Spotlight Pre-Requisites/Genesys Readiness

Introduction

This document presents the server sizing/requirements for Spotlight Core Audit and Release Management and the pre requisites/Readiness steps that must be in place before installation of the Spotlight software commences.

If you wish to arrange assistance with your sizing or installation, please contact installationsupport@theblackchair.com

Blackchair Data Capture Spreadsheet

The Blackchair Audit and SAM data capture Excel sheet is designed to capture all the data required to implement Spotlight Audit and the SAM module, and to confirm that all pre-requisites have been met.

Other than sections in the SAM module where your configuration may not be applicable, such as Genesys GVP, WFM Genesys Agent Desktop and Interaction Workspace all sections need to be completed unless highlighted as optional.

The data collection sheet will need to be completed for each system that you want to track, e.g. Production, Pre Production, Test.

A check pre-requisites check list is also included to allow the customer to confirm that the system is ready for installation.

Spotlight Server

Hardware

Following are the minimum estimated requirements to host the Spotlight components for Core Audit and Release Management. The server may be physical or virtual; if virtual its performance characteristics must match those of a physical server of the same specification. Load on the server is generally determined by two metrics; the size of the Genesys environment being monitored and the volume and profile of changes made to the system. The latter is rarely available until Spotlight is actually installed and tracking changes so sizing has to be based just on the size of the environment. It must be noted that a small system may turn out to have a disproportionately high volume of changes in which case sizing may in exceptional circumstances need to be revisited.

The sizing below is for a single Spotlight system monitoring up to three environments, typically Production, Pre-Production and Development systems. The sizing is for the Core Audit plugin with Release Management only; if the customer is purchasing additional platform plugins or Spotlight modules please contact Blackchair for assistance.

Note: We recommend SQL Server and components be located on separate infrastructure but have provided estimated sizing for collocating SQL server and components onto a single host.

Option 1 - Contact Centre less than 7000 seats

- Processor – two 4 core Xeon 2.3Ghz or better
- 32GB RAM (up to 3 environments, add 4GB RAM for each additional environment) *Note: Additional environments can be placed across multiple servers*
- 120GB minimum for the C: drive operating system only
- 400GB minimum Spotlight application installation drive
- 100GB minimum Spotlight log drive

SQL Server collocated on local machine add additional 32GB RAM

- DB Data Drive 500GB minimum
- DB Log Drive 500GB minumum

Option 2 - Contact Centre 7000 – 15000 seats

- Processor – two 4 core Xeon 2.3Ghz or better
- 32GB RAM (up to 3 environments, add 4GB RAM for each additional environment) *Note: Additional environments can be placed across multiple servers*
- 120GB for the C: drive operating system only
- 400GB minimum Spotlight application installation drive
- 100GB minimum Spotlight log drive

SQL Server collocated on local machine add additional 48 GB RAM

- DB Data Drive 750GB minimum
- DB Log Drive 500GB mimimum

Option 3 - Contact Centre 15000 – 25000

- Processor – four 4 core Xeon 2.3Ghz or better
- 32GB RAM (up to 3 environments, add 4GB RAM for each additional environment) *Note: Additional environments can be placed*

across multiple servers

- 120GB for the C: drive operating system only
- 400GB minimum Spotlight application installation drive
- 100GB minimum Spotlight log drive

SQL Server collocated on local machine add additional 64 GB RAM

- DB Data Drive 1TB minimum
- DB Log Drive 750GB minimum

Hardware - High Availability (HA)

Spotlight can be run in a high availability configuration using 3 x geographically collocated servers (nodes). All 3 x servers shall meet the minimum server specification for an equivalent single server instance to ensure that the system performs in failover. Please ensure these additional considerations and customer responsibilities when Spotlight running in an HA configuration:

Database

The Spotlight database shall be a resilient DB cluster hosted separately and cannot run locally on any of the Spotlight servers. The resilient database/cluster must be accessible via single IP address and is the responsibility of the customer to both provide and maintain.

Spotlight User Access

Users access requests must be sent to the 'active' node. The customer is responsible providing a route from the user to the active node by means of a 'broker' or some equivalent load balancer.

Network Broadcast Events

Spotlight can receive and process network events such as SNMP traps or other 'UDP' type broadcasts. Where customers have purchased plugins to process broadcast events in an HA configuration It remains the responsibility of the customer to ensure all events are sent to all Spotlight servers/nodes.

Software

The following server software is required before commencing installation of the Spotlight software

Spotlight installed using a Microsoft SQL Database:

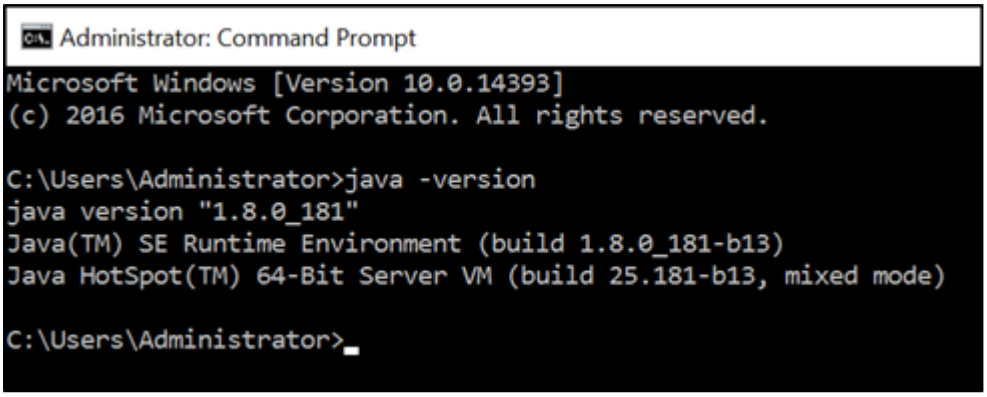
- Microsoft Windows Server 2012/2014/2016 64 bit Operating System with latest service pack and Windows updates.
- Microsoft SQL Server 2012/2014/2016 with latest service pack.
- Microsoft SQL Server Reporting Services installed and configured.
- Microsoft SQL Management Studio.
- Windows web server (IIS) installed (see below).
- Windows .Net Framework 3.5.1 Feature installed
- Windows .Net Core 2.1 (or later) Hosting Bundle
- Standard Java 64-bit JRE 1.8 (Note: specifically the 64-bit JRE must be installed and only Java version 1.8).

There must not be any other software installed on the server. Installation of the Spotlight software must be performed using the local administrator account or an account that is a member of the local administrator group, the account requires “Logon as Service” rights.

JAVA

To check the correct version of Java is installed:

- Open a command window
- Type ‘**java -version**’ this should then display current version as shown in the example below.



If the version is not shown this could indicate that either Java is not installed or it is not installed correctly.

IIS

- **Microsoft IIS** must be installed with the following role services:

Role/Sub Roles			Installed/Not Installed
Web Server	Common HTTP Features	Static Content	Installed
		Default Document	Installed
		Directory Browsing	Not Installed
		HTTP Errors	Installed
		HTTP Redirection	Not Installed
	Application Development	ASP .NET	Installed
		.NET Extensibility	Installed
		ASP	Installed
		CGI	Not Installed
		ISAPI Extensions	Installed
		ISAPI Filters	Installed
		Server Side Includes	Not Installed
	Health & Diagnostics	HTTP Logging	Installed
		Logging Tools	Not Installed
		Request Monitor	Installed
		Tracing	Not Installed
		Custom Logging	Not Installed
		ODBC Logging	Not Installed
	Security	Basic Authentication	Not Installed
		Windows Authentication	Installed
		Digest Authentication	Not Installed
		Client Certificate Mapping Authentication	Not Installed
		IIS Client Certificate Mapping Authentication	Not Installed
		URL Authorisation	Not Installed
		Request Filtering	Installed

		IP and Domain Restrictions	Not Installed
	Performance	Static Content Compression	Installed
		Dynamic Content Compression	Not Installed
	Management Tools	IIS Management Console	Installed
		IIS Management Scripts & Tools	Not Installed
		Management Service	Not Installed
		IIS 6 Management Compatability	Not Installed
		IIS 6 Metabase Compatability	Not Installed
		IIS 6 WMI Compatability	Not Installed
		IIS 6 Scripting Tools	Not Installed
		IIS 6 Management Console	Not Installed
	FTP Publishing Services	FTP Server	Not Installed
		FTP Management Console	Not Installed

In Internet **Information Services IIS Manager** ensure the **IIS Authentication** settings at server level enable **Windows Authentication only**

Database Server

Access to the Databases hosting Spotlight will be required during the installation and a user with Database owner privileges is required for the installation process.

When configuring the SAM module access to create Jobs using SQL Server Agent will be required. This access it only to create and schedule the Job required for License Tracking, however SQL Server Agent should be running on a continual basis to execute the job.

