SOLUTION BRIEF
THE CA IDENTITY SUITE

Identity Management and Governance That Empowers Business Users

Bridging the gap between IT and the business user

ca technologies

Executive Summary

Challenge

As an IT leader, security executive, or business manager, you are living in changing—and challenging—times. IT environments are becoming increasingly distributed, complex and heterogeneous. But, deciding who has access to what, and reliably enforcing those policies is a multifaceted challenge that should involve all three constituencies—IT, security and the business.

Meanwhile, IT is often being given smaller budgets and fewer resources to carry out their responsibilities. So, you need a reliable but cost-efficient way to meet these critical identity challenges:

- Quickly onboard new users to make them productive as quickly as possible
- Ensure that all users have only the proper access entitlements according to their current role(s)
- Automate key identity processes for increased efficiency and reduced cost
- Identify and prevent potential policy violations (orphan accounts, improper entitlements, etc) before they occur
- Meet auditing requirements by knowing who has access to what

And, finally, one of the most important enablers in today's environment is to:

- Provide a simple and intuitive experience for so that business users can easily and conveniently access your core identity services.

Opportunity

The increased focus on empowering business users has created many challenges for users of most existing identity management solutions today. Unfortunately, the very few solutions that deliver a reasonable user experience typically lack the breadth of provisioning, role management, and governance capabilities and the ability to scale to support identity management across the extended enterprise. This forces you to choose between breadth of functionality and ease-of-use.

The CA Identity Suite uniquely helps bridge the divide between current IAM technologies and business users. It is an integrated suite of identity management and governance capabilities that combine robust functionality with an intuitive, convenient, and business-oriented experience. It can simplify your identity management processes, improve user satisfaction, support both on-premises and cloud applications, and provide consumer-level scalability. And, best of all, it can be deployed easily and quickly.

Key Challenges of Successful Identity Management and Governance

This paper highlights some key identity management challenges of today's open enterprise, describes why these challenges can drive or hinder your business, and provides an overview of capabilities offered by the CA Identity Suite that can help your organization successfully address these challenges.

Each of the challenges below has both a business and an IT aspect to it. In the past, the user experience for identity services has been dominated by an IT focus, resulting in difficult interfaces and reduced satisfaction. But, today's environment demands a bridge between IT and the business user, in order to expand the use of identity services, and improve the overall user experience. We will explore the business and technical side of these challenges.

These challenges require extensive planning and should be part of every rollout plan:

- **User adoption**—Improving and simplifying the overall user experience to increase user adoption of identity processes
- **Access requests**—Simplifying the process of gaining access to apps that users need
- **Entitlement risk management**—Preventing entitlement policy violations
- **Access certifications**—Improving the productivity of managers
- **User application access**—Providing a convenient way for users to access their key apps
- **Identity real-time analytics**—Ensuring efficiency of core identity services
- **Deployment challenges**—Improving ROI and time-to-value

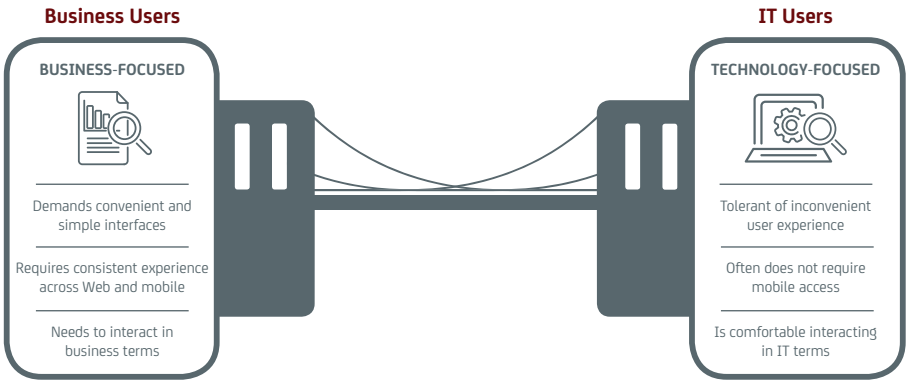
The challenge: user adoption

"My users are frustrated by the inconvenient user interface for many of the identity functions that they must deal with. This is severely limiting our ability to roll out these services to a wider user population within my company."

