NEXTLABS®

Dynamic Authorization

Data Access Enforcer for SAP ERP

THE SITUATION

Business success 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 striking a balance between giving stakeholders access to sensitive data on one hand and the need to protect business critical data while adhering to applicable compliance requirements on the other.

THE SOLUTION

NextLabs Data Access Enforcer for SAP (DAE for SAP) provides dynamic data-level security controls and fine-grained data access governance for SAP applications. Through NextLabs' patented Dynamic Authorization platform, organizations can leverage attribute-based policy and centralized policy management to improve their security and compliance posture for SAP. DAE for SAP enforces data-level security controls - such as field-level data masking and record level data segregation and monitors data access activity directly from within the data access layer of the SAP S/4 HANA and SAP ECC.

DAE for SAP complements SAP Dynamic Authorization Management (SAP DAM), which operates at the application layers of the SAP S/4 HANA and SAP ECC. DAE is UI, API, microservice, batch job, report, Transaction, and Fiori app independent – and will support any UI with a single set of policies within a single solution.

DAE for SAP prevents unauthorized access to sensitive SAP data through fine-grained data-level security controls, protecting data and addressing compliance requirements at the same time. DAE for SAP enables employees and external partners to share critical information and collaborate in business processes to improve workforce productivity and business agility.

THE BENEFITS

DAE for SAP is a policy-driven data-centric security solution that uses dynamic authorization to enforce data-level entitlement and data security controls natively to protect SAP data in real-time. Benefits include the following:

Protect Sensitive Data
Leverage an SAP data-model aware and transactional data access level enforcement system to control data manipulation operations and protect data across all SAP applications. DAE for SAP's policies control authorized operations on business-critical data and mask and filter sensitive data based on attributes such as data classification, environmental information, user roles and metadata, location, and client system.

Ensure and Streamline Compliance
Create information barriers to segregate regulated data or 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. Automate the process of auditing authorization and data access to demonstrate compliance to auditors, regulators, and customers. 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.

Improve Business Agility
Works natively with SAP and manages authorization logic through an externalized, standards-based policy framework. This slashes application development time and automates change management processes, enhancing business agility.

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.

KEY FEATURES

Attribute-Based Access Control (ABAC)

