Infosys® | CONSULTING

Dynamic Data Protection using Attribute-Based Access Control (ABAC)

An Infosys Consulting and NextLabs Technical Whitepaper

By Nitin Aggarwal and Krishna Mohan Dubbaka

Consulting@Infosys.com | InfosysConsultingInsights.com
info@nextlabs.com | NextLabs.com

NEXTLABS®

Abstract

In this technical white paper, the importance of dynamic data protection in relation to **Attribute-Based Access Control (ABAC)** is discussed. Role-Based Access Control (RBAC), the precursor to ABAC, while commonly used today, was designed for simpler organizational structures. With the introduction of ABAC companies can enhance their existing roles using attributes and policies. This is a more scalable method, which can adapt to ever-changing dynamic environments. As seen through multiple use cases, **NextLabs Data Access Enforcer (DAE)** can be used to dynamically protect data using ABAC to ensure data remains secure through data masking, filtering, and data manipulation controls.

Key Concept

Data is the New Gold of Digital Era and protecting the data is critical for survival of companies. There is an increasing number of regulations demanding data protection or even geographical data segregation due to trade sanctions. While most of the applications / systems used in companies have inherent security concepts, it is exceedingly difficult to protect / segregate data at the lowest level without engaging in big time-consuming projects and extensive developments. This becomes a bottleneck for companies as most of the requirements are time sensitive and require a fast way to achieve protection / segregation.

Learning Objective

Reading this article, you will learn:

- Difference between Role-based and Attribute-based access control mechanism
- How to use NextLabs Data Access Enforcer (DAE) to achieve dynamic data protection

Role Based Access Control (RBAC)

RBAC is the most used access control mechanism in companies today. It relies on the creation of a role / group comprising of multiple access privileges that can then be assigned to a user. Therefore, access is given to a role and the User may be assigned one or more roles for the user to get that access. While this is the most used method, it lacks the flexibility and scalability required for addressing data protection / segregation use cases as it leads to role explosion (creation of hundreds and thousands of small roles to control access at lowest level).

As shown in example below, Roles IT/Finance/HR are created with respective access to Documents X/Y. These roles are then assigned to the four users thereby giving them the access that assigned role carries.

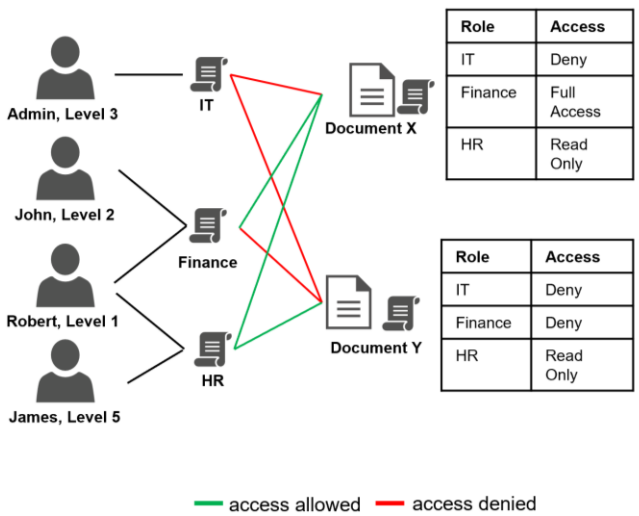


Figure 1: Example of RBAC

NEXTLABS®

Attribute Based Access Control (ABAC)

ABAC is an alternative approach to access control which is increasingly becoming popular because of its benefits. It relies on runtime determination of access using predefined policies which are then evaluated by providing attributes of the user whenever a user tries to access the applications. The attribute values provided for policy evaluation can be fetched at runtime from any data source. This makes the whole access control mechanism simplified, automated, and consistent across multiple applications.

