

IDEERA

SQL Secure

Version 4.1



Table of Contents

1	Take full control of SQL Server permissions.....	6
2	Release notes	7
2.1	New features and fixed issues	8
2.2	Known issues.....	9
3	Get started.....	10
3.1	Upgrade to this release.....	11
3.2	Welcome to IDERA SQL Secure.....	16
3.3	Installation and deployment.....	20
3.4	Configure your deployment	35
4	Explore Security Settings.....	79
4.1	Analyzing permissions	79
4.2	Experiencing irregularities when searching user and object permissions.....	80
4.3	Explore object permissions	81
4.4	Explore role permissions	84
4.5	Explore user permissions.....	88
4.6	View all audited servers	96
4.7	View single server summary	98
4.8	View snapshot summary.....	100
4.9	View snapshot properties.....	109
4.10	Decommissioned SQL Servers.....	110
5	Assess Your Security Model	111
5.1	Information available at the enterprise level	111
5.2	Information available the server level	111
5.3	Analyze enterprise security	112
5.4	Analyze server security	118
5.5	Define policies for custom assessments.....	123
5.6	Policy assessments	161
5.7	Compare assessments.....	178
5.8	Select audit data for assessment	182
6	Report on SQL Server Security	183

6.1	How to use the Deploy Reports wizard	184
6.2	Use the Console to generate reports	187
6.3	Use Reporting Services to generate reports	191
7	Manage SQL Secure	193
7.1	View the SQL Secure Repository status	194
7.2	Manage SQL Secure logins.....	196
7.3	Manage policies.....	202
7.4	View SQL Secure activity.....	204
7.5	Manage server group tags	206
7.6	Bulk Email Notifications	207
8	Manage your license	210
8.1	SQL Secure licensing with Azure SQL Database	211
9	Edit audited SQL Server properties.....	214
9.1	Change general properties	215
9.2	Change connection credentials.....	217
9.3	Define folders	219
9.4	Change audit filters.....	220
9.5	Change snapshot schedule.....	222
9.6	Change email notification	224
9.7	Change which policies audit this instance.....	225
10	Monitor Azure Databases.....	226
10.1	Register Azure SQL Database in SQL Secure	226
11	Monitor Amazon Databases.....	227
11.1	Manage Microsoft Active Directory with Amazon AWS.....	227
11.2	Setting up a VPN Tunnel to connect to Amazon instances	227
11.3	Connecting to your existing AD infrastructure	227
11.4	Authorizing Inbound Traffic for Your AWS security group	228
11.5	Permissions to RDS for SQL Server log in	228
12	Configure email settings.....	230
13	SQL Secure Collector Job Keys.....	231
13.1	Configure the Data Collector Job Keys:	231
14	Delete a Data Snapshot	232

15	Troubleshooting WMI connectivity issues	233
15.1	Resolve WMI Issues using WbemTest.....	233
16	Select audited SQL Server to explore data	236
17	Troubleshooting guide/ Advanced solutions	237
17.1	Active Directory Permissions Exceptions.....	238
17.2	Domain Services Permissions Exceptions	255
17.3	File Permission Exceptions.....	257
17.4	Registry Permissions Exceptions.....	259

[Go to Version 3.4.x](#)

[Go to Version 3.3.x](#)

[Go to Version 3.2.x](#)

[Go to Version 3.1.x](#)

1 Take full control of SQL Server permissions

- Identify existing vulnerabilities in your SQL Server, Azure, and Amazon environments.
- Harden security policies across SQL Server, Azure, and Amazon SQL databases.
- Rank security levels with the security report card.
- Analyze and report on user permissions across database objects.
- Comply with audits using customizable templates for PCI, HIPAA and more.

2 Release notes

IDERA SQL Secure is a security analysis solution that identifies SQL Server security violations and ensures security policies are enforced. Find out who has access to what and identify each user's effective rights across all SQL Server objects. Alert on violations of your corporate policies, monitor changes made to security settings, and provide security audit reports as well as recommendations on how to improve your security model.

To get a quick glimpse into the newest features, fixed issues, and known issues in this release of IDERA SQL Secure, review the following sections of the Release Notes:

- [Learn about key new features in this release](#)
- [Review issues fixed by this release](#)
- [Review previous features and fixed issues](#)
- [See known issues](#)

2.1 New features and fixed issues

IDERA SQL Secure provides the following new features and fixed issues.

2.1.1 4.0 New features

- The [SQL Secure Data Collector Job Keys](#) allow you to manage snapshot collection jobs. Use this option to throttle the collector jobs so that they do not overload the SQL Server instance.
- SQL Secure supports TLS 1.2 to send email requests to SMTP.

2.1.2 4.0 Fixed issues

- SQL Secure enhanced the assessment's loading time; they no longer take several minutes to display information.
- Snapshot collection on Availability Group Nodes no longer generates a file permissions warning message.
- Snapshot collection completes successfully for a log-shipped database.
- The number of Stored Procedures in the Stored Procedures Encrypted details of the security check no longer differs from the number of Stored Procedures in SSMS.
- SQL Secure no longer displays timeout errors while generating the Database Roles Reports.
- Renaming and disabling sa login account no longer shows a "sa Account Not Disabled" security check.
- "Public Server Role only granted default Microsoft permissions" security check shows the correct information related to Server Roles
- The Snapshot Comparison Report no longer displays server changes when no changes have been made.
- The User Permission Report works correctly with different collations set.
- SQL Secure imports hidden instances using CSV files.
- The Snapshot collection process completes successfully for imported instances using CSV files.
- The Risk Assessment Report no longer reports the sa login account incorrectly.
- SQL Secure no longer has issues with bulk email notification settings.
- Renaming the sa login in a SQL Server instance no longer generates a false warning risk level in the 'sa account is not disabled' check.
- SQL Secure enhanced the SQL Job Permission security check.

2.2 Known issues

IDERA strives to ensure our products provide quality solutions for your SQL Server needs. **If you need further assistance with any issue**, please contact Support (www.idera.com/support).

2.2.1 4.0 Known issues

- Exporting reports to PDF may generate blank spaces within the document.
- The export policy process may change the number of security checks enabled for each policy.
- Importing policies may display the following error: "This security check requires at least one criterion".
- SQL Secure displays an error message when a user with Audit Data User permissions launches the console. To fix this error message, consider granting explicit "Select" permissions to the user on the SQLSecure repository database as shown in the image below.
- When launching the application with the "Run as Administrator" option, the UAC (User Account Control) prompt shows "Unknown" for the Publisher information.
- Snapshot collection process may name the database files incorrectly.

3 Get started

Use the following checklist to guide you through the process of getting started with IDERA SQL Secure.

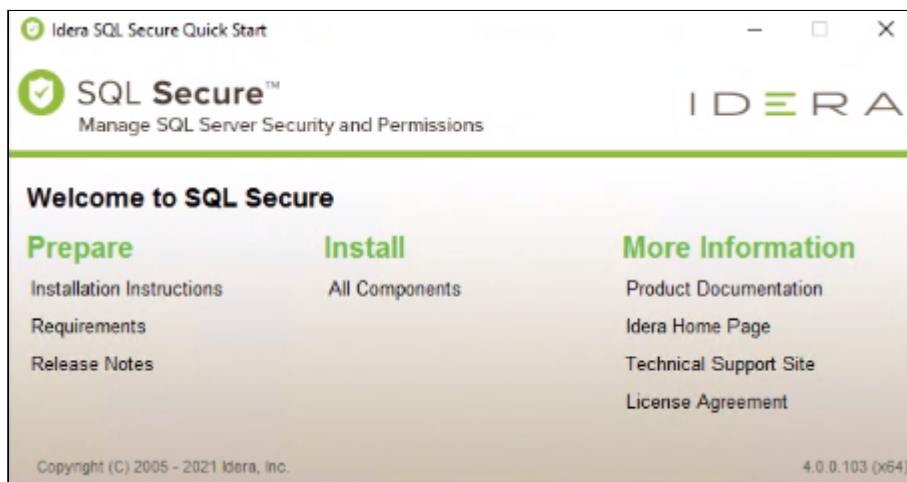
✓	Follow these steps ...
✓	Register the SQL Server instances whose security models you want to assess and audit.
✓	Configure snapshots to collect audit data from the registered instances.
✓	Find security issues using the default All Servers policy .
✓	Create custom policies to assess compliance to specific security regulations.
✓	Save assessments for policies you want to use in your audit process.
✓	Compare assessments to identify changes over time.
✓	Perform forensic analysis of your security model using the Permissions Explorer .
✓	Discover vulnerabilities using the built-in reports .

3.1 Upgrade to this release

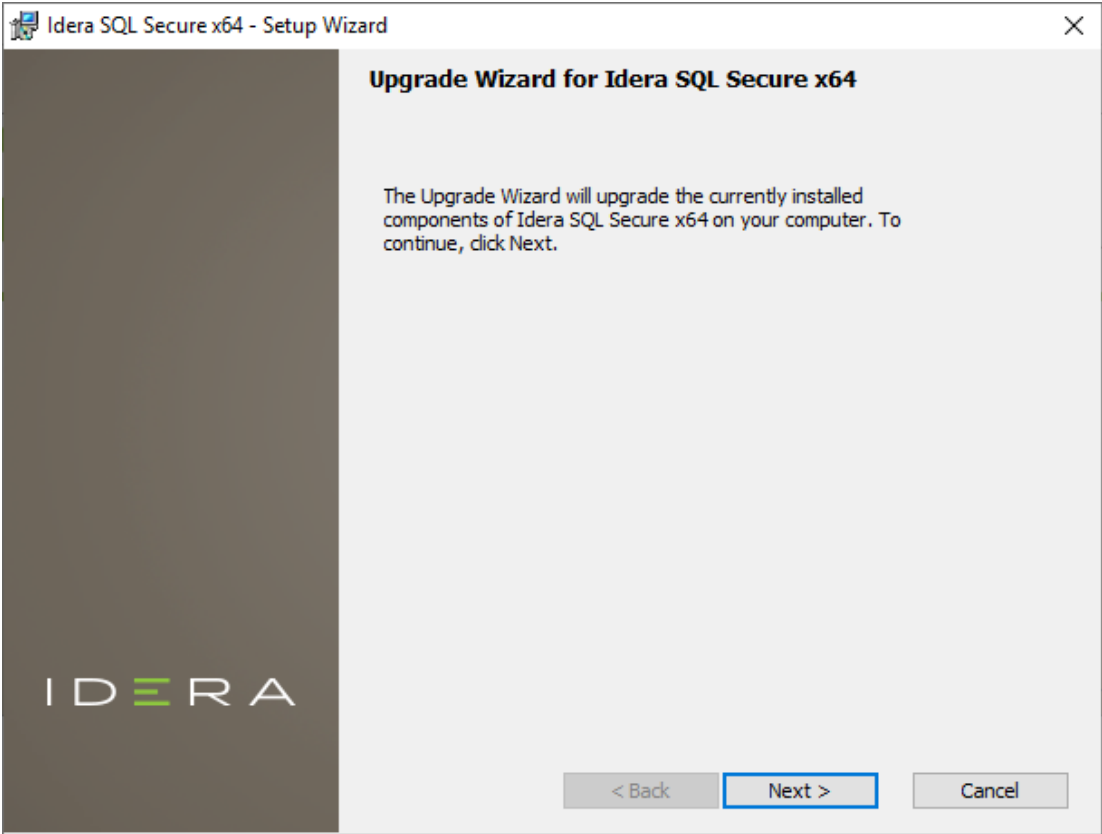
You can easily and quickly upgrade to the latest version of IDERA SQL Secure. Upgrading will not delete or alter any existing snapshots or policies. For more information about this release, see [what's new](#).

3.1.1 To upgrade to the latest version of IDERA SQL Secure:

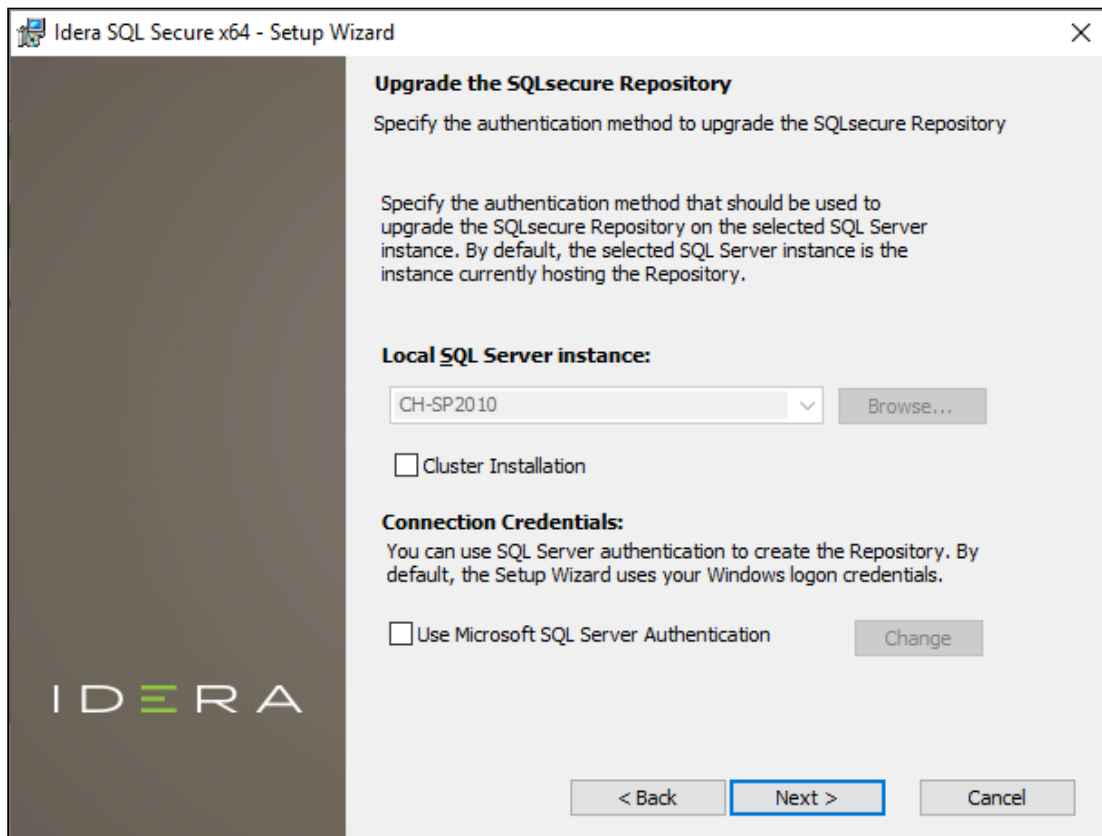
1. Use an administrator account to log onto the computer on which you previously deployed IDERA SQL Secure.
2. Close all open applications.
3. Run `Setup.exe` in the root of the installation kit.
4. Click **All Components** under Install on the **Idera SQL Secure Quick Start** window.



5. An **Upgrade Wizard** will display, click **Next** to continue.



6. On the Upgrade the SQLsecure Repository Wizard:



3.1.2 To install on a cluster:

If you are installing on a Failover Cluster, check the **Cluster Installation** checkbox.

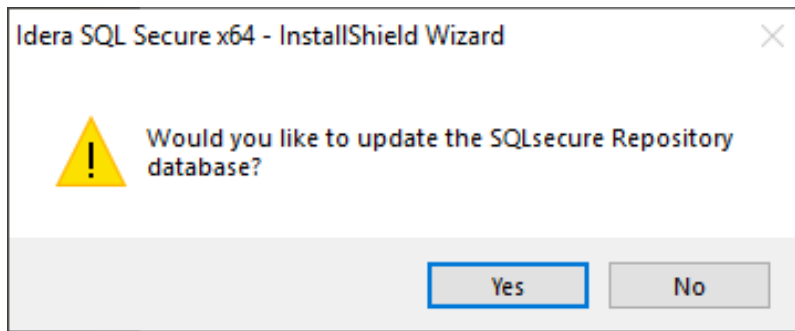
3.1.3 To specify the Connection Credentials:

By default, SQL Secure will connect to the selected SQL Server instance using the credentials of your current Windows login account. For your first install, we recommend using your current login account credentials.

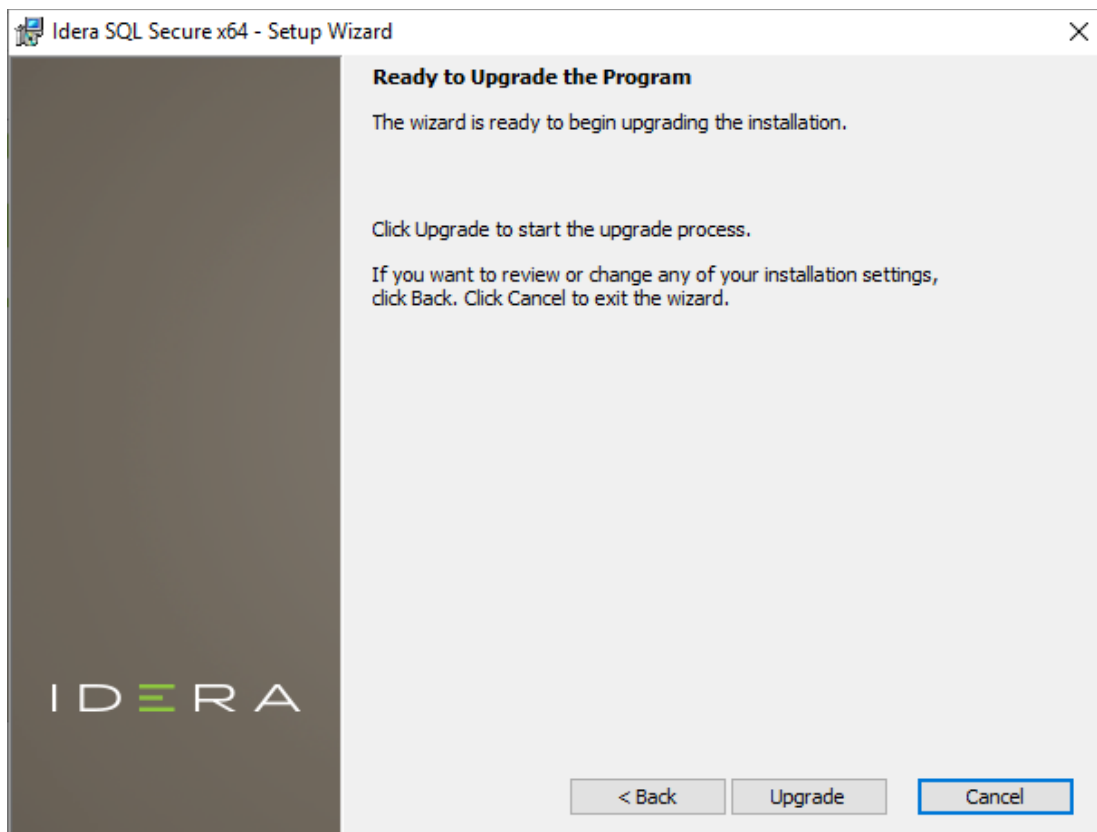
3.1.4 To use a SQL Server login:

- Click **Use Microsoft SQL Server authentication**. A new window for specifying the login credentials opens.
- Specify the credentials of the login with sysadmin privileges on that instance, and then click **OK**.
- Click **Next**.

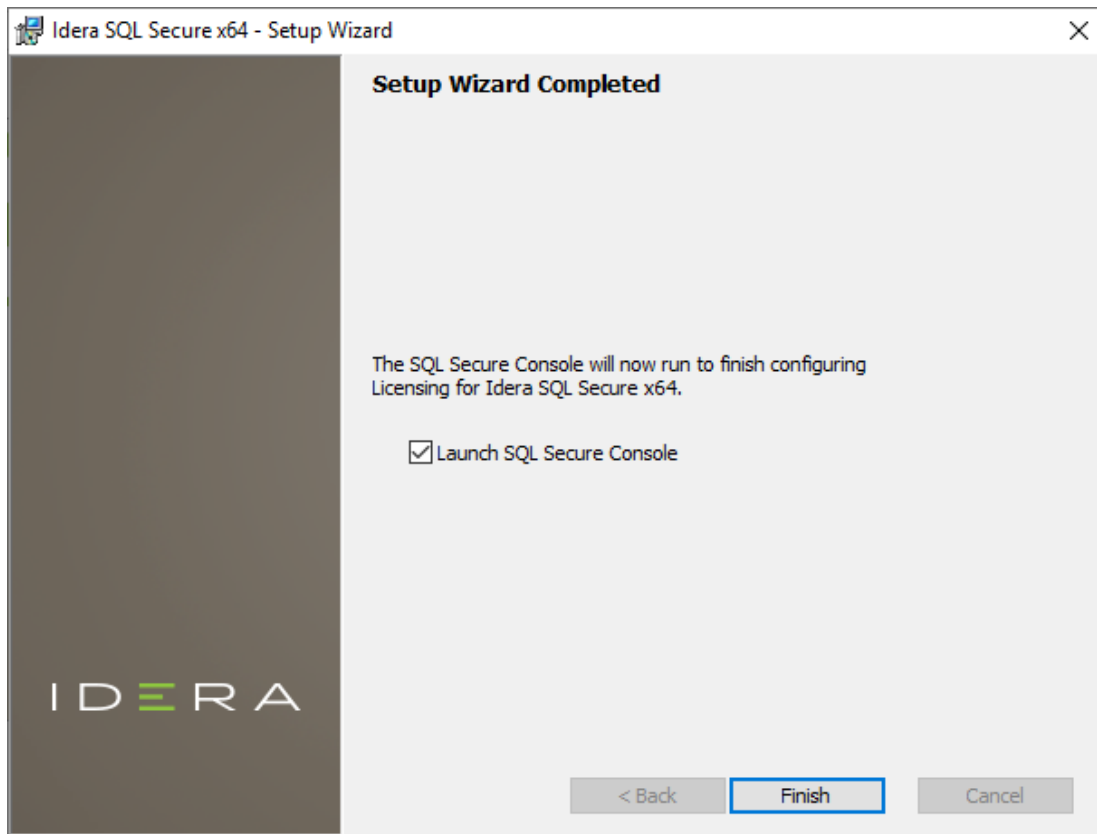
7. An update message will display, click **Yes** to continue.



8. Click **Upgrade** to start the process.



9. Check the **Launch SQL Secure Console** checkbox to run the application after the process completes. Click **Finish** to exit the IDERA SQLsecure Setup Wizard.



i **If you have previously deployed Reports**, use the [Deploy Reports wizard](#) to upgrade your deployment.

i **If your existing policies include security checks that cite OS and SQL Server versions**, you must manually update the related security checks to include the latest releases, such as SQL Server 2017.

3.2 Welcome to IDERA SQL Secure

IDERA SQL Secure identifies security holes and verifies your SQL Server security model by analyzing the effective rights for any user, on any given object or access control, across SQL Server and Active Directory.

Need help using IDERA SQL Secure? See the following sections:

- [Get started](#)
- [Assess Your Security Model](#)
- [Explore Security Settings](#)
- [Report on SQL Server Security](#)

3.2.1 What is IDERA SQL Secure?

IDERA SQL Secure discovers security vulnerabilities and user permissions for SQL Server and Cloud Hosted SQL Server databases running in Azure or Amazon. SQL Secure can identify who has access to what, monitor changes made to security settings, generate alerts and audit reports and make recommendations on how to improve your security model.

3.2.2 How SQL Secure helps

Because of the many different and complex ways to grant access to SQL Servers whether they are running in private network, or public cloud as Azure or Amazon databases – including server and database roles, Active Directory and local groups, inherited permissions, explicit grants and denies, just to name a few – it is virtually impossible to manually analyze a security model across instances or determine a user's rights on specific database objects. IDERA SQL Secure does this for you, answering the important question "Who can do what, where, and how on my SQL Servers?" SQL Secure provides a comprehensive, automated solution for analyzing, monitoring, and reporting on security access rights across database objects.

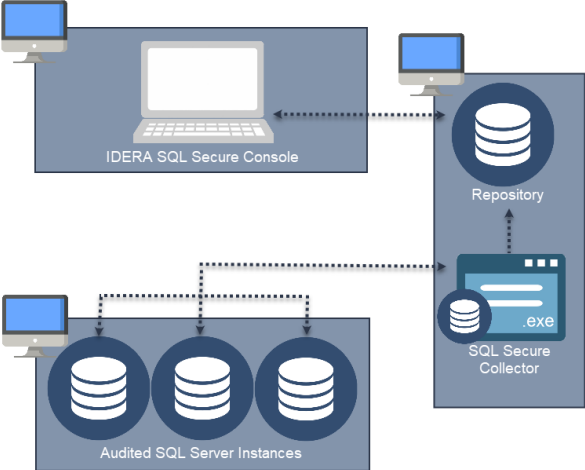
With IDERA SQL Secure, you can:

- Identify vulnerabilities and harden security across your SQL Server instances and databases hosted in your private network or a public cloud (Azure VM, Amazon EC2, Azure SQL Databases or Amazon RDS)
- Diagnose and protect against violations of your security policies and security best practices
- Analyze and manage user permissions across all database objects with our powerful security model analysis
- Create policies using customizable templates for various security level needs

3.2.3 How SQL Secure works

IDERA SQL Secure uses a Collector to gather permissions information at scheduled intervals. SQL Secure runs this executable using a SQL Server job. The Collector stores each data set as an audit snapshot in a SQL Secure Repository database. The SQL Secure Console connects to the Repository to view your permissions data.

The following diagram displays the IDERA SQL Secure workflow.



3.3 Installation and deployment

You can install and deploy IDERA SQL Secure in any sized environment.

- Learn about the [product components and architecture](#)
- Review the [product requirements](#)
- View trial [installation instructions](#)

3.3.1 Product components and architecture

IDERA SQL Secure provides a robust, easy-to-use SQL Server audit and reporting solution. Behind a friendly user interface, SQL Secure offers a unique architecture that is both flexible and extremely powerful. SQL Secure fits your environment, no matter how simple or complex.

Product components

SQL Secure Console

The SQL Secure Console component is the interface you use to set up and manage your SQL Secure configuration, view and search your audit snapshots for user and object permissions, and generate reports to display the audit information that is most important to you.

SQL Secure Repository

The SQL Secure Repository is where your audit snapshot information and SQL Secure configuration information is stored. You can schedule routine grooming that automatically delete snapshots older than a specified date.

SQL Secure Collector

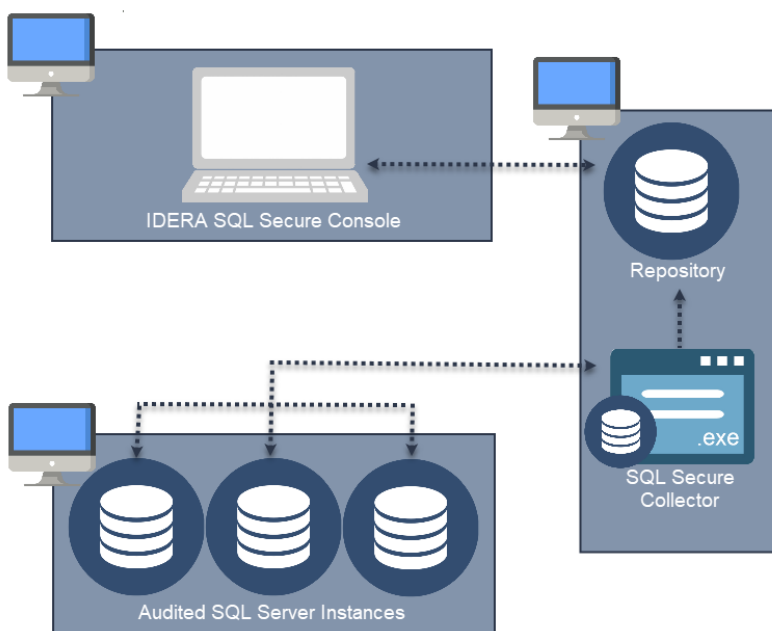
The SQL Secure Collector gathers SQL Server permission information from your audited SQL Server instances (using your filter criteria) and stores the information in the SQL Secure Repository database.

Audited SQL Server Instances

The audited SQL Server instances are SQL Server instances that have been registered with SQL Secure. These SQL Server instances are audited periodically at the dates and times you schedule. The resulting data is stored in the SQL Secure Repository and displayed in the SQL Secure Console as a snapshot of your SQL Server security model.

Product architecture

The following diagram illustrates the components of the SQL Secure architecture.



3.3.2 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	<ul style="list-style-type: none"> • Windows 8 • Windows 10 • Windows Server 2008 SP2 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 <p>Plus:</p> <ul style="list-style-type: none"> • .NET Framework 4.5 SP1 or later • MDAC 2.8 or later
Microsoft SQL Server for Repository	<p>Supports all editions except SQL Server Express for the following versions:</p> <ul style="list-style-type: none"> • SQL Server 2008 R2 • SQL Server 2012 SP1 • SQL Server 2014 • SQL Server 2016 • SQL Server 2017 • SQL Server 2019 • SQL Server on Azure VM • SQL Server on Amazon EC2

Hardware/software	Requirement
Microsoft SQL Server for audited instances	<ul style="list-style-type: none"> • SQL Server 2008 R2 • SQL Server 2012 SP1 • SQL Server 2014 • SQL Server 2016 • SQL Server 2017 • SQL Server 2019 • Azure SQL Database • SQL Server on Azure VM • SQL Server on Amazon EC2 • Amazon RDS for SQL Server
Browser for online Help	<ul style="list-style-type: none"> • Internet Explorer 11.0+ • Google Chrome • Mozilla Firefox • Microsoft Edge • Safari

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	<ul style="list-style-type: none"> • Windows 8 • Windows 10 • Windows Server 2008 SP2+ • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 Plus: <ul style="list-style-type: none"> • .NET Framework 4.6
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)
2000	X				
2005	X	X			
2008 R2	X	X	X		X
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)

3.3.3 Ensure FIPS compliance

You can use IDERA SQL Secure to audit and assess your SQL Server security in environments where Federal Information Processing Standard (FIPS) compliance is required.

For more information about FIPS compliance, see the corresponding [Microsoft TechNet Web article](https://technet.microsoft.com) (technet.microsoft.com) and [Microsoft Knowledge Base Article #811833](http://support.microsoft.com/kb/811833) (http://support.microsoft.com/kb/811833).

Verifying whether your environment requires FIPS compliance

Ask your Windows security administrator whether the FIPS system cryptography setting has been enabled in the Local Security Policy or a Group Policy that applies to the SQL Server computer.

3.3.4 How to install IDERA SQL Secure

This procedure guides you through a typical install of IDERA SQL Secure. A typical install sets up all SQL Secure components on the same computer. Use this procedure for first-time installs and evaluation installs.

i Before you begin the installation process, ensure you have all permissions to create databases on SQL Server and review the [product requirements](#).

! SQL Secure installer do not support remote installation or installing the repository on Azure SQL Database instances or Amazon RDS for SQL Server instances.

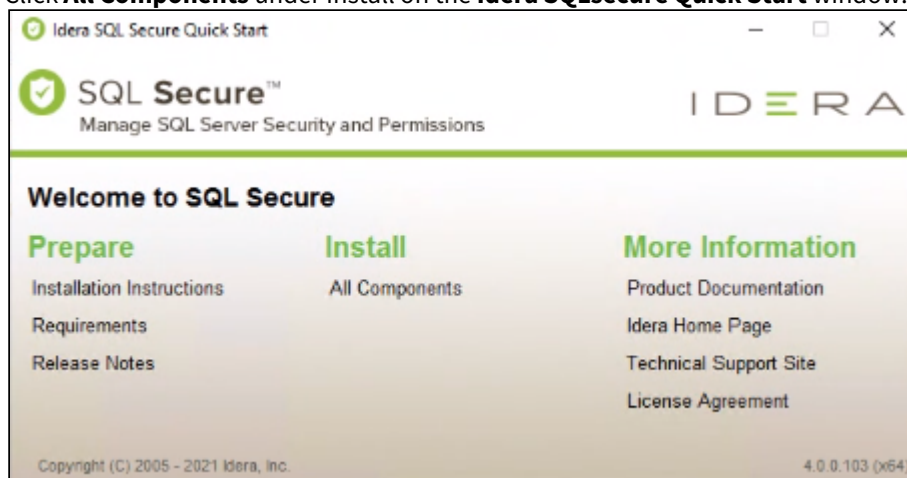
i Installing the Repository on remote SQL Server instances is not supported.

Start the setup program

You can install SQL Secure on any computer that meets or exceeds the product requirements.

To start installing SQL Secure:

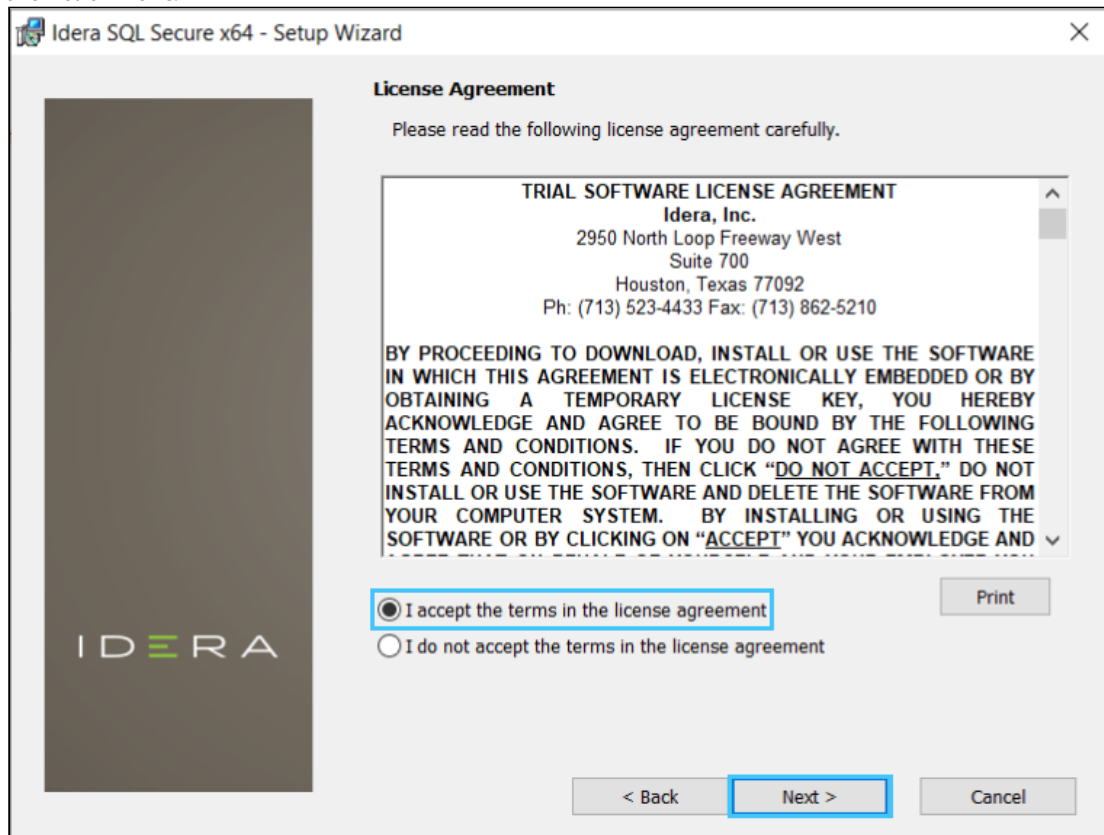
1. Log on with an administrator account to the computer on which you want to install SQL Secure.
2. Close all open applications.
3. Run `Setup.exe` in the root of the installation kit.
4. Click **All Components** under Install on the **Idera SQLsecure Quick Start** window.



5. On the Welcome to the Setup Wizard for Idera SQLSecure, click **Next**.

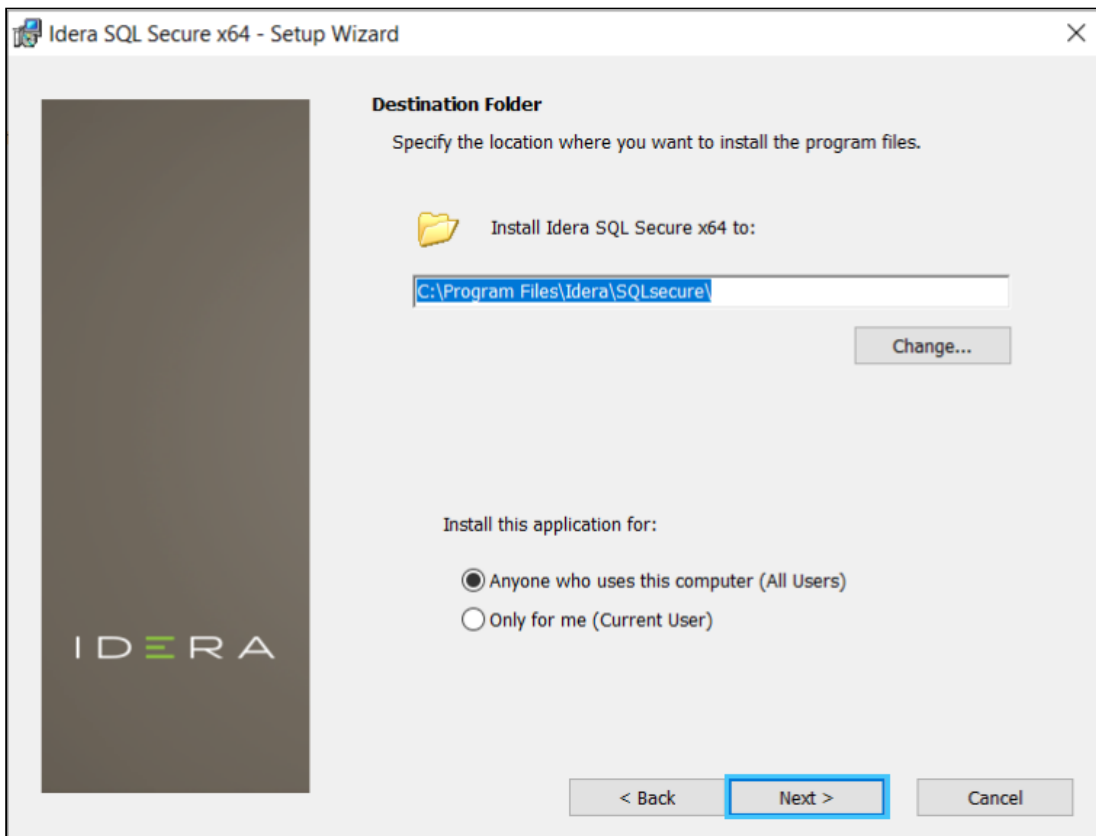


- Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.



Choose where you want to install SQL Secure and who should use the product on this computer

You can use the default install location or specify a different location. For your first install, we recommend using the default location.



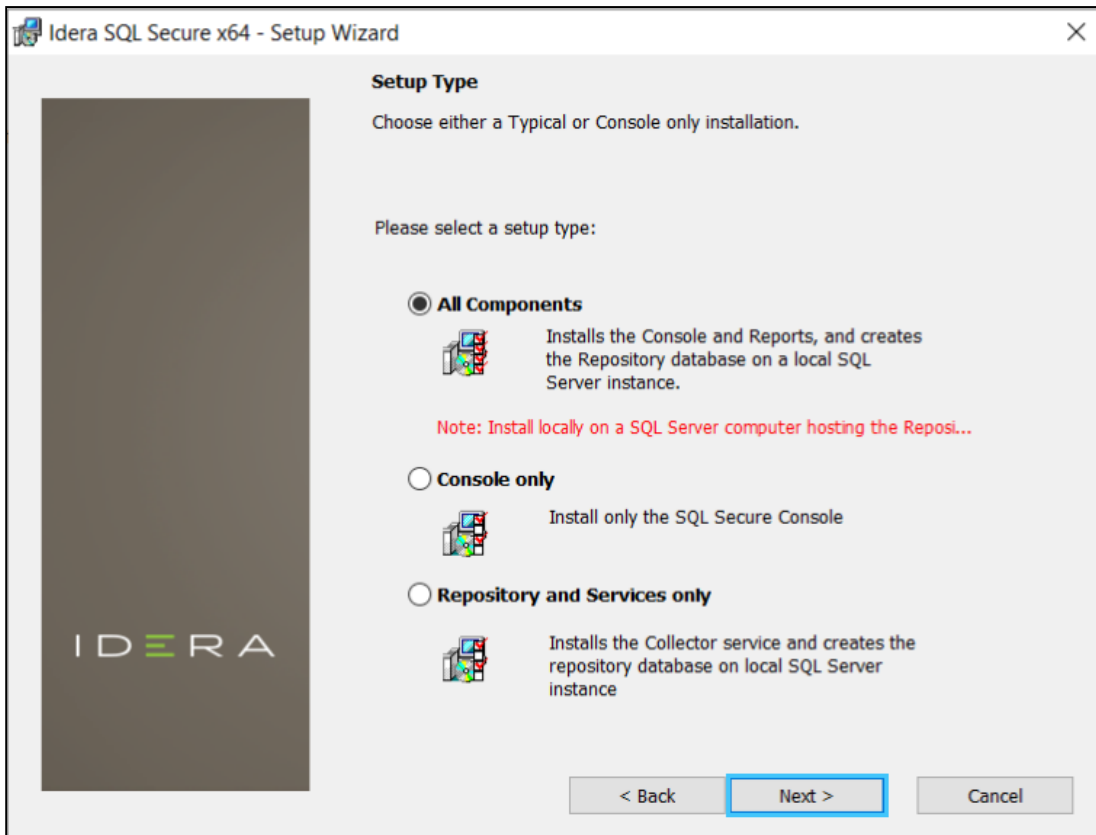
To choose a different location:

- Click **Change** to navigate to the location you want to use, and then click **Next**.

To restrict access:

1. Choose whether you want any user (Anyone who uses this computer) or only the current user (Only for me) to access this application,
2. Click **Next**.

Choose the type of install you want to perform



All Components

For your first install, we recommend that you select to install **All Components**. This option ensures that you install and configure all required SQL Secure components locally on the SQL Server computer hosting the Repository, so you can immediately begin using SQL Secure in your environment.

To perform a typical install, click **All Components**, and then click **Next**.

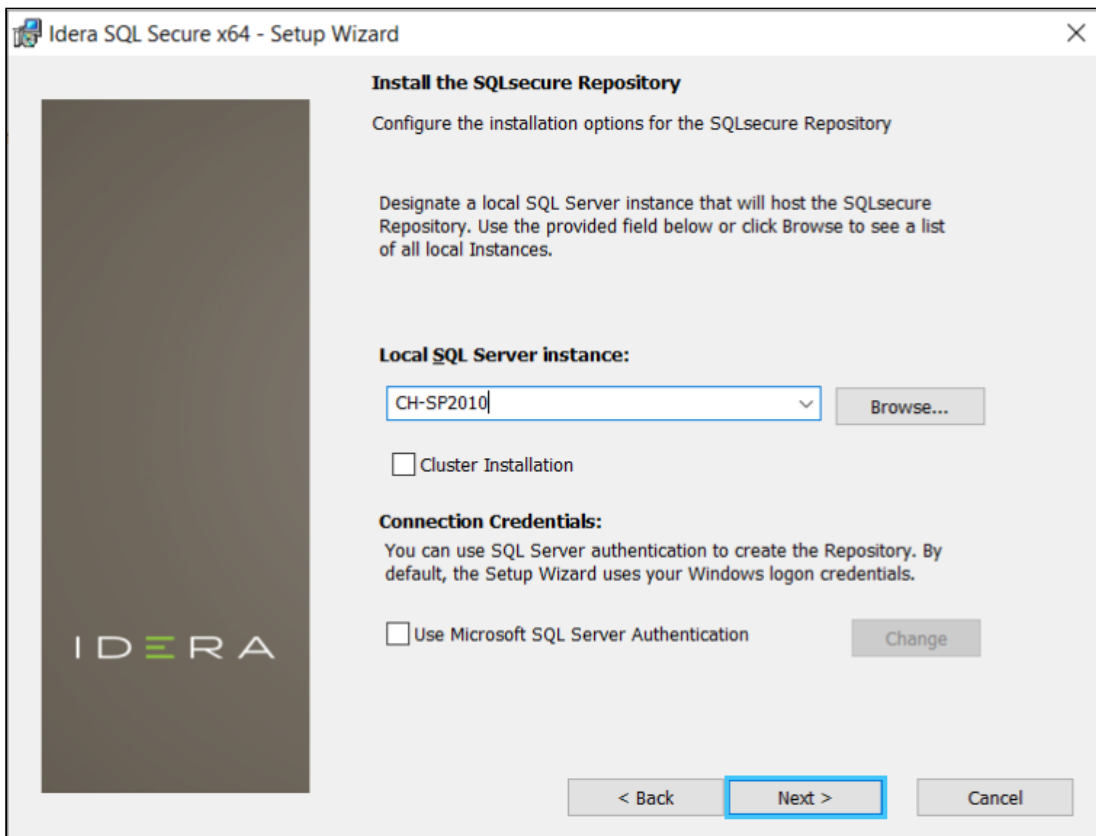
Console only or Repository and Services only

Alternatively, you can choose to install the **Console only** or the **Repository and Services only**. These options allow you to customize installation on each computer.

To install only the SQL Secure Console or the Repository and Services, select the appropriate option, and then click **Next**.

Choose which SQL Server instance you want to host the Repository database

Select the local SQL Server instance where the SQL Secure repository will be installed.



To choose the instance where the repository will be installed:

1. Click **Browse** to access a new window where a list of all available instances, in your current domain and other trusted domains will be displayed. Select the SQL Server instance you want to use.
2. Click **OK**.

✔ If you do not see your SQL Server instance in the list, enter the host name and instance in the space provided.

To install on a cluster:

If you are installing on a Failover Cluster, check the **Cluster Installation** checkbox.

To specify the Connection Credentials:

By default, SQL Secure will connect to the selected SQL Server instance using the credentials of your current Windows logon account. For your first install, we recommend using your current logon account credentials.

To use a SQL Server login:

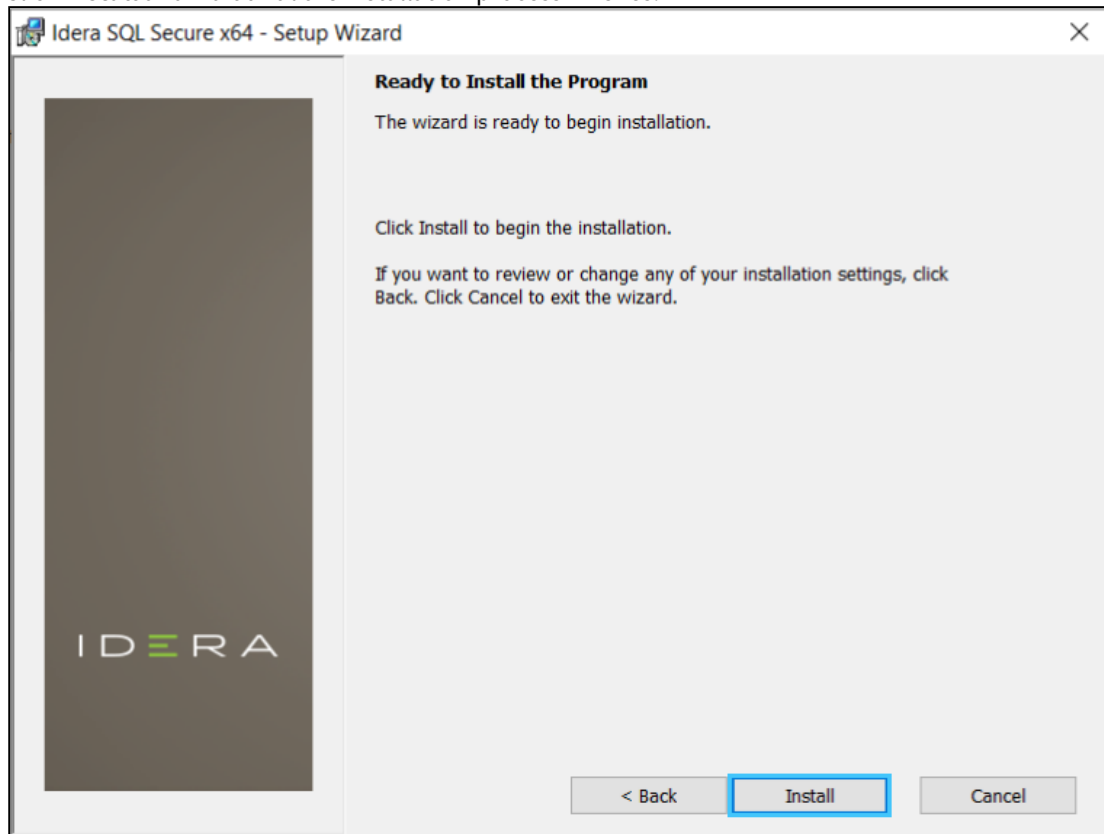
1. Click **Use Microsoft SQL Server authentication**. A new window for specifying the login credentials opens.
2. Specify the credentials of the login with sysadmin privileges on that instance, and then click **OK**.
3. Click **Next**.

Complete the install

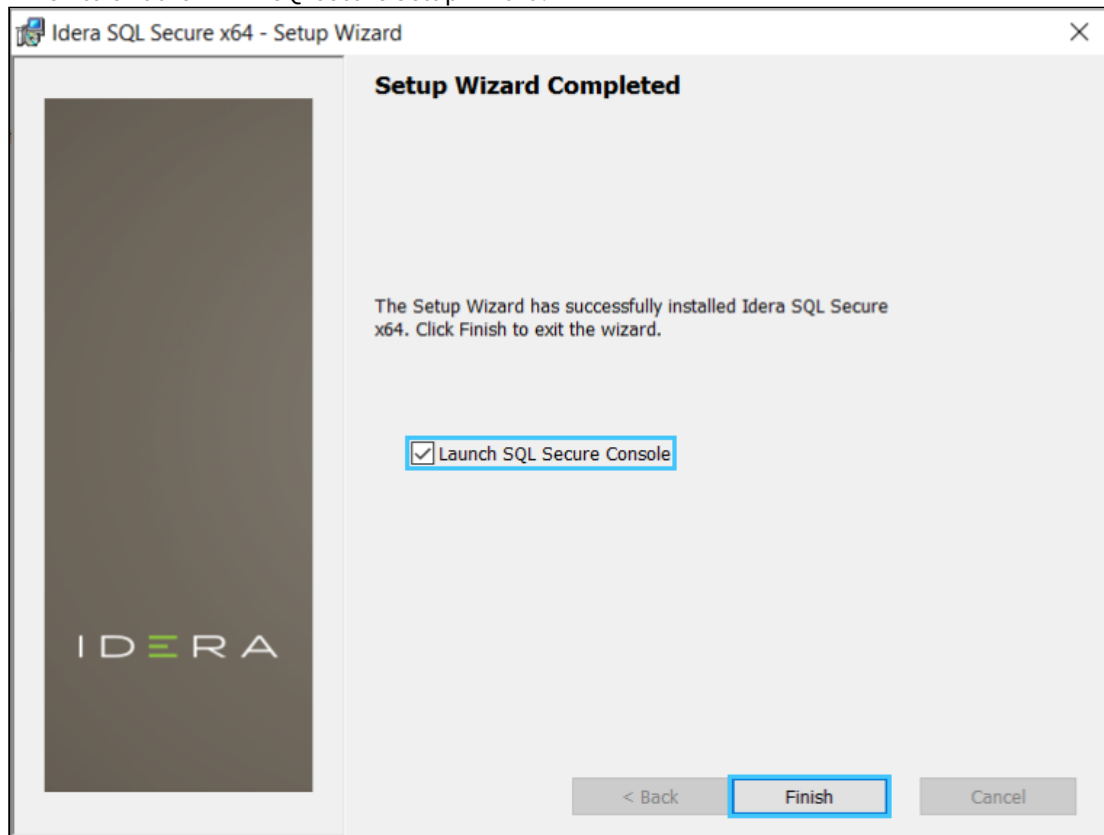
Indicate that you are ready to complete your install and apply the configurations you specified. If you want to make changes or review your installation settings, click **Back**.