An estimation of the expected Spotlight Database size can be calculated using the Database Sizing spreadsheet

---

Genesys Pure Engage

Genesys CME

Spotlight Audit requires at least Genesys Configuration Server and Message Server be installed and running correctly. Spotlight Audit uses the following components in the Genesys system:

- A **Message Server** connected to Configuration Server (Connection added in Config Server). Spotlight will connect to this Message Server on its standard port and network connectivity must allow this. Primary and Backup pair is supported.
- **Configuration Server**. Spotlight will connect to the Configuration Server (Pair if enabled
- There must be an Application in the Genesys configuration of type '**Configuration Manager'** – eg "**Default**"
- A **Genesys login** with minimum Read access to the entire environment
- Applications (**SpotlightAuditServer & SpotlightAuditServerEC**) of type **Third Party Server** with connection to **Configuration Server (CS)** and **Genesys Message Server (MS)** should be created**.** It is not necessary to set an 'install directory' or 'host/port'.

Spotlight Release Management (if enabled) will write to **Configuration Server**. The same Configuration Server may be used for both **Audit** and **Release Management.** Configuration Server settings and connections must be configured as follows:

Message Server

- No specific logging settings required
- No connection settings required from Message Server

Config Server Proxy

Spotlight should not connect to a config server proxy for release managent based on the following extracts from Genesys Documentation

“Configuration Server clients that require write access to Configuration Server must still connect directly to Configuration Server”

"Updates made in bulk might result in a significant extra load on the system when done by the Proxy server rather than the Master server."

Config Server

Spotlight will connect to the main config server:

- **Configuration Server application (primary and backup)**
  - Logging must be set to include **standard=network**
  - Log section must include - **buffering = false**
- **Configuration Server connection**
  - Configuration Server must have a connection to Message Server.

Genesys GAX

Spotlight can audit changes to objects in the GAX database, if you are using it.

Note : you may use the GAX web interface to generally manage your system, but not have the specific objects in your system that are stored in the GAX database. This section only applies if you have objects such as Parameters and Audio Resources in your system that are stored in the GAX database.

Spotlight uses the GAX webservice to audit the GAX database and to apply changes through Release Management. A Genesys login is required with at least Read access in GAX. Release Management write requests use an individual Genesys login supplied at the time the request is created, not the Genesys login used to access the GAX webservice for audit.

If Spotlight is to track changes in GAX –

- GAX Server needs a connection to message server. The same message server as config server & Spotlight Applications. This must be the only message server that is connected to the GAX server
- The following options should also be configured

Section	Option	Value
general	auditing	true
general	scs_max_switchovers	1
general	msgsrv_attempts	1

general	msgsrv_warmstandyby_timeout	60
general	msgsrv_timeout	30
log	standard	network
log	buffering	false

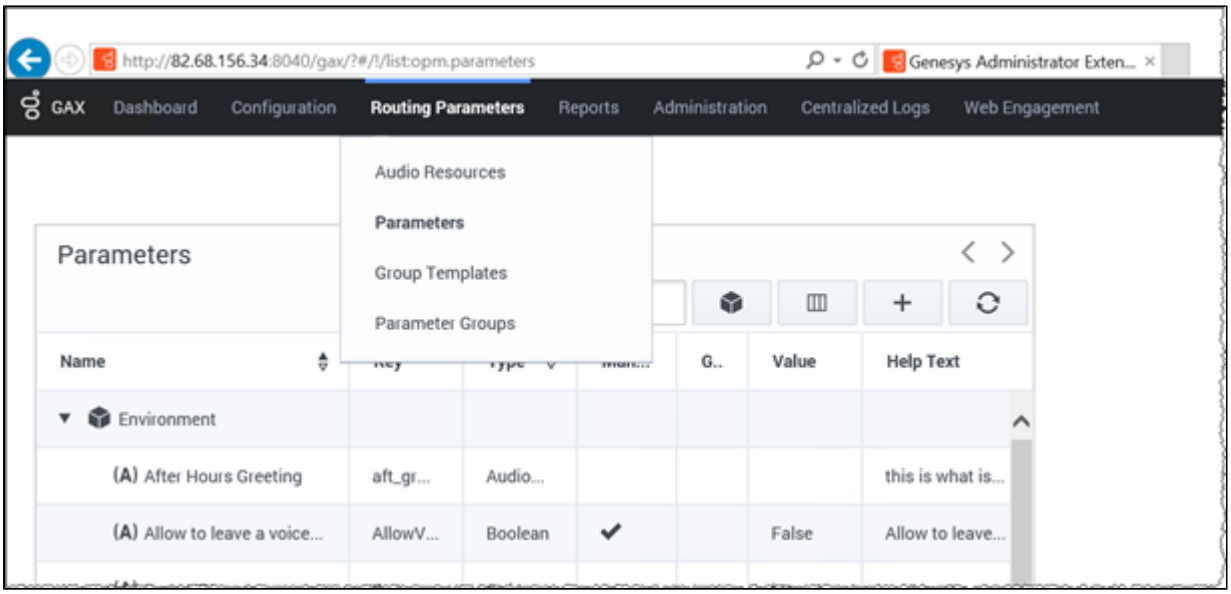
Spotlight Genesys User

For a Spotlight Audit and SAM deployment, a single Genesys user is required to be configured in CME/Administrator. At the Top level allow a user (spotlight in this example) to have Read, Execute and Read Permissions on all objects. Without the Read Permissions the Security Audit feature in Spotlight will not work.The user defined must have all but Delete access to Agent Groups folder.

- Create a user in Administrator/CME with **Read**, **Execute**, **Read Permission** only to start with
- The 'Genesys' user defined access to the Agents Groups folder is managed by adding the "**Create**" and "**Change**" access rights. The Spotlight SAM module creates the required agent groups and assigning agents to the groups created. Without create and change the agent groups will not be created correctly and the agents will not be assigned.
- The user also requires read only access to GAX

To test the GAX User access:

- Open a browser and navigate to the GAX web URL and login using the Genesys user provided.
- Once logged in you should be able to click on 'Routing Parameters' and then click on 'Parameters' and that should then display all the Parameters in GAX as shown in the example below.



If any of these options are unavailable then the Genesys user does not have the required permissions to read the whole of the GAX environment.

Spotlight Applications

Applications (**SpotlightAuditServer & SpotlightAuditServerEC**) of type **Third Party Server** with connection to **Configuration Server/Proxy (CS/CSP)** and **Genesys Message Server (MS)** should be created as follows**:**

Create a new application in Genesys with the following settings

- **Name -** SpotlightAuditServer
- **Template -** Third Party Server
- **Working Directory -** dot (.)
- **Command Line** - dot (.)
- **Command Line Arguments** - dot (.)
- **Connections -** add connections to config server and message server
- This Account should be set to **Default** user

- Create a duplicate application by selecting **Make New**
- Rename as **SpotlightAuditServerEC**

NB: When Spotlight SDP are to be installed in High Availability mode, six applications will have required to be created rather than two per environment.

- SpotlightAuditServer1
- SpotlightAuditServer2
- SpotlightAuditServer3
- SpotlightAuditServerEC1
- SpotlightAuditServerEC2
- SpotlightAuditServerEC3

Genesys SAM

The following sections only need to be followed if SAM (Spotlight Asset Management - License Tracking) is being installed. The sections on **GVP** and **WFM** again only require to be followed if these ate license types that are in place within your contact centre.

SQL Server Agent

SQL Server Agent must be running on the server that the Spotlight databases are located (normally only required for the PROD database)

GVP

The SAM module is required to only track **GVP MCP** applications used for **XML** Applications. It is not required to configure **GVP MCP** applica tions used only for **Queueing** purposes.

In order to track the utilisation of **GVP** each **MCP** to be tracked must be connected to a running **Genesys SNMP Master Agent** application. Multiple MCP’s can be connected to a single SNMP Master Agent application or it can be a one to one mapping, the choice in the deployment methods for the SNMP Master Agents is not provided by Blackchair but is a Genesys Architectural decision made by your

Genesys Architect.

For each MCP to be configured in the SAM modules the following information will need to be provided in the Spotlight data capture spreadsheet

- The Name of the MCP application as it appears in CME/Administrator
- The IP Address of the SNMP Master Agent the MCP is connected to
- The SNNP Master Agent Port number used
- The version of SNMP configured (1, 2 or 3)

If the SNMP Master Agent is running on Linux, it must be started as the Root user, this is due to Linux restricting Ports 0-1024 when not running as Root. Even if the SNMP Master Agent is running on a Port higher than 1024 it will still utilise the underlying standard SNMP Port 162 and so will fail to work for Spotlight SAM.

