NEXTLABS

DATA SHEET

NextLabs Entitlement Management

Microsoft Dynamics 365

Maximum Data Security for Distributed Teams

THE SITUATION

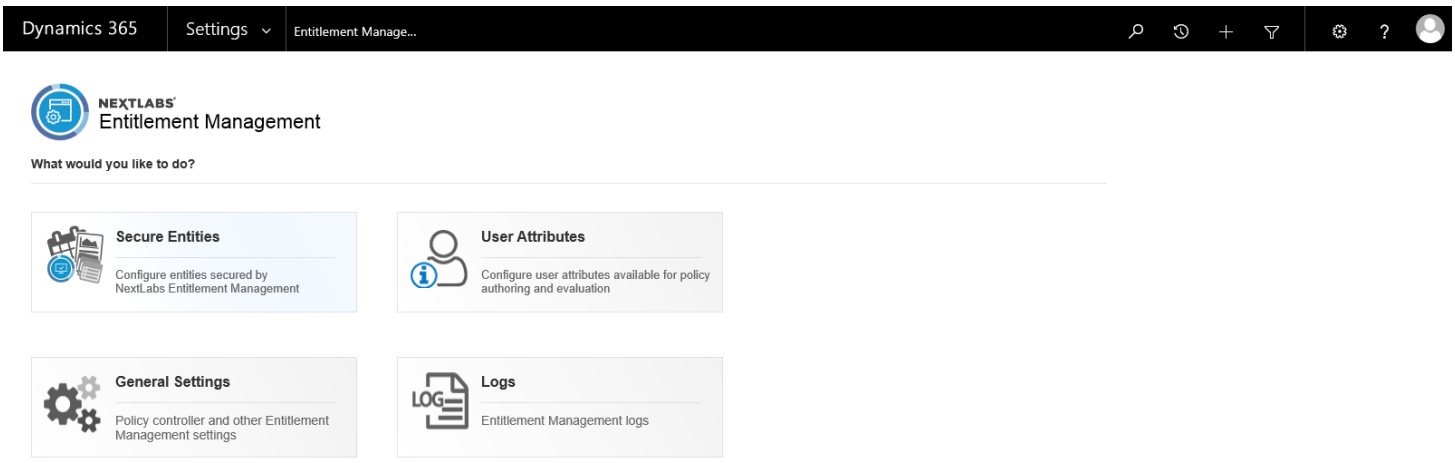
With its focus on usability and functionality, Microsoft Dynamics 365 has ascended very quickly into a leading market position. Customer Resource Management (CRM) and Enterprise Resource Planning (ERP) applications house some of the most sensitive data and yet most frequently accessed data in the enterprise today. But, tighter security over enterprise data has traditionally meant a trade off with accessibility and usability and therefore speed of transacting. Microsoft Dynamics 365 provides secure identity, secure apps and secure infrastructure with a robust security model as part of its solution. But for enterprises who need to manage growth and transition – scaling the workforce, expanding or consolidating through M&A, forming joint ventures to enter new markets, employing a mobile workforce that is geographically dispersed, or operating in heavily regulated industries, they need a dynamic and granular approach to balance rapid access with proper safeguards for critical digital assets.

To help overcome the challenge of scale, role explosion and enterprise distribution while preventing wrong disclosure, NextLabs has extended its Entitlement Management product line to cover Microsoft Dynamics 365, through a native integration, providing the market's first and only Attribute-Based Access Control (ABAC) solution for Microsoft Dynamics 365.

OVERVIEW

NextLabs Entitlement Management for Microsoft Dynamics 365 (**EM365**) provides an advanced security capability - granular access control and data governance - to create a robust and consistent mechanism to safeguard your data in Microsoft Dynamics 365. Using its patented dynamic authorization engine and policy management platform, EM365 provides an additional layer of protection with Attribute-Based Access Control (ABAC) to protect critical data in Dynamics 365 seamlessly while providing a central audit and reporting capability. EM365 allows customers to address their complex access management and data entitlement requirements with the same product focus on usability Microsoft has executed so well.

EM365 extends standard Dynamics 365 authorization and role-based access control to provide a policy-driven, fine-grain access control to safeguard data and business functions - such as transactions and batch processes. Policy authorizes users to execute specific business functions and batch processes in Dynamics 365 based on data classification and user identity attributes. Unlike custom authorization logic which must be implemented and maintained by the customer, EM365 works natively with Dynamics 365 applications and externalizes authorization logic to a powerful policy management system, based on the eXtensible Access Control Markup Language (XACML) standard from OASIS.ORG.



