

Automated provisioning, or automated user provisioning, is the method of granting and managing access to applications, systems and data within an organization, through automated practices. Automated Provisioning is the first key tenant to identity and access management (IAM).

Importance of automated provisioning in an organization's IT management and its benefits to businesses and system administrators. By the end of this article, you'll have a deep understanding of automated provisioning and how it works.

What Is Automated Provisioning?

Automated provisioning is a solution for managing user access and privileges for organizational applications, websites, data, and other systems. Rather than manually assigning rights for each user and system, automated provisioning enables access automatically based on preset rules allocated to predefined roles or groups.

Automated provisioning is an essential process within [identity and access management \(IAM\)](#) and [privileged access management \(PAM\)](#), specifically used when onboarding and offboarding employees. Because of its purpose, IAM platforms often offer automated provisioning as a feature, used by system administrators and IT managers to standardize provisioning rights based on roles and company policies.

👤 Learn how [Makespace](#) streamlined steps to onboard and offboard staff with StrongDM.

Importance of Automated Provisioning

Automated provisioning takes the manual labor out of managing user access to every individual application. When there is a new employee, or someone changes job positions, IT teams need to ensure the user has secure access to the resources required to fulfill their role. They must create user accounts for the appropriate applications, set modular privileges, assign system credentials, and remove access when the user leaves the business.

If an IT team were to complete those tasks manually for every employee and enterprise system, they would spend much of their time deciphering the user requirements and then enabling proper data access in each application's admin settings. Even in facilitating automated user provisioning with [Active Directory \(AD\)](#), the administrator still needs to manually provision users and configure the resources within the system each time.

When IT teams automate user provisioning, they get their time back to focus on other

technology or cybersecurity initiatives. Automated provisioning uses pre-configured access and privilege settings for each organizational resource based on the employee's role and governance policies. From there, once an admin adds, edits, or removes a user, applications and resources automatically adjust—activating, altering, or deactivating system access.

Four Benefits of Automated Provisioning

Automated provisioning creates value across the board for IT and security departments, human resources (HR) onboarding teams, individual users, and the organization as a whole. The main benefits of automated provisioning include the following:

1. Speeds up user onboarding processes

Automated account provisioning gives employees and contractors quick and smooth access to the resources they need to complete their work. With a faster onboarding process than would be achieved with manual provisioning, users can immediately get started and hit peak productivity.

2. Improves organizational security

Because automated provisioning follows policies set by the company, ideally, ones that follow the [principle of least privilege](#), organizations can maintain a more robust data security posture. By only giving users specific system permissions and granular resource access based on their role, security teams don't need to worry about underqualified and negligent employees compromising the integrity or confidentiality of [sensitive data](#) systems.

3. Minimizes user onboarding costs

Automated provisioning allows organizations to utilize personnel and resources for higher-value tasks. Rather than manually configuring user permissions for each enterprise resource, teams can automate those workflows within their [IAM technology](#). The ultimate result is less time and money spent during employee onboarding.

4. Reduces provisioning errors

One of the positives about using automation technology is that it minimizes work-related mistakes, whereas tasks completed manually come with the risk of human error. Automated user provisioning is no different when it comes to error reduction. Teams can be confident that the exact applications and permissions will be granted to the proper, authorized users during every onboarding process, then revoked or revised if the person leaves or changes roles.

How Does Automated Provisioning Work?

Automated provisioning works by configuring permissions and resource access within an IAM platform based on predefined settings. The organization would create automation rules that automatically give new users certain resource access rights based on their role, group, and

company policies. Using those predefined conditions, once added, a user automatically gets access and appropriate permissions for the applications and resources defined for that role.

For instance, say a company was onboarding new sales reps. Knowing that this particular group of users needs to use customer relationship management (CRM) software with regular permissions, the IT team creates a workflow: When a "sales" user gets added to the HR system, they automatically activate in the [cloud IAM platform](#). Once activated in the IAM tool, all newly added reps will have a CRM account with standard privileges and credentials created for them for system access.

The same workflow would simultaneously apply to any other network resources required for that role, such as a cloud drive with sales materials or a commission tracking system. Additionally, if a rep were to part ways, the IT team would update the user status in the IAM system—automatically and immediately, revoking access rights to all applications. Alternatively, if a rep got promoted to sales manager, the workflow would automatically expand their system privileges.

How StrongDM Simplifies Automated Provisioning

StrongDM's [People-First Access Platform](#) connects to all applications, data sources, clusters, and websites, which gives businesses full control of the user and resource access. Once connected, system administrators can facilitate cloud provisioning automation for all their applications in one central system—integrating automated access workflows into their current deployment and onboarding pipeline.

🚀 Before StrongDM, it would take up to a week to get someone provisioned. With StrongDM, we can now do that in minutes.

- Ali Khan, CISO at Better ([source](#))

[StrongDM](#) is the single source of truth for automated user and group onboarding—allowing quick and secure provisioning and least privilege administration. In addition to developing automated provisioning workflows, teams can use StrongDM for one-click [onboarding and offboarding](#), [just-in-time access](#) approvals, and complete [granular access](#) based on user roles or attributes.

Automate Your User Provisioning with StrongDM

When done manually, user provisioning for applications is time-consuming and only worsens as the business grows. Automated provisioning is the ultimate solution to expedite onboarding and offboarding. StrongDM empowers organizations with workflows that automatically grant user access and set permissions to technology resources based on the employee's role—offering a more reliable, hands-free provisioning experience that saves time and money.