To complete your install:

1. Click **Install** and wait until the installation process finishes.



2. Check the **Launch SQL Secure Console** checkbox to run the application after the installation finishes. Click **Finish** to exit the IDERA SQLsecure Setup Wizard.



After the installation is complete, you can start the Management Console to immediately begin experiencing the benefits SQL Secure provides.

3.4 Configure your deployment

After your initial installation and set up of IDERA SQL Secure, you may want to perform the following tasks to further customize and streamline your deployment.

- [Connect to your SQL Secure Repository](#)
- [Set up weak password detection to audit password health](#)
- [Use filters to specify which data is collected](#)
- [Use snapshots to collect audit data](#)
- [Register your SQL Server instances](#)

3.4.1 Connect to the IDERA SQL Secure Repository

By default, IDERA SQL Secure connects to the Repository when you start the Console. You may need to reconnect to the Repository database under these circumstances:

- You installed multiple Repository databases
- You moved the Repository database to another SQL Server instance
- You lost connection to the SQL Server instance hosting the Repository and must reconnect

Users who have an Azure environment can connect to the Repository by authenticating with either an Azure Active Directory account or a role-based access control (RBAC) account that is an authorized database administrator.


IDERA SQL Secure supports multi-part server fully qualified domain names entered in the following format:

[name.server.secure.database.net](#)

i IDERA SQL Secure verifies that the Repository is current. If auto-detection discovers the Repository is out of date, SQL Secure displays a warning message and allows the user to update it using installed Repository upgrade scripts

To connect to the Repository

1. Go to **File**, in the menu options, and select **Connect to Repository**.

2. A new window opens where you can enter the name of the SQL Server that hosts the Repository or access the list of available SQL Servers by clicking the ellipsis button .
3. Select the appropriate account authentication method, whether Azure Active Directory, SQL Server, or Windows authentication.
4. After you specify the account credentials, click **Connect**.

3.4.2 How does Weak Password detection help you?

The **Weak Password Detection** option lets you set up how IDERA SQL Secure enforces password health. When setting up this option, take the following points into account:

- Users should not use blank passwords, passwords with common words, or passwords that match a login name.
- The SQL Logins of your audited SQL Server instances will be checked against a list of known words used in weak passwords.
- SQL Secure allows you to specify a custom list that includes words and phrases you have restricted in order to ensure passwords meet corporate security policies.
- Password detection is enabled by default for all SQL Server instances registered with SQL Secure.

⚠ SQL Secure determines the password health for all SQL logins but not for Windows user accounts or groups who have privileges on the audited SQL Server instance.

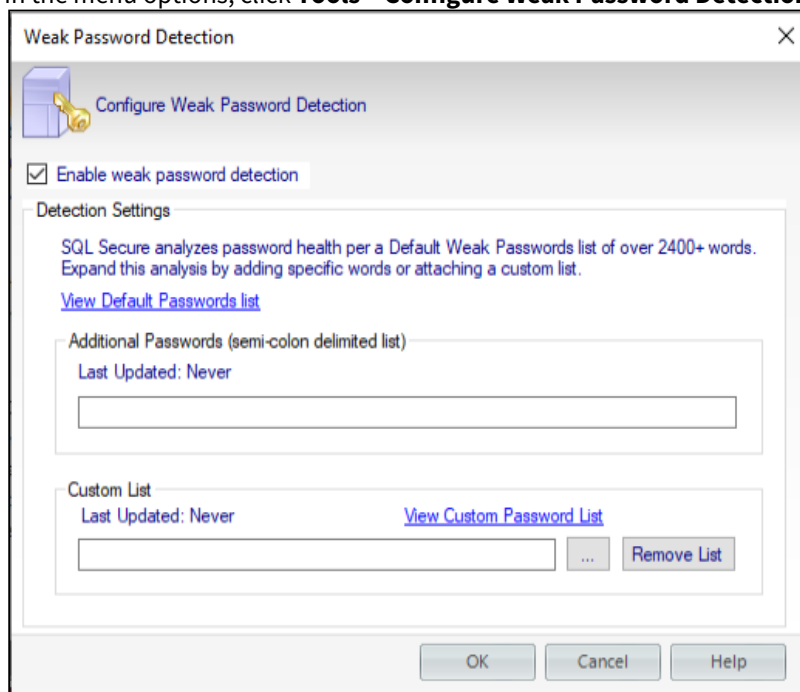
Weak password detection

The password analysis is performed during snapshot collection. When a snapshot is taken, the passwords of all SQL logins on the target SQL Server instances are collected and then compared against the default weak password list as well as any custom lists you defined. Each password is also compared against the name of its login.


The result (a security check finding) is stored in the Repository database but the passwords themselves are not stored.

To configure your Weak Password Detection settings:


1. In the menu options, click **Tools > Configure Weak Password Detection**.



2. Select **Enable weak password detection**. SQL Secure uses a default list with over 2400+ words. In the **Detection Settings** you can:

- Add new words to the default list by typing the additional words or phrases separated by a semicolon in the Additional Passwords textbox. If you want to access the Default Passwords list, click **View Default Password List**.
- Customize the password analysis by importing a custom list. For this purpose, type the name of the list file (text file *.txt) or click the ellipsis button  to browse a file in your computer. Format the text file such that each word or phrase is located on a separate line. If you want to view the imported list, click **View Custom Password List**. To specify a different text file, click **Remove List**, and then add the new file.

3. Click **OK**.


 Determine which policy assessments should analyze password health. For each assessment, review its settings to ensure the **Weak Passwords** security check is enabled. Test your configuration by [taking a snapshot](#) and then [reviewing the security check findings](#) for your target servers.

About the Default Weak Passwords list

The Default Weak Passwords list was compiled by industry experts. This list includes over 2,400 common words and phrases used in passwords that are considered weak (easy to guess or hack), including blank passwords. By default, SQL Secure uses this list to analyze your enterprise's password health, comparing each SQL login password to the list, then reporting the result as a security check finding.

 The weak password check is currently **case-sensitive**. For example, "password" can trigger weak password alerts but "Password" don't.

You can add specific words and phrases to the default list, such as popular Internet memes like "kittteh" and "double rainbow." You can also add a custom list, such as words restricted by your corporate password policy or words that are common in your own environment.

 To create stronger passwords and help to ensure password security in your environment, enable the 'Enforce password policy' test. The security check name for this test is '*SQL Logins Not Using Password Policy*', find it enabled by default for the 'All Servers' audit policy, you can enable it manually in other custom policies."

Security Checks that enforce password health

To audit and enforce password health, enable the **Weak Passwords** security check in your assessment policies. This security check is enabled by default in the IDERA Level 2 and Level 3 [policy templates](#).

Detected types of password health

As SQL Secure analyzes the password health of your SQL logins, it records one of the following results. These findings are displayed in the corresponding [Login Properties window](#) and the [Login Vulnerability report](#).

Password health results	What it means
Blank	The password for this login is either blank or null, which means no password is required for authentication or successful connection to databases hosted by your audited SQL Server instances.

Password health results	What it means
Matches login name	The password for this login matches the name of the login.
N/A	The password for this login was not checked, most likely because either the login is a Windows user account or weak password detection is disabled.
OK	This login most likely has a strong password because the password does not match any of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.
Weak	The password for this login matches one or more of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.

About password detection

When weak password detection is disabled, SQL Secure stops collecting password health data. All previously collected data remains stored in the SQL Secure Repository database and can be evaluated using your policy assessments. For future assessments, SQL Secure will no longer report on whether any SQL login passwords are considered weak but it will continue to report on whether a password is blank.

If the **Weak Passwords** security check is enabled for a policy assessment and the snapshot you selected does not include password health data, the **Snapshot May Be Missing Data** security check will warn you that weak password detection has been disabled and password health data is not available to analyze.

- ✔ To stop reporting on password health, disable the **Weak Passwords** security check in your policy assessments.

3.4.3 Add server to begin auditing

Before auditing with IDERA SQL Secure, you need to register those SQL Server instances you want to monitor. You can register servers using the **Register a SQL Server** wizard or by importing a file containing details of your SQL Server instances in .CSV format. The wizard is recommended if you have only a few instances while the import option is best for larger environments. For more information about importing your SQL Server instances, see [Import SQL Server instances](#).



⚠ Take into account that you have to complete the **Register a SQL Server** wizard for every SQL Server instance you want to monitor before it can be audited by SQL Secure.

On the **Register a SQL Server** wizards, you will be able to specify the SQL Server location, credentials to use for auditing, object filter criteria, the schedule of your audits, and email notifications configuration. Once you have set up your SQL Server instance for auditing, SQL Secure will apply your settings and display the registered instance in the Security Summary and Explore Permissions tree panes. These configuration settings are stored in the Repository.

Monitoring Always On Availability Groups

Users can monitor Always On Availability Groups using IDERA SQL Secure. Note that instead of monitoring the listener, you must monitor each individual node of the Availability Group. This is because the security configurations for each of the different nodes of the Availability Group are not always identical and monitoring only the listener could possibly leave gaps in the security check.

Access the Register a SQL Server wizard

You can open this wizard from the following locations:

- **File** menu - **Register a SQL Server** option.
- **Security Summary** view - **Register a Server** option in the ribbon menu options from the **Summary**, **Settings**, or **Users** tabs.

Register a SQL Server using the Register a SQL Server wizard

SQL Server instances must first be added to SQL Secure before the auditing process can begin. The Register a SQL Server wizard guides you through several sections that allow you to specify the required settings for SQL Secure to audit your server. In this wizard you will:

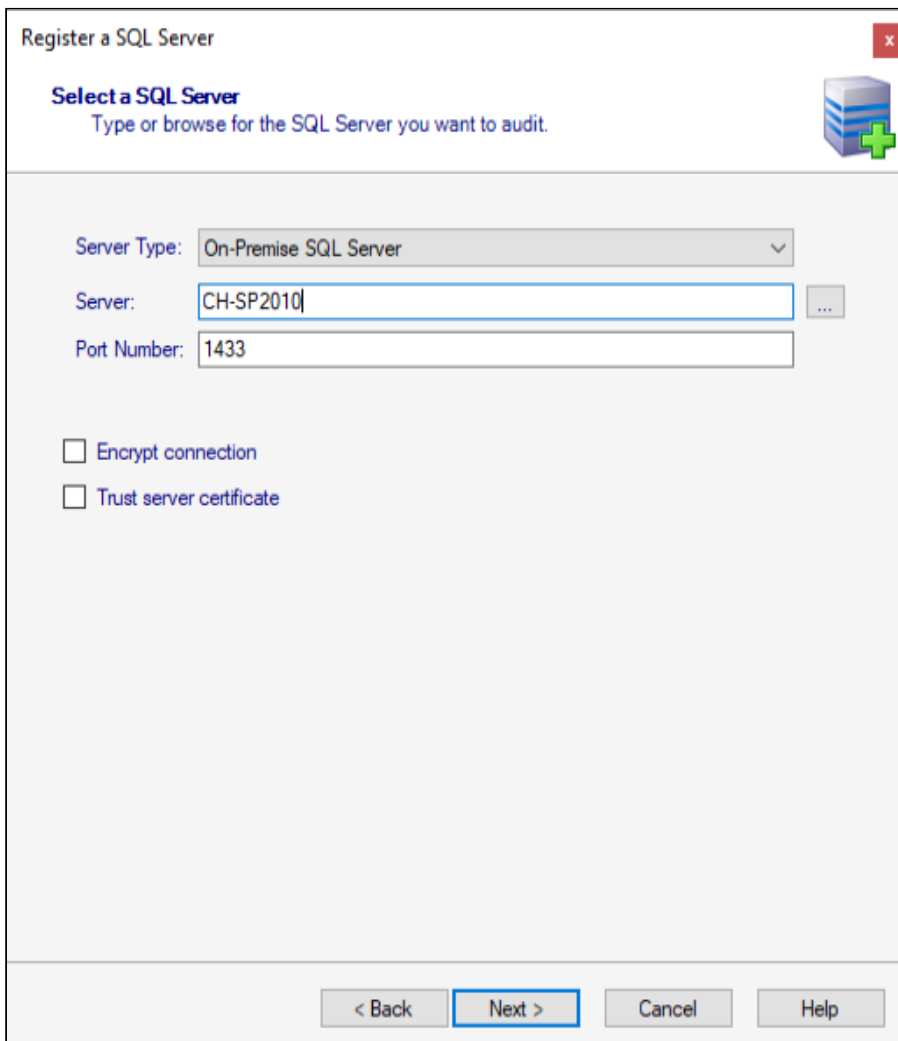
- [Select the SQL Server instance you want to audit with SQL Secure](#)
- [Specify the credentials used to connect to your SQL Server instance and collect data](#)
- [Select which objects you want SQL Secure to audit in your instance](#)
- [Schedule collection times for snapshots](#)
- [Configure your email notifications](#)
- [Choose if you want to take a snapshot after registration](#)
- [Review all configured settings in the wizard](#)

Select a SQL Server

In the **Select a SQL Server** section of the **Register a SQL Server** wizard, specify the Server Type you want to add to IDERA SQL Secure for auditing.

Monitoring Always On Availability Groups

Users can monitor Always On Availability Groups using IDERA SQL Secure. Note that instead of monitoring the listener, you must monitor each individual node of the Availability Group. This is because the security configurations for each of the different nodes of the Availability Group are not always identical and monitoring only the listener could possibly leave gaps in the security check.



Register a SQL Server

Select a SQL Server
Type or browse for the SQL Server you want to audit.

Server Type: On-Premise SQL Server

Server: CH-SP2010

Port Number: 1433

Encrypt connection


Trust server certificate


< Back Next > Cancel Help

To specify an instance:


1. Select the type of server you want to audit. Available options include:
 - **On-Premise SQL Server**
 - **SQL Server on Azure Virtual Machine**
 - **Azure SQL Database**
 - **SQL Server on Amazon EC2**

- **Amazon RDS for SQL Server**

2. Type the name of the instance you would like to audit. IDERA SQL Secure supports multi-part server fully qualified domain names entered in the following format: [name.server.secure.database.net](#)
or click the ellipsis button  to access a list of monitored SQL Servers in your domain, browse to locate your respective instance, then click **OK** to add it. This feature is not available when working with Azure and Amazon VMs or databases.
3. Specify the port number, the default port number (1433) or set the port number you configured on the Instance you are registering.
4. SQL Secure includes two registration options to secure connectivity between client and server, available for all server types:
 - **Encrypt connection:** Need the same certificate to be installed on the client and server machines. For more information click [here](#).
 - **Trust Server Certificate:** When user selects this option do not need any certificate to continue with the registration.

 The certificate is created on the server machine once Encrypt Connection option is selected on SQL Server, you can export and import the certificate to the client machine.

5. Click **Next** to go to the following section and [Specify your connection credentials](#).

 You can add as many instances as your SQL Secure license provides. For more information, see [Managing Your SQL Secure Licenses](#).

Specify connection credentials

The **Specify Connection Credentials** wizard allows you to designate the credentials that IDERA SQL Secure will use to access the SQL Server instance you are adding whether the SQL Server instance is running private network or public cloud such as Azure VM, Azure SQL Databases, Amazon EC2 or Amazon RDS. You have to specify credentials according the type of server you want to register:

On-Premise SQL Server

For **On-Premise SQL Server** servers, you have to specify the following credentials:

On the first section you will see the **SQL Server credentials to connect to audited SQL Server**, choose one of the following options:

- Select **Windows Authentication** and enter the credentials in the fields provided.
- Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

On the **Windows Credentials to gather Operating System and Active Directory objects** credentials section, you have the following options:

- Check the **Use same Windows Authentication as above** box to use the Windows credentials specified above.
- Specify a different Windows account that SQL Secure will use use to gather information about OS and AD objects.

Register a SQL Server

Specify Connection Credentials
Specify which credentials SQL Secure should use to collect audit data.

SQL Server credentials to connect to audited SQL Server

Windows Authentication

Windows User:

Password:

SQL Server Authentication

Login Name:

Password:

Windows Credentials to gather Operating System and Active Directory objects

Windows credentials are used to connect to the target server to gather Active Directory objects and file and registry key permissions. The specified account must have admin access to the target server and at least login access to the SQL

Use same Windows Authentication as above

Windows User:

Password:

< Back Next > Cancel Help

SQL Server on Azure Virtual machine

For **SQL Servers on Azure Virtual machines**, you have to specify the following credentials:

On the **SQL Server credentials to connect to audited SQL Server**, choose one of the following options:

- Select **Windows Authentication** and enter the credentials in the fields provided.
- Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

The **Azure Active Directory to gather Operating System and Active Directory objects** section, asks for credentials to connect the target server to gather Active Directory objects and key permissions.

The accounts need **Administrator** access to the target server.

Register a SQL Server

Specify Connection Credentials
Specify which credentials SQL Secure should use to collect audit data.

SQL Server credentials to connect to audited SQL Server

Windows Authentication

Windows User:

Password:

SQL Server Authentication

Login Name:

Password:

Azure Active Directory to gather Operating System and Active Directory objects

Azure AD Credentials are used to connect to the target server to gather Active Directory objects and file and registry key permissions. The specified account must have admin access to the target server.

Azure AD Authentication

Azure AD Account:

Password:

< Back Next > Cancel Help

SQL Server on Amazon EC2

For **SQL Servers on Azure Virtual machines**, you have to specify the following credentials:

On the **SQL Server credentials to connect to audited SQL Server**, choose one of the following options:

- Select **Windows Authentication** and enter the credentials in the fields provided.
- Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

The **AWS Directory Service for Microsoft Active Directory to gather Operating System and Active Directory objects** section, asks for credentials to connect the target server to gather Active Directory objects and key permissions.

The accounts need **Administrator** access to the target server.

Register a SQL Server

Specify Connection Credentials
Specify which credentials SQL Secure should use to collect audit data.

SQL Server credentials to connect to audited SQL Server

Windows Authentication

Windows User:

Password:

SQL Server Authentication

Login Name:

Password:

AWS Directory Service for Microsoft Active Directory to gather Operating System and Active Directory objects

Amazon AD Credentials are used to connect to the target server to gather Active Directory objects and file and registry key permissions. The specified account must have admin access to the target server.

Amazon AD Authentication

Amazon AD Account:

Password:

< Back Next > Cancel Help

Azure SQL Database

On the SQL Server credentials to connect to audited SQL Server section, choose one of the following options:

- Select **Azure Active Directory** and enter the credentials in the fields provided.
- Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

Register a SQL Server
x

Specify Connection Credentials
Specify which credentials SQL Secure should use to collect audit data.

SQL Server credentials to connect to audited SQL Server

Azure Active Directory

Azure AD Account:

Password:

SQL Server Authentication

Login Name:

Password:

< Back
Next >
Cancel
Help

⚠ Connection Error

Configure your [Azure SQL Server Firewall](#) if a Connection Error displays.

Amazon RDS for SQL Server

On the SQL Server credentials to connect to audited SQL Server section, choose one of the following options:

- Select **AWS Directory Service for Microsoft Active Directory** and enter the credentials in the fields provided.
- Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

Register a SQL Server x

Specify Connection Credentials
Specify which credentials SQL Secure should use to collect audit data.

SQL Server credentials to connect to audited SQL Server

AWS Directory Service for Microsoft Active Directory

Amazon AD Account:

Password:

SQL Server Authentication

Login Name:

Password:

⚠ Case Sensitive accounts

Take into account that if the login configuration for the SQL Server you want to audit is case-sensitive, you must enter your login credentials in the case-sensitive format.

⚠ Permissions and Privileges


You should keep in mind the following permissions for the accounts specified in this section:

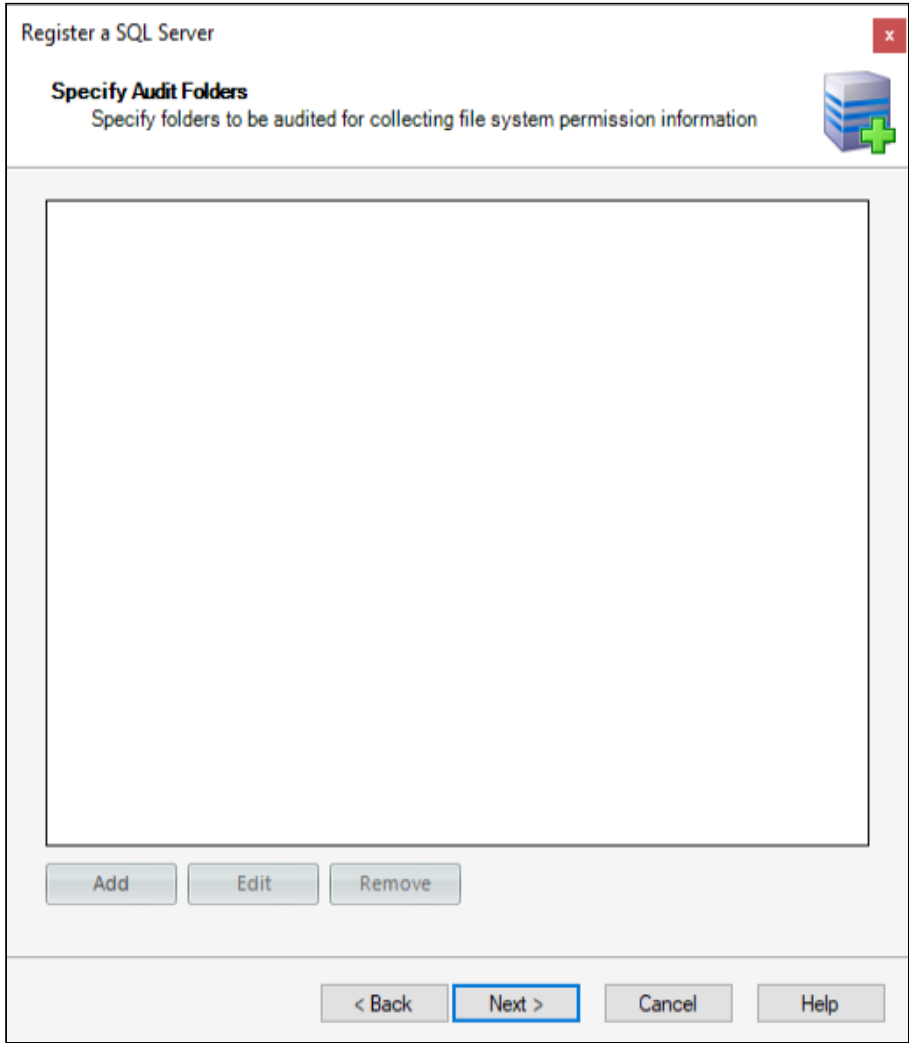
- The SQL Server login must belong to the sysadmin fixed role on the target instance.
- The Windows account must have Windows Administrator privileges on the target instance to collect group membership information.
- The account specified for gathering information about OS and AD objects must have admin access to the target server and at least login access to the SQL Secure Repository.

After you specify your connection credentials, click **Next** to go to [Add server group tags](#).

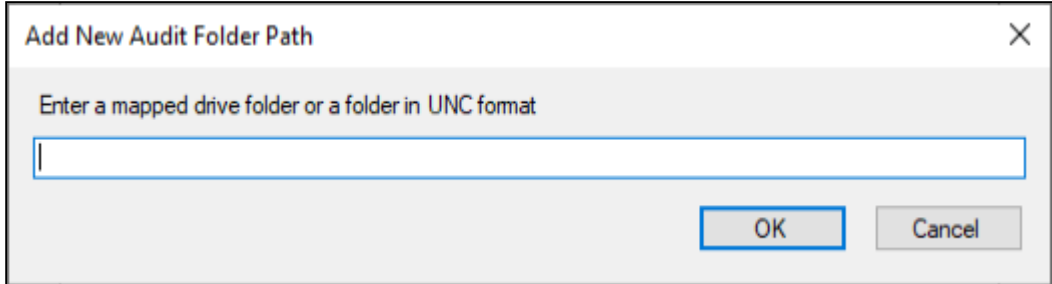
Define folders for file system permissions checks

In the **Specify Audit Folders** section, you can select which folders will be audited for collecting file system permission information.

 Amazon RDS accounts do not have this option available.



Click **Add** and type a mapped drive folder or a folder in UNC format. You can add as many folders as you require.



If you want to change or delete any of the previously added folders, click **Edit** or **Remove** respectively.
Click **Next** to go to [adding Server Group Tags](#).

Add server group tags

In the **Add to Server Group Tag** section you can specify which tags you want to apply to the SQL Server you are registering. Tags allow you to group SQL Servers for better management as you are making changes to the group as a whole instead of to each SQL Server individually. By default, the **All Servers** tag is already added.

Register a SQL Server

Add to Server Group Tag
Select tag(s) to add new server to.

Server Group Tag	Description
<input checked="" type="checkbox"/> All Servers	All Servers

Add Edit Remove

< Back Next > Cancel Help

Select the tag you want to apply, and then click **Add**. You can add as many tags as you require. If you want to change or delete any of the previously added tags, click **Edit** or **Remove** respectively.

If no tag is selected, SQL Secure applies the **All Servers** tag.

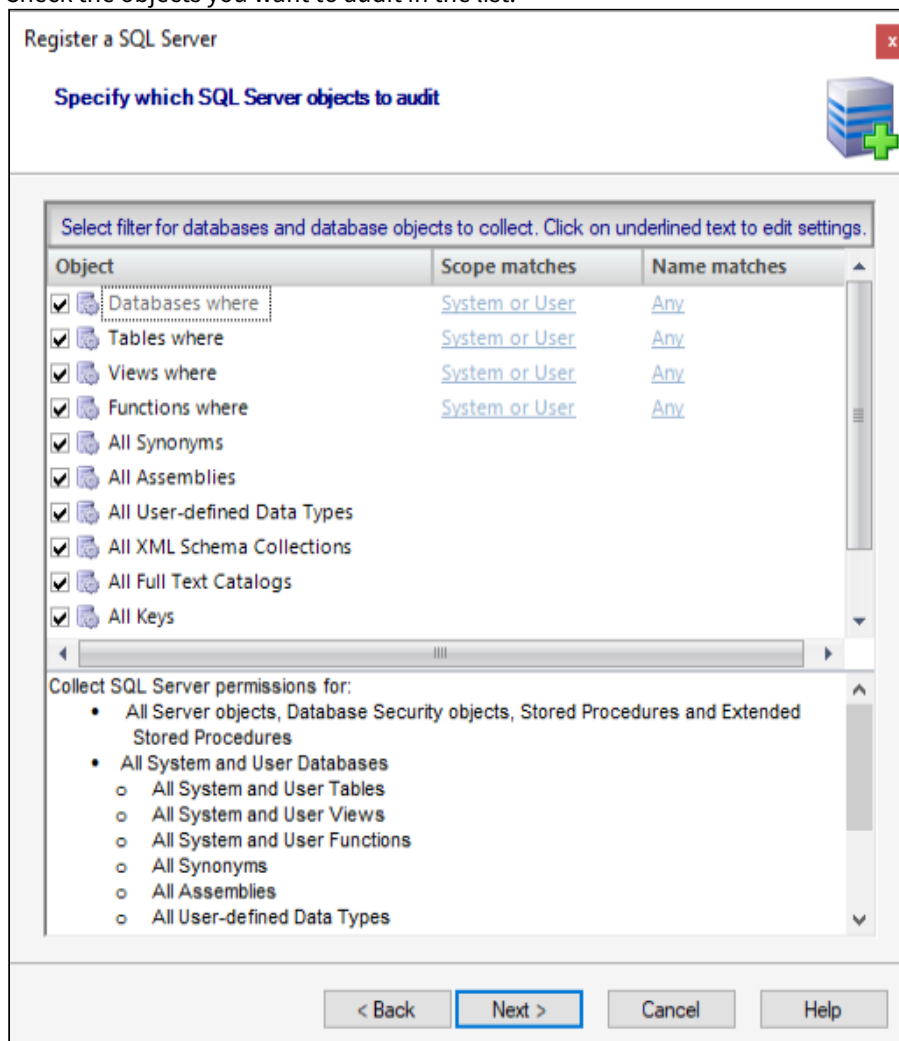
Click **Next** to go to [Select SQL Server objects to audit](#).

Select SQL Server objects to audit

In the **Select SQL Server Objects to Audit** section of this wizard, you can specify which database or server objects IDERA SQL Secure will audit to collect security information. By default, SQL Secure audits all SQL Server objects.

To select objects to audit:

1. Check the objects you want to audit in the list.



2. For those objects that have scope options, click the text in the **Scope matches** column, and select the appropriate option (User, System, System or User).
3. For those objects that have naming options, click the text in the **Name matches** column, and a new window opens with the following options:
 - In the first part of the window, select the elements you want to move to the **Selected** list, and then click **Add**. You can remove the added elements from the list by selecting the element and clicking **Remove**.
 - On the Names matching box, select **Any** if you want to include all elements names in your snapshot.
 - If you want to specify strings that your filter will use to match the names of your databases, click **Like** to enable new options on the **Name matching** box. You can search for a specific element by typing a specific string in the **Enter match string** field (you can use wildcards),

and then click **Add**. The **Match strings** field added strings. You can also remove strings from this box by selecting the string and clicking **Remove**.

4. SQL Secure displays at the bottom section of this window a summary of all selected objects and their specified settings.
5. Click **Next** to go to [Schedule Snapshots](#).

i For Amazon RDS and Azure SQL Databases the **Full Text Catalogs** objects are supported


! When you are selecting objects to audit, be aware that you need to include all the objects your policies need to appropriately assess security risks.

Schedule snapshots

The **Schedule Snapshots** section allows you to choose the best times to collect data from your SQL Server instance.

The screenshot shows a dialog box titled "Register a SQL Server" with a "Schedule Snapshots" section. The section includes a sub-header "Schedule Snapshots" and a description "Select when audit data (snapshots) should be collected." Below this, there is a control for "Keep snapshots for" set to "60" days, with a range of "(1 - 10000 days)". The "Collection Schedule" section has a checked "Enable Scheduling" checkbox and a text box containing "Occurs every week on Sunday at 3:00:00 AM", with a "Change..." button. The "SQL Server Agent Status" section shows a green power icon and the text "Started". At the bottom of the dialog are buttons for "< Back", "Next >", "Cancel", and "Help".

By default, snapshots are scheduled to run at 3:00 am every Sunday morning (using the local time of the computer hosting the IDERA SQL Secure Repository). The first snapshot is taken at the first scheduled snapshot collection time. You can manually take a snapshot at any time by right-clicking the SQL Server instance in the Explore Permissions view and then selecting **Take Snapshot** from the context menu.

 SQL Secure requires that a user be logged in as the SQL Secure Administrator to view snapshot schedules.

To change the default schedule, click **Change** and select the new time and frequency. When possible, schedule snapshots to run during non-peak or off-hour times.

Schedule Snapshots window actions

Item	Description
Keep snapshot for [number] days before allowing them to be groomed.	Specify the number of days that you want to store snapshots in the SQL Secure Repository. Specify a number between 1 and 10000 days. By default, this value is set to 60 days.
Enable Scheduling	Select this option to enable the audit snapshot schedule. If this option is disabled, you have to take snapshots manually.
Change	<p>Click this button to change the default snapshot collection schedule (3:00 am every Sunday morning). A new window opens where you can specify:</p> <ul style="list-style-type: none"> • The schedule to be Daily, Weekly, or Monthly • The respective settings according to the type of schedule selected. For example if you choose Weekly, you can select which days of the week SQL Secure will collect the data and how frequently the schedule will run, for instance, every 1 or 2 weeks. • The specific time of the day when the information will be collected, its frequency, and the Starting and Ending dates for this schedule option.

SQL Server Agent Status

Additionally, this section of the wizard allows you to see the status of your SQL Server Agent. Take into account that SQL Secure uses the SQL Server Agent for data collection and grooming. This Agent is located in the SQL Server hosting the Repository Database. You can see in this section whether the Agent status is Started or Stopped.

Click **Next** to go to the following section to [Configure your email notifications](#).

View snapshot properties

To view the properties of a specific snapshot, go to the **Explore Permissions** view, expand the SQL Server from which the snapshot was taken, right-click the respective snapshot, and select **Properties** from the context menu. For more information about what properties you can see, go to [View Snapshot Properties](#).

In this same view, you can also see the list of snapshots and baselines for a specific SQL Server. To see this information select your required server from the Audited SQL Servers tree and SQL Secure displays an **Audit History** section on the respective **Server Summary**. For more information about this view, go to [View single server summary](#).

Enable email notification

The **Configure Email Notification** section allows you to determine the way email notifications are sent after a snapshot is collected. You can set the following notifications:

- Email notifications sent after a snapshot is collected successfully, or only if there are warnings or errors. (Always, On Warning and Error, or Only On Error)
- Email notifications sent depending on the level of the security risks discovered. (Any Risk, On High and Medium Risks, or Only on High Risks)

Register a SQL Server

Configure Email Notification
Select whether email notifications should be sent after each snapshot.

Send Email Notification after Data Collection

Always

On Warning and Error

Only On Error

Send Email Notification for Security Findings

Any Risk

On High and Medium Risks

Only on High Risks


Email Recipient

(specify multiple email recipients by separating each address with a semicolon)


< Back Next > Cancel Help


Once you have configured when notifications are sent, specify who should receive these emails by specifying the appropriate email address in the **Email Recipient** field. To enter multiple email addresses, separate each address with a semi-colon.

If you do not want to receive email notifications for snapshots status or security findings, uncheck **Send Email Notification after Data Collection** and **Send Email Notification for Security Findings**.

 Email notifications cannot be sent until IDERA SQL Secure has been configured to communicate with your SMTP provider. You can configure these settings by selecting **Tools > Configure SMTP Email** from the menu bar. For more information, see [Configure Email Settings](#).

Click **Next** to continue.

 Take into account that when you have no policies created yet, the wizard will go directly to the [Take a Snapshot](#) section. However, the new registered SQL Server will be automatically added to the default **All Servers** policy and to any other policies defined with **Automatic Policy Membership**.

 SQL Secure provides an option to make bulk changes to email notification settings.

Choose to take snapshot now

The **Take Snapshot** section gives you the option to collect audit data at the end of the registration process. Choose this option when you want to immediately perform a security assessment on the newly registered instance. Note that you can also manually take a snapshot later by selecting **Take Snapshot** on the **Explore Permissions** view (Click [here](#) for more information about Snapshots). IDERA SQL Secure must collect data from the Registered Server to assess and audit security risks and access rights.

Register a SQL Server

Take Snapshot
Specify whether you want to collect audit data after registering this SQL Server.

Do you want to collect audit data (take a snapshot) after registering this SQL Server?

SQL Secure must collect data from the Registered Server to assess and audit security risks and access rights. This data collection can be scheduled or run manually.

Yes, collect data upon completion of the registration process.

< Back Next > Cancel Help

SQL Server Agent

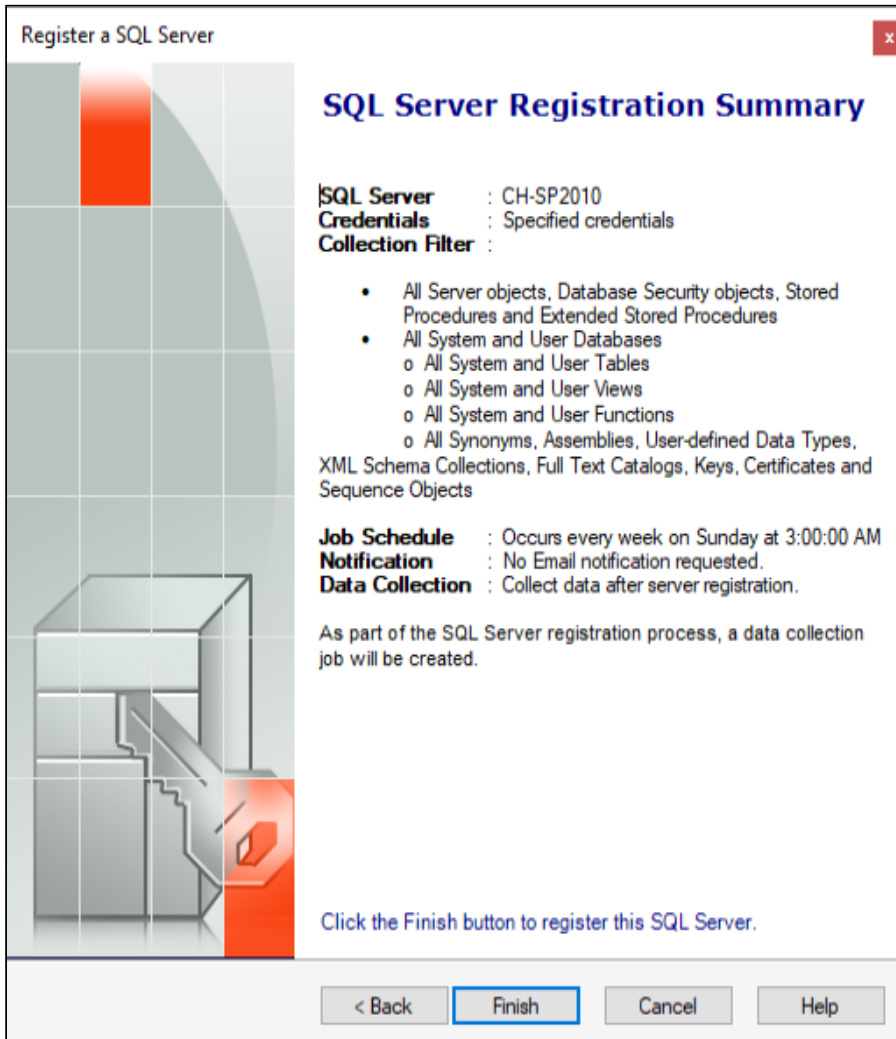
Before you begin collecting data make sure that the **SQL Server Agent** is running, otherwise the data collection will fail.

If you want to take a snapshot as soon as finish registering your SQL Server instance, make sure to check the option **Yes, collect data upon completion of the registration process.**

Click **Next** to go [Registration Summary](#) section.

Review registration summary

Review the provided summary for the instance you are adding to IDERA SQL Secure, and then click **Finish**. If you want to change a setting now, click **Back** to return to the appropriate section. You can also change audit settings later using the [Audited SQL Server Properties](#) window.




⚠ Before finishing this process, make sure the **port number** is the correct one, it throws an error when trying to change it after registration.

When you **Finish** this wizard, SQL Secure enables auditing on the selected SQL Server instance.

3.4.4 Import SQL Server instances

IDERA SQL Secure requires that you register any SQL Server instances that you want to monitor before auditing begins. The **Register a SQL Server** option allows you to add instances to SQL Secure one at a time. For environments having many SQL Server instances, a quick time saver is to import a .csv file. The **Import SQL Servers** option lets you quickly upload a file containing some data for the instances in your environment that you want to audit. Once imported, new SQL Server instances are registered directly in the repository with default settings. If the SQL Server instance already exists in the repository, then SQL Secure updates the login credentials for the server. IDERA SQL Secure supports SQL Server and Cloud Hosted SQL Server databases running in Azure or Amazon.

 After importing your SQL Server instances, be sure to go to the Server Group Tags view to add the new servers to the tag for better management. For more information about tags, see [Manage server group tags](#).

Acceptable .CSV format

You must use a properly-formatted .csv to successfully import a list of SQL Server instances, Azure SQL Database, or Amazon SQL Databases. There is no limit to the number of rows included in the file, but note that if a row is incorrectly formatted, IDERA SQL Secure displays a message stating that the file is not in the proper format.

For a successful import of SQL Server instances, please use the following general rules and .csv file format.

- **Server Name.** Name of the SQL Server you want to register.
- **Authorization Type.** Type of SQL Server authentication used to connect to the audited SQL Server.
 - **0** = Windows authentication
 - **1** = SQL Server authentication
 - **2** = Azure AD authentication
 - **3** = Amazon AD authentication (RDS for SQL Server)
- **User.**
 - **If the authorization type selected is 0 (Windows authentication)**, use Windows credentials.
 - **If the authorization type selected is 1 (SQL Server authentication)**, use the default credentials of the SQL Server Agent.
 - **If the authorization type selected is 2 (Azure AD authentication)**, use Azure AD credentials.
 - **If the authorization type selected is 3 (Amazon AD authentication)**, use Amazon AD credentials.
- **Password.** Password associated with the user account used previously.
- **Use Same Credentials.**
 - **TRUE** = Use Windows/Azure AD/Amazon AD credentials specified previously.
 - **FALSE** = Specify a different Windows account.
- **Windows User.** Credentials used to gather information about the OS, AD objects.
 - **If Use Same Credentials is TRUE (Use Windows/Azure AD/Amazon AD credentials specified previously)**, type a comma (,) in this column.
 - **If Use Same Credentials is FALSE (Specify a different Windows/Azure AD/Amazon AD account)**, specify a different Windows user account.
- **Windows User Password.**
 - **If Use Same Credentials is TRUE (Use Windows/ Azure AD/ Amazon AD credentials specified previously)**, type a comma (,) in this column.
 - **If Use Same Credentials is FALSE (Specify a different Windows/ Azure AD/ Amazon AD account)**, specify the password for the different Windows user account.
- **Port Number.** Port number on which the SQL Server instance, Azure SQL DB, or Amazon RDS for SQL Server is running. The default number is 1433.
- **Server Type.** Type the number of instances that is getting added.
 - **0** = On-premise
 - **1** = SQL Server on Azure VM

- 2 = Azure SQL Database
- 3 = Amazon RDS for SQL Server
- 4 = SQL Server on Amazon EC2

Examples

IDERA SQL Secure supports different Server Names and Users formats:

Server Name	Authentication Type	User	Password	Use Same Credentials	Windows User	Windows User Password	Port number	Server Type
FINSVR	0	myhouse\william	Test123	TRUE	,	,	1433	0
SQLSVR1	0	thathouse\jim	Num1DBA	FALSE	Tools	Test123	1433	0
acidr1.usercntry.com\MSSQLSERVER1	2	temp@xyz.com	abc@1234	TRUE	,	,	1433	1
sqlsecureacc.database.windows.net	2	test@clientlabs.com	abc@1234	TRUE	,	,	1433	2
IDR-SQL2008R2.US-EAST-1.RDS.AMAZONAWS.COM	3	clientlabs\administrator1	control*123	FALSE	,	,	1433	3
ec3-53-0-86-183.computelDR-1.amazonaws.com	0	simpclient\administrator	control*159	TRUE	,	,	1433	4

Sample .csv file:

Server


Name,AuthType,User,Password,UseSameCredentials,WindowsUser,WindowsUserPassword

FINSVR1,0,myhouse\william,Test123,TRUE,,,,, 1433, 0

SQLSVR1,0,thathouse\jim,Num1DBA,FALSE,Tools,Test123,1433,0

acidr1.usercntry.com\MSSQLSERVER1,2,temp@xyz.com, abc@1234,TRUE,,, 1433, 1

```
sqlsecureacc.database.windows.net, 2, test@clientlabs.com, abc@1234,TRUE,, ,
1433, 2
IDR-SQL2008R2.US-
EAST-1.RDS.AMAZONAWS.COM,3,clientlabs\administrator1,control*44,FALSE,, ,1433
,3
ec3-53-0-86-183.computeIDR-1.amazonaws.com
,0,simpclient\administrator,control*44,TRUE,"","","",1433,4
```

 The first row in the previous table must be included in the .csv file as shown.

Importing a .csv file

To import SQL Server instances:

1. In the Security Summary view, click **Import SQL Servers** at the top of the Summary tab. Alternatively, you can go to **File** menu and select **Import SQL Servers**.
OR
In the Manage SQL Secure view, click **Import SQL Servers** at the top of the Repository Status window. Alternatively, you can go to **File** menu and select **Import SQL Servers**.
The **Import SQL Servers** window opens.
2. Locate the file you want to import. Note that the file must be in the .csv format.
3. Click **Open**, and then click **OK**. SQL Secure validates the file format and displays the message, "Any registered servers found in the import file will have their credentials updated based on those specified in the file."
4. Click **OK**.

3.4.5 Use filters to specify which data is collected

IDERA SQL Secure uses snapshot filters to control the data collected from your audited SQL Server instances. Each filter rule defines which data, such as permissions on user tables in a specific database, is collected and included in the snapshot.

By default, SQL Secure collects all available audit data. You can edit this default filter rule or delete it after you have defined your custom filter.

Filters applied per Instance

Custom filters are applied at the instance level and are unique to that instance. You can create a different filter for each instance. You can also create more than one filter, depending on your assessment needs. When multiple filters are defined, SQL Secure aggregates them, collecting all data identified by all the filters associated with this instance.

Go to [Add Filters](#) to view about specifying filter properties, databases, and objects.

Add new filter

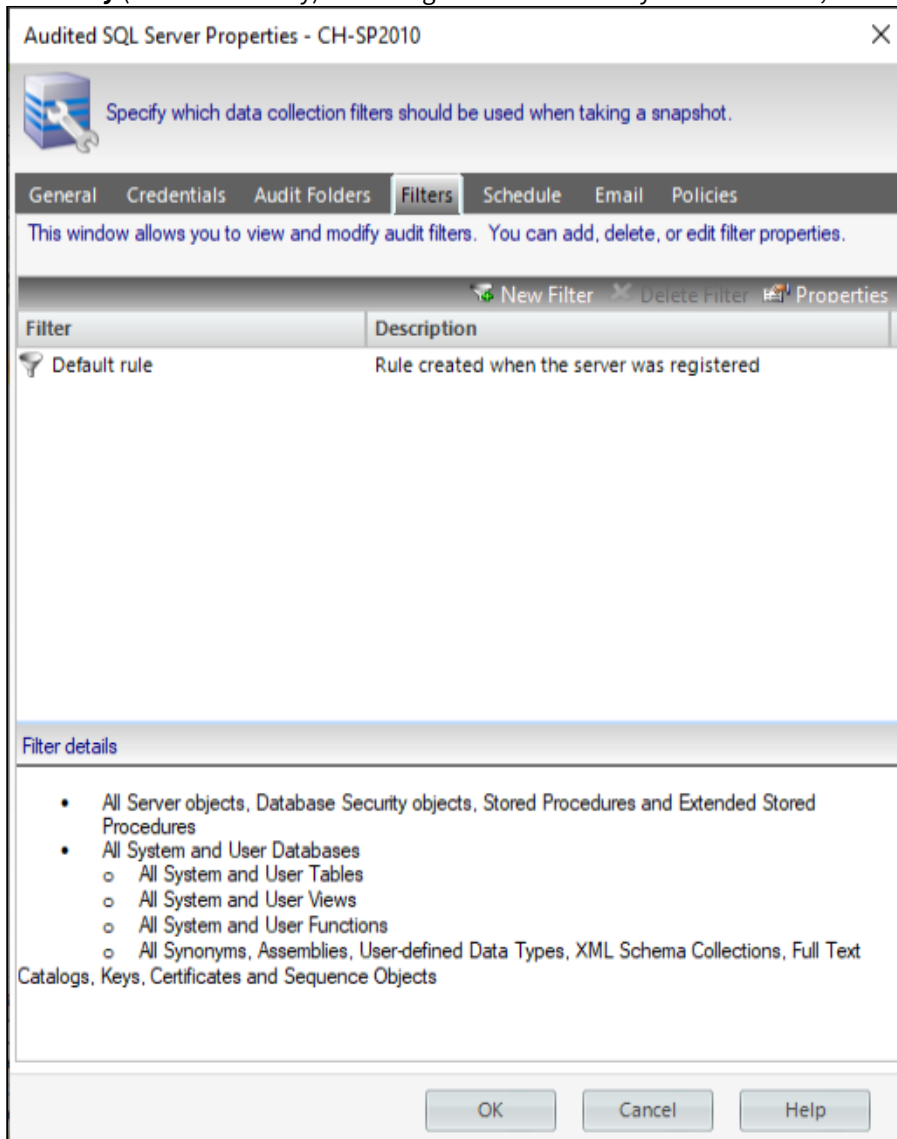
The **Add Filter** wizard allows you to choose the appropriate criteria to use when collecting snapshot information. By default, IDERA SQL Secure collects all security information.

- ✔ Consider using the default filter settings in your initial policy assessments until you know exactly which data your policies will require. Using the default filter settings ensures that all the data required by your policies is collected

Access this wizard

To open the Add Filter wizard:

1. You can find your registered servers on the **Explore Permissions** (Audited SQL Servers tree) or **Security Summary** (Servers in Policy) views. Right-click the server you want to edit, and select **Properties**.



2. Select the **Filters** tab.

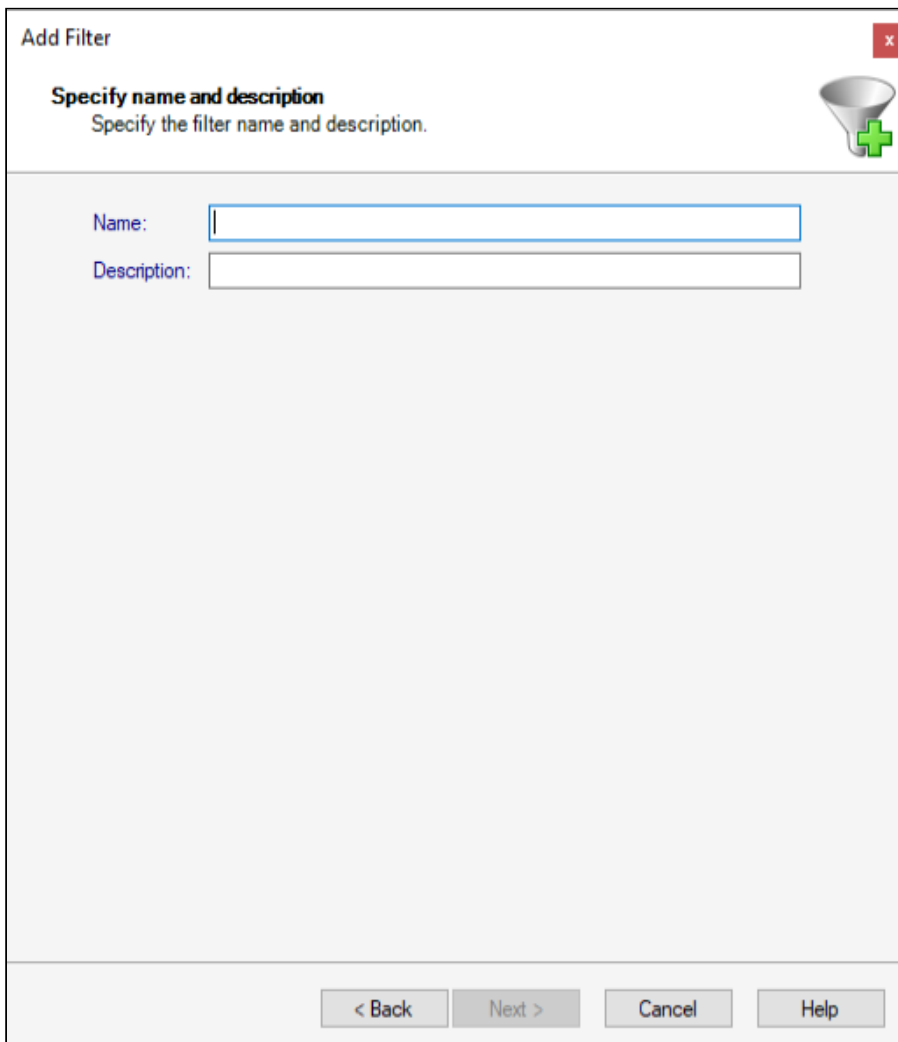
3. Click **New Filter** on the top section.

