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.computeIDR-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**.