

# Trends in Identity and Access Management

By Jonathan Gershater with contributions from Yvonne Wilson and Lauren Wood

**One of the biggest challenges organizations face today is managing users and complying with regulatory requirements that enforce access controls and require audit trails of user management activity.**

One of the biggest challenges organizations face today is managing users and complying with regulatory requirements that enforce access controls and require audit trails of user management activity. Specifically, organizations need to manage the lifecycle of user activity:

- Enable access for new users and terminate departing users' access
- Control what applications users can access
- Manage user access rights as their job roles change
- Provide logs and audit trails of the above actions

Organizations benefit as well by enabling users to manage their own identity information and relieving overburdened help desks with mundane tasks such as password reset, name changes, etc.

The momentum behind identity management is the change in scope of users. When organizations first opened their applications to the Internet, most users were on the organization's campus and internal network. Firewalls were implemented as a single point of entry. In addition, the organization needed protection from malicious external users or internal users inadvertently downloading viruses, etc., from the Internet.

Today, users comprise customers, partners and remote employees, using computers and mobile devices, who require access to data and applications. Additionally, threats come from within an organization, not only from without. Thus security has migrated from the single, monolithic firewall at the entrance to the network, to the addition of fine-grained controls throughout the enterprise – authenticating, authorizing and entitling users at the application and data level.

Firewalls are still a critical necessity, keeping undesired users from accessing the organization's network. However, users

with legitimate authority should be able to access data in a controlled manner. Identity and Access Management control who accesses applications and data, what they are entitled to access, and provides an audit trail. Identity Management comprises access control – policies that govern who can access what – and provisioning, which in conjunction with separation of duty and role management solutions, automates the process of adding and removing users from systems.

## Identity management

Identity management focuses on the management of user identities and their access. The following concepts are within the realm of identity management.

### Provisioning

Provisioning means giving users something that enables them to do their tasks: for example, creating a login identity for a customer in a CRM system, providing a new employee an operating system login credential, email address and assigning a cubicle or providing a contractor with badge access to a laboratory for six weeks. Provisioning typically takes place when a new user is hired as an employee or contractor, an existing employee changes job roles, a new application goes online for customers or a new partnership is established requiring access between organizations.

### De-provisioning

De-provisioning is essentially the opposite: removing access and identity information for users. For example, removing all access to applications, buildings and networks for 5000 employees who were downsized on one day, denying badge access to contractors after they completed their project,

and disabling login access to a financial system when a user changes job functions.

Deprovisioning is especially important when users leave a company, and an organization needs to remove access immediately to prevent the user from accessing sensitive or confidential information. De-provisioning also reduces costs. Organizations have reported that after an employee terminates employment, their DSL bill is still paid by the organization because of inadequate de-provisioning tools.

### Password management

Another essential element is password management. This is often the first phase of an identity management roll-out. Organizations report that calls to the help desk for password reset account for a third of calls. Password management may allow a user to have the same password across multiple systems and provide self-service interface for password reset.

### Identity reconciliation and modification

Since applications are brought online by different organizations, by acquisition, etc., user identities need to be reconciled and matched. Joe Smith may exist in email as *joe.smith*, on Unix as *jsmith* and in another application as *joes*. When a user's attributes change, for example change of name or address, this activity can (optionally) be modified by user self-service and thereafter the details propagated across all applicable applications.

### Implementing solutions

Until identity management products were developed, provisioning was either paper-based or ad-hoc scripts and procedures developed by each system owner or department. Early implementations of provisioning software created a user in the target system, subject to the manager or owner of that system authorizing the request. This approval provided an audit trail that partially fulfilled compliance requirements, showing which users were granted access to systems and who authorized the request. Examples of such requests are self-directed requests such as customers self-registering their credentials in a new online application. Often requests are triggered by an event such as upon an employee added to the HR system automatically creating an email address for the

