Importing and Securing Data in ServiceNow

Team ID : LTVIP2025TMID28567

Team Size : 3

Team Leader : vallu Mahendra

Team member : Devaki v

Team member : cheekatla sarat Chandra

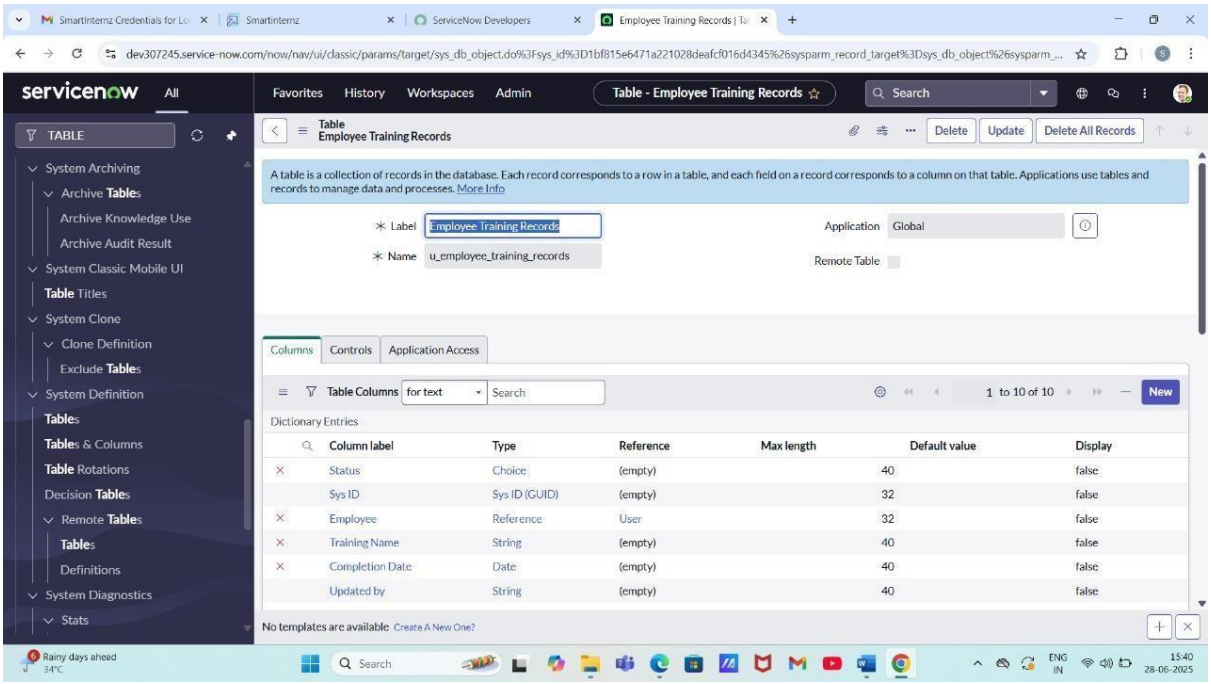
INTRODUCTION:

ServiceNow is a cloud-based platform widely used for IT service management (ITSM), business workflow automation, and enterprise operations. One of its key capabilities is handling data — including importing, organizing, and securing it efficiently.

Data Importing in ServiceNow involves bringing external data (e.g., from Excel, CSV, or databases) into the platform to populate tables, automate workflows, or support business processes. This is typically done using tools like **Import Sets**, **Transform Maps**, and **Data Sources**. These tools ensure that raw data is accurately mapped to ServiceNow's structured tables, preserving data integrity and usability.

On the other hand, **Data Security** in ServiceNow is critical to protect sensitive information and ensure proper access control. ServiceNow employs a robust **role-based access control (RBAC)** system, allowing administrators to define who can view, edit, or delete specific data. Additionally, **Field-level encryption**, **Access Control Rules**, and **Data Policies** are used to safeguard data throughout its lifecycle.

Tables in ServiceNow:



In ServiceNow, tables are the foundational components where data is stored. Each table contains fields (columns) and records (rows) similar to a relational database.
Tables can represent:

- Users (sys_user)
- Incidents (incident)
- Departments (cmn_department)
- Assets (alm_asset)
- Configuration Items (cmdb_ci)
- Custom business records (via custom tables)

Field Types in Tables

Each table contains **fields**, each with a defined data type. Common field types include:

Field Type	Description
String	Text values (e.g., Name, Description)
Integer	Whole numbers
Date/Time	Date and time information
Reference	Link to another table
Choice	Dropdown list of predefined values
Boolean	True/False checkbox
Glide List	List of references to other table records
Journal (Notes)	Tracks history (e.g., comments/work notes)

System Tables:

ServiceNow also includes **system tables** that handle internal configurations:

Table Name	Purpose
sys_user	User profiles
sys_group	User groups
sys_user_role	User roles
sys_dictionary	Defines fields and attributes
sys_metadata	Stores metadata about configurations
sys_properties	Global system properties
sys_audit	Audit logs