There are three categories of attributes that can be used in ABAC (refer figure 2 below)

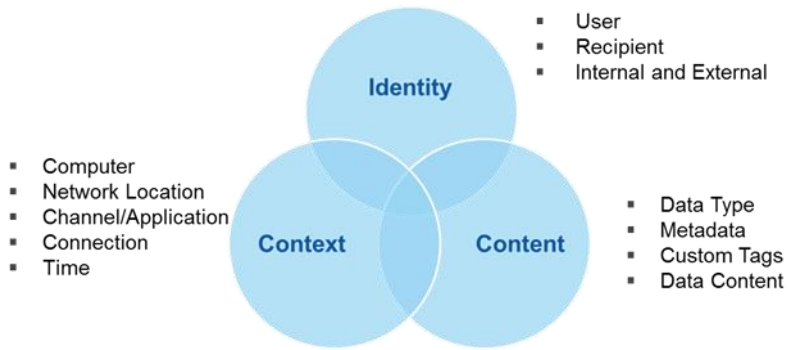
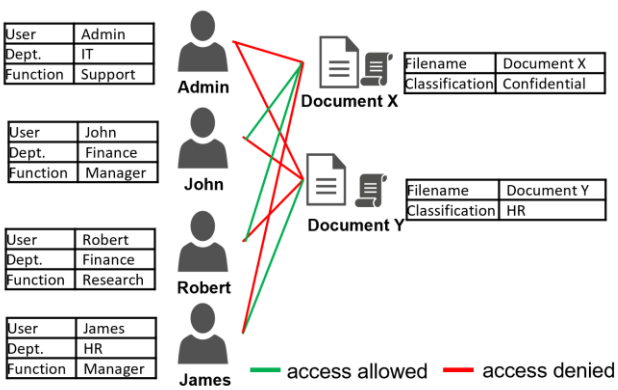


Figure 2: Categories of attributes

As shown in example below, 3 policies control access to the documents. The 1st policy denies access to these documents for all users. The 2nd policy then allows users who are HR managers to access documents classified as HR i.e., document Y in this example. The 3rd policy allows Finance staff to access documents classified as Confidential i.e., document X in this example.

The benefit using this approach is that in future there may be new documents created or new users added but ABAC will not require any change to be made in access as the system will read the classification of these new documents and the attributes of the new users and allow/deny them access accordingly.



Policies:

- Allow all **HR Staff** with function **Manager** to read documents classified as **HR**.
- Allow all **Finance staff** to **read** all documents classified **confidential.**

Figure 3: Example of ABAC

NEXTLABS®

How does ABAC work?

Based on **XACML standards**, access control systems providing ABAC capabilities comprise of the following:

1. Policy Enforcement Point (PEP)
2. Policy Decision Point (PDP)
3. Policy Information Point (PIP)
4. Policy Repository Point (PRP)
5. Policy Administration Point (PAP)

Abbr.	Term	Description
PAP	Policy Administration Point	Point which manages access authorization policies
PDP	Policy Decision Point	Point which evaluates access requests against authorization policies before issuing access decisions
PEP	Policy Enforcement Point	Point which intercepts user's access request to a resource, makes a decision request to the PDP to obtain the access decision (i.e., access to the resource is approved or rejected), and acts on the received decision
PIP	Policy Information Point	The system entity that acts as a source of attribute values (i.e., a resource, subject, environment)
PRP	Policy Retrieval Point	Point where the XACML access authorization policies are stored, typically a database or the filesystem.