Key Features

ATTRIBUTE BASED ACCESS CONTROL (ABAC)

AABAC can control access to data, business transactions, and batch processes based on policies that use attributes of the data being accessed, the context of the request and the user's identity. EM365 takes into account any changes in the attributes of the data or the user and dynamically applies the relevant policies to enforce access to data and business transactions that the user can execute. EM365 is therefore able to enforce fine-grained access control across a diverse range of business functions that the user can execute in accordance with the changes in data or user attributes. This greatly simplifies the cumbersome task of role management by reducing the need to develop customized code to extend existing roles to account for changes in the user's attributes, such as, business functions, organizational assignments, location changes, etc. By reducing the need to change the roles of the user when the user's access to data changes, EM365 also greatly reduces the complexity in the change management process associated with roles changes and the redundancy of provisioning additional access to users.

Authorization policies are defined as human-readable business rules that determine what data a user can view and what business transactions they can perform within Dynamics 365 based on information (attributes) about the user, the account, lead, opportunity, marketing campaign, support case, and environmental factors such as location and mode of access. A simple policy may state that account executives can view and edit accounts, leads, and opportunities that belong to the industry, region, and size of company for which the user is responsible.

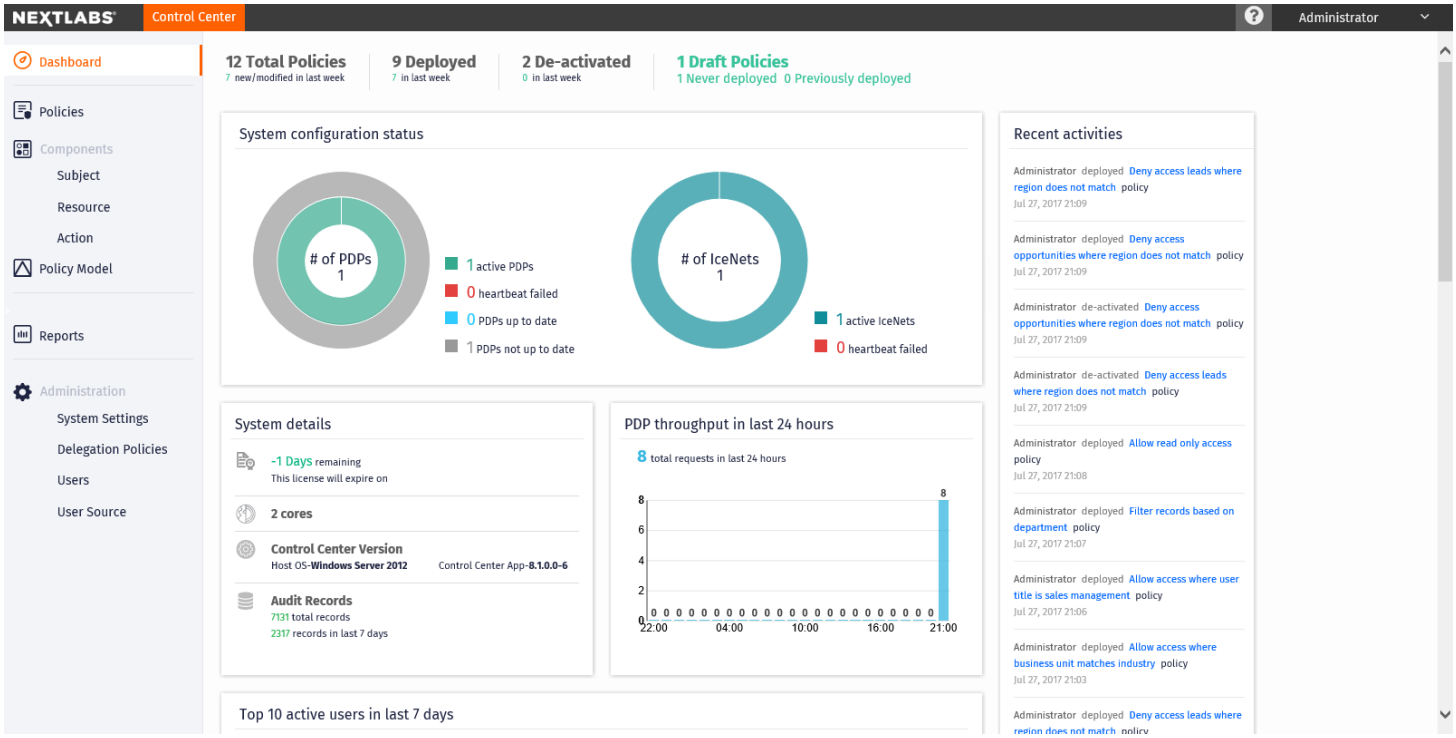
CENTRALIZED POLICY MANAGEMENT

Authorization policies stored in the central Control Center Policy Server can be managed directly by data or compliance owners with an easy-to-use graphical Policy Studio application that provides full lifecycle management and workflow. Control Center server allows you to centrally manage and review authorization policies across your applications and services. For example, a policy that determines what accounts a user can view in Dynamics 365 can also determine that the user can only access documents in SharePoint related to those accounts.

DYNAMIC RUNTIME POLICY ENFORCEMENT

EEM365's Policy Engine performs policy evaluation dynamically using the real-time value of the attributes specified in the policies to determine if the user is authorized to perform the business transaction or has access to the data at runtime. This means that administrators no longer need to maintain and keep track of role, permission, and data ownership assignments as users move between departments, territories, locations; when accounts, campaigns, or support cases are modified; or as other conditions and attributes change.

Attributes can be dynamically retrieved at runtime from a variety of sources, including but not limited to Dynamics 365, HR and Identity Management systems, Azure AD, LDAP servers, from APIs and web services, or any other system of record.