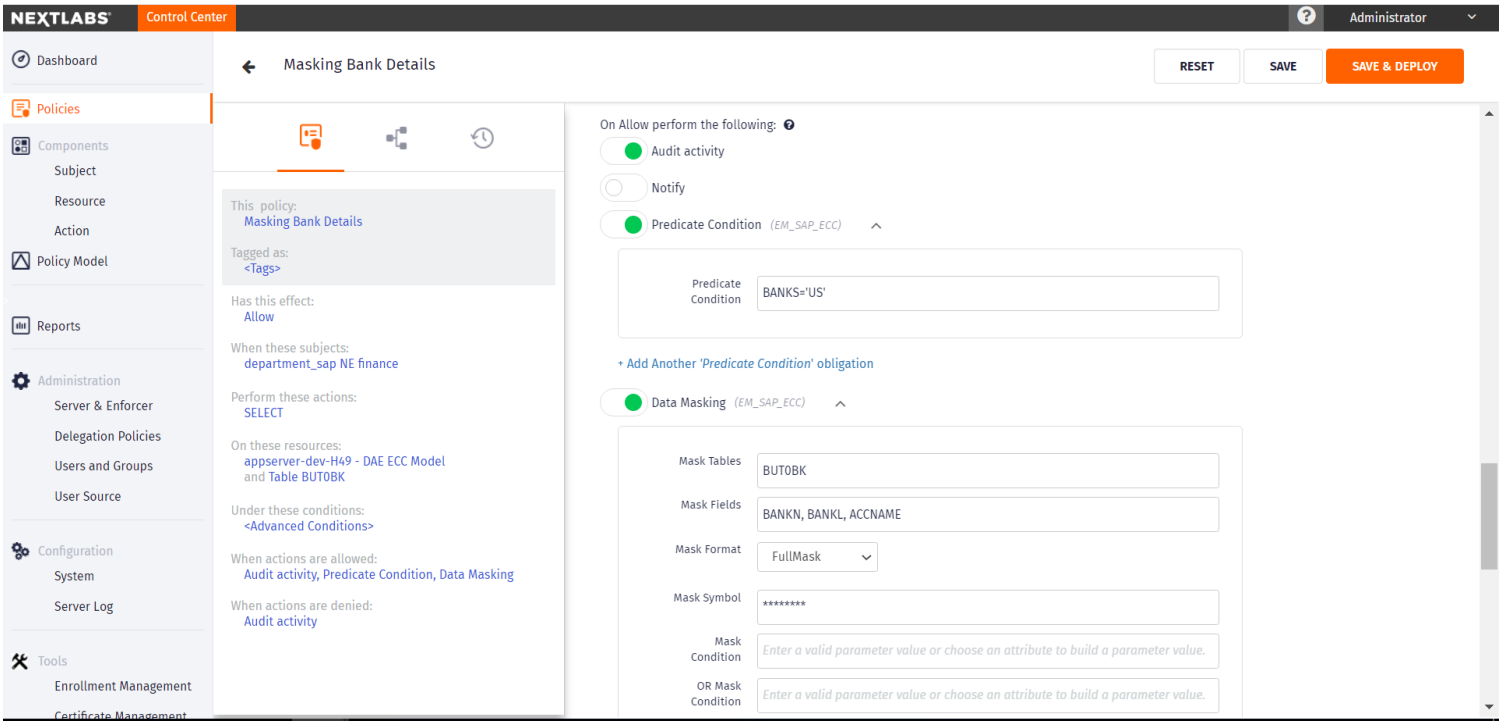
Access to data based on policies that examine attributes of the data being accessed, the context of the request, and user identity.

DAE for SAP dynamically applies the relevant policies, factoring in changes in the attributes of data or the user to enforce fine-grained entitlement and security controls to data regardless of business transaction. Rules are validated in real-time when a user attempts to access data, only then granting access.

This flexibility streamlines change management processes by eliminating the need for customized code to modify existing roles every time they are updated (e.g., changes in a user's business function, organizational assignment, location, etc.).

Centralized Policy Management

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



Example of a Fine-grained Attribute-driven Policy

Dynamic Runtime Policy Enforcement

DAE 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. This simplifies role administration as conditions and attributes change.

Extensive Support of SAP Applications

DAE for SAP works natively with SAP ERP (ECC), SAP S/4HANA®, SAP Fiori®, SAP Advanced Planning and Optimization, SAP Financial, SAP Human Capital Management, SAP Supply Chain Management, SAP CRM, SAP Product Lifecycle Management (PLM), and SAP Document Management System without requiring any T-or Z-Code modification.

Extensible to Custom Applications

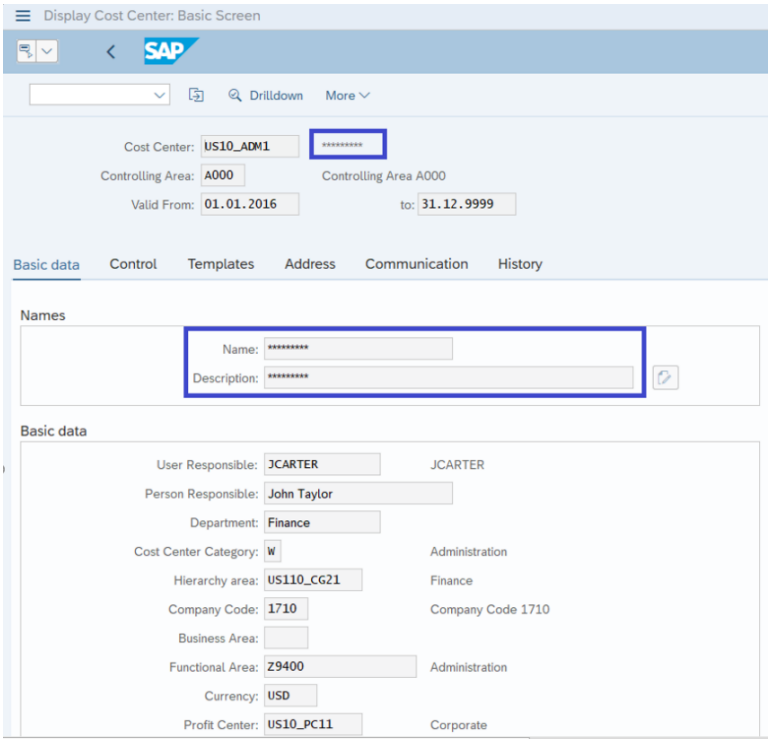
In addition to native support of several SAP applications, DAE for SAP supports batch programs, reports, and custom applications (aka "Z Programs") without code modifications.