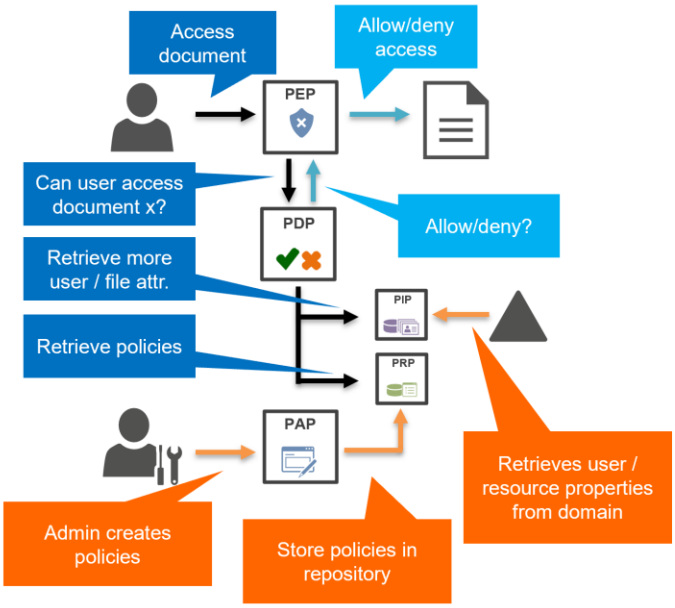


Figure 4: Components in ABAC

NEXTLABS®

PEP intercepts an attempt made by a user to access a document / data. A call is then made to the **PDP** for decision making which in turn fetches the policies and attribute data from PRP and **PIP** respectively to make a decision. The decision is then communicated back to PEP. In case of an Allow decision, PEP allows the user to access the document / data whereas in case of Deny decision, PEP denies the user access to the document / data. The types of enforcements through PEP can be customized based on different systems such as data masking, segregation, filtering, deletion, encryption etc.

NextLabs Data Access Enforcer

NextLabs Data Access Enforcer (DAE) provides dynamic data-level security controls and fine-grained data access governance to a variety of applications out-of-the-box. Through NextLabs' patented **Dynamic Authorization** platform, organizations can leverage attribute-based policy and centralized policy management to improve their security and compliance posture.

DAE enforces data-level security controls - such as field-level data masking and record level data segregation, ensuring that only those with authorization can view the fields/and or records they have been granted access to. DAE monitors data access activity directly from within the data access layer of the application, allowing the solution to track, report, and alert on risky access activity through its centralized dashboards, reports, and automated monitoring facilities. Data access requests, whether allowed or blocked, across the application are tracked and logged centrally, simplifying compliance management and audits.

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. The solution enables employees and external partners to share critical information and collaborate in business processes to improve workforce productivity and business agility.

The diagram below explains at high-level, the functioning of NextLabs Data Centric Security and Data Protection for Enterprise

Data Access Enforcer – How does it work?

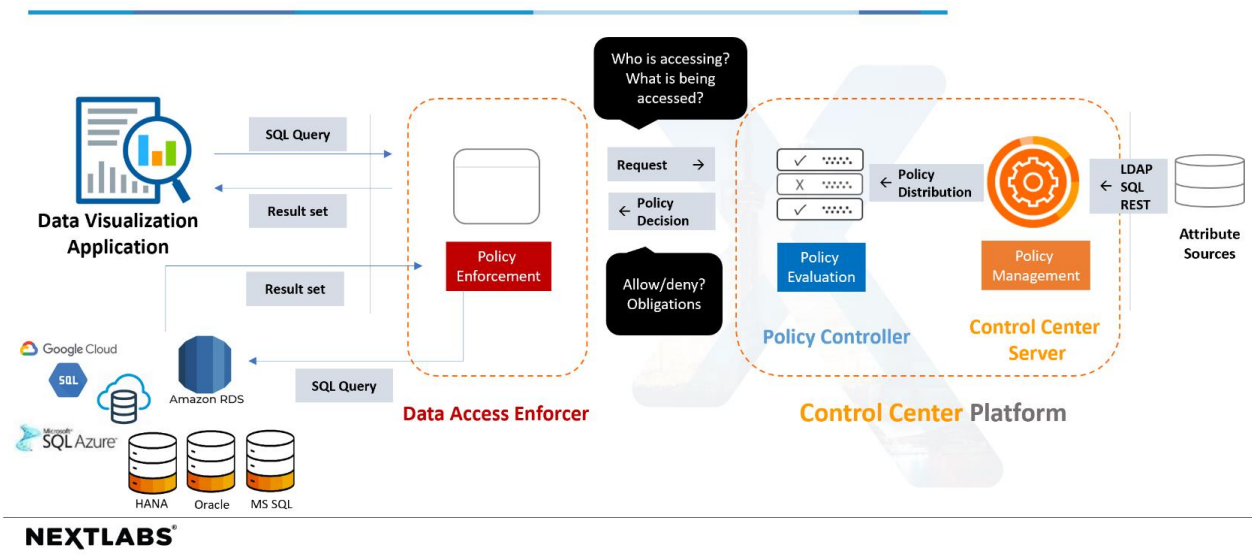


Figure 5: DAE's High Level Functionality

NEXTLABS

Using NextLabs DAE to Dynamically Protect Data

The following are the key features of DAE:

Data Masking

There are 2 types of masking that are supported: 1. FPE – **Format Preserving Encryption** 2. **Dynamic Data Masking**

Using FPE, you can mask/obfuscate data at rest, meaning the sensitive fields are obfuscated at the database level and then decrypted for authorized users based on policy

Contrary to FPE, Dynamic Data Masking is applied on the fly. As an example, when an unauthorized user views a sensitive field, data masking is applied at the data access level based on policy. These centrally managed policies define masking patterns and rules to determine who, what, when, where, and why to mask field(s) in real-time.

Dynamic Data Filtering

DAE also provides the option to **filter data** ensuring users to 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.

Data Manipulation Controls

Apart from protecting data from view/read, DAE can also be used to control who can or who can't perform data manipulation actions such as inserting new data, changing existing data or deleting existing data. These controls can be applied to both application layer level and at the database level.

Example Use Cases

Let us consider the following context and business scenario as an example to demonstrate NextLabs Data Access Enforcer's ability to implement Dynamic Data Protection using ABAC (Attribute Based Access Control)

Company X is a semiconductor company with headquarters in North America. They manufacture flash memory products including memory cards, readers, USB flash drives and SSDs.

'Procurement' is one of their key business groups with 200+ users spread across the world supporting the function. Purchase Managers take the lead on the core procurement activities both direct (tangible products such as raw materials) and indirect (intangibles such as services, consulting) procurement, they deal with 100+ vendors across the globe.

To comply with external regulations as well as internal mandate to streamline the organization setup, Mr. Smith (Director of Procurement) has the following data protection requirements in the Procurement to Pay life cycle:

#	Process & App	Data Protection Requirements
1	Vendor evaluation & Contract Negotiation **(Service Now)**	Vendor evaluation data should be visible to authorized users only based on the "project" attribute.
2	Vendor master data **(SAP)**	There are certain sensitive fields on Vendor record that should be visible only to authorized users. Un-authorized users should not see actual data but masked data
3	Accounts Payable **(SAP)**	In AP SSC (Share Services Center), only authorized users should view/process invoices for PO (Purchase Order) containing sensitive or ITAR controlled materials

Use Case-1:

In the given business scenario, vendor evaluation and contract negotiation are managed via ServiceNow service management. Vendor details including some financial information are stored in "Service" record either as direct attribute or as an attachment. Only authorized users can view "vendor evaluation" service requests and the connected attachments. Unauthorized user access should be denied.

Every time a user tries to access a service request, DAE will check if the user is assigned to the same project as the project of the service request. In case the check is fulfilled, user will be allowed to access the service request. However, if the check fails, the user will be denied access to the service request.

User ID	User Project	SR#	SR Project	Expected Behavior
DEMOUSER01	Project-1	INC0010596	Project-1	Allow
DEMOUSER02	Project-2	INC0010596	Project-1	Deny
DEMOUSER02	Project-2	INC0010600	Project-2	Allow
DEMOUSER03	(empty)	INC0010596	Project-1	Deny
DEMOUSER03	(empty)	INC0010600	Project-2	Deny

How to achieve it using NextLabs DAE

The above requirement can be achieved using the following attribute model and policy model

Subject Attributes : Project

Resource Attributes: Project

Policy-1: Top level deny policy that denies access to any service requests in ServiceNow

***Policy-2*:** As a child policy under Policy-1, allow access to service request if user. Project = service request. Project

NEXTLABS®

Use Case-2:

Vendor bank details are stored and maintained in SAP via t-code BP. Sensitive information such as Bank Account No, Bank Account Key needs to be protected so that only authorized users can see the data and for un-authorized users such data should be masked

Transactions/Fiori : BP

Tables : BUT0BK

Field : BANKN, BANKL, ACCNAME

Finance department users with Mgr II and above position level can see the actual data for these sensitive fields whereas others see them as masked.

