Omada

Identity Lifecycle Management

IdentityPROCESS+

A key element of managing identities is managing access rights as employees, contractors and others join the company, shuffle between departments, change roles, or depart the organization. This is also often referred to as Joiner, Mover, Leaver.

Handling the entirety of each identity's lifecycle without automated processes is time-consuming, costly, and error prone. As an example, say a third-party contractor has a 3-month contract to perform a job managing an HRapplication, but it takes a week to provision access so that the contractor can do their job.

This is clearly a sub-optimal business process and results in lost funds in productivity, with 1/12th of the duration of the contract essentially wasted on operational overhead. Another example would be if a software developer leaves the company under unforeseen circumstances.

This can pose a serious risk for the organization if an employee retains access to code after they depart, either due to malicious insider threat or if unmonitored access persists. As part of Omada IdentityPROCESS+, there are several key components to Identity Lifecycle Management; critical best practices to ensure that business efficiency is optimized, security is tight, and compliance is met.

Employee onboarding

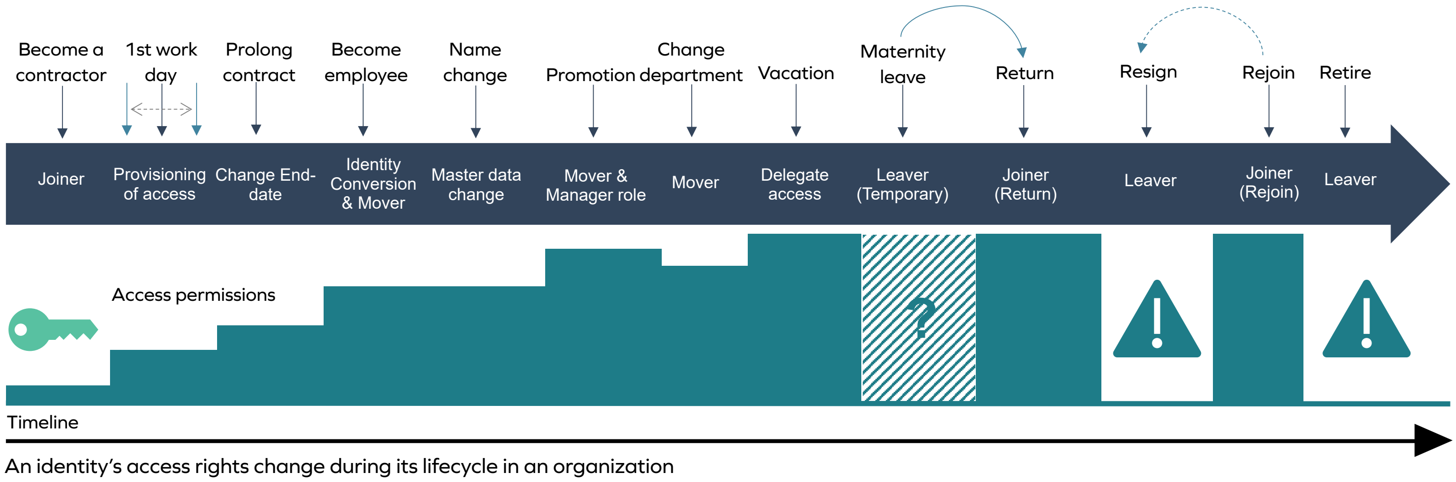
Attempting to manually onboard employees can lead to IT burnout, excessive permissions being granted, and/or too little access being granted, resulting in stunted productivity.

As such, the first step in the Identity Lifecycle Management process is to ensure that employees are provisioned with the proper access to the proper resources such as the directory service, email, shared drives, and company benefits. This process should also allow for specialist applications to be used based on role or context.

The next step is to onboard employee identities by creating a new employee record in the master HR system. There, a new identity is made up of a unique username and imported and automatically processed in Omada*.An approval task is then sent to the employee's manager so they can confirm the onboarding of the new employee. In order to ensure productivity on day one, these tasks can be done ahead of time, by setting the "Valid from Date" field in the Omada interface to coincide with the date of the employee's first day of employment.

***Identity Naming**

Create an identity naming policy to only create unique identities and have that explicitly written for the entire organization. User identities should not be tied to identity data in case a user changes their name. If someone leaves and rejoins later, create a new user ID so that there is a separation in logs and historical records to make it easier to analyze.



An identity's access rights change during its lifecycle in an organization

Contractor Onboarding

In addition to employee onboarding, organizations also spend lots of time provisioning access to third-party vendors and contractors who are brought in for set periods to perform specific tasks. Failure to provision access properly can not only hinder productivity but also be a massive security gap, as vendors are inherently not following the same security protocols as internal employees and can be harder to monitor. IdentityPROCESS+ outlines a repeatable process where the manager responsible for the contractor creates a new identity and specifies which systems and resources the contract needs.