One of the biggest challenges in successful identity management deployments is that the user experience for identity services is usually highly IT-centric. In the past, this might have been OK. But, as identity management extends past the domain of the pure IT user, this approach no longer is effective. Terminology and processes that might be second nature to an IT-savvy user can be confusing and frustrating for most business users. The result - reduced adoption of identity processes, higher IT burden, failure to comply with regulatory requirements and user frustration. Users need to have easy, quick, no-training-needed business applications, available on the device of their choice. They must be brought into the basic identity processes, but this will only work if they find the experience simple, intuitive, and most importantly, oriented towards business users rather than IT users.

The CA Identity Suite solution

The CA Identity Suite uniquely helps bridge the divide between current IAM technologies and business users. It is an integrated suite of identity management and governance capabilities that combine robust functionality with an intuitive, convenient, and business-oriented experience. By improving business user productivity and satisfaction, the CA Identity Suite user experience is designed to dramatically increase the IAM solution value proposition for large enterprises while removing a significant administrative burden from the IT organization.



Some of the many significant user experience advantages that the Suite offers include:

- A Business Language Entitlements Catalog
- A Web and mobile application dashboard and launcher
- One Stop Shop – centralized, easy access to all identity services for business users
- Shopping cart experience for access requests and tracking
- Social network-like experience for tracking access requests
- Proactive advice tools
- Mobile application allowing the user to manage identity anytime, anywhere

The CA Identity Suite also makes it easy to generate individualized, custom dashboards tailored to the unique needs of specific roles, such as executives, security officers and business partners. Administers can configure an interface based on the user role, and what services they can get access to. The Suite's interface can also be fully customized for the branding needs of your organization, including your corporate logo, color scheme, fonts, selected background images and more. Your portal will thoroughly reflect your business' identity.

"In a survey done by an external analyst firm, 97% of surveyed customers reported that the Identity Suite user experience was superior to the competition"

source: TechValidate survey

The challange: access requests

"It's hard for my users to easily request access to apps and systems that they need for their job. The process is cumbersome, and the resource names are often confusing to my business users."

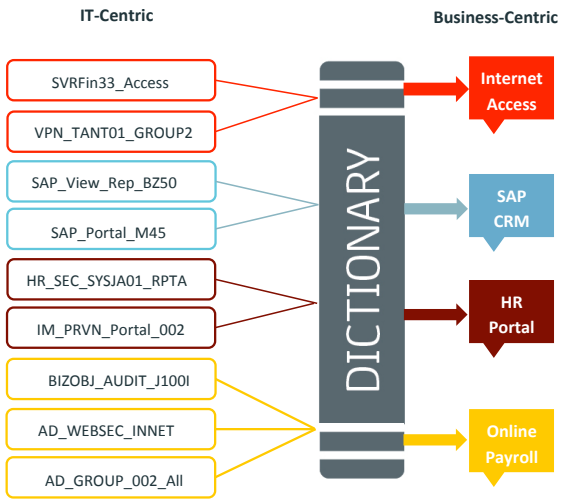
Users need to get access to the apps and data that they need, quickly and easily while maintaining compliance with regulatory requirements. But, access request systems have tended to be based around a set of entitlements that were designed for Admins who understood their meaning, and foisted on users who had to learn an almost new language of "IT-speak" terminology. As more and more business users are engaging with the corporate identity processes, this non-intuitive experience hampers adoption, reduces satisfaction, and often ends up with the IT folks getting involved anyway to help answer questions from the confused business user.

A new way of interacting with business users is needed, and the area of access requests is a prime example of the benefits that this new approach can provide. But, IT has valid needs in this area also, such as automation of basic access request processes, and easy auditing of requests and approvals. So, capabilities that meet the automation needs of IT but are easily usable by business users is essential.