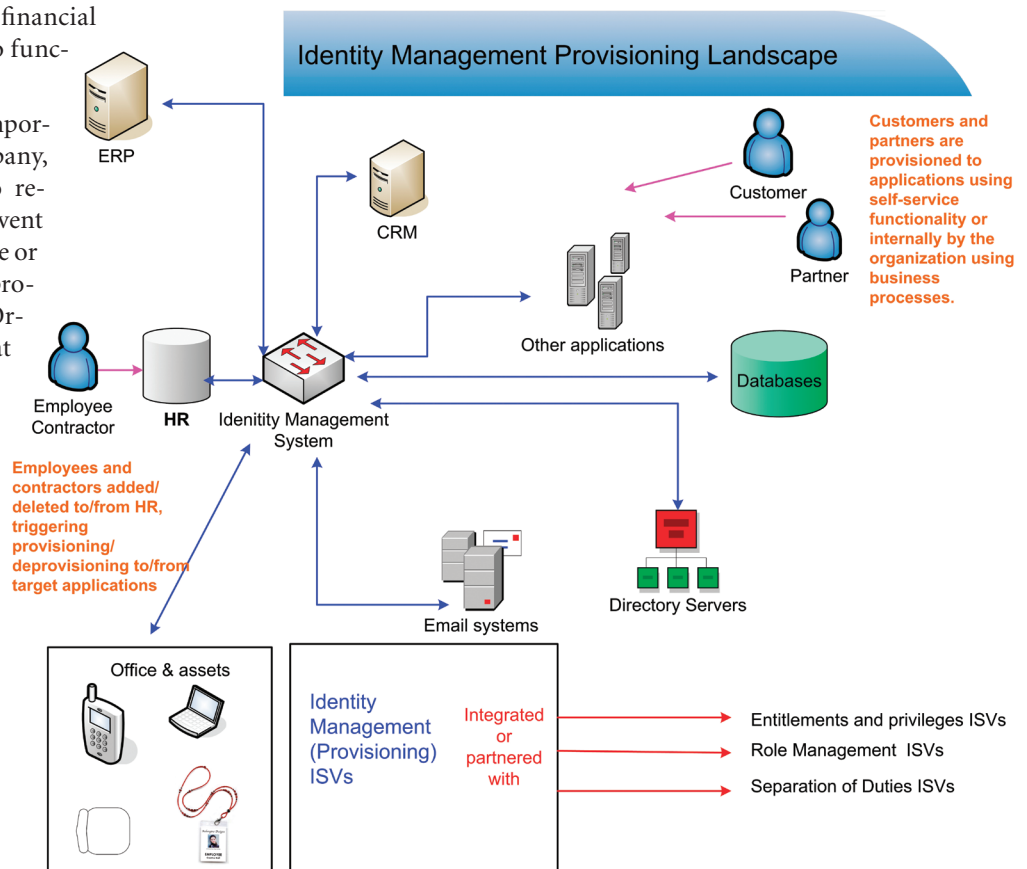


Figure 1 – Identity management provisioning landscape

user or a user changing job roles and requesting access to an application that he requires to perform his new job.

These early identity management implementations usually superseded paper-based processes, although they are by no means trivial. While software exists to automatically add and remove users to and from systems, the greatest challenges to a successful identity management deployment are:

1. Re-engineering paper-based or other processes to be automated
2. Getting buy-in and co-operation from different departments within an organization whose systems will be affected by automated provisioning and de-provisioning tools
3. Getting acquiescence from IT system administrators, since an automated tool may need superuser access to manage users within systems.
4. Staffing the project
5. Funding the project

Overcoming these non-technical barriers is usually more difficult than coding extensions to provisioning software to provision users to applications or customizations to fulfill special requirements.

## Access management

### Current implementations

Access management focuses on policies that govern what a user can access. In the early days of access management this was called AAA:

- **Authentication** – first prove **who** you say you are, typically providing a **userId** and password suffices, though stronger forms of authentication such as biometric or smart-card are often used for organizations or applications that demand extra security
- **Authorization** – after you have proven who you are, **what** can you access. What applications is a user entitled to access?
- **Auditing** – **who** accessed what, providing logs and audit trails of who logged in and what applications were accessed.

Users in this context are typically employees, contractors and visitors who are on the organization's network or the Internet accessing web-based applications. This is often called "single sign-on." A user authenticates once and is provided access to all applications he is entitled to access, without requiring further authentication. However, pure single sign-on is almost nirvana as not every application can be wrapped under a web access management product. Thus access control deployments are often called "reduced single sign-on" since some applications remain outside the umbrella of the web access management product.

Web access management also offers delegated administration. Traditionally the IT department or help desk managed users across the entire organization and even external facing applications. Delegated administration allows an organization to provide departments or external communities with the ability to manage their own groups of users.

