

# Simplify and Secure: Managing User Identities Throughout their Lifecycles

## CA Identity & Access Management (IAM)

- Identity Lifecycle Management
- Secure Web Business Enablement
- Data & Resource Protection
- Security Information Management

---

# Identity Lifecycle Management

---

CA Identity Manager

CA Role & Compliance Manager

CA addresses the critical business need for identity lifecycle management by delivering modular, yet integrated capabilities to automate the comprehensive set of identity-related processes across the enterprise. This increases operational efficiency and improves overall enterprise security, while simplifying and streamlining the management of user identities throughout their lifecycles. Building the foundation for consistent and auditable business operations also helps you to effectively maintain and validate compliance.

---

## Overview

Organizations are constantly challenged to keep pace with ongoing changes to users and their roles, responsibilities and requirements — making the processes involved in managing user identities complex and arduous. Compounding this problem of providing timely access is the need to ensure users have access only to the resources they need. To help, organizations are looking for solutions that simplify, automate and secure the activities for creating, modifying and validating user identities and roles throughout their relationship with the business.

---

## Benefits

CA delivers a unified approach for managing users' identities throughout their entire lifecycles and providing them with timely, appropriate access to applications and information. This increases operational efficiency and user productivity while decreasing help desk workload and costs. In addition, the right approach to identity lifecycle management helps improve your overall security posture with a consistent, auditable method for managing identity-related activities and a platform to help maintain adherence to regulations.

---

## The CA Advantage

CA's solutions for Identity Lifecycle Management provide integrated and comprehensive capabilities that automate identity processes across your IT enterprise for all user types. These leading solutions can be deployed independently or together to deliver unique and incremental value. As part of CA's vision for Enterprise IT Management (EITM), CA's solutions help you unify and simplify your overall IT management by automating and securing the comprehensive user identity lifecycle.

---

## Managing All Aspects of the Identity Lifecycle

Keeping pace with the management of identity information and user access is an ongoing challenge. One source is the explosion in the number of users of various types — employees, partners, contractors and customers. Each of these users, in turn, requires specific accounts and access privileges. Managing these identities, often across multiple IT systems and approval processes, must account for when the user's identity is first known to the organization, continuous modification and eventual removal of identities or privileges. The net result is a state of growing complexity for the enterprise in trying to meet their users' needs.

Organizations have implemented various processes to keep up with the barrage of access requests and volume of changing identity information. Unfortunately, most of these current “solutions” amount to poorly coordinated, manual processes. The result is too often a fragmented or siloed approach to managing access rights that exposes enterprises to higher costs and risks. This inconsistency also negatively impacts the user, as inefficient processes have downstream effects on user satisfaction, productivity and effectiveness.

Further complicating this picture is the fact that most organizations must secure user identity information, protect sensitive system data and prove their compliance with security regulations. This begins by maintaining all access privileges commensurate with users' specific roles and responsibilities and terminating that access when necessary. Thus, enterprises need to build in assurances that individuals can use only the assets they need to do their jobs at any given point in time. No more, no less — regardless of how frequently their status might change.

Unfortunately, mitigating the risk of over-privileged users and demonstrating that no one has inappropriate access rights can involve many hours of manual identity policy evaluation and process enforcement. This is very resource-intensive and error-prone — and even more challenging when the goal is proving that there has been no inappropriate access over a period of time. In response, organizations are looking to be more proactive by implementing consistent, predictable identity processes, auditing them and then refining them as necessary.

### **Balancing the Needs for Efficiency and Security**

The traditional security management challenge is in successfully implementing additional access controls without impeding business productivity. Granting users with greater access than necessary is often the default to ensure the user has immediate access in the event they need privileges outside their typical profile, but this also increases the organization's risk profile. Depending on the organization, the rigor of security checks and balances often takes on greater or lesser importance relative to ensuring a seamless user experience.

By contrast, when it comes to managing the lifecycle of identities, business efficiency and security are actually complementary elements. The challenge is really one of automating identity-related processes in a cost-effective manner and then deriving the greatest return possible from your investment. How do you introduce efficiency into the identity management lifecycle process with a focus on information protection and an enormous volume of users with frequently changing organizational roles and responsibilities?