The CA Identity Suite solution

The CA Identity Suite offers an intuitive, simple "shopping cart" experience, which dramatically simplifies the access request process. Modeled after the process familiar from retail shopping sites, users can conveniently place roles and entitlements needed to perform their job duties into their carts, view current access privileges and check the status of previous requests.

The user-friendly Business Entitlements Catalogue is at the heart of how the CA Identity Suite helps provide a simple, business-oriented experience. It translates cryptic resource names, such as "TSS_MNG_per_view" into more intuitive ones, such as "Online Payroll," making it easier for business users to locate the resources they need. You can also group applications into logical categories for further ease of access—for instance, creating an group named "SRM access" that includes the SAP apps, Oracle apps, and SalesForce capabilities business users typically need—all defined in terms familiar to those users. The following graphic highlights the mapping between IT-centric and business-centric terms that the Catalog performs.



The Identity Suite includes proactive advice tools that can greatly simplify the access request process. The user can view suggested roles, and access rights for users similar to themselves. This proactive advice helps the user make the right request about the access that they want. It also provides you with a risk score, based on the access you requested and how "risky" that access right may be. The user can then make a more educated decision as to which access to request.

The challenge: Entitlement risk management

"Sometimes users are assigned entitlements by mistake that violate our security policy. I want those violations to be prevented before they occur."

Improper user entitlements have been the root cause of a number of recent public breaches. This is especially true for privileged users because they tend to have very broad entitlements. But, the principle is the same for all users—we need to correct improper entitlements that violate security policy before they get granted ("preventative control"), and terminate any that may already have been granted in the past ("reactive control"). Unless effective controls are in place for both cases, risk will be increased, and compliance audits will be more challenging.

In a similar vein, sometimes policies change and access granted long ago now violates the new policy. During regular access certifications, this needs to be made very visible to the manager so that she can also de-certify this user for that access entitlement.

The CA Identity Suite solution

The CA Identity Suite enables you to formulate, enforce and validate sets of business process rules (BPRs) to implement segregation of duties and other logical constraints regarding relationships between users, roles and privileges. For example, a BPR can model a constraint of "people with permission to access X cannot have permission to access Y," or a dependency relationship such as "only people with access A can have permission to do B." So, instances that violate these security policies can be prevented before they occur.

The Suite can also warn you if conflicting rights are being requested (the Preventative Controls described above). It assigns a risk score based on the access being requested and the related policy. The risk score is based on the user, their other entitlements and any contextual factors that might be relevant. The requester is provided with this risk level when the approval request is made, so as to warn her of a potentially improper request. Similarly, the approver sees this risk score during the approval process, providing full visibility that can prevent granting high-risk access.

The Suite also provides Reactive Controls to remediate improper access that has already been granted. At the time of certification, the Suite runs policy checks against access and tells you whether this user has improper access rights that violate any policies. The Manager sees violations clearly marked for each user in order to allow for immediate correction. Both types of controls can significantly reduce the risk of improper entitlements being granted, or remaining undetected.

The challange: Access certification

"I want to make certifications simple and intuitive, and so I can improve the productivity of my managers, and simplify my compliance audits"

We have already seen the importance of an automated capability to translate user access information into the appropriate language and format for each type of certification campaign you run. If the access names are intuitive and business-friendly, if flexible workflow can be designed to meet your individual needs, and if tracking and status of each campaign is easily available, then your certification program is more likely to be successful.

The CA Identity Suite solution

The CA Identity Suite certification capabilities are based around the Business Entitlements Catalog, which makes it very easy for managers to understand the access rights of each employee, and easily approve, reject, or delegate each user's access rights. In addition, a risk score is available to managers if a certain access right, or combination of rights, is particularly risky. By enabling visibility to these risk ratings, certification becomes not just a "yes/no" proposition, but one that can highlight risks that otherwise would not be visible.

The CA Identity Suite has the flexibility to support many different types of certification campaigns, including:

- **Entity certification**—Used to certify the access rights associated with selected users, roles or resource entities by managers, role owners and resource custodians.
- **Recertification**—Allows you to repeat the certification process based on a previous campaign.
- **Differential**—Initiates a certification campaign based solely on the entitlements which have changed since a previous campaign.
- **Self-attestation**—Allows each user—as opposed to a manager or resource owner—to certify their own privileges. This type of campaign may satisfy some legal requirements for data security certification.

