Deploy the SQL Compliance Manager Agent manually

To deploy the SQL Compliance Manager Agent manually, run an Agent Only or Custom setup to install the agent on the physical computer that hosts the SQL Server instance or database you want to audit. Use manual deployment when you want to install the SQL Compliance Manager Agent in a unique environment, such as on a workstation or a computer that belongs to a non-trusted domain.

If you want to audit a virtual SQL Server, use the Cluster Configuration Console to deploy and configure the SQL Compliance Manager Agent on each cluster node hosting the server. For more information about installing and configuring the SQL Compliance Manager Agent for a virtual SQL Server, see Deploy the SQL Compliance Manager Agent to cluster nodes.

Perform a silent installation

Use the following commands to perform a silent installation or upgrade the IDERA SQL Compliance Manager Agent for **versions 5.5.1 and later**.

For a fresh installation:

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log COLLECT_SERVER="IderaCollectionServerName"
INSTANCE="AgentSQLServerInstanceName" TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE" SILENT="1" /qb+
```

Minor/Maintenance Upgrade (from 5.x to this version):

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log COLLECT_SERVER="IderaCollectionServerName"
INSTANCE="AgentSQLServerInstanceName" TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE" SILENT="1"
REINSTALLMODE=vamus REINSTALL=All AllUsers=1 /qb+
```

Major upgrade (from 4.5 to this version):

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log SERVICEUSERNAME="Domain\Username" PASSWORD="!
mySec@tP@55w0rD" STARTSERVICE="TRUE" SILENT="1" AllUsers=1 /qb+
```

Use the following commands to perform a silent installation or upgrade the IDERA SQL Compliance Manager Agent for **version 5.5**.

For a fresh installation:

```
msiexec /i "<Path_to_Agent_MSI>\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log COLLECT_SERVER="
IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName" TRACE_DIRECTORY="C:\Program
Files\Idera\SQLcompliance\AgentTraceFiles" SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD"
STARTSERVICE="TRUE" SILENT="1" /qb+
```

For an upgrade:

```
msiexec /i "<Path_to_Agent_MSI>\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log COLLECT_SERVER="
IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName" TRACE_DIRECTORY="C:\Program
Files\Idera\SQLcompliance\AgentTraceFiles" SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD"
STARTSERVICE="TRUE" SILENT="1" REINSTALLMODE=vamus REINSTALL=All AllUsers=1 /qb+
```

Associated parameters include:

Parameter	Description
COLLECT_SERVER	The machine where the Collection server is installed and where you want to collect audited data.
INSTANCE	The SQL Server instance name where you want to install the Agent.

TRACE_DIRECTORY	The Agent trace file directory where you want to generate the trace files on the Agent server.
SERVICEUSERNAME	The Windows service account used to run the Agent service. This account must be local admin and have sa rights to the monitored SQL Server.
PASSWORD	The password for the service account.
STARTSERVICE	Denotes whether to start the service.
SILENT	Indicates to the installer that it is installed silently.
REINSTALL MODE	**Vamus,** indicates the type of reinstall to perform.
REINSTALL	**All,** instructs the installer to reinstall all pre-installed features.

The login and password must be encrypted strings. On IDERA SQL Compliance Manager 3.0 and later, you can encrypt the login and password using the encrypt command on the command line to get an encrypted version of the string that can then be used:

```
sqlcmcmd encrypt THESTRING
```

Note

Should the password contain the ¨^¨ special character, please consider enclosing the password string in between quotation marks, as shown below.

sqlcmcmd encrypt "THESTRING"

Also, note that this option would work if the password string does not contain double-quotes.