SQL Discovery

The SQL Discovery tool helps you find new or rogue SQL Server instances that are online in your network. This tool allows you to locate SQL Server instances and create a server group for the SQL Server instances you locate. Once you identify and group newly-discovered SQL Server instances, you can properly lock down these instances to prevent any security issues.

SQL Discovery searches computers hosting SQL Server instances by specifying IP ranges, a list of computers, or servers registered with Active Directory or Network Browser Service. You can also use a number of different scans or probes to increase the effectiveness of your search. The following table displays a list of available probes and their purposes.

Type of probe	What it does
Active Directory Probe	Checks for SQL Server instances registered with Windows Active Directory.
Browser Service Probe	Checks for SQL Server instances registered with Network Browser Service.
Service Control Manager Probe	Checks with Service Control Manager for installed SQL Server instances.
SQL Server Resolution Service Probe	Checks port 1434 to determine whether SQL Server instances are registered with the SQL Server Resolution Service.
TCP Probe	Checks the standard or custom ports SQL Server uses to listen. The standard ports are 1433 and 2433. Type a specific port or ports in the available field to scan those ports.
Windows Registry Probe	Checks the registry on each computer to detect whether SQL Server services are installed.
WMI Enumeration Probe	Checks for installed SQL Server instances by using WMI for the search.

Once the results are available, you can review the list of discovered SQL Servers, see which probe found each instance, and check the configuration details of each instance.

Considerations before using the SQL discovery tool

One factor to consider before using SQL Discovery is to check the firewall settings your local computer, such as the native Windows Firewall or any third-party firewall application.
SQL Discovery uses ports 1433,1434, and 2433 to scan your network for SQL Server instances. Make sure these ports are open and enabled for communication.

You can use Inventory Reporter, Patch Analyzer, and Password Checker with SQL Discovery to further enhance your validation. These other tools work with the SQL Discovery tool in the following ways:

Inventory Reporter

Save the found SQL Server instances as a new server group, and then run Inventory Reporter against this server group to capture configuration details.

Patch Analyzer

Use Patch Analyzer to verify that the found SQL Server instances are properly patched and are running supported versions of Microsoft SQL Server software.

Password Checker

Use Password Checker to test the security of the found SQL Server instances.

Use the SQL Discovery tool

To find new or rogue SQL Server instances using SQL Discovery:

1. Open the IDERA SQL Admin Toolset Launchpad, and then click **SQL Discovery**.
2. On the Welcome window, click **Next**.
3. Select which scan technique you want to use to locate SQL Server instances on your network, and then click **Next**.
4. ***If you selected IP Range in the previous window***, specify one or more IP addresses that you want to scan.
5. ***If you selected SQL Server(s) in the previous window***, specify one or more SQL Servers or the server group on whose host computers you want to perform a scan. To specify multiple SQL Servers, separate each name with a semicolon.
6. ***If you selected Computer(s) in the previous window***, specify one or more computers to scan for SQL Servers. To specify multiple computers, separate each name with a semicolon.
7. Click **Next**.
8. Choose which probes you want SQL Discovery to run as part of the discovery process, and then click **Finish**. ***If you select to use a TCP Probe***, type the SQL Server port(s) you want to scan.
9. Review the scan results. To see more details about a discovered instance, select that instance from the Scan Results list, and then view the details displayed below.
10. ***If you want to create a server group that contains these instances***, click **Save as Server Group**.
11. ***If you want to save the results***, click **Copy Results To Clipboard**, or export the list as an XML or CSV file.