

# Delivering Identity and Access Management as an Automated Service

Chris Lavagnino

CA SERVICES GLOBAL SECURITY PRACTICE

---

## Table of Contents

---

---

### Executive Summary

---

#### SECTION 1 **Toward IT Service Delivery of IAM** 2

Simplifying Through Integration

CA Stands Alone

More to Come

---

#### SECTION 2 **Examining the Business Case** 3

A Complex Process

Not Just On Boarding

What Integration Brings

Counting Up the Benefits

---

#### SECTION 3 **Inside the Integration — The CA Approach** 7

CA Service Catalog Integration

CA Service Desk Integration

CA Identity Manager Integration

CA SiteMinder® WAM Integration

Peace of Mind

---

---

#### SECTION 4 **An Eye to the Future** 11

Service Accounting

Standards-based Integration

---

#### SECTION 5: CONCLUSIONS 11

---

#### SECTION 6: ABOUT THE AUTHOR 12

# Executive Summary

## Challenge

---

Effective service management processes help organizations build a solid IT infrastructure for delivering high quality services. Identity and Access Management (IAM) solutions enable them to manage their users' identities and associated privileges while securing access to sensitive resources. Today, these IAM services are generally not available to users within a service management framework, or when they are, they still depend on manual, organization-specific procedures. Establishing the user's identity, role and access rights within the organization often involves filling out a series of forms that are transferred from one department to another to obtain the necessary authorization. A similar process is followed when an employee's personnel profile or business role changes or when his or her tenure with the organization comes to an end. The end-to-end process for any one of these operations is often manual, subject to error, and costly.

## Opportunity

---

Incorporating IAM services into an existing service management framework provides comprehensive automation for processes such as provisioning while allowing users to leverage interfaces they already use to request other IT services. The CA Identity and Access Management as an Automated Service satisfies this requirement. The integration builds upon an organization's IT service management strategy to simplify and automate the identity lifecycle management process using CA's service management solutions. Users access the organization's central point of contact for IT services, CA Service Catalog, to order IAM services, and then CA Service Catalog works transparently with CA Identity Manager to fulfill their requests. The integration also offers organizations the option to include CA Service Desk to increase the level of control over the change order process, or CA SiteMinder® Web Access Manager (WAM) to secure access to the major web components of the integration.

## Benefits

---

Encapsulating IAM services within an organization's IT service management framework provides a number of benefits. The approach:

- Enhances the quality of IT services provided by the organization, thereby increasing organizational and user productivity
- Strengthens the alignment of IAM IT services to the business needs of the organization
- Leverages the organization's single point of contact for IT services by including identity administration service requests
- Improves the organization's ability to comply to regulatory restrictions through end-to-end transaction logging and auditing functionality

---

## Introduction: Toward IT Service Delivery of IAM

To remain competitive and viable in today's business world, organizations are being challenged to supply their customers and users with high quality services using cost-effective measures. Whether these IT services pertain to users' requests for workspace, computer equipment, telecommunication services, or productivity applications, organizations are adopting service management strategies to create effective processes that automate some of their most cumbersome organizational activities. Consider the act of welcoming a new user to the organization. Today, the onboarding process is arduous, typically involving manual communication mechanisms among multiple departments. Different departments fulfill the new user's physical facility requirements, their telecommunications and computing hardware requirements, their human resources or personnel requirements, and their application security access requirements. The overall process is typically disjointed, with no single point of visibility from which to monitor it end-to-end. Streamlining and automating such processes are paramount to solidifying the competitive viability of the organization.

### Simplifying Through Integration

Beyond the basic identity administration tasks of identity provisioning, deprovisioning, and role-based identity administration, most services within the IAM domain are viable candidates to become part of an overall service management strategy. The success of such a strategy depends upon well-defined objectives and policies, as well as effective and efficient service management processes which include: 1) providing a single point of contact for service delivery (in the form of a service catalog) to facilitate users' access to IT's portfolio of service offerings; 2) ensuring the collaboration among departments by providing process components that automate the integration among disparate domains; 3) accommodating varying degrees of change management pertaining to user requests, by engaging a service desk as a single point of contact for service support; and 4) securing access to corporate resources pertaining to the Web applications that are central to the solution.