## Trends in identity management solutions

### Roles

Roles are a coarse-grained method of associating users with job functions. Example: Joe is an Accounts Payable clerk, Mary is VP of HR, Henry is a contractor System Administrator and James is a partner within the CRM application. Roles are the foundation for finer-grained entitlement manage-

ment, also known as rules. Entitlements or rules are managed on objects such as printers, files, disk-drives and conference rooms. For example the executive conference room can only be booked by VPs and higher; the color printer can only be used by users with a marketing role. By using roles to ad-

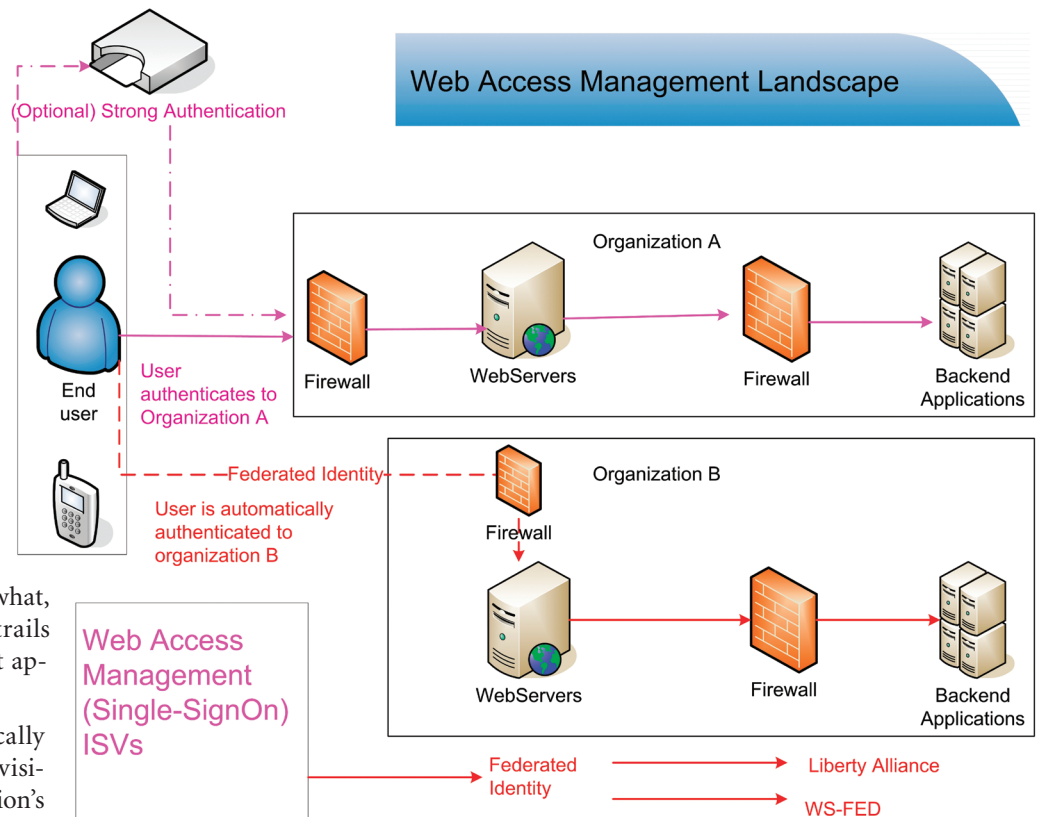


Figure 2 – Web access management landscape

menter rights: an organization can significantly reduce the number of transactions needed to initially assign user rights as well as to maintain, modify and remove them.

From the above example, when Joe is first hired, he is assigned to cubicle 7-2001 in the San Francisco head office. Before he starts work he is assigned these roles:

- Employee – all badged employees
- Finance – all finance department employees
- AP Clerk – all Accounts-Payable clerks within finance
- SFO – all employees (full-time and contract) at the San Francisco campus
- B7SFO – all employees who work in building seven

This suffices to grant Joe access access to buildings, rooms, parking lots, basic applications and benefits. When Joe completes an on-line HR form, he could be pre-assigned roles that would enable his access to the facilities and applications on his first day of work. These minimal functions allow Joe to become productive immediately. These privileges granted are based on Joe's role, not who Joe is. It is not Joe who needs ac-

cess to building seven but anyone who has the employee role assigned to building seven and entitled to park in building seven's garage.

Independent Software Vendors (ISVs) have begun to produce software that manages roles. Rather than utilizing disparate spreadsheets across the organization, products exist that provide centralized role management, design and discovery.

### **Fine-grained entitlement management**

Roles provide coarse-grained privilege management. Joe is an employee and can access building seven, etc. However, once Joe is employed and productive, finer-grained entitlement management is required. For example, ensure Joe cannot pay an invoice over \$10,000; or ensure the HR system cannot be accessed outside the USA between 10PM and 7AM except by the VP of HR, Mary. While these entitlements are often controlled within the individual applications, software solutions are emerging that centralize entitlement management across all applications, providing one view of what a user can and cannot access. Entitlement management ISVs produce solutions that centrally manage entitlements that are policy driven.

### **Context-based access control**

Context-based access provides finer access controls within web access control products based on a user's context. For example: the time of day, their location, the network sub-net their computer is on. From the above examples, an organization could stipulate that Joe can only access the finance system from 9AM to 5PM, Mary cannot access HR from outside the USA and James can only access the CRM from the VPN sub-net dedicated to his partner organization. Essentially, context-based access controls who, what, when, where, how and maybe why a user, who has a certain role, wants to access an object or application governed by a rule.

