



STEALTHtip #4

How-to Tip: Create Business Rules to Analyze Data Collected by StealthAUDIT.

1. Start by creating a query-job to collect information you wish to analyze.
2. Run the job to collect the desired information.
3. Select the Configure\analysis node and click "Create Analysis."
4. Provide an appropriate name and description to describe the rule you are creating.
5. Select 'Business Rules' from the Analysis Module drop-down list.
6. The "Enable execution of this task when this job is run" checkbox can be used to disable execution of the rule. This is useful for troubleshooting when there are multiple rules, or when the job is being queried against a target host where this condition may not apply.
7. Click Configure Analysis to open the Edit Rules dialog box.
8. Select the Table drop down to select the data table containing the data for which you will create your condition(s). In addition to selecting tables from the current job's data table, it is also possible to use data from any table that is found in the StealthAUDIT database. By default only SA tables are presented, however if you check the "Show All tables" checkbox, all tables will be presented. (Tables that are not written by StealthAUDIT, or that do not contain an "SA_" prefix.)
9. Once you have selected the target table, the next step is to create a condition that will trigger an action. The condition you are building here is a "Transact SQL" Where clause. Click Add condition to open the "Edit Conditions" dialog box. Select a column from the table, an operator, and the value that you wish to test for, then click OK. The condition is placed in the conditions window. If you are conversant with T-SQL, you can type condition directly into the conditions window rather than using the provided condition editor. It is good practice to use the "test SQL Syntax" button to ensure your T-SQL is valid. Multiple conditions may be applied by selecting an appropriate Joining Rule. EXAMPLE: "MaxPasswordAge" <> 'N/A' AND "MaxPasswordAge" = 0.
10. It is important to note that if the configured conditions represent exceptions. When the condition is true it will trigger the action that is to be configured in the Action section of the dialog. Click Add to select an action to configure. The only action currently available is a "Scorecard" Action.
11. The Scorecard action configuration dialog is presented. This dialog presents the following fields for configuration:
 - a. Action Name: A simple name to refer to this scorecard item. Example: Maximum Password Age.
 - b. Description: Describes the scorecard Item. Example: The Maximum Password Age is set to 0.
 - c. Category: When creating multiple conditions, it may be useful to create categories for grouping like items. This provides a pivot point that can be leveraged when creating reports. Example: Password Policy.
 - d. Index: This represents an index number that can be used to reference this rule to a standard, or as a simple numbering scheme. Example: This Password Policy Item Maps to CIS standard 1.1.1.3.
 - e. Score: A score can be provided that could also be mapped to a well known standard, or based on your own internal requirements. The score can be used to quantify the overall compliance posture based on the overall score of all items. The Score should also be set in relation to the severity of this condition, i.e. The higher the severity, the higher the score.



STEALTHtip #4

- f.** Severity: The severity could be mapped to the severity settings of well known standards or based on internally defined severity standards. Example: Critical, Important, Moderate, Low or Hi Medium Low, etc.
 - g.** Knowledge: This field allows you to provide information that describes the method or methods to be used for correcting the deficiency. Useful information also includes URLs to MS KBs or other vendor articles, or internal links to prepared documents, etc.
 - h.** Property 1, and Property 2: The drop downs permit you to select the column item that is being tested within your defined condition. This allows you to select the interrogated value so it may be referenced in the Scorecard record.
- 12.** Click OK to commit the Scorecard record, and click OK again to commit the rules dialog. When you run the query job, a scorecard table will be created in the StealthAUDIT database containing all scorecard records that were triggered by each of your defined conditions. The scorecard table therefore represents all items found on each queried host where the conditions were found to be “TRUE” or “In Exception” to the conditions you defined. You can use StealthAUDIT’s built in reporting features to configure, and automatically publish scorecard reports to a report audience.
- 13.** Test the rule to ensure it functions as expected by running the query job against a small sampling of query-hosts.

For additional troubleshooting tips and information email support@stealthbits.com.