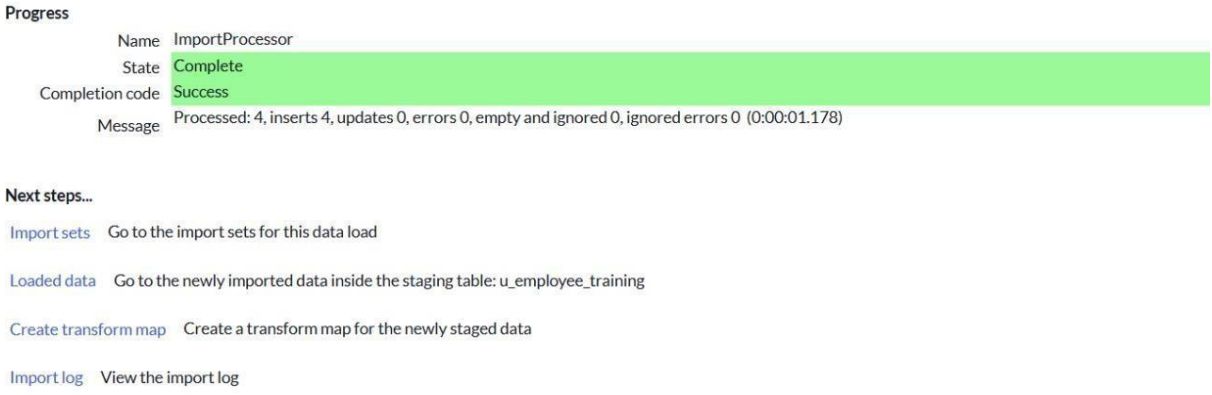
Importing Data:

Import Process Overview:
To bring data into ServiceNow, follow these steps:
Step 1: Prepare Your Data

- Format the data in CSV, Excel, or XML.

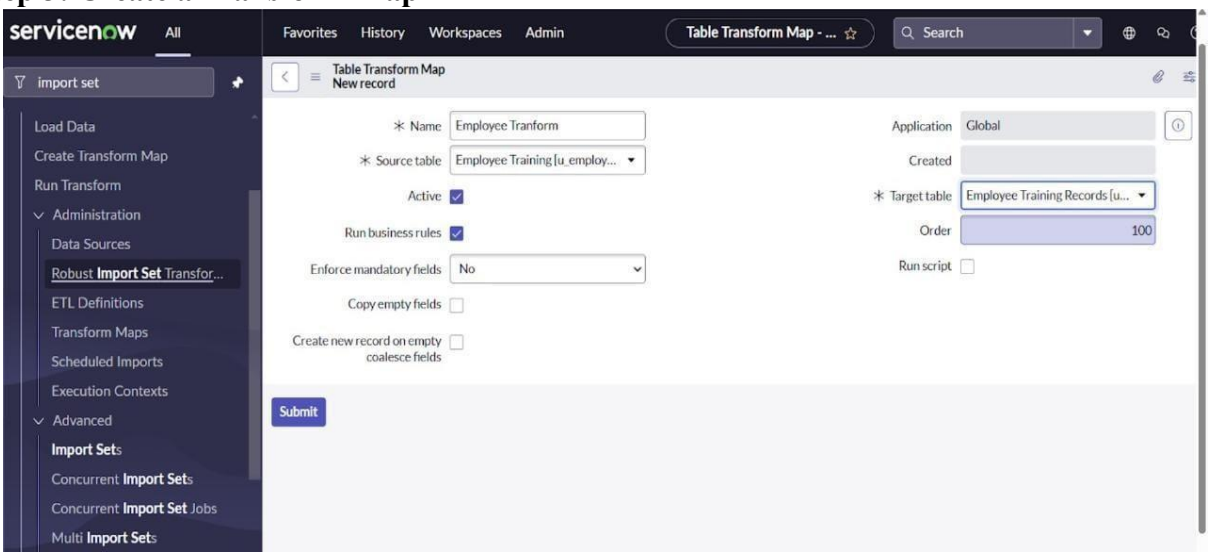
- Include necessary fields like employee_id, name, department, etc.

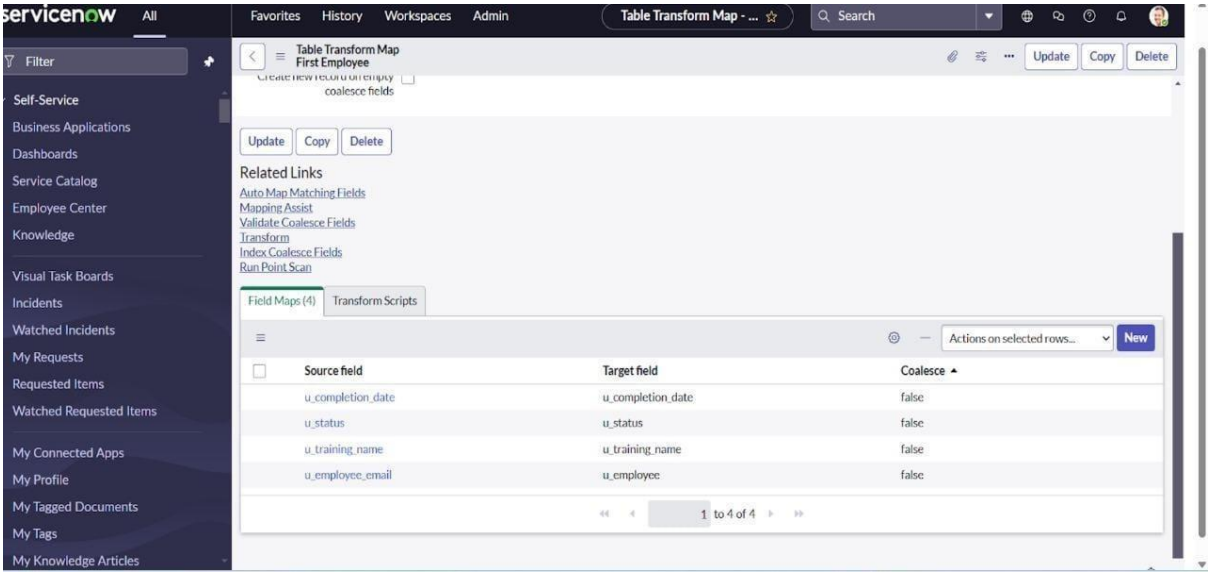
Step 2: Create an Import Set



- Go to System Import Sets > Load Data.
- Upload your file and create a new Import Set Table.