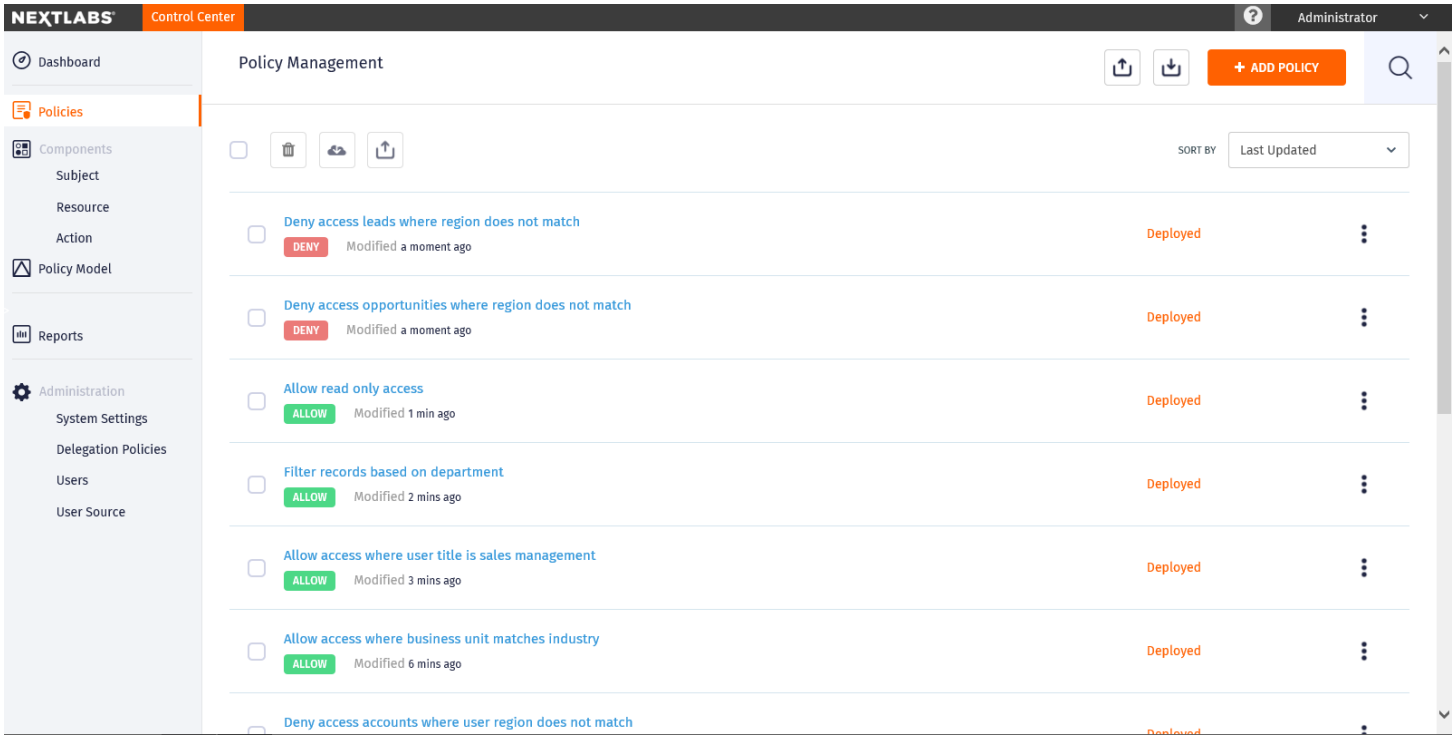
ROW LEVEL DATA FILTERING

Using policies, EM365 ensures that users can only view accounts, opportunities, leads, contacts, campaigns, support cases, or other entities they have been granted access to. 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 the attributes of each entity and record such as the account industry, region, and revenue, support case severity, sensitivity, and product assignment, or any other information about the record.

only see the social security number and date of birth for contacts that they created.

PREVENTATIVE RUNTIME SOD ENFORCEMENT

EM365 can prevent Segregation of Duties (SoD) and other compliance violations from happening as policies are dynamically evaluated to prevent conflicting activities and unauthorized actions at runtime. For example, to remove risk of fraud where users could create fictitious vendors, users should be prevented from submitting purchase orders for any vendor that they themselves created.



POLICY INHERITANCE AND ENFORCEMENT ACROSS RELATED ENTITIES

EM365 provides the capability to enforce policies across related entities using inheritance. For example, an account executive can only access opportunities and leads for the accounts that they have been authorized to view.

SAFEGUARD BUSINESS TRANSACTIONS

Users can be given the permission to view a set of accounts and other entities while being authorized to edit, create, and delete a subset of these records, based on policies. An account executive may be given the permission to view all accounts in North America, while only allowed to create, edit, and delete accounts that belong to the West Coast region and Financial Services industry.

FIELD LEVEL DATA REDACTION & MASKING

Authorization Policies can be defined to redact and mask sensitive fields on a row by row basis. For example, an account executive can

CENTRALIZED AUDIT & MONITORING

Policy compliance and end user activity are collected in a central audit server for reporting by the Reporter application - a graphical analysis, charting, and reporting application. EM365 tracks and stores user activity and data access across Dynamics 365 and other applications and services in a central audit server. Insight into user behavior and access patterns is provided through dashboards, reports and automated monitoring facilities.

SAAS, PRIVATE CLOUD, AND ON-PREMISE DEPLOYMENTS