A critical difference between a contractor and an employee is that with a contractor, the manager must indicate the start and end date. Once approved, this will provide a time-specific window during which the contractor will have access.

Omada uses this defined window to automatically onboard and offboard the contractor on the specified dates. This process starts with the manager manually adding the identity, either in the HR system if contractors are managed there, or directly in Omada. Omada is able to automatically detect if an identity with similar master data exists, and the manager can either create a new identity or update the existing one if they are similar.

Technical and Non-human User Onboarding

Technical users can include non-human accounts; service accounts, devices, robots, etc., that have access to various systems, applications, and infrastructure. The identities of technical users are critical to get correctly sized for access. Without enough access there are critical business tasks and operations that go undone - but with too much, serious damage can occur. Within IdentityPROCESS+, a process is outlined so that as system owners create technical accounts they must assign responsibility to an actual user, referred to as the primary identity, to ensure that tight governance is maintained.

One or many of these accounts can be linked to a technical identity, and a technical identity will subsequently always require a human owner to oversee and manage it. The system owner then completes a technical request form in Omada which then creates default properties for the technical identity.

Thereafter, the identity is mapped to an owner who has responsibility for the account, where it can be governed. If the owners of these accounts leave, or move roles, Omada enforces that ownership is updated and kept in order.

Change Identity

After someone joins the organization, it is very common to expect that over time they will hold multiple roles. This can be dangerous for organizations as, when employees change departments, they should naturally only retain access to systems they still need for their new role. Similarly, for productivity, they will need access to a new set of systems and data in order to perform their newly assigned tasks. Without a defined best practice for how to do so, this can take some time. IdentityPROCESS+ defines that when an employee or contractor moves within the organization, user access rights are reviewed and updated to ensure only appropriate system access remains.

This process is initiated when a transfer, promotion or other is entered into an authoritative source, such as an HR system. This then triggers Omada to clarify which new access policies should be added, removed, or edited. When the change happens, Omada revokes the access rights for the old role and adds the necessary assignments for the new role. The manager can then approve or deny the request and can also remove any direct resource assignments, if necessary. By default, the removed access rights are maintained for a predefined number of days, to enable the user to access and hand over work assignments, but this can also be deselected by the manager within Omada Identity.

Master Data Change

Master data changes are critical to maintain, otherwise duplicate identities can be created making it harder for teams to keep clean data. Changes to the master data occur when an employee changes personal data like a name change, address, or email. Within IdentityPROCESS+, a master data change process streamlines requested changes, updates, and additions to an identity's master data and ensures that changes are copied to systems that Omada is connected to, thereby ensuring continuous connectivity and provisioning. Users can change data records through a data update request, which must be approved by the identity's manager. When Omada detects a change in master data records, a change is initiated to gather the modified data and update the record in Omada, according to predefined datamapping

Process Stakeholders

Within IGA processes, it is critical that multiple stakeholders are aligned and working together. For Identity Lifecycle Management, the following teams must be involved in the following capacities:

Human Resources

- Ensure integrity and consistency of data in the HR system
- Make changes to employee records to reflect status
- Create accurate new employee records in HR system

IGA Team

- Work with HR to ensure clean records
- Integrate HR system and other authoritative sources into Omada
- Monitor data import integrity

Business System Owners

- Create technical identities
- Govern and secure IT systems

Line Manager:

- Work with IGA Team and Business System Owners to define roles
- Approve identity onboarding, transfer, master data changes and termination

Offboard Identity

Unfortunately, people do leave organizations they work, or are contracted for. Whether mutual or not, organizations must move swiftly to ensure that once an identity is no longer a part of the team, their access does not linger. An example of this could also be for something like parental leave, where access needs to be deactivated or suspended for a determinate period of time. IdentityPROCESS+ defines how teams can trigger this process for contractors and employees alike. For contractors, when the valid 'To Date' is reached, or if an identity record of the HR system is no longer delivered by the authoritative source, system and application access will be removed, disabled, or deleted automatically to ensure they do not have lingering access.

Data Management

If identity data is held in independent systems, then connectors need to be used to transfer data between each of those respective systems and Omada. If there is duplicate data, then the organization needs to decide which source should provide master data to Omada for attributes. Omada is able to leverage its flexible data model to join and match rules, including fuzzy matching, to de-duplicate data and authoritative source policies to control the attribute flow. Master data is then imported into Omada before work is started on implementing processes; data needs to be regularly imported from the HR database into the IGA system (1x per day is adequate for most).

Data Management

IdentityPROCESS+ always aims to standardize and refresh outdated business processes, such as certain processes being different for bank traders than they are for other employees. These types of one-offs make standardization difficult. Instead, processes should be defined in order to remove outdated processes and automate others. For example, if managers have to request access to systems on behalf of direct reports, Omada can introduce self-service. It is also critical to have documented standards to prove compliance to auditors and be able to continue best practices in the event that security and IT practitioners leave the organization.