Step 3: Create a Transform Map



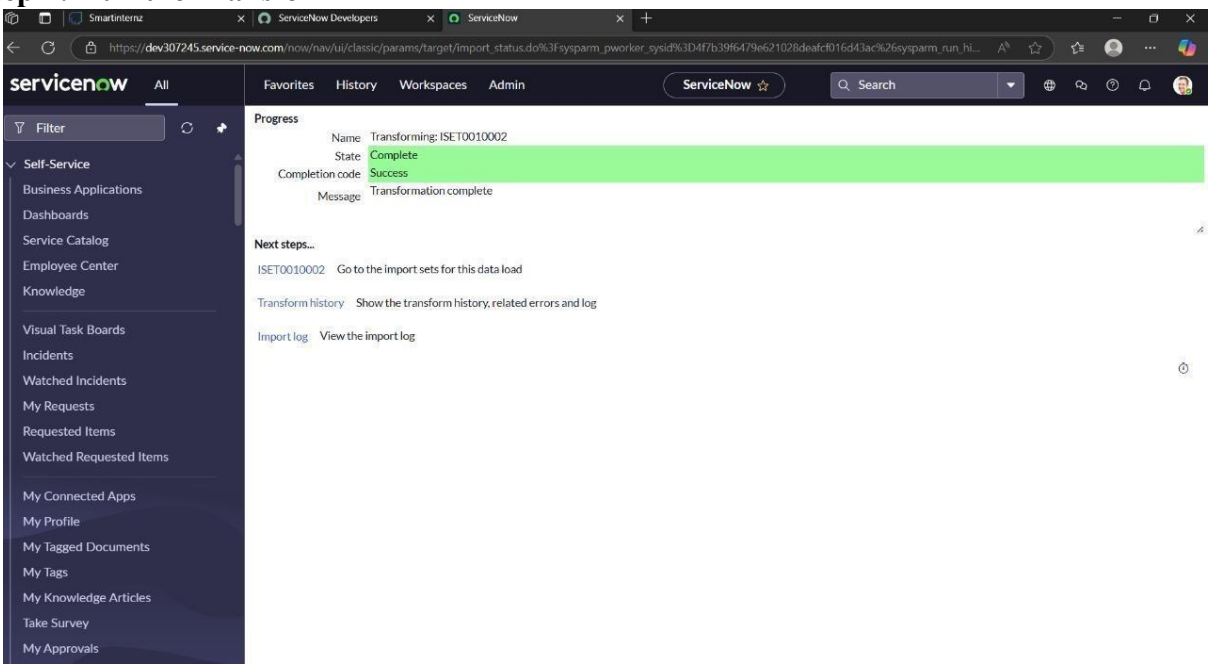


- Go to System Import Sets > Create Transform Map.

Choose the Import Set Table as the source and your target table (e.g., sys_user) as the destination.

- Map source fields to target fields.

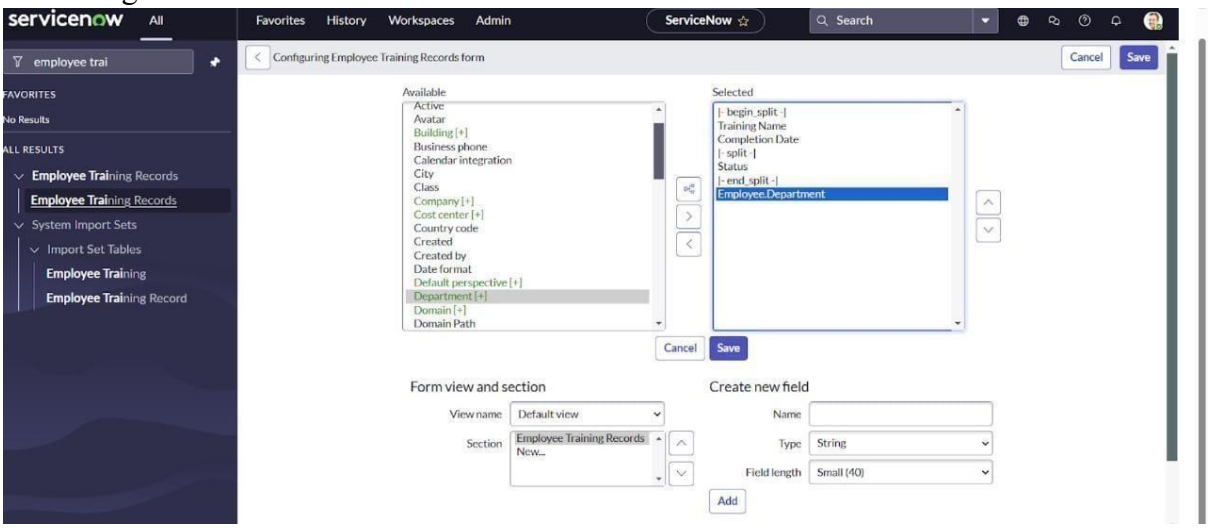
Step 4: Run the Transform



- Go to the import set and click Transform.
- Data will be moved from the import set into the actual ServiceNow table.

Using Dot-Walking to Access Employee Department Information:

Dot-walking is a method in ServiceNow to access fields in related tables.