Add Filter wizard

The **Add Filter** wizard lets you designate what types of permission and security data will be collected. Use this wizard to store your filters in the Repository database, which are then used by SQL Secure when taking [snapshots](#).

Specify filter properties

After you open the **Add Filter** wizard, click **Next** and access the **Specify name and description** section. This window allows you to name your filter and give it a description. It is important to give your filter a name you can easily distinguish.

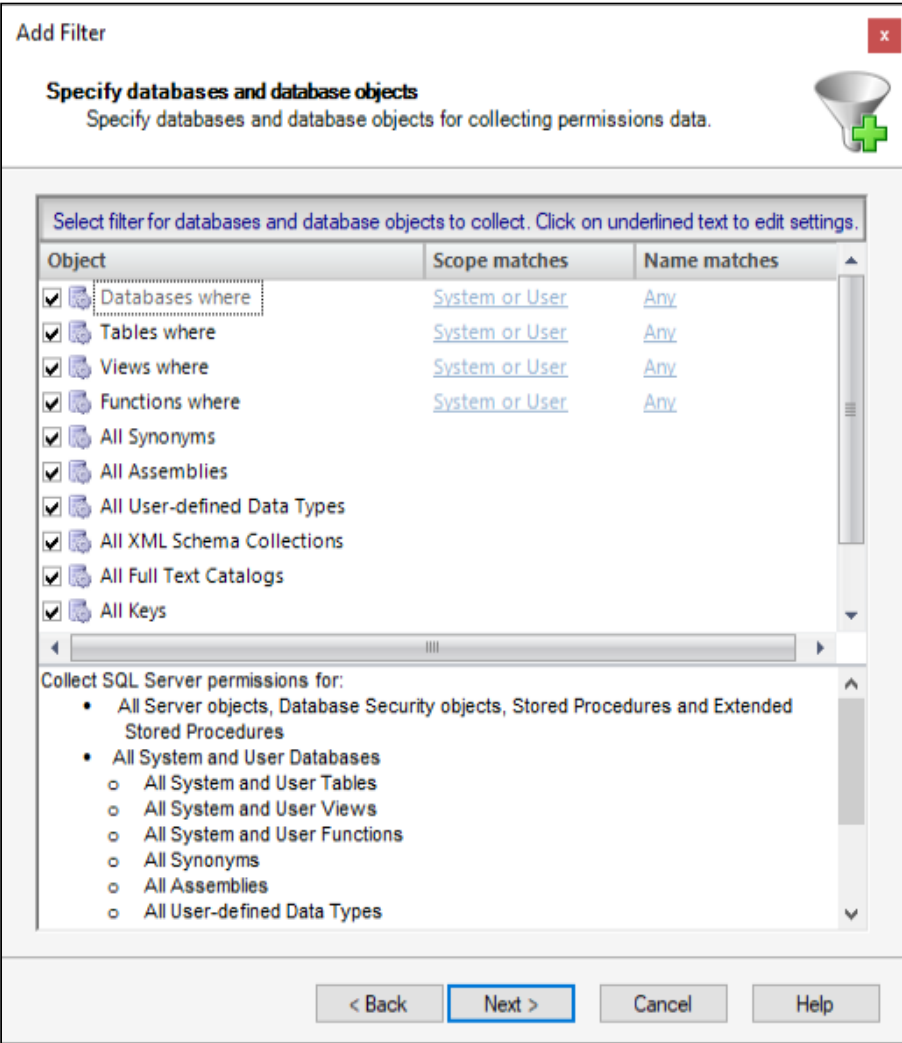


The screenshot shows a window titled "Add Filter" with a close button (X) in the top right corner. The main heading is "Specify name and description" with a sub-heading "Specify the filter name and description." and a funnel icon with a green plus sign. Below the heading are two text input fields: "Name:" and "Description:". At the bottom of the window are four buttons: "< Back", "Next >", "Cancel", and "Help".

Click **Next** to access the **Specify Databases and objects** section.

Specify databases and database objects

This window allows you to select which databases you want to audit using IDERA SQL Secure.



Options	Description
User databases and System databases	For some objects, the Scope Matches column allows you to select if you want to use System , User , or both (System or User) databases types for your snapshot.

Options	Description
Databases names matching	<ul style="list-style-type: none"> • In the list of available elements, click the elements you want to move to the Selected list, and then click Add. You can remove the added elements from the list by selecting the element and clicking Remove. • On the Names matching box, select Any if you want to include all elements names in your snapshot. • If you want to specify strings that your filter will use to match the names of your databases, click Like to enable new options on the Name matching box. You can search for a specific element by typing a specific string in the Enter match string field (you can use wildcards), and then click Add. The Match strings field added strings. You can also remove strings from this box by selecting the string and clicking Remove.

Complete the Add Filter Wizard

See name and the description of your filter

Click Back to change the information.

Click **Finish** to create the filter.

Edit filter settings

The **Filter Properties** window allows you to edit the properties of your snapshot filter. You can edit the name and description of your filter, see when it was last modified, and choose which audit data you want to collect in your snapshots.

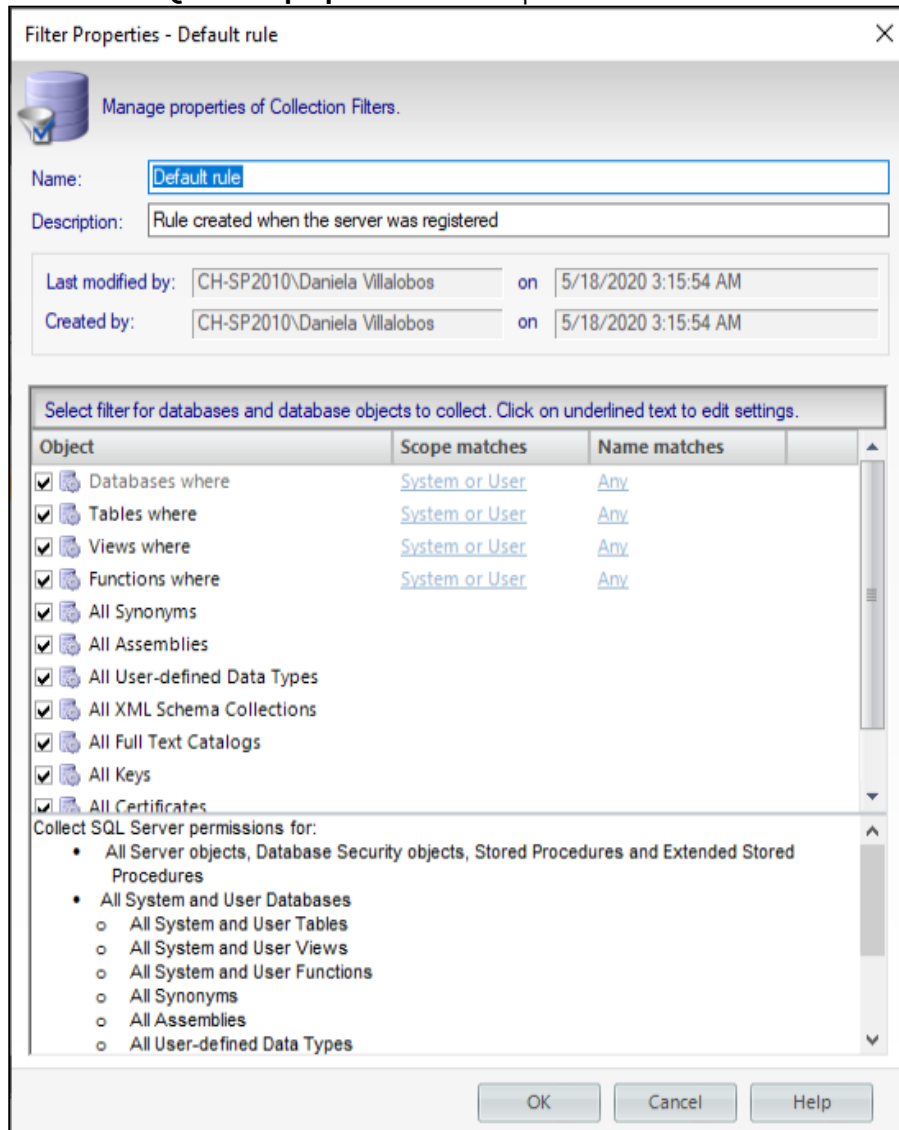
- ✔ Consider using the default filter settings in your initial policy assessments until you know exactly which data your policies will require. Using the default filter settings ensures that all the data required by your policies is collected.

Access this window

To access the Filter Properties window:

1. Right-click a SQL Server instance in the Policy Servers tree in the **Security Summary** view, and then select **Properties**.

The **Audited SQL Server properties** window opens.



- Click the **Filters** tab.
On the window you can see a list of all available filters.
- Select the filter you want to edit, and then click **Properties** at the top right of the list.
The **Filter properties** window opens, you can edit the name, description, and the objects you want to include in your snapshot. For more information about selecting objects and determining their settings, go to [Specify database objects](#).

3.4.6 Use snapshots to collect audit data

A snapshot is a set of audit data that IDERA SQL Secure has collected from a specific SQL Server instance. You can configure snapshot filters to select which SQL Server objects you want to audit. You can take snapshots [manually](#), as you need fresh data, or [schedule snapshots](#) to be taken at regular intervals.

SQL Secure uses audit snapshots to capture SQL Server user and object permission settings. These snapshots are listed in the **Explore Permissions** view by expanding the respective servers of the Audited SQL Servers tree. When you click a Snapshot, information about the snapshot is displayed on the right section of the console where the following tabs are displayed: Snapshot Summary, User Permissions, Role Permissions, and Object Permissions.

The **Snapshot Summary** tab provides all the information collected about your snapshot, some options change according to the type of server.

Data located on the Snapshot Summary


The Snapshot Summary contains the following types of information:

Snapshot Properties

Provides the basic status of the selected snapshot, the time it was collected, how long the collection took to complete, whether or not it has been selected as a baseline, and any comments associated with it.

Audit Summary

Lists the statistics of the snapshot. These statistics include the number of objects, permissions, databases, logins, Windows accounts, Windows well-known groups associated with the snapshot, and whether Weak Password Detection is enabled or not.

 To collect and review data about the password health of your SQL logins, you need to enable the [Weak password detection](#).

For On-premise, SQL Server on Azure VM, and SQL Server on Amazon EC2 accounts

Windows Accounts

Provides a partial list of the Windows users and groups that have access to the selected SQL Server instance either by a direct SQL Login or inherited via group membership.

OS Windows Accounts

Provides a partial list of the Windows users and groups that have access to OS objects but do not interact with SQL Server objects.

Suspect Windows Accounts

Lists the Accounts that SQL Secure was unable to collect data on. This can occur when SQL Secure does not have the proper rights to collect information on these users, or if the account was deleted. For more information, see [Identify Suspect Windows Accounts](#).

Suspect OS Windows Accounts

Lists the Accounts that SQL Secure was unable to collect data on. This can occur when SQL Secure does not have the proper rights to collect information on these users, or if the account was deleted. For more information, see [Identify Suspect Windows Accounts](#).

Unavailable Databases

Lists the databases that SQL Secure was unable to collect SQL Server security data on. This can happen when a database is unavailable during SQL Secure data collection; for example, a database being backed up is unavailable for data collection. For more information, see [Identify unavailable databases](#).

Filters

Provides the filter information associated with the selected snapshot. For more information, see [Add new filter](#).

For Azure SQL Database Amazon RDS for SQL Server accounts

Azure AD accounts and Amazon AD accounts

Provides a list of the Azure or Amazon users and groups that have access to the selected instance either by a direct SQL Login or inherited via group membership.

Unavailable databases

Lists the databases that SQL Secure was unable to collect SQL Server security data on. For more information, see [Identify unavailable databases](#).



SQL Secure cannot collect data from the **model database** on RDS servers because of Amazon restrictions.

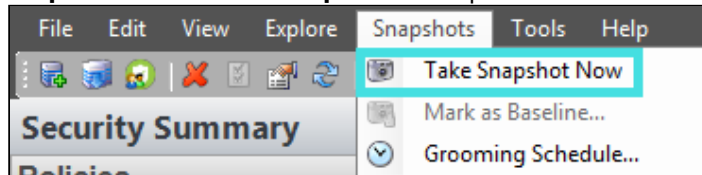
Filters

Provides the filter information associated with the selected snapshot. For more information, see [Add new filter](#).

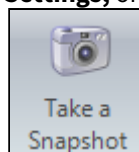
Take snapshot

To immediately collect a data snapshot (audit a SQL Server instance), you can take snapshot from the following locations

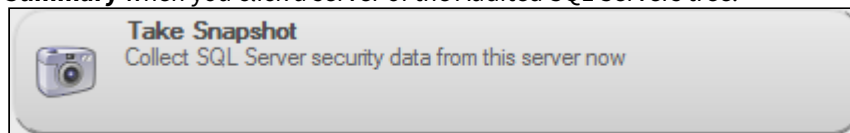
- **Snapshots** menu - **Take Snapshot Now** option



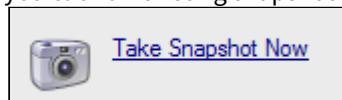
- **Security Summary** view - **Take a Snapshot** option in the ribbon menu options from the **Summary**, **Settings**, or **Users** tabs.



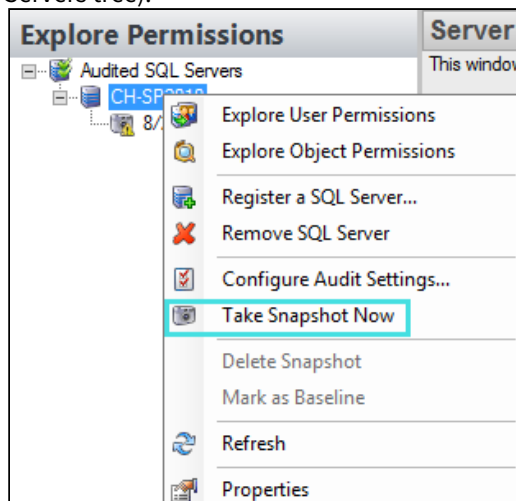
- **Explore Permissions** view - **Take Snapshot** option located in the **SQL Server Properties** of the **Server Summary** when you click a server of the Audited SQL Servers tree.



- **Explore Permissions** view - **Take Snapshot Now** option located on top of the **Snapshot Summary** when you click an existing snapshot of the Audited SQL Servers tree.



- Right Click the server to audit, select **Take Snapshot Now** from the context menu. You can right-click a server from the **Security Summary** view (Server in Policy tree) or **Explore Permissions** view (Audited SQL Servers tree).



Schedule snapshots for routine data collection

The **Schedule Snapshots** section allows you to choose the best times to collect data from your SQL Server instance.

By default, snapshots are scheduled to run at 3:00 am every Sunday morning (using the local time of the computer hosting the IDERA SQL Secure Repository). The first snapshot is taken at the first scheduled snapshot collection time. You can manually take a snapshot at any time by right-clicking the SQL Server instance in the Explore Permissions view and then selecting **Take Snapshot** from the context menu.

 SQL Secure requires that a user be logged in as the SQL Secure Administrator to view snapshot schedules.

To change the default schedule, click **Change** and select the new time and frequency. When possible, schedule snapshots to run during non-peak or off-hour times.

Schedule Snapshots window actions

Item	Description
Keep snapshot for [number] days before allowing them to be groomed.	Specify the number of days that you want to store snapshots in the SQL Secure Repository. Specify a number between 1 and 10000 days. By default, this value is set to 60 days.
Enable Scheduling	Select this option to enable the audit snapshot schedule. If this option is disabled, you have to take snapshots manually.
Change	Click this button to change the default snapshot collection schedule (3:00 am every Sunday morning). A new window opens where you can specify: <ul style="list-style-type: none"> • The schedule to be Daily, Weekly, or Monthly • The respective settings according to the type of schedule selected. For example if you choose Weekly, you can select which days of the week SQL Secure will collect the data and how frequently the schedule will run, for instance, every 1 or 2 weeks. • The specific time of the day when the information will be collected, its frequency, and the Starting and Ending dates for this schedule option.

SQL Server Agent Status

Additionally, this section of the wizard allows you to see the status of your SQL Server Agent. Take into account that SQL Secure uses the SQL Server Agent for data collection and grooming. This Agent is located in the SQL Server hosting the Repository Database. You can see in this section whether the Agent status is Started or Stopped.

Click **Next** to go to the following section to [Configure your email notifications](#).

View snapshot properties

To view the properties of a specific snapshot, go to the **Explore Permissions** view, expand the SQL Server from which the snapshot was taken, right-click the respective snapshot, and select **Properties** from the context menu. For more information about what properties you can see, go to [View Snapshot Properties](#).

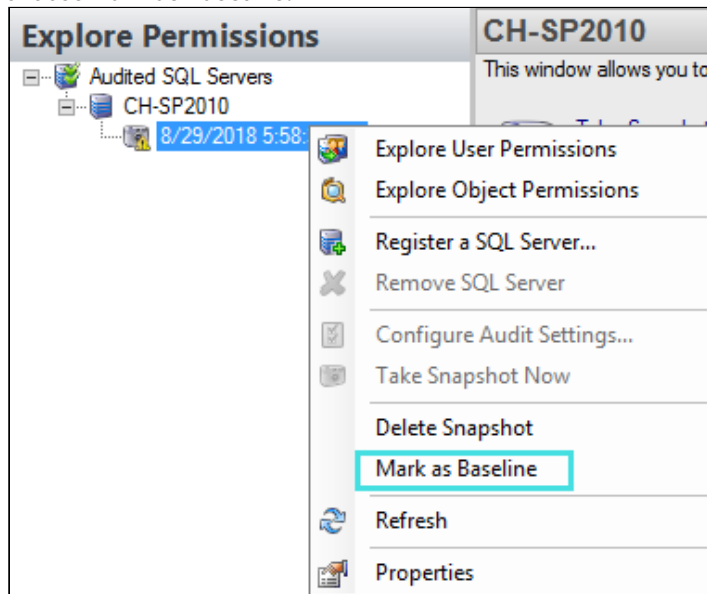
In this same view, you can also see the list of snapshots and baselines for a specific SQL Server. To see this information select your required server from the Audited SQL Servers tree and SQL Secure displays an **Audit History** section on the respective **Server Summary**. For more information about this view, go to [View single server summary](#).

Designate a baseline snapshot

A baseline snapshot will not be deleted in the normal IDERA SQL Secure grooming process.

To mark a snapshot as a baseline you can use any of the following paths (both available in the **Explorer Permissions** view):

- Expand the SQL Server instance of your Audited SQL Servers tree, right-click the respective snapshot, and choose **Mark as Baseline**.





- Click the respective SQL Server of your Audited SQL Servers tree. The **Audit History** section of the **Server Summary** lists all available snapshots (you can see here if any of them are marked as baseline or not). Right-click the selected snapshot and choose **Mark As Baseline**.
- Select an snapshot and from the menu toolbar select **Snapshots** and choose **Mark as Baseline**.

When you select a Snapshot with the option **Mark as Baseline**, a **Baseline Snapshot** window opens where you can enter a comment associated with the selected baseline. Click **OK** to continue.

Set snapshot grooming schedule

Grooming is the process of deleting audit snapshots from the IDERA SQL Secure Repository. Grooming allows you to keep only the permissions data you need for future reporting. SQL Secure allows you to schedule snapshot grooming at the enterprise and at the individual SQL Server instance levels. Keep in mind that baseline snapshots and snapshots associated with saved assessments cannot be groomed.

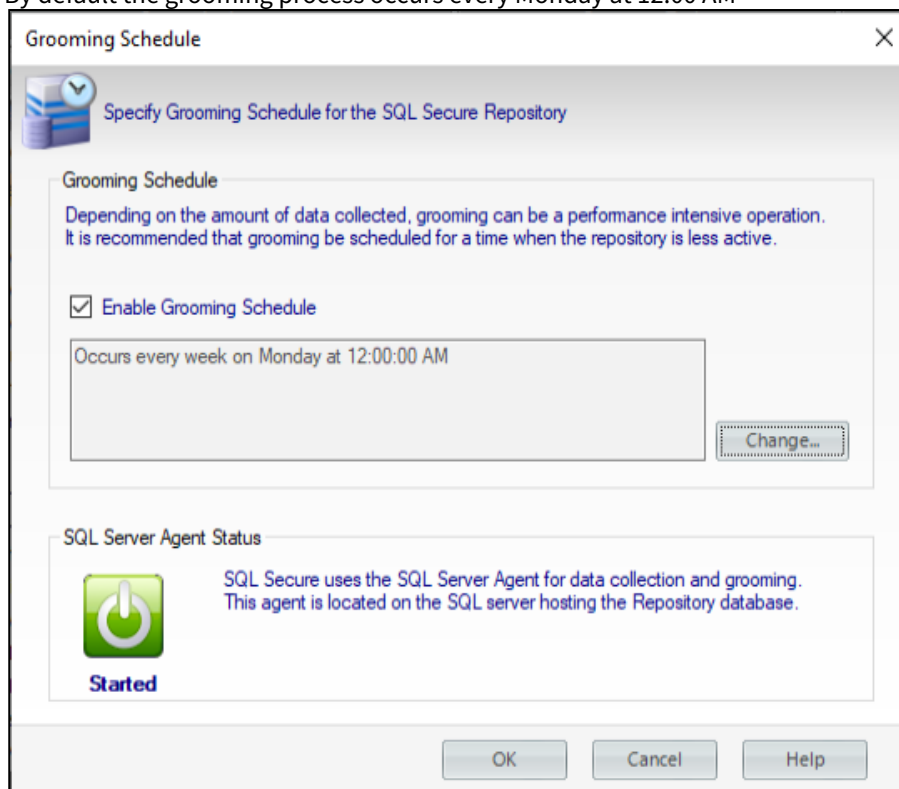
 Grooming should be scheduled for off-peak hours so that it does not interfere with your normal business operation. Depending on the amount of data collected, grooming can be a performance intensive operation.

 To keep a snapshot, mark it as a baseline. For more information, see [Designate a baseline snapshot](#).

You can configure the enterprise level grooming schedule on the **Grooming schedule** window.

To schedule the grooming schedule at the enterprise level:

1. Select from the menu toolbar **Snapshots > Grooming Schedule**. The **Grooming Schedule** window opens. By default the grooming process occurs every Monday at 12:00 AM



2. If you want to change the default grooming schedule, click **Change**. A **Job Schedule** window opens.
3. Edit the schedule according to your requirements. You can specify if you want to have a Daily, Weekly, or Monthly grooming schedule and define the respective frequency settings.
4. Click **OK** to save the schedule.

If you do not want to have a grooming schedule, you can disable the option **Enable Grooming Schedule**.

Additionally, the **Grooming Schedule** window informs you the SQL Server Agent Status of the SQL Server hosting the Repository Database. SQL Secure uses this agent for data collection and grooming.

i In addition to routine snapshot grooming, the grooming process deletes all the snapshots that are associated with any SQL Server instances you have removed from the SQL Secure Console

Set a grooming schedule at the SQL server instance level

Snapshot retention is the number of days SQL Secure will continue to store all your non-baseline audit snapshots in the SQL Secure Repository.

To schedule grooming at the SQL Server instance level:

1. Right-click the SQL Server instance you want to configure in the Audited SQL Servers tree of the **Explore Permissions** view and select **Properties**.
2. The **Audited SQL Server Properties** window opens, select the **Schedule** tab.
3. Specify the number of days between 1 and 10000 that SQL Secure will keep snapshots before grooming them.
4. Click **OK** to save changes.

4 Explore Security Settings

IDERA SQL Secure allows you to view the permission settings of individual users, roles, and objects, at a particular point in time, for each SQL Server instance that has been added to SQL Secure for auditing.

The **Explore Permissions** view allows you to review the following security information:

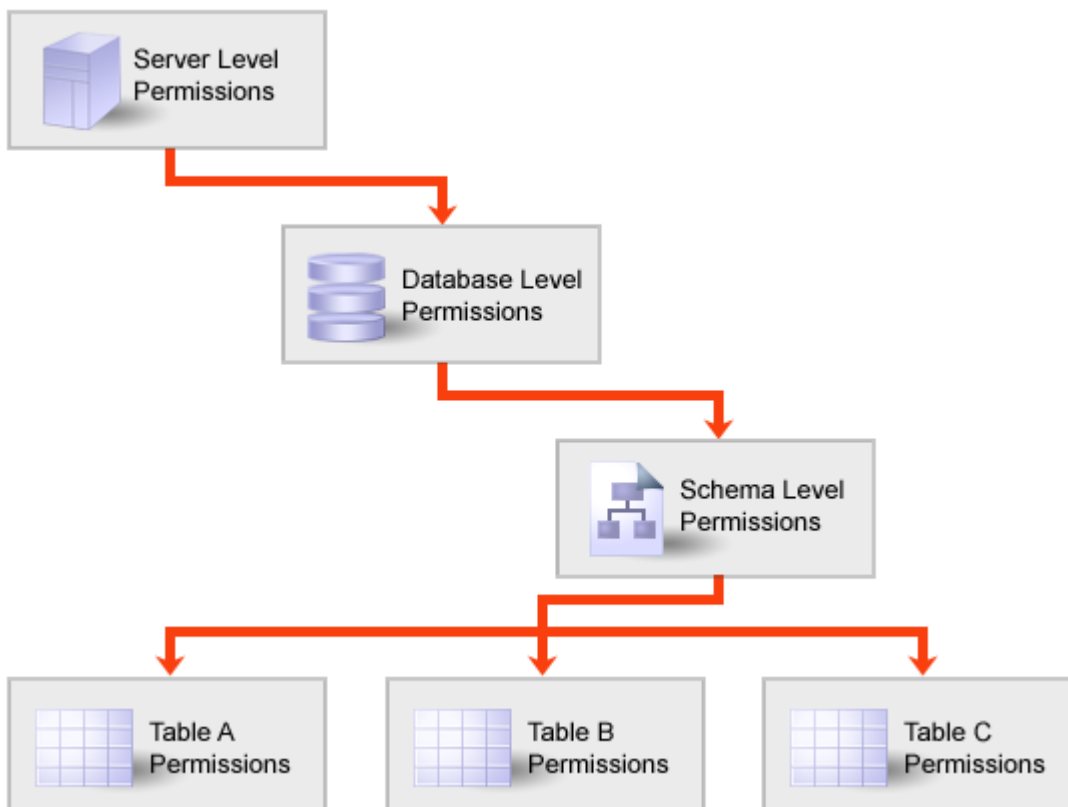
- Enterprise level permissions
- SQL Server level permissions
- Individual user permissions

Assigned permissions are permissions that are explicitly granted or denied to a user, group, or role for a particular server or database object. A user, group, or role can have more than one assigned permission. Effective permissions are the net effect of assigned permissions, permissions inherited from the group or role membership, and covering permissions (SQL Server 2005 and later).

4.1 Analyzing permissions

It is important to understand that when analyzing a user's permissions, SQL Secure shows multiple permissions when users have inherited object permissions from a parent role on the server. For example; User A has been given explicit delete permissions at the server, database, schema, and table levels. Your company is now restricting the rights to a particular table and you need to revoke User A's right to delete. To accomplish this task, revoke the user's right to delete at the particular table level and also at the parent levels.

The following illustration depicts an example permissions scenario:



4.2 Experiencing irregularities when searching user and object permissions

There may be times when it seems as though the permissions for a user or table have changed drastically when no changes have actually occurred. The following table lists some of the possible causes:

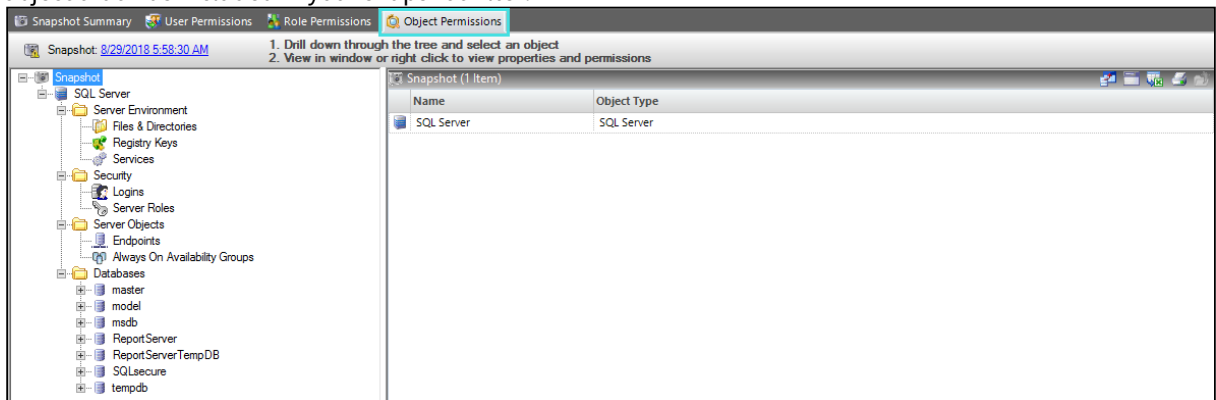
Cause	Solution
A user or table is deleted and then the same name is used again in the future.	Make sure that best practices are used when adding and deleting user and table names, or properly note the change to avoid confusion.
A user or table name is changed	Properly note the change to avoid confusion.
A user or table is deleted from the system	Properly note the change to avoid confusion.

SQL Secure allows you to audit all users and object permissions on SQL Server instances that have been registered with SQL Secure. For more information about SQL Server permissions, see Microsoft Books Online.

4.3 Explore object permissions

To view Object Permissions in IDERA SQL Secure, in the **Explore Permissions** view, follow these steps:

1. Click a snapshot from the Audited SQL Servers tree on the left.
2. Select the **Object Permissions** tab to explore SQL Server permission information for all database and server objects, as well as the password health of SQL logins.
3. Use the tree structure to navigate to the object for which you need permissions information, and click it.
4. Permissions information for that object will be displayed. You can view permissions information for every object that was included in your snapshot filter.



4.3.1 View the properties of the SQL Server object

From the **Object Permissions** tab, right-click the object you want more information on, and then select **Properties**. SQL Secure displays the **Object Properties** window and lists information relevant to the object type selected. For example, when you view Login Properties, you can review the security settings applied to this login plus its most recent password health.

i It could take up to a minute, depending on your specific configuration, to populate the **Object Properties** window.

According to the type of object you select, SQL Secure will display the object's Properties window. Click the following links to view a better description of the objects' specific properties window:

- [Database Properties](#)
- [SQL Login Properties](#)

4.3.2 View database properties

The IDERA SQL Secure **Database Properties** window displays the permissions information associated with the selected database. You can view:

- The owner and status of the selected database
- Whether the guest SQL Server login is enabled on this database
- The account or login (grantee) that was granted or denied permissions on the database
- The type of permission, and whether it was granted or denied
- The account or login (grantor) granting or denying this permission
- The source permission, object, and type from which the effective permission was inherited

You can view **Explicit Only** permissions or **Include fixed role and inherited** permissions, by checking the appropriate option and clicking **Show Permissions**. You can also save or print the database object permissions information by clicking the appropriate icon above the permissions table.

4.3.3 View SQL login properties

To access the **Login Properties** window for a specific login account in IDERA SQL Server, expand the Security folder in the Snapshot tree, select the **Logins** object, and then right-click the specific login on the table of the right and select **Properties**.

Use the **Login Properties** window to review the SQL login security properties for the selected login as well as its most recent password health.

Password health indicates whether or not the password associated with the account is considered weak. You can [configure how SQL Secure detects weak passwords](#).

✔ By default, the IDERA Level 2 and Level 3 [policy templates](#) enforce password health.

Possible password health states include:

Password health state	What it means
Blank	The password for this login is either blank or null, which means no password is required for authentication or successful connection to databases hosted by your audited SQL Server instances.
Matches login name	The password for this login matches the name of the login.
N/A	The password for this login was not checked, most likely because the login is a Windows user account.
OK	This login most likely has a strong password because the password does not match any of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.
Weak	The password for this login matches one or more of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.

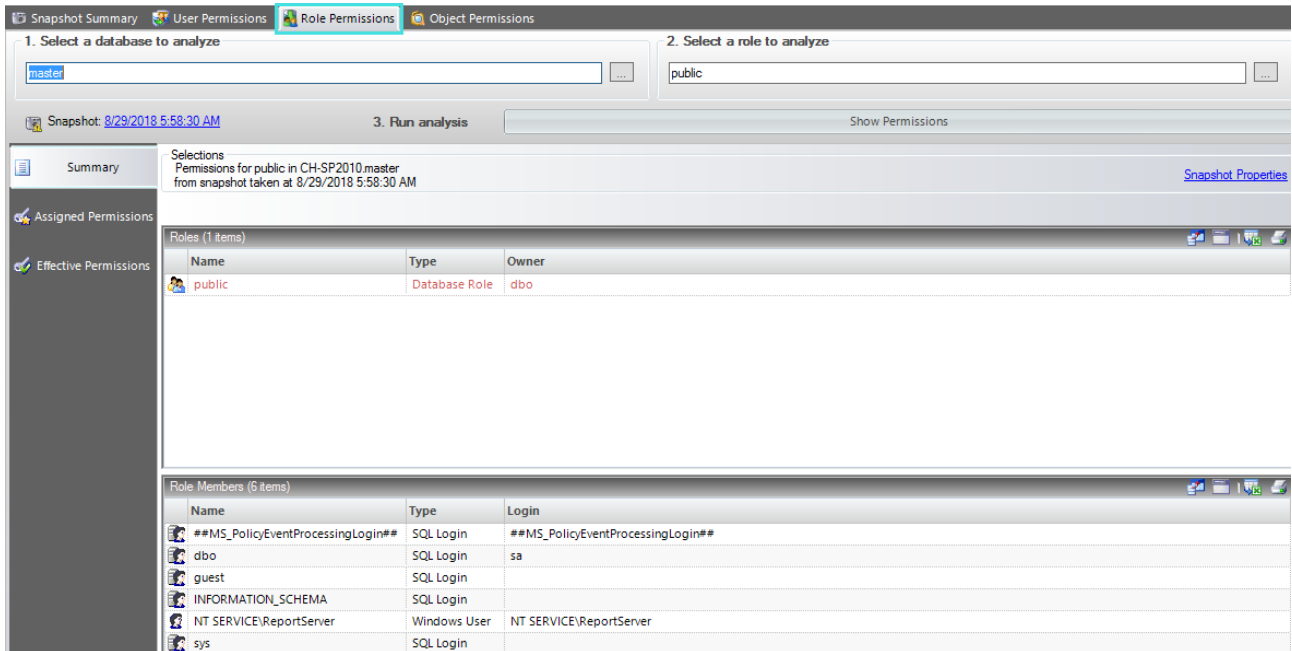
Available tabs on the Login Properties window

The **General** tab summarizes the key security settings and login properties typically found on the General, Server Role, and Status tabs in the Microsoft SQL Server client. For more information, see Microsoft Server Books Online.

The **Permissions** tab summarizes the key security settings and login properties typically found on the Explicit Permissions pane of the Securables tab of the Microsoft SQL Server client. For more information, see Microsoft Server Books Online.



4.4 Explore role permissions

The **Role Permissions** window of IDERA SQL Secure allows you to explore SQL Server permission information for specific roles on audited SQL Servers in your enterprise.



4.4.1 Find role permissions for a particular database

To view Role Permissions, in the **Explore Permissions** view follow these steps:

1. Click a snapshot from the Audited SQL Servers tree on the left.
2. Select the **Role Permissions** tab.
3. **Select a database to analyze** by either typing the database name into this box or by clicking the ellipsis button , selecting the database you want to analyze, and then clicking **OK**.
4. **Select a role to analyze** by either typing the name of the role into the field or by clicking the ellipsis button , selecting the role you want to analyze, and then clicking **OK**.
5. Click the **Show Permissions** button to see the results.

4.4.2 Change the audit data

To change which audit data you are exploring, click the hyperlink text, on top of the Summary section, that lists the date and time of the currently selected snapshot (by default, this date and time represents the last successful snapshot). SQL Secure opens a new window that displays all available snapshots, their status, and whether they are baseline snapshots or not.

Additionally, you can select any of the available snapshots and click **Properties** to access the respective Snapshot Properties window.

4.4.3 Role permissions summary

The IDERA SQL Secure **Summary** tab on the **Role Permissions** tab includes SQL Server permission settings for the role you specified in the Role Permissions search criteria.

Use the **Summary** tab to view the Role properties, role members, and information about their logins.

4.4.4 Assigned role permissions

The IDERA SQL Secure **Assigned Permissions** tab lists all the explicitly defined and inherited permissions that apply to calculating the role members' effective permissions.


You can view permissions information for the selected role and any parent role to which it belongs.

Usually this information is grouped by type of object. You can expand any type of object and see the properties of the objects that correspond to that type.

4.4.5 Effective role permissions


The IDERA SQL Secure **Effective Permissions** tab lists all the effective permissions the selected role has on objects in the target database. Effective permissions are the net effect of assigned permissions and permissions inherited from any parent roles.

Click **Calculate Effective Permissions** to view all the effective permissions the selected role has (at the time the data collection was taken) on the SQL Server instance being audited.

 Be aware that calculating effective permissions can take several minutes to run.

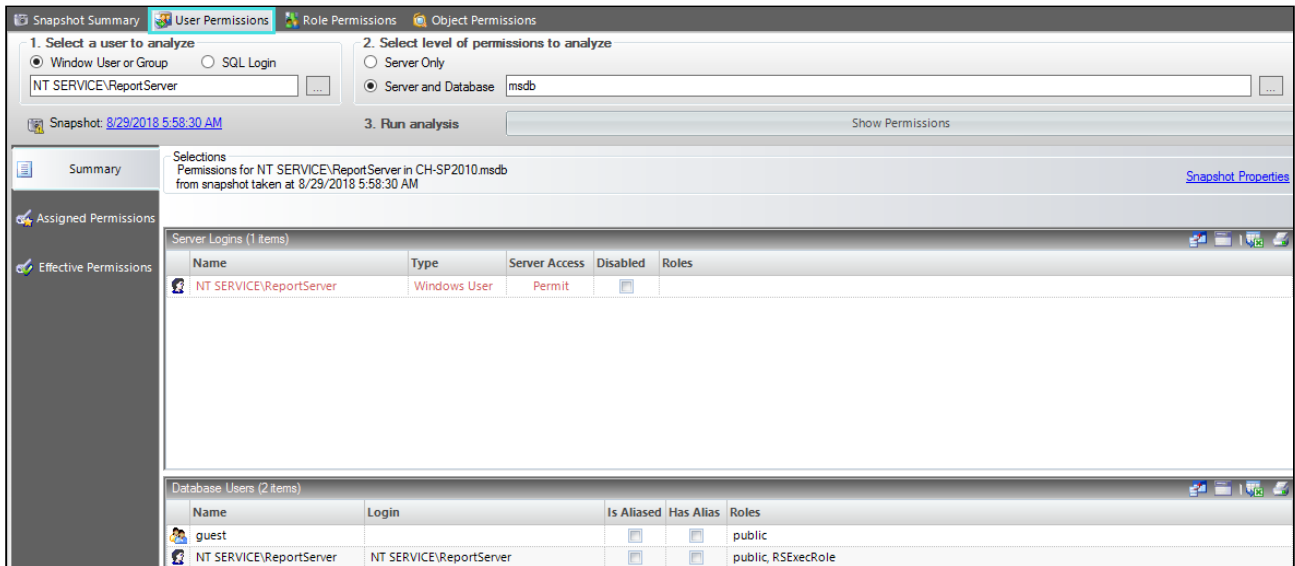
Available tabs

The **Effective Permissions** tab contains server and database permission information for the selected role. This includes the object names and types, the type of access granted to the role members, and who granted these permissions.

 You can save the permissions information to an Excel spreadsheet, print the permissions search, group or select columns to filter information. You can find these options on the top right section of the **Effective Permissions** section or by right-clicking any available object and choosing the appropriate option.



4.5 Explore user permissions

The IDERA SQL Secure Explore User Permissions window allows you to explore SQL Server permission information for specific users on audited SQL Servers in your enterprise.



4.5.1 Find the permissions associated with a particular user

To view **User Permissions**, in the **Explore Permissions** view follow these steps:

1. Click a snapshot from the Audited SQL Servers tree on the left.
2. Select the **Users Permissions** tab.
3. Select a user to analyze, it could be a **Windows User or Group** or **SQL Login**.
4. Type the account name of the user for whom you would like to search permissions or use the ellipsis button  to browse all users and groups contained in the collected audit data (snapshot).
5. To view about the options for filtering and finding your users, go to [Select a Windows Account](#) or [Select a SQL Server Login](#).
6. Select the level of permission to analyze, it could be a **Server Only** or a specific **Server and Database**. If you select **Server Only**, SQL Secure searches the permissions in all your current SQL Server instance. If you select **Server and Database**, you can type a specific database inside your SQL Server or click the ellipsis button  to see all available databases in your server.
7. On the Run analysis section, click **Show Permissions**. User Permission information displays on the bottom half of the window. The information is displayed on two sections: **Server Logins** and **Database Users**. The data is also separated into three tabs: **Summary**, **Assigned Permissions**, and **Effective Permissions**.

You can use the icons on the top right section, you have the following options:

- **Select Columns:** A new window displays where you can select the columns you want to display by checking the boxes.
- **Group By Box:** By clicking this option you can see a new section where you can drag a column header and crater boxes ordered by this column, you can select more than one column.
- **Save:** You can save the results on an Excel spreadsheet.
- **Print:** This option lets you print the results as a list.

 **Explore Security Settings**

For more information on permissions, see [Explore Security Permissions](#).


4.5.2 Change the audit data

To change which audit data you are exploring, click the hyperlink text that lists the date and time of the currently selected snapshot (by default, this date and time represents the last successful snapshot).

4.5.3 Check the password health of a user's login

Use the [Object Permissions tab](#) to check the password health of a specific SQL login. You can also [configure](#) how SQL Secure detects and enforces password health.

4.5.4 Select a Windows account

When you select the IDERA SQL Secure option **Windows User or Group** as the user to analyze, you can click the ellipsis button  to open the **Select Windows User** window to browse for all the Windows users contained in the snapshot you are exploring. In this window you can:

Search for a particular account

Your list may include many users and groups. SQL Secure makes the process of finding particular users easy. Click the **Filter** icon that is present in each column of the **Select Windows User** window, and then either select the group from the list, or click **Custom** to sort the list using conditions.

When you choose **Custom**, the **Enter filter criteria for Domain** window opens. In this window you can add as many conditions as you require for filtering your accounts. Click **Add a condition** and specify any of the following options for the operator:

Sorting Option	Description
Equals	On the Operand list select (Blanks), (DBNull), (Empty Text)
Does not equal	Select on of the options you have in the Operand list
Less than	Select on of the options you have in the Operand list
Less than or equal to	Select on of the options you have in the Operand list
Greater than	Select on of the options you have in the Operand list
Greater than or equal to	Select on of the options you have in the Operand list
Like	Select on of the options you have in the Operand list
Matches Regular Expression	Select on of the options you have in the Operand list
Starts with	Enter the first character or characters in the column to filter your list.
Contains	Enter a combination of letters or a name to filter your column list.
Ends with	Enter the last character or characters in the column to filter your list.


Sorting Option	Description
Does not start with	Enter the first character or characters in the column to omit from your listing.
Does not contain	Enter a combination of letters or name to omit from your list.
Does not end with	Enter the last character or characters in the column you want to omit from the listing.
Does not match	Enter the title you would like to omit from your column listing.
Not Like	Enter the name in the column you would like to omit from your column listing and all those names that are similar.

Then, specify the respective values in the **Operand** column.


Add or delete as many conditions as you want, and then click **OK**.

Search Active Directory

Alternatively, you can click **Browse Active Directory** to search Active Directory for the target Windows account or group. This action allows you to select the user or group from your Active Directory domain controller rather than from the selected snapshot. It is possible the user or group you select has not been granted permissions on the audited SQL Server instance.

 To successfully view the user permissions, ensure your login account has permission to access the Active Directory domain controller.

4.5.5 Select a SQL Server login

When you select to analyze a SQL Server Login through IDERA SQL Secure, you can click the ellipsis button  to open the **Select SQL Login** window that lists all of the SQL logins contained in the snapshot you are exploring.

You can filter this list by clicking the filter on the top right section of the **Type** column. You can filter by All, Custom, Blanks, NonBlanks, SQL Login.

If you select **Custom**, a new window for Enter filter criteria for type opens. In this window, you can add as many conditions as you require. To view more information about the operators for these conditions, you can go to [Select a Windows User](#).

Select the login whose permissions you want to explore, and then click **OK**.

4.5.6 User permissions summary

The IDERA SQL Secure **Summary** tab of the **User Permissions** Explorer contains SQL Server permission settings for the Windows account or SQL Server login you specified in the User Permissions search criteria.

Use the **Summary** tab to view which login permissions the individual user has, including the SQL Server roles to which the user belongs. You can print or save the results to an Excel spreadsheet.

4.5.7 Assigned user permissions

The IDERA SQL Secure **Assigned Permissions** tab lists all the explicitly defined permissions that apply to calculating the users' effective permissions. This includes groups, roles, and aliases; as well as, covering permissions available in SQL Server 2005 or later.

4.5.8 Effective user permissions

The IDERA SQL Secure **Effective Permissions** tab lists all the effective permissions the user has on server and database objects (contained within the audit filter criteria setup by the user). **Effective permissions** are the net effect of assigned permissions, permissions inherited from the group or role membership, and covering permissions (SQL Server 2005 and later).

Be aware that calculating effective permissions can take several minutes to run, depending on the number of permissions that have been granted and the complexity of your security model.

Click **Calculate Effective Permissions** to view all the effective permissions the selected user has (at the time the data collection was taken) on the SQL Server instance being audited.

Available tabs

The **Effective Permissions** tab contains server and database permission information for the selected user. This includes the object names and types, the type of access granted to the user, and who granted these permissions.

You can save the permissions information to an Excel spreadsheet or print the permissions search. To save or print the permissions information, click the grid on the top right section, and choose the appropriate option.

4.6 View all audited servers

When you click the **Audited SQL Servers** tree in IDERA SQL Secure, on the right side of the console you can review all SQL Server, Azure and Amazon audited instances, SQL Secure also gives you the option to view details of Decommissioned servers.

The screenshot shows the 'Audited SQL Servers' section with a table listing server details. Below it, the 'CH-SP2010 Databases' section shows a table of database information.

Server	Version	Last Audit	Audit Status
CH-SP2010	SQL Server 2012	8/29/20...	Warnings

Database	Status	Owner	Guest Enabled
master	Available	sa	Yes
model	Available	sa	No
msdb	Available	sa	Yes
ReportServer	Available	IDERAINFODEV\divitalobos	No
ReportServerTempDB	Available	IDERAINFODEV\divitalobos	No
SQLSecure	Available	IDERAINFODEV\divitalobos	No
tempdb	Available	sa	Yes

4.6.1 Audited SQL Servers

Server

Provides the name of the SQL Server instance.

Version

Provides the version of SQL Server that is running on each instance.

Last Audit

Provides the date and time when audit data was last collected for this instance.

Audit Status

Provides the status of the last snapshot taken for this instance.

4.6.2 Databases

According to the instance you select, you can see its SQL Server or Azure SQL database information.

Database

Provides the name of each database hosted on the selected instance.

Status

Provides the status of each database, such as whether the database is available or offline.

Owner

Provides the name of the owner for each database.

Guest Enabled

Indicates whether the guest account is enabled on the database.

On the top right section of each view, you have the following options:

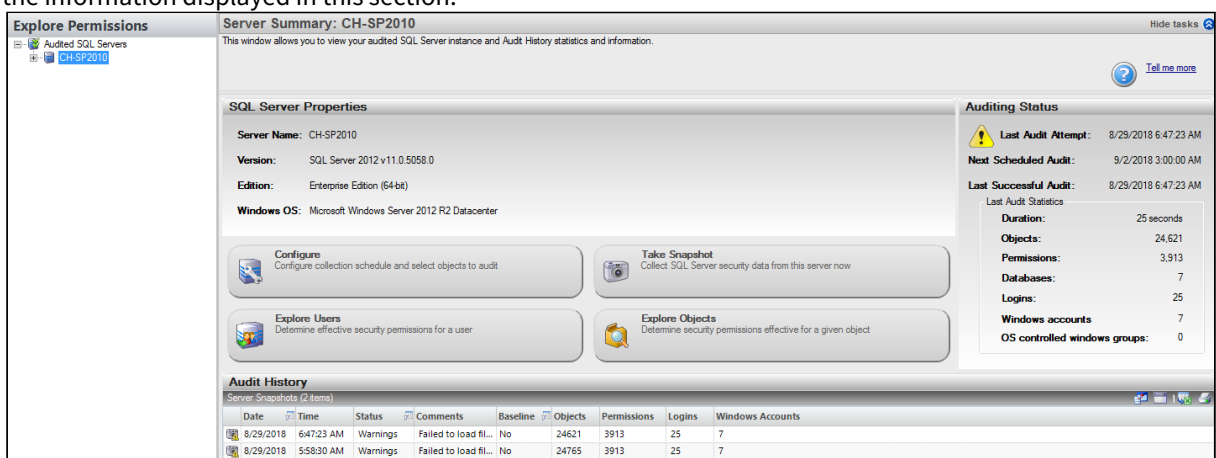
- **Select Columns:** A new window displays where you can select the columns you want to display by checking the boxes.
- **Group By Box:** By clicking this option you can see a new section where you can drag a column header and order your information according the selected column, you can select more than one column.

- **Save:** You can save the results on an Excel spreadsheet.
- **Print:** This option lets you print the results as a list.

4.7 View single server summary

To view IDERA SQL Secure information related to a specific SQL Server, click the server under the Audited SQL Servers tree, and on the right side of the console, SQL Secure displays the respective server summary information. The **Server Summary** window allows you to view the following:

- **SQL Server properties.** SQL Server Properties displays the name of the instance, the version and edition of the SQL Server being used, and the Windows Operating System the SQL Server instance is operating on.
- **Auditing status.** On the right section of the Server Summary, the Auditing Status displays the status of the last collection, the date and time of the next scheduled collection, and basic statistics for the latest snapshot.
- **Audit history.** Audit History provides detailed information about your snapshot. The table below describes the information displayed in this section.



4.7.1 Information contained in Audit History

The following table describes the information displayed in each of the columns:

Item	Description
Date	The date when the snapshot was taken.
Time	The time when the snapshot was taken.
Status	The status of the snapshot (audit data collection).
Comments	Description of any issues the collector encountered.
Baseline	Whether or not the snapshot is marked as a baseline.
Objects	The number of objects audited in the snapshot.
Permissions	The number of permissions collected in the snapshot.

Item	Description
Logins	The number of logins collected in the snapshot.
Windows Accounts	The number of Windows accounts collected in the snapshot.

4.8 View snapshot summary

The IDERA SQL Secure **Snapshot Summary** tab lists statistics and other information about the selected snapshot. To access this information, expand the SQL Server for which you want to see its snapshots and then select a specific Snapshot.