By encapsulating IAM services within an IT service management framework, the organization enhances the quality of IT services provided, thereby increasing both organizational and individual productivity. IT services become aligned with business needs and a single point of contact and interface is achieved thereby simplifying interaction with the IT infrastructure and automating the approval and fulfillment workflow processes required to complete identity administration requests. Finally, the organization obtains additional regulatory compliance benefits by virtue of the integration's end-to-end transaction logging and auditing functionality.

### CA Stands Alone

To date it has been difficult to achieve this level of integration within an organization. Few vendors offer all the required components: a service catalog, service desk, and identity and access management offerings.

Realizing this opportunity, CA is providing the CA Identity and Access Management as an Automated Service, including components and implementation services to automate identity management processes using CA Service Catalog, CA Service Desk, and CA Identity Manager. The resulting integration makes available a defined set of identity administration services within the organization's service catalog, thereby leveraging the common single point of entry for the organization's customers and users. The integration aligns with the concept of service as defined within the IT Infrastructure Library (ITIL®).

As part of ITIL's Service Level Management Service Delivery process, these services are published in the CA Service Catalog and can be ordered by users using a single interface. Following the approval processes associated with each of its service requests, the integration ensures that these requests are delivered when and where they are needed, and in a cost effective, secure, and efficient manner. The integration does this either directly through the CA Service Catalog or indirectly by optionally enabling CA Service Catalog to submit a Request for Change or Change Order to CA Service Desk. The integration also offers (as an option) CA SiteMinder Web Access Manager to protect access to the solution's Web applications.

### More to Come

The CA Identity and Access Management as an Automated Service is one of a number of integrations available from CA. As part of its Enterprise IT Management (EITM) initiative, CA has made it a priority to identify areas where customers can leverage their IT service investment in disparate organizational domains and publish these as services for the benefit of the entire organization. CA is also developing CA Catalyst, a modular application integration platform that will simplify the exchange of information among not only CA applications, but also those of other vendors. This platform will enhance the capabilities delivered by current integrations and make it even easier to implement new cross-domain opportunities in the future.

---

## SECTION 2

### Examining the Business Case

The effective use of service management tools to deliver IAM services begins with the following four functional areas:

- Provisioning a resource identity
- Changing a resource identity, such as a user's attributes or properties
- Modifying resource entitlements, such as adding a role or business function to a user
- Removing a resource identity

### A Complex Process

Examining the business processes that encompass the provisioning of a resource identity highlights the complexity that can be involved (see Figure A). While the processes of provisioning a user with the appropriate access to systems and applications vary among organizations depending upon their IT maturity level, they represent an important subset of the onboarding activities. They typically combine an overarching approval cycle with a number of forms-based email communications.

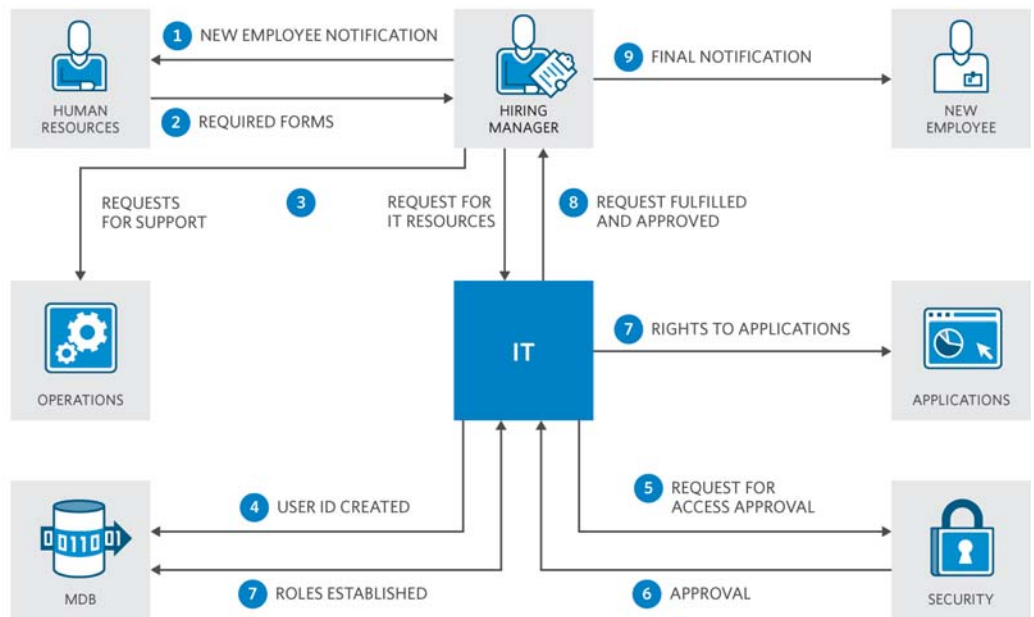
For example, a manager may have hired a new employee to fill a position in accounting. Typically, the manager must first go to Human Resources, where the manager is given a form asking for details on the employee, including the employee's title and role within the company. Human Resources also gives the manager requisition forms for resources that the employee will need. These include: physical facility requirements (cubicle, desk, chair, lamp); telecommunications and computing hardware requirements (phone, PDA, and computer); human resources requirements (corporate benefits); and provisioning or application security access requirements (access to email, office productivity, and financial applications).

