Snell Advanced Media

Installation Guide

Remote User Management V1.1

Go! Remote Production Suite

Information and Notices

Copyright and Disclaimer

Contact Details

Customer Support

For details of our Regional Customer Support Offices please visit the SAM web site and navigate to Support/Customer Support Contacts.

https://s-a-m.com/support/247-support/

Customers with a support contract should call their personalized number, which can be found in their contract, and be ready to provide their contract number and details.

Conventions Used

Text

<Text>	indicates a specific key press on the QWERTY keyboard.
NN/nn	indicates a value entered on a numeric keypad.
Text/text	indicates either an application menu function or a Windows/SAM installation/system setting.

Symbols

See: Reference to items in other documents.

Notes: System, software and workflow points to consider and remember.

Tips: Useful hints and advice when undertaking tasks.

Contents

1. Overview

1.1 Description

A properly configured deployment of the Go! Production Suite provides an Enterprise grade user management system in additional to the rich API, thick and thin applications that are available.

It allows administrators to control the logon of users, and the tasks and roles different levels of users can access.

The User Management software is installed with the HTTP Transformer but requires some specific additional components and configuration.

1.2 Pre-requisites

1.2.1 Microsoft SQL Server

An installation of Microsoft SQL Server Standard is required:

- A trial of Microsoft SQL Server Standard is suitable for demo and POC systems, but has restrictions. It is freely available, but registration may be required.
- A fully licensed copy of SQL Server Standard is recommended or operational deployments as it provides numerous levels of resilience. While SAM can provide the SQL Server software, it is likely that the customer can provide suitable SQL Server Standard licenses at a far lower cost than SAM can due to internal Volume License Agreements between the customer and Microsoft.

On a small system with the recommended one or two dedicated load balancers, the user management database can live on the Load Balancer(s) hardware, with the main and mirror database sitting on the two load balancers, and the third witness running on a lower spec machine.

For larger or very busy systems, a separate resilient installation of SQL Server Standard is recommended for maximum resilience and system loading without performance drops at peak times.

General information about the setup and configuration of SQL server can be found here:

https://msdn.microsoft.com/en-us/library/ms187048.aspx

1.2.2 HTTP Transformer Licenses

Each Transformer still requires a GenQ license - either using dongle or MAC code - to run, so ensure the installed software and VM instance of the HTTP Transformer are correctly licensed as has been the case previously.

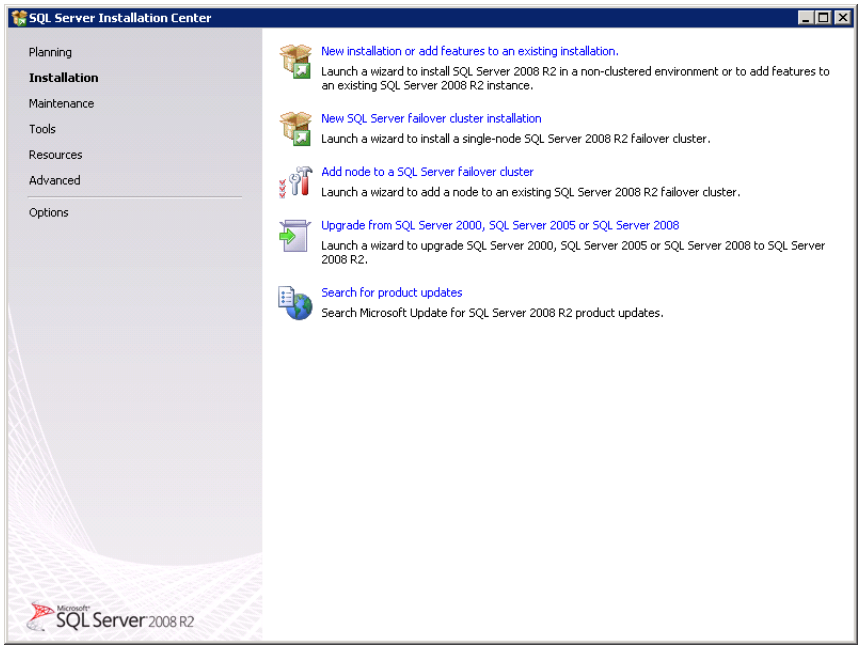
2. Installation and Configuration

2.1 Install and Configure a Non-resilient Database

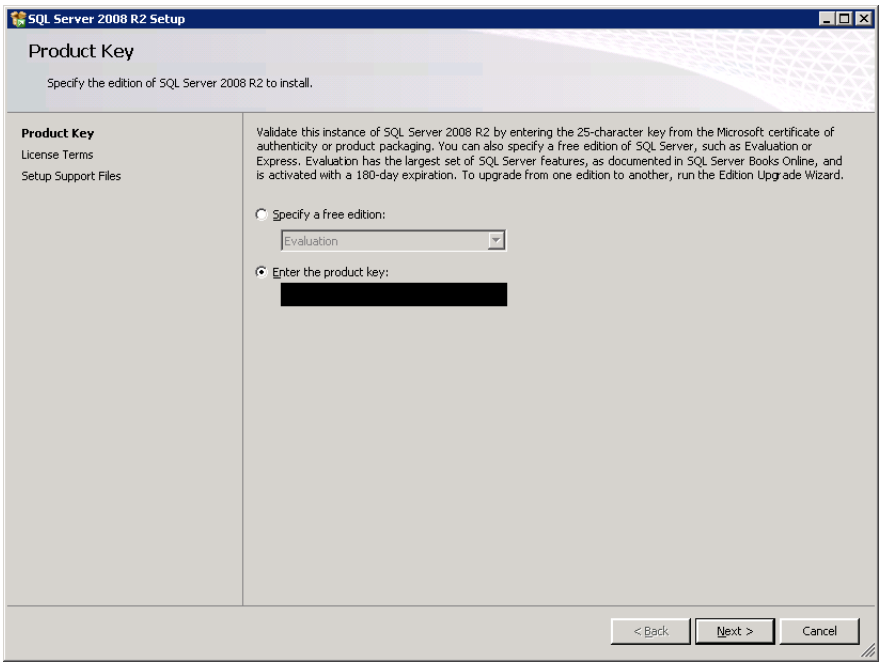
This installs a single database that is not resilient or redundant, suitable only for POC, demonstration or non-mission critical deployments.

2.1.1 Install Microsoft SQL Server

1. Run **setup.exe**.
2. Select **Installation**.
3. Select **New installation or add features to an existing installation**.