Each snapshot is a listing of permission settings on a SQL Server instance at a particular point in time. Snapshots help you assess and manage your security settings. This provides a powerful tool you can use to diagnose security problems and quickly see where changes occur.

The screenshot shows the 'Explore Permissions' window for a SQL Server instance named 'CH-SP2010'. The 'Snapshot Summary' tab is selected, showing the following details:

- Status:** Data Collection completed successfully, but the snapshot contains multiple warnings.
- Collection Time:** 8/29/2018 6:47:23 AM
- Duration:** 25 seconds
- Is baseline:** No
- Comment:**

The **Audit Summary** table is as follows:

Metric	Count
Objects:	24,621
Permissions:	3,913
Databases:	7
Logins:	25
Windows accounts:	7
OS controlled windows groups:	0
Weak Password Detection:	Enabled

Below the audit summary is a table of Windows Accounts with access to the SQL Server:

Icon	Domain	Account	Type	Access
	IDERAINFODEV	divillalobos	Windows User	SQL Login
	NT AUTHORITY	SYSTEM	Windows User	SQL Login
	NT SERVICE	MSSQLSERVER	Windows User	SQL Login
	NT SERVICE	ReportServer	Windows User	SQL Login
	NT SERVICE	SQLSERVERAGENT	Windows User	SQL Login
	NT SERVICE	SQLWriter	Windows User	SQL Login
	NT SERVICE	Winmgmt	Windows User	SQL Login

The **Snapshot Summary** displays the following sections:

- **Snapshot properties.** Gives general information about the snapshot, the status, the collection time, the duration, whether it is marked as a baseline snapshot or not, and any additional comments.
- **Audit Summary.** Displays the main summary information retrieved by the snapshot such as number of objects, permissions, databases, logins, windows accounts, OS controlled windows groups, and whether Weak Password Detection is enabled or not (Click [here](#) to enable/disable Weak Health Detection)
- **Accounts.** [Windows accounts](#), [OS Windows accounts](#), [Suspect Windows accounts](#), [Suspect OS Windows accounts](#), [Unavailable databases](#), and [Filters](#).

i Login counts may differ from what is displayed in SQL Server 2005 or later. This count displays the number of Server Principles collected. In SQL Server 2005 or later, Server Principles include Logins, Server Roles, and Certificates, while in SQL Server 2000, principles include only Logins.

4.8.1 Configuration before collecting snapshots

Before snapshots are taken, you must tell SQL Secure what permission data you would like to collect and when you want SQL Secure to collect it.

You can specify these settings in **Audited SQL Server Properties** window that you can access by clicking the **Configure Audit Settings** in the upper section of the **Snapshot Summary**.

Permission Data

Configure the permission data that it is most important to you to be taken by the snapshot.

To configure these settings, in the **Audited SQL Server Properties** window, select the **Filters** tab, then specify those filters that will help you collect the data you need.

For more information about defining filters, go to [Add Filter](#).

Snapshot schedule configuration

Snapshots capture security permission settings on SQL Server instances at configured intervals. At the scheduled time, a SQL Secure job is executed and data is collected from the SQL Server instance to the Repository database. This data set represents a single snapshot and is accessed directly by the SQL Secure Console. SQL Secure allows you to define when snapshots are taken.

You can specify these settings in the **Schedule** tab of the **Audited SQL Server Properties** window.

For more information of how to change the schedule collection time, go to [Schedule snapshots](#).

Scheduling snapshots

Consider taking snapshots on a routine, scheduled basis. Because snapshots are taken over time, they can be viewed to see when changes are made to user or object permissions.

4.8.2 Grooming Snapshots

Snapshots are managed through the grooming process. Grooming allows you to determine which snapshots should be deleted from the SQL Secure Repository. You can schedule grooming to occur on a routine basis, ensuring you keep only the snapshots you need. For more information, see [Set Snapshot Grooming](#).

Keep in mind

- Snapshots associated with saved assessments cannot be groomed.
- Snapshots that have been marked as baselines are not groomed

4.8.3 Mark a snapshot as a baseline

Baseline snapshots are snapshots that will not be deleted in the grooming process. To mark snapshots as baseline, you can right-click the snapshot and choose **Mark as Baseline**.

When a snapshot should be marked as baseline	Importance
When you take your first snapshot	To have a starting point to use to identify changes to permissions over time
At the end of the month, quarter, or year	To track compliance to your database security policies

When a snapshot should be marked as baseline	Importance
When you implement a new security model	To identify unwanted changes or issues with the new model
When you notice problems or irregularities in permission settings in a snapshot	To analyze the issue to correct problems and change permissions settings

✔ Viewing which snapshot is marked as baseline

To view which snapshot is marked as baseline, click the respective SQL Server. The **Audit History** section of the **Server Summary** properties displays a list of all snapshots in this server where you can find a **Baseline** column that informs you which snapshot is marked as a baseline and which ones are not.

4.8.4 Managing your snapshots

In addition to the setting above, you can perform the following actions with Snapshots.

- **Delete snapshots.** Right-click the respective snapshot (from the Audited SQL Servers tree or the **Audit History** of the **Server Summary**) and select **Delete Snapshot**.
- **Collect audit data manually.** Select **Take Snapshot Now** from the upper section of the **Snapshot Summary** or click the respective SQL Server, go to the **Snapshots** menu, and click the same option.

4.8.5 Resolve group names and group memberships across multiple domains

Using a single account to resolve group names and enumerate group memberships can be problematic when SQL Server grants permissions to accounts across multiple externally trusted domains.

In this situation, the server account specified on the Audited SQL Server Properties window should be an account that has been granted access to these external domains. This can be accomplished by either setting up two-way trusts between the account's domain and the external domains, or by creating pass-through accounts on all the external domains.

4.8.6 View Windows accounts in snapshot

The IDERA SQL Secure **Windows Accounts** tab lists the collected Active Directory users and groups that have permissions on SQL Server objects such as database tables. This tab also displays the associated domain, account name, type, and access information for each account.

Difference between Windows and OS Windows accounts

Windows Accounts

Users and groups that have access to SQL Server objects, such as database tables, either through association with a SQL login or permissions inherited from group membership

OS Windows Accounts

Users and groups that have access to OS objects, such as registry keys or files, either through direct permission assignment or group membership

4.8.7 View OS Windows accounts in snapshot

The IDERA SQL Secure **OS Windows Accounts** tab lists the collected Active Directory users and groups that have permissions on OS objects such as registry keys. This tab also displays the associated domain, account name, type, and access information for each account.

Difference between Windows and OS Windows accounts

Windows Accounts

Users and groups that have access to SQL Server objects, such as database tables, either through association with a SQL login or permissions inherited from group membership

OS Windows Accounts

Users and groups that have access to OS objects, such as registry keys or files, either through direct permission assignment or group membership

4.8.8 Identify Suspect Windows Accounts

The IDERA SQL Secure **Suspect Windows Accounts** tab lists the Windows user accounts about which SQL Secure was unable to retrieve information when the snapshot was taken. Windows accounts are Active Directory users and groups that have permissions on SQL Server objects.

For each suspect account, the following information is available:

Column	Description
Domain	Lists the domain the suspect account resides in
Account	Lists the name of the account
Type	Lists the type of account that is suspect

Additionally, in this tab you can set any of the following options available in the upper right corner of this section:

Option	Description
Show group by box	Allows you to organize the list by the column headers
Save as Excel File	Allows you to save your suspect windows accounts list to an Excel file
Print	Allows you to print out your list

- ✔ You can also click any column header and select to display All, Blanks, Non Blanks, or filter Custom criteria. For more information on how to add conditions to filter criteria for domain, click [here](#).

When SQL Secure considers an account suspect

A Windows account is considered suspect when SQL Secure cannot validate the account in Active Directory. Some common causes are:

- The user account has been deleted.
- The collection credentials do not have sufficient permissions to access Active Directory.
- A one-way trust exists between the domain of the collection credentials and the domain of the Windows account.
- The account is a well-known group, such as Everyone or Terminal Server User, whose membership is hidden by Active Directory and therefore cannot be collected.

- ✔ You can use a pass-through account to successfully collect Windows account information when encountering one-way trusted domains. A pass-through account is an account that has the same name and password as the account specified for gathering group membership information. A pass-through account does not require elevated Windows privileges in the trusted domain. For more information, search for "pass-through account" on the [Microsoft Help and Support Web site \(support.microsoft.com\)](https://support.microsoft.com).

4.8.9 Identify suspect OS Windows accounts

The IDERA SQL Secure **Suspect OS Windows Accounts** tab lists the Windows user accounts about which SQL Secure was unable to retrieve information when the snapshot was taken. OS Windows accounts are Active Directory users and groups that have permissions on OS objects such as registry keys.

For each suspect account, the following information is available:

Column	Description
Domain	Lists the domain the suspect account resides in
Account	Lists the name of the account
Type	Lists the type of account that is suspect

You can set one of the following options:

Option	Description
Group By	Allows you to organize the list by the column headers
Save as Excel File	Allows you to save your suspect windows accounts list to an Excel file
Print	Allows you to print out your list

- ✔ You can also click any column header and select to display All, Blanks, Non Blanks, or filter Custom criteria. For more information on how to add conditions to filter criteria for domain, click [here](#).

When SQL Secure considers an account suspect

An OS Windows account is considered suspect when SQL Secure cannot validate the account in Active Directory. Some common causes are:

- The user account has been deleted
- The collection credentials do not have sufficient permissions to access Active Directory
- A one-way trust exists between the domain of the collection credentials and the domain of the Windows account
- The account is a well-known group, such as Everyone or Terminal Server User, whose membership is hidden by Active Directory and therefore cannot be collected

- ✔ You can use a pass-through account to successfully collect Windows account information when encountering one-way trusted domains. A pass-through account is an account that has the same name and password as the account specified for gathering group membership information. A pass-through account does not require elevated Windows privileges in the trusted domain. For more information, search for "pass-through account" on the [Microsoft Help and Support Web site \(support.microsoft.com\)](https://support.microsoft.com).

4.8.10 Identify unavailable databases

The IDERA SQL Secure **Unavailable Databases** tab lists the databases about which SQL Secure was unable to collect SQL Server security data.

SQL Secure displays one of the following status messages for each database listed:

Status Message	Description
Database is loading or exclusively locked	SQL Secure is unable to audit the database because it is either being backed up or has been otherwise locked.
Suspect	SQL Secure is unable to report any data on the database.
Not Accessible	SQL Secure is unable to access the database. This could be because the database has been moved or deleted.

You can use any of the following options available in the upper corner of this section:

Option	Description
Show group by box	This button allows you to organize the list by the column headers
Save as Excel File	This button allows you to save your suspect windows accounts list to an Excel file
Print	This button allows you to print out your list

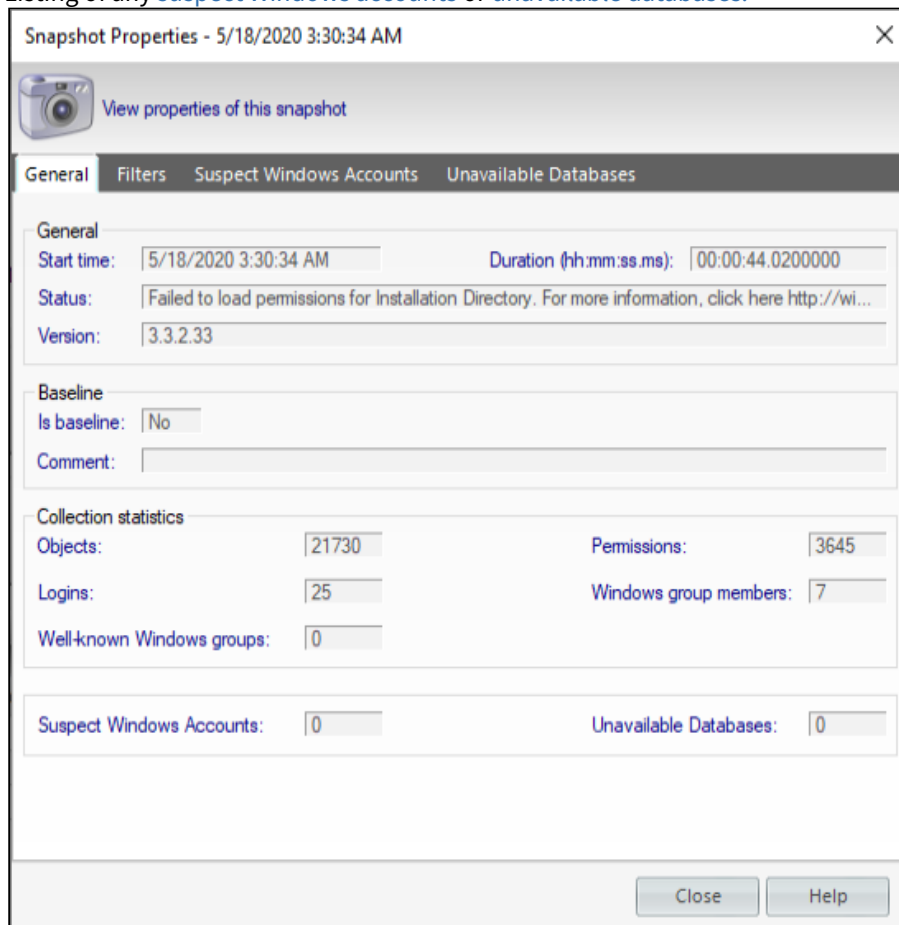
4.8.11 View filters for a snapshot

The IDERA SQL Secure **Filter** tab lists the collection filters that SQL Secure uses to collect audit data from your registered SQL Server instances and to create a snapshot. Each filter rule defines which data, such as permissions on user tables in a specific database, is collected and included in this snapshot. For more information about how filters work, see [Use Filters to Specify which Data is Collected](#).

4.9 View snapshot properties

The IDERA SQL Secure **Snapshot Properties** window contains detailed information about your snapshot, including:

- Date and time audit data was collected, and the status.
- Collection statistics.
- How audit data was [filtered](#) during collection.
- Listing of any [suspect Windows accounts](#) or [unavailable databases](#).



4.9.1 Access the Snapshot Properties window

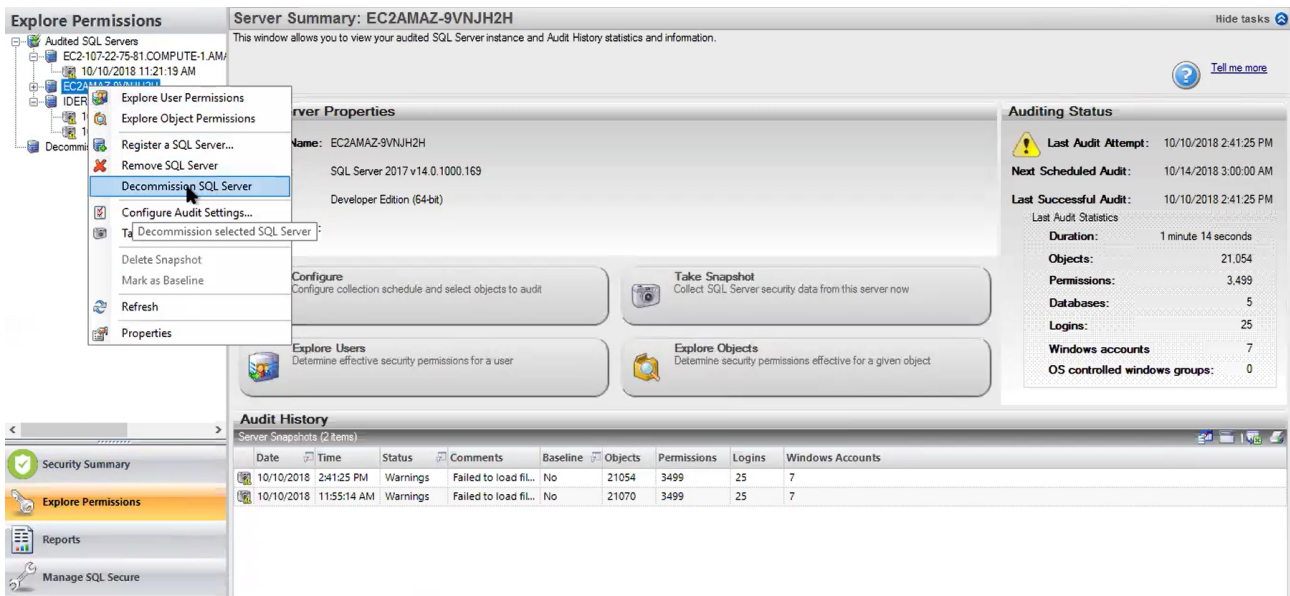
You can access the **Snapshot Properties** window by right-clicking a snapshot of the respective SQL Server under the Audited SQL Servers tree of the **Explore Permissions** view.

You can also access this window by clicking the relevant SQL Server, going to the **Audit History** section of the **Server Summary**, and right-clicking the respective Snapshot.

4.10 Decommissioned SQL Servers

On the Explore Permissions right side tree, you can find below all the audited SQL Servers the Decommissioned SQL Servers. You can decommission any monitored server once you do not need to perform any action on the server data, but you need to have the collected data available.

You can access the **Decommission SQL Server** option as by right-clicking the server you want to decommission.



The decommissioned servers are not taken into account on the number of servers allowed on each license.

Decommissioned servers let you check old snapshots and their properties, but you are not able to edit any of them. They will be listed at the end of the Server in Policy list.

You can **Approve** and **Publish** assessments with decommissioned servers. But **New Assessments** are not going to take into account decommissioned servers.

5 Assess Your Security Model

The IDERA SQL Secure **Security Summary** view allows you to check the status of your security policies at the enterprise and SQL Server instance levels. This view includes the overall policy status, a security report card that lists security risks, the settings of each of your SQL Server instances, and the associated user accounts.

5.1 Information available at the enterprise level

To view the **Security Summary** view at the enterprise-level, make sure you click **All Servers** in the Policy tree. This view includes the following enterprise-level information:

Summary tab

Policy Status

Displays the number of [security risks associated with the selected policy](#) and a break down of the risk levels.

Enterprise Security Report Card

Displays the [risks found on all SQL Server instances](#) assigned to the selected policy.

Server Summary

Displays the summary of SQL Servers included in the selected policy with statistics of the number of High, Medium, and Low Risks.

Settings tab

Allows you to [view and compare general and security-related settings](#) across your SQL Server instances.

Users tab

Lists the [user accounts and account settings](#) for the SQL Server instances assigned to the selected policy.

5.2 Information available the server level

To view the **Security Summary** view at a server-level, make sure you click the respective SQL Server in the left tree. This view includes the following server-level information:

Summary tab

Server Status

Displays the [number of security risks found](#) by your policy on the selected SQL Server instance.

Server Security Report Card

Displays all [risks discovered on a specific SQL Server instance](#) assigned to the selected policy.

SQL Server Info

Displays the main information of the selected SQL Server such as name, when last data was collected, version, edition, and Windows OS.

Settings tab


Lists the [general and security-related settings](#) for your SQL Server instance.

Users tab

Lists the [user accounts and account settings](#) for the associated SQL Server instance.

5.3 Analyze enterprise security

The IDERA SQL Secure Enterprise **Security Summary** displays the status of your security policies at the enterprise level. By default, SQL Secure displays the **All Servers** policy assessment.

 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.

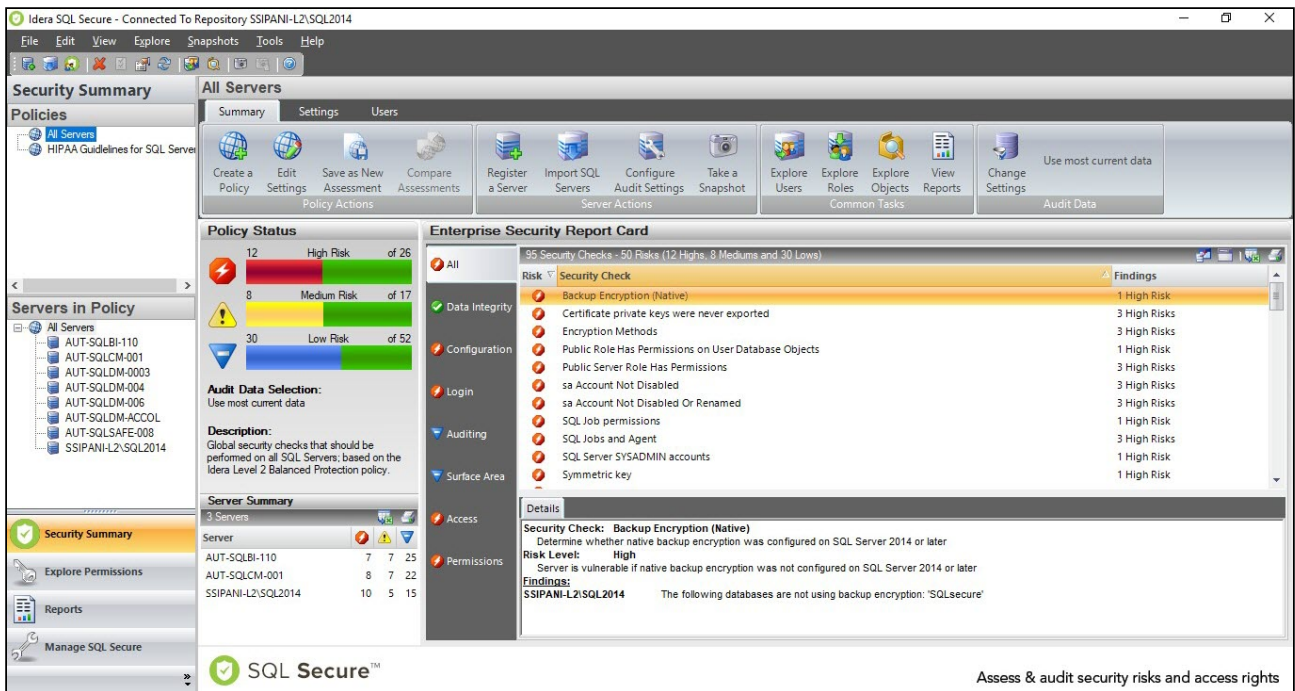
To see the Enterprise **Security Summary** for a specific policy, select the policy from the Policies tree on the Security Summary view.

The following information is available from the Enterprise Security Summary:

- [Enterprise Security Report Card](#)
- [Enterprise Security Settings](#)
- [Enterprise Security Users](#)

5.3.1 View Enterprise Report Card

Through the IDERA SQL Secure **Security Summary** view you can see the **Enterprise Report Card** for a selected policy. For this purpose click the respective policy in the Policies tree and in the **Summary** tab you can see this report card.



The **Enterprise Security Report Card** lists the security check findings for all SQL Server instances that have been assigned to the selected policy.

The default view of the **Enterprise Security Report Card** displays all the associated security findings, from highest to lowest risk, as configured in your policy. You can select security risk categories along the left side of the report card to filter the report card accordingly.

The **Enterprise Security Report Card** lists the number of security check violations found along with the level of risks associated with these findings. This status includes findings for all servers associated with the selected policy.

✔ You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

In addition to the **Summary** tab, the following tabs can provide detailed information on the associated risks:

Settings

The **Settings** tab lists the detailed SQL Server settings associated with the SQL Server instances assigned to your policy. On the top right section you can select between two view options, **By Setting** or **By Server**.

Users

The **Users** tab lists the security settings of the SQL Server logins and Windows accounts associated with the SQL Server instances assigned to your policy.

5.3.2 View settings across all servers

The IDERA SQL Secure Security Summary view allows you to see the Settings for a selected policy. For this purpose click the respective policy in the Policies tree, then go to the **Settings** tab.

The screenshot shows the IDERA SQL Secure interface. The main window is titled "CIS for SQL Server 2019::CH-SP2010". The left sidebar contains a "Policies" tree with "CIS for SQL Server 2019" selected, and a "Servers in Policy" section showing "CH-SP2010". The main area is divided into a "Summary" tab (selected), a "Settings" tab, and a "Users" tab. The "Settings" tab displays a table of security settings for all SQL Servers (1 item) associated with the policy. The table is sorted by setting. The bottom right of the window shows the "SQL Secure" logo and the text "Assess & audit security risks and access rights".

Setting	CH-SP2010
SQL Server	CH-SP2010
Authentication Mode	SQL Server and Windows Authentica...
Operating System	Windows Server 2019 Standard 100...
Version	15.0.20005
Edition	Enterprise Evaluation Edition (64-bit)
Collected	5/18/2020 3:30:34 AM
Objects	21730
Permissions	3645
Logins	25
Windows Group Members	7
Login Audit Mode	Failed logins only
Proxy	No
C2 Audit Trace	No
Cross DB Ownership Chaining	No
Case Sensitive	No
System Table Updates	No
Remote Admin Connections	No
Remote Access	Yes
Scan for Startup Procs	No
SQL Mail Xps	N/A*
Database Mail Xps	No

Note: N/A* in this case indicates that Data was not collected either due to an error, warning or no data available.

The **Settings** tab lists the security settings collected for all SQL Server, Azure, and Amazon instances associated with this policy. By default, SQL Secure sorts this data **By Setting** which you can change to **By Server** in the grid menu bar located on the top right section.

When you double-click a specific SQL Server instance from the **Servers in Policy** tree, SQL Secure displays the individual **Settings** tab for the selected instance.

- ✓ You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

Information displayed on the SQL Servers tab

SQL Server


Name of the SQL Server instances.

Authentication Mode

Login permission type.

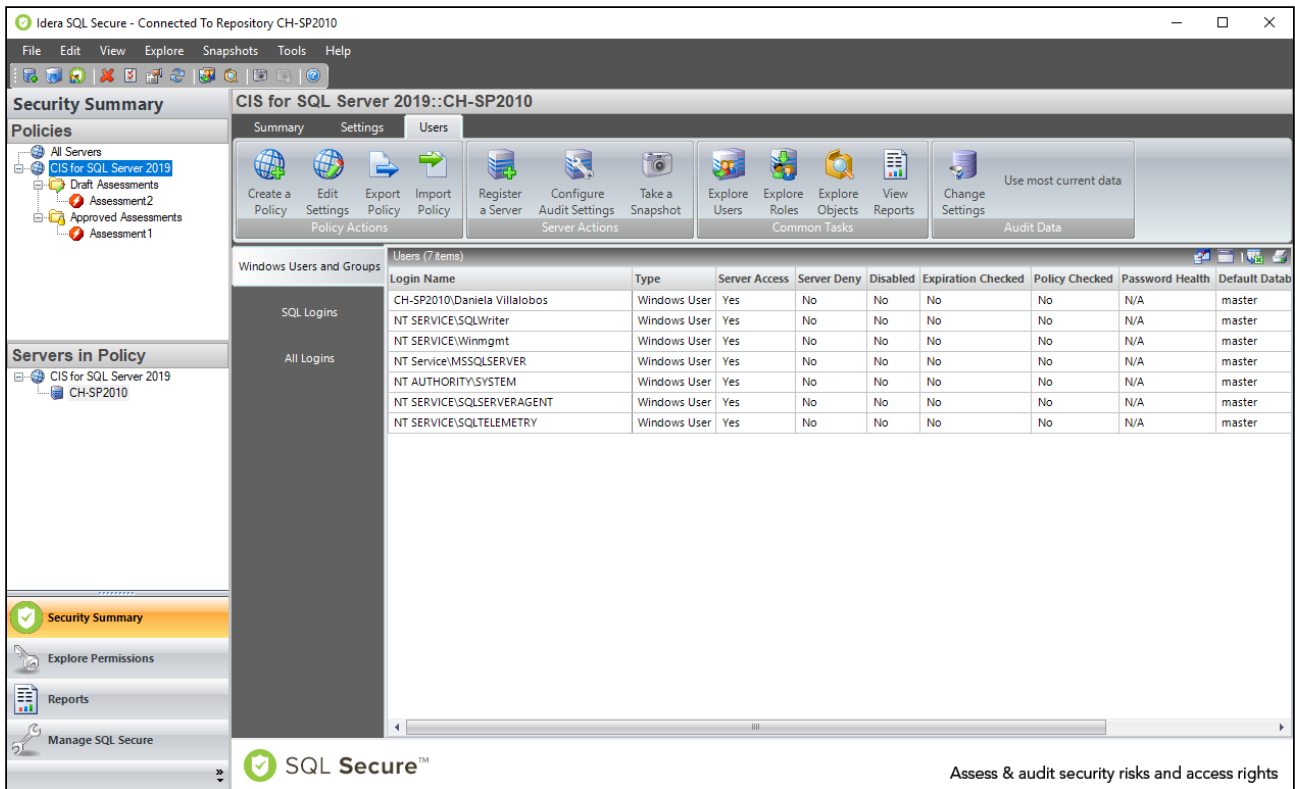
Operating System

Name and specifications about Server Operating System

 On the Operating System Information you can find **N/A** for "Not Aplicable" and **N/A*** for "Data not collected either due to an error, warning, or no data available"

5.3.3 View user security across all servers

The IDERA SQL Secure **Security Summary** view allows you to see the Users for a selected policy. For this purpose click the respective policy in the Policies tree, then go to the **Users** tab.



The **Users** tab allows you to view all the user accounts associated with the SQL Server, Azure, and Amazon instances assigned to the selected policy.

✔ You can right-click on a particular user account row and select **Show Permissions** to explore user permissions and see more detailed security information about the selected account.

Information displayed on the Users tab

You can filter user information according the login type along the left side of the Users list, after you select a login category (Windows Users and Groups, Azure AD Users and Groups, SQL Logins, and All Logins), you can see the following information:

Login Name

The full login name of the associated account

SQL Server

Name of the SQL Server instance the login is associated with

Type

Login permission type (Windows Group or SQL Login)

Server Access

Whether or not the user has access on the SQL Server instance

Server Deny

Whether or not the user is denied access to the SQL Server instance

Disabled

Whether or not the user account is disabled

Expiration Checked

Whether or not the password expiration is checked

Policy Checked

Whether or not the associated policy is checked for this user account

Password Health

Whether or not the password associated with the account is considered weak. You can configure [how SQL Secure detects weak passwords](#). Possible password health states include:

Password health state	What it means
Blank	The password for this login is either blank or null, which means no password is required for authentication or successful connection to databases hosted by your audited SQL Server instances.
Matches login name	The password for this login matches the name of the login.
N/A	The password for this login was not checked, most likely because the login is a Windows user account.
OK	This login most likely has a strong password because the password does not match any of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.
Weak	The password for this login matches one or more of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.

Default Database

The database that this login connects to and queries when no other database is specified

Default Language

The language that is set as the default for the user account



You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

5.4 Analyze server security

The IDERA SQL Secure **Security Summary** view displays the status of your security policies at the instance level. To see the Server Security Summary for a policy, expand the corresponding policy node in **Servers in Policy** tree, and then select the target SQL Server instance.

The following tabs are available from the Server Security Summary:

- [Server Security Report Card](#)
- [Server Security Settings](#)
- [Server Security Users](#)

5.4.1 View Server Report Card

To view the IDERA SQL Secure **Server Security Report Card** for a specific SQL Server instance, go to the **Security Summary** view, and then select the respective instance from the **Servers in Policy** tree, SQL Secure displays this report card in the **Summary** tab.

The **Server Security Report Card** lists the security checks evaluated for the selected SQL Server instance.

The default view of this report card displays all the associated security findings, from highest to lowest risk, as configured in your policy. You can select security risk categories along the left side of the report card to filter the report card accordingly.

The **Server Status** section lists the number of security check violations found along with the level of risk associated with these findings. This status reflects the findings for the selected instance only.

The **SQL Server Info** section displays the most important information for the selected instance like the time when the audit data was collected, the version, edition, and Windows OS on the respective instance.

✔ You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

Get more information on discovered risks

The following tabs of SQL Secure can provide detailed information on the associated risks:

Settings

The [Settings tab](#) lists the detailed SQL Server settings associated with the selected SQL Server instance.

Users

The [Users tab](#) lists the SQL Server logins and Windows accounts associated with the SQL Server instance.

5.4.2 View settings on this instance

To view the settings for a specific SQL Server instance in IDERA SQL Secure, go to the **Security Summary** view, select the respective instance from the **Servers in Policy** tree, then go to the **Settings** tab.

The **Settings** tab lists the security settings collected for the selected SQL Server instance. By default, SQL Secure sorts this data **By Setting** name. To sort by instance name, click **By Server** in the grid menu bar located in the upper right section.

- ✔ You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

5.4.3 View user security on this instance

To view the users for a specific SQL Server instance in IDERA SQL Secure, go to the **Security Summary** view, select the respective instance from the **Servers in Policy** tree, and then go to the **Users** tab.

The **Users** tab allows you to view all the user accounts associated with the selected SQL Server instance.

✔ You can right-click on a particular user account row and select **Show Permissions** to explore user permissions and see more detailed security information about the selected account.

You can filter user information according the login type along the left side of the Users list, after you select a login category (Windows Users and Groups, SQL Logins, and All Logins), you can see the following information:

Login Name

The full login name of the associated account

Type

Type of login (SQL Login, Windows User, Windows Group, and Certificate Mapped Login)

Server Access

Whether or not the user has access on the SQL Server instance

Server Deny

Whether or not the user has denied access to the SQL Server instance

Disabled

Whether or not the user account is disabled

Expiration Checked

Whether or not the password expiration is checked

Policy Checked

Whether or not the associated policy is checked for this user account

Password Health

Whether or not the password associated with the account is considered weak. You can configure how [SQL Secure detects weak passwords](#). Possible password health states include:

Password health result	What it means
Blank	The password for this login is either blank or null, which means no password is required for authentication or successful connection to databases hosted by your audited SQL Server instances.
Matches login name	The password for this login matches the name of the login.
N/A	The password for this login was not checked, most likely because either the login is a Windows user account or weak password detection is disabled.


Password health result	What it means
OK	This login most likely has a strong password because the password does not match any of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.
Weak	The password for this login matches one or more of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.

Default Language

The language that is set as the default for the user account

Default Database


The database that this login connects to and queries when no other database is specified

-  You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

5.5 Define policies for custom assessments

Policies are security standards implemented to monitor specific risks on one or more SQL Server instances. IDERA SQL Secure uses policies to assess your SQL Server security models by performing specific security checks. Each security check has a default value and associated risk level based on known industry regulations and best-practices. You can add, remove, or edit security checks in any policy.

Once a policy is configured, SQL Secure examines your audit data and displays any found risks in the **Security Summary** view. You can create multiple security policies, allowing you the flexibility to have several different standards that cover the varying security needs of your environment. Consider using the built-in [policy templates](#) to create policies that enforce industry standards and best-practice security guidelines.

 You can configure SQL Secure to send email notifications as security risks are found. For example, you can receive notifications when high and medium risks are found. For more information, see [Email Notifications](#).

You can perform the following actions:

- [Create Policies](#)
- [Edit Policy Settings](#)
- [Import Policies](#)
- [Export Policies](#)

5.5.1 Use policy templates to harden your security model

You can use the IDERA and industry-standard policy templates built into 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 Standards 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 Standards and Technology (NIST) - SQL Server 2014 Instance STIG.

DISA-NIST STIG for SQL Server 2016

Enforces security check settings derived from the Defense Information Systems Agency (DISA) National Institute of Standards and Technology (NIST) - SQL Server 2016 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 inefficient 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	Maturati on 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	<ul style="list-style-type: none"> SA account has a blank password Any SQL Server login has a blank password Public server role has been granted permissions


IDERA Level	Maturity Level	Security Level	Types of SQL Server Instances	Types of Business	Regulatory Model	Unique Security Checks
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	<ul style="list-style-type: none"> • Sysadmins own trustworthy databases • Public server role has been granted permissions • File permissions on executables are not acceptable • SQL logins have weak passwords

IDERA Level	Maturity Level	Security Level	Types of SQL Server Instances	Types of Business	Regulatory Model	Unique Security Checks
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	<ul style="list-style-type: none"> • 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 an acceptable level

5.5.2 Add new policy

The **Create Policy** wizard allows you to add a custom policy to IDERA SQL Secure. As a part of this wizard, you will name the policy, select the security checks and their associated risk levels, assign the SQL Server instances you want to assess, and specify additional internal review notes to include in the Risk Assessment report. When you create a policy, you can choose one of the built-in templates based on known industry regulations and best-practices.

To open the **Create Policy** wizard, click **Create a Policy** on the Policy Actions ribbons of any of the tabs of the **Security Summary** view.

 Individual SQL Server instances can belong to multiple security policies. For more information on adding SQL Server instances to a policy, see [Assign SQL Servers to Policy](#).

When you open the **Create Policy** wizard you need to configure the following actions:

- [Select policy template](#)
- [Specify policy properties](#)
- [Select Security Checks](#)
- [Assign SQL Servers to policy](#)
- [Enter internal review notes](#)
- [Review policy summary](#)

How policies work

By default, SQL Secure assesses the latest audit data for each SQL Server instance, using the policy's security check criteria to identify issues. You can also choose to assess audit data from a historical point in time.

Review the policy assessment in the following ways:

Security Summary

The [Enterprise and Server Security Summary](#) displays the results of your policy assessments.

Reports

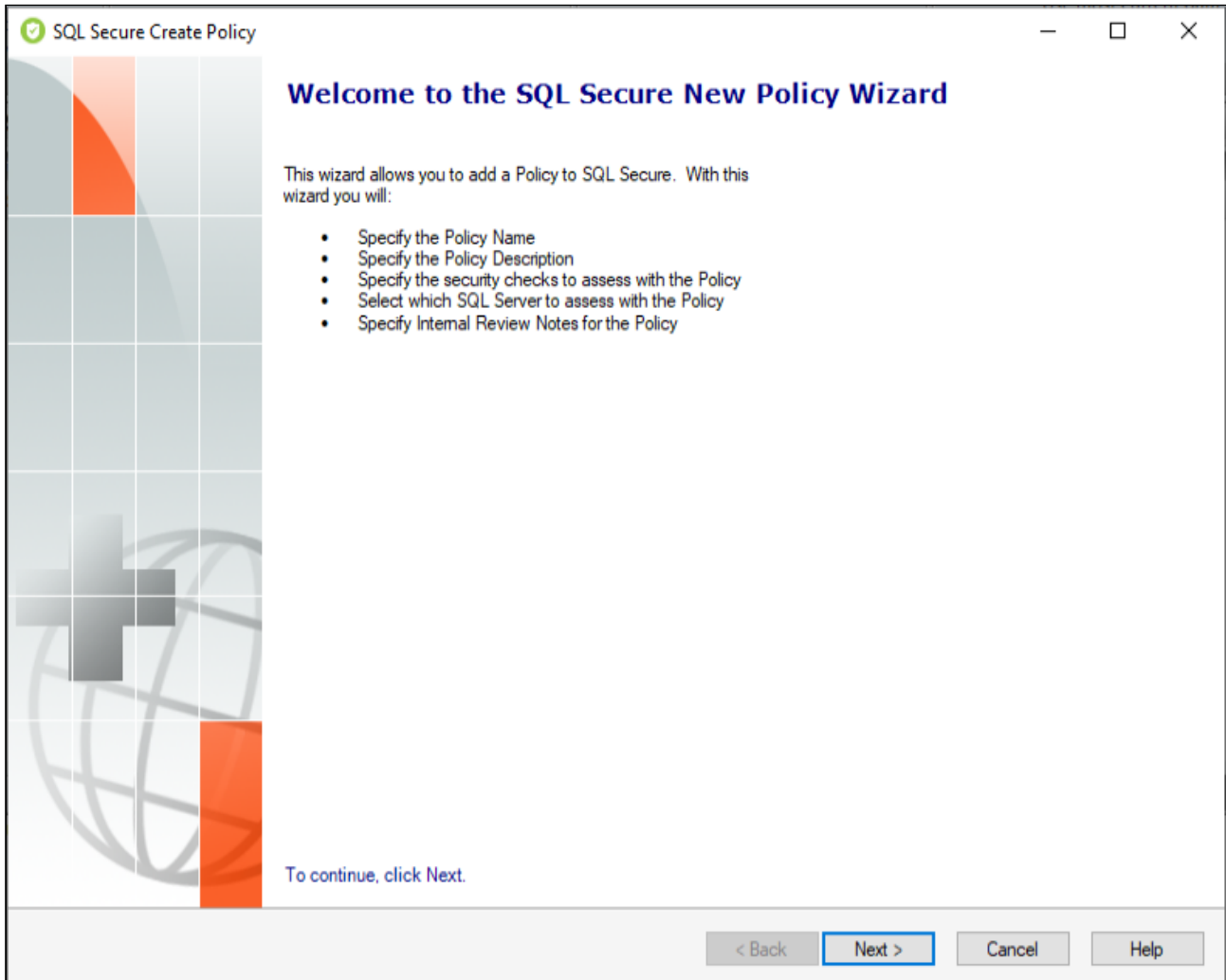
You can [run reports](#), such as the Risk Assessment report, on the policy or on specific SQL Server instances.

Email Notifications

You can [configure email notifications](#) to be sent, at each scheduled snapshot, when security risks are encountered.

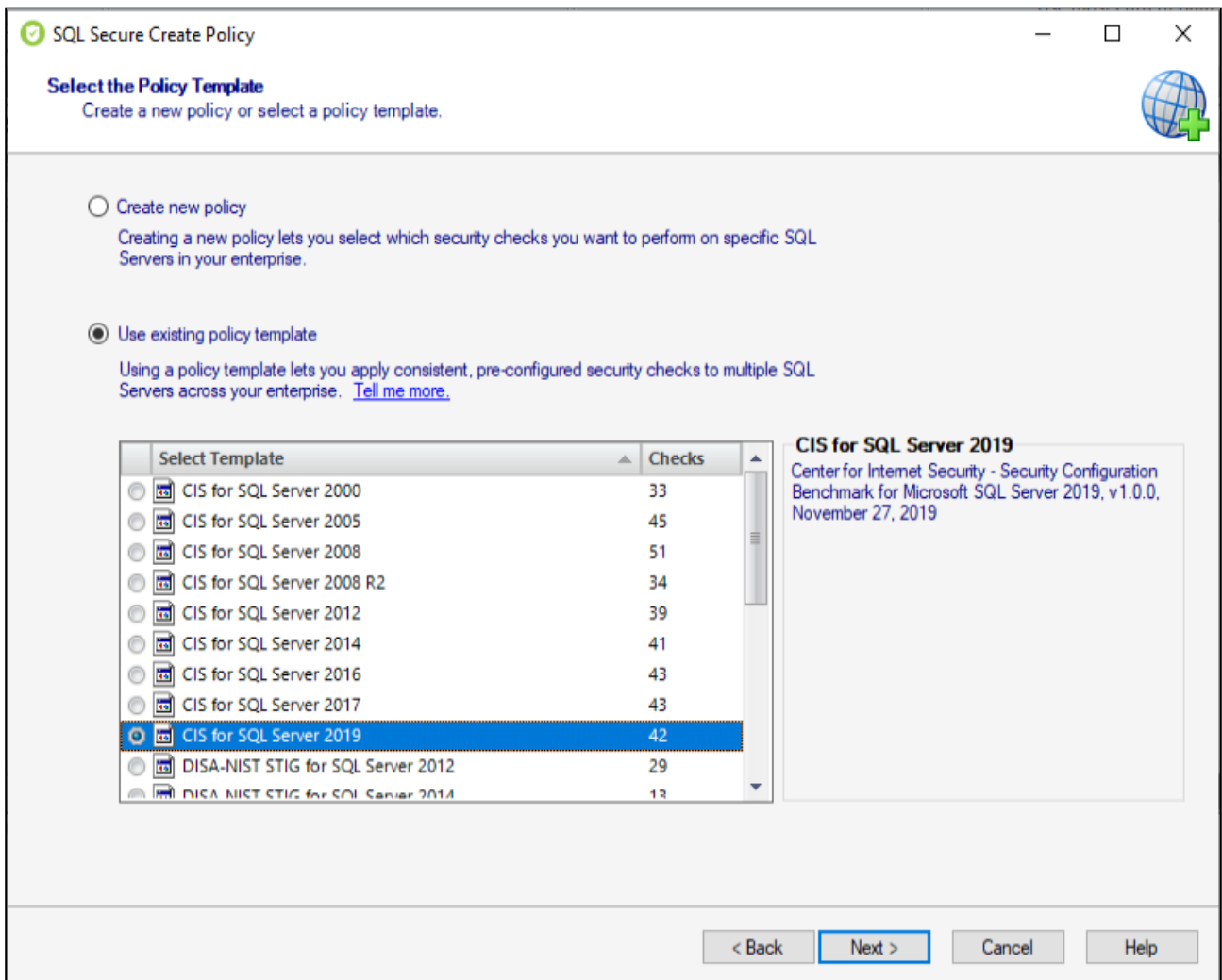
Select policy template

When you open the **Create Policy** wizard in IDERA SQL Secure, the Welcome window of this wizard opens, click **Next** to access the first section: **Select the Policy Template**.



The **Select the Policy Template** section allows you to choose between:

- Create a new policy
- Use existing policy template



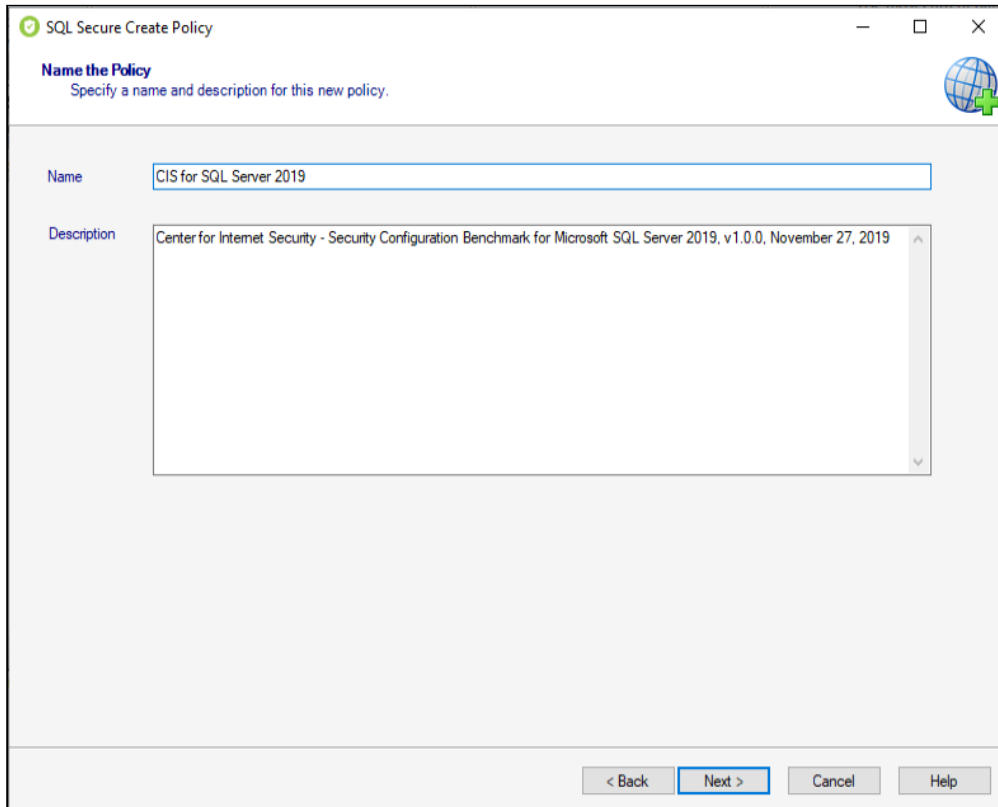
Policy templates are boilerplate policies whose security check definitions reflect known industry regulations and security best-practices. Although, you may choose to start with a template, you can later add, edit, or remove security checks as needed. For more information, see how [policy templates](#) can help you achieve your SQL Server security goals.

You can also create policy templates by exporting configuration settings from a specific policy to an XML file. Then, you can later reuse these settings by creating new policies based on this template. For more information, see [Import Policy](#).

Click **Next** to go to the [Name the Policy](#) section.

Specify policy properties

The **Name the Policy** section allows you to give your policy a name and a description. It is important to give your policies easily identifiable names and provide descriptions that help you select the appropriate policy during audits. The policy name and description can be changed later using the [Policy Properties](#) window.



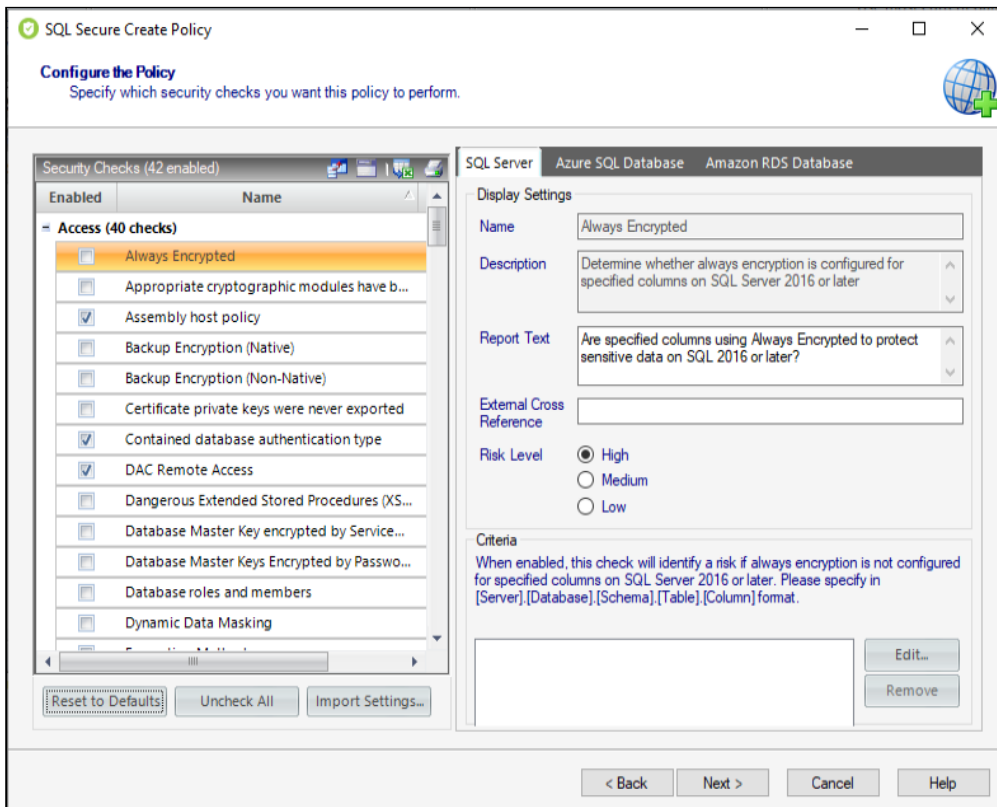
The screenshot shows a window titled "SQL Secure Create Policy" with a close button in the top right corner. Below the title bar, the section is titled "Name the Policy" with the instruction "Specify a name and description for this new policy." and a globe icon with a green plus sign. The "Name" field contains the text "CIS for SQL Server 2019". The "Description" field is a text area containing the text "Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2019, v1.0.0, November 27, 2019". At the bottom of the window, there are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

Click **Next** to go to the [Configure the Policy](#) Section.

Select security checks

The **Configure the Policy** section allows you to 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, Azure and Amazon 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](#)

i 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.

Access Security Checks

The Access Security Checks audit access and configuration for data access and objects. These security checks take a look at data encryption, remote access, and other object configurations that allows access to the data or object.