To fulfill the new employee's provisioning requirements, the manager must obtain the required approvals and send the forms to people within other departments to complete specific steps. Employee data must be entered into a corporate management database (MDB). Entering such data is usually a manual function performed by IT and also entails defining a specific role for the employee, with associated access rights. Such role assignments require sign-off by the security team and the hiring manager. As a result, a ticket is opened in the service desk system. The ticket eventually goes to the security team, which circles back with the hiring manager (and his or her superiors) to verify the request. Since the process takes place via email, it can take several hours or days to complete. Once approval is granted, the security team approves the request and closes the ticket. At that point, the original IT team is informed, the role request can be fulfilled and the employee is granted access to required applications.

FIGURE A

This figure illustrates a sample scenario of how the provisioning requirements of a new employee might be fulfilled as part of a traditional onboarding process. This is a best-case scenario, assuming no delays in the process.

EMPLOYEE ONBOARDING: A TRADITIONAL APPROACH



Such a process requires extensive human interaction with no single point of oversight. If a hiring manager fails to respond to an email requesting authorization, the entire process comes to a standstill and requires manual investigation to identify the bottleneck. Meanwhile, the new employee is left without the required resources.

### Not Just Onboarding

The onboarding activities involved in provisioning a user with the necessary access to systems and applications represent just one example of how a lack of integration among IT resources can cause problems. Throughout an employee's tenure with an organization, his or her profile may continually change, whether it is a new phone number because of an office move or a new role that may require changes to their access rights, with some being added and others removed.

When an employee leaves, companies face the same problem only in reverse: removing access to all corporate resources. Such a situation presents an even more critical problem to an organization. Access to corporate resources by a former employee represents a security risk, especially if the employee left under less-than-ideal circumstances.

### What Integration Brings

A more integrated approach enables users to manage the lifecycle of identity administration services using service management tools. Managers use the simple user interface in a service catalog to order IT services. Transparently, the service catalog works with the identity provisioning manager to fulfill their requests. The solution builds upon and complements an organization's IT service management strategy to deliver high quality identity administration services using automated and cost effective measures.