Security Classification Module

Because classification is crucial to data-level access control rules, DAE 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.

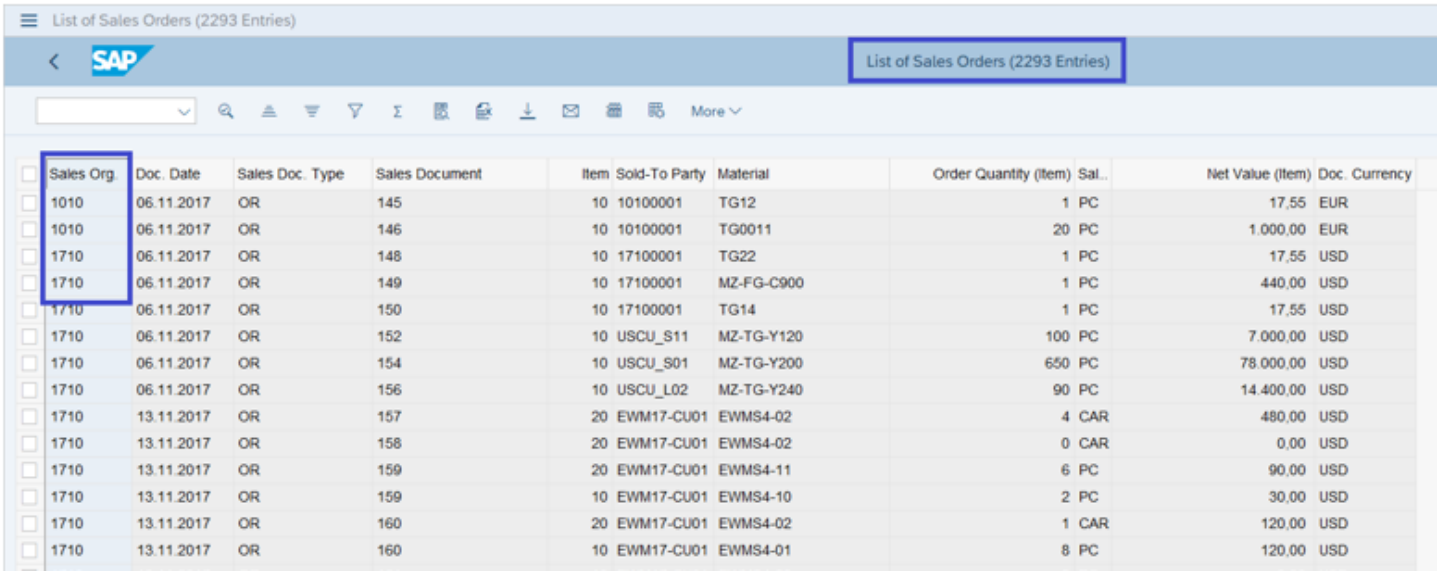
Dynamic Field-level Data Masking

Given the growing importance of data privacy and the various requirements mandating the protection of sensitive data, such as personally identifiable information (PII), customer data, technical data, financial data, etc., the need for data masking is as crucial as ever. DAE for SAP ensures that users can only view the fields on the record to which they have been granted access, the value of the field will be masked for those fields that users are not authorized. It uses policy-driven approach to mask the data in the unauthorized fields based on attributes. These centrally manage policies define masking patterns and rules to determine who, what, when, where, and why to mask field(s) in real-time.