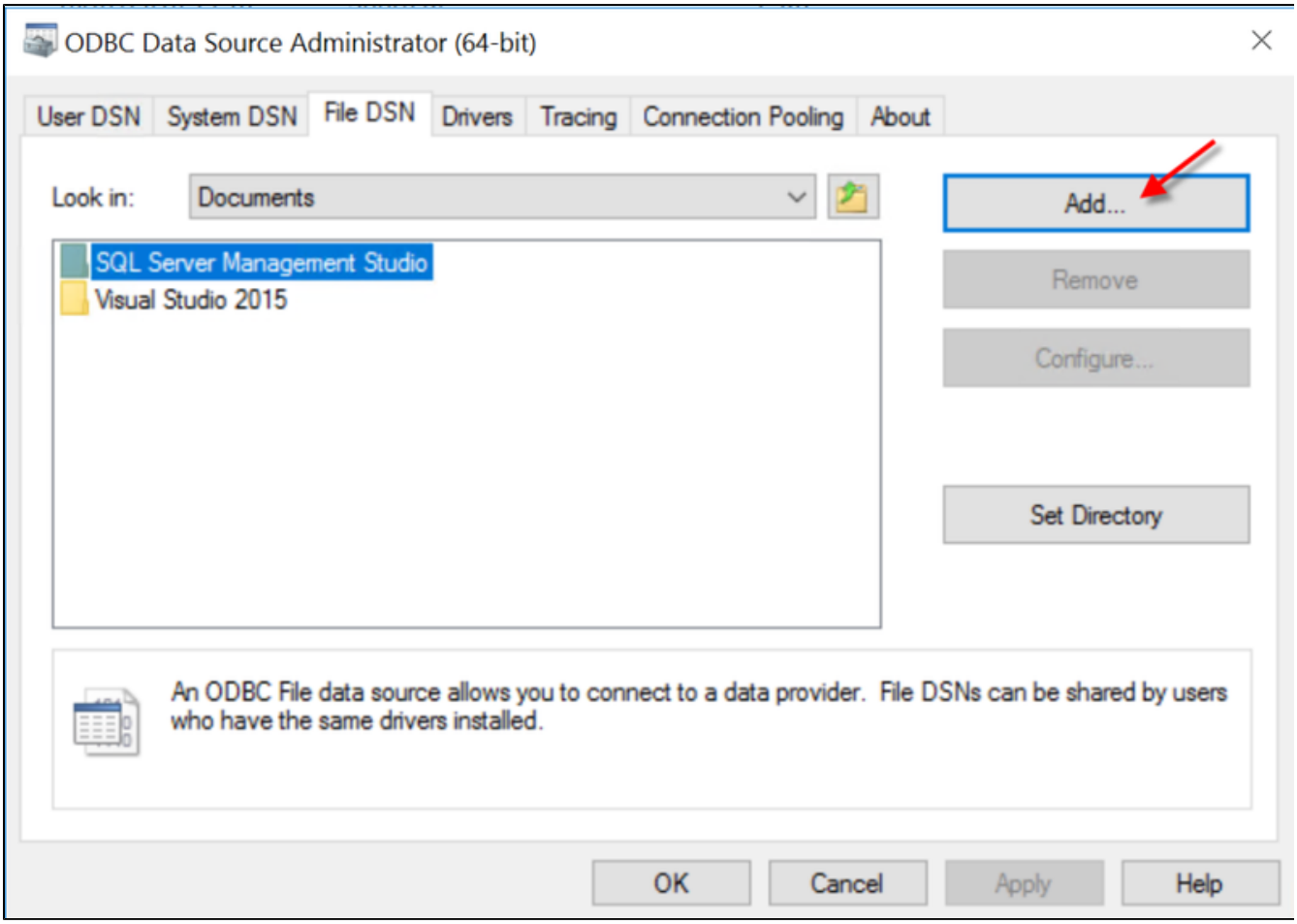
WFM

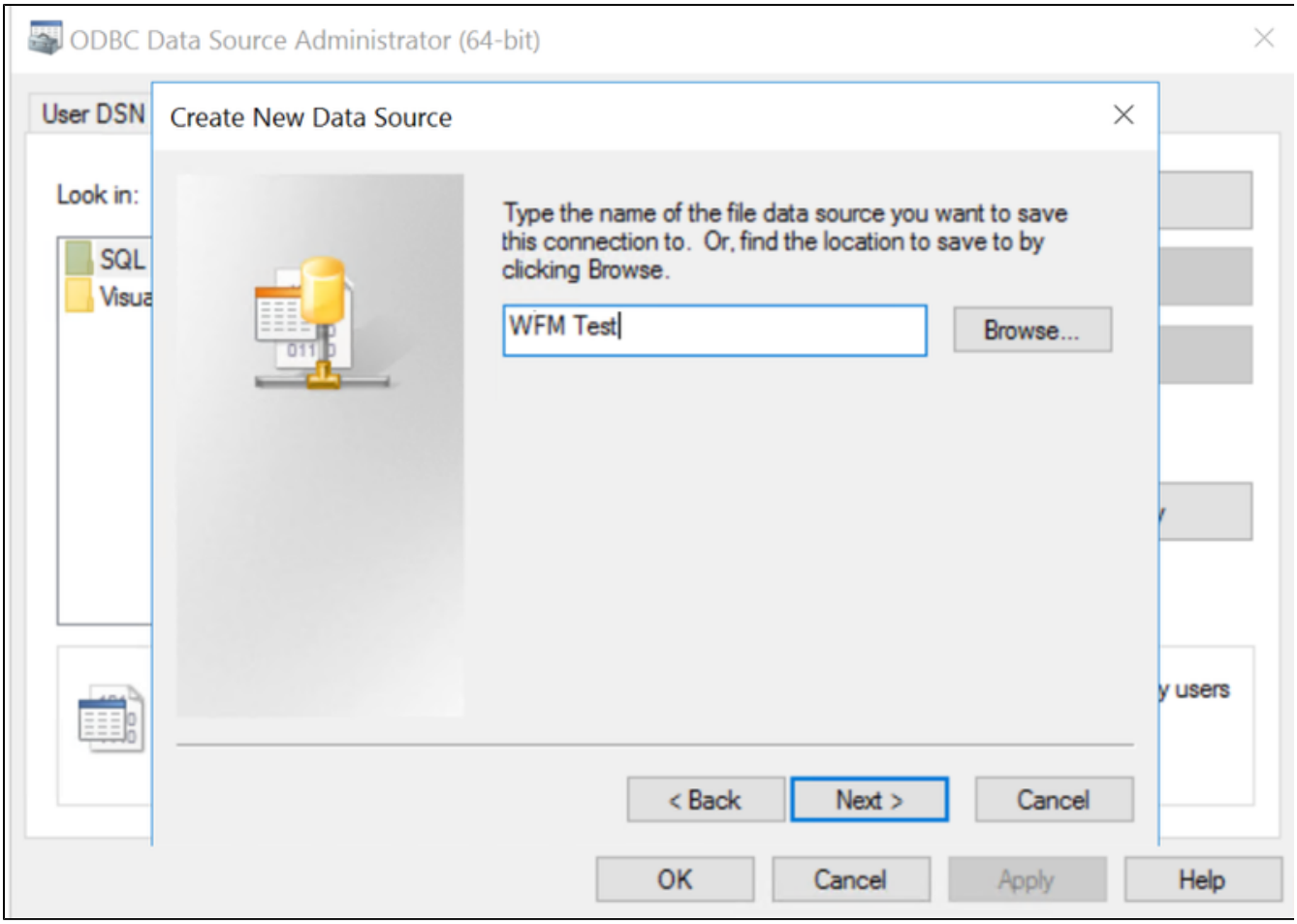
The Blackchair SAM module connects directly to the Genesys Workforce Management database using a Read only user name and password.