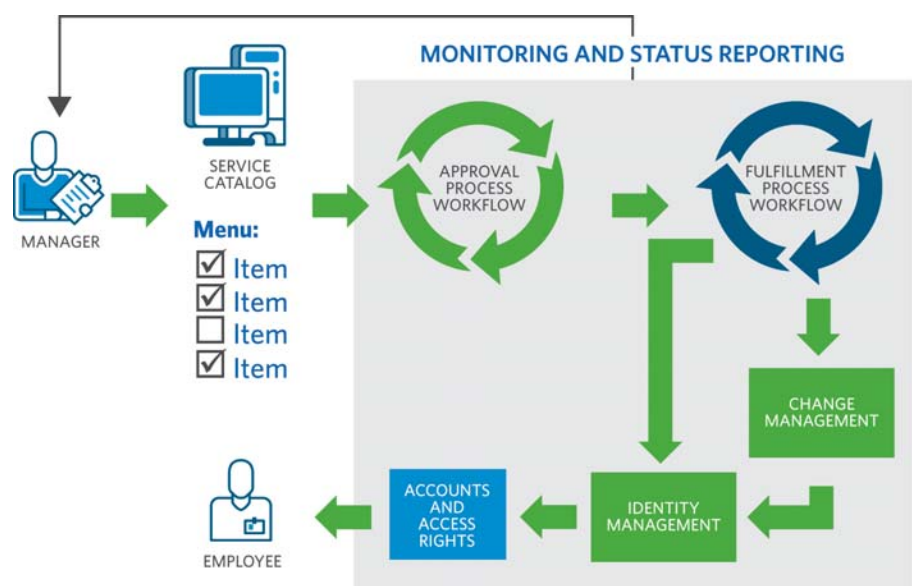
In practice, Figure B illustrates how provisioning a user could occur with the more integrated IT infrastructure approach.

Identity administration tasks are registered as services within the organization's service catalog. The hiring manager uses the service catalog to choose the IT resources the new employee needs.

FIGURE B

This example shows how the onboarding process can be streamlined and automated by integrating identity provisioning with service management tools.

THE INTEGRATED APPROACH TO IDENTITY PROVISIONING



Behind the scenes, the service catalog triggers a series of workflow processes that obtain the necessary approvals. Once all approvals are acquired, a fulfillment workflow process is executed that either triggers service desk change management to further analyze the change before submitting it to identity management, or executes identity management directly to fulfill the provisioning requests. The identity management process then creates the necessary accounts and access rights. Throughout this process, the identity management subsystem monitors the status of the provisioning request and updates the service catalog with the success or failure of the operation. Should any step be delayed, the service catalog tracks the current state of the request. Should anyone inquire as to the status of the request, support personnel can immediately determine where the process stands, thereby reducing the need to chase paper and follow email trails throughout the organization.

In a similar way, if the user changes roles or business functions or leaves the organization, the service catalog triggers a workflow process to obtain the necessary approvals, and then the same fulfillment process, as described above, takes place. While delivering these services, logs are maintained that facilitate any subsequent auditing of the changes.

### Counting Up the Benefits

Such an automated approach brings a number of important benefits to the process, including:

- Enhanced quality of IT services provided by the organization, increasing both organizational and user productivity.
- Improved alignment of business process and identity administration, allowing IT to become a business enabler. Specifically:
  - Employees get IT services delivered in a consistent fashion.
  - Security policies become more closely aligned with business goals and more consistently enforced.
  - Automation enables IT to be viewed as a service that is transparent to users.
- A single point of contact for all IT provisioning needs. Managers and users can perform either delegated administration or self-service identity administration functions.
- Central tracking, management and reporting. IAM services are delivered based upon established service level agreements.
- Improved security and compliance through:
  - Automated processes that improve consistency and accuracy in applying roles and access rights to individuals.
  - Creation of an audit trail, helping to ensure compliance with industry and government regulations.
  - Automated offboarding, which ensures that employees who have left the organization can no longer access corporate resources.
- Streamlined workflow. The integration results in a well-defined process that can be used to provision accounts, roles and access requests.
- Cost savings:
  - Less manual intervention in the procurement process means less productivity loss for all concerned.
  - Simplified training. With a single place to go for all IT service requests, educating staff on how to obtain access to systems and applications, processes is simplified.

