



# Manage user identities and access in the cloud

*User provisioning and access control to protect users and data in cloud deployments*

---

## Contents

- 1 Balancing scalability, usability and provisioning in and across the cloud
  - 2 Implementing federated single sign-on for secure access to cloud-based services
  - 3 Gaining full life-cycle identity and access management for cloud-based users
  - 3 Getting started—assessing cloud security and privacy risks
  - 4 Why IBM?
- 

The ability to share services and information with various departments, partners, customers and other parts of the business ecosystem is a major advantage of cloud computing. As a result, successful cloud deployments hinge on securely and efficiently managing individuals' access to resources, and protecting data from loss or corruption. From a legal and regulatory perspective, you must be able to control, monitor and report on who is accessing what cloud-based resources, and for what purpose. But the management of thousands, even millions, of individual IDs overwhelms most IT departments. IBM can help. IBM solutions enable clients to federate and centrally manage fine-grained access policies, and enforce them with security services in the cloud. In addition to enhancing cloud security, IBM solutions help reduce administration costs, ensure compliance and increase productive collaboration across the business environment.

## Balancing scalability, usability and provisioning in and across the cloud

When it comes to outsourcing key workloads and applications to the cloud, organizations must provide the right people with the right access to the tools and information they need to do their jobs or perform a task. But it can be challenging to strike the proper balance between security and usability. When millions of users need access to cloud-based resources, user provisioning (and de-provisioning) must be simple, efficient and scalable.



An automated identity and access management (IAM) solution can address these challenges, and encompass both cloud and traditional computing environments so you do not have to manage two sets of credentials. With an IAM solution, you can set and enforce policies for who can access what information, when, from what locations, and how much they can access in a set time period. Once credentials are established, authorized users will have single sign-on access. You can use the solution to reconfirm all entitlements over time and promptly revoke them as necessary. Tools should also be available to monitor, report and proactively prevent policy violations. Protection against privileged user threats is especially critical because of the catastrophic damage that insiders can cause, intentionally or inadvertently.

IBM identity and access management solutions for the cloud address several challenges and business requirements, including:

- A broad user base that can include employees, customers and partners accessing corporate applications and third party services
- An extremely large number of users (cloud access for customer communities could involve millions)
- Varied requirements and access controls applied to different circumstances, and sensitive and non-sensitive data (for example, procuring access to future product designs vs. inviting customers to attend an upcoming marketing event)
- Limited resources, tight budgets and the desire not to duplicate existing IT security infrastructure just for the cloud
- Comprehensive security that meets regulatory compliance requirements and helps prevent costly, reputation-damaging system breaches

## **Implementing federated single sign-on for secure access to cloud-based services**

Collaboration across an organization's business ecosystem requires businesses to extend their application access to partners, customers and consumers. While Identity and Access Management (IAM) practices may be well established and automated in traditional IT environments, the cloud extends services, applications and resources to a broad user base that may include employees, customers and partners coming from trusted and untrusted external locations. Organizations need the ability to tie cloud-based applications together with internal applications and enable users to access them easily with single sign-on. Federated identity management provides a secure and scalable approach to managing identities and access in a cloud, and within traditional computing infrastructures.

IBM federated identity management solutions help streamline life-cycle management and access control for internal and external users in the cloud. IBM solutions provide policy-based controls that address distinct user profiles and enable secure, authorized, audited and authenticated access—regardless of location or type of connection to cloud-delivered applications and workloads. By providing a federated approach, end users have a seamless sign-on experience to these applications, eliminating the need for multiple user IDs and passwords. The federated approach also enables organizations to more effectively manage identities across cloud infrastructure while preserving the confidentiality of user data. Based on open standards such as SAML, Open ID and OAuth, IBM solutions enable secure and flexible business collaboration. Integrated password self-service capabilities allow users to easily reset their passwords online without the assistance of help desk staff. This helps improve staff productivity, enhance the user experience and reduce the number of help desk calls—ultimately saving money.

Based on open standards, IBM identity and access management solutions provide:

- Single sign-on access to multiple web-based and cloud applications with a single ID and password
- User self-service for identity creation and management (that is, password resets)
- A consistent approach to managing identity and access security for both traditional and cloud-based users and applications
- Automated management and enforcement of access control policies across every application, data source, operating system and even company boundaries
- The ability to track and log user activities, report violations, and prove compliance with policies such as “separation of duties”
- A modular foundation for quick deployment and time to value, that can be enhanced with additional security over time

### **Gaining full life-cycle identity and access management for cloud-based users**

Enterprises need centralized, automated management of users, authentication, access, policy and provisioning in and across the cloud. These capabilities can help address compliance requirements, reduce operational costs, enhance security posture and develop operational efficiencies. IBM software for full life-cycle identity management in the cloud administers, secures and monitors user access to resources and provides compliance auditing. Capabilities include:

- Full life-cycle identity management (“cradle-to-grave”) for identities of cloud-based users
- The ability to monitor, control and report on privileged identities (that is, systems and database administrators) for cloud-based administrators

- Access and authorization control for applications and data in the cloud
- Role-based identity and access management to align users’ roles to their access capabilities, including cloud-based users and applications
- Desktop single sign-on for end users for client/server applications
- Security incident and event management for compliance reporting and auditing of users and their activities—in both cloud and traditional environments

### **Getting started—assessing cloud security and privacy risks**

IBM can help you create new sources of business value from the cloud by verifying identity and access practices against established policies for enterprise security. A cloud security compromise can adversely impact mission-critical operations and put users and sensitive data at risk. While security breaches are not unique to cloud environments, certain aspects of cloud computing can make them challenging to address, including:

- Multi-tenancy—which complicates policy, governance and the ability to manage users with widely varying missions and data access needs
- The virtual environment—clouds are highly virtualized environments, and virtual security is a relatively immature field
- Highly elastic, fast service execution—in which a corrupted virtual image could be provisioned dozens of times before the problem is discovered and corrected

IBM understands these challenges and applies its comprehensive strategy, research, services, solutions and experience to help clients securely embrace cloud computing. The benefits of partnering with IBM to manage identity and access in the cloud include:

- Reduced risk
- Increased visibility and control
- Improved scalability and user productivity
- More flexible provisioning
- Accelerated audit procedures

As a critical first step, IBM experts can perform a cloud security assessment to help identify security and privacy risks, and compare the current security state against industry best practices and internal objectives. With an in-depth understanding of cloud security controls, mechanisms and architecture, IBM assessment professionals can provide actionable recommendations for closing security gaps and improving overall cloud security posture.

## Why IBM?

IBM has adopted cloud computing for significant parts of its own business, has made considerable and ongoing investments in security initiatives, and is able to transfer its knowledge and holistic approach to cloud security to clients for rapid execution and return on investment. IBM knows that identity and access management are critical to building and maintaining a secure, auditable cloud. Let us help you address the challenges of large and varied cloud user communities. Our solutions balance security and usability, and enable simplified management of the complex user profiles and access needs present in cloud computing environments.

## For more information

To learn more about IBM Security, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: [ibm.com/security](http://ibm.com/security)

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: [ibm.com/financing](http://ibm.com/financing)



---

© Copyright IBM Corporation 2011

IBM Corporation  
Software Group  
Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America  
December 2011  
All Rights Reserved

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Other company, product or service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



Please Recycle