The Access Security Checks available on the **Configure the Policy** section are the following:

Name	Description
Always Encrypted	Determine whether always encryption is configured for specified columns on SQL Server 2016 or later.
Appropriate cryptographic modules have been used to encrypt data.	Check all databases for appropriate encryption algorithms.
Assembly host policy	Determine whether there are user defined assemblies with host policy other than SAFE.
Backup Encryption (Native)	Determine whether native backup encryption was configured on SQL Server 2014 or later.
Backup Encryption (Non-Native)	Determine whether non-native backups were configured on SQL Server 2008 or later.
Certificate private keys were never exported	Determine whether certificate private keys were not exported.
Contained database authentication type	Determine whether authentication type set to Mixed mode with contained databases exists on instance.
DAC Remote Access	Determine whether the Dedicated Administrator Connection is available remotely.
Dangerous Extended Stored Procedures (XSPs)	Determine whether permissions have been granted on dangerous Extended Stored Procedures (XSPs).
Database Master Key encrypted by Service Master Key	Check for databases where the Database Master Key is encrypted by Service Master Key. The Service Master Key is the root of SQL Server's Encryption Hierarchy. As such, there can only be one service master key per SQL Server instance. The service master key is used to protect (encrypt) other keys, mainly the database master keys. It cannot be used directly to encrypt data.

Name	Description
Database Master Keys Encrypted by Password	Returns Database Master Keys passwords that are stored in credentials within the database. This is simply a count of Database Master Keys, use the family_guid value for each credential to check against the backup file to identify the database the credential is associated with.
Database roles and members	Shows information about database roles and their members.
Dynamic Data Masking	Determine whether dynamic data masking is configured for specified columns on SQL Server 2016 or later.
Encryption Methods	Determine whether there are encryption keys with algorithms other than supported.
Files On Drives Not Using NTFS	Determine whether all SQL Server files are stored on drives that use NTFS.
Fixed Roles Assigned To public Or guest	Determine whether public or guest are members of any fixed database roles.
Guest User Enabled	Determine whether Guest user access is available on the SQL Server.
Linked server is running as a member of sysadmin group	Determine whether linked servers are running as a member of sysadmin group.
NTFS Folder Level Encryption	Determine whether NTFS folder level encryption is configured for Windows folders.
Operating System Version	Determine whether the Operating System version is at an acceptable level.
Public role permissions	Determine whether the public roles have permissions to user defined objects.
Remote Access	Determine whether Remote Access is enabled on the SQL Server.
Required Administrative Accounts Do Not Exist	Determine whether the required administrative accounts exist on the SQL Server.
Row-Level Security	Determine whether row-level security is configured for specified tables on SQL Server 2016 or later.

Name	Description
Server roles and members	Shows information about server roles and their members.
Signed Objects	Determine whether a digital signature has been added to sepcified stored procedure, function, assembly or trigger on SQL Server 2008 or later.
SQL Job permissions	Determine whether SQL Server Agent account or job proxies are members of local Administrators group.
SQL Jobs and Agent	Determine whether job steps are running on behalf of proxy account.
SQL Server Browser Running	Determine whether the SQL Server Browser is running on the SQL Server.
SQL Server database level encryption	Determine the encryption status of all databases in the instance.
Startup Stored Procedures	Determine whether there are unapproved stored procedures set to run at startup on the SQL Server.
Startup Stored Procedures Enabled	Determine whether the "Scan for startup stored procedures" configuration option has been enabled on the SQL Server.
Startup Stored Procedures permissions	Determine whether startup stored procedures can be run or are owned by accounts without sysadmin permissions.
Stored Procedures Encrypted	Determine whether user stored procedures are encrypted on the SQL Server.
Symmetric key	Determine whether master, msdb, model or tempdb have user-created symmetric keys.
Symmetric Keys Not Encrypted with a Certificate	Lists all symmetric keys in a database that are not the database master key and are encrypted by either password or another symmetric key.
Sysadmins Own Trustworthy Databases	Determine whether any trustworthy databases are owned by system administrators on SQL Server 2005 or later.
Transparent Data Encryption	Determine whether transparent data encryption is configured for any databases on SQL Server 2008 or later.

Name	Description
Unacceptable Database Ownership	Determine whether if a database is found with an unacceptable owner.
User Defined Extended Stored Procedures (XSPs)	Determine whether unapproved user-defined Extended Stored Procedures (XSPs) exist.

Auditing Security Checks

The Auditing Security Checks take a look at auditing configuration for SQL Server databases and instances to ensure logs and events are running and properly setup.

The Auditing Security Checks available on the Configure the Policy section are the following:

Name	Description
C2 Audit Trace Enabled	Determine whether C2 Audit Trace is enabled on the SQL Server.
DISA Audit Configuration	The DISA/NIST specifications require a specific SQL Server trace to exist for auditing SQL Server use. Check to see if there are any traces outside of the existing default trace. Audit specification for DISA tracking to be used in place of a trace if trace does not exist.
Implement Change Data Capture	List databases that have Change Data Capture enabled.
Login Audit Level	Determine whether the SQL Server login auditing configuration is acceptable.
SQL Server Audit is Configured for Logins	SQL Server Audit is configured to record both failed and successful logins. This check is only valid for Enterprise Edition SQL Server 2008 R2 and above.
SQL Server Audit is in use	This check returns the name, status and target file locations of any SQL Server Audits that are on the server. In order for the results to be compliant with GDPR specifications, the audit should be enabled and recording data.

Configuration Security Checks

The Configuration Security Checks analyze the configuration and settings of the database, instance, or server in the policy.

The Configuration Security Checks available on the Configure the Policy section are the following:

Name	Description
Analysis Services Running	Determine whether Analysis Services (OLAP) is running on the SQL Server.
Asymmetric Key Size	Check to verify that the encryption key length for asymmetric keys is 2048 bits and above. It is recommended that asymmetric keys are not created in the system databases (master, model, msdb, and tempdb).
Auto_Close set for contained databases	Check to see if Auto_Close is set for contained databases. Auto_close should be set to OFF for these databases.
Backups compliance with RTO and RPO requirements	Check for most recent backups and validate that they are in compliance with Recovery Point Objective (RPO) and Recovery Time Objective (RTO) policies.
BUILTIN/Administrators Is sysadmin	Determine whether BUILTIN/Administrators is a member of the sysadmin fixed server role.
CLR Enabled	Determine whether the CLR is Enabled on the server.
Common criteria compliance	Determine whether the Common criteria compliance is enabled.
Data Files On System Drive	Determine whether data files exist on the system drive.
Database-level Firewall Rules	Determine whether unapproved database-level firewall rules have been configured on Azure SQL Database.
Databases Are Trustworthy	Determine whether any unapproved databases are trustworthy on SQL Server 2005 or later.
Default Trace Enabled	Determine whether the Default Trace Enabled on the server.
Full-Text Search Running	Determine whether Full-Text Search is running on the SQL Server.

Name	Description
HADR is configured	Return each database that is configured in an HA configuration, and its current state. Possible configurations are Availability Groups, Database Mirroring or Log Shipping. Replication is not considered an HA technology for the purposes of this check, as it is not applied to the entire database.
Hide Instance Option is set	'HideInstance' determines whether or not the SQL instance can be discovered by the SQL Server Browser service. Check examines registry setting for 'HideInstance'. If 1, the instance is hidden.
Integration Services	Determine whether permissions have been granted on Integration Services stored procedures.
Linked servers are configured	Determine whether linked servers are configured.
Max Number of concurrent sessions	Determine maximum number of allowed concurrent sessions.
Maximum number of error log files	Determine whether the Maximum number of error log files is more than 11.
Ole automation procedures	Determine whether the Ole automation procedures are enabled.
Other General Domain Accounts	Determine whether general domain accounts added to the instance.
Replication Enabled	Determine whether replication is enabled on the SQL Server.
sa Account Not Disabled	Determine whether the SQL Server sa account has been disabled on SQL Server 2005 or later.
sa Account Not Disabled Or Renamed	Determine whether the SQL Server sa account has been disabled or renamed on SQL Server 2005 or later.
Sample Databases Exist	Determine whether sample databases exist on the SQL Server.
Server Is Domain Controller	Determine whether the Server is a domain controller.
Server-level Firewall Rules	Determine whether unapproved server-level firewall rules have been configured on Azure SQL Database.
Shutdown SQL Server on Trace Failure	Determine if traces exist that will not cause SQL Server to shut down if the trace encounters an error.

Name	Description
SQL Agent Mail	Determine whether the SQL Server Agent has been configured to allow email.
SQL Mail Or Database Mail Enabled	Determine whether SQL Mail or Database Mail has been enabled on the SQL Server.
SQL Server Installation Directories On System Drive	Determine whether SQL Server installation directories are on the system drive.
SQL Server Version	Determine whether the SQL Server software is at an acceptable minimum version.
System Table Updates	Determine whether the "Allow Updates to System Tables" configuration option is enabled on SQL Server 2005 or later.
Transport Layer Security	Return a bit value indicating whether SQL Server is requiring encryption at the protocol layer. (0 for no, 1 for yes.) This indicates if the server is requiring encryption for connections over the network, though clients can still request an encrypted connection to SQL Server even if the server is not requiring it.
Unauthorized Account Check	Determine whether unauthorized accounts have sysadmin privileges on the SQL Server or has SoD roles like "CONNECT ANY DATABASE", "IMPERSONATE ANY LOGIN", "SELECT ALL USER SECURABLES", "ALTER ANY COLUMN MASTER KEY", "ALTER ANY COLUMN ENCRYPTION KEY", "VIEW ANY COLUMN MASTER KEY DEFINITION", "VIEW ANY COLUMN ENCRYPTION KEY DEFINITION", "ALTER ANY SECURITY POLICY", "ALTER ANY MASK", "UNMASK".
User created 'sa' account does not exist	Ensure that a user account has not been created, named 'SA'.
VSS Writer Running	Determine whether VSS Writer is running on the SQL Server.
xp_cmdshell Enabled	Determine whether the xp_cmdshell extended stored procedure is enabled on SQL Server 2005 or later.
xp_cmdshell Proxy Account Exists	Determine whether a Proxy Account is enabled on the SQL Server.

Data Integrity Security Checks

The Data Integrity Security Checks monitor that SQL Secure data is not missing or out of date.

The Data Integrity Security Checks available on the Configure the Policy section are the following:

Name	Description
Audit Data Is Stale	Determine whether the nearest snapshot collection occurred within an acceptable timeframe from the selected date
Baseline Data Not Being Used	Determine whether all audit data for the selected timeframe is from baseline snapshots
Snapshot May Be Missing Data	Determine whether all audit data for the selected servers is complete and without warnings
Snapshot Not Found	Determine whether all servers in the policy have valid audit data for the selected timeframe

Login Security Checks

Login Security Checks ensure credentials from users and permissions, meet the organization's policy, and alert if there are changes.

The Login Security Checks available on the Configure the Policy section are the following:

Name	Description
Active Directory Helper Login Account Not Acceptable	Determine whether the Active Directory Helper account is acceptable
Analysis Services Login Account Not Acceptable	Determine whether the Analysis Services account is acceptable
Blank Passwords	Determine whether any SQL Logins have blank passwords
DISTRIBUTOR_ADMIN Login	Determine whether DISTRIBUTOR_ADMIN account should be deleted.
Ensure Windows BUILTIN Groups are not SQL Logins	Determine whether the Windows BUILTIN groups and accounts are not SQL logins. Windows BUILTIN groups have broad memberships and should not be used to get access to the SQL Server Database Engine instance.
Ensure Windows Local Groups are not SQL Logins	Determine whether Windows Local groups are used as logins. Allowing local Windows groups to be used as SQL Logins creates a loophole where an OS administrator could add users and give access to SQL Server instances.
Full-Text Search Login Account Not Acceptable	Determine whether the Full-Text Search Service account is acceptable
Integration Services Login Account Not Acceptable	Determine whether the Integration Services account is acceptable
Notification Services Login Account Not Acceptable	Determine whether the Notification Services account is acceptable
Orphaned users	Determine whether any orphaned users exist in databases.
Reporting Services Login Account Not Acceptable	Determine whether the Reporting Services account is acceptable
sa Account Has Blank Password	Determine whether the SQL Server sa account has a blank password

Name	Description
sa Account Not Using Password Policy	Determine whether password policy is enforced on the sa account
SQL Authentication Enabled	Determine whether SQL Authentication is allowed on the SQL Server
SQL Logins not using Must Change	Ensure that all SQL Authentication Logins have the 'must_change' option set to ON.
SQL Logins Not Using Password Expiration	Determine whether password expiration is enabled for all SQL Logins
SQL Logins Not Using Password Policy	Determine whether password policy is enforced on all SQL Logins
SQL Server Agent Login Account Not Acceptable	Determine whether the SQL Server Agent Service account is acceptable
SQL Server Browser Login Account Not Acceptable	Determine whether the SQL Server Browser Service account is acceptable
SQL Server Service Login Account Not Acceptable	Determine whether the SQL Server Service account is acceptable
SQL Server SYSADMIN accounts	Determine whether SQL SYSADMIN accounts that are in the local Administrator role for the physical server.
Suspect Logins	Determine whether suspect logins exist on the SQL Server
Unauthorized SQL Logins Exist	Determine whether unauthorized SQL Logins have been created on the SQL Server
VSS Writer Login Account Not Acceptable	Determine whether the VSS Writer account is acceptable
Weak Passwords	Determine whether any SQL login passwords match the login name or a list of common and restricted passwords.

Permissions Security Checks

Permission Security Checks control the permissions for objects and roles.

The Permissions Security Checks available on the Configure the Policy section are the following:

Name	Description
Agent Job Execution	Determine whether only administrators can execute SQL Agent CmdExec Jobs
ALTER TRACE Permission Granted To Unauthorized Users	Determine whether unauthorized users have been granted the ALTER TRACE permission on SQL Server 2005 or later
CONTROL SERVER Permission Granted To Unauthorized Users	Determine whether unauthorized users have been granted the CONTROL SERVER permission on SQL Server 2005 or later
Database File Owners Not Acceptable	Determine whether SQL Server database files have unapproved owners
Database File Permissions Not Acceptable	Determine whether users have unapproved access to SQL Server database files
Database Files Missing Required Administrative Permissions	Determine whether the required administrative accounts have access to all database files
Direct Access Permissions	Check for logins that have had server-level permissions granted directly to them.
Ensure public role is not granted access SQL Agent proxies in msdb database	Determine whether the public role is granted access to SQL Agent proxies
Everyone Database File Access	Determine whether the Everyone group has access to SQL Server database files
Everyone System Table Access	Determine whether the Everyone group has read access to system tables on the SQL Server
Executable File Owners Not Acceptable	Determine whether SQL Server executable files have unapproved owners
Executable File Permissions Not Acceptable	Determine whether users have unapproved access to SQL Server executable files

Name	Description
Executable Files Missing Required Administrative Permissions	Determine whether the required administrative accounts have access to all executable files (any .exe or .dll file)
Integration Services Roles Have Dangerous Security Principals	Determine whether dangerous security principals belong to any SQL Server Information Services (SSIS) database roles.
Integration Services Roles Permissions Not Acceptable	Determine whether unapproved roles have been granted permissions on an Integration Services stored procedure.
Integration Services Users Permissions Not Acceptable	Determine whether unapproved users have been granted permissions on an Integration Services stored procedure.
Limit Propagation of access rights	Check for users that have GRANT_WITH_GRANT_OPTION, as they can grant those rights to other users.
Public Database Role Has Permissions	Determine whether the public database role has any permissions
Public Role Has Permissions on User Database Objects	Determine whether the public database role has been granted permissions on user database objects.
Public Server Role Has Permissions	Determine whether the public server role has been granted permissions
Public Server Role only granted default Microsoft permissions	Determine that the Public Server Role only has default permissions granted by Microsoft. In keeping with the principle of least privileges, the public server role should not be used to grant permissions at the server scope as these would be inherited by all users.
Registry Key Owners Not Acceptable	Determine whether registry keys that can affect SQL Server security have unapproved owners
Registry Key Permissions Not Acceptable	Determine whether users have unapproved access to registry keys
Registry Keys Missing Required Administrative Permissions	Determine whether the required administrative accounts have access to all SQL Server registry keys
Sysadmins Own Databases	Determine whether any databases are owned by a system administrator

Surface Area Security Checks

Surface area represents potential attack vector that can be compromised. The Surface Area Security Checks examine the security settings for configurations and components on the database and instance to reduce the surface area vector.

The Surface Area Security Checks available on the Configure the Policy section are the following:

Name	Description
Ad Hoc Distributed Queries Enabled	Check if Ad Hoc Distributed Queries is enabled. If configured_value is 1, then SQL Server will enable the configuration on startup. If value_in_use is 1, it is currently enabled.
Common TCP Port Used	Determine whether TCP is using a common port on the SQL Server
Cross Database Ownership Chaining Enabled	Determine whether Cross Database Ownership Chaining is enabled on the SQL Server
FILESTREAM is configured	Return the FILESTREAM configuration state for the server, and which databases contain FILESTREAM file groups, if any.
Integration Services Running	Determine whether Integration Services is running on the SQL Server
Notification Services Running	Determine whether Notification Services is running on the SQL Server
Reporting Services Running	Determine whether Microsoft Reporting Services is running on the SQL Server
SQL Server Agent Running	Determine whether the SQL Server Agent is running on the SQL Server
SQL Server Browser Running	Determine whether the SQL Server is hidden from client computers
Unapproved Protocols	Determine whether unapproved protocols are enabled on the SQL Server

Assign SQL Servers to Policy

The **Assign SQL Servers to the Policy** window allows you to choose the registered SQL Server instances you want to audit and add them to the policy you are creating. Each registered SQL Server instance can belong to multiple policies.

SQL Secure Create Policy

Assign SQL Servers to the Policy
Specify which SQL Server instances you want to audit with this policy.

Select SQL Servers to include in this Policy

- All SQL Server Instances
- All SQL Server 2000 Instances
- All SQL Server 2005 Instances
- All SQL Server 2008 Instances
- All SQL Server 2012 Instances
- All SQL Server 2014 Instances
- All SQL Server 2016 Instances
- All SQL Server 2017 Instances
- All SQL Server 2019 Instances
- All Azure SQL Database
- All Amazon RDS

Select SQL Server Instances

Audited SQL Server
<input checked="" type="checkbox"/> CH-SP2010

< Back Next > Cancel Help

To select SQL Server instances you can select from the options that group SQL Server versions or choose **Select SQL Server instances** and check those specific instances you want to include.

The **All SQL Server Instances** option includes Azure and Amazon instances.

You can use **Audited SQL Servers** tab of the **Policy Properties** window to change which instances belong to this policy. For more information, see [Audited SQL Servers](#).

Click **Next** to go to the [Internal Review Notes](#)

Enter Internal Review Notes

Use the **Internal Review Notes** section to specify text or questions that IDERA SQL Secure should include in your Risk Assessment and Assessment Comparison reports. These notes can serve as a questionnaire to be used for manually gathering additional data that may be required in your assessment.

SQL Secure Create Policy

Internal Review Notes
Specify any additional information that should be included in the policy report.

Text can be added to your security assessment report to enable manually gathering data and reporting it in one comprehensive place. Enter an optional title and additional text for your report here.

Title
CIS Interview Checks

Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2019, v1.0.0, November 27, 2019

1 Installation, Updates and Patches

1.1 Ensure Latest SQL Server Service Packs and Hotfixes are Installed (Not Scored)

1.2 Ensure Single-Function Member Servers are Used (Not Scored)

2 Surface Area Reduction

2.1 Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0' (Scored)

2.2 Ensure 'CLR Enabled' Server Configuration Option is set to '0' (Scored)

2.3 Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0' (Scored)

2.4 Ensure 'Database Mail XPs' Server Configuration Option is set to '0' (Scored)

2.5 Ensure 'OLE Automation Procedures' Server Configuration Option is set to '0' (Scored)

2.6 Ensure 'Remote Access' Server Configuration Option is set to '0' (Scored)

2.7 Ensure 'Remote Admin Connections' Server Configuration Option is set to '0' (Scored)

2.8 Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0' (Scored)

2.9 Ensure 'Trustworthy' Database Property is set to 'Off' (Scored)

2.10 Ensure Unnecessary SQL Server Protocols are set to 'Disabled' (Not Scored)

2.11 Ensure SQL Server is configured to use non-standard ports (Not Scored)

2.12 Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances (Scored)

2.13 Ensure 'sa' Login Account is set to 'Disabled' (Scored)

2.14 Ensure 'sa' Login Account has been renamed (Scored)

2.15 Ensure 'AUTO_CLOSE' is set to 'OFF' on contained databases (Scored)

Check Spelling

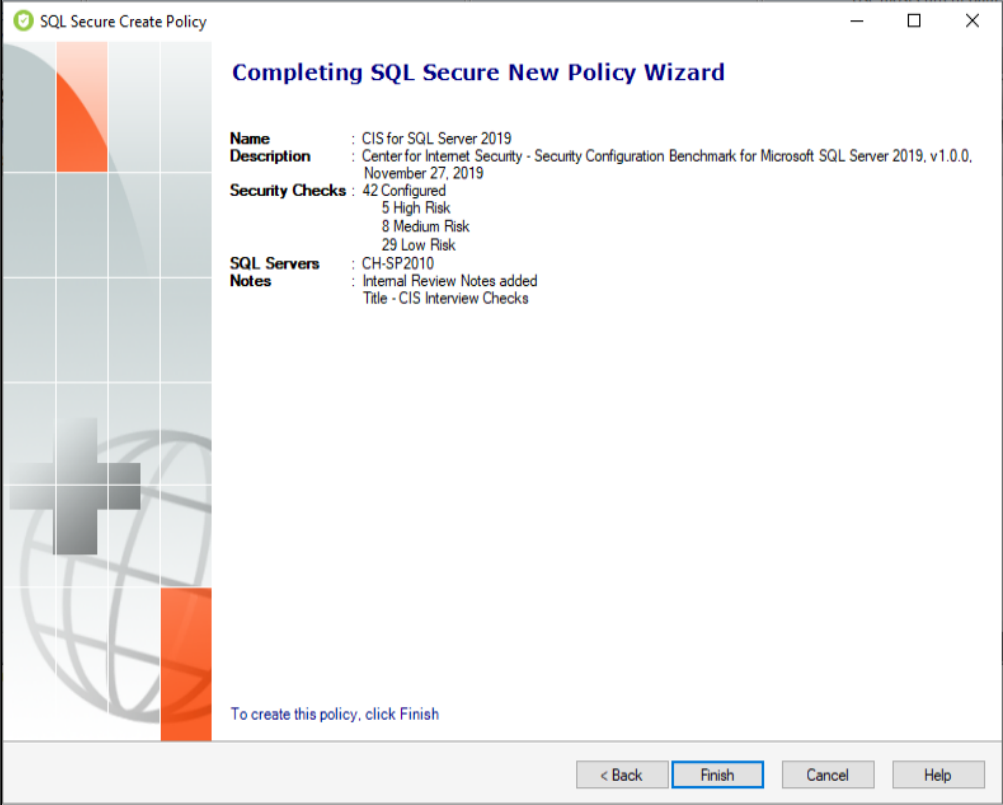
< Back Next > Cancel Help

- ✓ You can use the option **Check Spelling** to make sure the information displayed on your report is well written.

Click **Next** to go to the [Completing SQL Secure New Policy Wizard](#) section.

Review policy summary

The **Completing SQL Secure New Policy Wizard** section lists all the details of the policy you are creating. Click **Finish** to add your policy to IDERA SQL Secure. Your new policy will now display in the Policies tree on the **Security Summary** view where you can see the assigned SQL Server instances and determine their compliance with your policy.



5.5.3 Edit policy properties

The **Policy Properties** window allows you to quickly edit your policy settings. Changes made on the **Policy Properties** window are instantly applied to your policy.

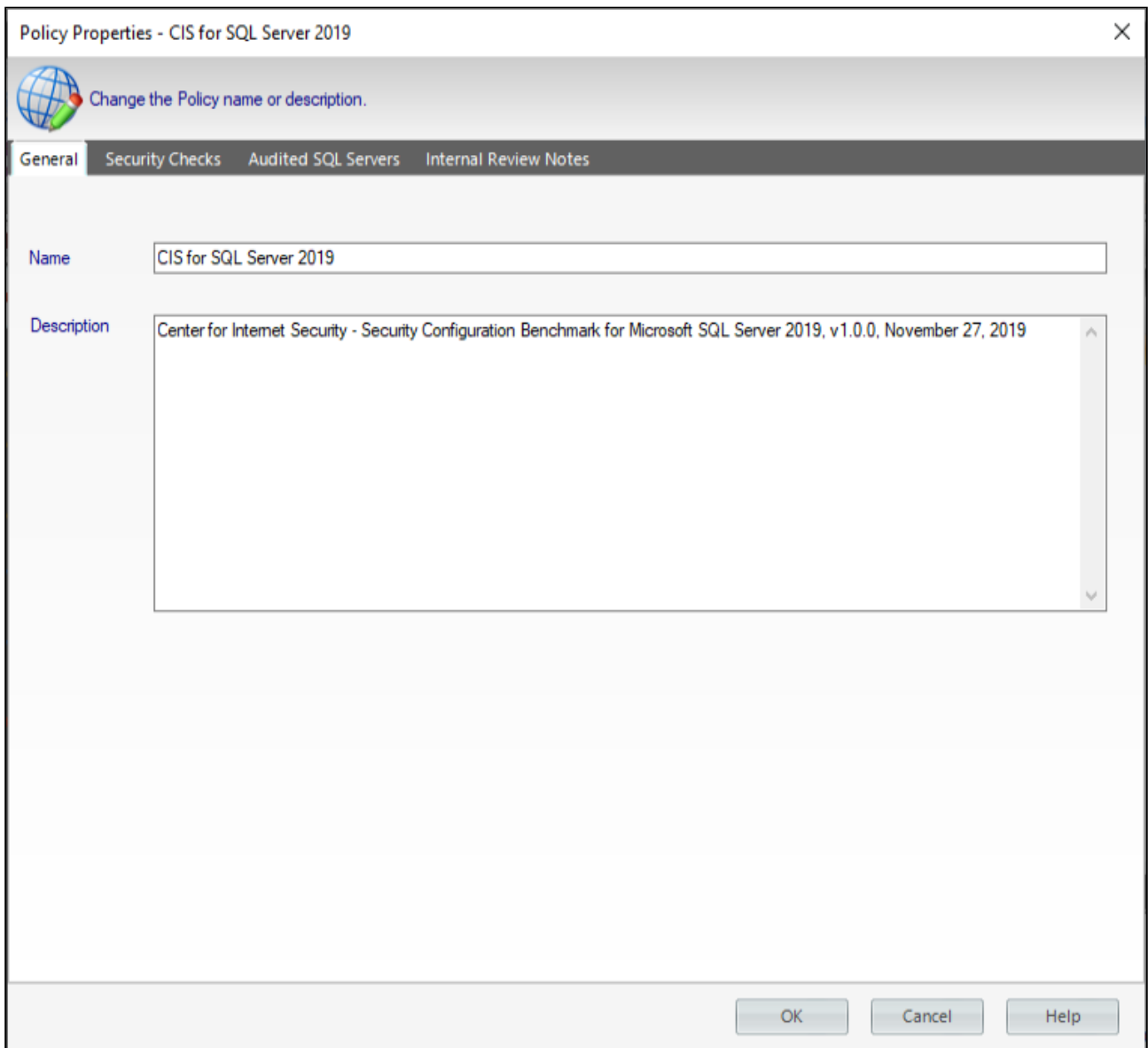
In the **Security Summary** view you can open the **Policy Properties** window by using any of the following options:

- Right-click your policy from the Policies tree and select **Properties**
- Select your policy and click **Edit settings** in the ribbon options available at any of the tabs (Summary, Settings, Users)

The following tabs are available on the **Policy Properties** window:

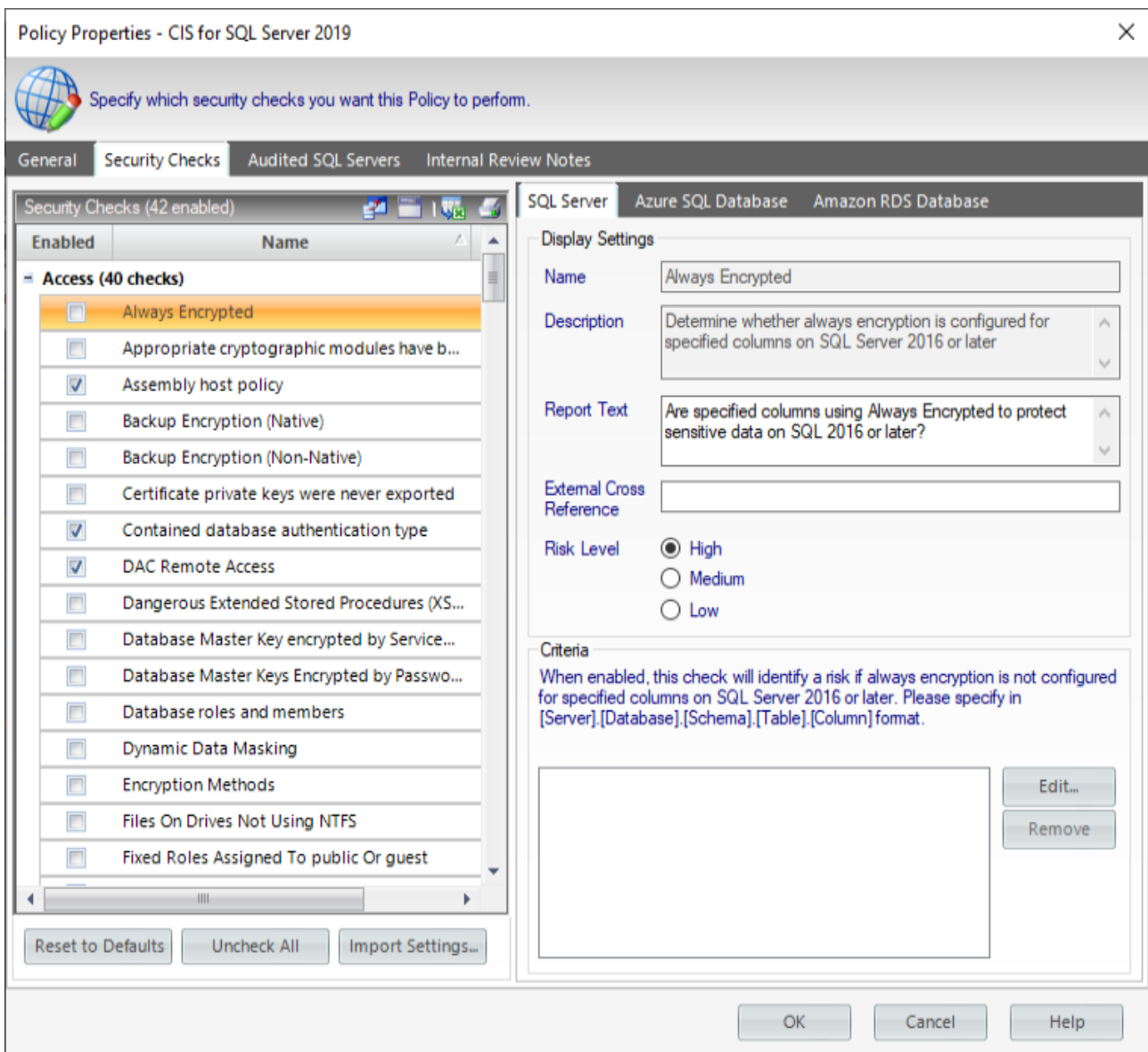
General

The **General** tab of the **Policy Properties** window allows you to update the name and description of the selected policy. The policy name appears in the **Security Summary** view under the Policies tree.



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

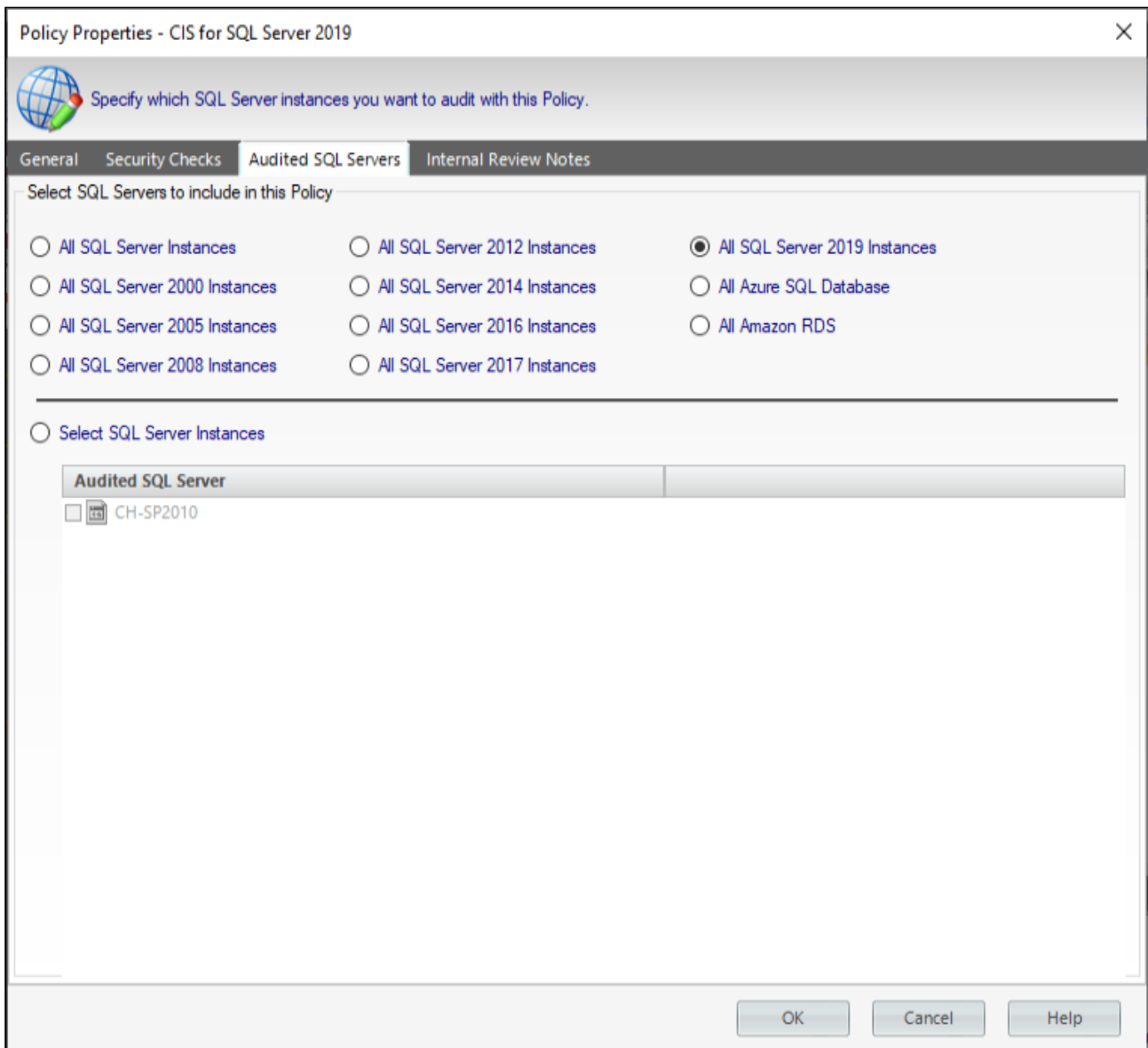
The text entered in this field appears on your policy reports. For example, the Protocols security check includes the report text "Are unexpected Protocols enabled?". When unexpected protocols are enabled, the report displays the SQL Server instances where the risk is encountered.

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.

Audited SQL Servers

The **Audited SQL Servers** tab allows you to change which registered SQL Server instances are assigned to this policy. You can add or remove instances from this policy to better match your auditing needs. Each registered SQL Server instance can belong to multiple policies.

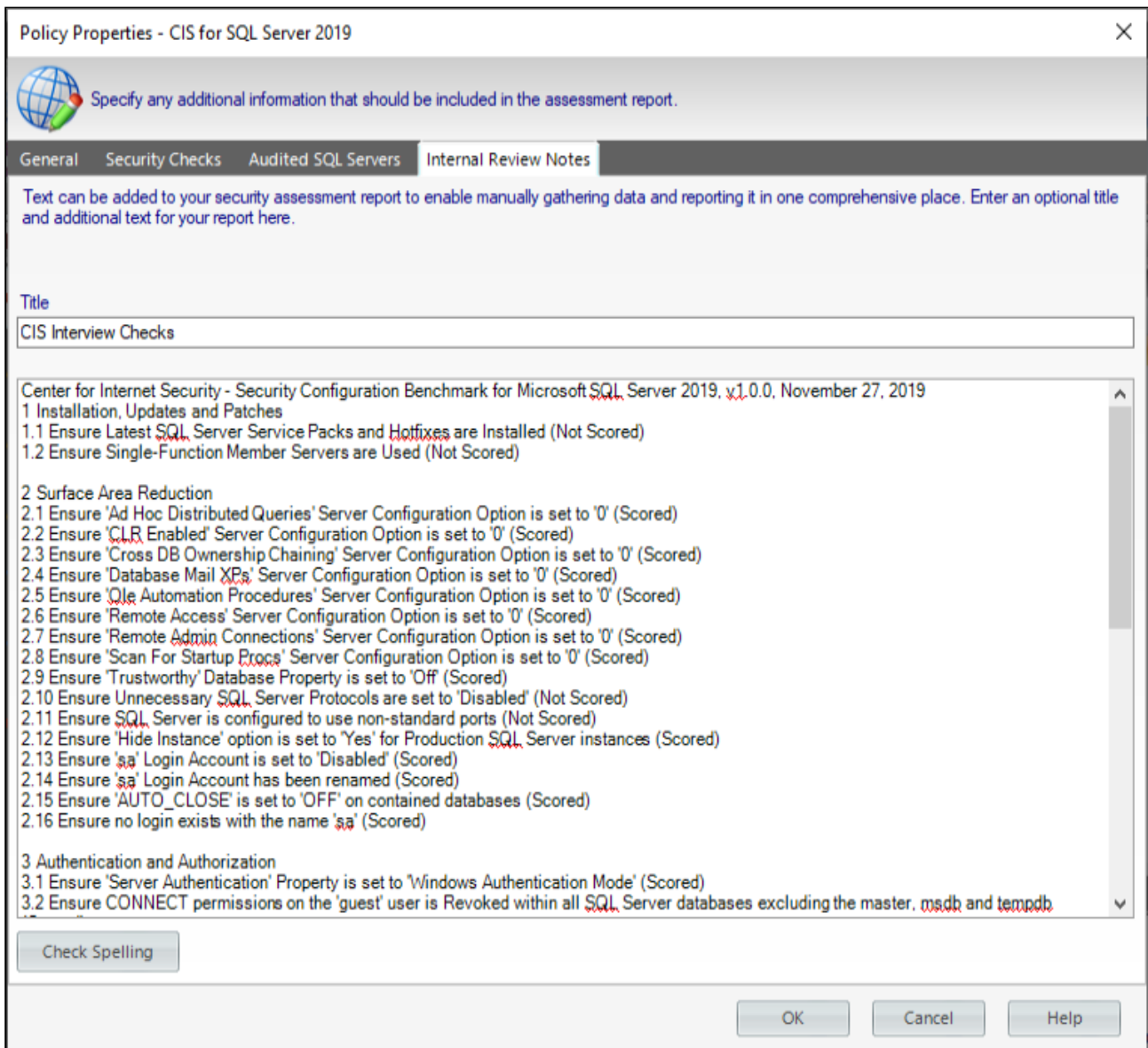


The **Audited SQL Servers tab** is located in the **Policy Properties** window.

Edit the instance list by either selecting one of the version-group options or by selecting instances specifically, and then click **OK**. SQL Secure automatically re-assesses the policy based on this new scope.

Internal Review Notes

The **Internal Review Notes** tab allows you to edit the manually-collected data applied to your policy. Manually-collected data is security information that cannot be gathered and assessed through IDERA SQL Secure.



You can find the **Internal Review Notes** tab in the **Policy Properties** window.

SQL Secure includes your Internal Review Notes to the Risk Assessment report, providing a fuller picture of your security status. These notes can also serve as a questionnaire to be used for manually gathering additional data that may be required to fully enforce your policy.

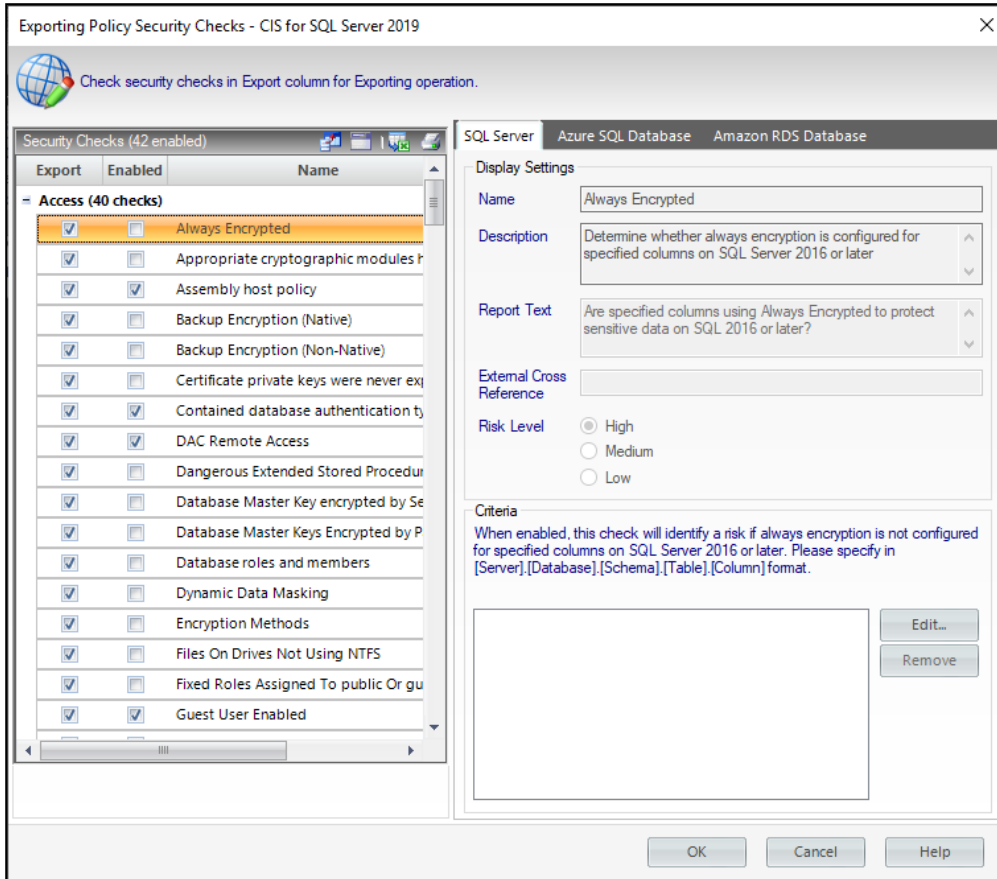
To edit these notes, click inside the provided text box and enter your changes.



You can use the **Check Spelling** option to make sure the text you typed in the Internal Review Notes is well written.

5.5.4 Export policies

The **Export Policy** window allows you to save the currently selected policy as a template to base other policies on.

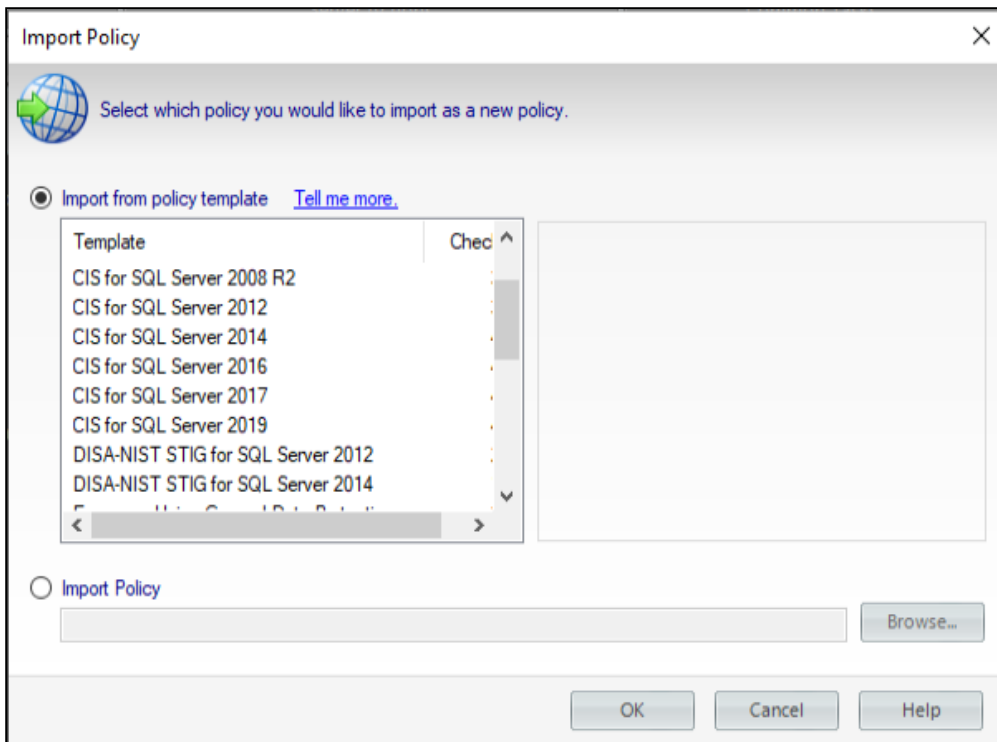


To export your policy you can follow these steps:

1. Select **Export Policy** from the **Summary** tab on the **Security Summary** view, or select your policy from the Policies tree in the **Security Summary** view and Right-click to select **Export Policy**.
2. SQL Secure opens the **Exporting Policy Security Checks** window where you can review which checks are enabled in your selected policy and which ones are selected for exporting. Edit the security checks you want to export in the Export column. Take into account that you cannot edit the settings of any security check. Click **OK**.
3. Browse to the desired location you want to store your policy template, type a file name, and click **Save**.

5.5.5 Import policies

The **Import Policy** window allows you to choose to either add a policy template or to import a previously exported policy to the Policy tree. Once the policy is selected, you can configure the policy and select the SQL Server instances to add to the policy.



To import a policy follow these steps:

1. Select **Import Policy** from the **Summary** tab on the **Security Summary** view, or Right-click any section in the **Policies** tree of the **Security Summary** view and select **Import Policy**
2. The **Import Policy** window opens with the following options:
 - **Import from policy template** - Select this option if you want to import from a policy template. Click the template to import, then click **OK**. For more information, see how [policy templates](#) can help you achieve your SQL Server security goals.
 - **Import previously exported policy** - Select this option if you want to import a previously exported template. Click **Browse** to locate your policy template, click **Open**, and then **OK**.
3. Once you select the source for importing your policy (from policy template or previously exported policy) follow these steps:
 - In the **Importing Policy Security Checks** window, you can review in the Import column which security checks you want to import. Click **OK**.
 - The **Importing Policy** window opens where you can edit the properties of the policy (name, description), the security checks you want this policy to perform, specific settings for a security check, the SQL Server instances added to the policy, and the Internal Review Notes. For more information about the settings of a policy, go to [Add new policy](#). Take into account that you need to change the name of the selected policy to import a new one. Click **OK**.

5.6 Policy assessments

By creating and comparing policy assessments, you can integrate your IDERA SQL Secure policies into your existing audit process. The recommended assessment workflow is:

1. [Save as draft.](#)
2. [Publish assessment.](#)
3. [Approve assessment.](#)

5.6.1 Use saved assessments in an existing audit process

Your Audit Process Step	Corresponding Assessment Step
Prepare for upcoming audit.	Create a draft assessment from an existing policy or previously approved assessment.
Set up the security requirements requested by the auditors.	Update the draft assessments to address the audit requirements. You can change the security check settings , choose different audit data , and add or remove SQL Server Instances .
Get your security status and findings.	Run the draft assessment using audit data from a specific point in time.
Identify differences from last time this audit was performed.	Compare the draft assessment to a previously approved assessment.
Distribute the assessment findings to an internal team to investigate any new violations or discrepancies.	Publish the assessment and distribute to the team. To distribute the assessment, run the Risk Assessment report , and then print or save the results.
Confirm that violations were fixed.	Take a new snapshot and then run the published assessment using your new audit data.
Document any discrepancies as known issues.	Add an explanation note for each security check finding that is a known issue.
Give assessment to auditors.	Run the Risk Assessment report , and then print or save the results.
Apply feedback from auditors.	Update the published assessment to address the auditors' feedback. You can change the security check settings , add or remove explanation notes , and change which instances are being audited .

Your Audit Process Step	Corresponding Assessment Step
Obtain "sign-off".	Approve the assessment.

5.6.2 Save new assessment

Use the **Save as New Assessment** option to create a new assessment that uses the same audit data and settings of an existing assessment. Specify a unique name and description for this new assessment, and then click **OK**.

To **Save as New Assessment** use any of the following options

- Right-click an existing policy or assessment from the Policies tree of the **Security Summary** view. Select **Save as New Assessment**.
- Select an existing policy or assessment from the Policies tree of the **Security Summary** view. Click **Save as New Assessment** from the ribbon options of the **Summary** tab.

Both options open a new window where you have to specify the name for the new assessment and the description.

✓ Consider using a name and description whose details will help you later when you refer back to this assessment.

⚠ Explanation notes associated with security checks in the selected assessment are not copied to the new assessment. To transfer notes from one assessment to another, [compare the assessment security checks](#) and then select which explanation notes you want to copy.

5.6.3 Working with draft assessments

Use draft assessments to fine-tune your data and settings when you begin your audit process. A draft assessment represents the first step, or stage, in the audit process. Draft assessments typically contain your initial findings, including any discrepancies that should be investigated before your review.

When you save a new assessment, it is automatically set to draft mode. You can update and change draft assessments as often as you want. However, changes made in draft mode are not tracked. For more information about how to use saved assessments in your audit process, see [Save Assessments](#).

Use the draft mode to set up your assessment configuration settings to reflect the goals and requirements of your upcoming audit, identify discrepancies, and obtain internal feedback on your findings.

Available actions and tasks for Draft Assessments

The following options are available for draft assessments. You can find these options in the ribbon menu options of the **Summary** tab of your draft assessment. Most of these options are also available by right-clicking the assessment in the Policies tree of the **Security Summary** view.

CIS for SQL Server 2000 - Assessment 1

Summary

Assessment Actions: Edit Settings, Refresh Audit Data, Publish, Save as New Assessment, Compare Assessments, Remove Assessment

Security Check Actions: Configure Security Check, Edit Explanation Notes, Take a Snapshot

Draft Assessment Status

- 1 High Risk of 3
- 0 Medium Risk of 3
- 7 Low Risk of 27

Enterprise Security Report Card

33 Security Checks - 8 Risks (1 High and 7 Lows)

Risk	Security Check	Findings
High	Public Database Role Has Permissions	1 High Risk
Low	Analysis Services Running	1 Low Risk
Low	Common TCP Port Used	1 Low Risk
Low	Dangerous Extended Stored Procedures (XSPs)	1 Low Risk
Low	Integration Services Running	1 Low Risk
Low	Remote Access	1 Low Risk
Low	SQL Server Version	1 Low Risk
Low	Stored Procedures Encrypted	1 Low Risk
OK	Agent Job Execution	OK
OK	Audit Data Is Stale	OK
OK	Blank Passwords	OK
OK	BUILTIN/Administrators Is sysadmin	OK
OK	Cross Database Ownership Chaining Enabled	OK
OK	Files On Drives Not Using NTFS	OK
OK	Fixed Roles Assigned To public Or guest	OK
OK	Guest User Enabled	OK
OK	Integration Services	OK

Details | Explanation Notes

Security Check: Public Database Role Has Permissions
 Determine whether the public database role has any permissions

Risk Level: High
 Server is vulnerable if the public role has been granted any permissions or is a role member.