Every time a user tries to access Vendor master record, DAE will check the department of the user. Data for the 3 sensitive fields above will be shown masked to the user if he/she does not belong to the Finance department.

User ID	Department	Position Level	Expected Behavior
DEMOUSER01	Purchasing	Mgr III	Data for sensitive fields shown as masked
DEMOUSER02	Finance	Mgr I	Data for sensitive fields shown as masked
DEMOUSER03	Finance	Mgr II	Data for sensitive fields is shown (actual data)
DEMOUSER04	Finance	Mgr III	Data for sensitive fields is shown (actual data)

How to achieve it using NextLabs DAE

The above requirement can be achieved using Dynamic Data Masking policy. Such policies are defined directly on the corresponding table(s) and field(s). In this scenario, following would be the “Data Masking” policy definition

Attribute(s) used : Department, Position Level

There are multiple ways in SAP to define the association between a user and his/her department. The most common one is using SAP HCM data to determine user’s department.

Subject condition : if user.department != ‘finance’ OR (user.department = finance AND user.positonlevel < Mgr II)

NEXTLABS®

Data Masking Obligation

Table : BUT0BK

Field(s) : BANKN, BANKL, ACCNAME

Mask Symbol : ********

With the above policy in place, whenever user is viewing the bank account details of a Vendor, his/her department is checked. In case his/her department is not finance, then DAE applies masking for the fields BANKN, BANKL, ACCNAME.

