com)

### Corporate Headquarters

A10 Networks, Inc.  
2125 Oakland Road  
San Jose, CA 95131-1578  
USA

### A10 Sales

+1-888-A10-6363 (North America toll free)  
+1-408-325-8616 (International)