### **Separation of duties**

As regulatory requirements such as Sarbanes Oxley (SOX) and Gramm-Leach-Bliley (GLB) have evolved to demand controls in place, software has spawned to aid in the compliance of these regulatory requirements. One of the compliance requirements is separation of duties. This ensures that a user cannot have two roles that create a conflict of interest. In the above example, ensure that Joe does not have rights to create and pay invoices (he could pay himself or his friend).

### **Federated identity**

Federation refers to the establishment of business agreements, trust of encryption methods and user identifiers between two or more organizations' security and policy domains. As more and more businesses go online, organizations are creating partnerships and business relationships. Web access management has expanded from users only accessing applications within the organization's network to the need for organizations to enable access to applications between organizations.

Federation technologies insulate each organization from the details of the others' authentication and authorization mechanism, allowing the authentication within one organization to be trusted at another organization. This is known as Federated Identity as the identity is federated between more than one organization. In order to establish trust across organizations, a central body is often established within which organizations trust each other and abide by standards and technologies within each. Removing the need to re-authenticate as an application takes a user from one organization to another provides a seamless experience for customers. Examples include a research professor accessing an on-line library at another university, a county sheriff accessing police records, and the police granting a detective only limited access.

### **Is single sign-on attainable?**

Efforts are underway to achieve ubiquitous single sign on, not only to corporate applications, but consumer applications as well. Wouldn't you like one login to your online bookstore, travel site, portal and personal email? CardSpace is a software product that enables users to provide their digital identities in a familiar, secure and easy method. In the physical world users present a driver's license as proof of identity. CardSpace provides digital identities to use with any online application configured to authenticate users using CardSpace identities.

Similarly, OpenID is software that provides a method for individuals to create an identity online and use it anywhere OpenID is supported. For users, OpenID means the elimination of multiple user names and passwords. For businesses, this means a lower cost of password or account management, the opportunity for easier and higher numbers of new user registrations and the reduction of missed transactions because of user frustration with lost and forgotten passwords. In addition to authentication, OpenID allows users to control what components of their digital identity are shared, such as their name, address, or phone number.

SAML defines a standard for communicating identity information between organizations. SAML allows organizations to deploy applications that adhere to a common standard for exchanging identity information.

Higgins is a community-based identity protocol-independent software framework for managing and sharing personal profile and identity information on the web. Specific combinations of components can be combined to create distinctly different kinds of software solutions called "deployment configurations."

Finally, the Concordia project is a global initiative designed to drive interoperability across identity protocols in use today. It does this by soliciting and defining real world use cases and requirements for the usage of multiple identity protocols together in various deployment scenarios, and encouraging and facilitating the creation of protocol solutions in the appropriate "homes" for those technologies.

## Conclusion

Firewalls are still essential barriers against unwanted users. However, providing controlled access to customers, partners and employees outside the corporate network enables business and drives productivity. Identity and Access Management solutions not only manage user identities and what they can access but also provide compliance with regulatory requirements. Access control systems govern who can access what by employing static and dynamic policies. Provisioning solutions automatically add and remove users from systems and employ functionality from role management and separation of duty solutions to ensure users are only granted access required by their role.

Ask yourself these questions before deploying an identity and access management system:

1. How do you definitively authenticate users who request access to applications and approve this access?
2. How do you decide who should legitimately have the ability to grant access initially and track this over time?
3. How do you delegate administrative duties so that the model is sustainable over time and acceptable to users?

## References

- Federated Identity: [http://en.wikipedia.org/wiki/Federated\\_identity](http://en.wikipedia.org/wiki/Federated_identity).
- Liberty Alliance: <http://www.projectliberty.org>.
- SAML: [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=security#overview](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#overview).
- OpenID: <http://openid.net>.
- Cardspace: [http://en.wikipedia.org/wiki/Windows\\_CardSpace](http://en.wikipedia.org/wiki/Windows_CardSpace).
- Single sign-on: [http://en.wikipedia.org/wiki/Single\\_sign\\_on](http://en.wikipedia.org/wiki/Single_sign_on).

## About the Author

*Jonathan Gershater's career started at 3Com, managing servers and networks. His initial foray into Identity Management began in 1999 at enCommerce, which was later acquired by Entrust. At Sun Microsystems since 2005, Jonathan architects and deploys identity solutions for customers using Sun Java System Identity Manager, Access Manager and Directory Server. He may be reached at [jgershater@sun.com](mailto:jgershater@sun.com).*