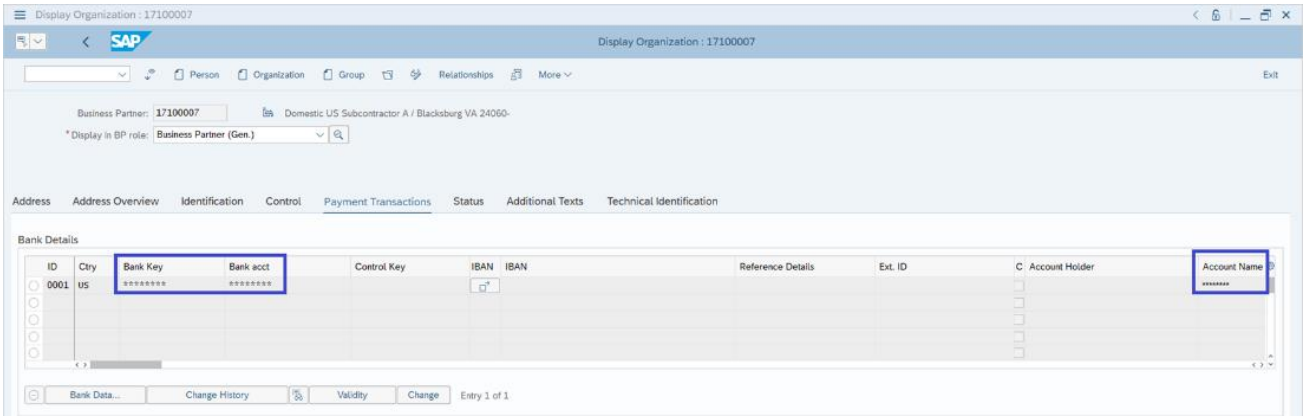


Figure 6: DAE Masking example using SAP GUI

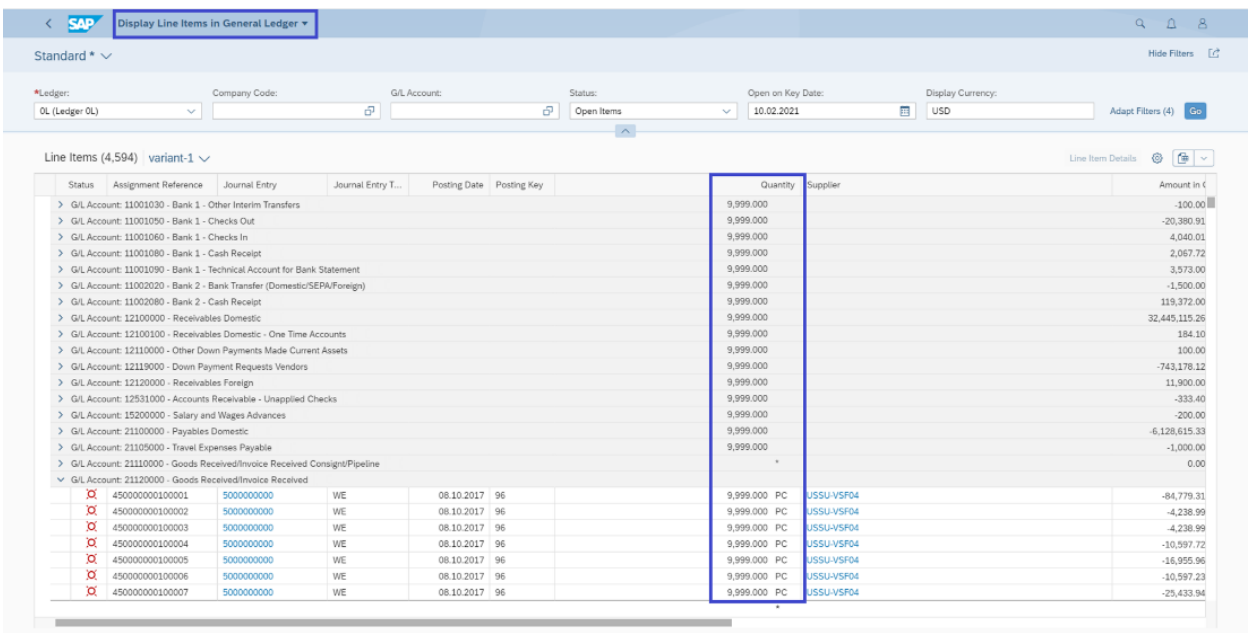


Figure 7: DAE Masking example using SAP Fiori – Masking of a numeric field

NEXTLABS®

Use Case-3:

Only authorized users (users from US) should see invoices related to sensitive material in the AP cockpit. Such invoices should get filtered out for users outside the US.

Transactions/Fiori : Accounts Payables Overview

Tables : ACDOCA

Field : PURCHASE ORDER

Only US citizens when accessing in the US can view and process invoices for sensitive materials. US citizens accessing data from outside of the US should not be allowed to see invoices for sensitive materials. If a non-US citizen is accessing the data, then he should not be allowed to see invoices for sensitive materials.

Every time a user tries to access the AP cockpit, DAE will check the citizenship of the user (from user attribute data source) and the geolocation from where he/she is accessing the data. In case the user accessing is not a US citizen, DAE will filter out all invoices that relate to sensitive materials.

User ID	Citizenship	Geolocation	Expected Behavior
DEMOUSER01	US	US	The user is shown invoices for sensitive materials, and he/she can process the same
DEMOUSER02	Non-US		User does not see invoices for sensitive materials as they are filtered out
DEMOUSER03	US	Canada	User does not see invoices for sensitive materials as they are filtered out

How to achieve it using NextLabs DAE

The above requirement can be achieved using Dynamic Data Filtering policy. Such policies are defined directly on the corresponding table(s) and a filter condition is defined for un-authorized users.

Attribute(s) used : Citizenship of User, IP address of the user's machine

Subject condition : if user.Citizenship != 'US' OR (user.citizen = 'US' AND user.locationip IS NOT in the range of IP addresses for US)

