



SIMPLIFYING THE MOVERS, JOINERS, LEAVERS PROCESS WITH RESPONSIV CLOUD



AT A GLANCE

Challenges

- Handling movers, joiners, and leavers (M,J,L)
- Manual process requiring large amounts of staff time and effort.
- Decentralised access management across enterprise
- Risk of incorrect user privilege and data vulnerability.

Benefits

- RC-SS available on Microsoft Azure, IBM Cloud, and Responsiv Cloud Platforms.
- Manage user access in a way that best suits you with different options available on RC-SS.
- Centralise and automate your process to improve efficiency; saving staff time and effort.

FURTHER OPPORTUNITIES

To further streamline the movers, joiners, leavers on- and off-boarding process, organisations can use the Responsiv Cloud Automation Platform (RC-AP) to automate user set up in the identity store and manage other aspects of the process.

The result is a reliable audit of skills and permissions, efficient allocation of assets, and improved timeliness of moving people.

Permissions can be allocated to roles, allowing the role to be allocated to a person and the permissions to silently be granted.

CHALLENGE

People join the business, move between roles and departments, and leave. Each time a person changes from one role to another, the company needs to maintain record of their skills, experience, security status, and assets.

Business efficiency is undermined when a mover or joiner is left waiting for permission to do their work, for assets to be delivered, or for training. Business risk is realised when a person does not receive the right training or assets, and most importantly, when permissions are not assigned accurately.

Cloud services increase the importance of assigning and revoking permission when the business need has passed, due to the ability to access services remotely.

SOLUTION

Responsiv Cloud Security Service (RC-SS) controls all user and API access to the Responsiv Cloud services. It federates with your existing identity stores to simplify the user experience and centralise Identity and Access Management (IAM).

The result is that your Mover, Joiner, leaver processes have a single point of reporting and control for security access to our cloud services that is integrated with your existing M-J-L processes.

Federated Trust

Trust established between otherwise independent security realms allows each realm to share and trust credentials obtained from any of the other mutually trusting realms. In this case, the Responsiv Cloud Security realm is federated to one or more existing customer realms to allow users to authenticate themselves and obtain permissions in one realm and be trusted in another.

The importance of this becomes clear when companies use multiple cloud services, for example if a person has access to several cloud systems, and internal systems.

Responsiv Cloud Security Service

The Responsiv Cloud Security Service uses federated trust associations to allow the company's existing controls to be seamlessly extended to our cloud platforms. In addition, our integration platforms can be used to maintain API access to cloud services without giving out authorisation to people.

Identity tokens are attached to the user's browser following an authenticated login. This token is accepted by other applications - this is done under the covers and will eventually expire before needing to re-sign in. Applications will need to know to ask for the token when the user access the system; Responsiv can set this up as part of the agreed service preparation.

BENEFITS

By federating identity management and trust, the user experience, business efficiency, and operational resilience and control are all improved.

The Responsiv Cloud Security Service is a highly capable security mechanism that can be connected to business processes to automate all aspects of the M-J-L process to assure that skills are known, and that movers receive the necessary assets and permissions in a timely and accurate way.



Scan
for more
information