With thousands or millions of users, maintaining accurate access privileges on an individual-by-individual basis would be a nearly impossible task. Beyond granting appropriate access, the organization must also track who authorized that access, when it was granted and proactively certify and remediate user access on a continual basis to help meet compliance objectives. The key is in building a strong role-based foundation for identity management and leveraging those combined investments to help address business and compliance goals.

---

## CA's Modular, but Integrated Approach

CA's solutions for identity lifecycle management provide a comprehensive approach to the management of user identities throughout their lifecycles. With modular capabilities, they provide the flexibility to incrementally deploy at your organization's pace — starting in the areas where you have the most significant need. At the same time, the solutions integrate with one another to provide exponential value in combined business processes. This way, you can show immediate gains and position yourself for future growth and additional advantages.

With the right foundation firmly in place, you can:

- Create synergies for greater effectiveness and cost efficiency
- Ensure economies of scale with predictable and automated processes
- Deliver higher levels of consistency and quality throughout the identity lifecycle
- Ensure user satisfaction, while enhancing identity-based security
- Create a platform to establish consistent identity security policies and help address compliance requirements

### CA Identity Manager

CA Identity Manager is a comprehensive identity administration and provisioning solution for managing all types of identities (internal users, external users, non-user IDs). It manages identities across a complete set of target systems (from mainframe to Web applications) throughout the full identity lifecycle (from creation, to modification, to removal). Additionally, CA Identity Manager improves security by providing an authoritative point of identity administration, enforcing consistent identity policies and auditing identity-related actions. Features include:

**PROVISIONING/DE-PROVISIONING** Automates the granting of role- and rule-based access to make your users more immediately productive. CA Identity Manager also enforces consistent workflow processes for approvals and access removal as each user changes to help secure corporate resources.

**USER SELF-SERVICE** Enables users to resolve identity-related issues on their own such as password resets, requests for additional access and identity profile management. Decreasing their dependency on IT or your help desk frees these departments to focus on more strategic initiatives and reduces organizational costs across the board.

**DELEGATED ADMINISTRATION WITH CENTRALIZED CONTROL** Reduces overall IT costs by enabling you to delegate the administration of certain users to the person or organization that owns them. This also enables your business partners or other business units to manage elements of their own identities, thereby significantly reducing the burden on your IT staff.

**INTEGRATION** Serves as a central engine to drive your processes and synchronize identity information across multiple systems. CA Identity Manager provides out-of-the-box connectors to common end-point systems in addition to a variety of flexible integration methods, allowing you to deploy quickly and with the most flexibility possible.

**AUDITING AND REPORTING** Provides the ability to audit all identity-related events along with comprehensive event processing and alerting capabilities. CA Identity Manager includes out-of-the-box entitlements reports which are complemented by the Business Objects XI reporting engine and open reporting interfaces to enable enterprise-class, custom reporting.

### **CA Role & Compliance Manager**

CA Role & Compliance Manager enables fast and accurate role model creation and maintenance while automating security processes required to address identity security and compliance objectives. The solution complements identity management projects through clean-up of user entitlements and development of accurate role-based models. It also helps you validate that users have appropriate privileges on a continual basis while enforcing consistent identity compliance policies across your enterprise to reduce security risk. Features include:

**PRIVILEGE CLEAN-UP** Aggregates data from various sources to provide a consolidated environment for analyzing user, privilege and role entitlements. This enables you to correlate user accounts across systems to a unique identity, identify out-of-pattern privilege assignments and take corrective action to establish a clean and reliable data set on which to base your role definitions.

**ROLE DISCOVERY** Includes top-down and bottom-up role analysis powered by pattern-recognition technology and role mining to automate discovery of access patterns. CA Role & Compliance Manager features an interactive interface for role creation and a collaborative Web-based environment for review and approval of change requests.

