CHALLENGE OF USER & ACCESS MANAGEMENT IN THE CLOUD

As cloud computing becomes more prevalent, the management of cloud applications becomes increasingly important. Addressing the challenges of user access and security is crucial in ensuring that cloud applications are effectively managed and utilized.
CHALLENGE OF USER & ACCESS MANAGEMENT IN THE CLOUD

As the need to expand within manufacturing, working applications has consequences that need to be in terms of user and access management.
Controlling who has access to specific applications and corresponding data is even more complicated with cloud applications. Providers of cloud solutions confer little priority to developing better management of user accounts and access rights in their applications; often more occupied developing new, business-oriented features.

Consequently, user and access management in cloud applications entails a number of challenges.

**Single Authentication**

Active Directory is the central link in the chain for user access to applications and systems. The traditional LAN-based applications often have specific integration, such as LDAP, with the central user account directory. Working with cloud applications means more authentication sources; Active Directory in one’s own corporate network and one or more authentication sources -- for example, AD, LDAP directory or database in the cloud.

There are only a few possibilities for synchronising user accounts between both authentication sources, (like AD Federation Services from Microsoft and the SAML standard). In this manner, end-users can log in transparently to the cloud applications.

However, federation is not a replacement for provisioning and basic user account management. Maintaining roles within a cloud application and linking accounts to central authentication remains an important task with which access to specific data is regulated.

**Manual actions**

Providers who do not support federation frequently offer a web-browser that MDs and CEOs can use to control access to the cloud application directly. However, there is no automatic provisioning and this necessitates a sequence of manual operations – a time consuming and error-prone process.

Also, when it’s possible to import a basic CSV file into the cloud

> *Federation is not a replacement for provisioning and basic user account management*”
> — Dean Wiech, Managing Director, Tools4ever
application, it still requires manual intervention by the application manager, creating a lot of unnecessary work.

Consider the procedure required when an employee leaves the organisation, which often occurs in phases. First the user log-in is removed then the account is removed, data is transferred to a different user and finally, an e-mail notification is sent to the manager. All these phases require a separate manual operation for user management in the cloud application.

**Naming and password conventions**

Conventions governing naming standards and passwords are often inconsistent between network and cloud applications. In the network, a user ID might be based on the log-in name, and in the cloud it might be the e-mail address.

This complicates exchanging user account details between the environments, and, in many cases, differences also apply to password conventions. When extremely complex passwords are required in the corporate network, cloud applications might not be able to handle this type of password.

The possibility also exists that the cloud application requires a different duration for password expiration than within the corporate network. Synchronising passwords between the network and cloud applications can be exceedingly difficult.

**Organisational structure**

The reporting hierarchy structure within an organisation is often utilised to assign authorisations to employees based on their role or position, commonly referred to as role-based access control (RBAC). This structure is contained in
an HR system or within Active Directory. Cloud applications normally cannot translate this organisational structure, and the web-based provisioning functionality they offer doesn’t offer a robust method for incorporating this level of detail.

Naturally, it’s possible to transfer the entire organisational structure to the cloud application, but this requires an enormous volume of management activity when something in the hierarchy changes.

**What if the connection drops?**

Providers who offer links between the network and cloud applications often use event-based synchronisation between the systems. However, they don’t have a procedure in place to deal with a temporary drop in the connection.

Imagine a user account needs to be created for a new employee, but at that precise moment the connection with the cloud application is lost; resulting in the request for a new user account being also lost. Cloud applications don’t provide any guarantee or notification that synchronisation completed successfully.

**Bulk actions**

Performing bulk actions in cloud applications is occasionally rejected by the application. Consider a manufacturer wants to create 1,000 user accounts for employees in a cloud application. Some cloud applications impose restrictions on the number of actions that can be carried out in one pass, or require that no management activities are undertaken during working hours to prevent overloads on their network.

Working with cloud applications generally means that organisations no longer have user and access management in their own hands, and that the rules and service level agreements of the cloud applications apply. User and access management are of secondary importance to business requirements. If it’s requisite for an organisation to have control of user and access management, there are third-party developers that provide software solutions to ease the transition to cloud-based applications.


"Synchronising passwords between the network and cloud applications can be exceedingly difficult"

– Dean Wiech