NextLabs is available for SaaS, Private Cloud and on premise deployments of Dynamics 365.

KEY BENEFITS

EM365 provides a scalable access management and data governance framework to protect your data in Microsoft Dynamics 365 either in the cloud or on premise. The benefits of EM365 include:

Scalable and Sustainable Access Management – Using the advanced policy-driven transaction and data level access management system to secure access and protect data in Dynamics 365 and other business applications. EM365's policies control access to business functions and the most sensitive customer data based on attributes such as data classification, environmental information, user roles and metadata, location, and client system.

Segregate data within a single global Dynamics 365 instance – Create information barriers to segregate regulated data or between confidential projects to avoid data spills or contamination.

Ensure compliance and protect sensitive data – Manage, educate, enforce, and audit access policies to the company, partners', and customers' sensitive data to ensure compliance with regulations such as the GDPR, Privacy, ITAR, EAR, and NERC.

Reduce security management costs – Attribute-driven dynamic authorization eliminates the need to maintain multiple Dynamics 365 instances or manage individual authorization or user groups.

Improve business agility and eliminate expensive customizations – No need to implement and maintain costly customizations to meet compliance and governance requirements. EM365 works natively with Dynamics 365 and manages authorization logic through an externalized, standards-based policy framework. Increased business agility by minimizing manual change management and eliminating code changes when user status or the business process changes.

Automate audit and compliance reporting – Automate the process of auditing authorization and data access to demonstrate compliance to auditors, regulators, and customers. EM365 provides comprehensive visibility about who is accessing what data and when, identifies anomalies before they become major breaches, and an extensible reporting facility to monitor and track events and data access for audit, oversight, and investigation.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. 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 such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.

NEXTLABS


NEXTLABS