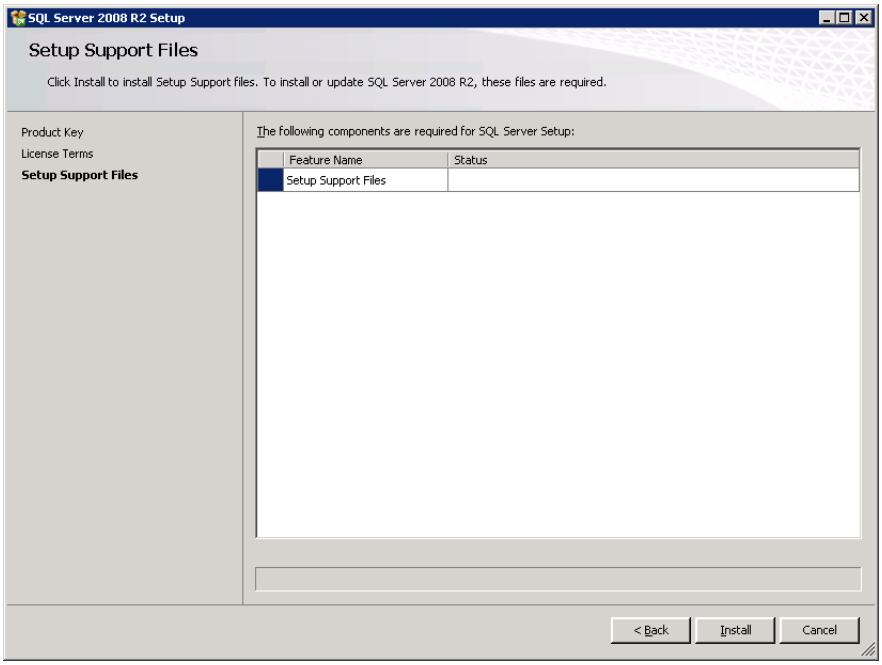


4. Enter the Product key or specify an Evaluation:

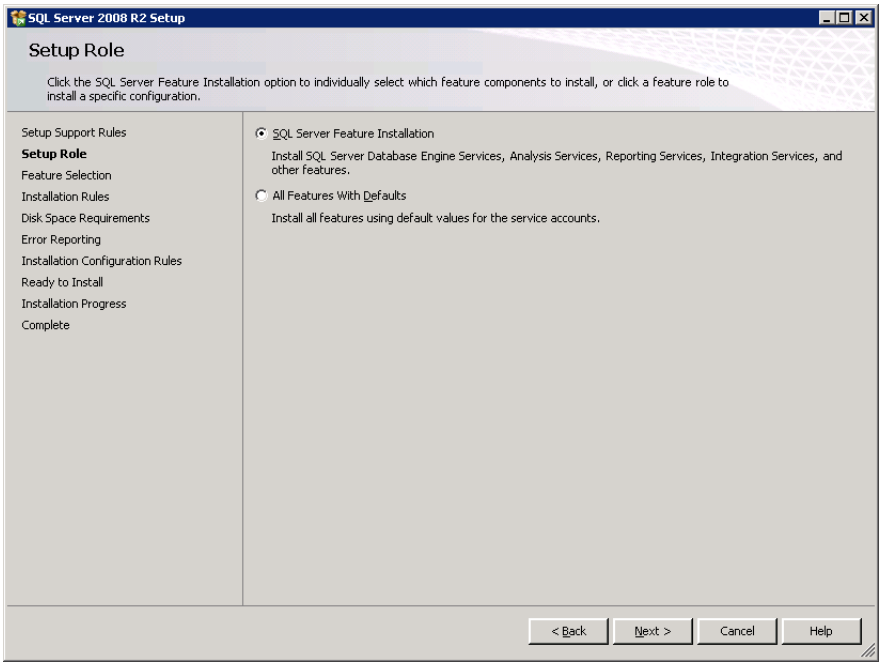


5. Press **Next** and accept terms.

6. From Setup Support Files, press **Install**.



7. From Setup Role select **SQL Server Feature Installation**. Press **Next**.



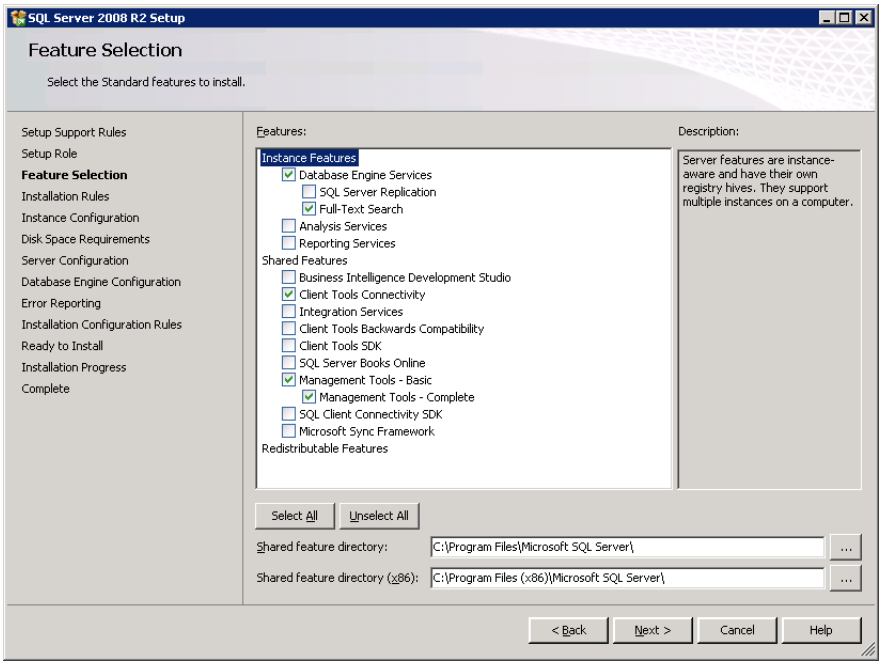
8. From Feature Selection, select the following:

Instance Features

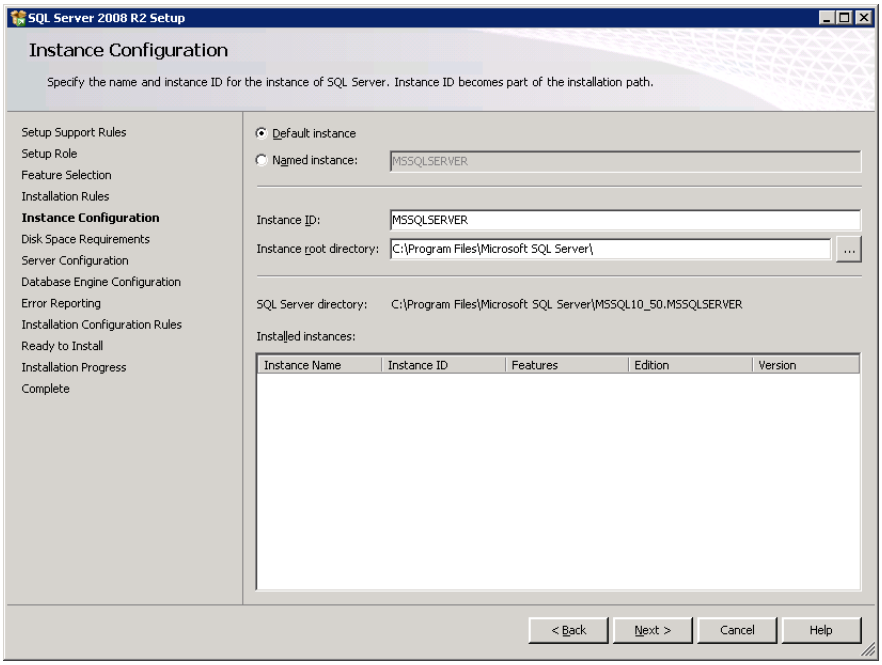
- Database Engine Services
    - Full Text Search

Shared Features

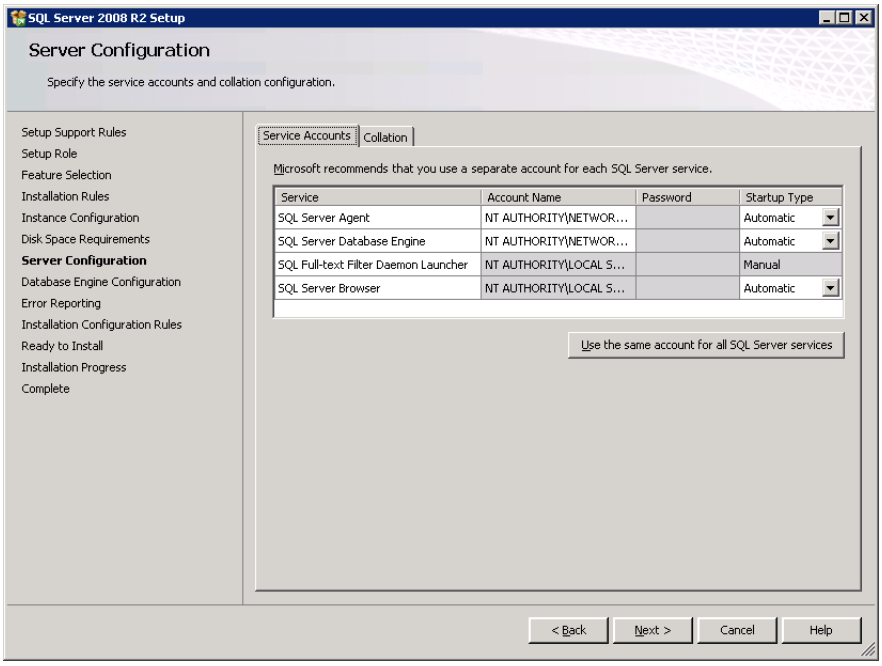
- Client Tools Connectivity
- Management Tools
    - Management Tools Complete



