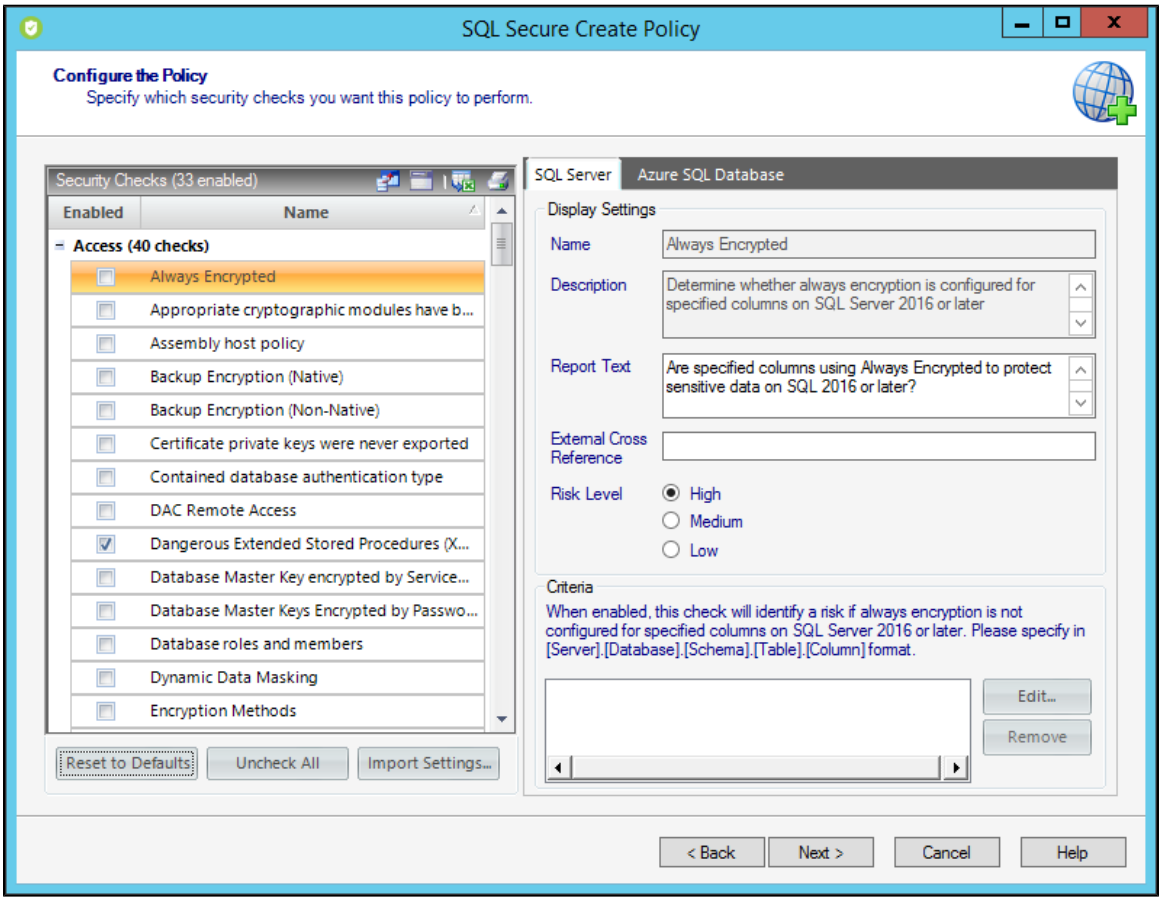
Select security checks

The **Configure the Policy** section allows you the define the security checks this policy should use to evaluate your audit data.

Security checks assess the vulnerability of specific Windows OS, SQL Server objects, and Azure environments based on your criteria. Each policy has a predefined number of enabled security checks, however the user can remove or add security checks in this section.



The list of security checks is separated by the following groups according to the type of evaluation they perform:

- Access Security Checks
- Auditing Security Checks
- Configuration Security Checks
- Data Integrity Security Checks
- Login Security Checks
- Permissions Security Checks
- Surface Area Security Checks

Define criteria on the Security Checks that require it; otherwise, you cannot go back nor continue with the creation of a policy.

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.

After security checks are configured and your SQL Server instances are assigned to the policy, you can view the assessment results on the **Security Summary** view 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 Notifications.

Configure check settings

When you select security checks, you can configure the check settings on the right side of this window. Below the **Name** and **Description** of the respective security check you can find the following fields:

Report Text

This text displays on your policy reports, such as the **Risk Assessment** report. By default, SQL Secure provides a report text question for each security check. You can edit this question to better fit it to your audit reporting needs.

For example, the Protocols security check includes the report text "Are unexpected Protocols enabled?". If unexpected protocols are enabled, the report displays this question as well as the SQL Server instances on which the vulnerability was found.

External Cross Reference

This field allows you to cross reference a security vulnerability included in your report to a number or name contained in an external security standard, such as a specific HIPAA regulation.

Risk Level

This option allows you to set the severity of the risk for this security check 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.

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%` .

Even though you are creating a policy "from scratch", SQL Secure has enabled several common security checks you may need, to help you configure your policy quickly and easily. These security checks are also included in the default **All Servers** policy. You can add, edit, or disable any security check as needed.

By default, the **All Servers** policy enforces the Idera Level 2 - Balanced template. For more information, see how policy templates can help you achieve your SQL Server security goals.

The **Import Settings** option allows you to import security check definitions from either a built-in policy template or an existing policy whose settings you previously exported.

Click **Next** to go to the Assign SQL Servers to the Policy section.