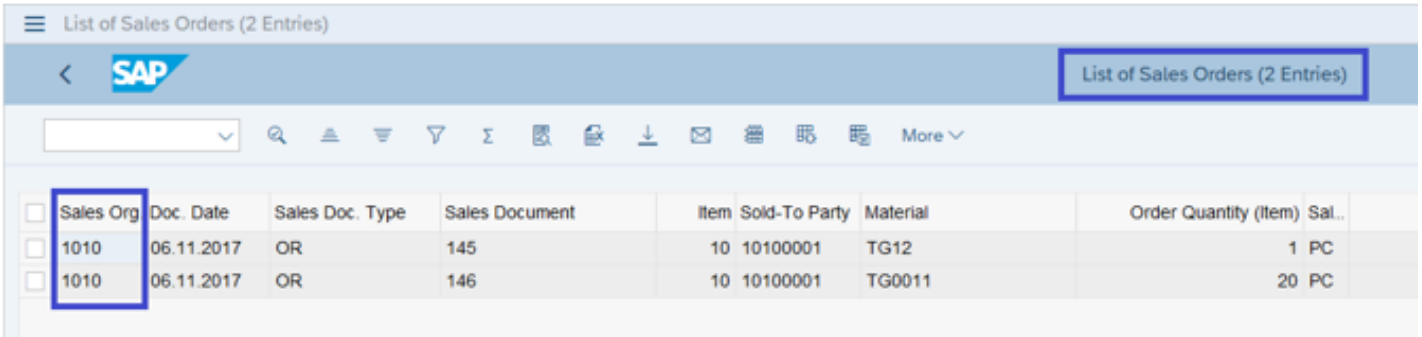
Granular Record-level Data Filtering

DAE 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.



Sales Org.	Doc. Date	Sales Doc. Type	Sales Document	Item	Sold-To Party	Material	Order Quantity (Item)	Sal..	Net Value (Item)	Doc. Currency
1010	06.11.2017	OR	145	10	10100001	TG12	1	PC	17,55	EUR
1010	06.11.2017	OR	146	10	10100001	TG0011	20	PC	1.000,00	EUR
1710	06.11.2017	OR	148	10	17100001	TG22	1	PC	17,55	USD
1710	06.11.2017	OR	149	10	17100001	MZ-FG-C900	1	PC	440,00	USD
1710	06.11.2017	OR	150	10	17100001	TG14	1	PC	17,55	USD
1710	06.11.2017	OR	152	10	USCU_S11	MZ-TG-Y120	100	PC	7.000,00	USD
1710	06.11.2017	OR	154	10	USCU_S01	MZ-TG-Y200	650	PC	78.000,00	USD
1710	06.11.2017	OR	156	10	USCU_L02	MZ-TG-Y240	90	PC	14.400,00	USD
1710	13.11.2017	OR	157	20	EWM17-CU01	EWMS4-02	4	CAR	480,00	USD
1710	13.11.2017	OR	158	20	EWM17-CU01	EWMS4-02	0	CAR	0,00	USD
1710	13.11.2017	OR	159	20	EWM17-CU01	EWMS4-11	6	PC	90,00	USD
1710	13.11.2017	OR	159	10	EWM17-CU01	EWMS4-10	2	PC	30,00	USD
1710	13.11.2017	OR	160	20	EWM17-CU01	EWMS4-02	1	CAR	120,00	USD
1710	13.11.2017	OR	160	10	EWM17-CU01	EWMS4-01	8	PC	120,00	USD

Example of Unfiltered Records



Sales Org	Doc. Date	Sales Doc. Type	Sales Document	Item	Sold-To Party	Material	Order Quantity (Item)	Sal..
1010	06.11.2017	OR	145	10	10100001	TG12	1	PC
1010	06.11.2017	OR	146	10	10100001	TG0011	20	PC