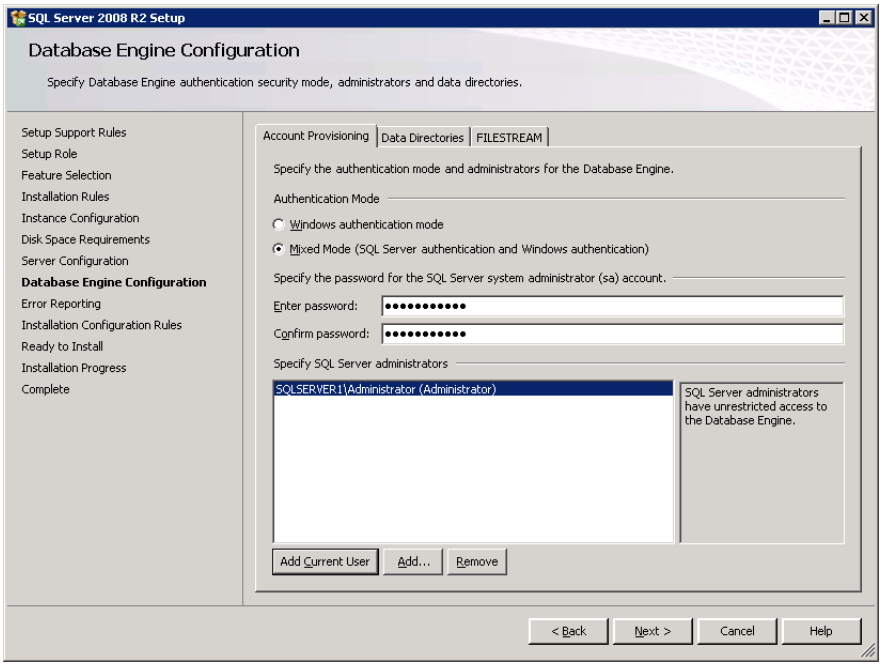
9. Press **Next**.



10. From Instance Configuration select **Default instance**. Press **Next**.



11. Press **Next** until the Server Configuration option displays, then set start-up type to **Automatic** for **SQL Server Agent**, **SQL Server Database Engine** and **SQL Server Browser.**
12. Press **Next** to go to Database Engine Configuration.
13. Under Authentication Mode, select the Mixed Mode radio button and set the following password for the **sa** account: **0Sam0@1Sam1**



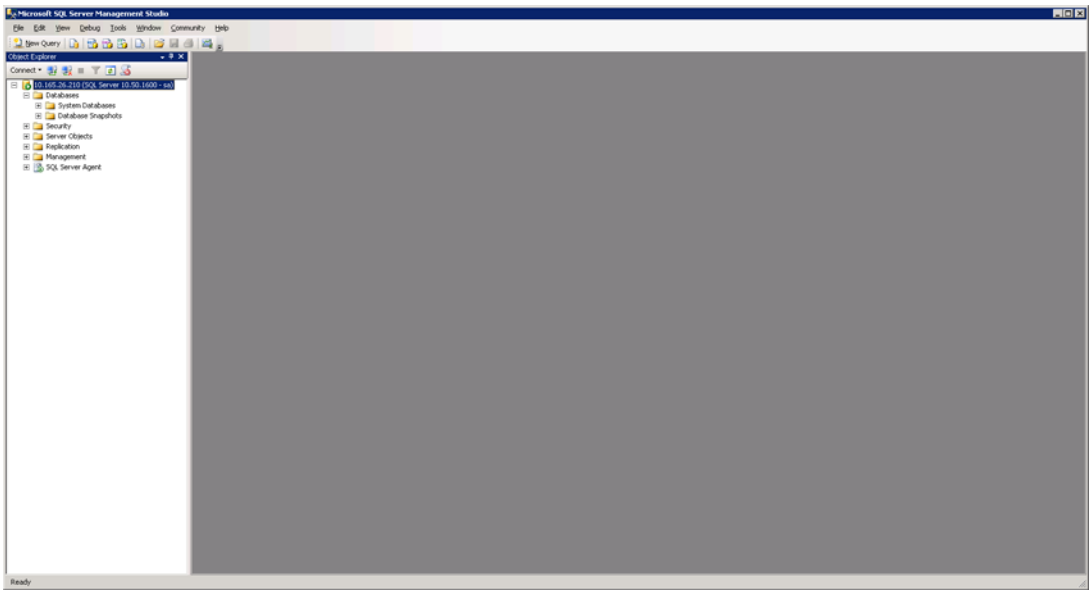
14. Press **Add Current User**.
15. Press **Next** for all the remaining options and at the final screen press **Close** to complete installation.

2.1.2 Set up the User Management Database

Once the SQL set-up is complete, launch **SQL Server Management Studio** to login to the SQL Server Engine / Instance using the following credentials:

Server Name	IP address of the server the MS SQL Server is installed on
Authentication	SQL Server Authentication
Login	sa
Password	0Sam0@1Sam1

- Press **Connect**. Once logged in the following displays:



2.1.2.1 Run Scripts to Generate the Database

Firstly, acquire the **Go! Production Suite Database Setup Scripts** from Support. These are in a zip file that must be decompressed before use.

1. Create a folder in **C:\Data\Usermanagement**.
2. Run the scripts below in the order specified. In the SQL Management Studio to run a script, press Ctrl + O.
   a Inside the uncompressed ZIP file navigate to **Usermanagement_InstallScripts\DB_Gen_and_Scheduled_Jobs**.
   b Select the required .sql file.
   c Once loaded, press **F5**.

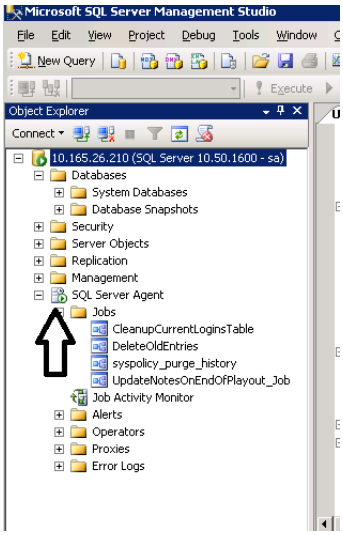
Perform the same steps for all of the following scripts in the folder **in this order**:

1. Session_DB_GenScript_with_Data
2. CleanupCurrentLoginsTable
3. DeleteOldEntries
4. UpdateNotesOnEndOfPlayout_Job

Running these scripts sets up the database with one user with the following credentials:

Username	admin
Password	quantel@

Ensure SQL Server Agent is running by checking that there is a green play button as part of the icon.



2.2 Install and Configure a Resilient Database

Setting up SQL Server for redundancy and fail-over uses three instances, each set-up with the following role:

- Principal
- Mirror
- Witness

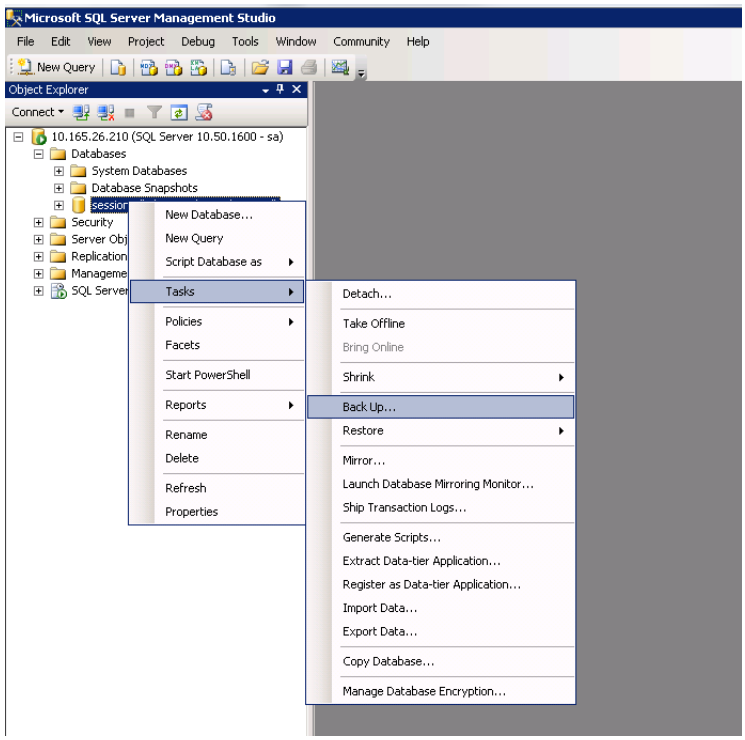
Before proceeding, ensure three instances of SQL are running.