**ONGOING ROLE MAINTENANCE** A centralized role management capability ensures role changes are properly designed, managed and executed following the designated approval processes. This allows you to detect business changes that require changes to the role model, enact business processes for role approval and role adaptation and support executive reporting and audit.

**ENTITLEMENTS CERTIFICATION** Addresses the highly labor-intensive and manual process of certifying entitlements for individuals, roles or resources. A convenient web user interface enables managers to view their workers' accounts and access rights, certify their accuracy or flag certain entitlements for corrective action. As exceptions are identified in the certification process, CA Role & Compliance Manager can initiate the remediation process with identity management solutions, including CA Identity Manager.

**IDENTITY COMPLIANCE POLICIES** Allows you to establish a centralized set of security policies which can be enforced on a detective or preventative basis to ensure your users do not receive or maintain inappropriate privileges. This includes segregation of duties policies which keep users from receiving potentially conflicting roles or access rights.

**REPORTING** Enables easier account clean-up and role planning through intelligent analysis while implementing policies to ensure roles and privileges are properly assigned on a continual basis. CA Role & Compliance Manager reports and dashboards provide you with a variety of capabilities that deliver easily understandable operational, managerial and regulatory insight.

---

## The Combined Identity Lifecycle Management Value

Organizations require the flexibility to address role management, identity management or identity compliance independently to meet their immediate or specific needs. However, the promise of identity lifecycle management is to leverage opportunities where the whole is greater than the sum of the parts. Deploying multiple identity lifecycle management elements together provides exponential value with minimal corresponding investment. The following scenarios illustrate specific examples of how CA's various identity lifecycle management components work together to help you achieve that "greater whole":

**SMART PROVISIONING** Users often need to request additional access through identity management interfaces. Through CA Identity Manager's web user interface, users have the ability to select accounts or role membership that they would like. However, for organizations with hundreds or thousands of roles it is difficult for users to determine which role they need. CA Identity Manager can use real-time role analytics from CA Role & Compliance Manager to suggest roles for a user based on their attributes, existing entitlements or peer entitlements. Instead of hundreds of available roles, your user can be presented with the top 15 suggested roles that they might need. This improves the user experience while minimizing the inefficiency of initiating provisioning and approval processes for inappropriate account requests.

**CERTIFICATION WITH AUTOMATED REMEDIATION** This common compliance process involves requiring managers to review their employees' entitlements, so they can certify that each worker has the appropriate privileges. Unfortunately, this tends to be a manual process supported by circulating spreadsheets and sign-off forms for manager certification, then relying on IT to coordinate with application owners to remove users' privileges as needed. As an alternative, CA Role & Compliance Manager provides a centralized system that managers can access online to view the list of their users and associated entitlements. Should they identify any inappropriate privileges, integration with CA Identity Manager can initiate automatic de-provisioning and/or the appropriate workflow processes.

**ANALYTICS-SUPPORTED CERTIFICATION** A challenge with the compliance certification process is that when managers or IT has to review many users and account privileges, they can easily overlook inappropriate privilege assignments due to the volume of data that requires review. Introducing role analysis into this scenario allows you to identify out-of-pattern privileges and visually flag these anomalies during the attestation process for each manager. This enables them to be more efficient about which entitlements to scrutinize and leads to a more accurate certification process.

---

## Secure, Efficient Identity Lifecycle Management

By introducing a structured foundation for the full complement of identity-related management tasks and processes, CA's approach to identity lifecycle management provides a number of benefits, including:

**REDUCED COSTS** Automating individual identity-related processes, such as provisioning, approval workflow and entitlements certification, reduces the cost of business overhead. In addition, putting key account, password and identity administration functionality in the hands of your end users greatly decreases IT and help desk costs. Basing these individual services on a role-based model allows you to maintain privilege accuracy while minimizing IT management overhead.

**IMPROVED BUSINESS EFFICIENCY** Streamlining identity processes based on a consistent role hierarchy provides the foundation for improved business efficiency. Specifically, through activities, such as automated provisioning or certification, your users can become immediately productive and your IT administrators can focus on business goals and core competencies, rather than mundane, labor-intensive tasks.