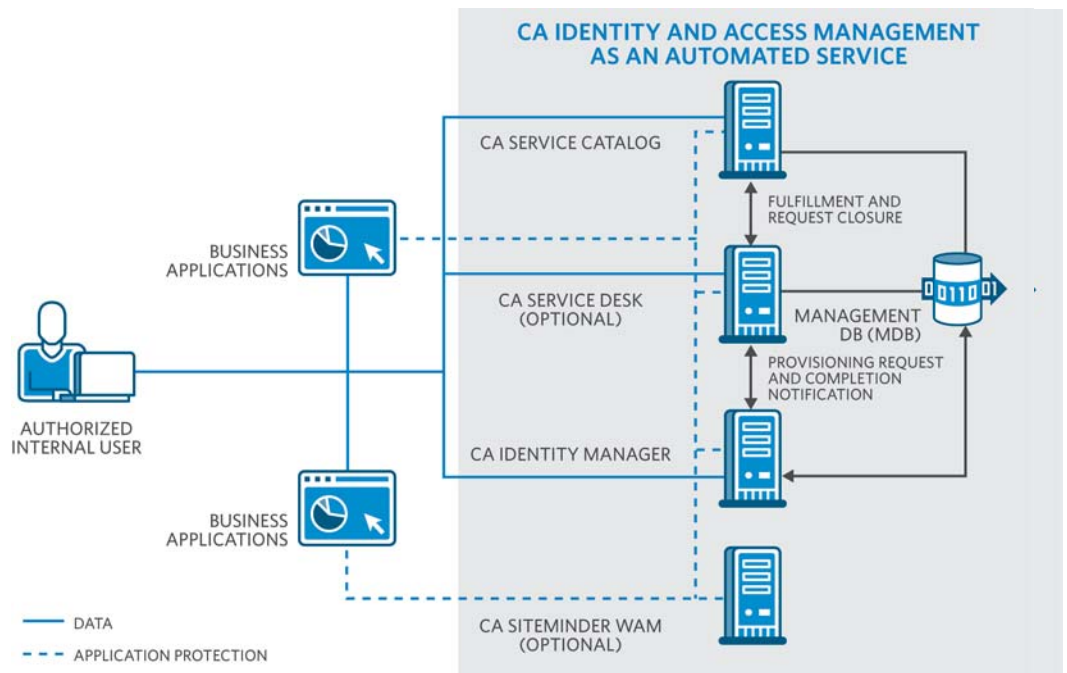
## Inside the Integration — the CA Approach

CA realizes this vision of integrating IAM IT Services within a service management framework and the benefits it brings by providing the CA Identity and Access Management as an Automated Service, a set of prebuilt components and implementation services that help customers leverage service management tools to automate identity and access management. (See Figure C.)

FIGURE C

Integrated and automated processes among CA Service Catalog, CA Service Desk, CA Identity Manager and CA SiteMinder WAM enable the streamlining of IT service request fulfillment.

### THE CA APPROACH TO SERVICE MANAGEMENT AND IAM INTEGRATION



Maintaining a list of standardized IAM services, the CA Service Catalog presents a single point of interface. Following the approval processes associated with each of its service requests, the integration ensures that these requests are delivered when and where they are needed. This is done either directly by the CA Service Catalog or indirectly by the CA Service Catalog submitting a Request for Change or Change Order to the CA Service Desk. In the latter approach, the CA Service Desk manages the request for changes or change orders and ensures that they are fulfilled and that the status of the request is updated in the CA Service Catalog. The service request is then fulfilled by CA Identity Manager. The integration optionally includes CA SiteMinder Web Access Manager to protect access to Web applications.

## CA Service Catalog Integration

CA Identity and Access Management as an Automated Service includes the following major functional integration components for the CA Service Catalog: (See Figure D.)

- Provision a resource identity:
  - Request forms soliciting basic personnel information
  - Approval workflow processes
  - Fulfillment workflow process

Managers enter the information for the user to be granted access to systems and applications, add the form to the shopping cart, and then proceed to checkout. This triggers the approval workflow process cycle, and then the fulfillment workflow process executes, sending a request to CA Service Desk or to CA Identity Manager to fulfill the identity administration request.

- Change a resource identity:
  - Request forms providing personnel information
  - Approval workflow processes
  - Fulfillment workflow process

Individual users or their managers update the contents of the request form with the desired properties, add the form to the shopping cart, and proceed to checkout. The process continues as outlined above in provisioning.

- Modify a resource identity:
  - Hyperlink to CA Identity Manager to solicit information regarding existing roles for the given user
  - Request forms providing personnel information
  - Approval workflow processes
  - Fulfillment workflow process

Individual users or their managers select application roles that they wish to have added or removed from the user's profile, add the form to the shopping cart, and proceed to checkout. The process continues as outlined above in provisioning.