Setting up the SQL Server for high availability requires the following steps:

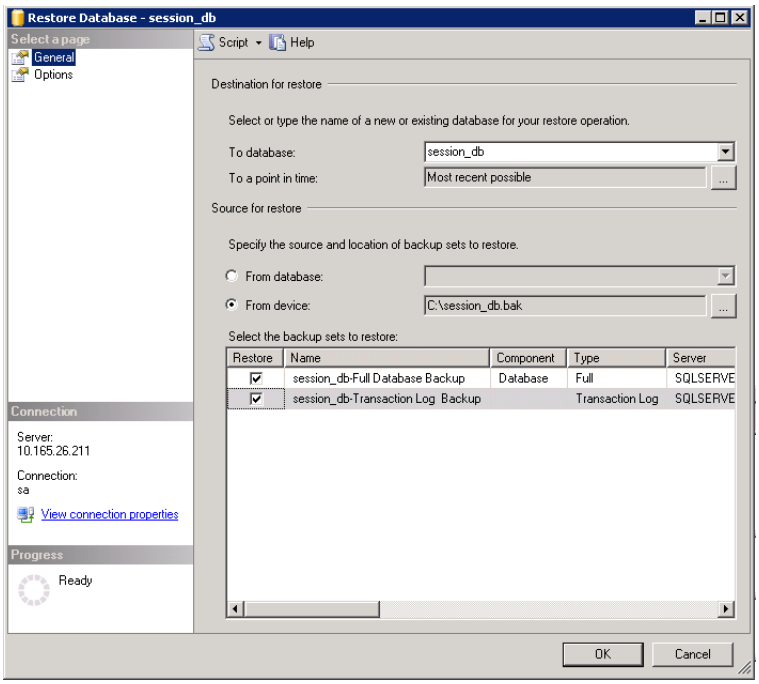
1. Restore a copy of the Principle database in NO RECOVERY MODE on the mirror
2. Install SQL Server as the witness (no manual configuration is required).
3. Configure all three databases to be aware of each other.
4. Modify the User Management **web.config** to point to the fail-over SQL Server cluster.

2.2.1 Restore a Copy of the Database on the Mirror

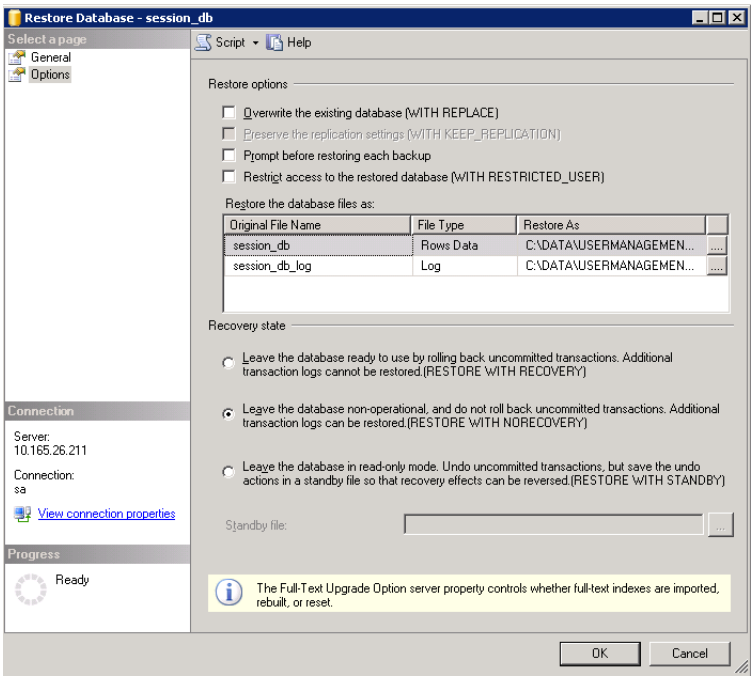
1. The restore is best performed when there are minimal or no logged on users.
2. On the principal SQL machine, right click on **session_db > Tasks > Back up**. Select the correct database and set backup type to **Full**.
3. Press **OK**.



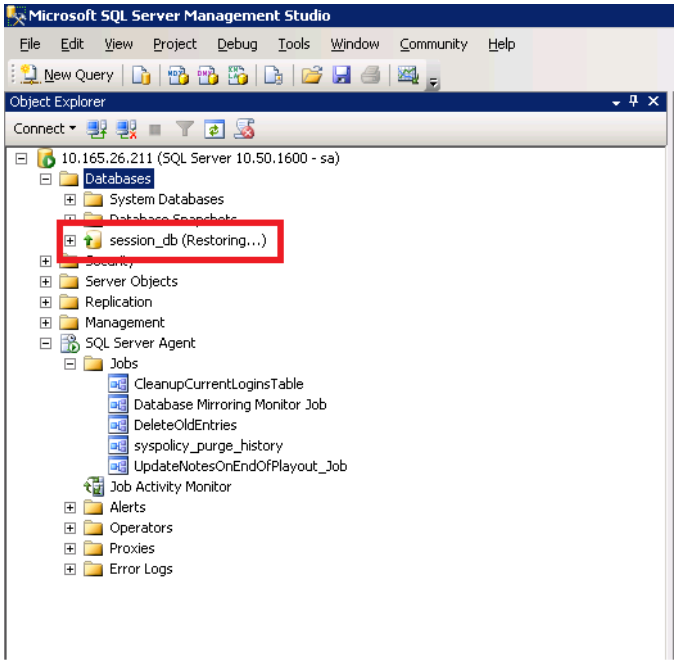
4. Copy the **.bak** file on to the Mirror machine. In SQL Server Management Studio, right click on databases and select **restore database**.
5. In the To database field as enter **session_db** and specify the source to point to the **.bak** file.



6. Select **Options** from the left column and set Recovery state to "...(RESTORE WITH NORECOVERY)"



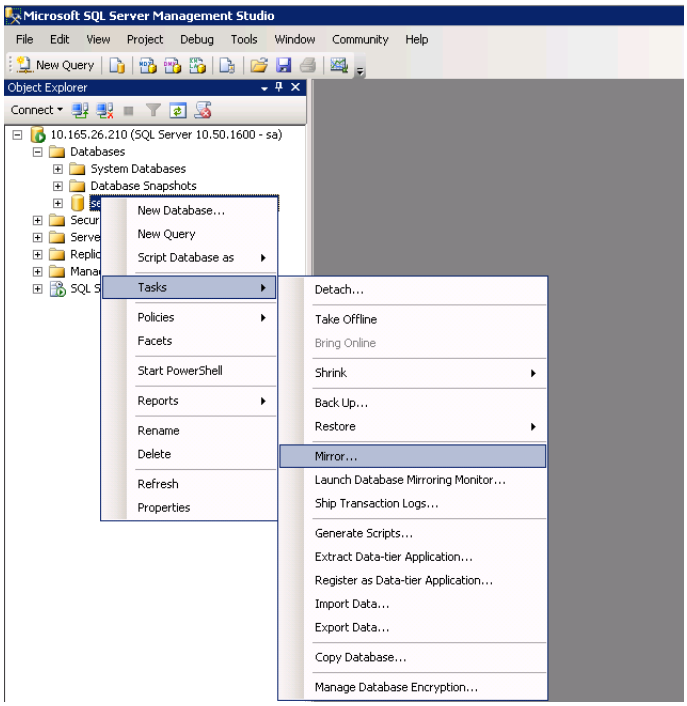
7. Press **OK**, and session_db is restored in read-only mode.