**COMPLIANCE RISK MITIGATION** Identity lifecycle management allows you to minimize your security risk with the ability to audit identity-related actions and the assurance that users have access only to the information and systems they need. Centralized, policy-driven identity controls help you prevent the accumulation of unnecessary access privileges through de-provisioning or segregation of duties enforcement. Meanwhile, dynamic remediation ensures that when security lapses, such as orphaned accounts or excessive access rights, do occur, they are corrected as soon as possible upon discovery.

---

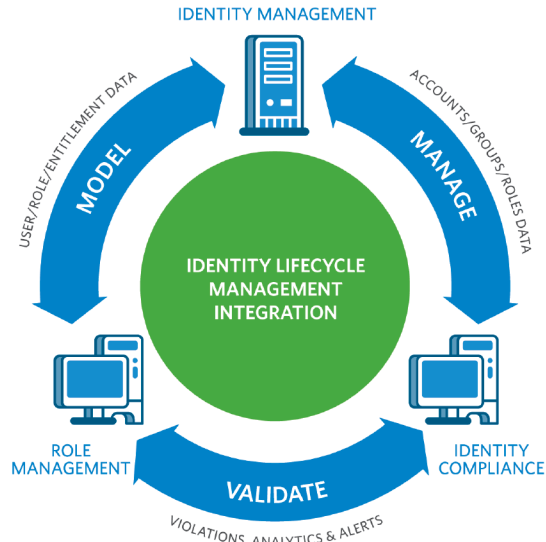
## The CA Advantage

CA provides an unprecedented end-to-end solution for automating and improving the many time-consuming tasks associated with identity lifecycle management. This flexible approach allows you to leverage functionality at your own pace and starting in the areas where you have the most pressing need. More importantly, CA's solutions for identity lifecycle management build structure around the complete identity lifecycle, ensuring repeatability and the ability to leverage standardized processes for additional improvement.

FIGURE A

CA enables effective identity lifecycle management by providing the modular, yet integrated capabilities needed for all processes related to managing user identities throughout their lifecycles.

CA'S APPROACH TO IDENTITY LIFECYCLE MANAGEMENT



Integration extends to other CA Identity & Access Management (CA IAM) solutions, which help you manage your users and their access to your IT resources, address compliance concerns and expand your customer and partner relationships to help grow your business. The next step is to tightly integrate the control and management of distinct functions, such as operations, storage and lifecycle and service management, along with IT security.

This higher level of management control is EITM — CA's vision for a dynamic and secure approach that integrates and automates the management of services, applications, databases, networks, storage and systems across departments and disciplines to maximize the full potential of each. CA's comprehensive portfolio of modular IT management solutions helps you unify and simplify IT management across the enterprise for greater business results.

CA supports a complete approach to identity lifecycle management by supplementing technology with comprehensive services and educational offerings. CA Services has the experience and proven methodologies needed to help you implement identity lifecycle management in a way that delivers rapid results now and into the future. CA Education offers training courses on CA Identity Manager and CA Role & Compliance Manager with the ability to customize the right training plan to meet your specific needs.

---

## Next Steps

Consider the following when analyzing your identity lifecycle management needs:

- How long does it take for a new employee to gain access to the applications they need to perform their job?
- What percentage of help desk or IT support calls are related to issues that the user could have fixed on their own (forgotten password, updating profile, requesting additional access)?
- Do you have a way to consistently audit who approved new user access?
- How timely are your access review processes such as manager's review of employees' access, privileged access reviews or terminated accounts review?
- Do you have a problem with "orphaned" accounts that may exist after employees or contractors leave your organization, exposing you to risk?
- Do you have an accurate representation of the roles in your organization? If so, how is this maintained?

If you struggle to keep pace with the ongoing management of identity information and user access, help is available from one of the most respected names in IT management. Take the next step and contact CA today.

---

To learn more, and see how CA software solutions enable other organizations to unify and simplify IT management for better business results, visit [ca.com/security](https://ca.com/security).



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.

MP340000509

---

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

