Industry: General Business | Product: HelloID

FLYER

HelloID
Cloud. Identity. Access.

PROVISIONING

MANUAL VS. AUTOMATED

OVERVIEW

Every IT department faces the 'revolving door' problem of user lifecycle management. Accounts and permissions must be continuously created, assigned, modified, and revoked. This has to happen in response to organizational changes — without delay.

This process is called user provisioning. There are two ways to do it: manually, or via automation.

MANUAL

Manual provisioning happens on an ad-hoc basis. HR sends a request to IT, usually via helpdesk or email. An IT technician then grants the needed entitlements by hand. An entitlement is any internally-controlled IT resource, such as directory accounts, email accounts, network folders and file shares, group memberships and permissions, software licenses (e.g., Salesforce, Office 365, payroll, SAP)

But this is only the first step. Updates are required for promotions, transfers, terminations, new responsibilities, and so on. When an employee departs, IT has to de-provision their entitlements. Plus, IT may be responsible for cyclical audits in which entitlements are evaluated for compliance, inventory, and oversight purposes. This is often a 'rolling', never-ending process.

All of this creates extra work for IT teams who are already busy with outages, troubleshooting, and supporting remote work — not to mention driving new initiatives forward.

Each step also represents a potential mistake. For example, HR may fail to communicate changes to IT. Or, IT may fail to grant all relevant entitlements.

Such oversights are not uncommon in the absence of an automated process. As a result, new hires may end up stranded and unproductive, unable to start work on day one.

But even more, pernicious effects arise from skipped de-provisioning. Permission creep is the most common example. This occurs when old permissions gradually accumulate on employees' accounts. Worse, old accounts themselves can accumulate over time. If this accumulation goes unchecked, ex-employees may retain account access for weeks, months, or longer. This presents a tremendous compliance and security risk.

AUTOMATED

Automated provisioning solves all of these problems. A dedicated provisioning solution (usually SaaS software) continuously monitors the organization's HR system. It automatically grants, modifies, and revokes entitlements as needed. Manual intervention is eliminated to the fullest extent possible.

The process works as follows:

1

STEP 1

The provisioning solution is connected to a source system containing personnel data. Typically, this is the organization's primary HR system. But it can be anything — even a flat CSV file.

2

STEP 2

The provisioning solution is connected to multiple target systems. Target systems are those in which users need entitlements. For example: Active Directory, Salesforce, Office 365, Google G Suite, Paychex, SAP, etc.

3

STEP 3

Business rules are developed. This is the most important step. This logic tells the provisioning solution how to parse the imported personnel data. It determines which entitlements will be granted in the connected target systems.

4

STEP 4

Once configured, the provisioning solution monitors the source system and automatically modifies the target systems.

Flexibility is paramount. Organizations may use any variety of legacy and/or proprietary source and target systems. Thus, every good provisioning solution supports custom connector development and complex attribute mapping.

Compared to manual provisioning, automated solutions are quick, efficient, secure, and cost-effective. Moreover, they liberate IT staff from routine work, freeing them to work on more impactful projects.

Automated provisioning also significantly improves security. By minimizing human interaction, the number of opportunities for mistakes plummets.

BUSINESS RULE DEVELOPMENT

Business rule development, the most important step in automated provisioning, deserves more elaboration. The goal here is to develop a 'matrix' which maps job roles onto entitlements. This allows entitlements to be determined and granted in a structured way. Most commonly, the RBAC (Role-Based Access Control) methodology is used. The first step in RBAC is to identify fundamental job roles and/or responsibilities.

These may be based on:

- Department
- Function
- Job title
- Location
- Cost center
- Or any other relevant factors.

For example, a hospital's roles may include "nurse", "doctor", "surgery", "radiology", "billing", "security", and so on.

Each role is then associated with the necessary entitlements. For example, "nurse" and "doctor" may need access to patient records. Security personnel, on the other hand, should not have that access. Or, for example, "radiology" may need key fob access to rooms which are off-limits to "billing".