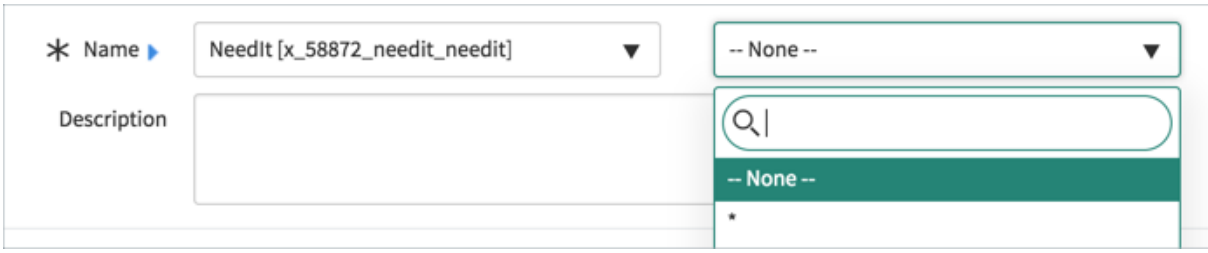
ServiceNow Application Developer

Securing Applications Against Unauthorized Users > To * or Not to *

The *Name* field in an Access Control specifies the table records to protect and a field to protect. The field list has a *--None--* option and a *** option.



- ***--None--***: Grant access to records and all fields in the records.
- ***:** Grant access to all fields where there is no field-specific Access Control.

At first glance, *--None--* and *** seem to grant the same thing: access to all fields on a record. To tell the difference in behavior, review how *--None--* and *** work together and with other Access Controls in a demonstration.

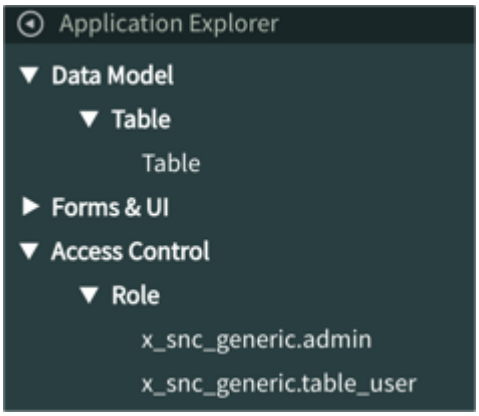
Demonstration Setup

The examples use an application called *Generic* that has a single table called *Table*. *Table* has five columns: *Field 1*, *Field 2*, *Field 3*, *Field 4*, and *Field 5*.

The application has two roles:

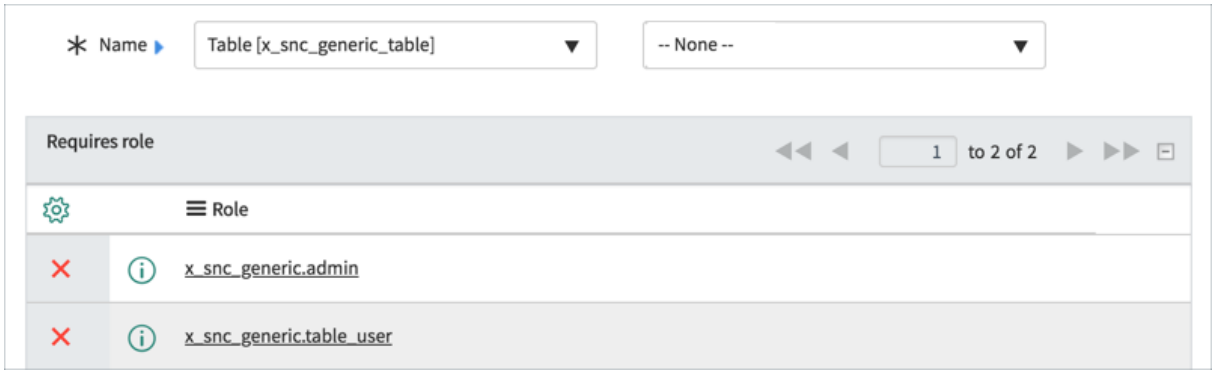
- *x_58872_generic.admin*, assigned to *Fred Luddy*