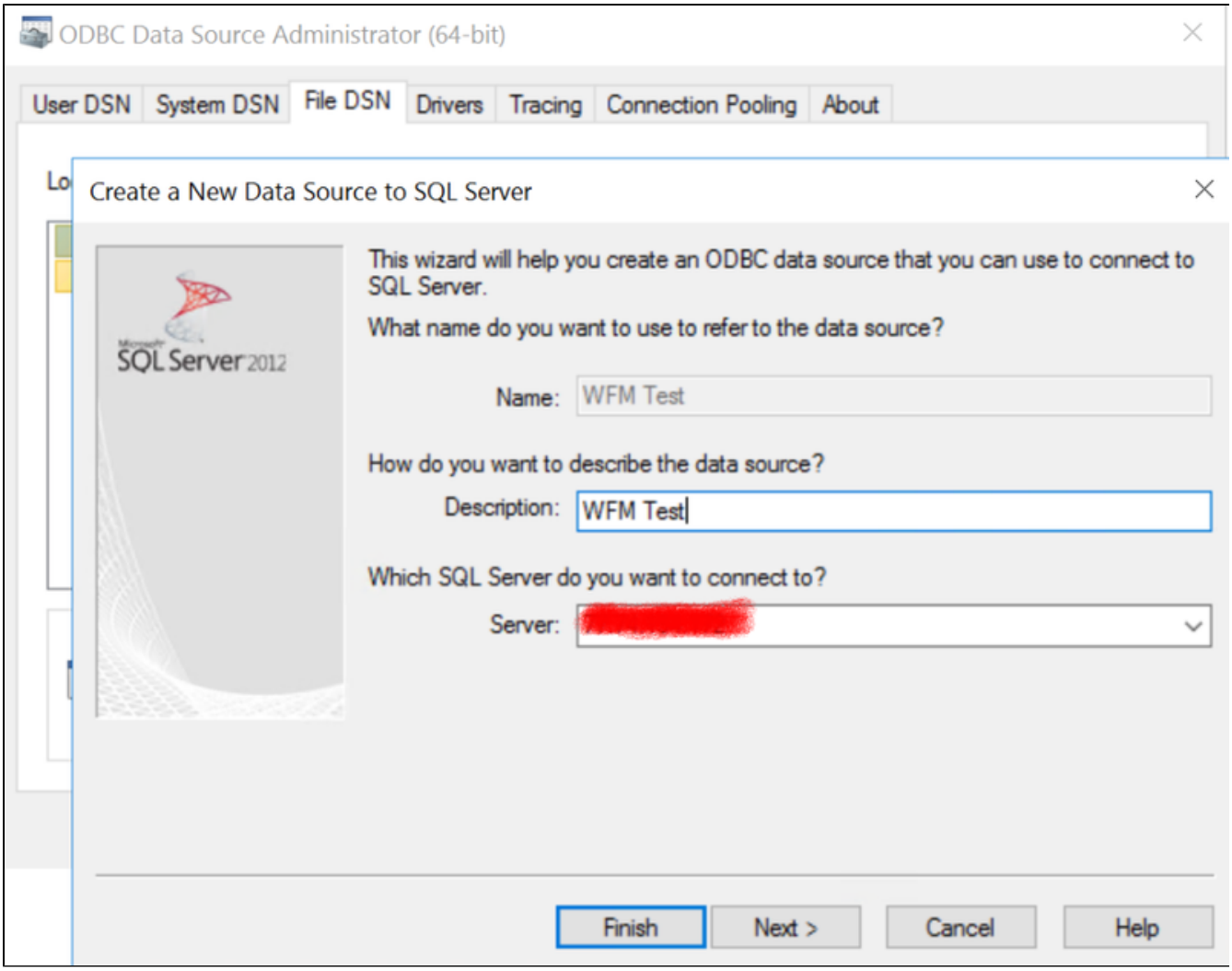
SQL

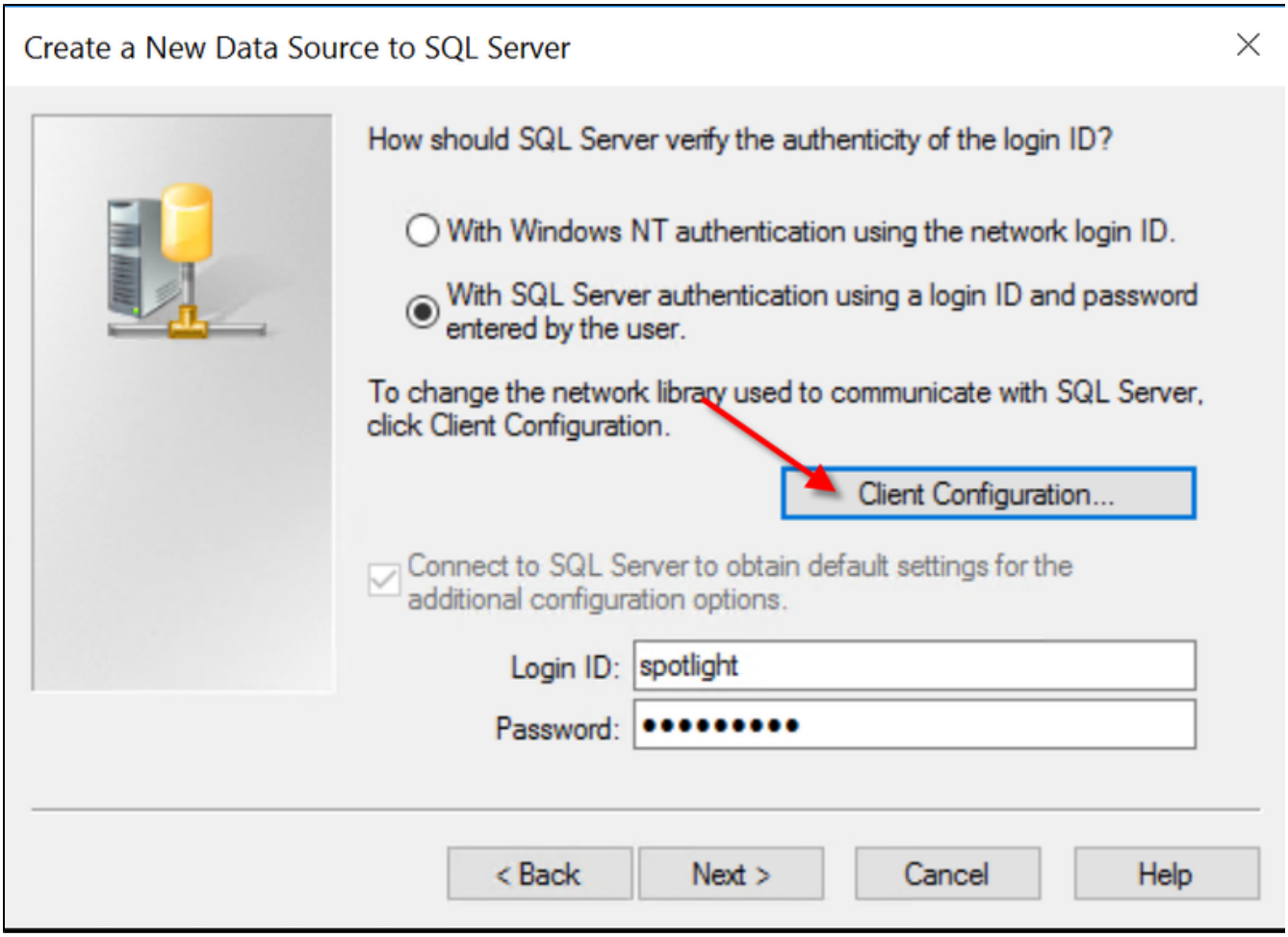
If Genesys WFM is using a Microsoft SQL Server then create a read only user name and password and test the user can connect from the Spotlight server using an ODBC connection from the Spotlight server as follows

Create an ODBC Connection ensuring to use the Port Number for SQL server, do not have the port dynamically assigned as this can provide a false positive.

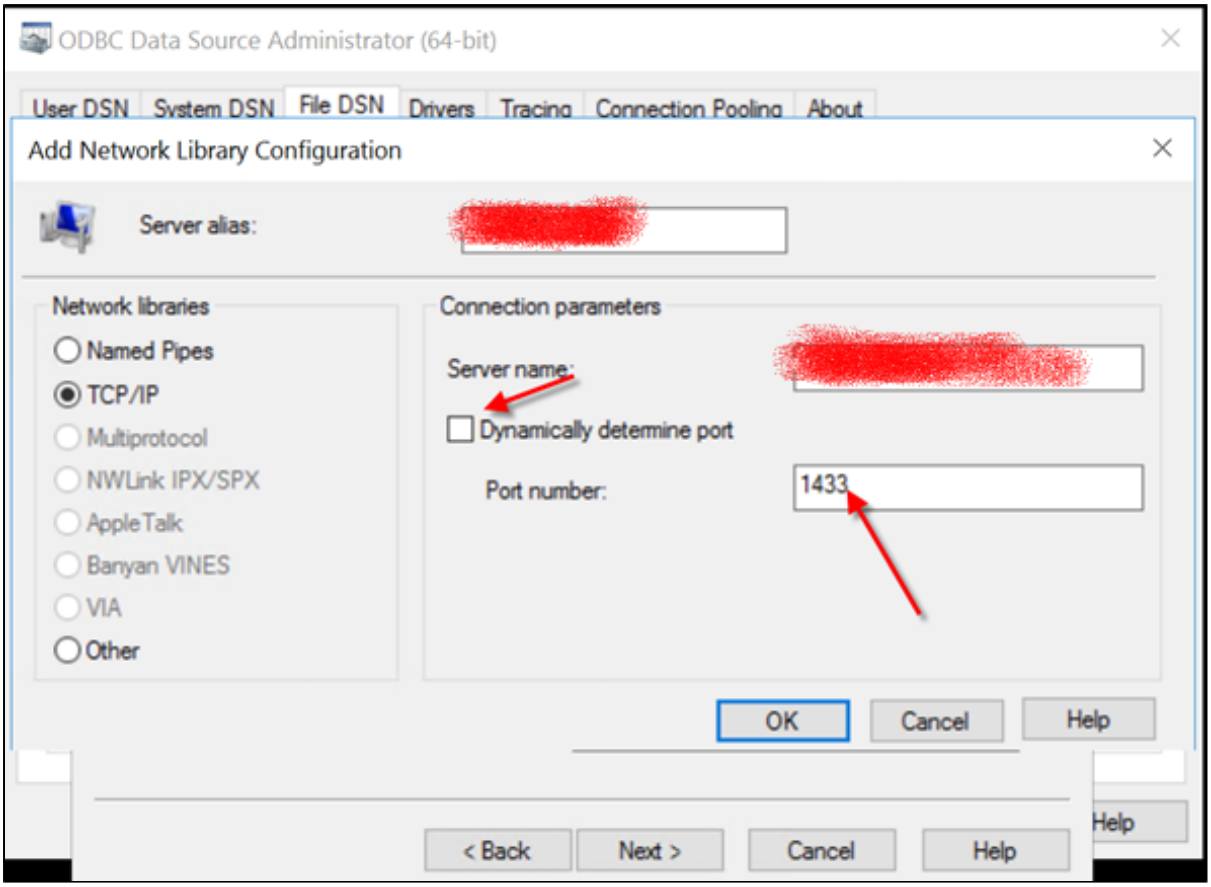

ODBC Data Source Administrator (64-bit)
User DSN
System DSN
File DSN
Drivers
Tracing
Connection Pooling
About
Look in:
Documents
SQL Server Management Studio
Visual Studio 2015
Add...
Remove
Configure...
Set Directory
An ODBC File data source allows you to connect to a data provider. File DSNs can be shared by users who have the same drivers installed.
OK
Cancel
Apply
Help