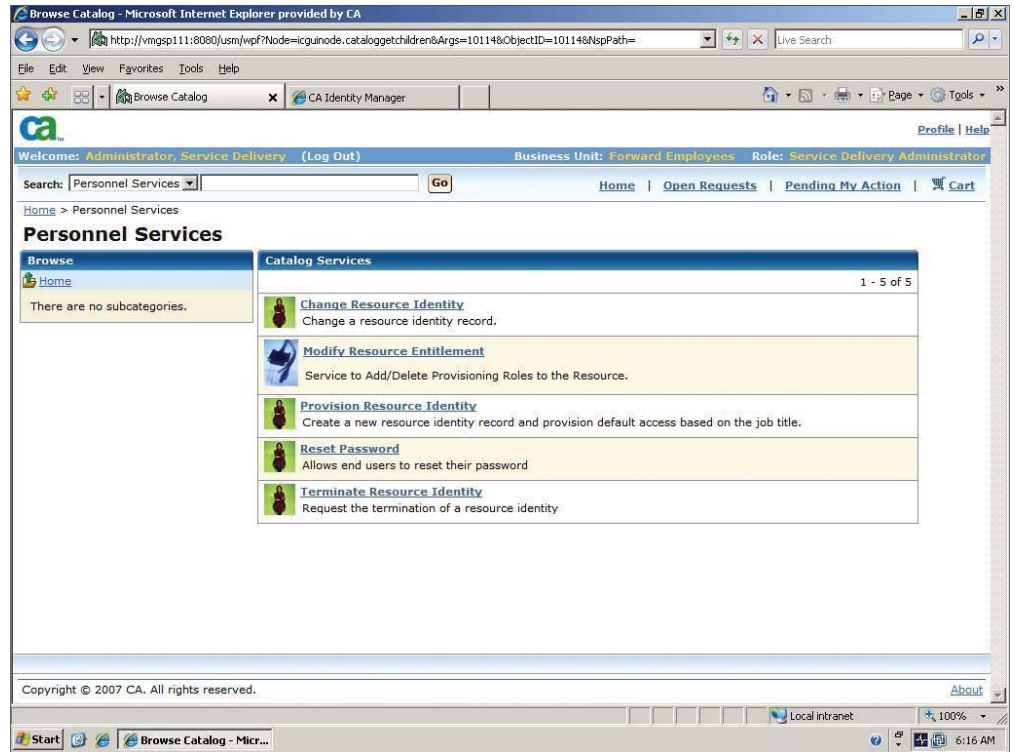
- Remove a resource identity:
  - Request forms providing personnel information
  - Approval workflow processes
  - Fulfillment workflow process

Managers select users whose accesses are to be removed from the organization's systems, add the form to the shopping cart, and proceed to checkout. The process continues as outlined above in provisioning.

FIGURE D

From the simple CA Service Catalog interface, users can perform multiple identity management related functions.

## CA SERVICE CATALOG: SIMPLIFYING IDENTITY MANAGEMENT



### CA Service Desk Integration

The CA Identity and Access Management as an Automated Service provides the organization with an option to leverage the facilities of CA Service Desk. These facilities manage all requests that are submitted by users and manage and control the risk associated with those requests.

If an organization chooses to include CA Service Desk, the integration offers two alternative process flows:

In the first, the CA Service Catalog workflow fulfillment process executes a direct call to CA Service Desk Change Management to create a CA Service Desk Change Order which launches a workflow fulfillment process once the Change Order is saved.

In the second, the CA Service Catalog workflow fulfillment process executes a direct call to CA Service Desk Request Management to open a CA Service Desk Request and assign it to the Change Management Team. The approver selects Create Change Order to copy the pertinent data from the Request and push this information into the new Change Order. The process flow then proceeds in the same manner as the first process flow.

### CA Identity Manager Integration

The CA Identity and Access Management as an Automated Service includes the following major functional integration components for CA Identity Manager:

- An identity provisioning connector to create, read, and update records in the MDB.
- A transaction acknowledgment component to maintain status of all transaction requests, acknowledge them, and log their successful or unsuccessful completion status.
- A role-object event listener component to monitor updates to identity role objects and update the solution's role table.
- A generate User ID component enabling organizations to customize the structure of the User IDs that are generated.

