



Entitlement Manager for SAP ERP

THE SITUATION

Business success nowadays often hinges on the ability to share information quickly and easily across organizations and geographies. This includes sharing roadmaps, product designs, inventory forecasts, etc., both internally and externally (e.g., with contractors, suppliers, and partners). However, challenges abound when trying to strike a balance between giving stakeholders access to sensitive data on one hand and the need to protect the “crown jewels” while adhering to applicable compliance requirements on the other.



OVERVIEW

NextLabs Entitlement Manager for SAP (EM for SAP) provides granular access control and data governance for SAP applications. Through NextLabs’ patented Dynamic Authorization platform, organizations can leverage attribute-based access control and centralized policy management to improve their security and compliance posture for SAP.

EM for SAP prevents unauthorized access to sensitive SAP data through fine-grained access controls, allowing customers to protect data and address compliance requirements at the same time. Ultimately, EM for SAP enables employees and external partners to share critical information, which encourages collaboration, boosts workplace productivity, and increases business agility.

The screenshot shows the NextLabs Control Center interface. The top navigation bar includes the NextLabs logo, 'Control Center', a user profile icon for 'Administrator', and buttons for 'RESET', 'SAVE', and 'SAVE & DEPLOY'. The main content area is titled 'Deny UK Production Manager access to classified data'. On the left, a sidebar menu lists 'Dashboard', 'Policies', 'Components' (with sub-items: Subject, Resource, Action), 'Policy Model', 'Reports', and 'Administration' (with sub-items: System Settings, Delegation Policies, Users, User Source). The central panel displays policy details: 'This policy: Deny UK Production Manager access to classified data', 'Tagged as: S4H', 'Has this effect: Deny', 'When users with these attributes: UK Production Manager', 'Perform these actions: RUN', 'On these resources: EXPORT SECURITY - PR01', and 'Under these conditions:'. The right panel shows 'Policy Effect' set to 'Deny', 'Subject Components' with a dropdown set to 'In' and a selected component 'UK Production Manager User', and 'RESOURCE COMPONENTS' with a dropdown set to 'In' and a selected component 'EXPORT SECURITY - PR01 SAP_Policy_Model'. An 'ADD CONDITION' button is visible below the subject components.

Example of an ABAC policy

KEY FEATURES

Attribute-Based Access Control (ABAC)

ABAC solutions control access to data, business transactions, and batch processes based on policies that examine attributes of the data being accessed, the context of the request, and the user's identity.

EM for SAP takes into account any changes in the attributes of the data or the user and dynamically applies the relevant policies to enforce fine-grained access controls across a wide range of business functions. For instance, a rule may state, "Allow only US-based employees to access ITAR-classified materials from US locations." When a user attempts to access materials, this rule is validated in real-time before access is granted.

This flexibility greatly streamlines change management processes by reducing the need to develop customized code to modify existing roles every time they must be updated, i.e., to account for changes in a user's business function, organizational assignment, location, etc.

Centralized Policy Management

Authorization policies can be centrally managed and reviewed across all of an organization's SAP applications, substantially reducing administration costs.

Dynamic Runtime Policy Enforcement

EM for SAP uses contextual information (e.g., location, device, department) to determine if a user is authorized to access data at runtime. It also segregates the data virtually with view- and field-level security controls for added granularity. Ultimately, EM for SAP simplifies role administration as conditions and attributes change.

Extensive Support of SAP Applications

EM for SAP is an out-of-the-box, SAP-endorsed solution, integrated with several SAP applications natively, including SAP ERP, SAP S/4HANA®, SAP Fiori®, SAP Advanced Planning and Optimization, SAP Business Warehouse, SAP Customer Relationship Management, SAP ERP Human Capital Management, SAP Product Lifecycle Management, SAP Document Management System, the Public Sector Management module, and the Collaboration Folders application.

Security Classification Module

Because classification is crucial to data-level access control rules, EM for SAP includes a module that simplifies the process of identifying and maintaining classification values to address multiple security and compliance concerns at the same time. Security classifications can be easily configured, extended, and managed using batch, interactive, or programmatic interfaces.

Extensible to Custom Applications

In addition to native support of several SAP applications, EM for SAP provides a framework utilizing API calls that can be leveraged within custom applications (aka "Z Programs").

Granular Data Filtering

EM for SAP ensures that users can only view records or other data to which they have been granted access. Authorization can be determined based on the industry, location, department, position, project assignment, or any other attribute of the user, which can then be compared against other attributes of an entity or record such as sensitivity level, type of transaction, etc. For example, you can filter data in charts and reports to quickly identify inventory shortages in Thailand.

Safeguarding of Business Transactions

Users can be given permission to view a set of data and other entities while being authorized to edit, create, and delete only a subset of these records. For instance, a finance manager may be given permission to view detailed cost information on all oil pipeline projects in North America but only allowed to create and edit information for similar projects in Texas.

Enforcement of Segregation of Duties

EM for SAP enables the creation and real-time enforcement of segregation of duties policies, ensuring that no single individual can control all phases of a process or transaction. For instance, to reduce the risk of fraudulent behavior, no person should be able to both create a vendor profile and initiate a payment to said vendor.

User Attributes and Identity Management Integration

User attributes can be leveraged from existing sources, including SAP Central User Administration, Identity Management, Human Capital Management, and other third-party identity management providers, directory servers, or federated identities.

