Omada

Access Management

IdentityPROCESS+

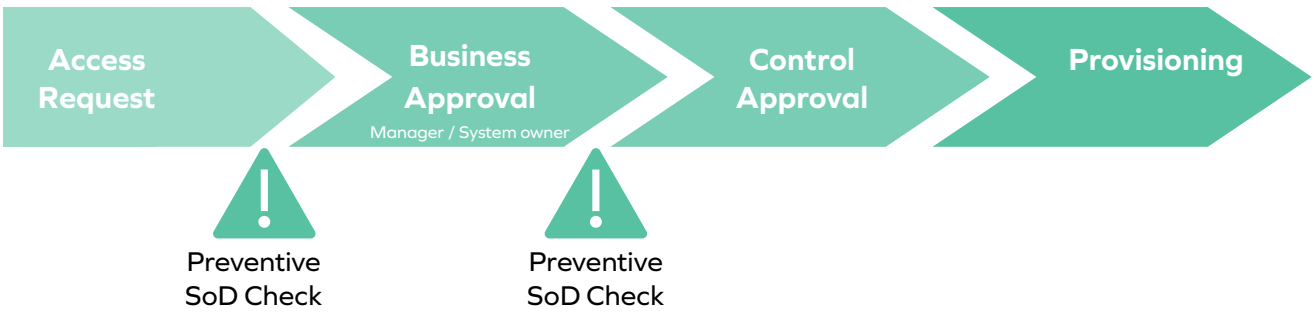
Employees, contractors, or any identity within an organization will often need to make additional access requests. Ideally, these requests are then seen and approved or denied by managers. IT departments and security teams have traditionally kept track of access rights in spreadsheets and/or disparate systems to document various processes and current states of access to auditors. This traditional method of maintaining access management processes is very time-consuming for end-users, since they must jump through hoops for simple access requests. It also introduces potentially error-prone workflows for administrators who may not fully understand what they are granting access to.

Manually handling access management leads to fragmented documentation that is needed for audits. It also can lead to the accumulation of unnecessary access for identities that move departments or stop working on projects. Employees or third-party contractors may accumulate access over time because they are not revoked when they move departments and will likely result in internal policy or regulatory violations, as well as potential data breaches.

Omada IdentityPROCESS+ allows organizations to control the granting of access rights while ensuring that access does not violate security or compliance policies. It provides documented best processes that are built to help any organization successfully deploy Identity Governance and Administration (IGA). As part of Omada IdentityPROCESS+, there are several key components to Access Management that are critical to follow best practices to ensure business efficiency is optimized, security is tight, and compliance is met.

Provisioning

The first step to access management is provisioning each identity with access to the various business systems, applications, and resources that they need to perform their jobs. Provisioning or assigning access rights for any identity to a target business system is automated with Omada, but sometimes there is a requirement or business case to incorporate manual workflows as well. Another common use case would be organizations with an ITSM system choosing to use that system to notify and execute provisioning where automation is not possible, feasible, or desired. Manual provisioning, or provisioning done via ITSM, allows IAM and security teams to provision access to systems not connected to Omada, while still monitoring and logging activities within Omada.



Steps in the access request process

Request Access Rights

One of the most common workflows that needs to be operationalized in any organization is requesting access. IdentityPROCESS+ provides organizations with a framework to help create a repeatable, scalable, and secure process for access requests.

Within Omada, a business user, or their manager on behalf of the business user, is prompted to fill in a business justification for new access rights. When the user goes to request access they can also be provided with additional intelligence and suggestions, including preventative Segregation of Duty (SoD) checks, and peer analytics to see what other users within their business context are requesting. The access request can also incorporate business context attributes like department of the user, the specific project, or what business unit they are associated with (sometimes referred to as a 'cost center'). This access request will then trigger a notification to the manager, application owner or other, who then can either approve or reject the request, based on the justifications and business context that is submitted.

All access requests are automatically logged within Omada so that an approval history is maintained for each requested resource assignment. This data is also accessible to approvers within this process to see who previously approved a request and why.