Findings:
 CH-SP2010 Public has permissions on 'master', 'model', 'msdb', 'ReportServer', 'ReportServerTempDB', 'SQLSecure', 'tempdb'

Edit or View Assessment Settings

Allows you to edit or view the configuration settings for the draft assessment, such as the security checks the assessment performs. Go to [Edit Assessments](#) for more information and to view what settings you can change.

If your SQL Secure login does not have administrator permissions, you can only view assessment settings.

Refresh Audit Data

Allows you to re-run this assessment using different audit data (up to a specific point in time). Go to [Refresh Audit Data](#) for more information.

Publish Assessment

Allows you to publish this assessment. Publishing an assessment lets you safely distribute your findings and explanation notes. When an assessment is published, SQL Secure begins tracking each subsequent change applied to the assessment. Go to [Working with published assessments](#) for more information.

Use the [Change Log](#) tab to review this activity and ensure your audit data and resultant assessment is correct and accurate, and validate any updates.

Publish a draft assessment when it is ready for internal or external review by the audit team.

Save as New Assessment

Allows you to create a new assessment that uses the same settings and audit data as the selected assessment. When you save a new assessment, SQL Secure lists the assessment in the **Draft Assessment** folder under the associated policy in the Policies tree. Go to [Save new assessment](#) for more information.

Compare Assessments

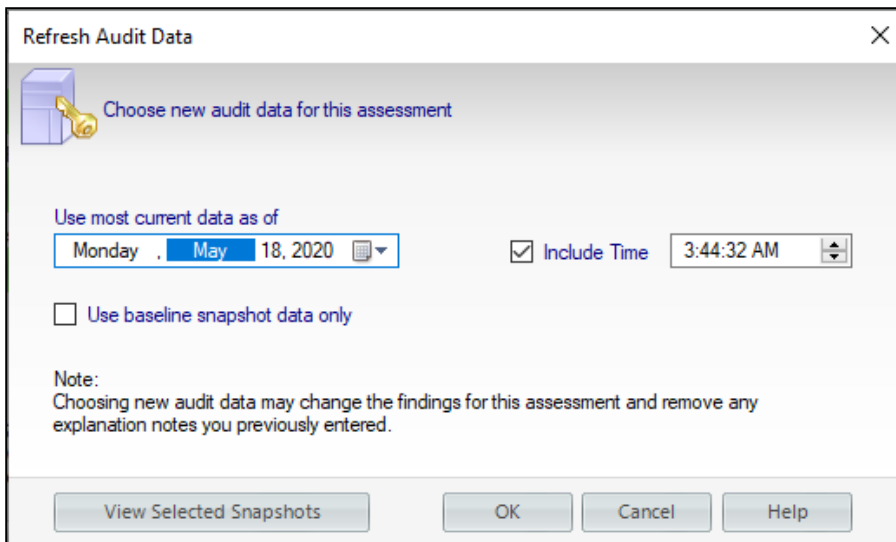
Allows you to compare the findings and settings of a draft assessment against another saved assessment or the original policy. You can compare different types of assessments (draft, published, or approved). When you compare assessments against the original policy from which it was saved, you can identify changes that have occurred since the assessment had been saved. For more information, go to [Compare Assessments](#).

Remove Assessment

Permanently deletes the selected assessment from the SQL Secure Repository.

5.6.4 Refresh audit data

Use the **Refresh Audit Data** option to change which audit data (snapshots) this assessment is using to perform the assigned security checks. Choosing a different set of audit data may alter the assessment findings. After you choose a new data set, IDERA SQL Secure updates the assessment.



Consider refreshing the audit data when:

- Your environment has changed and you need to re-run the assessment against the most recent audit data
- You have responded to a high or medium finding by adjusting a security setting in your environment and need to validate your change
- You want to run the same assessment against a point in time in the past, such as last week or last month

Baseline snapshots can be used as a guide about how your SQL Server security model should be configured. By running your policy against baseline snapshots only, you can test the thoroughness of this guide.

To change the audit data follow these steps:

- Select your assessment from the Policies tree of the **Security Summary** view.
- Click **Refresh Audit Data** from the ribbon options of the **Summary** tab, a new window opens.
- Specify the date until which the audit data will be taken into account. You can include a specific time by checking **Include Time**.
- Optionally, you can select to **Use Baseline snapshot data only**.
- You can choose to **View Selected Snapshots** to review the baseline snapshots that will be used for this assessment. This list includes all available snapshots that were collected up to the specified time period.
- Click **OK**.

5.6.5 Edit Assessments

Edit the settings of your assessment by using the **Assessment Properties** window to change basic properties or how the assessment performs its security evaluation.

To access this window, click the respective assessment or policy on the Policies tree of the **Security Summary** view, then select **Edit Settings** from the ribbon options. You can also right-click the assessment and select **Properties** to access the same window.

You can edit in the following tabs:

General

The **General** tab of the **Assessment Properties** window allows you to update the name and description of the selected assessment as well as any notes you want to provide.

Assessment Properties - CIS for SQL Server 2019 - Assessment2

Change the Assessment name or description.

General | Security Checks | Audited SQL Servers | Internal Review Notes

Name: Assessment2

Description: Center for Internet Security - Security Configuration Benchmark for Microsoft SQL Server 2019, v1.0.0, November 27, 2019

Notes

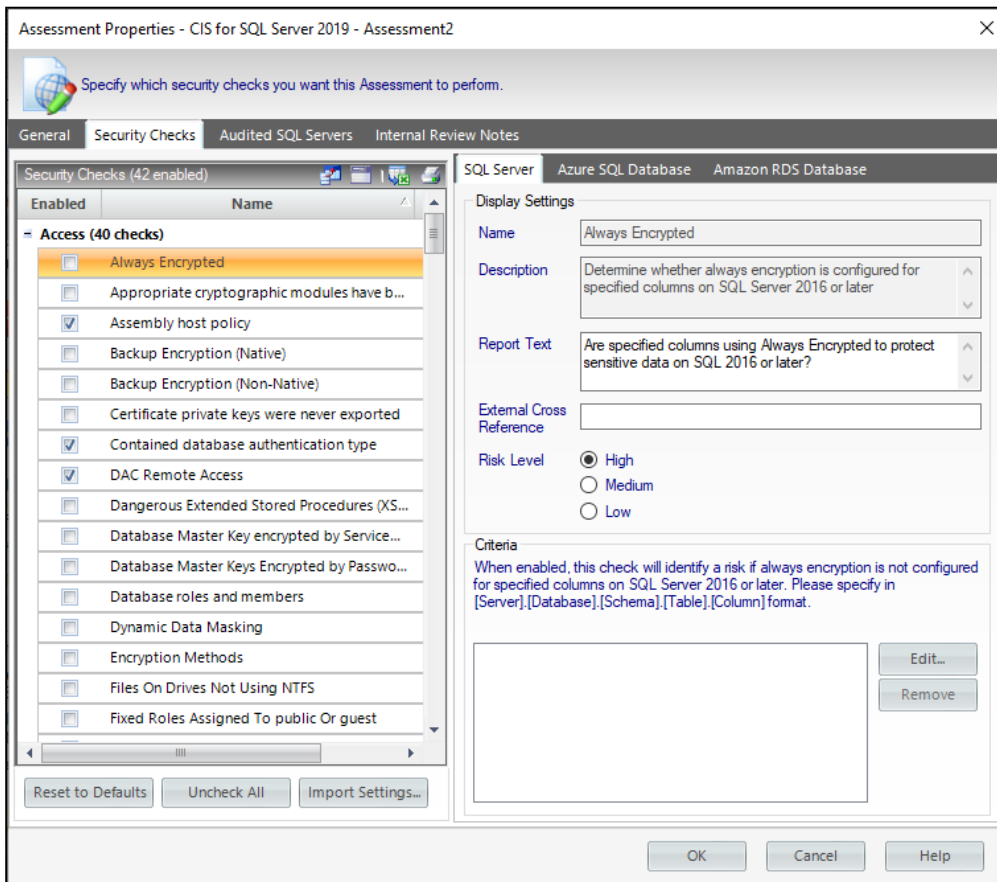
OK Cancel Help

The **Notes** field allows you to enter notes, questions, and other information about this assessment. Use these notes as a "cheat sheet" to remember details about your environment or security assessment from one audit to another. This approach ensures you gather all the data you need.

Security Checks

Security checks assess the vulnerability of specific Windows OS and SQL Server objects based on your criteria. The security checks performed by the selected assessment were copied from the policy associated with this

assessment. You can modify the criteria of these checks to better fit your auditing needs for this assessment. Changes made to the assessment security checks will not affect the associated policy.



Available fields

You can update the following fields for SQL Server or Azure SQL Databases:

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.

External Cross Reference

Allows you to cross reference a security vulnerability included in your report to a number or label contained in an external policy, industry standard, or government regulation.

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.

Criteria

Some security checks allow you to enter criteria the policy will check for, such as specific user accounts, stored procedures, or the login audit level. Text entered into these fields must be the exact spelling of the object or user being checked.

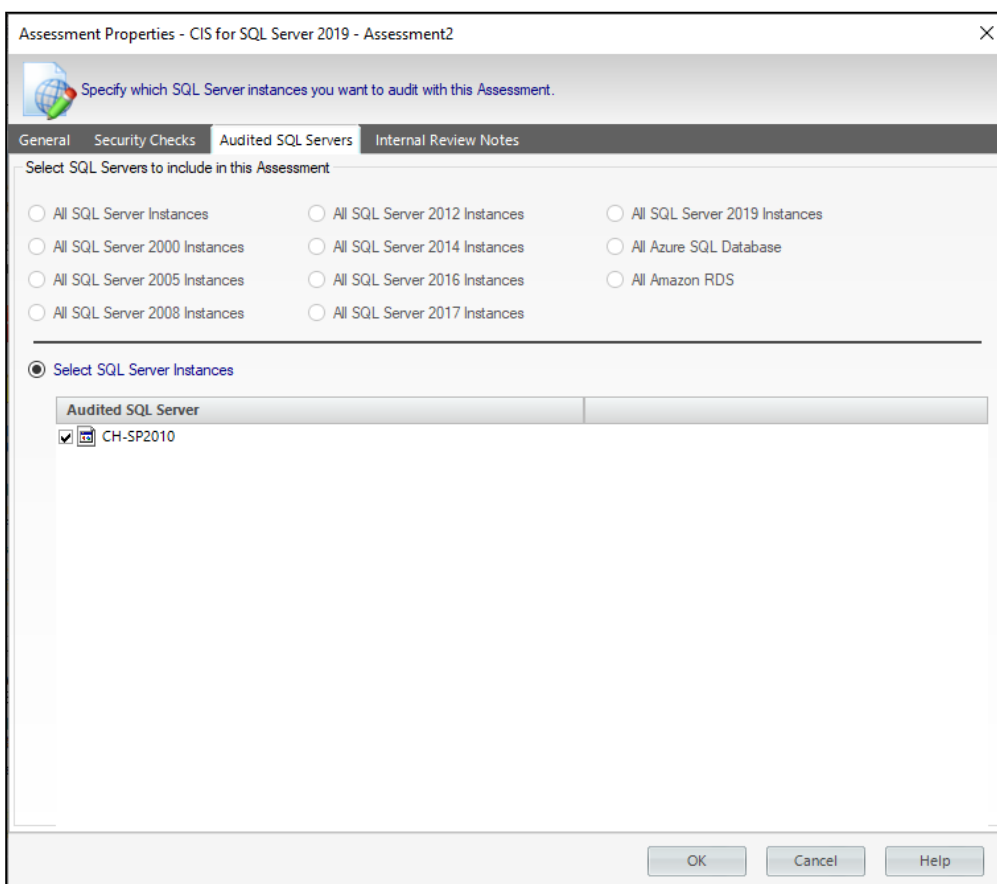
⚠ If the criteria for any given security check is entered incorrectly, the risk will appear in the Security Report Card. Select the risk and you can see the correct criteria names in the Details section. Open the Policy details window and enter the correct name on the Security Checks tab.

✓ 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%`.

Any criteria you introduce, you can change it with the option **Edit**, or delete it by using **Remove**.

Audited SQL Servers

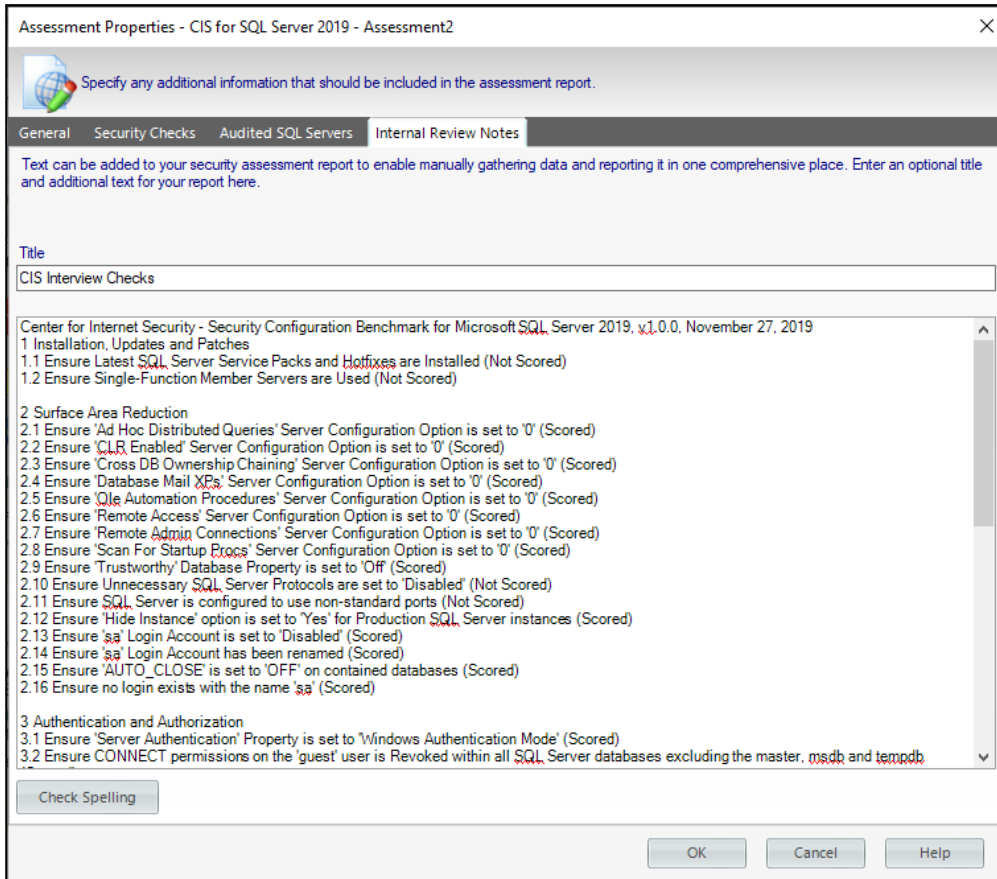
The **Audited SQL Servers** tab allows you to change which registered SQL Server instances are assigned to this assessment within IDERA SQL Secure. You can add or remove instances from this assessment to better match your current auditing needs. Each registered SQL Server instance can belong to multiple assessments.



Edit the instance list, and then click **OK**. SQL Secure automatically re-runs the assessment based on this new scope.

Internal Review Notes

The **Internal Review Notes** tab allows you to edit the manually-collected data applied to your assessment. Manually-collected data is security information that cannot be gathered and assessed through IDERA SQL Secure.



SQL Secure adds your **Internal Review Notes** to the Risk Assessment report, providing a fuller picture of your assessment status. These notes can also serve as a questionnaire to be used for manually gathering additional data that may be required in your assessment.

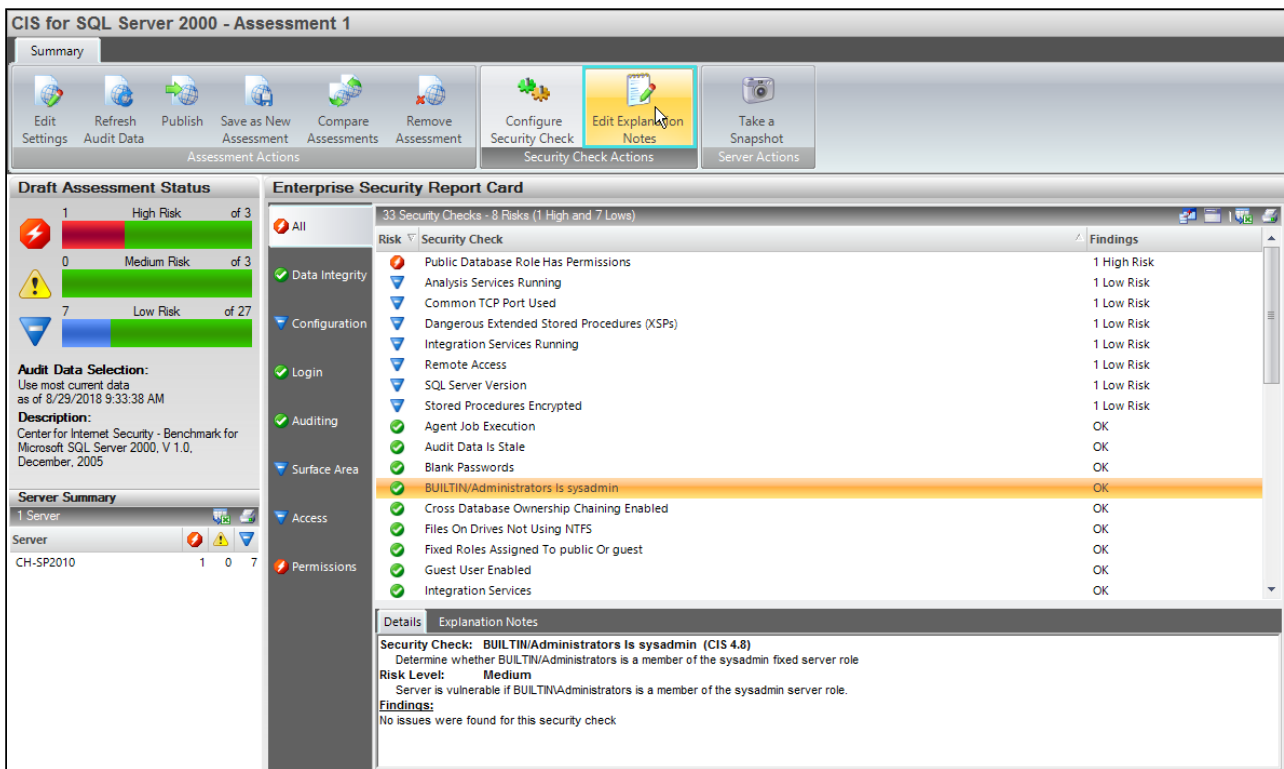
To edit these notes, click inside the provided text box and enter your changes.

5.6.6 Edit explanation notes

Use the **Edit Explanation Notes** option to add or change the explanation notes associated with a selected security check. You can specify a different explanation note for each finding on each affected SQL Server instance.

Explanation notes let you clarify why a specific finding has been found. For example, you may need to justify why a high or medium risk finding should be ignored due to a special configuration or need in your environment.

To use this option, go to your respective assessment in the **Security Summary** view, click a security check on your **Server Security Report Card**, and then click **Edit Explanation Notes** on the ribbon options of the **Summary** tab. A new window opens for the selected security check where you can choose to mark the check as **Explained** and/or type **Notes**.

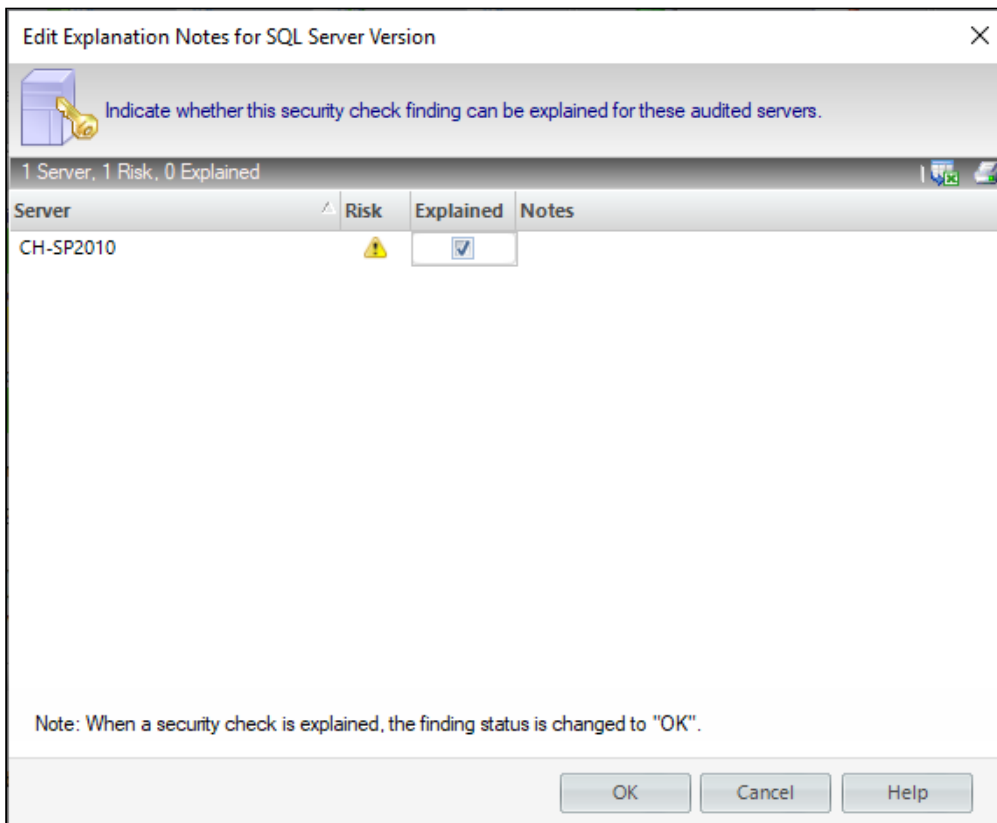


When a finding is marked as **Explained**, SQL Secure regards the finding as "OK" and changes the status of the security check in the assessment report card. **If you do not want the finding to be regarded as "OK"**, enter the appropriate note but leave the **Explained** option unchecked.

✔ You can copy explanation notes from one assessment to another when you [compare the assessment security checks](#).

Available fields

When the **Edit Explanation Notes** window is opened, the following fields are available:

**Server**

Provides the name of the SQL Server instance on which the security check found a violation.

Risk

Provides the level of risk set for this security check (high, medium, or low).

Explained

Indicates whether this security check finding has been explained for the specified instance.

Notes

Displays the note that has been entered about each finding, per each affected SQL Server instance.

5.6.7 Working with published assessments

Use published assessments to apprise internal or external auditors of your security status and settings. A published assessment represents the review phase of your audit process. Published assessments typically contain the required security checks and an accurate security status for your audited instances, as well as any explanation notes regarding known violations or discrepancies.

When you publish an assessment, it is automatically set to the published mode. IDERA SQL Secure begins tracking each subsequent change applied to the assessment. Use the [Change Log](#) tab to review this activity.

Use the published mode to create and maintain a historical electronic trail of change activity, ensuring you can validate and document when, how, and why changes were made.

Approve a published assessment

Approving an assessment lets you safely archive your assessment for future reference. An approved assessment proves you are in compliance with specific corporate and government regulations, and have successfully completed an audit. For each subsequent audit, you can [start \(save\) a new assessment](#) using the approved assessment as a template.

Approve an assessment when the internal or external audit team has "signed off" on your assessment and it is ready to be archived. Approved assessments accurately represent your security status at a specific point in time and no longer require changes.

Actions and Tasks for Published Assessments

The following options are available in the ribbon menu options of the **Summary** tab of your published assessment.

CIS for SQL Server 2000 - Assessment 1::CH-SP2010

Summary | Change Log

Edit Settings | Refresh Audit Data | Approve | Save as New Assessment | Compare Assessments | Remove from Assessment | Configure Security Check | Edit Explanation Notes | Take a Snapshot

Server Status

- 1 High Risk of 3
- 0 Medium Risk of 3
- 7 Low Risk of 27

Audit Data Selection:
Use most current data as of 8/29/2018 9:33:38 AM

Description:
Center for Internet Security - Benchmark for Microsoft SQL Server 2000, V 1.0, December, 2005

SQL Server Info

Server Name: CH-SP2010

Audit Data Collected: 8/29/2018 6:47:23 AM

Version: SQL Server 2012 v11.0.5058.0

Edition: Enterprise Edition (64-bit)

Windows OS: Microsoft Windows Server 2012 R2 Datacenter

Server Security Report Card

33 Security Checks - 8 Risks (1 High and 7 Low)

Risk	Security Check	Findings
High	Public Database Role Has Permissions	1 High Risk
Low	Analysis Services Running	1 Low Risk
Low	Common TCP Port Used	1 Low Risk
Low	Dangerous Extended Stored Procedures (XSPs)	1 Low Risk
Low	Integration Services Running	1 Low Risk
Low	Remote Access	1 Low Risk
Low	SQL Server Version	1 Low Risk
Low	Stored Procedures Encrypted	1 Low Risk
OK	Agent Job Execution	OK
OK	Audit Data Is Stale	OK
OK	Blank Passwords	OK
OK	BUILTIN/Administrators Is sysadmin	OK
OK	Cross Database Ownership Chaining Enabled	OK
OK	Files On Drives Not Using NTFS	OK
OK	Fixed Roles Assigned To public Or guest	OK
OK	Guest User Enabled	OK
OK	Integration Services	OK

Details | Explanation Notes


Security Check: Public Database Role Has Permissions
Determine whether the public database role has any permissions

Risk Level: High
Server is vulnerable if the public role has been granted any permissions or is a role member.

Findings:
CH-SP2010 Public has permissions on 'master', 'model', 'msdb', 'ReportServer', 'ReportServerTempDB', 'SQLsecure', 'tempdb'

Edit or View Assessment Settings

Allows you to edit or view the configuration settings for the published assessment, such as the security checks the assessment performs. Any changes performed to the assessment settings will be recorded in the [change log](#).

 If your SQL Secure login does not have administrator permissions, you can only view assessment settings.

Refresh Audit Data

Allows you to re-run this assessment using different audit data (up to a specific point in time). Each time you refresh the audit data, SQL Secure registers the action in the [Change Log](#).

Approve

Allows you to approve this assessment. Approving an assessment lets you safely archive a final version of this assessment, preserving your findings and explanation notes. When an assessment is approved, SQL Secure locks the assessment, preventing you from changing or deleting the assessment settings as well as the associated audit data. However, you can manually add or remove notes about an approved assessment by editing the **Notes** field on the [Assessment Properties](#) window. You can also continue to use the [Change Log](#) tab to review activity that previously occurred on this assessment.

Save as New Assessment

Allows you to create a new assessment that uses the same settings and audit data as the selected published assessment. When you save a new assessment, SQL Secure lists the assessment in the **Draft Assessment** folder under the associated policy in the Policies tree.

Compare Assessments

Allows you to compare the findings and settings of the published assessment against another saved assessment or the original policy. You can compare different types of assessments (draft, published, or approved). When you compare this assessment against the original policy from which it was saved, you can identify changes that have occurred since the assessment had been saved.

Remove from Assessment

Removes the selected SQL Server instance from the assessment. This option is available when you have selected a registered instance from the **Servers in Policy** tree.

Remove Assessment

Permanently deletes the selected assessment from the SQL Secure Repository.

5.6.8 View assessment change log

The **Change Log** tab lists all changes that have been made to the selected published assessment. After you publish an assessment, IDERA SQL Secure begins tracking any change that has been made to the assessment's settings. These changes may include the addition or removal of audited instances as well modifications to the security checks to be performed by the assessment.


The change log gives you an electronic, "paper trail" that documents exactly how a published assessment is being processed during an internal or external audit review.

Available actions and fields at the Change Log tab

In the **Change Log** tab you have the following available actions:

Edit or View Assessment Settings

Allows you to edit or view the configuration settings for the published assessment, such as the security checks the assessment performs. Any changes performed to the assessment settings will be recorded in the Log entries.

 If your SQL Secure login does not have administrator permissions, you can only view assessment settings.

Refresh Audit Data

Allows you to re-run this assessment using different audit data (up to a specific point in time). Each time you refresh the audit data, SQL Secure registers the action in the [Change Log](#).

The following columns are displayed in the **Log Entries**:

Changed At

Provides the date and time at which the change occurred.

Assessment Status

Indicates the assessment status (published or approved) at the time of this change. Once an assessment is approved, only the assessments notes can be changed. Changes are not tracked when an assessment is in the draft status.

Changed By

Provides the name of the SQL Secure login who applied the change.

Change

Describes what change was applied.

5.6.9 Working with approved assessments

Approved assessments accurately represent your security status at a specific point in time. An approved assessment represents the final step, or stage, in your audit process. Approved assessments typically contain your accepted and official security status in response to an audit. When you approve an assessment, it is automatically locked and set to approved mode.

Use the approved mode to safely archive the assessment, preserving your findings and explanation notes.

To approve assessments:

- The assessment must be published. Go to [Working with published assessments](#) for more information.
- Select your published assessment from the Policies tree of the **Security Summary** view and click **Approve** in the ribbon menu options of the **Summary** tab of your published assessment.

- ✓ You can perform the following actions in the approve mode:
 - Manually add or remove notes about an approved assessment by editing the **Notes** field on the assessment **Properties** window.
 - Continue to use the **Change Log** tab to review activity that previously occurred on this assessment. However, no other changes are allowed.

Actions and Tasks for Approved Assessments

The following options are available in the **Summary** tab of a selected approved assessment:

CIS for SQL Server 2000 - Assessment 1::CH-SP2010

Summary | Change Log

View Settings | Refresh Audit Data | Save as New Assessment | Compare Assessments | Remove from Assessment | Configure Security Check | Edit Explanation Notes

Server Status

- 1 High Risk of 3
- 0 Medium Risk of 3
- 7 Low Risk of 27

Audit Data Selection:
Use most current data as of 8/29/2018 9:33:38 AM

Description:
Center for Internet Security - Benchmark for Microsoft SQL Server 2000, V 1.0, December, 2005

SQL Server Info

Server Name: CH-SP2010
Audit Data Collected: 8/29/2018 6:47:23 AM
Version: SQL Server 2012 v11.0.5058.0
Edition: Enterprise Edition (64-bit)
Windows OS: Microsoft Windows Server 2012 R2 Datacenter

Server Security Report Card

33 Security Checks - 8 Risks (1 High and 7 Lows)

Risk	Security Check	Findings
High	Public Database Role Has Permissions	1 High Risk
Low	Analysis Services Running	1 Low Risk
Low	Common TCP Port Used	1 Low Risk
Low	Dangerous Extended Stored Procedures (XSPs)	1 Low Risk
Low	Integration Services Running	1 Low Risk
Low	Remote Access	1 Low Risk
Low	SQL Server Version	1 Low Risk
Low	Stored Procedures Encrypted	1 Low Risk
OK	Agent Job Execution	OK
OK	Audit Data Is Stale	OK
OK	Blank Passwords	OK
OK	BUILTIN/Administrators Is sysadmin	OK
OK	Cross Database Ownership Chaining Enabled	OK
OK	Files On Drives Not Using NTFS	OK
OK	Fixed Roles Assigned To public Or guest	OK
OK	Guest User Enabled	OK
OK	Integration Services	OK

Details | Explanation Notes

Security Check: Public Database Role Has Permissions
 Determine whether the public database role has any permissions

Risk Level: High
 Server is vulnerable if the public role has been granted any permissions or is a role member.

Findings:
 CH-SP2010 Public has permissions on 'master', 'model', 'msdb', 'ReportServer', 'ReportServerTempDB', 'SQLSecure', 'tempdb'

View Assessment Settings

Allows you to view the configuration settings for an approved assessment, such as the security checks performed by the assessment.

Save as New Assessment

Allows you to create a new assessment that uses the same settings and audit data as the selected assessment. When you save a new assessment, SQL Secure lists the assessment in the **Draft Assessment** folder under the associated policy in the Policies tree.

Compare Assessments

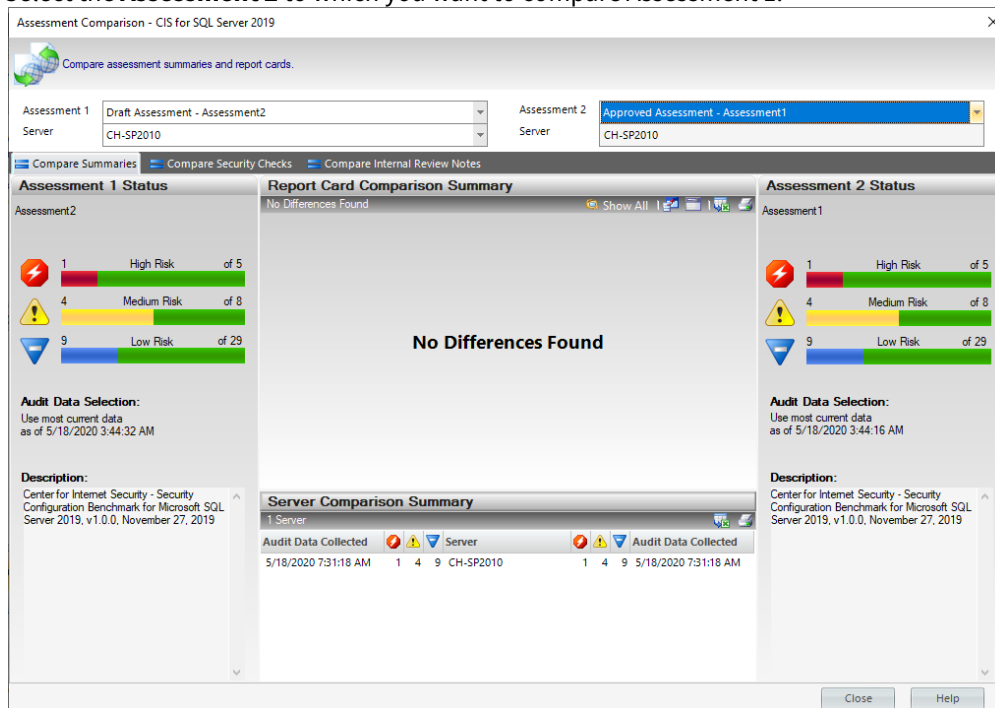
Allows you to compare the findings and settings of an approved assessment against another saved assessment or the original policy. You can compare different types of assessments (draft, published, or approved). When you compare this assessment against the original policy from which it was saved, you can identify changes that have occurred since the assessment had been saved.

5.7 Compare assessments

Use the **Assessment Comparison** window to compare any two assessments saved from the same policy. You can compare assessments previously saved from the default **All Servers** policy or from any custom policy you created. For example, you may want to compare a draft assessment of this quarter's **All Servers** audit to an approved assessment of last quarter's **All Servers** audit.

To compare assessments:

- Select one of the assessments you want compare and click **Compare Assessments** in the ribbon options of the **Summary** tab of your selected assessment.
- The selected assessment is displayed in **Assessment 1**, click the drop-down options to select another assessment or the corresponding policy. Notice, it will only display the respective policy and its associated assessments. You can select from draft, published, or approved assessments.
- You can select to compare All Servers or a specific SQL Server instance from the list of available instances in the drop-down options.
- Select the **Assessment 2** to which you want to compare Assessment 1.



The **Compare Assessment** results will be displayed in the section below with the following three tabs:

- [Compare Summaries](#)
- [Compare Security checks](#)
- [Compare Internal Review Notes](#)



For more information about how to use assessments in your existing audit process, see [Save Assessments](#).

5.7.1 Compare assessment summaries

Use the **Compare Summaries** tab on the **Assessment Comparison** window to identify any differences in the security status of the two selected assessments. IDERA SQL Secure highlights each difference in yellow in the **Assessment Status** of each assessment.

The **Report Card Comparison Summary** shows where findings are equal (=) or not equal (≠).

From this tab, you can:

- Identify changes in risk level
- Compare security check findings
- Monitor whether security checks are enabled or disabled
- Monitor whether SQL Server instances are added or removed
- Review security status for all instances audited by each assessment

For a detailed comparison of each security check, see the [Compare Security Checks](#) tab. For more information, see [Compare Assessments](#).

5.7.2 Compare assessment security checks

Use the **Compare Security Checks** tab on the **Assessment Comparison** window to identify any differences in the security check settings of the two selected assessments.

The **Security Checks Comparison Summary** displays what differences have been found between the security checks of both assessments using (=) and (≠) to show where the differences are. Security Checks can be different in the Findings, Explanation Notes, Display Settings, and/or Criteria.

By using the options in the top right section you can:

- **Show All** security checks or **Show Differences Only**
- **Select Columns** to be displayed
- **Group by box**
- **Save**
- **Print**

Compare security check settings

The **Details** section allows to see, for each security check, the specific details in the following tabs:

Findings

Displays the findings returned by the selected security check when run by each assessment. The findings also display in the **Details** tab of the assessment **Report Card** at the enterprise and server levels.

Explanation Notes

Indicates whether an explanation note has been entered for this security check. Explanation notes are available from the assessment **Report Card** at the enterprise and server levels. To enter or edit an explanation note, select the target security check from the **Report Card**, and then click the **Explanation Notes** tab.

Display Settings

Provides the Risk Level, Report Text, and External Cross Reference assigned to this security check. For more information about these settings, see [Select Security Checks](#).

Criteria

Provides the criteria used to assess whether your audited instances are in compliance with this security check.

For a comparison of the overall security status, see the [Compare Summaries](#) tab. For more information, see [Compare Assessments](#).

5.7.3 Compare Internal Review Notes

Use the **Compare Internal Review Notes** tab on the **Assessment Comparison** window to identify any differences in the internal review notes associated with the two selected assessments. IDERA SQL Secure displays both notes and identifies whether notes are equal (=) or not equal (≠).

For more information, see [Compare Assessments](#).

5.8 Select audit data for assessment

Choosing a different set of audit data may alter the policy findings. After you choose a new data set, IDERA SQL Secure updates the policy. Use the [Refresh Audit Data](#) option to change the audit data for your policy.

By default, SQL Secure always uses the most recent audit data available.

5.8.1 When to select different audit data

Consider refreshing the audit data when:

- Your environment has changed and you need to re-run the assessment against the most recent audit data
- You have responded to a high or medium risk by adjusting a security setting in your environment and thus need to validate your change
- You want to run the same policy against a point in time in the past, such as last week or last month

5.8.2 Use only baseline snapshots

Baseline snapshots can be used as a guide about how your SQL Server security model should be configured. By running your policy against baseline snapshots only, you can test the thoroughness of this guide.

6 Report on SQL Server Security

The **Reports** component of IDERA SQL Secure allows you to generate reports on SQL Server permissions. Use reports to confirm regulatory compliance and enforce security policies.

SQL Secure contains two different ways to access reports. Quick Reports are reports that have been built into SQL Secure to allow you to quickly generate reports that answer the most common SQL Server security questions. You can also generate reports using Microsoft Reporting Services. Microsoft Reporting Services allows you to build powerful, custom reports for a comprehensive auditing solution.

SQL Secure allows you to:

- [Generate reports within the SQL Secure interface](#)
- [Generate reports using Microsoft Reporting Services](#)

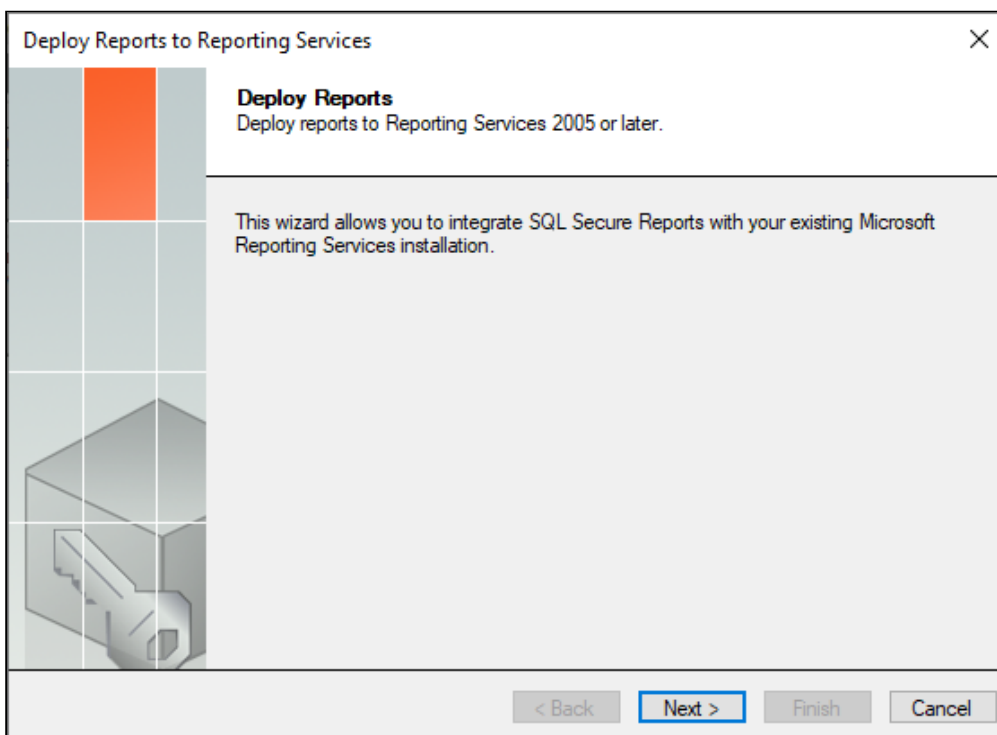
6.1 How to use the Deploy Reports wizard

You can deploy the IDERA SQL Secure Reports to your existing Microsoft Reporting Services installation.

If you previously deployed SQL Secure Reports, verify which version of Reporting Services is currently running in your environment. SQL Secure supports Reporting Services version 2005 or later.

⚠ If you are upgrading reports from SQL Secure 2.0, delete all of the previously-installed SQL Secure reports before deploying new reports.

To integrate your SQL Secure Reports with your existing Microsoft Reporting Services Installation you must deploy them by clicking **Deploy Reports to Reporting Services** in the **Microsoft Reporting Services** section of the **Reports** view. The **Deploy Reports to Reporting Services** window opens, click **Next** and you will access the following sections:



6.1.1 Connect to Reporting Services

The **Connect to Reporting Services** section allows you to specify the Report Server to which you want to deploy the IDERA SQL Secure Reports. The Deploy Reports wizard automatically applies connection settings based on a default Microsoft Reporting Services installation. You can use the default connection settings, or specify custom connection settings.

To specify connection settings, click **Show advanced connection options**, and then enter the appropriate settings. Click **Next** to go to the next section.

⚠ To successfully deploy reports, you must have Content Manager rights on the Report Server. For more information, see the Reporting Services Books Online.

6.1.2 Specify Repository as report data source

The IDERA **SQL Secure Repository** section allows you to determine:

- **Repository Server** - Specify the name of the SQL Server instance that hosts the Repository
- **Repository Credentials** - The Windows user account SQL Secure should use to connect to the Repository. You can use the same account that the Collection Service runs under, or you can specify a different account. The specified account should have permission to execute stored procedures on the Repository database.

Click **Next** to go to the next section.

6.1.3 Specify the Reports virtual directory

This **Report Deployment Location** section allows you to specify the name of the folder where the reports should be stored. This folder belongs to the Virtual Directory specified in the Reporting Services connection settings, and is displayed when you access the reports using the Report Manager interface.

You can also specify whether you want to overwrite existing reports. Click **Overwrite existing reports** to enable this option. By overwriting existing reports, you ensure all deployed reports are current. **If you decide not to overwrite existing reports**, the Deploy Reports wizard installs only the reports that are new or updated in this version of IDERA SQL Secure.

Click **Next** to continue to the Summary section before finishing the wizard.

6.1.4 Finish the Reports Deployment


Review the provided summary, and then click **Finish**. When you finish this wizard, IDERA SQLSecure installs the corresponding RDL files in the specified virtual directory on your Report Server.

If you want to change a setting now, click **Back** to return to the appropriate window. You can also change your deployment settings later through the Report Manager interface installed with Microsoft Reporting Services.

6.2 Use the Console to generate reports

IDERA SQL Secure includes built-in reports specially designed to generate commonly requested audit reports using the SQL Server permission data collected in your snapshots.

SQL Secure built-in reports allow you to quickly and easily meet the demands of on-the-spot audits, routine audits, and long-term event trending. Each report provides detailed information about events in your SQL Server environment.

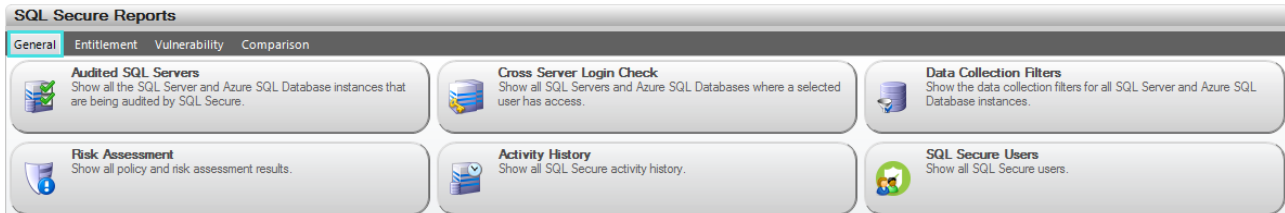
 Using the Console to generate reports against large audit data sets can result in degraded performance. For example, when the selected snapshot is large (contains thousands of objects and permissions), the report performance may be impacted. **If you experience degraded performance**, try increasing the Console timeout value and, if the performance issues continue, run the report with Microsoft Reporting Services instead.

6.2.1 Generate a report

To report on audit data:

1. In the console tree pane, click **Reports**.
2. In the view pane, select the report you want to generate.
3. Specify the appropriate parameters for the selected report, and then click **View Report**.

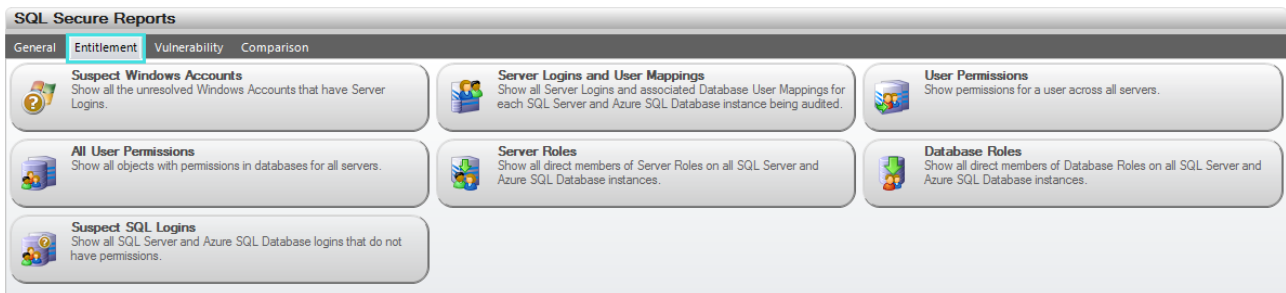
6.2.2 Available general reports



Report Name	Report Description
Audited SQL Servers	Displays all the SQL Server instances that are being audited by SQL Secure
Cross Server Login Check	Displays all SQL Server instances where a selected user has access
Data Collection Filters	Displays the data collection filters for all SQL Server instances
Risk Assessment	Displays all policy and risk assessment results. You can customize this text using the Policy Properties window. For more information, see Internal Review Notes .
Activity History	Displays all SQL Secure activity history

Report Name	Report Description
SQL Secure Users	Displays all SQL Secure users

6.2.3 Available entitlement reports



Report Name	Report Description
Suspect Windows Accounts	Displays all the suspect Windows Accounts that have Server Logins or Server Files Permissions. For more information, see Suspect Windows accounts .
Suspect SQL Logins	Displays all the suspect SQL Server Accounts that do not have any assigned permissions, i.e. databases, objects, or server files.
Server Logins and User Mappings	Displays all Server Logins and associated Database User Mappings for each SQL Server instance being audited
User Permissions	Displays permissions for a user across all SQL Server instances
All User Permissions	Displays all objects with permissions in the database for all SQL Server instances
Server Roles	Displays all direct members of Server Roles on all SQL Server instances
Database Roles	Displays all direct members of Database Roles on all SQL Server instances

6.2.4 Available vulnerability reports


The screenshot shows the 'SQL Secure Reports' interface with a navigation bar containing 'General', 'Entitlement', 'Vulnerability', and 'Comparison'. The 'Vulnerability' tab is active. Below the navigation bar, there are nine report cards arranged in a 3x3 grid. Each card features an icon, a title, and a brief description of the report's content.


Report Name	Report Description
Mixed Mode Authentication	Displays all SQL Server instances where Windows Authentication is not the only login method
Guest Enabled Databases	Displays all databases on a SQL Server instance where the Guest user has access
OS Vulnerability via XSPs	Displays all extended stored procedures that allow access to operating system features that could compromise system security
Vulnerable Fixed Roles	Displays all SQL Server instances that contain fixed roles assigned to public or guest
System Administrator Vulnerability	Displays all SQL Server instances that include built-in Administrators as members of the sysadmin role
Dangerous Windows Groups	Displays all SQL Server instances that grant access to any OS controlled Windows Group
Database Chaining Enabled	Display all SQL Server instances that have cross-database ownership chaining enabled
Mail Vulnerability	Displays all SQL Server instances with SQL Mail stored procedures
Login Vulnerability	Displays any SQL logins that have weak (easily guessed or hacked) passwords and lists their security properties, including the state of their password health.

6.2.5 Available comparison reports

SQL Secure Reports

General Entitlement Vulnerability **Comparison**

 **Assessment Comparison**
Identify discrepancies in the findings and security check configurations of two different assessments.

 **Snapshot Comparison**
Identify discrepancies in the audit data collected by two different snapshots.

Report Name	Report Description
Assessment Comparison	Displays any differences identified in the security settings and findings of two assessments.
Snapshot Comparison	Displays any differences identified in the configuration settings and audit data of two snapshots.

6.3 Use Reporting Services to generate reports

IDERA SQL Secure includes the ability to take the existing built-in SQL Secure reports and seamlessly integrate them into Microsoft Reporting Services. For each built-in SQL Secure report, the Deploy Reports wizard installs a Report Definition Language (RDL) file. These RDL files define the report layout and parameters, using the data source (SQL Secure Repository) you specified during install. Reporting Services automatically acknowledges these files, allowing you to immediately generate and view reports on audit data using the Reports Manager Web interface.

You can view, customize, and develop new reports based on any of the built-in SQL Secure reports to fit your unique auditing needs. Reports can be viewed in an existing SQL Server environment that uses a dedicated Report Server. If you decide to use Microsoft Reporting Services, consider the following best practices:

- Save your new and modified reports to a separate folder
- Use a different file name for modified reports

For more information about the Reporting Services architecture, see the Reporting Services Books Online. For more information about developing custom reports using Microsoft Reporting Tools, see the Reporting Services Books Online.

6.3.1 Microsoft Reporting Services and SQL Secure

You can implement Reports on any computer running Reporting Services. The following installation scenario illustrates how you can implement Microsoft Reporting Services reports in an existing SQL Server environment that uses a dedicated Report Server.