Centralized Audit and Monitoring

EM for SAP tracks and stores user activities and data access across all SAP applications in a central audit server, simplifying compliance management. Analytics for user behavior and access patterns are provided via dashboards, reports, and automated monitoring facilities.

KEY BENEFITS

EM for SAP is a scalable data security solution that protects SAP data in real-time. Benefits include the following:

■ Protect sensitive data

Leverage a transaction- and data-level access management system to secure access and protect data across all SAP applications. EM for SAP's policies control access to business functions and sensitive customer data based on attributes such as data classification, environmental information, user roles and metadata, location, and client system.

■ Ensure compliance

Create information barriers to segregate regulated data or between confidential projects to avoid data spills or contamination. Manage, educate, enforce, and audit access policies to sensitive corporate data to ensure compliance with regulations such as GDPR, ITAR/EAR, and SOX.

■ Streamline compliance

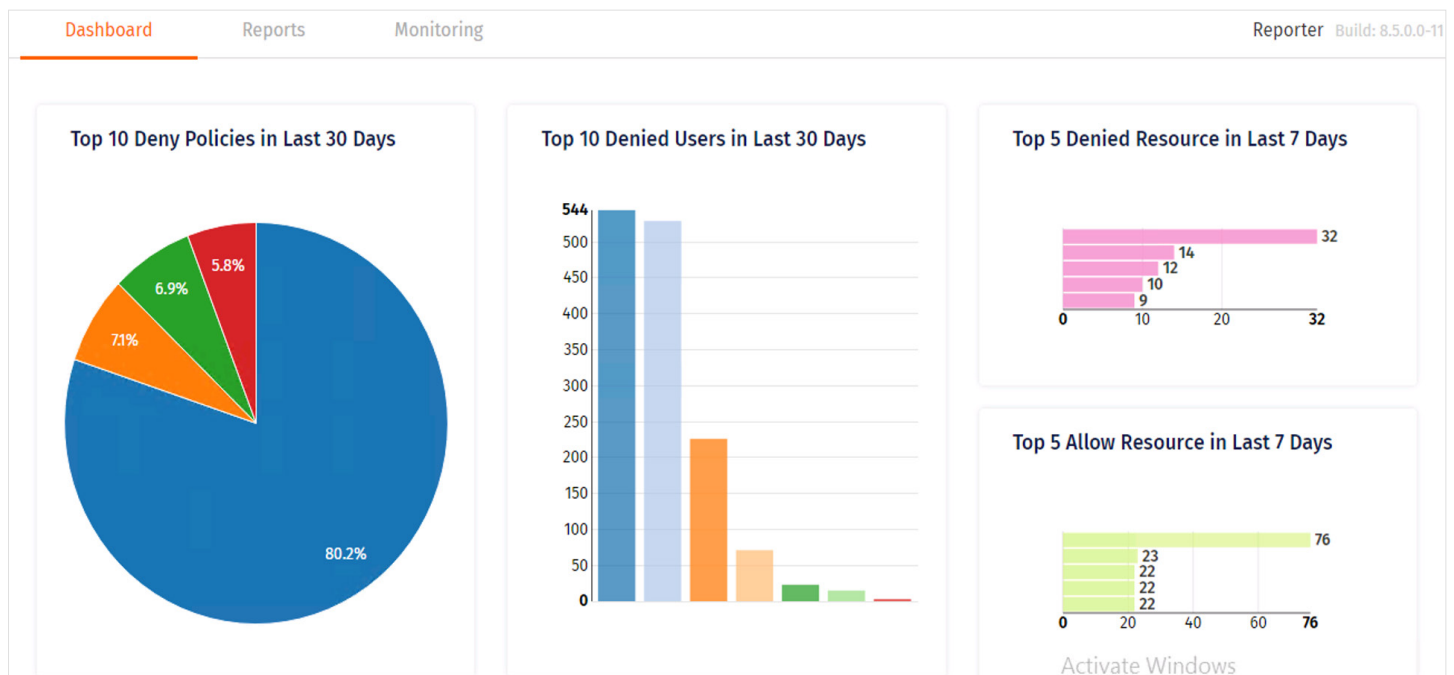
Automate the process of auditing authorization and data access to demonstrate compliance to auditors, regulators, and customers. EM for SAP provides comprehensive visibility about who is accessing what data and when, identifies anomalies before they become major breaches, and monitors and tracks events for audit, oversight, and investigation.

■ Reduce security and compliance management costs

Eliminate the need to implement and maintain costly customizations to meet security, compliance, and governance requirements. Attribute-driven dynamic authorization eliminates the need to maintain multiple SAP instances or manage individual authorization or user groups.

■ Improve business agility

EM for SAP works natively with SAP and manages authorization logic through an externalized, standards-based policy framework. As a result, this slashes application development time and automates change management processes, thereby enhancing business agility.



Centralized audit and reporting

ABOUT NEXTLABS

NextLabs provides data-centric security software to protect business-critical data and applications. Our patented dynamic authorization technology and industry-leading attribute-based policy platform help enterprises identify and protect data, monitor and control access to sensitive data, and help prevent regulatory violations—whether on the cloud or on premise.

The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders.

For more information on NextLabs, please visit <http://www.nextlabs.com>