Approve or Deny Access Rights Request

After access requests are made (if explicit approval is enabled) they are automatically sent to a manager with the full gamut of business justifications, contexts, and the actual request itself; what is being requested, why, and when. The access request is also checked against all existing SoD policies to ensure that, if granted, this access does not present a toxic combination of access for the business user. If the request is denied, the user is notified, and it can also be configured within Omada to send notifications to system or application owners, Omada system administrators, and others who may want to be notified of potentially malicious access requests. If approved, the requested access is automatically provisioned by adding entitlements that give the identity the ability to perform the requested task either through added assignments or via policy. The period for access is set in the access request, or if no period was stated it is available until revoked, or if the identity changes roles to one that does not have the entitlement. Provisioning can be automatic, manual, or relayed to an external system (i.e. ITSM).

Critically, an audit log is created for each approval, which enables approvers to see a historical record of identities requesting access (and for what reasons) as well as maintain tidy records of access grants for potential audits. Within these logs, there is also data to confirm that the granting of access does not violate any predefined business policy.

Before being able to manage all access rights, there are a couple of things to keep in mind that need to be thought about and configured in advance. Within Omada IdentityPROCESS+, the following prerequisites must be set before commencing:

- Determine which users can request access rights for others
- Determine who can remove access rights from individuals

  If there is a security breach or one is suspected it may be necessary to remove access and understand the business implications of doing so
- Determine if approvers can modify requests and who should be able to

  If a 'valid to' date doesn't meet guidelines, then changes can be made rather than redoing the whole process
- Decide between implicit vs. explicit approvals

  Implicit granting of access is efficient because it doesn't require managerial approval, but role definitions need to be in place for this to work. For 'explicit' there are fewer upfront steps as no roles need to be defined ahead of time, but access rights then need to be approved for each new employee. Use line managers for access rights approvals

  Determine whether explicit approval steps are needed in some cases

Process Stakeholders

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

Business Users

• Request new access rights to carry out their work.

• Remove access when it is no longer needed (if being done manually).

Line Managers

• Analyze access requests when assigned, including business context, justifications and more.

• Respond to access processes by approving / rejecting requests.

• Remove access from direct reports when no longer required.

System or Resource Owners

• Approve access requests and respond to access requests on ongoing basis for the systems they own.

IGA Team

• Monitor the process flows and handle exceptions when approvers are not available.

• Set SoD policies to enforce potentially risky / toxic combinations of access

• Determine which users can request access rights for others.

• Determine who can remove access rights from individuals

Delegate Access

Another common workflow that IdentityPROCESS+ helps with is if someone needs or wants to pass off their access rights to others. This is otherwise known as access delegation. Examples of where access needs to be delegated include when a manager wants to delegate their access rights to a personal assistant for a given period, or a business user assigns their access rights to a colleague within their department while they go away on vacation. Delegating access helps to remove single points of failure maintain business operations, but must be done efficiently and securely.

Within Omada, the delegator first chooses to whom they want to delegate access, what access rights they want to delegate and for how long that access should be delegated. If the delegator decides to withdraw the access granted, IdentityPROCESS+ helps define that if delegated access rights are withdrawn by the delegator, they are also removed from whoever they have been delegated to. Just as when access is granted in a standard access request, Omada ensures that SoD policies are checked during the delegate access process. The system checks against existing prioritization and control policies to make sure it is proper and approves or rejects the provisioning of access. If there is an SoD policy violation, the provisioning is put on hold until a human evaluates the violation and determines next steps.

Remove Access

After access has been granted and the user performs their tasks, the access should eventually be removed. This helps institute and maintain the principle of least privilege. This can happen in a variety of different ways, and IdentityPROCESS+ helps businesses decide which routes are preferred to meet their business needs. A business user can remove their own direct access, a manager can remove access for a direct report, or a system/resource owner can remove direct access to a system they own. If possible, it is always recommended to set expiry dates for each grant of access so that once the date arrives, access is removed without any manual intervention, or an administrator remembering to do so. In the event that access will be removed manually, the user simply logs into Omada, selects the access they no longer require, and access will be automatically removed. Any explicitly assigned access is also included in annual (or more frequent, depending on preference) access certification campaigns.