

## ▶ Access Management Services In The Cloud

---

Tech Tip  
by Philip Cox

Organizations should position themselves for cloud services by using open standards for access management

## ► Access Management Services In The Cloud

---

Extending an organization's access management services into the cloud is currently ad hoc, very dependent on your cloud service provider, and rudimentary at best. However, with that said, there are some steps that you can take to position yourself to utilize cloud services as they become more mainstream:

- Ask your cloud service provider to support open standards for access management;
- Standardize and automate your user provisioning as much as possible;
- Create a centralized entitlement management mechanism within your organization;
- Extend policies and procedures regarding access management to include cloud services.

Let's take a closer look at these steps, particularly the two key architectural and process components of access management services that need to be considered in the cloud:

- Entitlement (privilege)management: assignment and enforcement
- User provisioning and de-provisioning

### Entitlement management

Organizations who want to utilize access management in the cloud will need to spend a significant amount of time ensuring their systems and applications have the ability to consume an externalized entitlement management service. In a nutshell, this means designing your application and systems to provide and consume eXtensible Access Control Markup Language (XACML) type information. XACML is the leading general-purpose standard for describing policy management and access decisions. It describes a language as well as a processing environment model. The main purpose of XACML is to allow organizations to implement a common authorization standard across all systems and applications by providing a standardized language, a method of access control, and policy enforcement. In contrast, Security Assertion Markup Language (SAML) is an open standard used for federated identity.

The key is that you will have to ensure your systems and applications can consume the XACML information, and that your IAM system can provide it.

The reason I stress XACML is that it is an open standard; you should be wary of spending significant amounts of resources to integrate into a cloud service provider's proprietary entitlement management system. When it comes to the cloud, open is better.

However, I know of no existing cloud service provider that supports the ability to have externalized entitlement management on any large scale. Meaning that while this is an admirable goal, the reality of cloud providers being able to consume or provide entitlement management is currently not practically feasible. For now, focus on providing the entitlement service and consume it with your own applications or systems. Think of this as a very early frontier; as time passes, adoption of standards such as XACML will pave the way for a more universal entitlement management across cloud services.

### User provisioning

Along with identity and entitlement management, user provisioning and de-provisioning) are key elements of an identity and access management service. User provisioning is the process of allocating users to systems and applications, effectively granting identities required access to information and systems. In order to effectively utilize IAM in the cloud, you will need to have an efficient process for user creation and removal. This process of provisioning and de-provisioning will set the initial entitlements and link them to an identity.

You should look to see how your current provisioning process integrates Service Provisioning Markup Language (SPML) in order to make providing and consuming the service as seamless as possible with your cloud service provider. Like XACML, SPML is a standard and utilizing it as the basis for your service provisioning will provide future benefits of interoperability that you would not get if you decide to integrate with proprietary

## ► Access Management Services In The Cloud

---

cloud solution. Using SPML can allow you to standardize and automate much of the provisioning process, which is critical for a successful IAM operation in the cloud.

### The need for standards

Standards for access management services are critical to ensure future cloud adoption. By using open standards — as well as requiring cloud service providers to support them — we set the foundation for a consistent and secure method of service offering and use. If the Internet has taught us anything, it is that the use of standards is the way to promote wide adoption and use of technology.

### About The Author

Philip Cox is Director, Security and Compliance at SystemExperts Corporation, a consulting firm that specializes in system security and management. He is a well-known authority in the areas of system integration and security.

His experience includes Windows, UNIX, and IP-based networks integration, firewall design and implementation and ISO 17799 and PCI compliance. Phil frequently writes and lectures on issues dealing with heterogeneous system integration and compliance with PCI-DSS. He is the lead author of *Windows 2000 Security Handbook Second Edition* (Osborne McGraw-Hill) and contributing author for *Windows NT/2000 Network Security* (Macmillan Technical Publishing).