Certification campaigns can be tedious, time-consuming, and ultimately not effective as a risk reduction activity. The CA Identity Suite not only improves the effectiveness of this process from a security and compliance viewpoint, but does it in the context of a simple, highly intuitive experience that managers love.

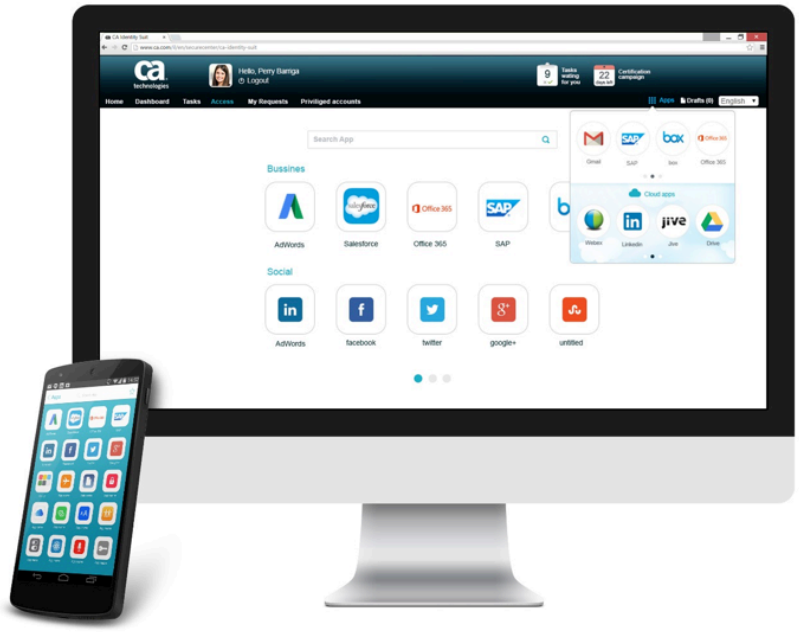
The challange: Convenient access to apps

"I would like my users to have very easy access to all their apps—both cloud and on-premises—but only those that they have proper access rights to use. And, I need easy access across all their devices"

Users become frustrated when they are faced with cumbersome steps to get access to one of their many apps. Multiple logins and inability to easily launch apps is a common complaint. And, as mobility increases and users become used to the convenience of these device interfaces, frustration and productivity challenges can increase. What is needed is a more convenient method of getting quick and easy access to each user's apps, that provides single sign-on across all of them, and includes only those apps that each user is authorized to access.

The CA Identity Suite solution

The CA Identity Suite includes a Web and a Mobile Application Launchpad that provides users a single dashboard to easily and quickly access all authorized web, cloud and mobile applications. The Launchpad can be accessed from any device and offers enhanced search capabilities. Once users have logged in to the CA Identity Portal, any web application is just one click away and all of the apps that users access on their desktop are always available through CA Identity Portal Mobile as well. This Launchpad keeps employees productive on-the-go with complete single sign-on to mobile web applications in a mobile-friendly format.



The challenge: ensuring process efficiency to meet SLAs

"Some of my identity processes aren't working very well, so I'm getting complaints from other managers about the service levels that am providing. But, I just don't have enough information about where the bottlenecks are in order to fix them."

Identity-related processes are often complex and may involve multi stage workflow steps. When these processes are not operating efficiently, like when a set of users simply don't complete their task in a timely way, the entire system can bog down and service level goals cannot be met. This can lead to audit weaknesses or simply increased inefficiency when basic processes such as access certifications are not completed according to agreed-to service goals. Without adequate visibility into the detailed operation of these processes, the cause of these issues cannot be identified, let alone remediated quickly.