Example:

If you're accessing a user (sys_user) record and want to get the department name:

user.department.name

- user: sys_user record
- department: reference field to cmn_department
- name: the name of the department Use Case in a Script or Report: **Java script** var user = gs.getUser();

var dept = user.getRecord().

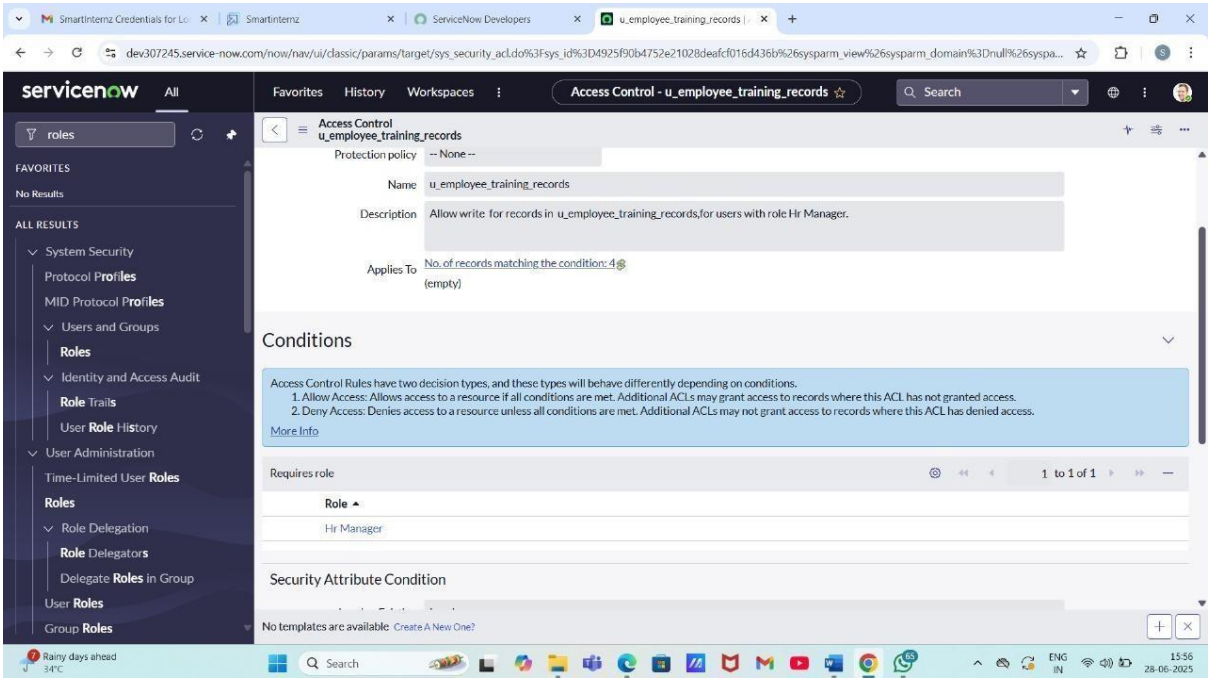
getValue('department.name'); gs.info ("Department: " +

dept); Dot-walking also works in:

- Reports
- Email Templates
- Business Rules
- UI Policies

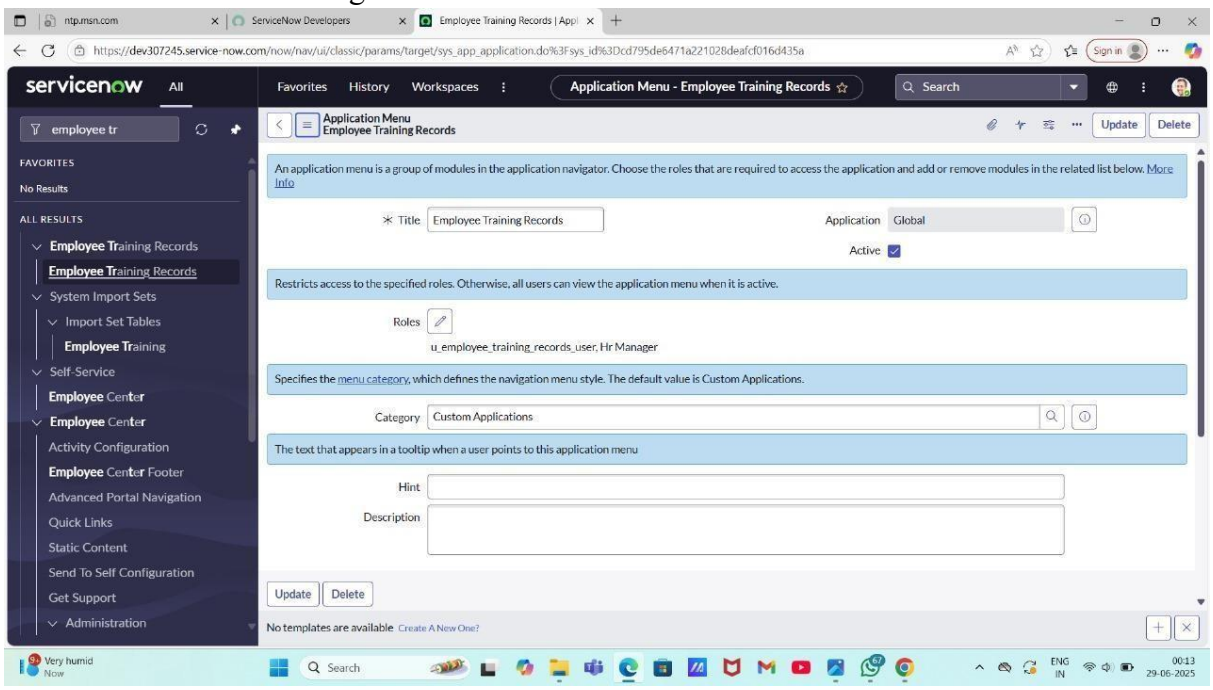
Access Control List (ACL):