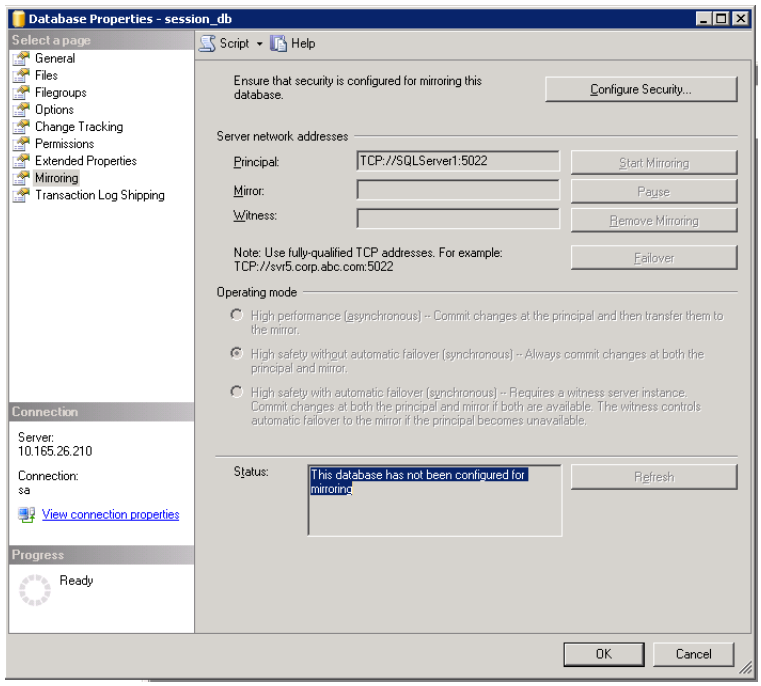
As long as SQL Server is installed properly, witness doesn't require any manual configuration.

2.2.2 Run the Wizard to Set-up Mirroring and Fail-over

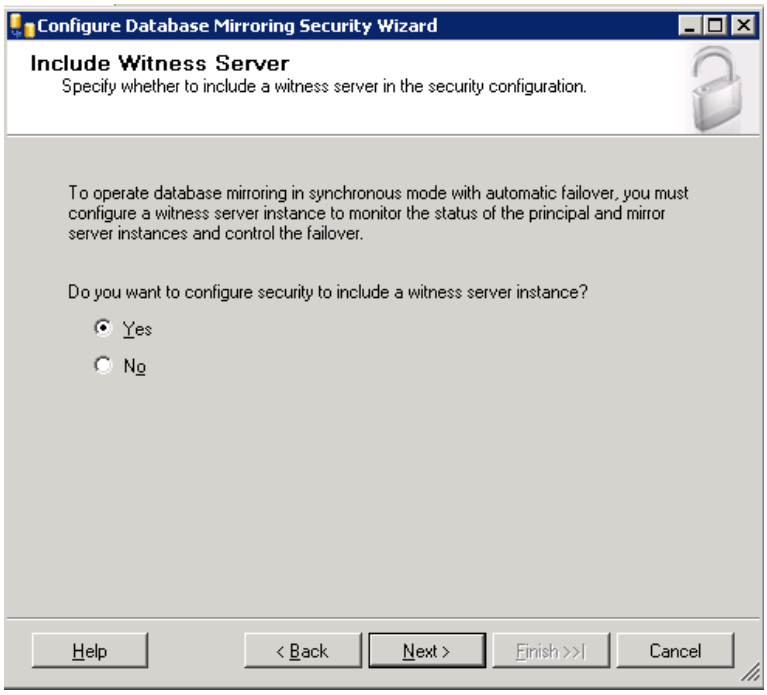
1. On the **Principal** SQL instance, right click on the database and select **Tasks**, then **Mirror.**



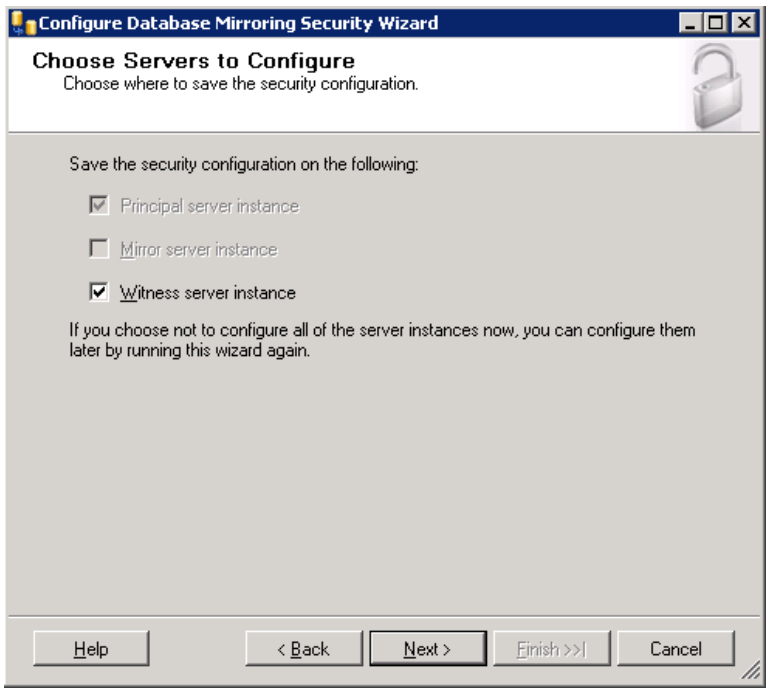
2. Select **Configure Security**.

