

Access Control List (ACL) Configuration Report

1. Objective :

The objective of this task was to implement field-level security for the **task table 2** using Access Control Lists (ACLs). This ensures that only authorized users with specific roles have "write" permissions for critical data fields within the application.

2. Configuration Steps Followed :

The security rules were established using the following administrative workflow in ServiceNow:

- **System Navigation:** Navigated to **All > System Security > Access Control (ACL)**.
 - **Security Elevation:** Clicked on **Elevate Role** to gain the necessary `security_admin` privileges required to modify ACLs.
 - **ACL Initialization:** Selected **New** to create a fresh security rule.
 - **Rule Definition:**
 - **Type:** Set to **record**.
 - **Operation:** Set to **write**.
 - **Name:** Selected **task table 2 [u_task_table_2]** and specified the target field (e.g., **status**).
 - **Role Requirement:** Scrolled to the **Requires role** section and added the **team member** and **u_task_table_2_user** roles.
 - **Finalization:** Clicked **Submit** to activate the security rule.
-

3. ACL Implementation Details :

To ensure full data integrity, specific **write** ACLs were created for the following fields on the **u_task_table_2** table:

- **u_task_table_2.u_assigned_to**
- **u_task_table_2.u_due_date**

- **u_task_table_2.u_task_id**
- **u_task_table_2.u_task_name**
- **u_task_table_2.status**

4. Verification via User Impersonation

To validate the security configuration, the following test was performed:

- **Action:** Used the profile icon to **Impersonate User** as **bob p.**
- **Navigation:** Accessed the **task table 2** through the application menu bar.
- **Observation:** Confirmed that the **status** and **comments** fields are accessible and have the correct **edit access** as defined by the ACLs.
- **Result:** The security rules are functioning correctly, restricting write access to only those users holding the designated roles.


The screenshot shows the ServiceNow interface for configuring an Access Control rule. The rule is named 'u_task_table_2.u_assigned_to' and is set to 'Global' application. The configuration details are as follows:

- Type:** record
- Operation:** write
- Decision Type:** Allow If
- Admin overrides:** ☒
- Protection policy:** -- None --
- Name:** u_task_table_2.u_assigned_to
- Description:** Allow write for u_assigned_to in u_task_table_2, for users with roles (u_task_table_2.user, team member).
- Applies To:** (empty)
- Advanced:** ☐
- Active:** ☒

Below the configuration details, there is a 'Conditions' section. Under 'Requires role', the roles 'u_task_table_2.user' and 'team member' are listed. The 'Security Attribute Condition' section is currently empty.

Access Controls

Actions on selected rows...

	Name ▲	Decision Type	Operation	Type	Active	Updated by	Updated
	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<div><input type="checkbox"/> 0</div>	u_task_table_2	Allow If	create	record	true	admin	2026-02-10 00:54:09
	u_task_table_2	Allow If	write	record	true	admin	2026-02-10 00:54:10
	u_task_table_2	Allow If	delete	record	true	admin	2026-02-10 00:54:10
	u_task_table_2	Allow If	read	record	true	admin	2026-02-10 00:54:09
	u_task_table_2.u_assigned_to	Allow If	write	record	true	admin	2026-02-10 22:22:00
	u_task_table_2.u_due_date	Allow If	write	record	true	admin	2026-02-10 22:20:55
	u_task_table_2.u_status	Allow If	write	record	true	admin	2026-02-10 22:16:31
	u_task_table_2.u_task_id	Allow If	write	record	true	admin	2026-02-10 22:23:15
	u_task_table_2.u_task_name	Allow If	write	record	true	admin	2026-02-10 22:24:08
	VA Channel Integration ACL	Allow If	execute	REST_Endpoint	true	admin	2023-04-05 00:28:13
	VA Designer Config	Allow If	execute	REST_Endpoint	true	admin	2024-05-22 12:09:23
	VoCallbackPropertyUtil	Allow If	execute	client_callable_script_include	true	admin	2022-05-09 01:51:24
	Valid employee profile user	Allow If	execute	REST_Endpoint	true	admin	2024-06-12 13:17:06
	ValidateAlternatePortal	Allow If	execute	client_callable_script_include	true	admin	2024-03-06 16:53:36
	ValidateAppVersionAjax	Allow If	execute	client_callable_script_include	true	admin	2021-10-05 03:00:09
	ValidateEnvironment	Allow If	execute	client_callable_script_include	true	admin	2022-01-06 09:58:13
	ValidateSACIsPortalRecord	Allow If	execute	client_callable_script_include	true	admin	2023-06-16 07:21:47
	ValidateTextIndexFields	Allow If	execute	client_callable_script_include	true	admin	2017-11-16 23:12:51
validator_run_summary	Allow If	delete	record	true	system	2025-12-03 18:12:46	
validator_run_summary	Allow If	create	record	true	system	2025-12-03 18:12:46	