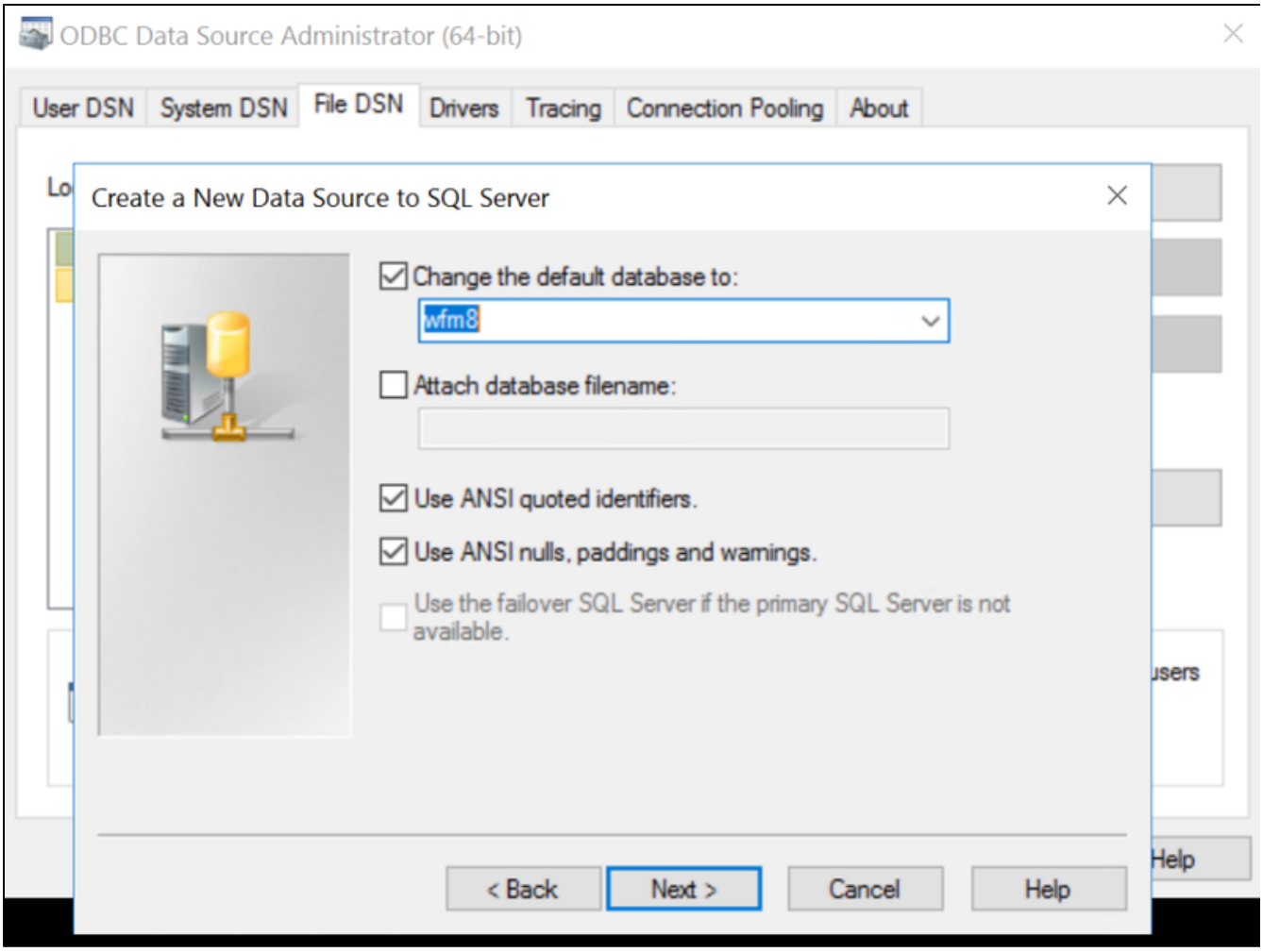

ODBC Data Source Administrator (64-bit)
User DSN
Look in:
SQL
Visua
Create New Data Source
Type the name of the file data source you want to save this connection to. Or, find the location to save to by clicking Browse.
WFM Test
Browse...
< Back
Next >
Cancel
OK
Cancel
Apply
Help
y users

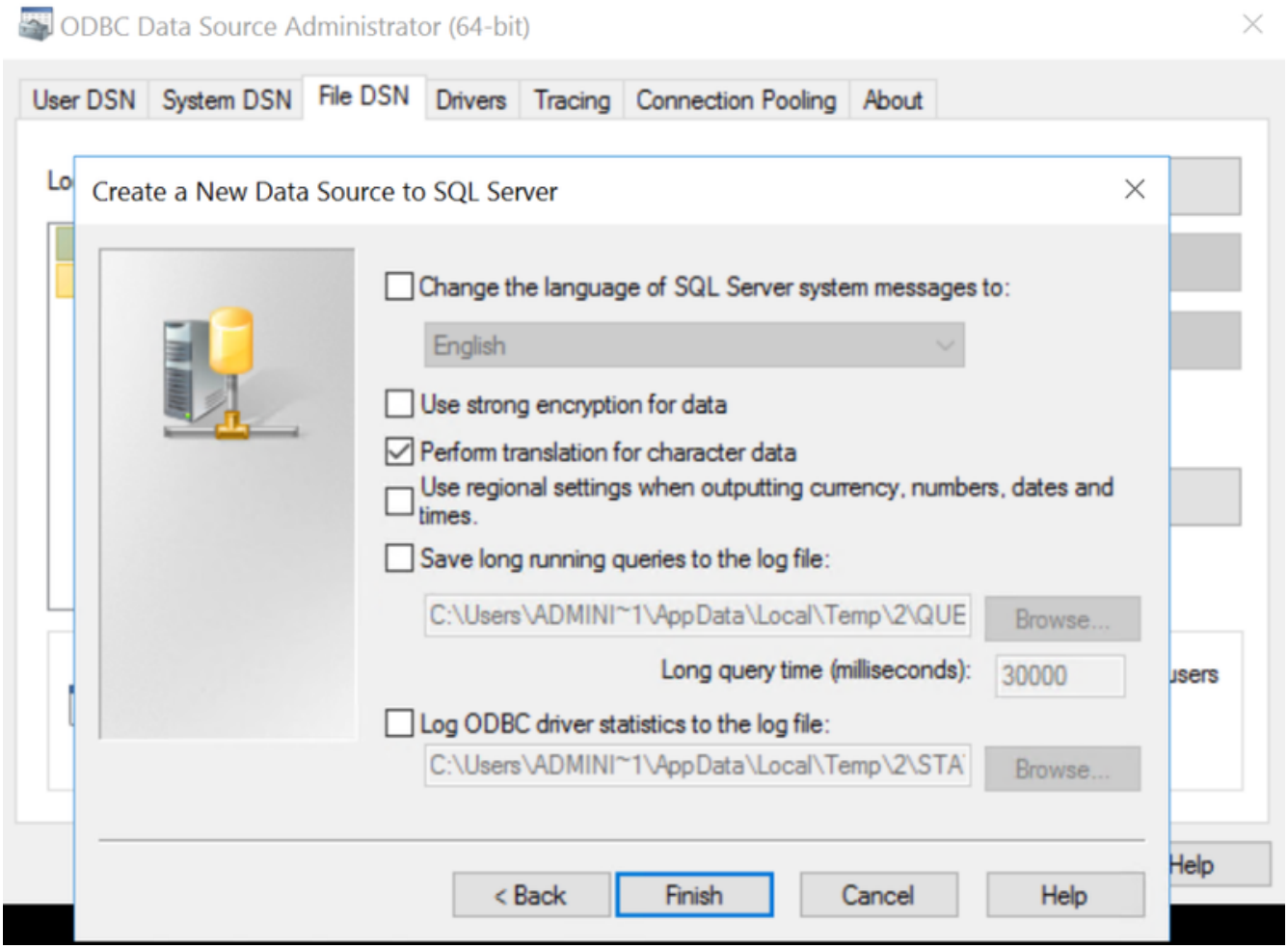

ODBC Data Source Administrator (64-bit)
User DSN
System DSN
File DSN
Drivers
Tracing
Connection Pooling
About
Create a New Data Source to SQL Server
SQL Server 2012
This wizard will help you create an ODBC data source that you can use to connect to SQL Server.
What name do you want to use to refer to the data source?
Name:
WFM Test
How do you want to describe the data source?
Description:
WFM Test
Which SQL Server do you want to connect to?
Server:
Finish
Next >
Cancel
Help