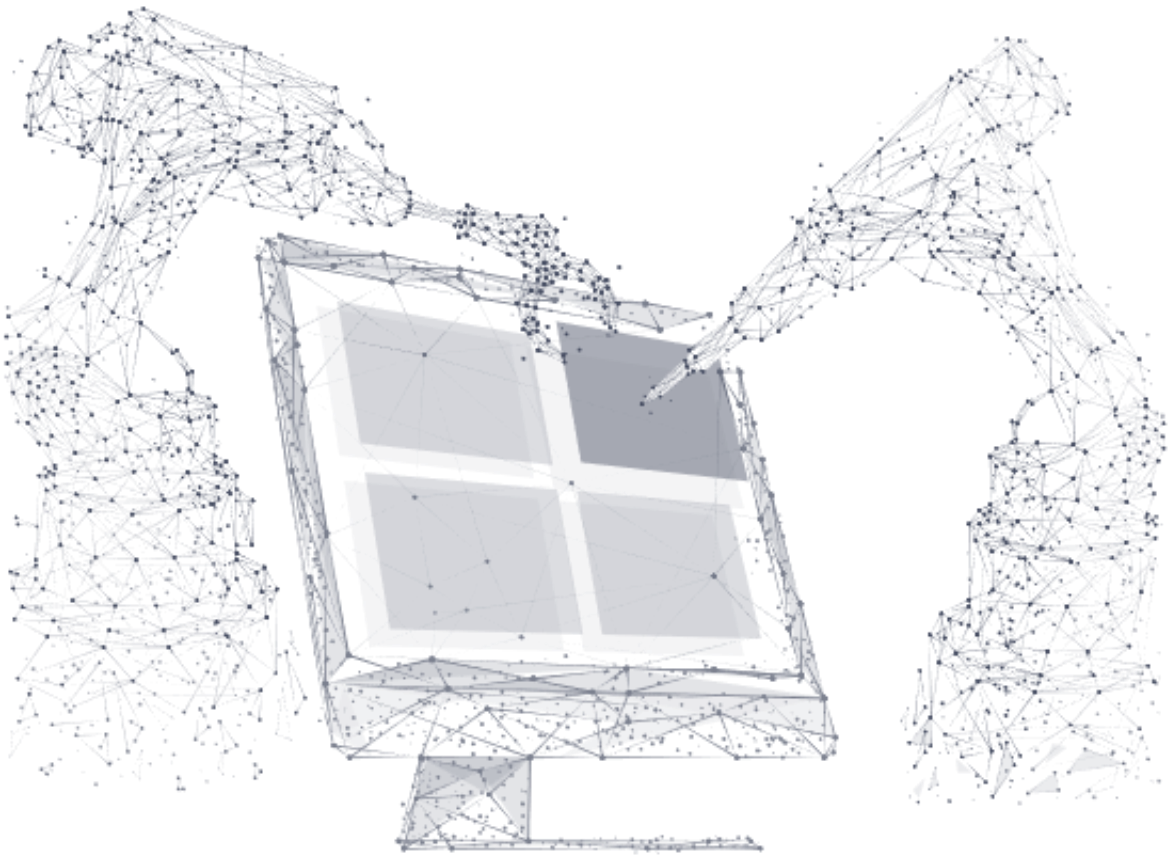
Predicate (Data Filter) Condition

Table : ACDOCA

Predicate : MATNR NOT IN (SELECT MATNR FROM /NXLDAE/CLASSIF)

NEXTLABS®

With the above policy in place, whenever user tries to access AP cockpit, DAE will check the citizenship of the user (from user attribute data source) and the geolocation from where he/she is accessing the data. In case the user accessing is not a US citizen or user is US Citizen but accessing from outside of US, DAE will filter out all invoices that relate to sensitive materials.



consulting@Infosys.com
InfosysConsultingInsights.com

LinkedIn: /company/infosysconsulting
Twitter: @infosysconsltng

info@nextlabs.com
NextLabs.com

LinkedIn: /company/nexlabs

About Infosys Consulting

Infosys Consulting is a global management consulting firm helping some of the world's most recognizable brands transform and innovate. Our consultants are industry experts that lead complex change agendas driven by disruptive technology. With offices in 20 countries and backed by the power of the global Infosys brand, our teams help the C-suite navigate today's digital landscape to win market share and create shareholder value for lasting competitive advantage. To see our ideas in action, or to join a new type of consulting firm, visit us at www.InfosysConsultingInsights.com.

For more information, contact consulting@infosys.com