6.3.2 Required permissions for Microsoft Reporting Services

Microsoft Reporting Services Reports leverage the existing role-based security model provided with Reporting Services. These reports support Windows authentication (mixed mode on SQL Server) and require the following permissions and rights to successfully generate reports on your audit data.

Assessing the appropriate role on the SQL Secure folder in Report Manager, the individual report files inherit the permissions you set. By default, the Deploy Reports Wizard writes the report files to the `C:\Program Files\IderaSQLsecure\Reports` folder on the Report Server computer.

Account	Action	Requirement
Logon account used for install	Write RDL files to the Report server computer and configure reports	Write access to the Report Server file system and Content Manager role
Proxy user	Connect to the Repository and read data per report parameters	Read access to the Repository databases
Administrator	Configure reports and set security	Content Manager role
End user (auditor or manager)	Generate and view audit reports	Browse role

6.3.3 Install reports

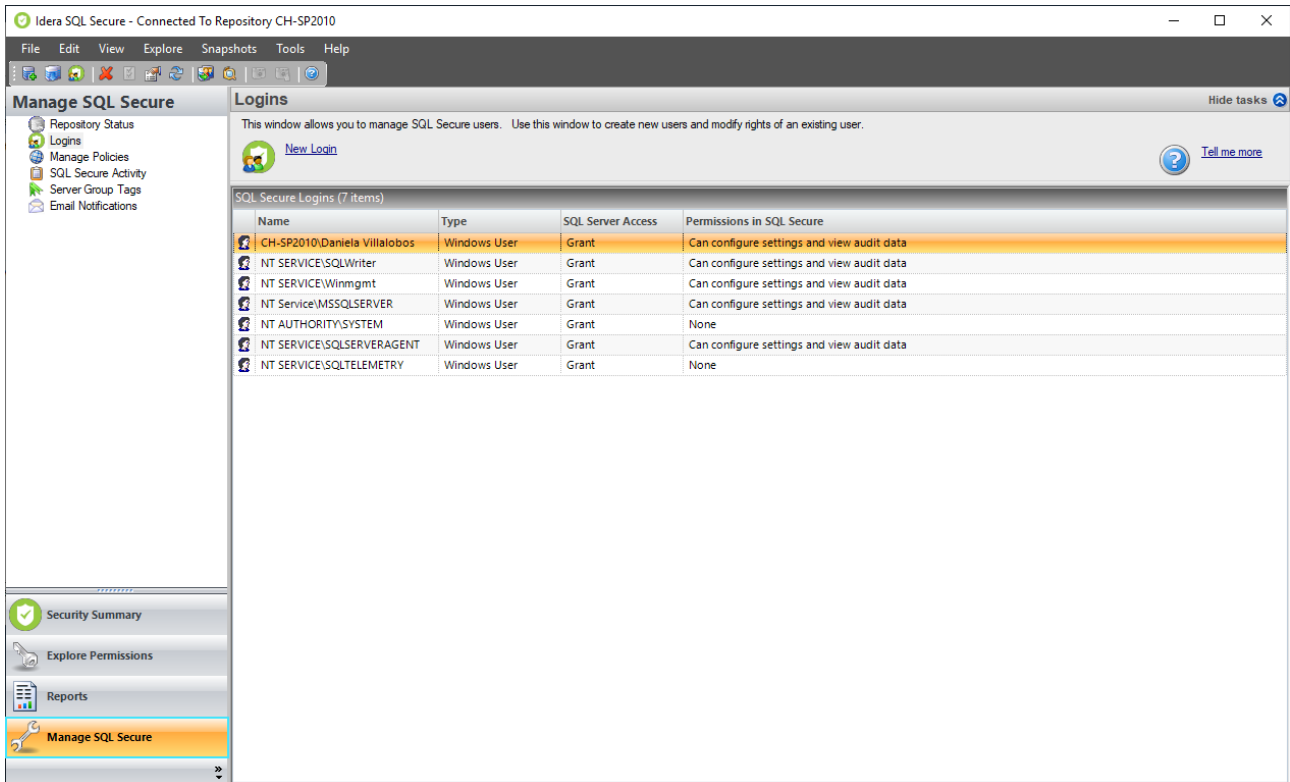
The [Deploy Reports wizard](#) allows you to specify the proxy user account credentials and deploy the reports. Perform this deployment for each Repository that contains data you want to audit using Reports. Once installed, click the **View Deployed Reports** link at the bottom of the SQL Secure Reports window to find your reports.

6.3.4 Set up permissions for auditors to generate reports

To grant auditors the ability to view and generate reports, create a SQL Server login and grant the **Can view** and **Report on audit data** permissions. Ensure that this account has the **Browse** role on the root folder.

7 Manage SQL Secure

The **Manage SQL Secure** view lets you easily and quickly change your IDERA SQL Secure configuration and review SQL Secure activity. From the **Manage SQL Secure** view, you can access the following information:



Repository Status

Allows you to [view status of the SQL Server instances](#) that are registered with SQL Secure, SQL Secure licenses, and the SQL Server Agent used for collecting data.

Logins

Allows you to [view a list of logins that are active in SQL Secure](#).

Policies

Allows you to [view and change properties of existing policies](#), view which assessments have been saved for each policy, or create a new policy.

SQL Secure Activity

Allows you to [see the logged events](#) associated with changes or actions that occur within SQL Secure.

Server Group Tags

Allows you to [view a list of tags](#) and servers that are available in IDERA SQL Secure.

Email notifications

Allows you to select the servers you want to receive notifications from.

7.1 View the SQL Secure Repository status

The **Repository Status** window allows you to view status of the SQL Server instances that are registered with IDERA SQL Secure, SQL Secure licenses, and the SQL Server Agent used for collecting data.

Repository Status

This window lists the SQL Server instances that are registered with SQL Secure. Registering a SQL Server instance allows you to perform comprehensive capture, analysis and reporting on SQL Server and related AD and OS security.

[Register a SQL Server](#) [Import SQL Servers](#)

System Status

All features are functioning normally

Repository: CH-SP2010
SQL Server 2012 v11.00.5058

License: 20 servers

Size on Disk: 44.75 MB

Last Groomed: Never

License Summary

Server Licenses:

Audited Servers:

Remaining Licenses:

SQL Server Agent Status

Started

SQL Secure uses the Repository SQL Server Agent for data collection and grooming. The SQL Server Agent must be started for SQL Secure to collect data or groom the Repository.

Audited SQL Servers Status

Audited SQL Servers (1 items)

SQL Server	Status	Last Successful Collection	Last Collection	Collector Job Status
CH-SP2010	Warnings	8/29/2018 6:47:23 AM	8/29/2018 6:47:...	Succeeded

7.1.1 System Status

The **System Status** section lists the SQL Server instance where the Repository resides and the version of SQL Server being utilized. In addition, the total number of SQL Secure licenses, the amount of space the Repository is using, and the time of the last Repository grooming is listed. For more information on grooming, see [Grooming Snapshots](#).

7.1.2 License Summary

The **License Summary** provides a graphical representation of the total number of SQL Server instances that can be monitored using your current SQL Secure licenses, the number of SQL Server instances currently being monitored by SQL Secure, and the number of additional SQL Server instances that can be monitored by SQL Secure. For more information, see [Managing Your SQL Secure Licenses](#).

7.1.3 SQL Server Agent Status

The **SQL Server Agent Status** section displays the current status of the SQL Server Agent that SQL Secure uses to collect security information.

If the SQL Server Agent is stopped, you must start the agent on the SQL Server instance hosting the Repository or snapshots cannot be taken. For more information, see Microsoft Books Online.

7.1.4 Audited SQL Servers Status

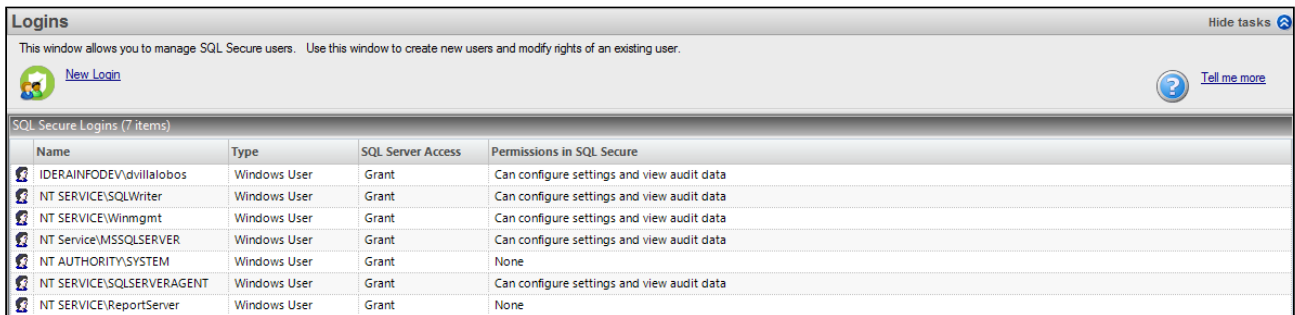
The **Audited SQL Servers** section lists each audited SQL Server registered with SQL Secure. The list contains the status, last successful collection, and last collection attempted for each of the audited SQL Servers. Right-click a SQL Server instance in the list to explore user or object permissions, view the SQL Server instance summary, register a new SQL Server instance, remove the SQL Server instance from SQL Secure, configure the snapshot collection, manually take a snapshot, refresh, or view the properties of the SQL Server instance.


The following information is provided for each SQL Server instance:

Property	Column Description
SQL Server	Displays the name of the SQL Server instance that is being audited
Status	Displays any warnings or errors that may have occurred with the last snapshot
Last Successful Collection	Displays the date and time that the latest snapshot was taken and completed successfully
Last Collection	Displays the date and time that the last snapshot was attempted (whether or not it was completed successfully)
Collector Job Status	Describes the current status of the SQL Server job running the audit data collection

7.2 Manage SQL Secure logins

The **Logins** window allows you to view a list of logins that are active in IDERA SQL Secure. This list provides the name, type of login, SQL Server access, and permissions in SQL Secure for each login. From this window, you can add new logins, delete logins, and edit login properties.



 A user must have a SQL Secure login to use SQL Secure features, such as Reports.

Each SQL Secure access level maps to a specific SQL Server role that SQL Secure provides in the Repository. You can assign these SQL Secure roles to an existing login using SQL Server Enterprise Manager or Management Studio.

The following information is displayed in the **Logins** window:

Column	Description
Name	List the logins that are associated with the SQL Secure Repository database.
Type	Describes the type of login (Standard, windows Group, Windows User)
SQL Server Access	Describes the type of access the user has on the SQL Secure Repository database.
Permissions in SQL Secure	Describes the type of access the user has within the SQL Secure Console.

To know how to add or edit logins, go [Add New Login](#) and/or [Edit Login settings](#).

7.2.1 Add new login

The IDERA **SQL Secure New Login** Wizard allows you to add new SQL Server logins to SQL Secure. In this wizard, you will be asked to supply the [Windows user account name](#) and [level of access](#) for the user you would like to add.

To access the **SQL Secure New Login** wizard, click **New Login** at the top of the **Logins** window in the **Manage SQL Secure** view. Alternatively, you can go to **File** menu and select **New SQL Secure Login**.



The **SQL Secure New Login** has the following sections:

Specify Login Properties

SQL Secure New Login

Add a new SQL Server login
Specify a Windows user account name that will be given access to SQL Secure.

Name

Do you want to grant this user access to SQL Secure?


Grant access
 Deny access

< Back Next > Cancel Help

The **Add a new SQL Server login** window allows you to enter the Windows account name of the user you would like to add to IDERA SQL Secure. You can also specify whether or not you would like to grant access to this user. Follow these steps to add a new login:

1. Type the Windows user account in the **Name** field.
2. To grant the user access to SQL Secure, select the **Grant access** option, then click **Next**.

By selecting the **Deny access** option, the user will be blocked from accessing SQL Secure.

 The user account must be entered in a domain\username and case-sensitive format.

Select Permissions

SQL Secure New Login

Set the SQL Secure permission level
Specify the permission level of the new user.

To grant permissions to configure audit settings, the login will be added to the sysadmin role on the SQL Server that hosts the Repository.

Do you want to add this login to the sysadmin server role?

Yes, grant this user permission to configure SQL Secure.

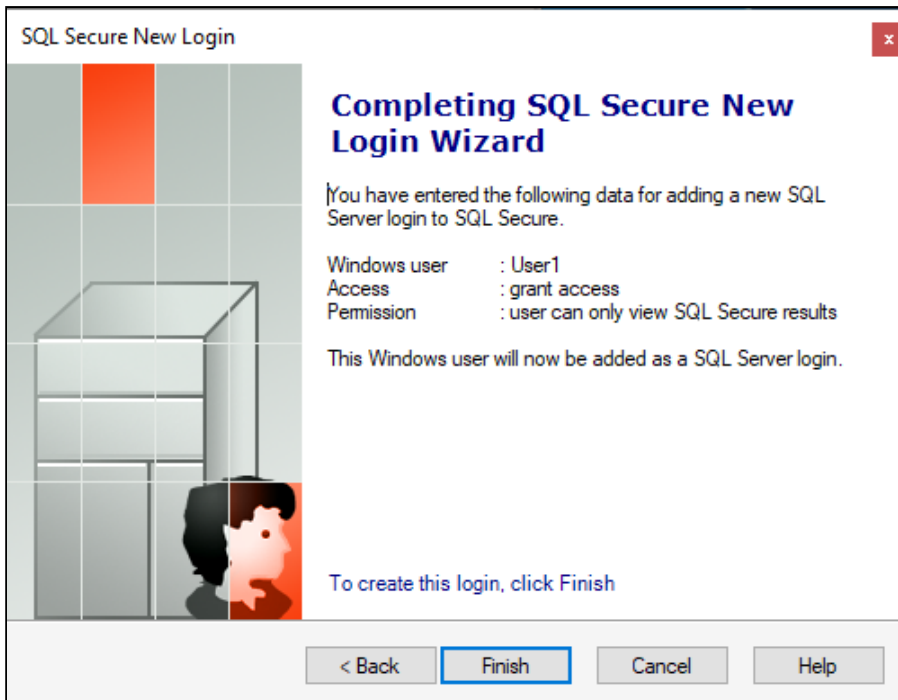
No, only allow this user the ability to view audit data.

< Back Next > Cancel Help

The **Set the SQL Secure Permission level** window allows you to choose whether or not the user should have access to IDERA SQL Secure and at what level. The user can have permissions to configure SQL Secure settings or only permissions to view audit data.

⚠ If you choose to grant permissions to configure audit settings, then you are assigning administrative level permissions; therefore, the login will be added to the sysadmin role on the SQL Server that hosts the Repository.

Review Login Summary



Review the provided summary of the login you are creating, and then click **Finish**. When you finish this wizard, IDERA SQL Secure creates a SQL Server login with the specified permissions on the SQL Server instance that hosts the Repository databases.

If you want to change a setting now, click **Back** to return to the appropriate window. You can also change login settings later using the [Login Properties window](#).

i A Repository login (database user) can be assigned SQL Secure permissions. These permissions control what tasks you are able to do in SQL Secure.

7.2.2 Edit login settings

IDERA SQL Secure allows you to edit individual login permissions (to SQL Secure) from the **Manage SQL Secure** view.

To edit SQL Secure login properties:

1. Select **Logins** from the **Manage SQL Secure** view.
2. In the list of Logins, right-click the login you want to edit and select **Properties**.

3. You can edit the **Security Access** properties (Grant or Deny access) or the **Permissions within SQL Secure** (where you decide if the login has Administrator server role or not). Click **OK** to queue your changes. The SQL Secure login has been edited and the new settings will apply the next time the user logs into SQL Secure.

7.3 Manage policies

Use the **Manage Policies** view of the **Manage SQL Secure** view to obtain a quick overview of which policies are enabled and have saved assessments.

The screenshot shows the 'Manage Policies' interface. It features a 'Policies (3 items)' table and an 'Assessments - CIS for SQL Server 2000 (3 items)' table.

Name	High Configured	Medium Configured	Low Configured	Assessments	Dynamic	Review Notes	Description
All Servers	36	21	55	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Global security checks that should be performed on all SQL Servers; based on the I...
CIS for SQL Server 2000	3	3	27	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Center for Internet Security - Benchmark for Microsoft SQL Server 2000, V 1.0, Dec...
DISA-NIST STIG for SQL Server 2014	3	6	4	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Defense Information Systems Agency (DISA) & National Institute of Standards and...

Name	High Configured	Medium Configured	Low Configured	State	Date	Description			
Assessment 3	6	1	3	27	7	Published	8/29/2018 10:22:26 AM	Center for Internet Security - Benchmark for Microsoft SQL Server 20...	
Assessment 2	3	1	3	0	27	7	Draft	8/29/2018 10:02:12 AM	Center for Internet Security - Benchmark for Microsoft SQL Server 20...
Assessment 1	3	1	3	0	27	7	Approved	8/29/2018 9:33:38 AM	Center for Internet Security - Benchmark for Microsoft SQL Server 20...

7.3.1 Available columns

These are the available columns in the **Policies** section:

Name

Provides the name of the policy

High Configured

Indicates how many high risk security checks were configured for this policy

Medium Configured

Indicates how many medium risk security checks were configured for this policy

Low Configured

Indicates how many low risk security checks were configured for this policy

Assessments

Indicates how many assessments have been saved from this policy.

Dynamic

Indicates whether this policy dynamically includes any newly registered SQL Server instance.

Review Notes

Indicates whether this policy has Internal Review Notes.

Description

Provides the description specified for this policy

Policy ID

Indicates the ID SQL Secure has defined for the policy

These are the available columns in the **Assessments** section:

Name

Provides the name of the assessment

High Configured

Indicates how many high risk security checks were configured for this assessment

High Icon

Indicates how many high risk findings this assessment had when last run

Medium Configured

Indicates how many medium risk security checks were configured for this assessment

Medium Icon

Indicates how many medium risk findings this assessment had when last run

Low Configured

Indicates how many low risk security checks were configured for this assessment

Low Icon

Indicates how many low risk findings this assessment had when last run

State

Provides the state (Draft, Published, Approved) of this assessment

Date

Indicates the date and time of the audit data used by this assessment. SQL Secure pulls the audit data from the snapshot that most closely matches this date and time

Description

Provides the description specified for this assessment

Assessment ID

Indicates the ID SQL Secure has defined for the assessment

7.4 View SQL Secure activity

Each time a change or action occurs in IDERA SQL Secure, an event is logged. These logged events appear in the **SQL Secure Activity** view. This log includes collection activity, snapshot configuration changes, SQL Secure login changes, and any other changes made to your SQL Secure settings.

The screenshot shows the 'SQL Secure Activity' window with a table of activity logs. The table has the following columns: Type, Date, Time, SQL Server, User, Category, Code, and Description. The log contains 291 items, all of which are 'Success Audit' events. The descriptions include various security checks and assessments, such as 'Updated report configuration table', 'Assessment "CIS for SQL Server 2000"', and 'Security Check "Certificate private keys were never exported"'.

7.4.1 Available event data

The following columns are available in the **SQL Secure Activity** logs:

Column	Description
Type	Displays the type of event that occurred
Date and Time	Displays the date and time when the event occurred
SQL Server	Provides the name of the SQL Server instance where the event occurred
User	Provides the name of the user who initiated the event
Category	Provides the category of the event
Code	Displays a description of the code that is used in the event

Column	Description
Description	Displays a short description of the event

✔ You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

7.5 Manage server group tags

The **Server Group Tags** view lets you view a list of tags that are available in IDERA SQL Secure. Click a tag, and SQL Secure displays the list of SQL Servers within that tag at the bottom of the view. Use tags to group or organize instances for better management when taking snapshots. You can:

- snapshot all the servers you have registered
- snapshot a particular tagged group of servers
- snapshot a specific set of multiple tagged servers

For more information about snapshots, see [Use snapshots to collect audit data](#).

7.5.1 Managing tags

Users can create, edit, and delete tags using the Server Group Tags view available from the Manage SQL Secure view.

To create a server group tag:

- Click **Create Server Group Tag**.

To edit an existing tag:

1. Right-click the tag you want to edit, and then select **Edit Tag** where you can edit the name a description of the tag.
2. Make the appropriate change(s), and then click **OK**.

To add server(s) to the tag:

1. Right-click the tag to which you want to add a server, and select **Add Server(s)**.
2. Select the SQL Server you want to add to the tag from the list of available servers.
3. Click **OK**.

To delete an existing tag:

- Right-click the tag you want to delete, and then select **Delete Tag**. SQL Secure removes the tag from the list and no longer offers the tag as an option when registering a server.



You can choose which columns to display on this list, group by columns, save the information, and print it, by going to the menu grid located on the top right section.

7.5.2 Creating a snapshot on the tag

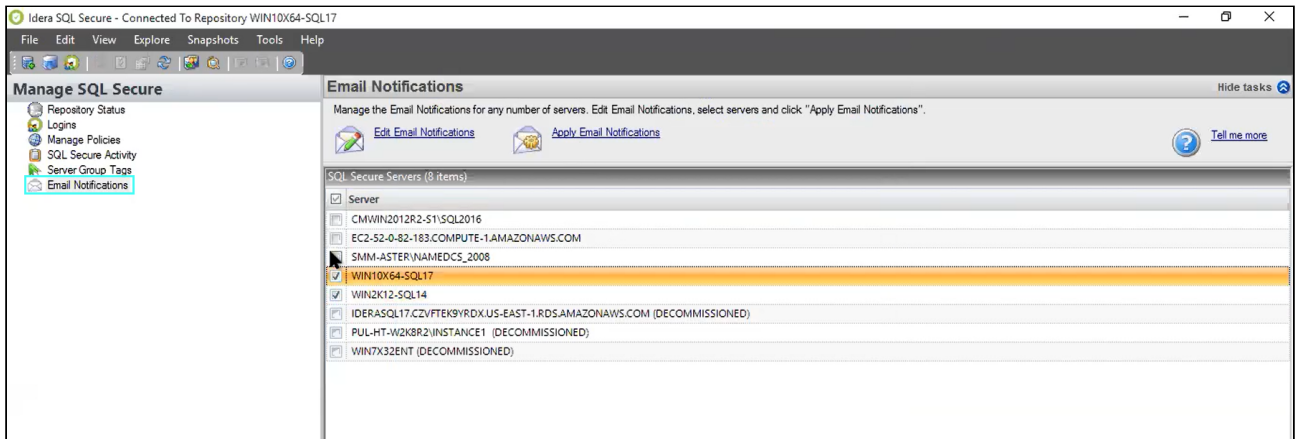
Selecting SQL Servers to include in a snapshot is much faster when the servers all are tagged with the same server group tag. Use the following steps to take a snapshot from a tag already populated with the appropriate SQL Servers.

To take a snapshot of the servers in a tag:

1. In the **Manage SQL Secure** view, click the **Server Group Tags** option.
2. Take the snapshot using one of the following processes:
 - Select the tag you want to snapshot, and then select Take Snapshot Now from the Snapshots menu.
 - Right-click the tag you want to snapshot, and then select **Take Snapshot Now**. SQL Secure takes a snapshot of the servers in the selected server group tag.

7.6 Bulk Email Notifications

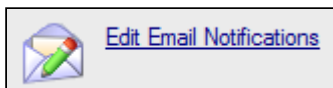
The **Email Notifications** option lets you configure the email notifications for the number of servers you select.



On the **SQL Secure Servers** section you will be able to see a list of all your monitored servers, each server with a check box. Select the number of servers from which you want to receive emails when snapshot collection process finishes.

7.6.1 Edit Email Notifications

You will have the option to **Edit Email notifications** at the top of the window.



A **Edit Email Notifications Settings** wizard will display after selecting the option.

Edit Email Notifications Settings [X]

Edit Email Notifications for snapshot status and findings. Any edits made in this dialog will not be applied to the servers until a server is selected from the list and "Apply Email Notifications" is clicked.

Send Email Notification after Data Collection

Always

On Warning and Error

Only On Error

Send Email Notification for Security Findings

Any Risk

On High and Medium Risks

Only on High Risks

Email Recipient:

(specify multiple email recipients by separating each address with a semicolon)

OK Cancel Help

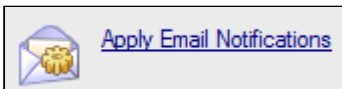
You can determine the way email notifications are sent after a snapshot is collected. You can set the following notifications:

- Email notifications sent after a snapshot is collected successfully, or only if there are warnings or errors. (Always, On Warning and Error, or Only On Error)
- Email notifications sent depending on the level of the security risks discovered. (Any Risk, On High and Medium Risks, or Only on High Risks)

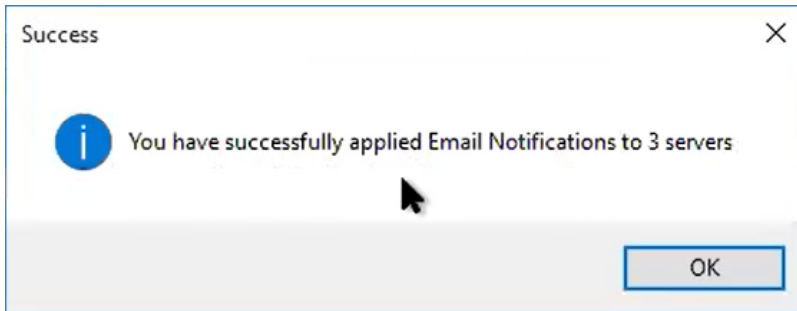
You can configure the **Email Recipient** space with one or more emails separating each email address with a semicolon.


7.6.2 Apply Email Notifications

After selecting the servers from which you want to receive emails, the **Apply Email Notifications** option will be available at the top of the window.



Click on the option and a confirmation notification will display, letting you know the number of servers the email notifications were configured for.




 You cannot select decommissioned servers as part of bulk email notifications.

8 Manage your license

IDERA SQL Secure provides an intuitive, simple-to-use interface for license key management. You can view the status of the license keys and add licenses to audit additional instances.

When you reach the SQL Server limit dictated by your license, SQL Secure will not let you add new servers. Take into account the following scenarios:

- **If your trial period expires** - you will be prompted for a new license when you start the SQL Secure Console.
- **If a valid license is not provided** - then SQL Secure will shut down and no longer be accessible.

 SQL Secure requires a license for each instance of SQL Server to be audited.

To view your **License Summary**, go to the **Manage SQL Secure** view, **Repository Status** window. The System Status section lists your Repository name, number of licenses, disk space, and the timestamp for the most recent grooming. In the **License Summary** section, SQL Secure displays bar graphs to help you compare between you number of Server Licenses, Audited Servers, and Remaining Licenses. **If you have Azure SQL Databases**, see [SQL Secure licensing with Azure SQL Database](#) for more information.

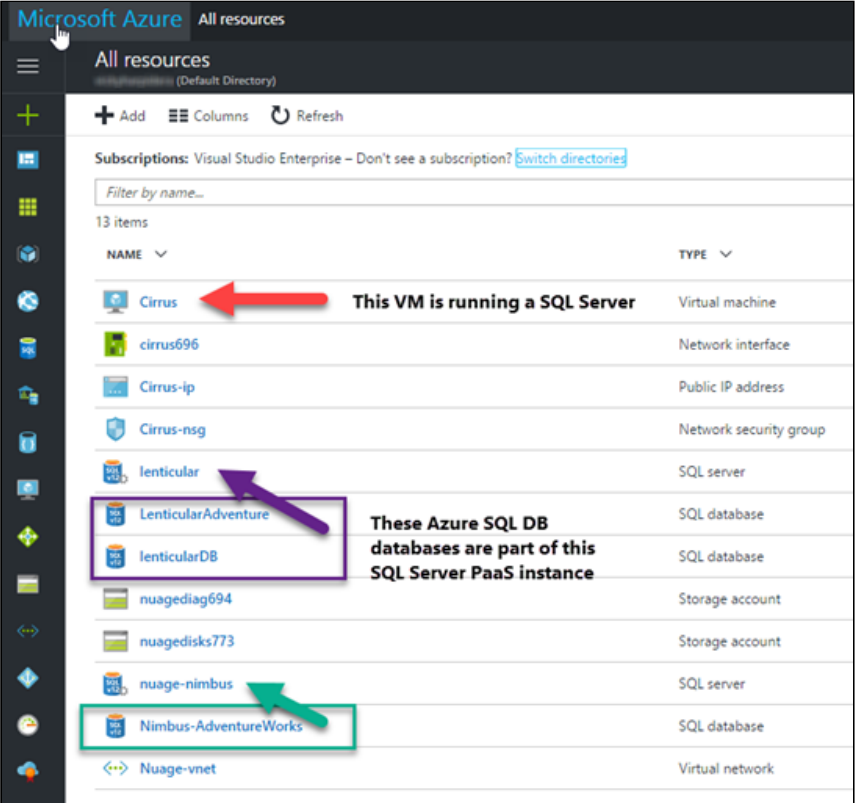
To manage your licenses, go to **File** menu, and select **Manage SQL Secure licenses**. In the Manage SQL Secure Licenses window, you can see your actual license key, the number of servers it is for, and the number of days until it expires. In the License details you can also see the type of license you have, the exact date of expiration, and the repository for which is licensed.

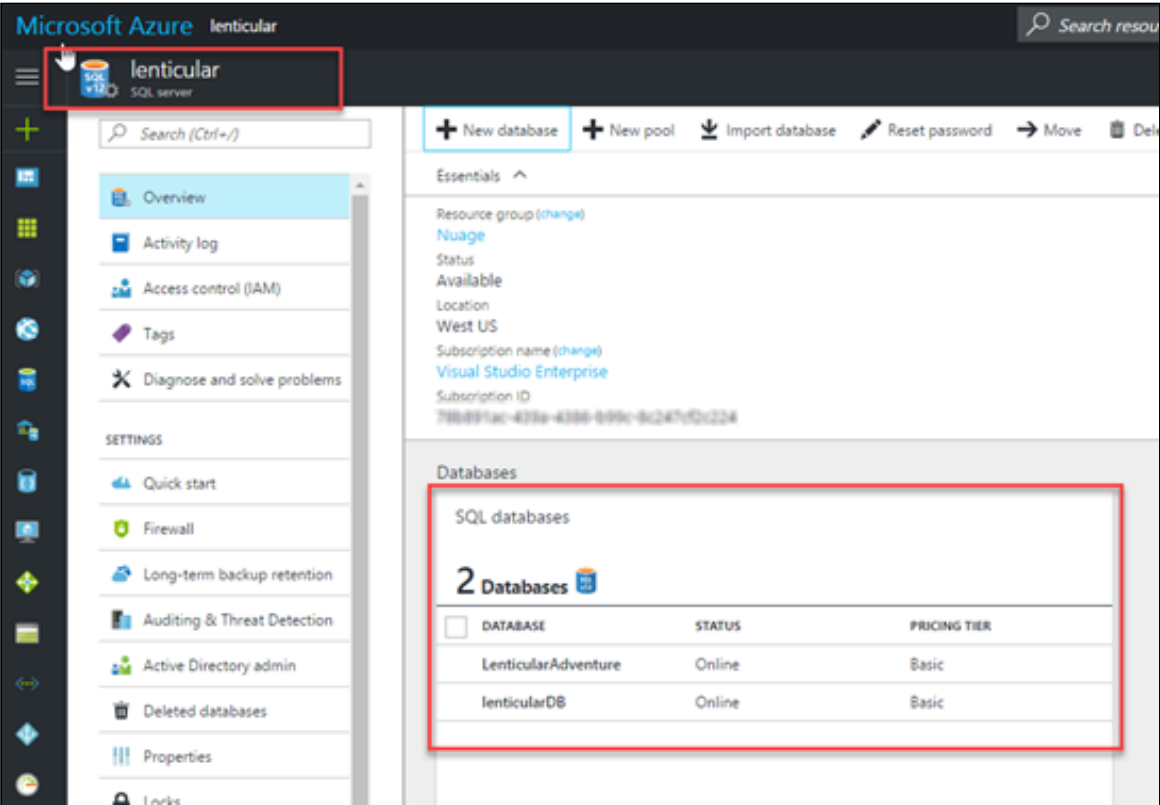
Click **Add** to add a new license key.

8.1 SQL Secure licensing with Azure SQL Database

This topic helps clarify the per-instance licensing of IDERA SQL Secure when dealing with Azure SQL Database instances. Simply, you add Azure SQL Database to monitor in SQL Secure using the instance name, just as you do with on-premises and Information as a Service (IaaS) instances. IDERA licensing works the same way.

In Azure SQL Database, there is still the logical construct of a "SQL Server," although it is a Platform as a Service (PaaS) implementation. When you set up an Azure SQL Database in the Azure Portal you do so by creating a SQL Server (which is not to be confused with a SQL Server running on a VM) and then you create databases. The following images help illustrate this concept:






In the previous images, the SQL Server "lenticular," which is located at **lenticular.database.windows.net**, is the host for a set of Azure SQL Databases. In IDERA SQL Secure, you would register the "lenticular.database.windows.net" name and have access to all of the SQL Databases in that instance. The following image shows how this license is applied in IDERA SQL Secure.

Repository Status


This window lists the SQL Server instances that are registered with SQLsecure. Registering a SQL Server instance allows you to perform comprehensive

[Register a SQL Server](#) [Import SQL Servers](#)

System Status

 All features are functioning normally

Repository: CIRRUS
SQL Server 2016 v13.00.4202



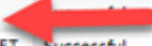

License: 3 servers 

Size on Disk: 592.00 MB

Last Groomed: 4/3/2017 12:00:00 AM

Audited SQL Servers Status

Audited SQL Servers (3 items)

SQL Server	Status	Last Successful Collection	Last Collection	Collector Job Status
 CIRRUS	Warnings	4/2/2017 3:00:01 AM	4/2/2017 3:00:0...	Succeeded
 LENTICULAR.DATABASE.WINDOWS.NET 	Warnings	4/2/2017 3:00:01 AM	4/2/2017 3:00:0...	Running
 SQLSECUREACC.DATABASE.WINDOWS.NET	Successful	4/2/2017 3:00:05 AM	4/2/2017 3:00:0...	Succeeded

9 Edit audited SQL Server properties

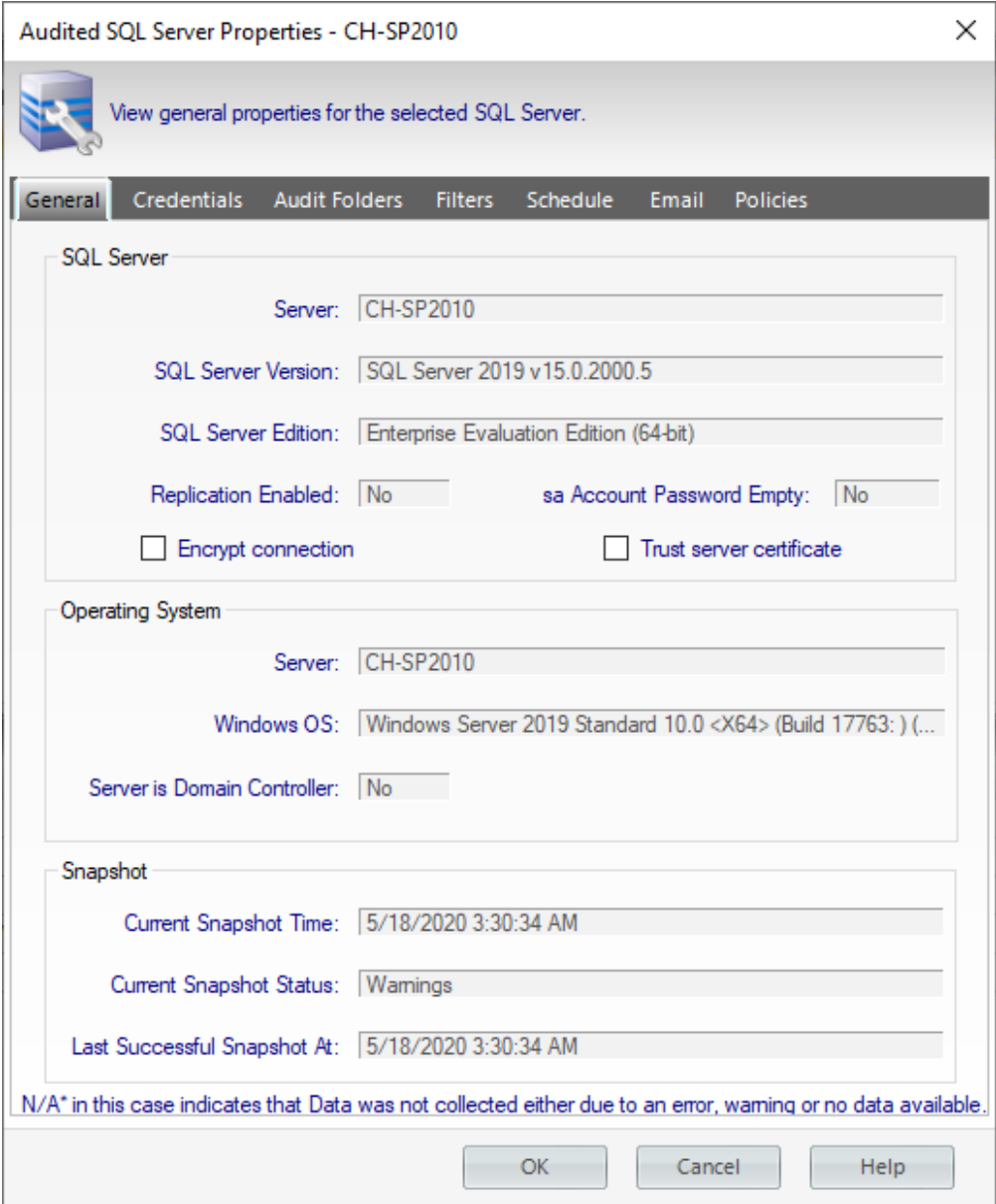
The **Audited SQL Server Properties** window allows you to edit the way IDERA SQL Secure monitors your SQL Server instances. The **Audited SQL Server Properties** window contains general SQL Server instance information, credentials used to collect data, specified audit folders, snapshot filter settings, audit data collection schedule, email notifications settings, and policies the SQL Server pertains to.

To access the **Audited SQL Server Properties** window use any of the following options:

- Right-click the SQL Server instance from the **Explore Permissions** view and select **Configure Audit Settings**.
- Select the respective SQL Server in the **Servers in Policy** tree from the **Security Summary** view, and either right click to select **Configure Audit Settings** or select the same option from the ribbon options available in the **Summary**, **Settings**, or **Users** tabs.

9.1 Change general properties

The **General** tab of IDERA SQL Secure contains basic information about your audited SQL Server, including the instance name, the SQL Server version, snapshot information, and security and auditing information.



Property Group	Description
SQL Server	<p>Contains the name of the computer hosting the SQL Server instance belongs to, the SQL Server instance name, version number, edition, if replication is enabled, and whether the sa account password is empty.</p> <p>Note that when viewing information for Azure SQL Database, this section includes a field for whether geo-replication (readable secondary databases) is enabled, but does not include the sa account password field.</p>
Operating System	<p>Contains the basic information of the operating system: server name, Windows OS, and if Server is Domain Controller</p> <p>Note that when viewing information for Azure SQL Database, this section does not include a field for whether the server is a domain controller.</p>
Snapshot	<p>Contains basic snapshot information including the time and date of the current snapshot, the snapshot status, and when the last successful snapshot was taken.</p>

9.2 Change connection credentials

The **Credentials** tab displays the credentials that IDERA SQL Secure uses to access the databases on the selected SQL Server instance. If you need to make changes to your credentials, change the information in the fields provided.

The screenshot shows the 'Audited SQL Server Properties - CH-SP2010' dialog box with the 'Credentials' tab selected. The dialog has a title bar with a close button (X) and a subtitle 'Specify which credentials SQL Secure should use to collect audit data.' Below the subtitle is a tabbed interface with 'General', 'Credentials', 'Audit Folders', 'Filters', 'Schedule', 'Email', and 'Policies'. The 'Credentials' tab is active, and a message states: 'This window allows you to change the credentials that are used to collect data for auditing.'


The main content area is divided into two sections:

- SQL Server credentials to connect to audited SQL Server:**
 - Windows Authentication:**
 - Windows User: CH-SP2010\Daniela Villalobos
 - Password: [masked]
 - SQL Server Authentication:**
 - Login Name: [empty]
 - Password: [empty]
- Windows Credentials to gather Operating System and Active Directory objects:**
 - Windows credentials are used to connect to the target server to gather Active Directory objects and file and registry key permissions. The specified account must have admin access to the target server and at least login access to the SQLsecure Repository.
 - Use same Windows Authentication as above**
 - Windows User: CH-SP2010\Daniela Villalobos
 - Password: [masked]

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

There are two types of credentials you need to specify:

Option	Description
SQL Server credentials to connect to audited SQL Server	Choose one of the following options: <ul style="list-style-type: none"> • Select Azure Active Directory and enter the credentials for your Azure AD account. • Select Windows Authentication and enter the credentials in the fields provided. • Click SQL Server Authentication to use the default credentials of your SQL Server Agent.
Azure AD or Windows Credentials to gather Operating System and Active Directory objects - These credentials are used to connect to the target server to gather Active Directory objects, file, and registry key permissions.	Select one of the following options: <ul style="list-style-type: none"> • Check the Use same Windows Authentication as above box to use the windows credentials specified above. • Specify a different Windows account that SQL Secure will use to gather information about OS and AD objects.


 If the login configuration for the SQL Server you want to audit is case-sensitive, you must enter your login credentials in a case-sensitive format.

Permissions and Privileges

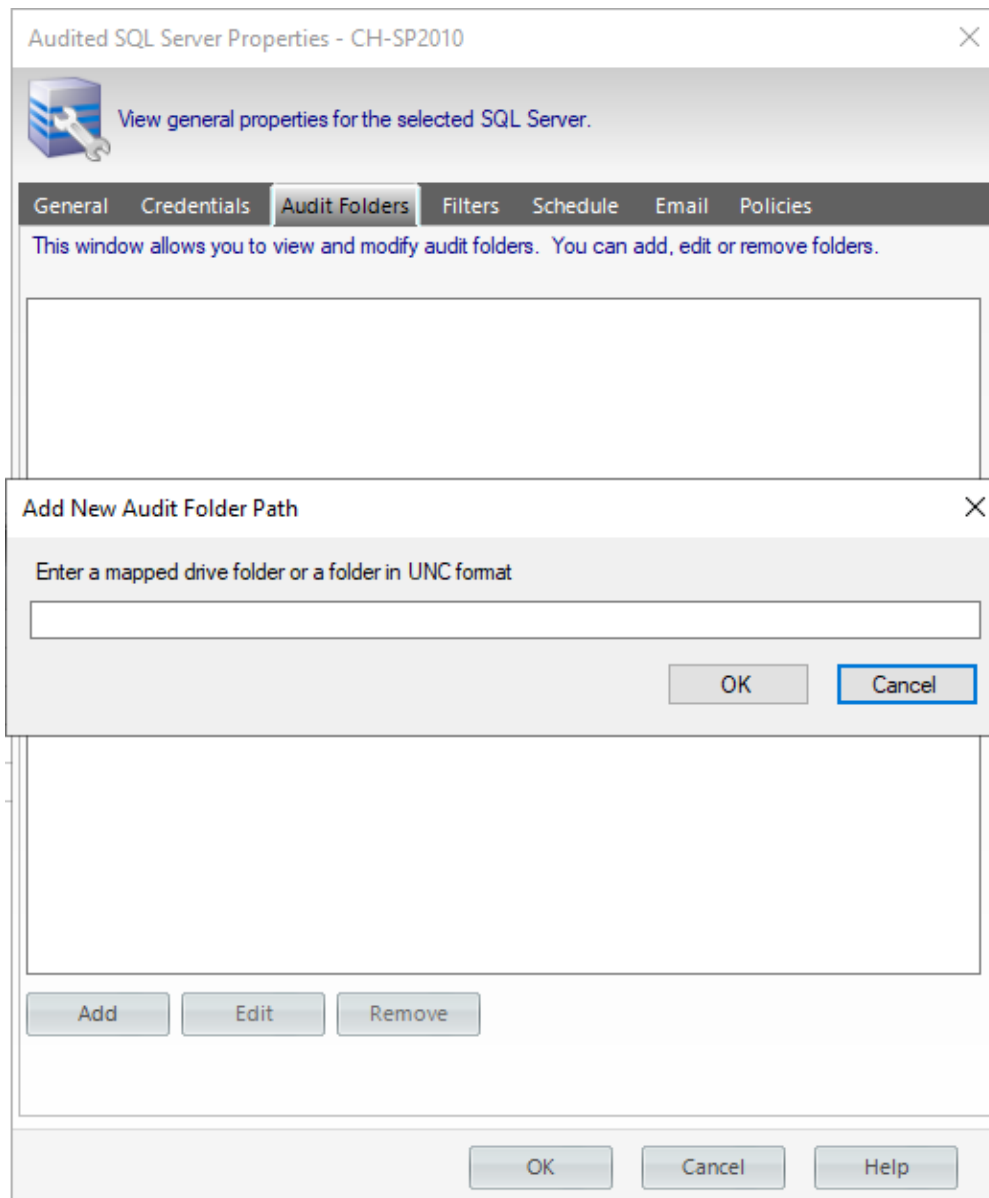
You should keep in mind the following permissions for the accounts specified in this section:

- The SQL Server login must belong to the sysadmin fixed role on the target instance.
- The Windows account must have Windows Administrator privileges on the target instance to collect group membership information.
- The account specified for gathering information about OS and AD objects must have admin access to the target server and at least login access to the SQL Secure Repository.

9.3 Define folders

 This tab is not available for Azure SQL databases.

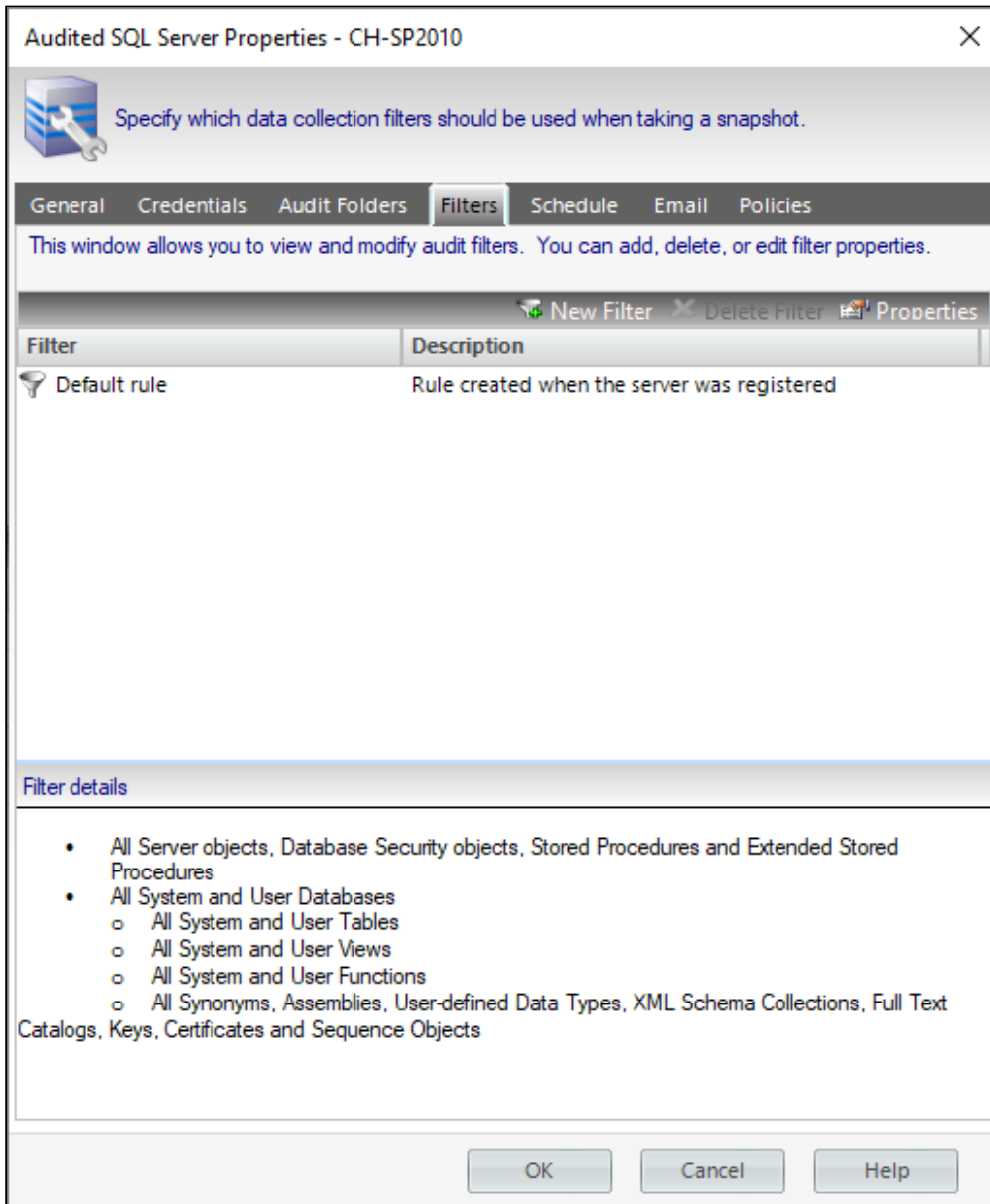
In the **Specify Audit Folders** section you can specify which folders will be audited for collecting file system permission information.



Click **Add** and type a mapped drive folder or a folder in UNC format. You can add as many folders as you require. If you want to change or delete any of the previously added folders, click **Edit** or **Remove** respectively.

9.4 Change audit filters

The **Filters** tab allows you to add a new filter, delete filters, and edit filter properties. Filters are the criteria used when collecting audit data for your snapshots.



Note that **All Extended Stored Procedures** and **All Full Text Catalogs** are disabled when viewing properties for Azure SQL Database.