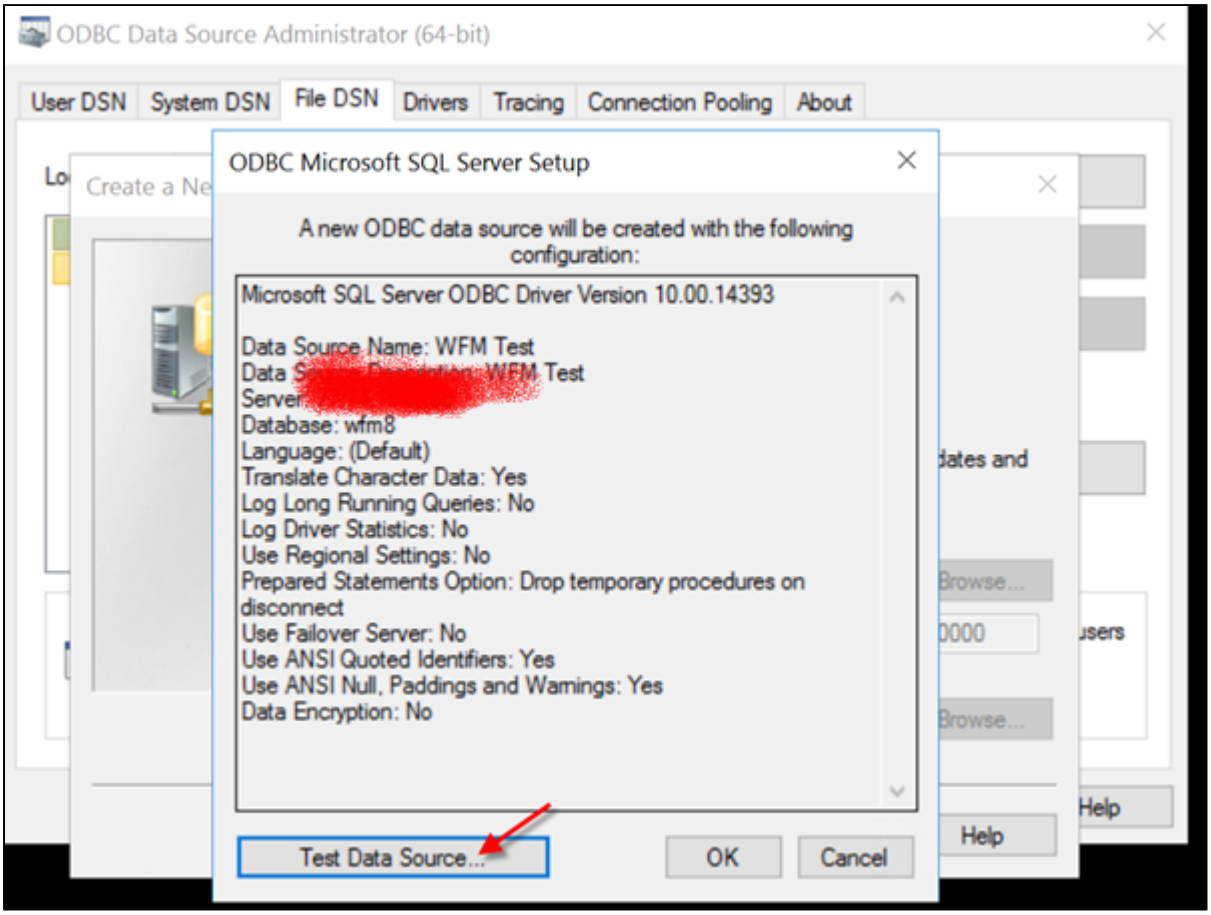


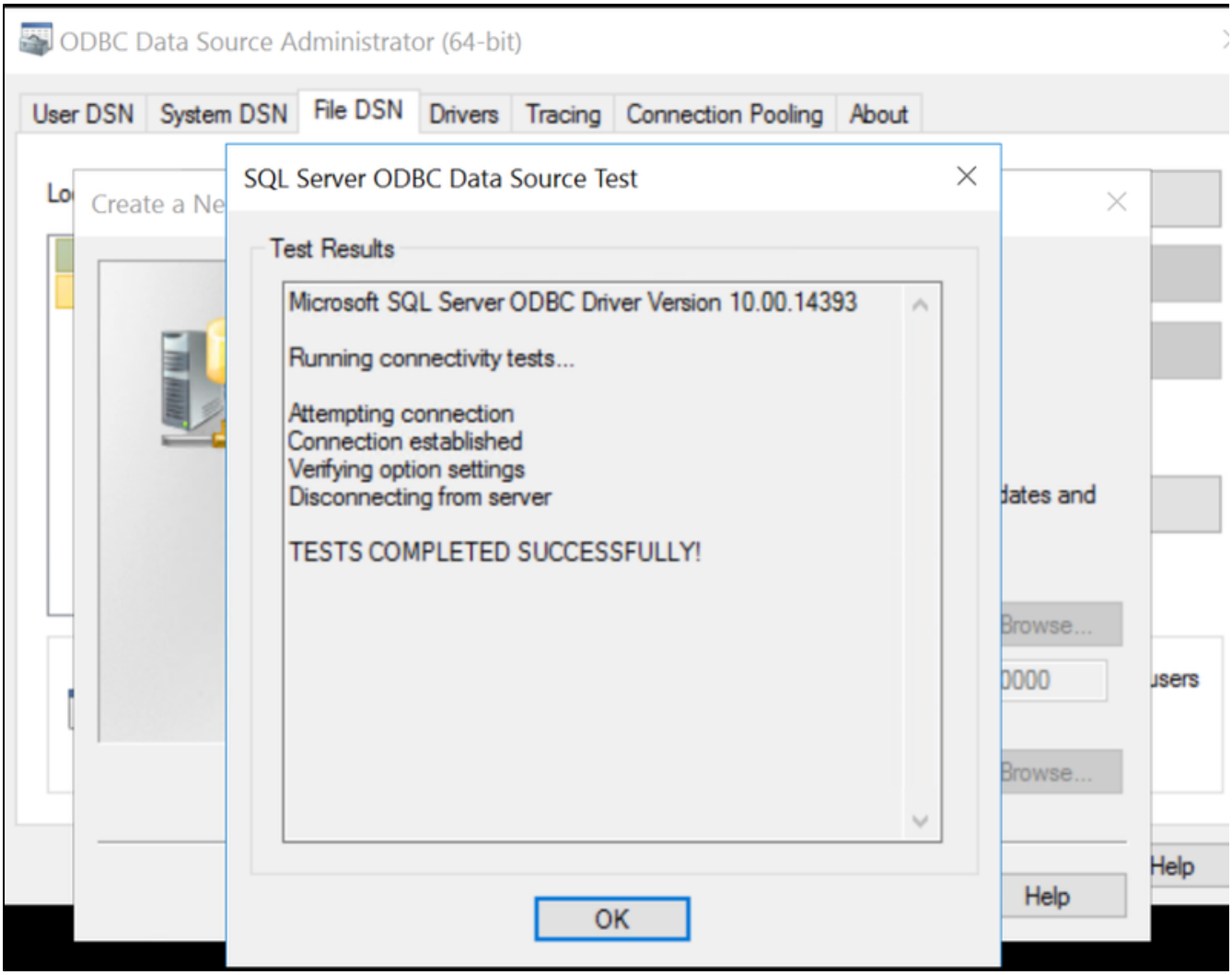
- Uncheck the "Dynamically determine port" option and set the SQL server port details you have been provided. The standard port is 1433
  If the connection is successful you will be able to change the default database to the WFM database


ODBC Data Source Administrator (64-bit)
User DSN
System DSN
File DSN
Drivers
Tracing
Connection Pooling
About
Add Network Library Configuration
Server alias:
Network libraries
Named Pipes
TCP/IP
Multiprotocol
NWLink IPX/SPX
AppleTalk
Banyan VINES
VIA
Other
Connection parameters
Server name:
Dynamically determine port
Port number:
1433
OK
Cancel
Help
< Back
Next >
Cancel
Help
Help


ODBC Data Source Administrator (64-bit)
User DSN
System DSN
File DSN
Drivers
Tracing
Connection Pooling
About
Create a New Data Source to SQL Server
Change the default database to:
wfm8
Attach database filename:
Use ANSI quoted identifiers.
Use ANSI nulls, paddings and warnings.
Use the failover SQL Server if the primary SQL Server is not available.
< Back
Next >
Cancel
Help


ODBC Data Source Administrator (64-bit)
User DSN
System DSN
File DSN
Drivers
Tracing
Connection Pooling
About
Create a New Data Source to SQL Server
Change the language of SQL Server system messages to:
English
Use strong encryption for data
Perform translation for character data
Use regional settings when outputting currency, numbers, dates and times.
Save long running queries to the log file:
C:\Users\ADMINI~1\AppData\Local\Temp\2\QUE
Browse...
Long query time (milliseconds):
30000
Log ODBC driver statistics to the log file:
C:\Users\ADMINI~1\AppData\Local\Temp\2\STA
Browse...
< Back
Finish
Cancel
Help