### CA SiteMinder WAM Integration

The CA Identity and Access Management as an Automated Service also provides an organization with the option to leverage CA SiteMinder WAM to add additional security functions to the integration. These include:

- Protecting access to CA Service Catalog and CA Service Desk to ensure that only users with proper authorization can initiate service requests.
- Protecting access to CA Identity Manager, ensuring that only authorized users can initiate requests.
- Protecting access to Web applications and ensuring that only authorized users can access web-enabled applications.

### Peace of Mind

No other vendor offers this level of integration among service catalog, service desk, and identity and access management offerings. Traditionally, to integrate such systems required customers to build custom applications using in-house developers or engage systems integrators, both of which would require substantial financial investment.

Both options have disadvantages. As vendors upgrade their respective products, the integration components would likewise need to be updated, again taking time and expense. And as names and faces change within the IT group, organizations could be left stranded without the expertise required to accomplish updates and routine maintenance.

The CA Identity and Access Management as an Automated Service realizes the vision of integrating IAM services within a service management framework. CA Services delivers this integration based on best practices and a proven methodology, leveraging the experience gained from hundreds of security implementations.

## An Eye to the Future

CA Identity and Access Management as an Automated Service represents the first step in encapsulating IAM services within the service management framework. Enhancing the solution with additional functionality promises to bring even greater value to organizations.

### Service Accounting

One such enhancement pertains to the CA Service Accounting package. With this addition, IT could set up a rate plan for all of its IAM services offered in CA Service Catalog. As users order IAM services, CA Service Accounting will automatically create a charge back for the services to the department that ordered them. Or, for organizations that do not charge back, CA Service Accounting can accurately track IT charges to aid in IT budgeting and cost-justification.

### Third-party Vendor Integration

Another enhancement pertains to generalizing the interfaces within the solution to substitute one or more of its subcomponents with those from other vendors. This way customers can leverage their existing investment in different service management or IAM products.

### Standards-based Integration

CA is also implementing a consistent standards-based application and integration platform, called CA Catalyst, to integrate its own and other compatible third-party applications. The platform will simplify integration of disparate applications. Whereas today, integrating two or more applications requires product-specific connections between them, CA Catalyst will usher in an era where distinct application elements are modularized and accessed using industry-standard web services. Each application will publish standardized SOA-based interfaces through which any application can connect and share data. Essentially, CA Catalyst will serve as a broker that allows disparate processes to learn about one another and work together.

## Conclusion

In its July 2008 examination of the identity management market, the Burton Group summed up the situation well. "The complexities of the identity system must be simplified as organizations are forced to manage an ever growing user community, integrate with partners, and offer identity related services to customers and other external entities."<sup>1</sup>

With the CA Identity and Access Management as an Automated Service implementation, CA delivers just such identity services. By integrating service management and security management domains, CA leverages service level management tools to publish identity administration services to customers in a highly simplified manner.

Organizations can put the solution in place today and gain significant, immediate advantages by streamlining the process of delivering IT services. At the same time, they will be positioned for the future, having taken a step in the direction of achieving a simplified, automated, and integrated application architecture.

---

<sup>1</sup> "Identity Management Market 2008: Busting at the Seams," by Lori Rowland with additional input from Bob Blakley and Gerry Gebel, Burton Group, July 2008.

## About the Author

Chris Lavagnino is a Vice President in the CA Services Global Security Management Practice, which focuses on Identity and Access Management and Security Information Management implementations. He has twenty years of business and security experience and is a member of the Institute of Electrical and Electronics Engineers (IEEE), the Computer Society of the IEEE and the Association for Computing Machinery (ACM). He has completed doctoral studies in epistemology, logic, formal systems, and cognitive philosophy at Claremont Graduate University, holds an MA in philosophy/formal systems from Antioch University/Eberhard-Karls-Universitaet in Tuebingen, Germany, and a BA in methodology/formal systems from Antioch College.

---

To learn more about the CA Identity and Access Management as an Automated Service implementation visit [ca.com/services](https://ca.com/services).

CA (NASDAQ: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

MP332571008

---

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