The CA Identity Suite solution

CA Identity Suite provides extension real-time analytics so that the operation of core identity processes can be more completely understood and optimized. This can help to identify bottlenecks, and ensure that your critical SLAs are met. As a simple example, the graphic below provides a time-based view of current SLAs over the past month, as well as key numbers such as the average, max, and min SLAs for a given process. It also shows the arrival rate of new requests over each day of the previous month, as well as a summary of the disposition (completed, rejected) of all these requests. This capability provides significantly improved insight to the manager so that processes can be optimized, and the complete state of all such processes can be viewed easily.

The challenge: difficult deployment

"Deployment of my identity management solution is time-consuming and difficult. First, simply installing and configuring the software takes days, and then it sometimes takes weeks to get some basic use cases up and running because I need custom code and to define workflows, policies and the UI."

Deployment of a robust identity management solution can be challenging and costly. It can easily take weeks to get some basic capabilities up and running. And, any requirements such as connectors to custom applications, can drain resources and eat up time significantly.

The CA Identity Suite solution

The CA Identity Suite can *dramatically* reduce the time it takes to get up and running, through these capabilities:

- **Virtual Appliance (vApp).** vApp eliminates the traditional installation phase and delivers a pre-installed, preconfigured virtual machine image, ready to run in production configurations under common virtualization platforms. The Virtual Appliance embeds a hardened operating system, application server and the CA Identity Suite software. It also includes built-in support for common DevOps procedures such as high-availability setups, capacity adjustments, log aggregations, platform patches and software updates.

  To deploy identity services, simply drag the service name onto the appropriate machine name, and the installation will be done automatically for you. If you drop the same service onto multiple machines, all the communication mechanisms for high availability (load balancing, failover, etc.) will be automatically done for you. No time-consuming, error-prone manual configuration is required. The time savings are dramatic.

  The outcome of this approach is a dramatic reduction in time-to-value and TCO, allowing you to achieve more with the same team and budget. This method can also save thousands of dollars a year in software licensing costs because all the core system components can be freely deployed without the need for additional licenses.
- **Deployment Xpress (Depx).** DepX represents a radical improvement on how identity management software is deployed. It consists of a collection of preconfigured user scenarios for common user cases that most organizations would typically require, including user onboarding, password reset, access certifications, partner onboarding and the like. Each scenario consists of all elements needed for an easy deployment, such as template user interfaces, workflows and policy definitions. The manager simply picks the scenarios you need, puts them in the shopping cart and then checks out. At that point, all of these key elements are automatically loaded into Identity Suite and deployed. You can make customizations to these elements (such as corporate branding for the interface), but there is no custom code required. These scenarios speed the deployment process and can significantly reduce the time-to-value for deployment of typical identity services.
- **Other Xpress tools.** Identity Suite includes additional tools that significantly streamline the process of managing your deployment environment, including:
  - Connector Xpress simplifies the process of creating connectors to homegrown apps and makes connecting to systems that don't have OOTB connectors easier.
  - Config Xpress allows you to more quickly and easily move components between staging environments for simplified configuration management and additional functional testing time.
  - Policy Xpress lets you configure policies that execute your unique, complex business processes. Typically done through custom code, this wizard-based tool lets you build policies in-house within hours, rather than requiring weeks of programming.

Key Capabilities

CA Identity Suite provides the following key capabilities:

- Self-service identity portal ("one-stop shop")—centralizes entitlement data and provides an intuitive access request shopping cart
- Dramatically reduced deployment time – days to minutes!
- Business-friendly entitlements catalog—makes access requests and entitlement certification more understandable for business people.
- Proactive analytics—advises, prevents and alerts the business user of potential policy violations.
- User provisioning to a broad range of on-premises apps, SaaS services and non-connected systems
- User self-service—enables users to manage their own information to reduce the IT burden.
- Deployment Xpress—preconfigured use case templates greatly simplify initial deployment and ongoing management.
- Customization without custom code—powerful features such as ConfigXpress, PolicyXpress, and ConnectorXpress let you customize your identity management infrastructure without custom code.
- Privilege cleanup—examines existing system entitlements and highlights excessive or unnecessary privileges.
- Role modeling with an advanced patented analysis engine—helps efficiently sort through extremely large volumes of user and privilege information to discover potential roles.

ca technologies

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-230014_1016