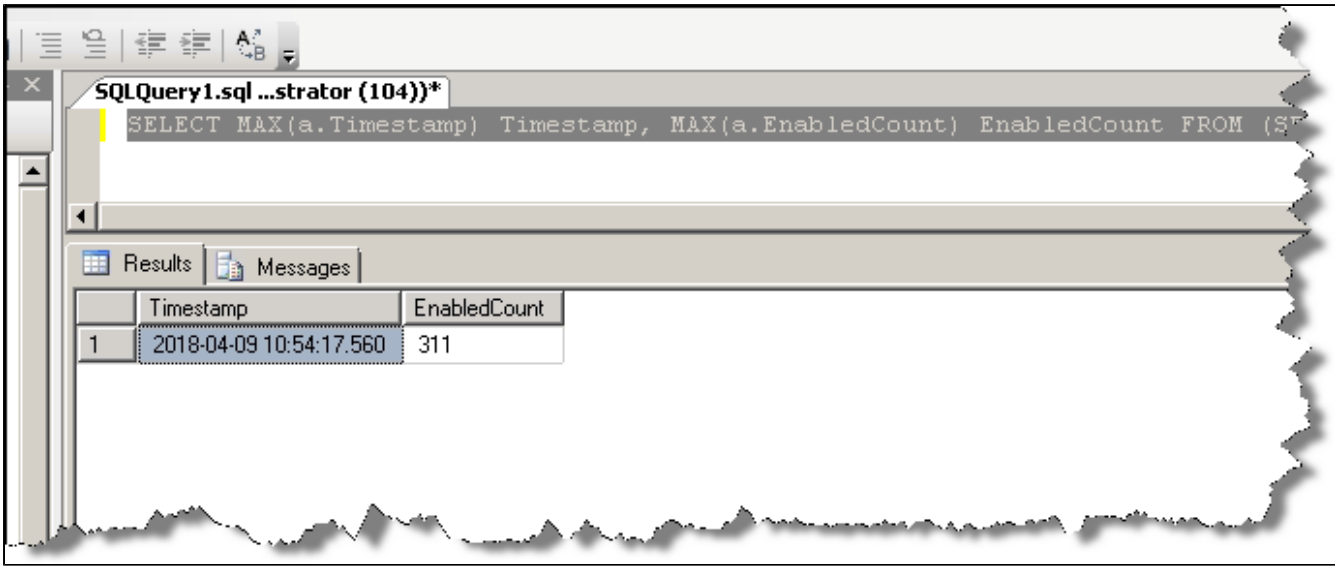

ODBC Data Source Administrator (64-bit)
User DSN
System DSN
File DSN
Drivers
Tracing
Connection Pooling
About
ODBC Microsoft SQL Server Setup
A new ODBC data source will be created with the following configuration:
Microsoft SQL Server ODBC Driver Version 10.00.14393
Data Source Name: WFM Test
Data S WFM Test
Server
Database: wfm8
Language: (Default)
Translate Character Data: Yes
Log Long Running Queries: No
Log Driver Statistics: No
Use Regional Settings: No
Prepared Statements Option: Drop temporary procedures on disconnect
Use Failover Server: No
Use ANSI Quoted Identifiers: Yes
Use ANSI Null, Paddings and Warnings: Yes
Data Encryption: No
Test Data Source...
OK
Cancel
Help



- Open an SQL Server Management Studio and connect to the WFM database, run the following SQL

```
SELECT MAX(a.Timestamp) Timestamp, MAX(a.EnabledCount) EnabledCount FROM (SELECT GETUTCDATE() Timestamp, COUNT(DISTINCT(S.GSW_AGENT_ID)) EnabledCount FROM WM_SCHEDULE_DAYS S WHERE S.WM_DAY_TYPE <> 0 AND S.WM_DATE = CONVERT(VARCHAR(10), GETDATE(), 120) UNION SELECT GETUTCDATE() Timestamp, 0 EnabledCount)a
```

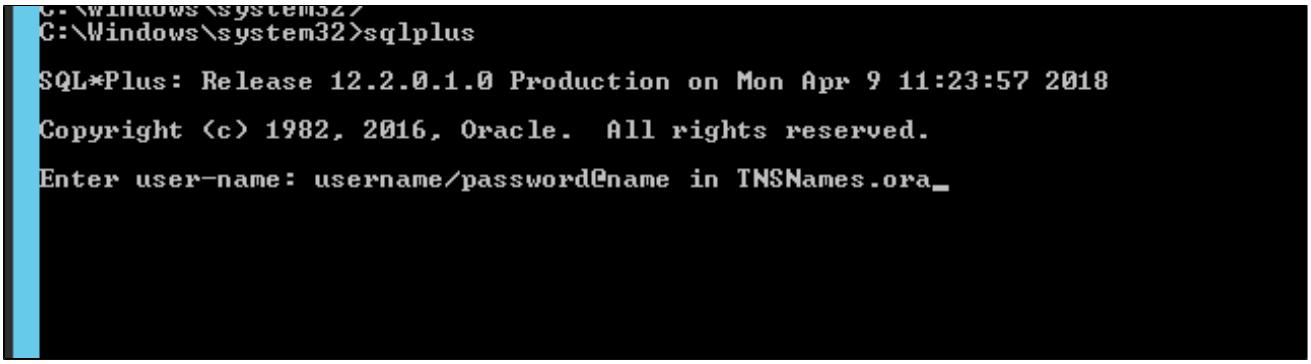
If the connections are correct then the value used for the SAM module will be returned



Oracle

If Genesys WFM is using an Oracle database a Read only user name and password on the schema owner is required. From the Spotlight server test access to the Oracle database using **TNSPING** and **SQL Plus** tools.

- The Oracle client needs to be installed on the Spotlight server and the **TNSNAMES.ORA** should be configured for the WFM connection.
- From the Spotlight Server open a command prompt and type **SQLPlus**, you will be then prompted for details to connect. This can be carried out using
    - **ReadonlyUserName/Password@OracleTNSNameEntry**



If connected to the database then connectivity is correct. Run a select statement against a table using the Schema owner to test access to the tables. Use the following SQL to test a value is returned

```
SELECT MAX(A.Timestamp) Timestamp, MAX(A.EnabledCount) EnabledCount FROM (SELECT SYS_EXTRACT_UTC(SYSTIMESTAMP) Timestamp, COUNT(DISTINCT(S.GSW_AGENT_ID)) EnabledCount FROM WM_SCHEDULE_DAYS S WHERE S.WM_DAY_TYPE <> 0 AND S.WM_DATE = TRUNC(SYSDATE) UNION SELECT SYS_EXTRACT_UTC(SYSTIMESTAMP) Timestamp, 0 EnabledCount FROM dual ) A
```

Statserver

- Some usage data comes from a Genesys Statserver, both by directly querying the Statserver using the SDK and by processing data

in a standard Genesys LOGIN table written in the Spotlight database. A statserver pair must be connected to all the T-Servers, SIP Servers and Interaction Servers in the Genesys system. For information on configuring statserver to write a LOGIN table please refer to the Genesys Stat Server Deployment Guide. A statserver pair dedicated to Spotlight is recommended but a shared statserver can be used if necessary.
- Spotlight requires a Statserver pair to connect to directly and to be writing its LOGIN table to the Spotlight database. Spotlight will connect to the statserver on its standard port and network connectivity must allow this and the connection to write to the Spotlight database.
- Spotlight requires a configuration server or writeable CSProxy pair to connect to and a Genesys login with minimum Create and Change permission to create Agent Groups in the CME "Agent Groups" folder and minimum Read and Execute permission on the whole CME. Spotlight will connect to the statserver and configuration server/CSProxy on its standard port and network connectivity must allow this.
- Statserver application must be connected to all Tenants that are to be used for license tracking.

Statserver LOGIN

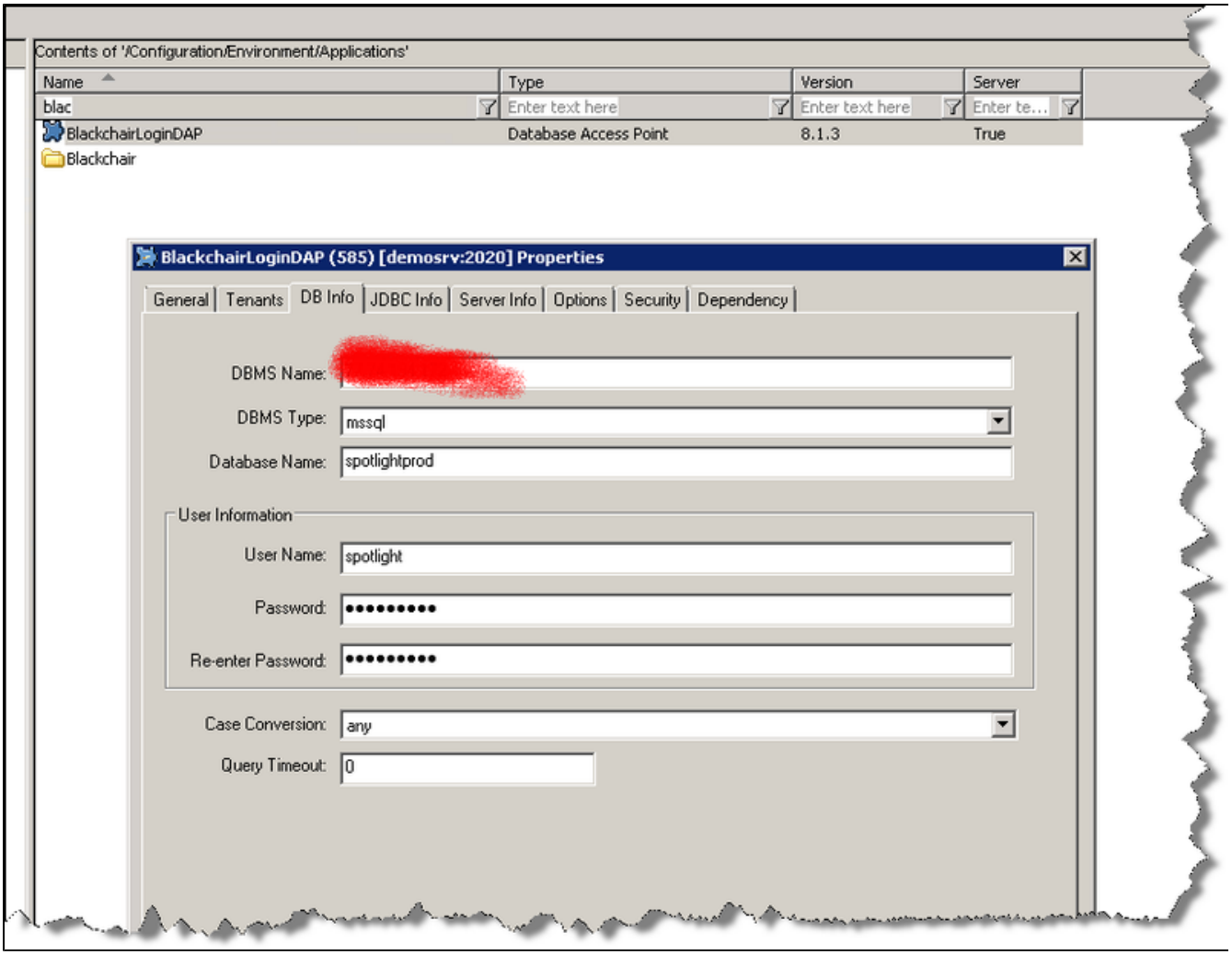
- A **Genesys Statserver** pair (Primary with backup) is required for the SAM installation.
- The StatServers are used to write to the Spotlight database **LOGIN** table.
- It is recommended to use a separate pair of StatServers to remove any potential issues with StatServers used for routing and reporting.
- A suitable **Genesys Data Access Point (DAP**) and **Genesys DB Server** will be required to support the writing of the data to the Login table.
- If the Genesys installation is on **Linux** hosts only, then it is likely that a **Genesys DB Server** that supports MS SQL server will not be available. If this is the case the Genesys DB Server can be installed on the Spotlight server.