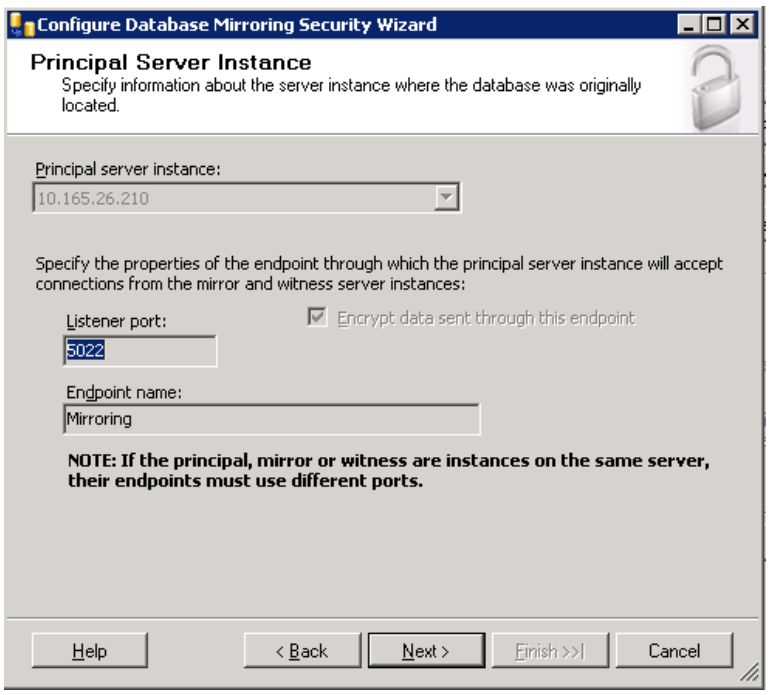


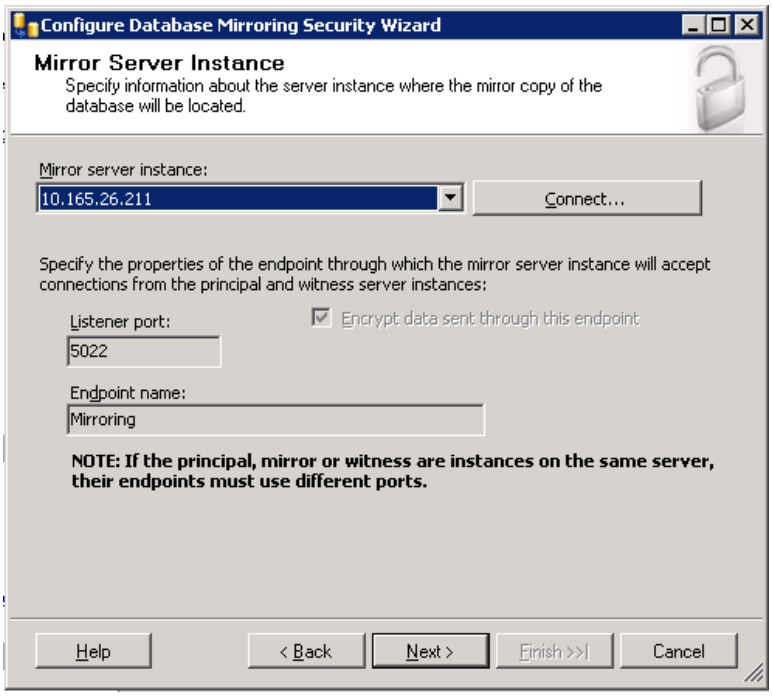
3. Select the **Yes** radio button.

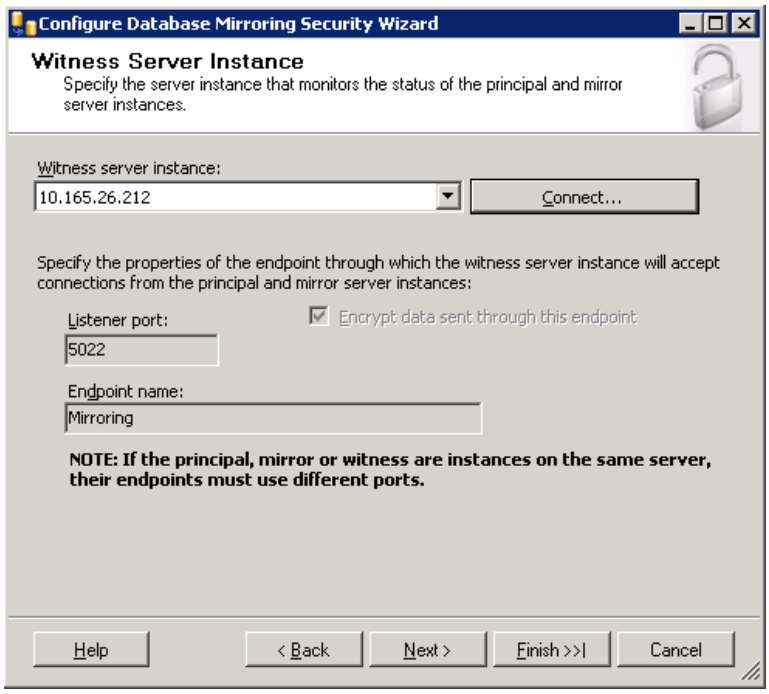


4. Press **Next**.
5. Specify the mirror and witness instances and connect to them as per the following screens.

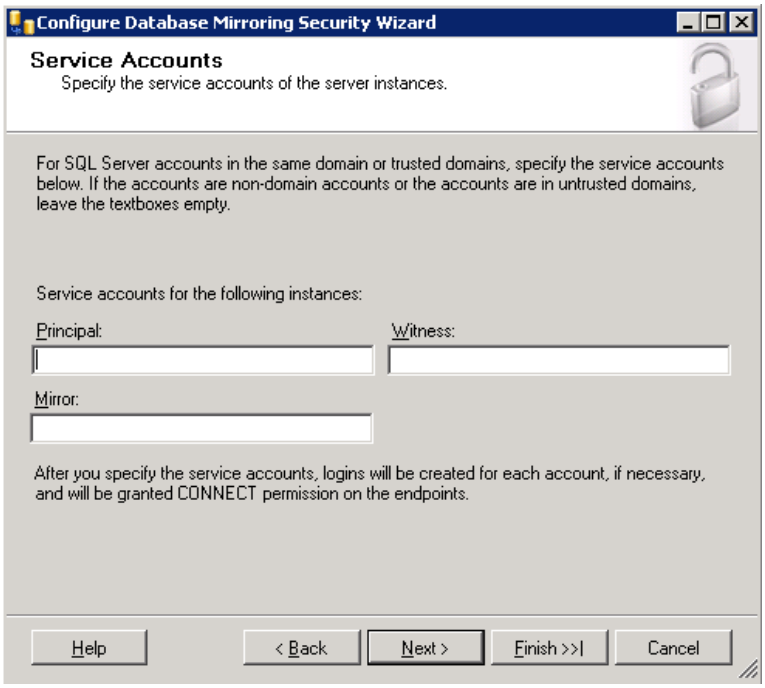

Configure Database Mirroring Security Wizard
Choose Servers to Configure
Choose where to save the security configuration.
Save the security configuration on the following:
Principal server instance
Mirror server instance
Witness server instance
If you choose not to configure all of the server instances now, you can configure them later by running this wizard again.
Help
< Back
Next >
Finish >>|
Cancel


Configure Database Mirroring Security Wizard
Principal Server Instance
Specify information about the server instance where the database was originally located.
Principal server instance:
10.165.26.210
Specify the properties of the endpoint through which the principal server instance will accept connections from the mirror and witness server instances:
Listener port:
5022
Encrypt data sent through this endpoint
Endpoint name:
Mirroring
NOTE: If the principal, mirror or witness are instances on the same server, their endpoints must use different ports.
Help
< Back
Next >
Finish >>|
Cancel

