

IDENTITY & ACCESS MANAGEMENT

Overview

Organizations need to follow a standard and formal way to manage access request or revocation across systems. IT and auditors need to be constantly informed on the accesses given to any system for corporate users or third-party collaborators.

Identity and Access Management module provides the appropriate workflows, forms and reports inside SWORDFISH platform in order for the organization to implement the Identity and Access Management process.

Identity and Access Management Process

SWORDFISH, implements the Identity and Access Management Process with the Access Request and Revocation workflows. Users initiate these workflows from SWORDFISH HUB in order to request or revoke access to one or more systems. Standard workflows provide approval paths based on company's organizational structure and e-mail notification reminders to make sure that appropriate escalations are followed if a process is delayed. Typical access/revocation steps are the following:

- Employee initiates the workflow and completes a form where he/she enters the employees or third-parties that access/revocation is requested for.
- Based on the organizational structure, Employee's manager receives the next step of the workflow and he/she can either approve, reject or return the form to the initiator for corrections.
- After Manager's approval, the form is redirected to the appropriate System Owners (per selected System) for implementation. System owner can implement or reject the request.

- As a final step, Employee is notified whether his/her request was implemented or rejected.

The Identity and Access Management processes can be configured to get approvals from employee's direct supervisor and -optionally- automatically escalate through the organizational structure until the highest level of approval is reached. Dynamic adjustment of the approval path based on specific factors, such as the criticality of systems (i.e. extra authorization from the DPO in case systems that process special categories of personal data are included in the request). Additionally, the Identity and Access Management processes can be customized to seek approvals from a specific group of users or configured to escalate to specific assignees in case the approval is delayed for a specific time period. The workflow steps and form fields can be easily customized in order for the process to fit the policies, procedures and reporting requirements of the organization.



Reporting

Out of the box reports are included in order for CISO to perform the Entitlements review process and provide evidence of Access/Revocation requests during an internal or external audit. Additional reports can be easily developed through a user interface and additional customizations can be implemented.

Identity and Access Management module provide the following out of the box reports:

- **Entitlements Review:** A report that provides information on which employees or third-parties have approved accesses to systems. More specifically the report provides the following:
 - Employee or Third-party name (including Third-party company name)
 - Date that the access was requested

- Form number associated to the access request (usually an incremental number like AGF010)
- System, Module, Privilege that was granted access to the user
- Username that was created by System Owner / Administrator
- **Pending Access Revocations:** A report that provides information on which access revocations are still pending after a number of days have passed since process initiation. It is important to have such a report in order to make sure that when employees leave the organization all access grants in systems are revoked as soon as possible.
- **Audit Trails for Access/Revocation request:** A report that provides a full log of all access and revocation requests that have been executed for a specific time period.

Organizational Structure

The SWORDFISH Platform offers embedded functionality in order to integrate and manage the organizational structure of your company. You can import your organizational structure from a simple Excel template or utilize our Active Directory connector and automatically synchronize SWORDFISH every time people change positions in your organization.

Users or user groups can be mapped to an organizational structure node and the respective workflow steps will automatically be assigned to the appropriate people during workflow execution.

Out of Office and task Delegation

SWORDFISH users can assign a delegate in case of absence. By using the Out of Office functionality, it is ensured that the Access Request or Revocation processes will not be delayed if a person cannot complete the task in time.

Additionally, the processes support a flexible escalation path, where a timed expiration after the step has been assigned to a user can be configured and the workflow will automatically escalate to the appropriate person inside the organization.

Workflow Engine

An embedded, sophisticated and powerful workflow engine can enforce security policies through automated and streamlined procedures that can be developed using the workflow builder embedded functionality. The procedures development process is structured upon a simple and solid 5-step concept allowing users with no extensive technical skills and knowledge to design procedures' workflows via a step by step approach within a user-friendly interface utilizing self-guided features such as readily available drop down menus, tick boxes and pre-configured action lists.

Integration with 3rd party systems.

Identity and Access Management can be easily integrated with any external system that supports a REST API. This way, SWORDFISH workflows can be part of a bigger business process (for example the Access Request / Revocation workflows can be part of the employee's on-boarding or off-boarding process by integrating with an HR system). The automation requires minimal implementation effort since the workflow engine is designed to support information exchange with 3rd party systems.



The Universe

One of the primary elements of SWORDFISH is the Universe Functionality. Universe functionality enables users to upload all information assets using a logical representation that enables security management in terms of risk and exposure. Assets can be assigned attributes that include criticality, ownership, physical location, information classification, type etc. All assets are logically represented under a relational ontology based on a business product decomposition method specifically developed

to address risk assessment requirements.

By using the Universe Functionality, Identity and Access Management module provides a list of Systems / Modules / Privileges for the employees to select during an Access or Revocation Request. For example, SWORDFISH can map a System to a specific user or a group of users or can split the responsibility of implementing access to different owners per system's module. Assets can be imported from a simple Excel template.

Benefits

How It Works

Best-practices enforcement

By using the Identity and Access Management module, you enforce the Access Request and Revocation processes in your organization. Users are encouraged to use this formal process which produces artifacts and supports the established Information Security Framework.

Fully Configurable Processes

SWORDFISH provides a workflow and form template for Access Request and Access Revocation. However, the organization can fully customize the workflow steps and form fields in order to align with the policies, procedures and reporting requirements.

The e-mail notifications of the workflow, can be customized in terms of subject title, body text and list of recipients.

Customizable Reporting

Ready-made reports are provided with the module:

- Entitlements Review Report
- Access Request Logs
- Access Revocation Logs
- Pending Access Revocation for a number of days

Additional reports can be created with the UI. Should the reporting requirements be more complicated, SWORDFISH can expose its data to visualization tools to cover any complex reporting requirements.

Task Delegation and Automatic step escalation

The powerful Workflow Engine of SWORDFISH supports automatic step escalation to the appropriate people inside the organization, to make sure that no Access or Revocation processes are delayed.

Out of Office functionality supports task delegation to cover employee absence needs. When Out of Office is enabled, all workflow steps are automatically assigned to the user's delegate person. Out of Office can be configured by the employee or by an administrator on behalf of the employee.



Benefits

Import of existing users, roles and Organizational Structure

Integration with Active Directory

Asset decomposition and owner mapping with Universe

Audit trail and transparency with Workflow History

How It Works

We have created a user friendly SWORDFISH onboarding process which includes Excel templates for importing users, roles and the organizational structure.

By integrating SWORDFISH with company's Active Directory, users can seamlessly login to the system via Single-Sign-On without the need to provide a username and password.

Additionally, if organizational structure data are embedded inside your Active Directory, a SWORDFISH connector can be used and automatically synchronize the organizational structure and user's data on a scheduled interval so that you don't have to maintain two information repositories.

SWORDFISH provides the Universe functionality, through which organizational assets are decomposed in terms of systems, locations, business units, business services etc.

Identity and Access Management module utilizes Universe in order to automatically assign the access or revocation implementation step to the appropriate system owner. Owners can be configured in System's level or further down on Module or Privilege level.

All workflow steps are automatically logged and provide full audit trails of the actions performed during the execution of a workflow. This way, dependable artifacts can be produced and provided as evidence during an internal or external audit. These artifacts along with the powerful reporting capabilities form a complete auditing solution for Identity and Access Management.



Obrela Security Industries provides security analytics and risk management services to identify, analyse, predict and prevent highly sophisticated security threats in real time.

Tel: +44 (0) 203 397 8723 / info@obrela.com
24th Floor, One Canada Square, Canary Wharf,
E14 5AB, London, United Kingdom

obrela.com