Created new ACL

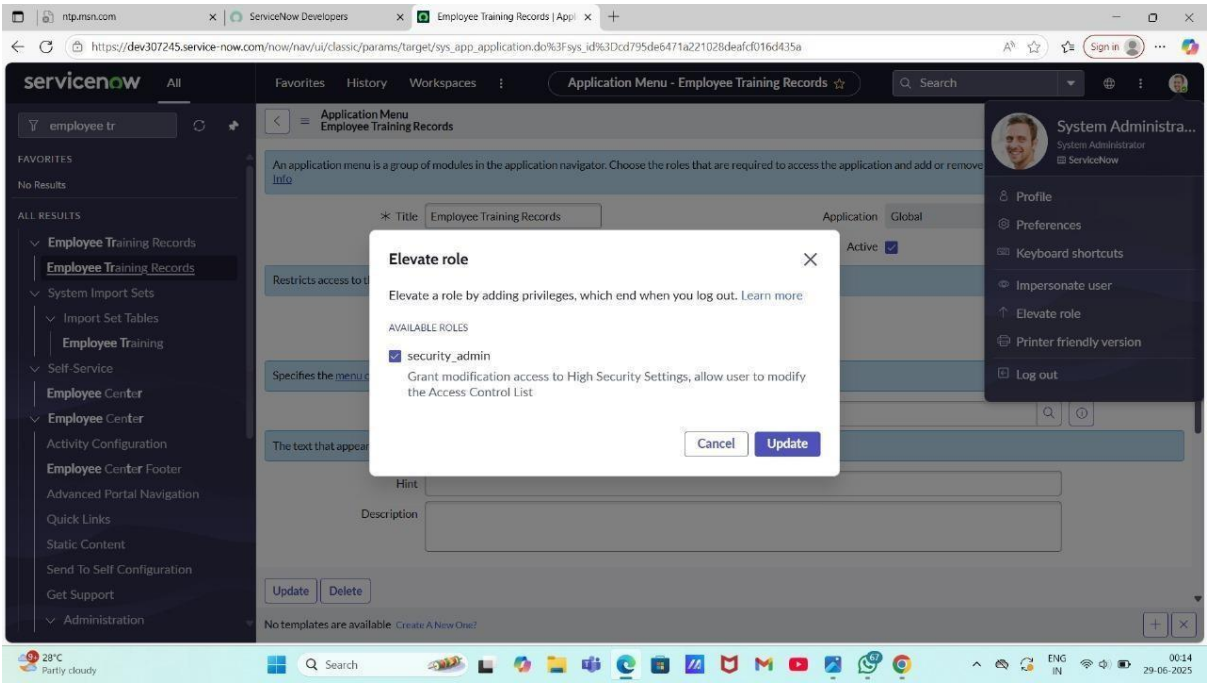


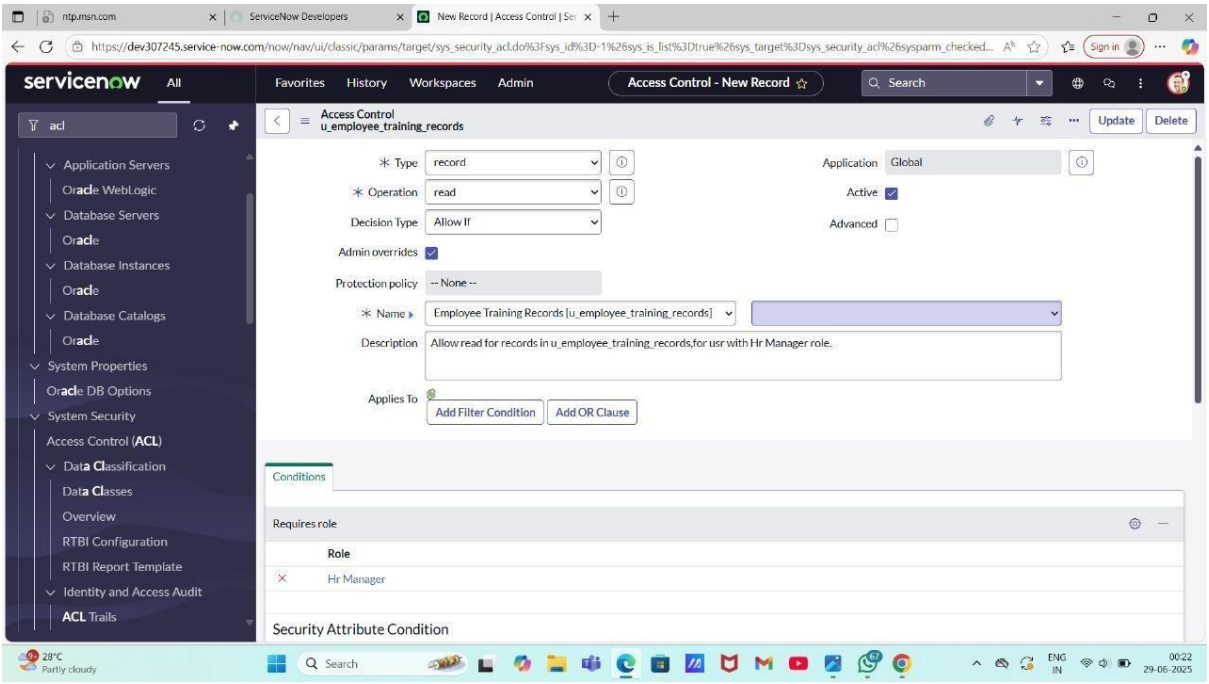
Roles in ServiceNow:

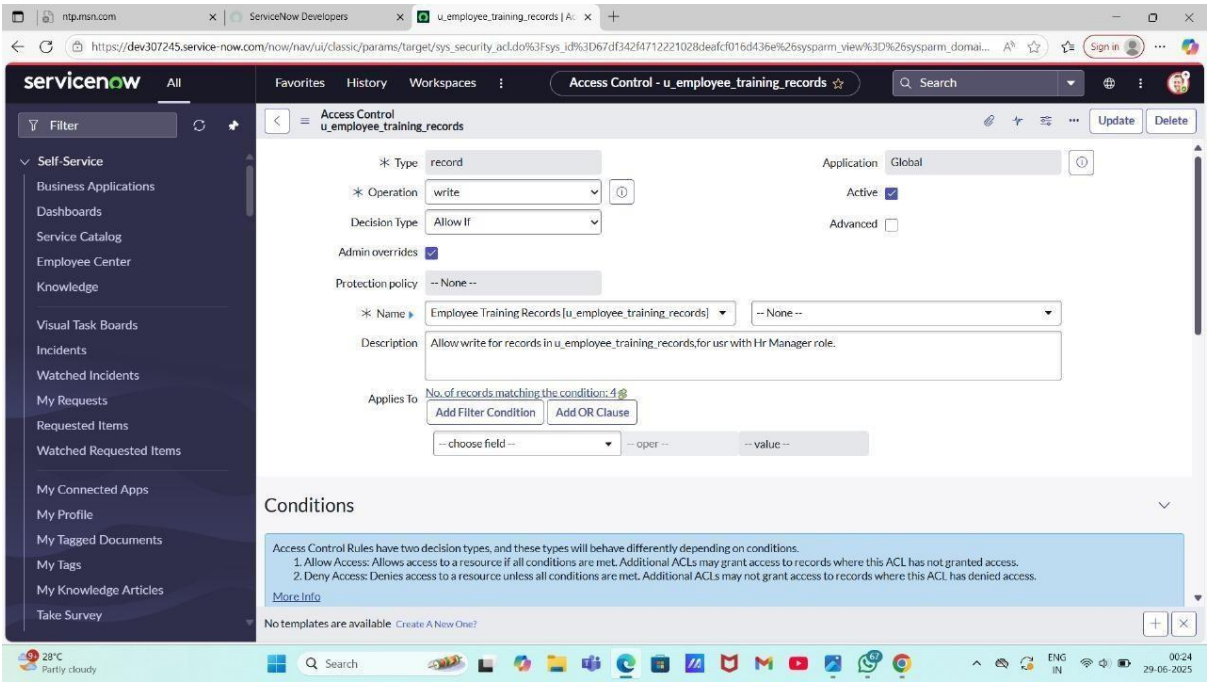
Created a new role HR Manager

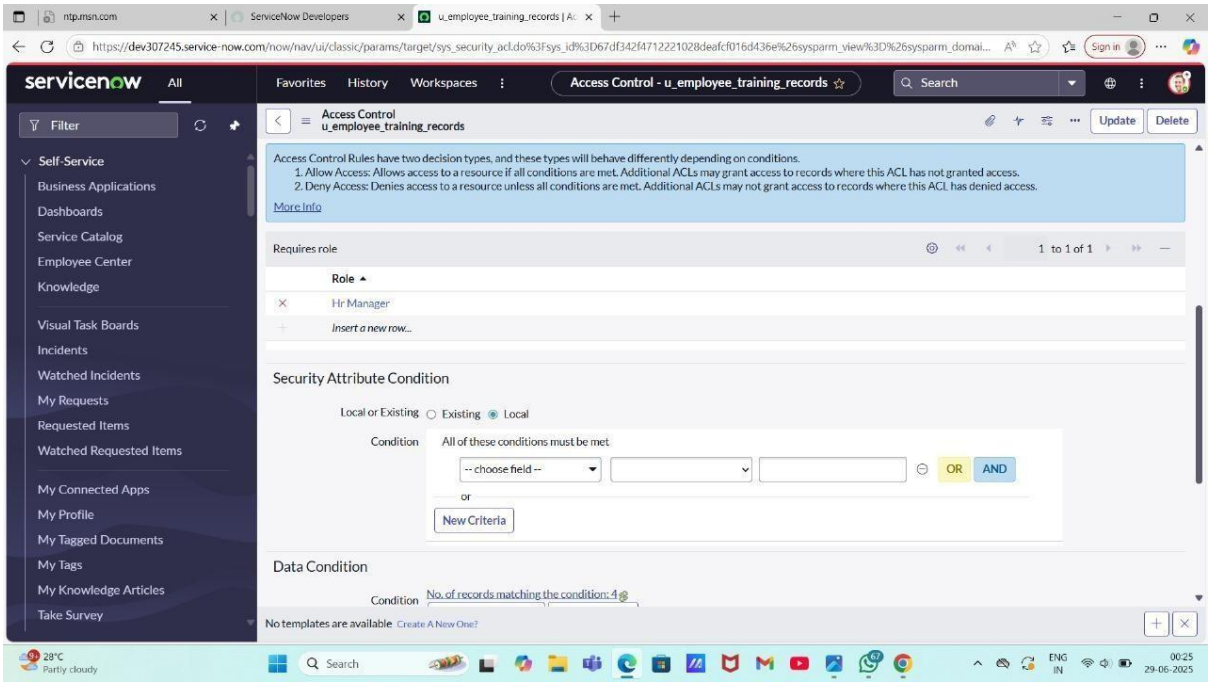


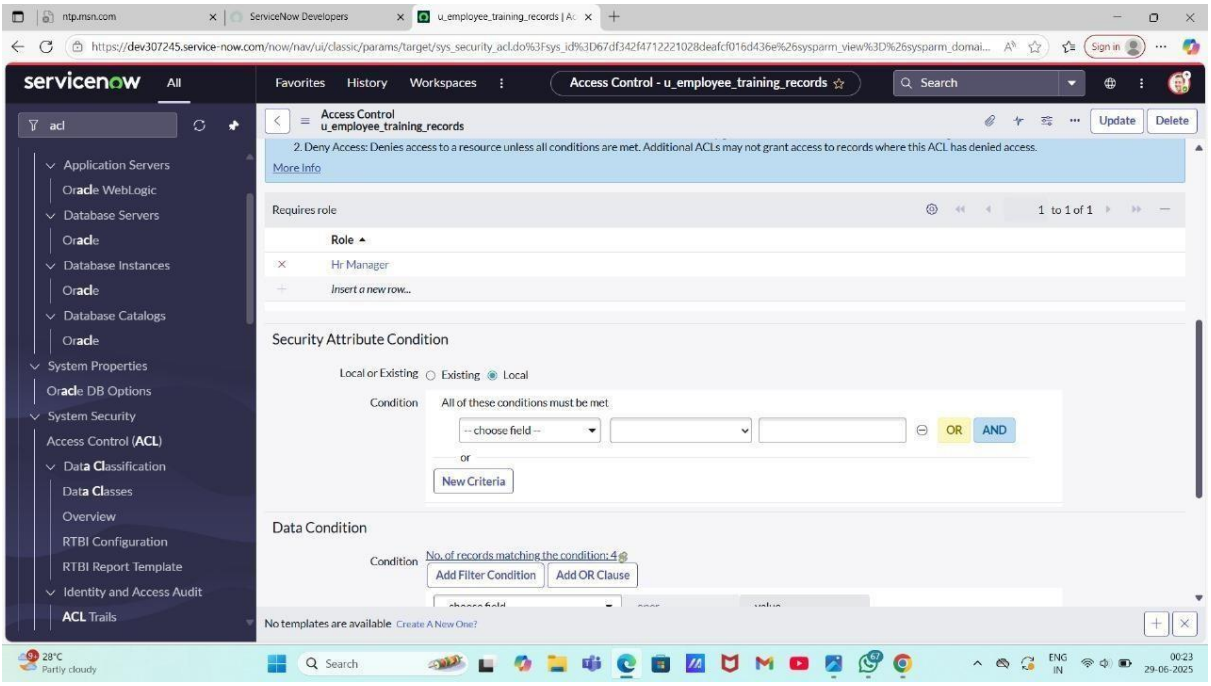
Elevate role:






servicenow
All
Favorites
History
Workspaces
Access Control - u_employee_training_records
Search
Filter
Self-Service
Business Applications
Dashboards
Service Catalog
Employee Center
Knowledge
Visual Task Boards
Incidents
Watched Incidents
My Requests
Requested Items
Watched Requested Items
My Connected Apps
My Profile
My Tagged Documents
My Tags
My Knowledge Articles
Take Survey
Access Control
u_employee_training_records
Update
Delete
Type
record
Application
Global
Operation
write
Active
Decision Type
Allow If
Advanced
Admin overrides
Protection policy
-- None --
Name
Employee Training Records [u_employee_training_records]
-- None --
Description
Allow write for records in u_employee_training_records,for usr with Hr Manager role.
Applies To
No. of records matching the condition: 4
Add Filter Condition
Add OR Clause
-- choose field --
-- oper --
-- value --
Conditions
Access Control Rules have two decision types, and these types will behave differently depending on conditions.
1. Allow Access: Allows access to a resource if all conditions are met. Additional ACLs may grant access to records where this ACL has not granted access.
2. Deny Access: Denies access to a resource unless all conditions are met. Additional ACLs may not grant access to records where this ACL has denied access.
More Info
No templates are available
Create A New One?


servicenow
All
Favorites
History
Workspaces
Access Control - u_employee_training_records
Search
Filter
Self-Service
Business Applications
Dashboards
Service Catalog
Employee Center
Knowledge
Visual Task Boards
Incidents
Watched Incidents
My Requests
Requested Items
Watched Requested Items
My Connected Apps
My Profile
My Tagged Documents
My Tags
My Knowledge Articles
Take Survey
Access Control
u_employee_training_records
Update
Delete
Access Control Rules have two decision types, and these types will behave differently depending on conditions.
1. Allow Access: Allows access to a resource if all conditions are met. Additional ACLs may grant access to records where this ACL has not granted access.
2. Deny Access: Denies access to a resource unless all conditions are met. Additional ACLs may not grant access to records where this ACL has denied access.
More Info
Requires role
1 to 1 of 1
Role
Hr Manager
Insert a new row...
Security Attribute Condition
Local or Existing
Existing
Local
Condition
All of these conditions must be met
-- choose field --
OR
AND
or
New Criteria
Data Condition
Condition
No. of records matching the condition: 4
No templates are available
Create A New One?



