Permissions requirements

SQL Compliance Manager requires specific permissions and rights to successfully audit events. By default, the setup program assigns the Collection Service and SQLcompliance Agent Service accounts read and write permissions on the respective trace directory.

Management Console user permissions

Actions	Permissions Requirements
Administer SQL compliance manager and configure audit settings	sysadmin rights on the Repository databases
Generate and view audit reports	Read permissions (public rights) on the Repository databases
Deploy SQLcompliance Agent to registered SQL Server instance	Administrator permissions on the computer hosting the target instance
Connect to the SQL Server that hosts the Repository databases	SQL Server login

Operating system permissions

Actions	Permissions Requirements
Store audit settings and manage archive databases in the Repository	sysadmin rights on each Repository database
Process trace files	Read, write, and delete permissions on the Collection Server trace directory
Manage trace directory	Local Administrator permissions on the computer that hosts the Collection Service
Run as a service	Log on as a Service right on the computer that is running the audited SQL Server instance

SQLcompliance Agent service permissions

Actions	Permissions Requirements
Starting and stopping traces, and managing SQLcompliance stored procedures	sysadmin rights on the audited SQL Server instance or database
Manage trace files	Read, write, and delete permissions on the SQLcompliance Agent trace directory
Manage trace directory for an audited SQL Server instance	Local Administrator permissions on the computer that hosts the registered SQL Server
Manage trace directory for an audited virtual SQL Server	Administrator permissions on each node in the cluster hosting the virtual SQL Server
Run as a service	Log on as a Service right on the computer that is running the audited SQL Server instance

SQL Server service permissions on the Collection Server

Actions	Permissions Requirements
Load trace files so the Collection Server can process these events	Read permissions on the Collection Server trace directory

SQL Server service permissions on the registered SQL Server

Actions	Permissions Requirements
Write events to trace files for the registered SQL Server instance and audited databases	Write permissions on the SQLcompliance Agent trace directory

Using Windows Authentication

The SQL Compliance Manager Managment Console and Agent require Windows authentication. Windows authentication uses the logged on user account to establish trusted connections through the operating system. The credentials of the logged on user account are passed to the SQL Server database servers. Your database server then verifies the user matches an established SQL Server login account that has the appropriate permissions. Only after verification will a connection open.

When using Windows authentication, the account logged on to the Management Console computer must have the appropriate SQL compliance manager permissions.

Using SQL Server Authentication

The SQLcompliance Collection Service leverages existing SQL Server logins that have been granted the appropriate SQL privileges. However, SQL Compliance Manager does not support SQL Server authentication.