Use policy templates to harden your security model

You can use the IDERA and industry standard policy templates built in to IDERA SQL Secure to further harden your SQL Server security model. By creating policies from these templates, you can enforce consistent security settings across your enterprise and proactively assess when and where vulnerabilities exist. You can also customize new policies based on these templates to further address your specific security needs.

Consider using policy templates when you:

- Must enforce an industry standard such as CIS, SRR, HIPAA, or PCI
- Need a more robust and comprehensive assessment of your security model than what Microsoft Best Practices can offer

Available templates

CIS for SQL Server 2000

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2000.

CIS for SQL Server 2005

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2005.

CIS for SQL Server 2008

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2008.

CIS for SQL Server 2008 R2

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2008 R2.

CIS for SQL Server 2012

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2012.

CIS for SQL Server 2014

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2014.

CIS for SQL Server 2016

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2016.

CIS for SQL Server 2017

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2017.

CIS for SQL Server 2019

Enforces security check settings derived from the Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2019.

DISA-NIST STIG for SQL Server 2012

Enforces security check settings derived from the Defense Information Systems Agency (DISA) National Institute of Standars and technology (NIST) - SQL Server 2012 STIG.

DISA-NIST STIG for SQL Server 2014

Enforces security check settings derived from the Defense Information Systems Agency (DISA) National Institute of Standars and technology (NIST) - SQL Server 2014 Instance STIG.

European Union General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data.

HIPAA Guidelines for SQL Server

Leverages the Health Insurance Portability and Accountability Act (HIPAA) guideline as well as the Department of Defense Database Security Technical Implementation Guide (STIG). These guidelines target conditions that undermine the integrity of security, contribute to inefficient security operations and administration, or may lead to interruption of production operations for health information that resides on Microsoft SQL Server.

IDERA Level 1 - Basic Protection

Establishes a realistic entry-level baseline for SQL Server and Azure SQL databases whose third-party applications do not interface with the World Wide Web. This template enforces MSBPA guidelines as well as additional security checks for logins, permissions, and other vulnerabilities.

IDERA Level 2 - Balanced Protection

Establishes a more secure baseline for production SQL Server and Azure SQL databases that are configured to support external connectivity while protecting against the most popular intrusion tactics. This template combines the CIS and MSBPA guidelines as well as additional security checks for permissions, configurations, and other vulnerabilities.

IDERA Level 3 - Strong Protection

Enables the maximum security checks for mission-critical SQL Server and Azure SQL databases that support Web-based, B2B, B2C, or external clients to prevent unauthorized disclosure and data tampering. This template combines IDERA Level 2 and the DISA guidelines with SRR regulations. Also included are additional security checks for auditing, permissions, surface area configurations, and other vulnerabilities.

MS Best Practices Analyzer

Enforces security check settings derived from the Microsoft SQL Server 2005 Best Practices Analyzer Security Recommendations.

NERC Critical Infrastructure Protection

Enforces security check settings derived from the North American Electric Reliability Corporation (NERC) Critical Infrastructure protection

PCI-DSS Guidelines for SQL Server

Enforces security check settings derived from the Payment Card Industry (PCI) v3.0 guideline. This guideline leverages the SQL Server Database Security Readiness Review (SRR) and targets conditions that undermine the integrity of security, contribute to ineficient security operations and administration, or may lead to interruption of production operations.

SNAC for SQL 2000

Enforces security check settings derived from the Guide to the Secure Configuration and Administration of Microsoft SQL Server 2000, Network Applications Team of the Systems and Network Attack Center (SNAC).

SOX Section 404

Enforces security check settings derived from the Sarbanes-Oxley (SOX) Section 404

SRR Checklist for SQL Server 2000

Enforces security check settings derived from the DISA for a security readiness review (SRR) of a Microsoft SQL Server RDBMS installed in a Windows NT or Windows 2000 host operation system environment.

SRR Checklist for SQL Server 2005 or later

Enforces security check settings derived from the Database Security Readiness Review (SRR) of a Microsoft SQL Server RDBMS. This SRR targets conditions the undermine the integrity of security, contribute to inefficient security operations and administration, and may lead to interruption of production operations. This version can also be applied to SQL Server 2008 and later.

Select a template

Use the industry standard policy templates, such as the CIS for SQL Server 2005 template, when your environment needs to meet the exact security criteria defined by that regulatory organization. However, your environment may contain SQL Server instances that only need to follow your corporate security policies. In those cases, you can create new or enhance existing corporate policies based on the built-in IDERA security level templates.

The IDERA Level 1, Level 2, and Level 3 templates allow you to mature your SQL Server security model over time, graduating from a solid baseline to an intermediate level to a more advanced and hardened approach. Each level is based on regulatory models and industry best-practices as well as additional security checks that identify vulnerabilities other standards do not address. The default **All Servers** policy enforces the IDERA Level 2 - Balanced template.

Use the following table to determine which IDERA security level template fits your current security needs and how your environment fits into the overall security maturation model.

IDERA Level	Maturation Level	Security Level	Types of SQL Server Instances	Types of Business	Regulatory Model	Unique Security Checks
1 - Basic Protection	Beginner	Baseline	Test, development, and low-risk production instances	Services internal groups by hosting data for third-party applications and does not require connections to external clients	MSBPA plus additional checks	• SA account has blank password • Any SQL Server login has blank password • Public server role has been granted permissions
2 - Balanced Protection	Intermediate	Medium	Average production instances	Services internal and external groups that require external connectivity to hosted data	CIS and MSBPA plus additional checks	• Sysadmins own trustworthy databases • Public server role has been granted permissions • File permissions on executables are not acceptable • SQL logins have weak passwords
3 - Strong Protection	Advanced	High	Mission-critical, sensitive, and high-risk production instances	Services internal and external groups by hosting data for Web-based, B2B, B2C, or external clients	CIS, MSBPA, and SRR, plus additional checks and auditing	• Required administrative accounts do not exist • xp_cmdshell proxy account exists • SA account is not using password policy • Public database role has unacceptable permissions • SSIS database role and stored procedure permissions • OS version is at acceptable level