Example of Filtered Records

Business Transaction-Independent Access to Data

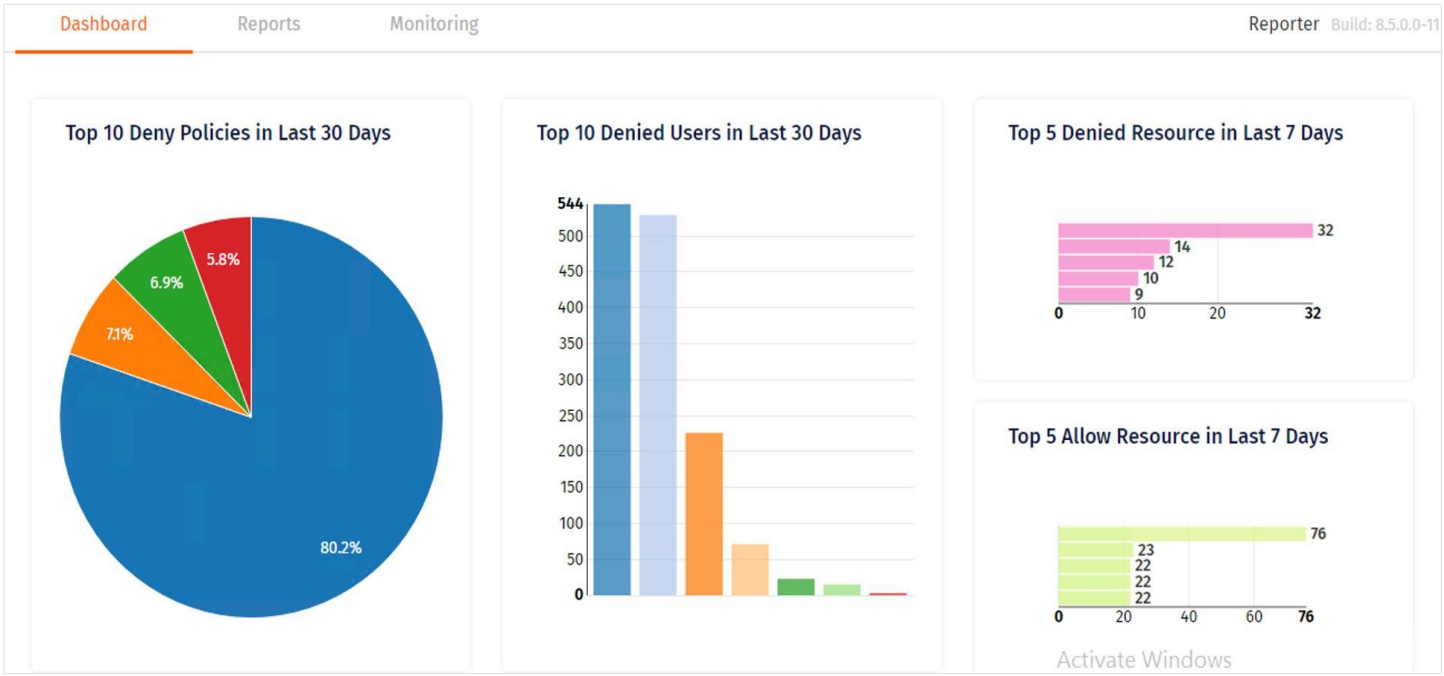
Users can be given permission to view a set of data and other entities while being authorized to edit, create, and delete only a subset of these records. For instance, a finance manager may be given permission to view detailed cost information on all oil pipeline projects in North America but only allowed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

SAP Business Object and User Attributes and Identity Management Integration

SAP Business Object attributes and metadata can be combined with user attributes 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. These attributes are dynamically accessed at runtime to allow access to the data.

Centralized Audit and Monitoring

DAE 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.



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

NEXTLABS®