The following notes define the setup required to set the Blackchair StatServers to write to the Login table in a Spotlight Database.

- First check the details of the host that has the Spotlight Database with the LOGIN Table, note the **DB Name, user name** and **passw ord**, these will be required for the DAP configuration.
- Locate your statserver
- Open the Options tab and filter on Statserver in Administrator to get the correct section.
- Set the following values
    - status-table = off
    - qinfo-table = off
    - voice-reasons-table=off
    - login-table=true
- Restart the statserver. The backup Statserver should be configured as the primary.

- Create a Database Access Point (DAP). Any existing DB Server that supports the SQL server client can be used with the DAP, although to ensure there is no issue with existing services it is recommended to create a new DB Server for this purpose:

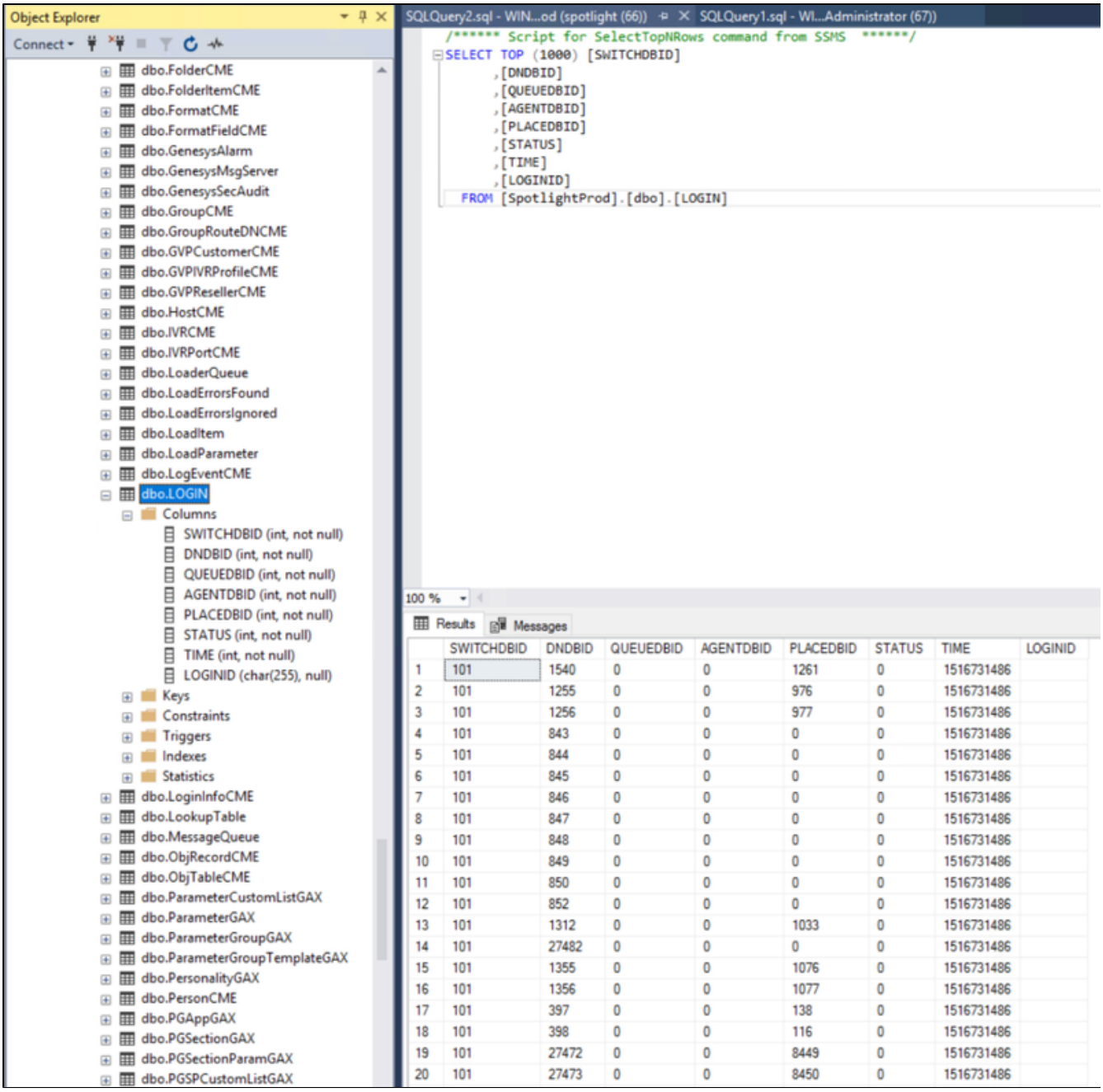
- Configure with the following information in the DB info tab
    - DBMS Name
    - DBMS Type
    - Database Name
    - User Name
    - Password



NB: if installing on Linux the SQL client will not be available and the DB Server should reside on a Windows box to provide the DB Server SQL client. If the customer has a Linux only environment then the DB Server could be placed on the Spotlight server and monitored for CPU and RAM utilisation.

- Once the DAP is configured, add a connection to the DAP in the Statserver
- ADDP and timeouts can be applied as the customer requires, Blackchair has no requirements for these values and so customer specific standards should be applied

- Log an agent in and out, data should then be seen in the Login table.



	SWITCHDBID	DNDBID	QUEUEDBID	AGENTDBID	PLACEDBID	STATUS	TIME	LOGINID
1	101	1540	0	0	1261	0	1516731486	
2	101	1255	0	0	976	0	1516731486	
3	101	1256	0	0	977	0	1516731486	
4	101	843	0	0	0	0	1516731486	
5	101	844	0	0	0	0	1516731486	
6	101	845	0	0	0	0	1516731486	
7	101	846	0	0	0	0	1516731486	
8	101	847	0	0	0	0	1516731486	
9	101	848	0	0	0	0	1516731486	
10	101	849	0	0	0	0	1516731486	
11	101	850	0	0	0	0	1516731486	
12	101	852	0	0	0	0	1516731486	
13	101	1312	0	0	1033	0	1516731486	
14	101	27482	0	0	0	0	1516731486	
15	101	1355	0	0	1076	0	1516731486	
16	101	1356	0	0	1077	0	1516731486	
17	101	397	0	0	138	0	1516731486	
18	101	398	0	0	116	0	1516731486	
19	101	27472	0	0	8449	0	1516731486	
20	101	27473	0	0	8450	0	1516731486	

Ports

When getting Genesys ready for Spotlight Audit and SAM the following Ports need to be open. It should be considered that all connections are bidirectional when configuring Firewall Rules.

Server 1	Server 2	Notes: Typical ports may not be the same as your system and should be confirmed

Blackchair Server	Configuration Server/Proxy Port	Standard port is 2020
Blackchair Server	Message Server	Customer defined port
Blackchair Server	WFM on SQL Database	Standard port 1433 but may be custom
Blackchair Server	WFM on Oracle Database	Standard port 1521 but may be custom
Blackchair Server	Spotlight Statserver	Customer defined port
Blackchair Server	SNMP Master Agent(s)	Customer defined port
Genesys Statserver pair	Blackchair Server	Customer defined port - LOGIN table writes to spotlight database normally on port 1433 inbound
Blackchair Server	GAX URL	Port used by GAX, normally HTTP Port 80 but may also be custom
Blackchair Server	GAX URL if GAX is being tracked	Typically 8040