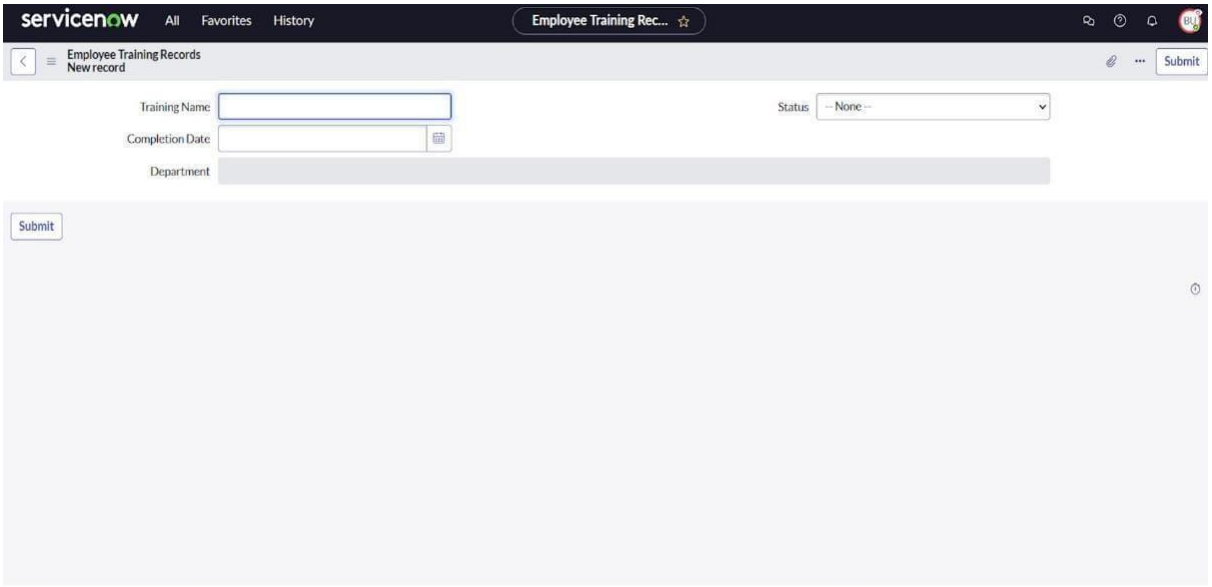
Results:

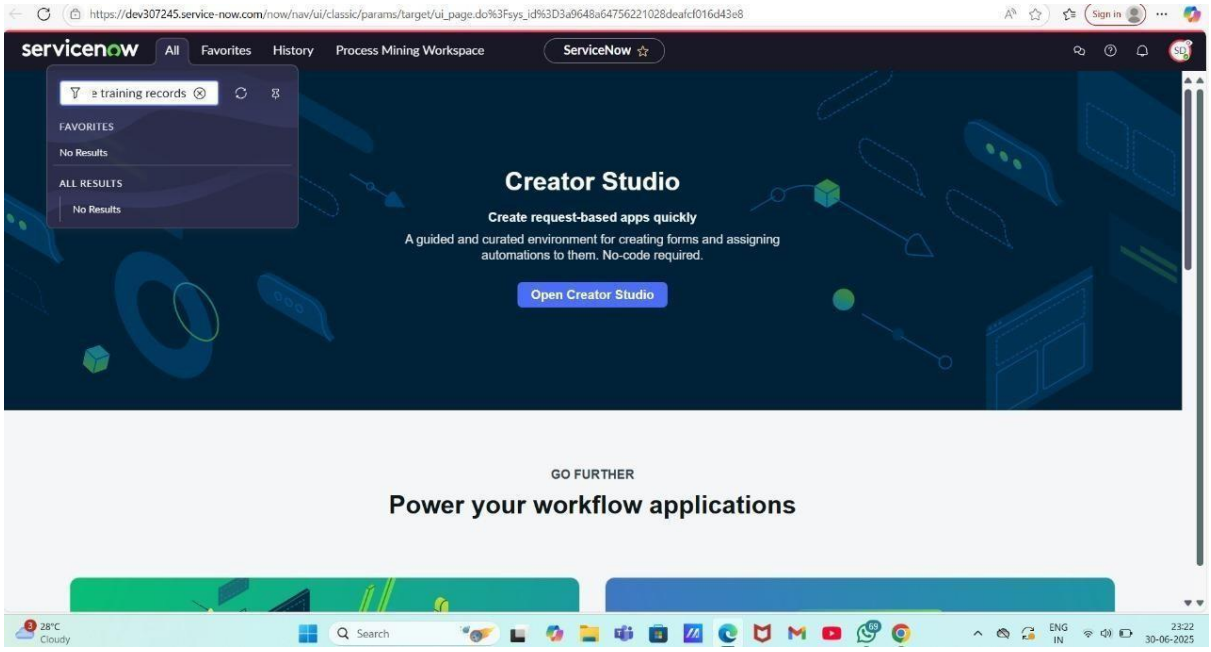
After importing and securing data:

- Data is structured in tables like sys_user, cmn_department.
- Using dot-walking, you can easily reference related data fields.
- ACLs ensure that only authorized users can see or edit sensitive data.
- Roles control what users can do, from viewing reports to importing data.

You can verify successful import by:

- Viewing records in the target table.
- Creating reports to visualize user and department info.□Checking logs for transform errors.





Conclusion:

Importing and securing data in ServiceNow ensures **data integrity, accessibility, and security**. The process involves:

- Structuring data in tables.
- Using **Import Sets** and **Transform Maps** to bring in external data.
- Leveraging **dot-walking** to navigate related records easily.
- Applying **ACLs** and **roles** to safeguard data access.

Proper data handling is critical for efficient ServiceNow operations and ensures compliance with organizational security standards.