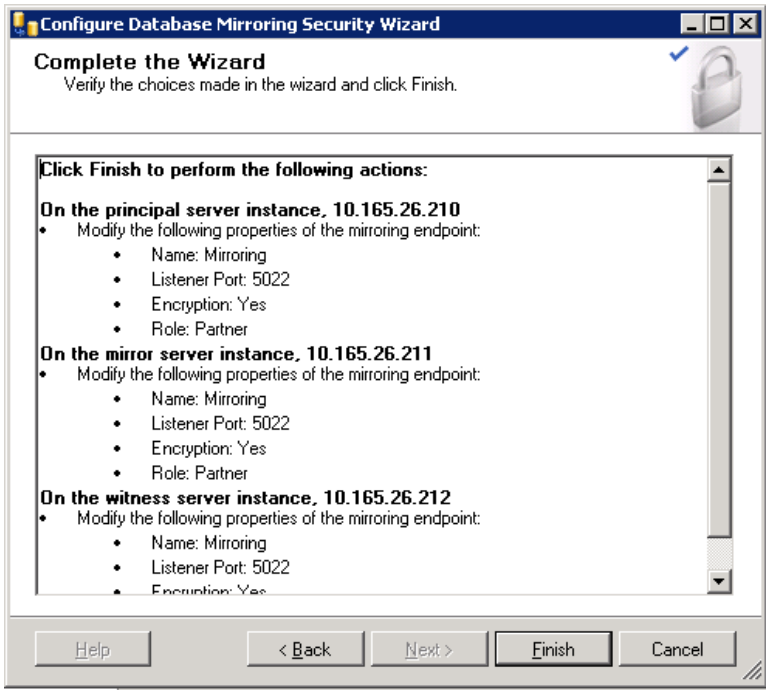




6. Press **Finish**.
7. Leave the service accounts fields empty.

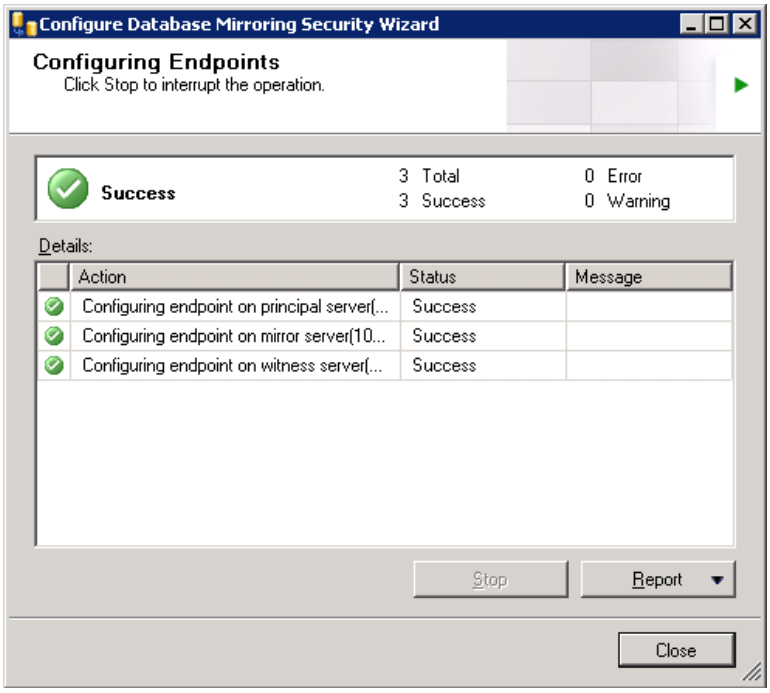


8. Press **Next**.



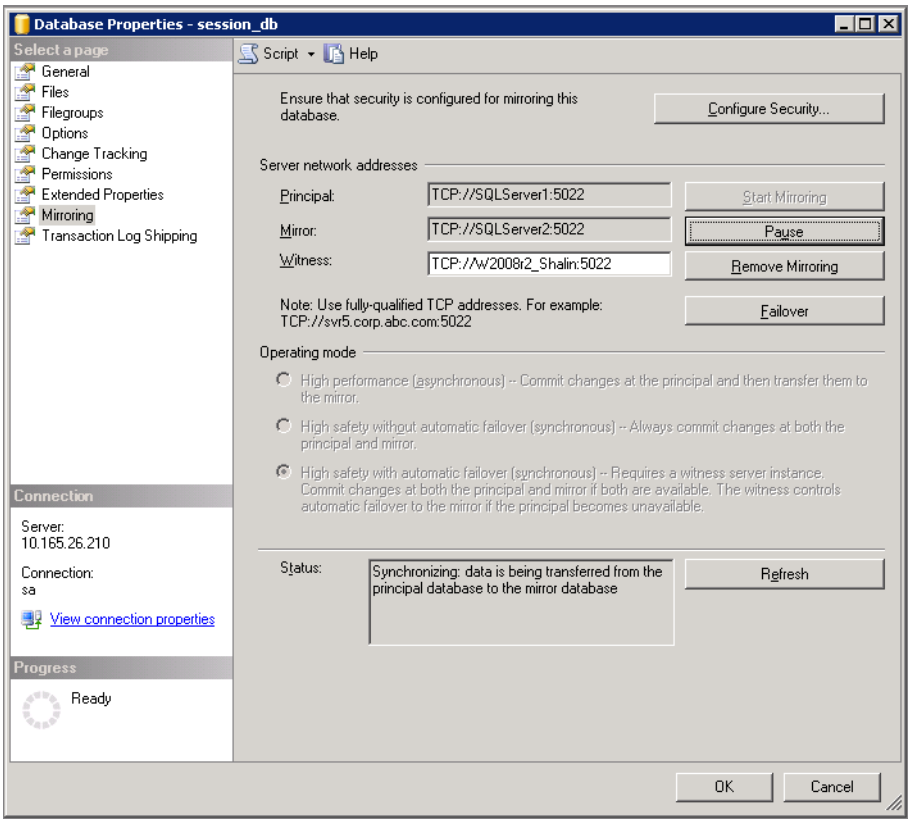
9. Press **Finish**.

The Configuring Endpoint screen displays the status of the configuration.

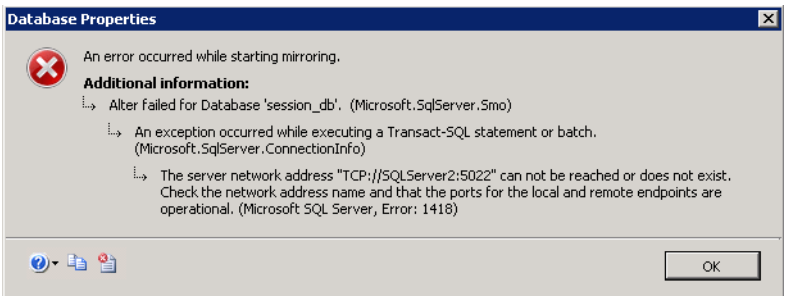


10. As long as the status indicates ‘Success’, press **Close**.
11. From the Database Properties screen, press **Start Mirroring**.

    Synchronisation progresses as per the status message.



If the following error message displays:



1. Backup and restore transactional logs from Principal to Mirror instance.
2. Try changing the user account running SQL Server and Server agent to **Administrator** and running the wizard again.

To add a user as SQL admin, run the following commands in an SQL Query window and press **F5**:

```
CREATE LOGIN [SQLServer1\Administrator] FROM WINDOWS

GO

exec sp_addsrvrolemember @loginname='SQLServer1\Administrator',
@rolename= 'sysadmin'

GO
```


2.3 Transformer Configuration

2.3.1 Transformer Web Server

Each HTTP Transformer has a **web.config** file. This file contains the logon credential for the user management database so that the SAM HTTP Transformer web application can access and authenticate users trying to logon.

1. Go to **DLL_Data\Quantel\QCIFSBin\web.config** and find the following XML:

```
<!-- For connecting to SQL server (SQL required for user man-
agement system) -->

<connectionStrings>

    <remove name="LocalSqlServer"/>

         <add name="LocalSqlServer" connectionString="Data
Source=10.165.250.251;Initial Catalog=session_db;User
ID=sa;Password=0sql0;Failover Partner=10.165.250.252" provider-
Name="System.Data.SqlClient"/>

</connectionStrings>
```

2. Edit the **Data Source** parameter to point at the correct IP address of the SQL Server, set the password to be **0Sam0@1Sam1**

2.3.1.1 Configure Non-resilient Database

1. Delete the **failover partner** tag and the preceding semi-colon as there is no failover server:

```
;Failover Partner=10.165.250.252
```

2. Resulting in:

```
...

   <add name="LocalSqlServer" connectionString="Data
Source=10.165.250.251;Initial Catalog=session_db;User
ID=sa;Password=0sql0; providerName="System.Data.SqlClient"/>

...
```

3. Save and close the file.
4. Restart the HTTP Transformer.

This configuration must occur on each HTTP Transformer instance. This includes any VMs that may be offline during configuration; run everything up during configuration.

2.3.1.2 Configure Resilient Database

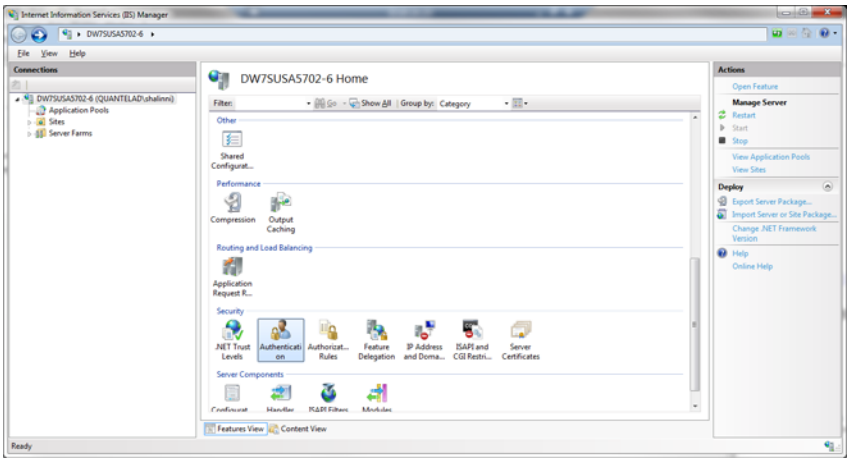
1. Edit **Failover partner** IP address to point to the newly setup failover server:

```
...

   <add name="LocalSqlServer" connectionString="Data
Source=10.165.250.251;Initial Catalog=session_db;User
ID=sa;Password=0sql0;Failover Partner=10.165.250.252" provider-
Name="System.Data.SqlClient"/>

...
```

