

# ServiceNow Application Developer

## Securing Applications Against Unauthorized Users > Debugging Access Controls

To enable Access Control debugging, use the Application Navigator in the main ServiceNow browser window (not Studio) to open **System Security > Debugging > Debug Security Rules**. The *Debug Security Rules* module runs a script that enables writing all Access Control debugging information to the bottom of each page in the content frame.

Only admin users have access to the *Debug Security Rules* module. In most cases, Access Controls need to be debugged for users other than the admin user. After enabling *Debug Security Rules* as an admin user, impersonate a user to test their access.

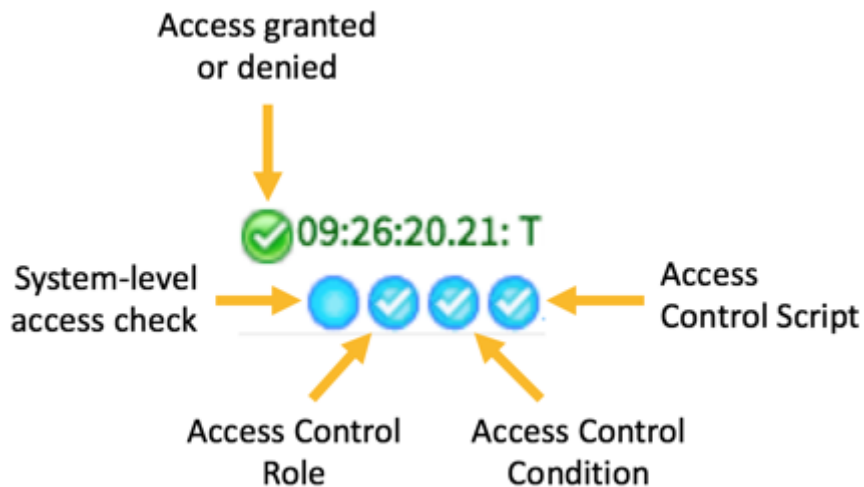
In this example, *Beth Anglin* is denied access to *Field 3* on Table in the *Generic* application:



The first row states the overall evaluation of the Access Control: Grant or Deny. The Access Control is a read Access Control for *Field 3*.

The second row shows the evaluation of the table-level Access Control followed by the field-level Access Control. In this case both the table-level and field-level Access Controls are shown to make it clear which Access Control denied access.

The debugging information is shown in order of evaluation:



Examine both the color code and the symbols to determine debugging results.

- **Green:** Access granted
- **Red:** Access denied
- **Blue:** The rule did not have to be re-evaluated because the result is already in the cache
- **Gray:** Not evaluated, typically because part of the rule has already denied access
- **Check mark:** Passed
- **X:** Failed

The system-level access check is not part of an Access Control. It runs before Access Controls are evaluated and looks for system/runtime reasons why a user should or should not be granted access. For example, Delegated Development grants developers permission to create only certain types of application files. Fred might be able to create Business Rules but Beth cannot. Permission to create application files in a Delegated Development environment is not controlled by Access Controls and is determined at runtime by a system-level access check.

Look again at the *Field 3* Access Control for Beth. Her access to *Field 3* was denied by the role on the field-level Access Control even though the table-level Access Control granted access. The condition and script on the field-level Access Control were not evaluated because the role denied access.




To disable Access Control debugging use the Application Navigator in the main ServiceNow browser window to open **System Security > Debugging > Stop Debugging**. If you have impersonated a user, impersonate the *System Administrator* to disable Access Controls.

**DEVELOPER TIP:** The *Admin overrides* option in Access Control configuration grants access to the admin user even if the admin user does not meet the requirements of the Access Control. Use caution when testing Access Controls as the admin user as the results may not be indicative of the Access Control's behavior.

## Debug a Single Field's Access Controls

To debug the Access Controls for a single field rather than the entire content frame, with *Debug Security Rules* enabled, open the table's form.

A *Debug* icon (  ) appears next to each field. Hover over the *Debug* icon to see how many Access Control messages there are for the field. Click the **Debug** icon to see the Access Controls for that field. This strategy, obviously, cannot be used to debug fields that are hidden by Access Controls.