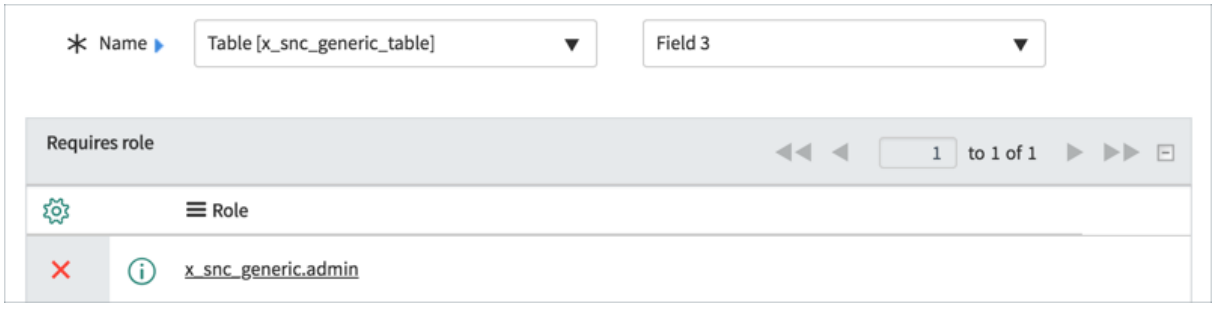
- *x_58872_generic.table_user*, assigned to *Beth Anglin*



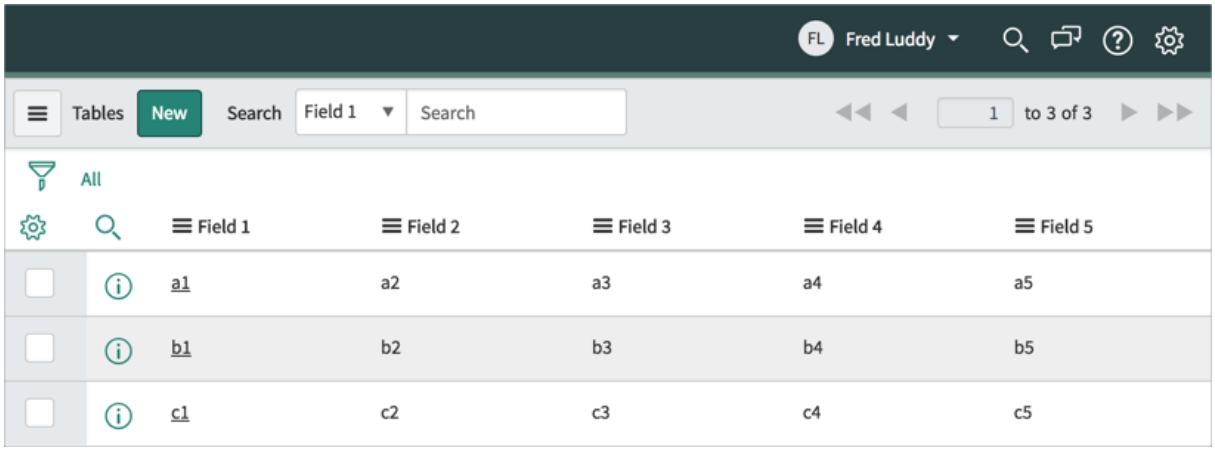
--None-- without *

Examine the two read Access Controls. Pay attention to the field value and the roles. The images have been edited to show only the pertinent parts of the Access Control.

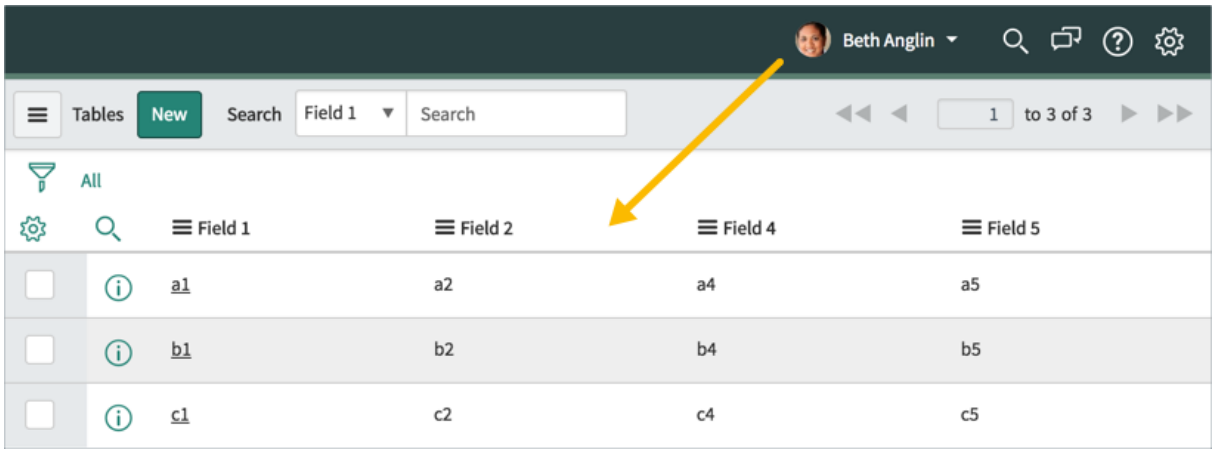




Using this Access Control List (ACL), Fred can see:



Using this ACL, Beth can see:

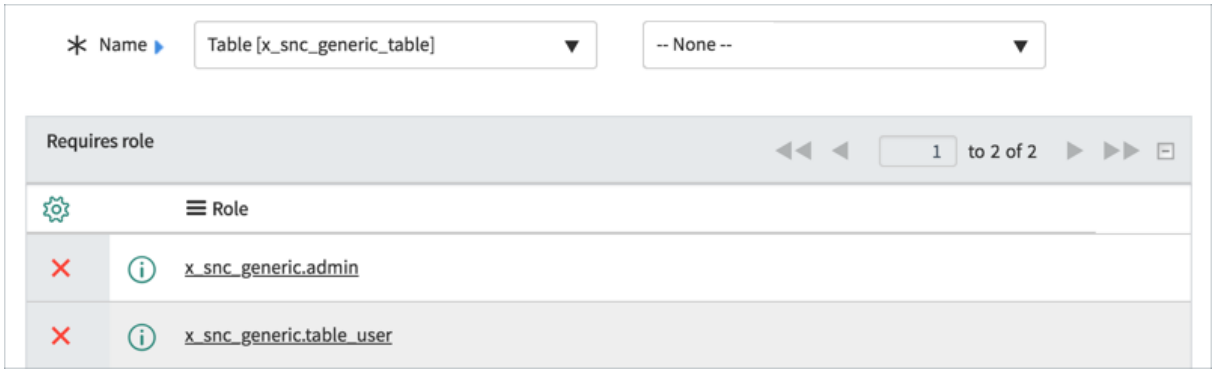


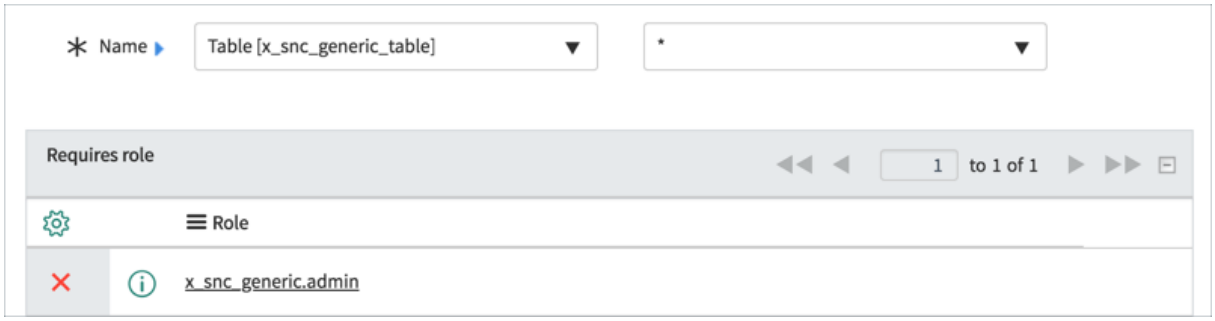
How does this work?

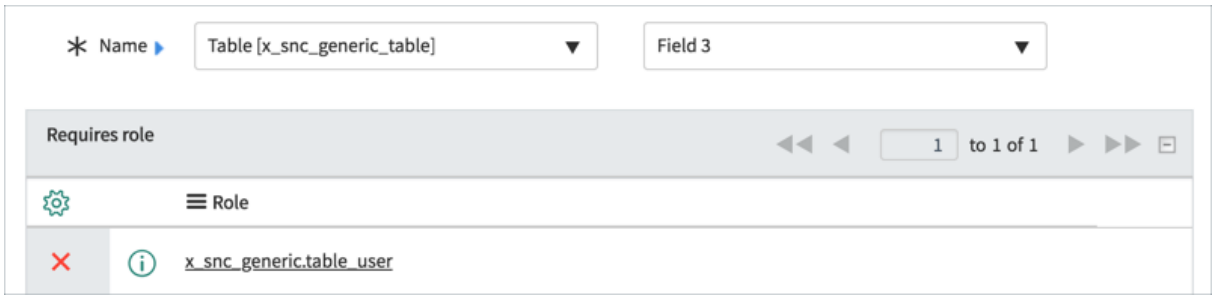
- The *None* Access Control granted all rows and all fields to both Fred and Beth.
- The *Field 3* Access Control granted *Field 3* access to Fred. Giving *Field 3* explicitly to Fred removed *Field 3* access from Beth *even though she was granted Field 3 access by the None Access Control*.