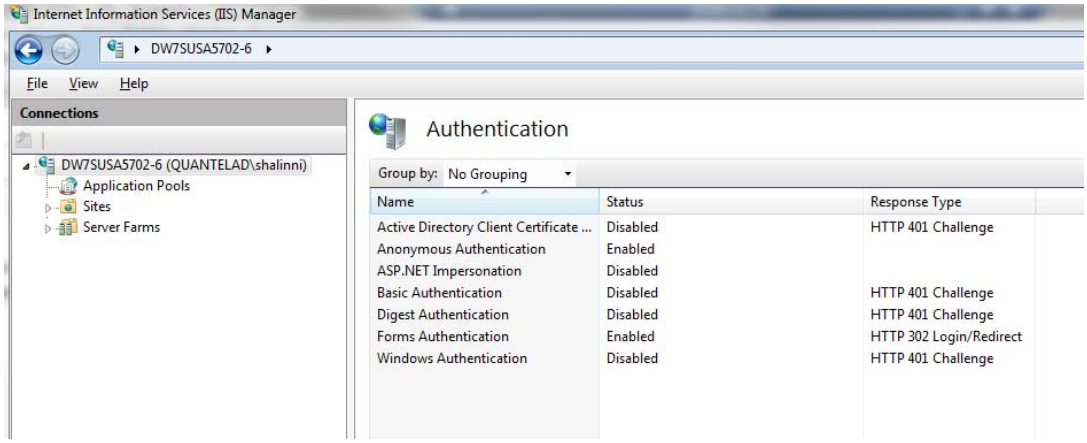
2. Save and close the file.
3. Restart the HTTP Transformer.

2.3.2 Configure Authentication in IIS

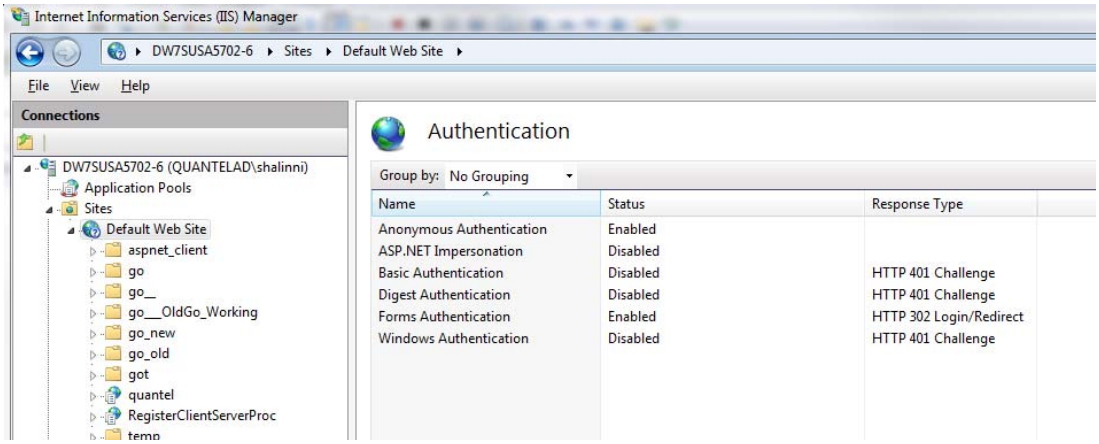
1. Open **Internet Information Services (IIS) Manager**.
2. Select **Authentication**.



3. Enable **Anonymous** and **Forms** authentication.



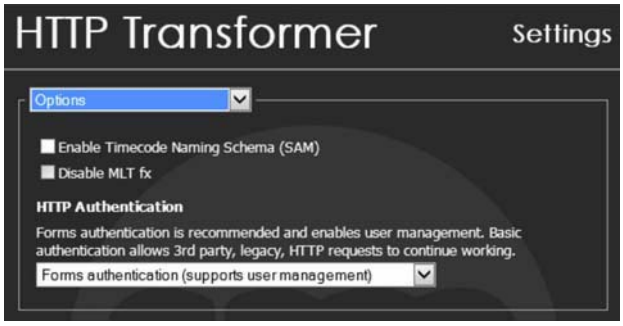
4. Select **Sites > Default Web Site** and enable the **Anonymous** and **Forms** authentication there too.



5. Restart IIS.
6. Run HTTP Transformer software.

2.3.3 Desktop Settings Application

In the **Options** section ensure the **Forms authentication - support user management** is selected:



This must be done on every HTTP Transformer instance. This includes any VMs that may be offline during configuration; run everything up during configuration.

2.3.4 Add CALs

Once the Microsoft SQL database engine and User Management is installed, CALs needs to be added to enable users to logon.

At least one CAL Key must be added to the system. This is 1 kB of encrypted text that contains:

- The number of CALs purchases in that order
- The system name
- System time zone
- A 'valid from' start date and time for the CALs
- A expiry date and time for the CALs
- IP address of the User management system
- CAL version, currently at v3

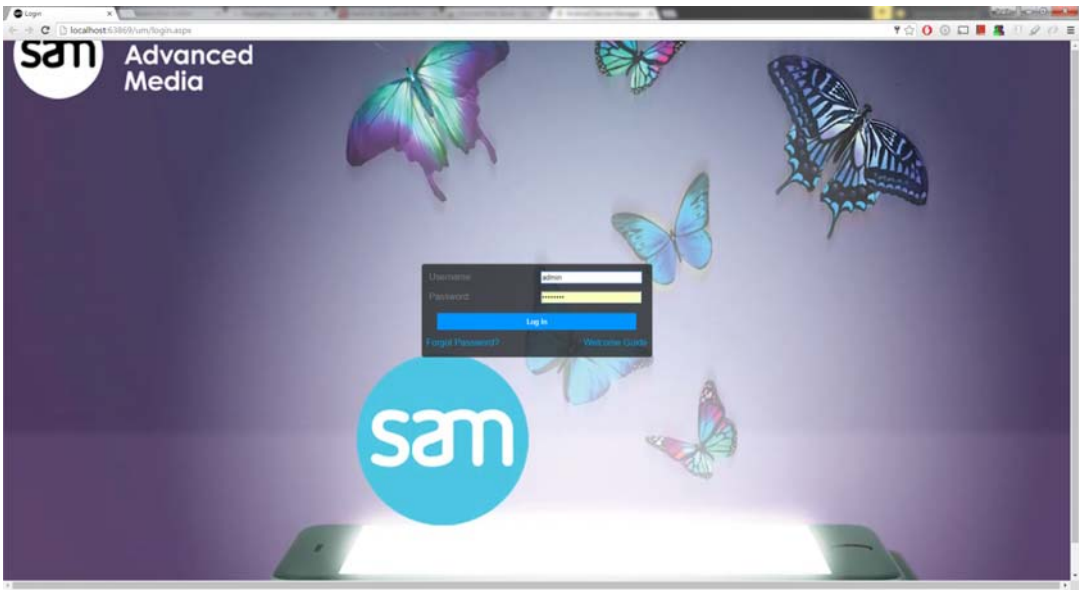
1. These details are entered into **TransformerGenerator.exe** tool at SAM, available to Support, Project or Sales Admin.
2. The tool creates the 1Kb CAL Key that can be emailed to the customer.
3. The customer logs on to User management and goes to the License dashboard where they can enter the CAL Key.
4. If accepted, The CALs are live and that number of user can log on concurrently.

Multiple CAL Keys can be added and run concurrently adding to the cluster total.

CALs are automatically removed from the cluster total when they expire.

2.4 Verify Installation

From a browser window navigate to **http://<TRANSFORMERIP>/quantel/um/** to display the following page:



Log in with the following credentials:

Username	admin
Password	quantel@

Navigate to the **License** task to see the correct number of CALS purchased: