

Product requirements

You can easily and quickly install IDERA SQL Secure on any computer that meets or exceeds the following hardware, software, and permission requirements. Before installing SQL Secure, also review the [product components and architecture](#) as well as [how the product works](#).

Typical requirements

A typical install sets up all SQL Secure components on the same computer. The following table lists the requirements for a typical installation.

Hardware/software	Requirement
CPU	2.0 GHz or higher
Memory	2 GB
64-bit Operating System	- Windows 11 - Windows 10 - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016 - Windows 2019 - Windows Server 2022 Plus: .Net framework 4.8 - MDAC 2.8 or later
Microsoft SQL Server for Repository	Supports all editions except SQL Server Express for the following versions: - SQL Server 2012 - SQL Server 2014 - SQL Server 2016 - SQL Server 2017 (Windows) - SQL Server 2019 (Windows) - SQL Server 2022 - SQL Server on Azure VM - SQL Server on Amazon EC2
Microsoft SQL Server for audited instances	- SQL Server 2012 SP1 - SQL Server 2014 - SQL Server 2016 - SQL Server 2017 (Windows) - SQL Server 2019 (Windows) - SQL Server 2022 - Azure SQL Database - SQL Server on Azure VM - Azure SQL Database - SQL Server on Amazon EC2 - Amazon RDS for SQL Server
Browser for online Help	- Internet Explorer 11.x+ - Microsoft Edge - Google Chrome - Mozilla Firefox - Safari  Current versions plus three previous versions of these browsers support SQL Secure.



Latest SQL Secure version no longer supports SQL Server 2000, SQL Server 2005 and SQL Server 2008R2 install Secure on a SQL instance with a different collation.

Console requirements

A console-only installation installs the SQL Secure Console. The console-only installation assumes that a full installation has already been completed on another machine. The following table lists all the requirements for a console-only installation.

Hardware/software	Requirement
CPU	2.0 GHz or higher
Memory	2 GB
32-bit or 64-bit Operating System	- Windows 11 - Windows 10 - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016 - Windows 2019 - Windows Server 2022 Plus: .Net framework 4.8 - MDAC 2.8 or later
Browser for online Help	Internet Explorer 9.0 or later

SQL Server Versions and Editions

SQL Secure runs on various Cloud Virtual Machines running Microsoft Windows Server and Microsoft SQL Server.

SQL Secure monitors different SQL Server versions installed on-premise or on cloud platforms.

SQL Versions Windows Only	On-Premise	Microsoft Azure VM (IaaS)	Amazon EC2 (IaaS)	Microsoft Azure SQL Database (PaaS)	Amazon RDS (PaaS)
2012 SP1	X	X	X		X
2016	X	X	X		X
2017	X	X	X		X
2019	X	X	X		X
Azure SQL Database V12				X	

Collector permission requirements

The following requirements are necessary for the SQL Secure Collector to access the SQL Server instances you want to audit. During install, you can input credentials for a Windows user account or SQL Server login.

Type	Requirement
Windows permissions	A Windows user account that has local administrator permissions.
SQL Server privileges	A Windows user account that is a member of the sysadmin fixed server role on the SQL Server instance.

Port requirements

SQL Secure uses the default ports opened by the Windows operating system for local and remote communications. To learn about Windows port assignments, see [Article 832017](#) on the Microsoft Support site. To better understand how port assignments work when Windows Firewall has been configured, see "[Connecting through Windows Firewall](#)" on the MSDN site.

Type	Requirement
SQL Server Object Permissions and configuration collection	Port 1433 (or the configured SQL instance port for the audited instance)
Windows file system and registry permissions collection	Port 135 (RPC connectivity)

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)