Change policy security checks

Security checks assess the vulnerability of specific Windows OS and SQL Server objects based on your criteria. After security checks are configured and your SQL Server instances are assigned to the policy, you can view the results on the Security Overview window and on the Risk Assessment Report.

In addition, you can configure email notifications to be sent out when a particular risk level has been passed. For more information, see Configure Email Settings.

When security checks are setup for your policies, it is important that accurate criteria is entered. For example, a typo in the Windows Operating System Version metric criteria could cause erroneous findings.

Available fields

The **Security Checks** of the **Policy Properties** tab allows you to update the following fields:

Criteria

Some security checks allow you to configure the assessment criteria, such as specific user accounts, stored procedures, or the login audit level. Text entered in this field must use the exact spelling of the object being checked. Use the option **Edit** and a new window opens where you can specify multiple criteria items (one per line). To delete any previous specified criteria, click the corresponding item, and then **Remove.**

If criteria for security checks is entered incorrectly, it may fail to correctly display its finding in the Report Card.

Some security check criteria support using the percent wildcard character (%) to specify objects whose names apply a naming convention. For example, to specify all users whose logon starts with sql, enter the following syntax: `domain\sql%`.

External Cross Reference

Allows you to cross reference a security vulnerability included in your report to a number or name contained in an external security standard.

Report Text

The text entered in this field appears on your policy reports. For example, the Protocols security check includes the report text "Are unexpected Protocols enabled?". When unexpected protocols are enabled, the report displays the SQL Server instances where the risk is encountered.

Risk Level

Allows you to set the severity of the risk posed by this finding. The risk level is important because it reflects how severe or risky a particular security finding is for your environment, allowing you to further customize security checks to meet your exact auditing needs. For example, finding an enabled Guest account on one instance may be a high risk, but on another instance it may be a low risk. The risk level also determines where the corresponding security finding appears on the policy or assessment Report Card and whether or not email notifications will be sent.