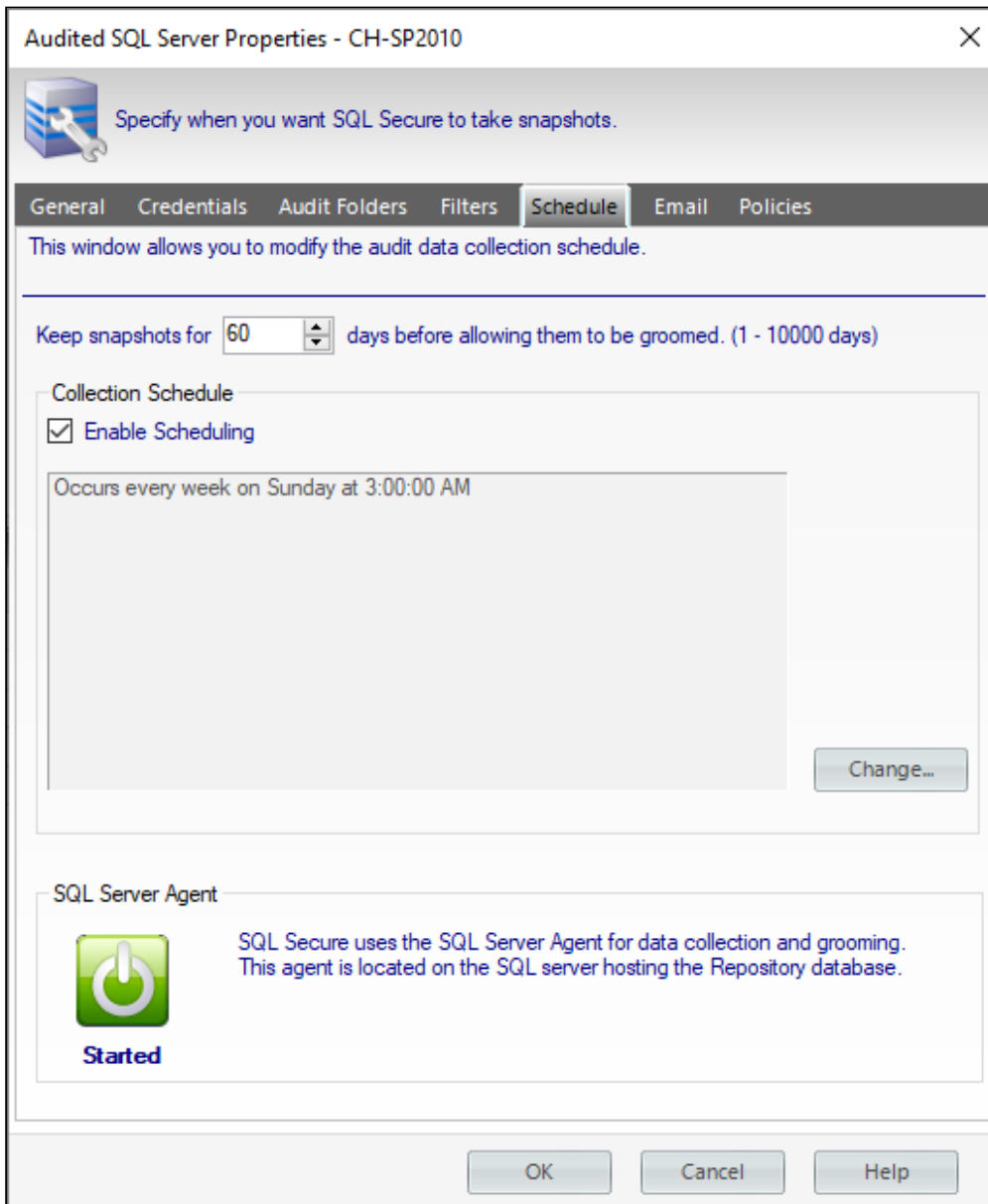
Option	Description
New Filter	This button opens the Add Filter Wizard, which allows you to add filters to your snapshot. For more information, see Add new filter .

Option	Description
Delete Filter	Click this button to delete the selected filter.
Properties	This button opens the Filter Properties dialog window, which allows you edit the selected filter settings. For more information, see Edit filter settings .

Once you have configured your snapshot collection settings, you can view your updated snapshots to ensure that they are set up the way you intended.

9.5 Change snapshot schedule

The **Schedule** tab allows you to choose the best times to generate a snapshot on your SQL Server instance. By default, snapshots are scheduled for every Sunday morning at 3:00 AM. It is recommended that you schedule snapshots to occur during "off-peak" hours.



The **Schedule** tab contains the schedule, if any, that is currently being used for the SQL Server selected instance. To change the schedule, click **Change** and select the new time and frequency for snapshot collection.

The first snapshot is taken at the first scheduled snapshot collection time. Snapshots can also be taken manually right-clicking the SQL Server instance in the **Explore Permissions** view and selecting **Take Snapshot Now**.

The **Schedule** tab displays the following information:

Option	Description
Keep snapshot for [number] days	Type, or use the up and down arrows, to indicate the number of days that you want to store snapshots in the SQL Secure Repository.
Enable Scheduling	Check this box to enable the defined audit snapshot schedule
Change	Click this button to edit your audit snapshot collection schedule.



- To view all properties of a snapshot, click the respective snapshot below the respective SQL Server in the **Audited SQL Servers** tree of the **Explore Permissions** view.
- You can also right-click the snapshot from the **Audited SQL Servers** tree of the **Explore Permissions** view and select **Properties**. The **Snapshot Properties** window opens with all its corresponding settings.

9.6 Change email notification

The **Email** tab allows you to configure the way email notifications are sent after a snapshot is collected. You can select to have email notifications sent after a snapshot is collected successfully, or only if there are warnings or errors. You can also select to have email notifications sent depending on the level of the security risks discovered.

Audited SQL Server Properties - CH-SP2010

Configure email notification for snapshot status and findings.

General Credentials Audit Folders Filters Schedule **Email** Policies

This window allows you to configure Email notification for Snapshots (data collections).

Send Email Notification after Data Collection

- Always
- On Warning and Error
- Only On Error

Send Email Notification for Security Findings

- Any Risk
- On High and Medium Risks
- Only on High Risks

Email Recipient:

(specify multiple email recipients by separating each address with a semicolon)

OK Cancel Help

Once you have configured when notifications are sent, enter the email address in the **Email Recipient** field. To enter multiple email addresses, separate each address with a semi-colon.

i **If you do not want to receive email notifications for snapshot status or security finding**, unchecked the associated option.

9.7 Change which policies audit this instance

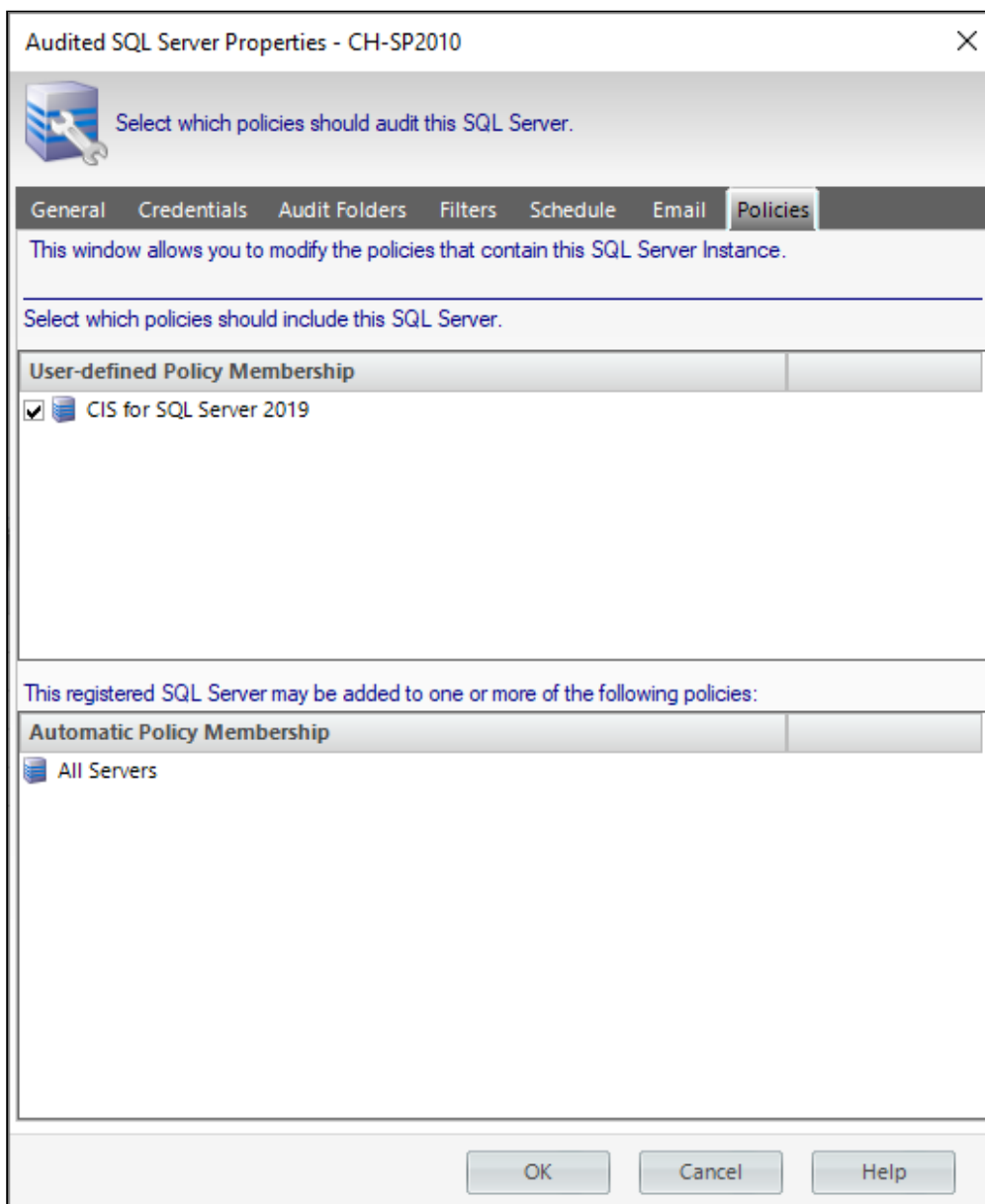
The **Policies** tab allows you to modify the policies to which the selected SQL Server instance is assigned. There are two kinds of policy memberships:

User-defined policy membership

A manual policy is a policy that must be manually assigned to a SQL Server instance.

Automatic policy membership

An automatic policy is a policy that is configured so that all SQL Server instances are automatically assigned to it.



10 Monitor Azure Databases

10.1 Register Azure SQL Database in SQL Secure

1. Run SQL Secure in the root of the installation kit.
2. On the main wizard select **File** and **Register a SQL Server**.
3. The **Welcome to the Register a SQL Server Wizard** displays a list of things to do in the registration process, click **Next** to continue.
4. In the **Select a SQL Server** page select and enter the following:
 - a. Server Type: Select **Azure SQL Database**.
 - b. Server: Enter your Server Name (i.e. [xxx.database.window.net](#)).
 - c. Port Number: Specify the default port number (1433) or the port number you configured on the Azure SQL Database Instance.
5. Click **Next** to continue.
6. Enter Azure Active Directory credentials or SQL Server Authentication credentials on the **Specify Connection Credentials** section, then Click **Next** to continue.

Connection Error

Configure your [Azure SQL Server Firewall](#) if a Connection Error displays.

7. On the **Add to Server Group** section, optionally select the **Server Group Tag** and click **Next**.
8. On the **Specify the SQL Server Objects to Audit** section, all objects are selected by default, select the ones you want to audit, and click **Next** to continue.
9. Set a schedule on the **Schedule Snapshots** section, and click **Next** to continue.
10. Configure notifications on the **Configure Email Notification** section, and click **Next**.
11. On the **Take a Snapshot** section, you have the following options:
 - a. Select the registration process option and wait until it ends, then begin with the collecting data process.
 - b. Let the data collection run on an schedule or manually collect data by selecting the registered server.

SQL Server Agent

Before you begin collecting data make sure that the **SQL Server Agent** is running, otherwise the data collection will fail.

12. Right Click and Take the snapshot.

11 Monitor Amazon Databases

SQL Secure lets you connect with Amazon instances in the following cases:

- Log in to RDS instance from On-Premise servers using On-Premise Directory service account user credentials (Windows Authentication).
- Log in to SQL Server installed on EC2 machines, from on-premise using a private IP address and Windows Authentication credentials on on-premise Directory service account.
- Read registry values and query Windows Operating System through WMI queries of EC2 machines from On-Premise using On-Premise Directory service account user credentials.

11.1 Manage Microsoft Active Directory with Amazon AWS

AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. For more details, please go through AWS documentation

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started.html

11.2 Setting up a VPN Tunnel to connect to Amazon instances

VPN tunnel is required to access SQL Server on Amazon EC2 and RDS from on-premise AD using windows authentication. Setting up VPN tunnel requires to essential steps:

11.2.1 Configuring AWS:

You can find the steps to configure the AWS in the following link:

<https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnections.html>

11.2.2 Configuring the Local Network:

This configuration mainly depends on the gateway device used. Identify the approach to create tunnel according the network being used. AWS provides the local gateway side configuration for many networks, like fortinet, as an example:

<https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnections.html>

<https://docs.aws.amazon.com/vpc/latest/adminguide/fortinet.html>

11.3 Connecting to your existing AD infrastructure

To use your existing AD infrastructure with AWS Managed Microsoft AD, trust relationship has to be established between both domains. Use the following documentation:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_tutorial_setup_trust.html

After establishing trust, you can connect to AWS EC2 instances using your on-premise AD.

Note: To log in into SQL Server on EC2 instance or RDS from on-premise using windows authentication, you can add on-premise active directory users to SQL Server Security -> Logins.

11.4 Authorizing Inbound Traffic for Your AWS security group

Security groups let you control and identify the kind of the traffic that can reach to your instance. Your default and created security groups include default rules that do not enable you to access your instance from the Internet. To enable network access to your instance, you must allow inbound traffic to your instance. To open a port for inbound traffic, add a rule to a security group that you associated with your instance when you launched it.

11.4.1 Adding a rule to a security group for inbound TCP traffic over IPv4 (AWS console)

Choose Instances in the navigation pane of the Amazon EC2/RDS console. Select your instance and look at the Description tab. A list of the security groups related with the instance displays. Choose view inbound rules to display a list of the rules that are in effect for the instance.

- In the navigation pane, choose Security Groups. Select one of the security groups associated with your instance.
- In the Details pane, on the Inbound tab choose Edit. In the dialog, choose Add Rule and then TCP from the type list.
- In the source field, choose Custom and specify the public IPv4 address of your computer or network in CIDR notation.
- Save the changes.

11.4.2 Some important ports to open:

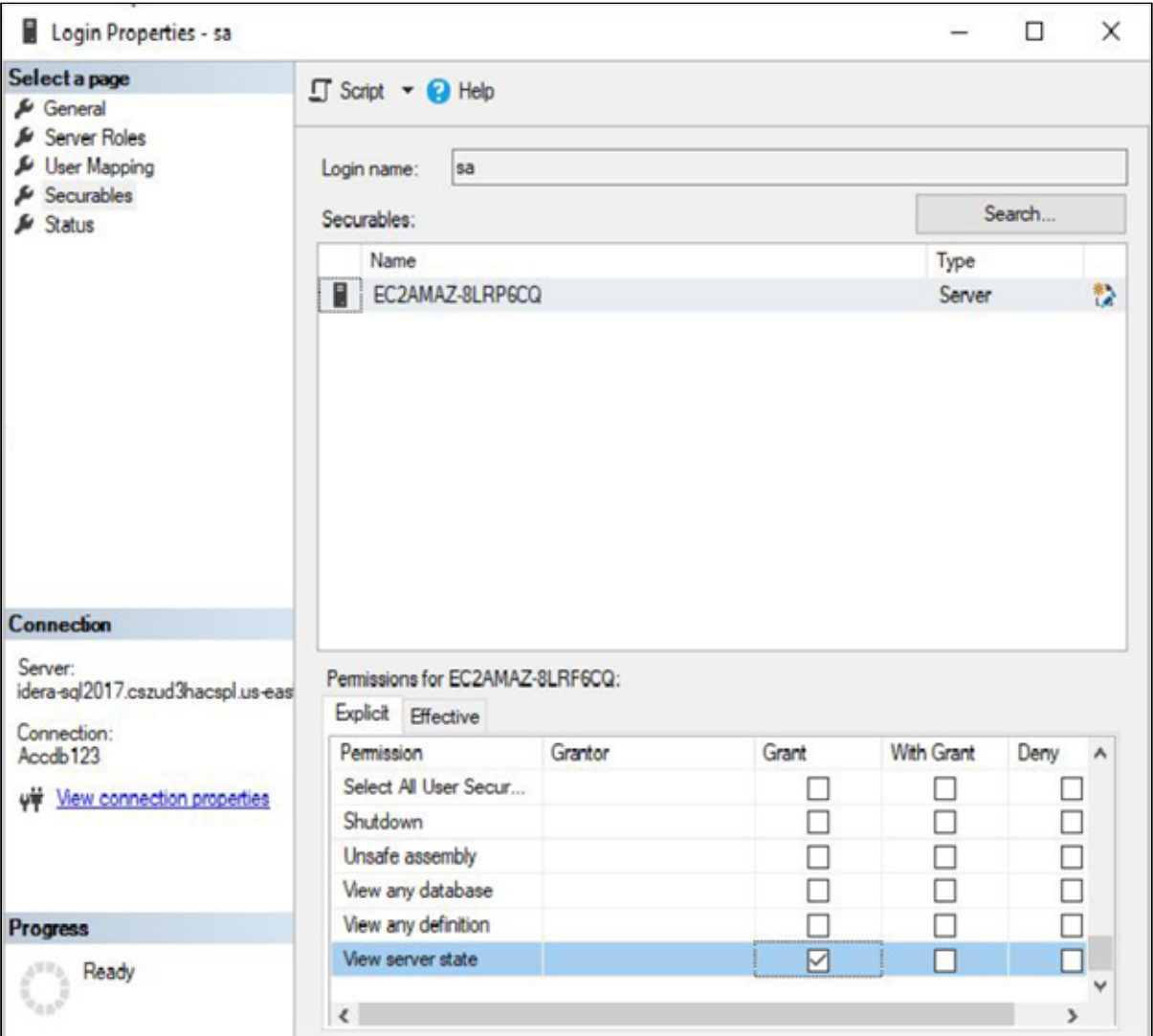
- TCP Port where SQL Server is installed. Default port is 1433.
- TCP Port for WMI. 135
- TCP Port for SMB. 445
- TCP Port for SQL Server Browser service. 1434
- TCP Port for RPC 49152-65535

Note: Note that other ports may be required depending on the respective environment.

11.5 Permissions to RDS for SQL Server log in

The login used for RDS for SQL Server needs permissions, right click on the log in and select Properties, then choose Securables and check Grant for:

- View server state
- Alter trace





12 Configure email settings

The **SMTP Email Provider** window of IDERA SQL Secure allows you to enter your provider information, through which email notifications are distributed.

To configure your SMTP Email Provider:

1. Open the **SMTP Email Provider** window from the **Tools** menu option and select **Configure SMTP mail**.
2. Enter the **Email Server Information**: the SMTP address, port number, and the number of seconds to wait before timing out.
3. If the logon for the SMTP Email Provider requires authentication, check the **Server requires authentication** box and enter the user name and password.
4. Enter the name and email address in the **Sender Information** section that will appear in the **From** field on the email notifications that are distributed by SQL Secure.
5. Click **OK**.

 To secure the transmission of your emails, check the **Requires SSL** checkbox to send your emails through an SSL channel.

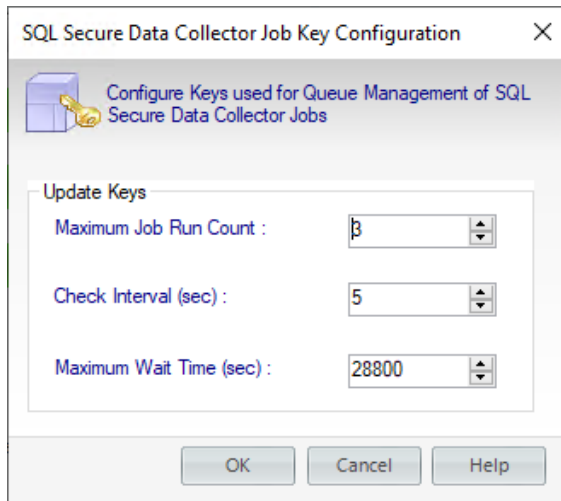
 You can use the option **Test** to see if your SMTP email server configurations are correct.

13 SQL Secure Collector Job Keys

The SQL Secure Data Collector Job Keys allow you to manage the flow of snapshot collection jobs. Use this step to throttle the collector jobs so that they do not overload the SQL Server instance.

13.1 Configure the Data Collector Job Keys:

1. In the menu options, click **Tools > Configure Collector Job Keys**.



2. Set the key parameters:

Maximum Job Run Count: - Controls the maximum number of SQL Agent jobs that can run before SQL Secure starts to throttle the execution of collector jobs. By default, this is set to 3.

SQL Secure doesn't include Non-SQL Secure jobs when calculating the number of running jobs.

Check Interval (sec): - Time in seconds the collector job waits before checking again to see if the number of running jobs is under the jobs throttle limit. By default, this is set to 5 seconds.

Maximum Wait time (sec): - Time in seconds the job attempts to run before failing. By default, this is set to 28800 seconds (8 hours).

With the keys described above, SQL Secure performs the following process before running a SQL Secure collector job:

- Checks to see if the Maximum Job Run Count has been hit. If SQL Secure reaches the throttle limit and a new collector job is scheduled to start, the collector job waits.
- After the number of seconds specified in the 'Check Interval' parameter, the job checks how many SQL Server agent jobs are running. The collector job starts if the number of jobs has dipped below the Maximum Job Run Count. If not, then the job continues waiting.
- If a job has been waiting for the Maximum Wait Time, the job ends the process, and the collector job fails.

14 Delete a Data Snapshot

When you no longer want to keep a snapshot (and do not want to wait for the grooming process to occur), go to the **Explore Permissions** view, expand the SQL Server instance from which the snapshot was taken, select the respective snapshot, right-click it, and select **Delete snapshot**. A confirmation window appears, click **Delete** to continue.

15 Troubleshooting WMI connectivity issues

The user account used by IDERA SQL Secure to gather Operation System and Active Directory objects must have administrator permissions on the remote server to be able to use WMI.

The most frequently encountered problems with WMI connectivity are:

- RPC traffic not getting through to the remote computer
- Invalid DCOM or WMI permissions
- Ports are not open or firewall is preventing access

The following Web links may provide additional information about how to troubleshoot WMI connectivity issues:

- [Securing a remote WMI Connection](#)
- [Help with Scripts](#)

15.1 Resolve WMI Issues using WbemTest

You can use the WbemTest (Windows Management Instrumentation Tester) tool to connect to a server and issue WMI queries. Download this tool from Microsoft TechNet. This tool can help you test and troubleshoot WMI issues.

To use WbemTest:

1. Run `wbemtest.exe`.
2. Click **Connect**.
3. In the **NameSpace test** box, enter `\\server\root\cimv2` where server is the name of the server you want to connect to.
4. Click **Connect**.
5. Click **Query**.
6. Enter **select*** from win32_process.
7. Click **Apply**.

If WbemTest was able to connect to the remote server and issue the query using WMI, you should see a query result with output. In this case, WMI to the required server is working and no further action is needed. For more information on the Windows Management Instrumentation Tester, refer to Windows Management Instrumentation Tester overview.

If you receive an error message, use the following processes to help identify and resolve the issue.

15.1.1 Error: The RPC Server Is Unavailable

This error usually indicates that the RPC traffic is not getting to the remote server, or there is no RPC listener on the remote server.

To troubleshoot this RPC error:

1. Ensure the Remote Procedure Call (RPC) service is running on the remote server.
2. Verify that there is a TCP listener on the remote server by running the `netstat -nao` command and verifying that there is the following entry: `TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1304`
3. In the Tools sub-directory, run `rpcping /s <servername> /t ncacn_tp_tcp` where `<servername>` is the name of the remote server. This command verifies that RPC can communicate with the remote server. The output should be similar to:
 - `Completed 1 calls in 15 ms`
 - `66 T/S or 15.000 ms/T`

4. Ensure that the traffic is not being blocked by local or internal network firewalls. Either disable the firewall or configure the Windows firewall to allow incoming RPC traffic.
5. Try to use the remote server IP address instead of the server name. If the IP address works, you may have a DNS issue.
6. **If the remote server resides in a different domain**, the two domains may not trust each other, or the user account being used does not have administrator permissions on the remote server/domain.
7. **If both computers are in the same domain**, and the user account has administrator permissions, try rejoining both computers to the domain.

15.1.2 Error: Access Denied

This error can indicate permission issues.

To troubleshoot this access error:

1. If the remote computer is running Windows XP, make sure Force Guest is disabled. This setting forces any connection to be impersonated as Guest.
 - a. Open the Local Security Policy console from Administrative Tools.
 - b. Browse to **Security Settings > Local Policies > Security Options**.
 - c. Double-click Network Access: Sharing And Security Model For LocalAccounts.
 - d. Change the settings from **Guest Only** to **Classic**.
2. Ensure that DCOM is enabled on the remote server:
 - a. Run `DcomCnfg` on the remote server.
 - b. Click **Component Services**.
 - c. Expand **Computers**.
 - d. Right click **My Computer** and select **Properties**.
 - e. Click the **Default Properties** tab.
 - f. Ensure **Enable Distributed COM** on this computer is checked.
3. Ensure the correct DCOM remote launch and activation permissions are configured:
 - a. Run `DcomCnfg` on the remote server.
 - b. Click **Component Services**.
 - c. Expand **Computers**.
 - d. Right click **My Computer** and select **Properties**.
 - e. Ensure **Enable Distributed COM** on this computer is checked.
 - f. Click the **Com Security** tab.
 - g. Under **Launch and Activation Permissions**, click **Edit Limits**.
 - h. In the Launch Permissions dialog box, make sure your user account or group is listed in the Groups or user names list. If your user account or group is not listed, click **Add** and add it to the list.
 - i. In the Launch Permission dialog box, select your user account or group in the Group or user names list. In the Allow column under Permissions for User, select **Remote Launch** and **Remote Activation**, and then click **OK**.
4. Ensure the correct DCOM remote access permissions are configured:
 - a. Run `DcomCnfg` on the remote server.
 - b. Click **Component Services**.
 - c. Expand **Computers**.
 - d. Right click **My Computer** and select **Properties**.
 - e. Ensure **Enable Distributed COM** on this computer is checked.
 - f. Click the **Com Security** tab.
 - g. Under **Access Permissions**, click **Edit Limits**.
 - h. In the Access Permission dialog box, select ANONYMOUS LOGON name in the Group or user names list. In the Allow column under Permissions for User, select **Remote Access**, and then click **OK**.
5. Ensure the correct WMI namespace permissions are configured.

- a. Run `wmimgmt.msc`.
- b. Right-click **WMI Control**, and then select **Connect to another computer**.
- c. Enter the remote server name, and then click **OK**.
- d. Right-click **WMI Control**, and then select **Properties**.
- e. In the Security tab, select the namespace, and then click **Security**.
- f. Locate the appropriate account, and then check **Remote Enable** in the Permissions list.


15.1.3 Warning: The Network Path Was Not Found

This warning typically indicates that SQL Secure cannot access the target computer due to closed ports or firewall access settings. Ensure the appropriate port is open on the target computer and check your firewall configuration.

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.

16 Select audited SQL Server to explore data

When you want to explore user or object permissions, you can select a specific SQL Server in any of the views of IDERA SQL Secure, right-click it, and select the options **Explore user permissions**, **Explore Role Permissions**, or **Explore Object permissions**. SQL Secure opens the respective tabs for the selected SQL Server.

 If the SQL Server instance you want to select is not listed, the instance may not be [registered with SQL Secure](#).

17 Troubleshooting guide/ Advanced solutions

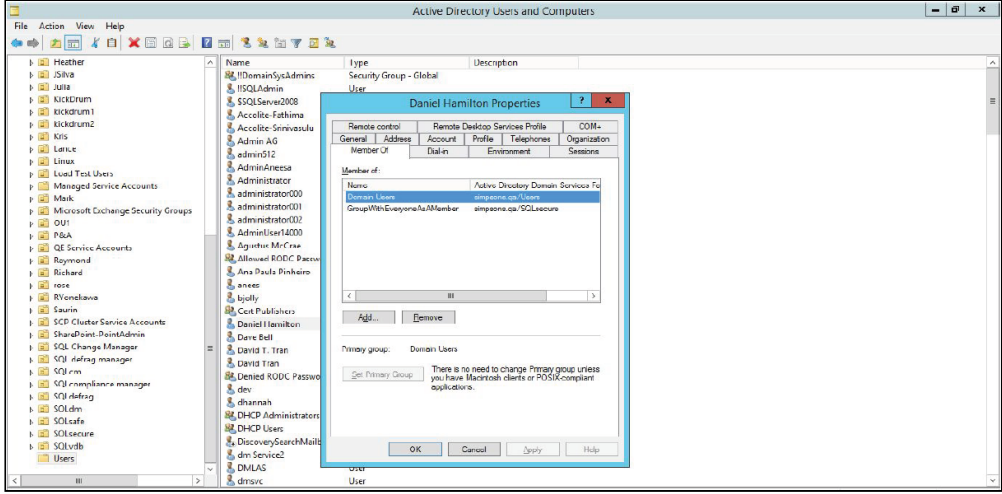
SQL Secure provides a list of possible exceptions and recommendations that help you resolve the issues that are affecting the product performance.

The following topics are covered in this section:

- [Active Directory Permissions Exceptions](#)
- [Domain Services Permissions Exceptions](#)
- [File Permission Exceptions](#)
- [Registry Permissions Exceptions](#)

17.1 Active Directory Permissions Exceptions

17.1.1 SID account

<p>Corresponds to warning on UI / Exception in Logs:</p>	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
<p>Type of exception:</p>	<p>ERROR - this SID is not a group</p>
<p>Cause:</p>	<p>Account corresponding to this SID is not part of the global group accounts or well-known group accounts (such as Everyone).</p>
<p>Solution:</p>	<p>One can try changing the scope of the account through Programs</p> <ul style="list-style-type: none"> • Administrative Tools. • Active Directory Users and Computers. 
<p>New Error Message:</p>	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects • User account [SID group] is not part of the global group accounts/well-known group accounts.

<p>Reason for not getting negative findings:</p>	<p>Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible.</p> <p>To get users and group account details, LookupAccountSid is executed which is a windows API, and since the account exists and is accessible, it returns the name for the specified SID. The users or groups account is an alias, group, or a well-known group. So in a normal functioning environment, the user or group return will always be amongst the alias, group, or well-known group. Therefore the negative case is not reproduced in a normal functioning environment.</p> <p>Source: https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-lookupaccountsida</p>
--	---

17.1.2 Active Directory account table

<p>Corresponds to warning on UI / Exception in Logs:</p>	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
<p>Type of exception:</p>	<p>ERROR - failed to lookup account for</p>
<p>Cause:</p>	<p>System error encountered when _LookupAccountSid() for given group SID is called.</p>
<p>Solution:</p>	<p>Add a user to the active directory using the given steps :</p> <ul style="list-style-type: none"> • Go to Start. • Select “Administrative Tools”. • Select “Active Directory Users and Computers”. • Either right-click the "Users" folder on the left side, or the blank area on the right side, And highlight "New" then click "User”. • In the next dialog, we can set the user’s First name, Last name, and various other pieces of information, including their log-on name, and domain to which we want to add them. • After clicking "Next" you are presented with the password-settings screen. • In the next dialog, we get a summary of the user to be created. Click "Finish" and the user has been created. <p>Verify that the user is active in the Active Directory.</p>
<p>New Error Message:</p>	<p>Suspect Windows accounts encountered processing OS objects</p> <ul style="list-style-type: none"> • User with groupSID - [SID group] is not present in the active directory/Account table. • User with username - [username] and groupSID - [SID group] is not present in the active directory/Account table.

Reason for not getting negative findings:	<p>Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible.</p> <p>To get users and group account LookupAccountSid is executed which is a windows API and, since the account exists and is accessible, it returns the name for the specified SID. So in normal functioning, it is not null. So the negative case is not reproduced.</p> <p>Source: https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-lookupaccountsida</p>
---	---

17.1.3 SID Group

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - unable to determine the location of the SID
Cause:	The location of the given groupSID is not found as this groupSID is not part of either the Well-Known account group, Domain server group role, or a Local server group.
Solution:	<p>Add a group to the active directory using the given steps :</p> <ul style="list-style-type: none"> • Go to Start. • Select “Administrative Tools”. • Select “Active Directory Users and Computers”. • Either right-click the "Group" folder on the left side, or the blank area on the right side, And highlight "New" then click "Group”. • In the next dialog, we can set the group’s name and various other pieces of information, including their log-on name, and domain to which we want to add them. <p>Verify that the group is active in the Active Directory.</p>
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • GroupSID [SID group] is missing from Active Directory.
Reason for not getting negative findings:	<p>Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. If the user or group account is not valid then the account location is returned as unknown. So in normal functioning, the account location will not be unknown therefore the negative case is not reproduced.</p>

17.1.4 Group accounts

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
---	--

Type of exception:	ERROR - group account object creation failed for
Cause:	Local account creation for group account object failed.
Solution:	Check if the directory entry obtained from WinNT path is valid and has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • The creation of a local account for the group account failed.
Reason for not getting negative findings:	A local account is created for the specified server name, SID Group, and Directory Entry Group. A negative case will arise when the group directory entry is empty or null which will not happen in a normal functioning environment as it is made using the server name and group name. So in the normal functioning environment, the account creation will not fail therefore the negative case will not be reproduced.
Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - enumeration of the group failed for
Cause:	Local account creation for group account object failed.
Solution:	Check if the directory entry obtained from WinNT path is valid and has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing the OS objects. • Retrieval of the directory members and their paths of the group directory corresponding to the groupSID failed.
Reason for not getting negative findings:	In a normal functioning environment, we get members and their paths of the group directory. It may fail during the run time due to some flaws in the environment. Then this error gets logged. It is a custom error and not a standard windows error. We couldn't reproduce this error in a normal functioning environment.

17.1.5 Directory Entry

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
---	--

Type of exception:	ERROR - group directory entry not found for
Cause:	Directory Entry for the given WinNT path not available.
Solution:	Please check if the directory exists at the given path. If the directory exists, please check if the user has permission to access the directory.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Directory entry [Directory name] for the given groupSID [SID group] WinNT path is not valid.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. If the directory entry for the SID is not found it returns null. But in a normal functioning environment, the directory entry will not be null for the given SID and therefore the negative case is not reproduced.

17.1.6 Domain Controller

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to get domain object for
Cause:	Failed to get the name of the domain controller for the specified domain. If Domain is AD, failed to get DNS name for the domain. The domain name was to be returned as either a flat name or a DNS name.
Solution:	<ul style="list-style-type: none"> • Check if the format of the specified Domain Name is invalid. • Check if the Flags parameter does not contain conflicting or superfluous flags. • Check if the memory allocation failure has not occurred. • Check if the domain controller is available for the specified domain or the domain does exist.
New Error Message:	Suspect Windows accounts encountered processing OS objects Failed to retrieve the name of the domain controller for the specified domain: [domain name].
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Since the server name and domain name will also be available in normal functionality, so the domain controller details will be accessible therefore the negative case is not reproduced.

17.1.7 SID Group Directory

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - domain group account object creation failed for
Cause:	This can mean directory entry for the given groupSID is not present or valid.
Solution:	Check if the directory path is valid or the user has required permissions to access the directory path.
New Error Message:	Suspect Windows accounts encountered processing OS objects. Active Directory entry [directory entry name] for the given groupSID [SID group] is not valid/does not exist.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Since the directory entry name for the users or group is not null or empty or the object class is not unknown for the users or groups in normal functionality therefore the negative case is not reproduced.

17.1.8 Group Members

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - domain group enumeration failed for
Cause:	Retrieving of the directory members and their paths, of the group directory corresponding to the groupSID has failed.
Solution:	<p>Add a group to the active directory using the given steps :</p> <ul style="list-style-type: none"> • Go to Start. • Select "Administrative Tools". • Select "Active Directory Users and Computers". • Select the server from the left side. • A list of groups and users will appear on the screen. • Select a particular group. • In the dialog opened there will be a tab to see members of the group. <p>Verify if the retrieved group members and their paths are valid entries in the server.</p>

New Error Message:	Suspect Windows accounts encountered processing OS objects. Retrieval of the active directory members and their paths of the group directory corresponding to the groupSID [SID group] failed.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. Since the directory entry name for the users or group is not null or empty and domain details are available for the users or groups in normal functionality therefore the negative case is not reproduced.

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - group directory entry not found for
Cause:	Directory entry for the given groupSID WinNT path is not valid.
Solution:	Check if the specified directory entry path is valid or has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Directory entry[directory entry name] for the given groupSID [SID group] WinNT path is not valid.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. If the directory entry for the SID is not found it returns null. But in a normal functioning environment, the directory entry will not be null for the given SID and therefore the negative case is not reproduced.

17.1.9 LDAP Path

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - no elements in the LDAP path
Cause:	No elements present in the given path.
Solution:	Check if the specified path is valid or has read/write permissions.

New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Given [ldap path] does not contain any elements.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Server Name and group names are available for the users and groups to get the LDAP path. Therefore the path will be generated and it will have elements in normal functionality therefore the negative case is not reproduced.

17.1.10 Path Elements

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - not a valid number of elements in the path
Cause:	This is logged when there are not enough elements in the path to extract the domain from the path.
Solution:	Check if the specified path is valid or has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • The given path [specific path] does not contain a valid number of elements.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Server Name and group names are available for the users and groups to get the LDAP path. Therefore the path will be generated and it will have a valid number of elements in normal functionality therefore the negative case is not reproduced.

17.1.11 Local Directory

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - Failed to get the local directory entry
Cause:	The local directory entry is not found.

Solution:	Check if the local Directory entry is valid or has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Local directory entry not found.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Members of these groups are also accessible and local directory path. So in normal functionality, the local directory entry for each member of the group will be available so the negative case is not reproduced.

17.1.12 Group Object Account

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - account object creation failed
Cause:	This error is logged when the group object account is tried to be created locally.
Solution:	Check if the local Directory entry supplied to this method is valid or has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Please check that the user [specific user] has the required permissions for the local directory [local directory name].
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Since the directory entry name for the users or group is not null or empty or the object class is not unknown for the users or groups in normal functionality, therefore the negative case is not reproduced.

17.1.13 Domain

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to get a domain, DN:

Cause:	Failed to get Domain for specified object path.
Solution:	Check if the specified path is valid or has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Failed to get Domain for specified object path [specific object path].
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. `Domain information for each user or group is fetched using the server name and the user or group members therefore the domain information is available in normal functionality, so the negative case is not reproduced.

17.1.14 Directory

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - FSP group directory entry not found for
Cause:	Directory entry not found for provided Foreign Security Principal sid or fspsid.
Solution:	Check if the specified path is valid or has read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Active directory entry not found for provided Foreign Security Principal sid/fpsid [specific sid\fpsid].
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path in normal functionality so active directory entry will be found for fspsid therefore in normal functionality the negative case is not reproduced.

17.1.15 SAM account

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to get SAM account name for the SID:

Cause:	Failed to get SAM account name for the SID
Solution:	Check if the Active DirectoryEntry from which the sid was obtained is valid or has read/write permission.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Active Directory entry from which SID [specific SID] was obtained is not valid or does not have required permissions.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class that will not be unknown in normal functionality, it will be amongst user, group, computer, or inetOrgPerson. So in normal functionality, the object class won't be unknown therefore the negative case is not reproduced.

17.1.16 SID Objective Category

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to get object category for the SID:
Cause:	Failed to get an object category for the SID.
Solution:	Check if the DirectoryEntry from which the sid was obtained is valid or has read/write permission.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Active Directory entry from which SID [specific SID] was obtained is not valid or does not have required permissions.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class that will not be unknown in normal functionality, it will be amongst user, group, computer, or inetOrgPerson. So in normal functionality, the object class won't be unknown therefore the negative case is not reproduced.

17.1.17 Directory Group Type

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to get group type
Cause:	Failed to group type of the Directory Entry with Object class as a group.
Solution:	Check if the DirectoryEntry obtained is valid or has read/write permission.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Active Directory entry obtained is not valid or does not have the required permissions.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class, if the object class is group and directory entry has more than one group type or the group type is not an integer which will not happen in normal functionality. So in normal functionality, the negative case is not reproduced.

17.1.18 ADSI path

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to get adsi path
Cause:	Failed to get adsi path from the given directory entry object
Solution:	Check if the DirectoryEntry obtained is valid or has read/write permission.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects • Active Directory entry obtained is not valid or does not have the required permissions.

Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path. The directory path will not be null or empty in normal functionality. So in normal functionality, the negative case is not reproduced.
---	---

17.1.19 Directory Entry

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - exception raised when querying dir entry object
Cause:	The exception to handle any other exception occurred while creating an account.
Solution:	Check if the DirectoryEntry obtained is valid or has read/write permission.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects • Active Directory entry obtained is not valid or does not have the required permissions.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class, if the object class is group and directory entry has more than one group type or the group type is not an integer which will not happen in normal functionality. So in normal functionality, the negative case is not reproduced.

17.1.20 WinNT path

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to get dom dir entry
Cause:	Failed to get domain directory entry for given WinNT path.
Solution:	Check if the WinNT path obtained is valid. If the path is valid, check if the account has elevated privileges and account used to get domain directory details have read/write permissions.

New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Failed to get domain directory entry for given WinNT path.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. For each user or group, there are domain details and for each domain, there is a directory path created. In normal functionality, the domain directory path will be created since it will not be null or empty therefore the negative case is not reproduced.

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR - failed to parse the member DN
Cause:	Error in parsing given WinNT Path.
Solution:	Check if the WinNT path obtained is valid. If the path is valid, check if the account has elevated privileges and account used to get domain directory details have read/write permissions.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Error in parsing the given WinNT path [specific WinNT path].
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. For each user or group, there are domain details and for each domain, there is a directory path created. In normal functionality, the domain directory path has the domain name which can be extracted successfully so it will not be null or empty therefore the negative case is not reproduced.

17.1.21 Group members

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR: Failed to load <path> group members
Cause:	No Group members retrieved for the given groupSID.

Solution:	<p>Check if the given SID is a valid group SID. If not, one try changing the scope of the account through :</p> <ul style="list-style-type: none"> • Programs. • Administrative Tools. • Active Directory Users and Computers.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • No group members retrieved for the groupSID - [specific SID group].
Reason for not getting negative findings:	<p>This error should come when a group with the respective groupSID does not have a member. According to code, an error will be reproduced when a member's object is null. members' object is never null even if there is no member. If there is no member, then members object will have count as 0. Since the check is if the members object is null, so this is not reproduced.</p>

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	ERROR: failed to read <path> AD group object
Cause:	Group members cannot be retrieved for the given groupSID.
Solution:	<p>Check if the given SID is a valid group SID. If not, one try changing the scope of the account through :</p> <ul style="list-style-type: none"> • Programs. • Administrative Tools. • Active Directory Users and Computers.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • No group members retrieved for the groupSID - [specific SID group].
Reason for not getting negative findings:	<p>This error should come when the group is null. Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. So, in a normal functioning environment, the group is not null. Therefore, the error is not reproduced.</p>

17.1.22 SID and SAM path

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2] • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]
Type of exception:	Failed to create an account for File Access Rights.
Cause:	Failed to create group account access rights for the given sid and sam path.
Solution:	<p>Check if the given SID is a valid group SID. If not, one try changing the scope of the account through:</p> <ul style="list-style-type: none"> • Programs. • Administrative Tools. • Active Directory Users and Computers. • Check if the given path is valid and has read/write permission.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Failed to create an account for File Access Rights.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. To get users and group account LookupAccountSid is executed which is a windows API and an account are created for files that have permissions for the file and is accessible, it returns file details for the specified SID. So in the normal functioning account will be created for file access rights therefore negative case is not reproduced.

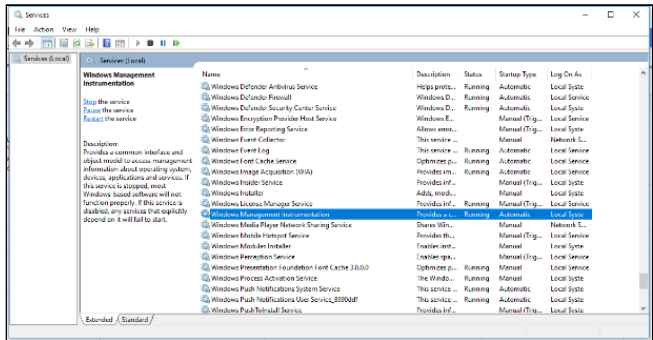
Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	Failed to create an account for File Audit Rights.
Cause:	Failed to create group account audit rights for the given sid and sam path.
Solution:	<p>Check if the given SID is a valid group SID. If not, one try changing the scope of the account through:</p> <ul style="list-style-type: none"> • Programs. • Administrative Tools. • Active Directory Users and Computers. • Check if the given path is valid and has read/write permission.

New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects. • Failed to create an account for File Audit Rights.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. To get users and group account LookupAccountSid is executed which is a windows API and an account are created for files that have permissions for the file and is accessible, it returns file details for the specified SID. So in the normal functioning account will be created for file access rights therefore negative case is not reproduced.

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]. • We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI].
Type of exception:	Failed to create an account for File Audit Settings.
Cause:	Failed to create group account audit settings for the given sid and sam path.
Solution:	<p>Check if the given SID is a valid group SID. If not, one try changing the scope of the account through:</p> <ul style="list-style-type: none"> • Programs. • Administrative Tools. • Active Directory Users and Computers. • Check if the given path is valid and has read/write permission.
New Error Message:	<ul style="list-style-type: none"> • Suspect Windows accounts encountered processing OS objects • Failed to create an account for File Audit Settings.
Reason for not getting negative findings:	Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible. To get users and group account LookupAccountSid is executed which is a windows API and an account are created for files that have permissions for the file and is accessible, it returns file details for the specified SID. So in the normal functioning account will be created for file access rights therefore negative case is not reproduced.

17.2 Domain Services Permissions Exceptions

17.2.1 Target Service

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> Error Getting Target Service. [Logged]
Type of exception:	
Cause:	If there is any exception encountered while doing the WMI query to get services from Target.
Resolution:	<p>Verify that the WMI service on the target machine is running successfully.</p>  <p>The screenshot shows the Windows Services console for a local machine. The 'WMI' service is highlighted in blue. Its status is 'Running', and its startup type is 'Automatic'. The service is located under 'System Tools' in the left-hand pane.</p>
New Error Message:	Error/Exception occurred while getting target services using WMI. Verify that the WMI service is running on [target server].

17.2.2 Local connection

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> Local connection attempt failed.[Logged]
Type of exception:	
Cause:	If management scope object creation or call to open connection fails.
Resolution:	Verify that the WMI service on the target machine is running successfully.
New Error Message:	WMI service failed to connect to the target server. Verify that the WMI service is running on [target server].

17.2.3 SQL Services

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> Failed to load properties for some SQL Services on target SQL Server [UI]
Type of exception:	
Cause:	If any of the above two exceptions encountered or if there is any exception encountered while saving services data in Secure repository.
Resolution:	Change the UI message to depict the actual issue rather than one generic message.
New Error Message:	

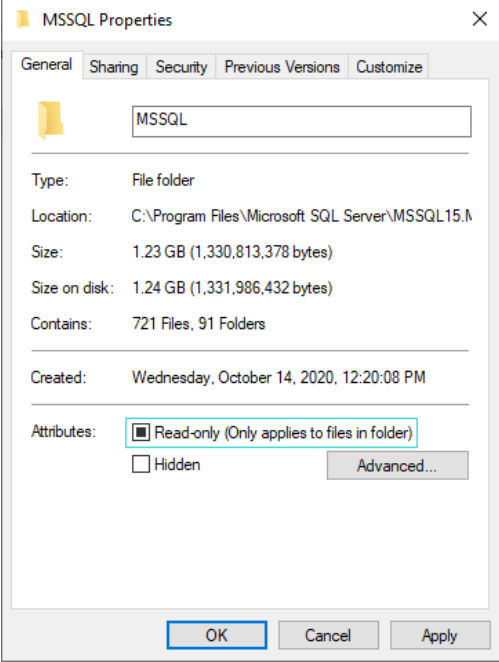
17.3 File Permission Exceptions

17.3.1 Security Privilege

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> Failed to load file permissions for target SQL Server [UI] Failed to load file permissions for '{0}' audit folder [UI] Failed to load file permissions for SQL Services on target SQL Server [UI]
Type of exception	SeSecurityPrivilage
Cause	The Server Collection Account configured in the server properties and under which SQL Secure collector is running, does not have enough permissions in the Active Directory.
Solution	<p>In order to fix this, perform the following steps:</p> <ol style="list-style-type: none"> Go to the Target Server Windows Settings <ul style="list-style-type: none"> Local Security Policy. Local Policies. User Rights Assignment on the server you are trying to install on. Look for the SQL Server collection account used to connect to audited SQL Servers and assign it the following rights: <ul style="list-style-type: none"> Back up files and directories. Debug Programs. Manage auditing and security log. Restore files and directories. Take ownership of files or other objects. Once you have done this, logout then log back in again.
New Error Message	Credentials/Authentication being used to collect details from the target server does not have the required File Permissions.

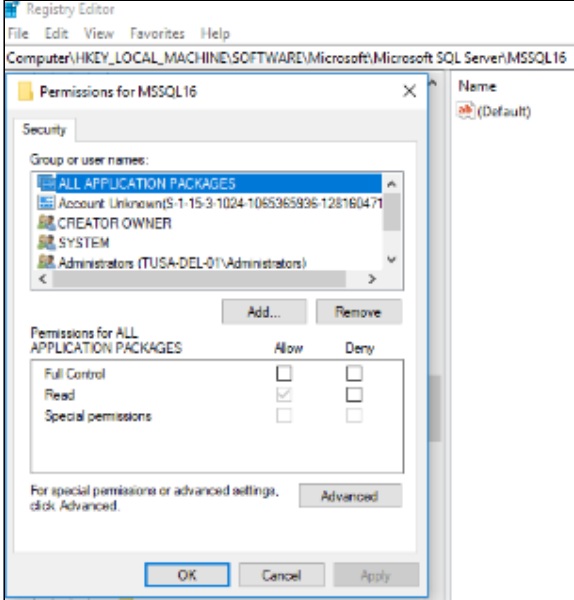
17.3.2 Unauthorized Access Exception.

Corresponds to warning on UI / Exception in Logs:	<ul style="list-style-type: none"> Failed to load file permissions for target SQL Server [UI] Failed to load file permissions for '{0}' audit folder [UI] Failed to load file permissions for SQL Services on target SQL Server [UI]
Type of exception	UnauthorizedAccessException
Cause	The path parameter specified a directory that is read-only.-or- This operation is not supported on the current platform.-or- The caller does not have the required permission.

<p>Solution</p>	<p>In order to fix this, we need to go to the SQL Server installation directory and make sure that the user under which SQL Secure collector is running have enough access permissions on all the folders and files inside the installation directory(uncheck "Read Only" checkbox in the properties) and not Read-only access.</p>  <p>The screenshot shows the 'MSSQL Properties' dialog box with the 'Security' tab selected. The 'Attributes' section at the bottom has the 'Read-only (Only applies to files in folder)' checkbox checked and highlighted with a red box. The 'Hidden' checkbox is unchecked. There is an 'Advanced...' button next to the attributes. The dialog also shows the folder name 'MSSQL', its type as 'File folder', location as 'C:\Program Files\Microsoft SQL Server\MSSQL15.M', size as '1.23 GB (1,330,813,378 bytes)', size on disk as '1.24 GB (1,331,986,432 bytes)', and creation date as 'Wednesday, October 14, 2020, 12:20:08 PM'. Buttons for 'OK', 'Cancel', and 'Apply' are at the bottom.</p>
<p>New Error Message</p>	<p>Collector tried accessing an unauthorized directory/credentials saved on the target server does not have the required permission.</p>

17.4 Registry Permissions Exceptions

17.4.1 Failed to load registry permissions or configuration

<p>Corresponds to warning on UI / Exception in Logs:</p>	<ul style="list-style-type: none"> Failed to load registry permissions for target SQL Server [UI] Failed to load some registry configuration options for target SQL Server [UI]
<p>Type of exception:</p>	<p>System.Security.SecurityException</p>
<p>Cause:</p>	<p>The account under which SQL Secure collector is running does not have read/write access on the registry settings.</p>
<p>Resolution:</p>	<p>The account under which SQL Secure collector is running needs to be given read/write access (Full control) over the registry.</p> 
<p>New Error Message:</p>	<p>Credentials/Authentication being used to collect details from the target server does not have read /write access over registry settings.</p>