--None-- with *

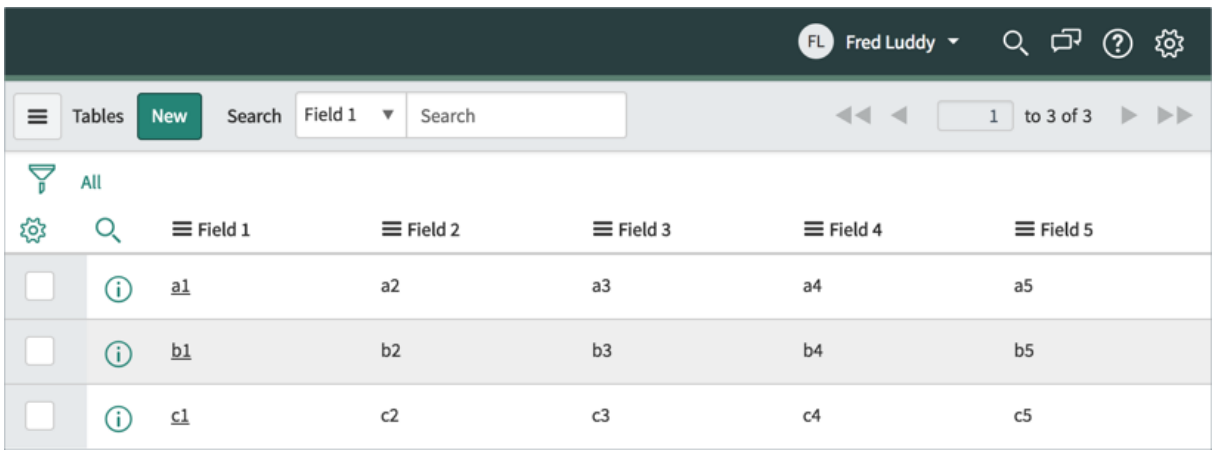
Examine the three read Access Controls. Pay attention to the field value and the roles. The images have been edited to show only the pertinent parts of the Access Control.



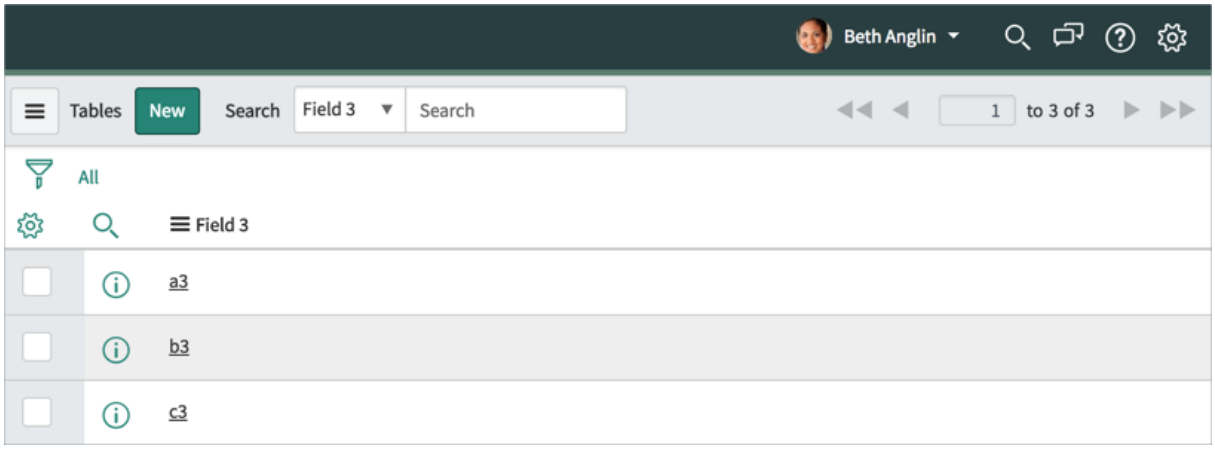




Using this ACL, Fred can see:



Using this ACL, Beth can see:



How does this work?

- The *None* Access Control granted all rows and all fields to both Fred and Beth.
- The * Access Control granted all rows and all fields to Fred. It seems redundant to have this Access Control because Fred already had access to all rows and all fields. The purpose of this Access Control is to deny access to all other roles, *even roles granted permission by the None Access Control*.
- The *Field 3* Access Control explicitly gives Beth access to *Field 3* even though Beth was denied access to *Field 3* by the * Access Control. Field-specific Access Controls take precedence over * Access Controls.

Conclusions

- When creating * Access Controls, also create a *None* Access Control because only None grants access to records.
- When writing an ACL that mostly grants access, use only *None*.
- When writing an ACL that mostly denies access, use *None* and *.