GO! REMOTE PRODUCTION SUITE

REMOTE USER MANAGEMENT

Installation Guide

Issue 2 Revision 1

2018-10-22

www.grassvalley.com

Copyright and Trademark Notice

Terms and Conditions

Please read the following terms and conditions carefully. By using Go! documentation, you agree to the following terms and conditions.

Grass Valley hereby grants permission and license to owners of Go! to use their product manuals for their own internal business use. Manuals for Grass Valley products may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose unless specifically authorized in writing by Grass Valley.

A Grass Valley manual may have been revised to reflect changes made to the product during its manufacturing life. Thus, different versions of a manual may exist for any given product. Care should be taken to ensure that one obtains the proper manual version for a specific product serial number.

Information in this document is subject to change without notice and does not represent a commitment on the part of Grass Valley.

Warranty information is available from the Legal Terms and Conditions section of Grass Valley's website (www.grassvalley.com).

Title	Go! Remote Production Suite Installation Guide
Part Number	Issue 2 Revision 1
Revision	2018-10-22, 14:00

Table of Contents

1 Overview

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 login of users, and the tasks and roles accessible to different levels of users.

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

Pre-requisites

Microsoft SQL Server

An installation of Microsoft SQL Server Standard or Express 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 Grass Valley 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 Grass Valley 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

Media 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 Media Transformer are correctly licensed as has been the case previously.

2 Installation and Configuration

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.

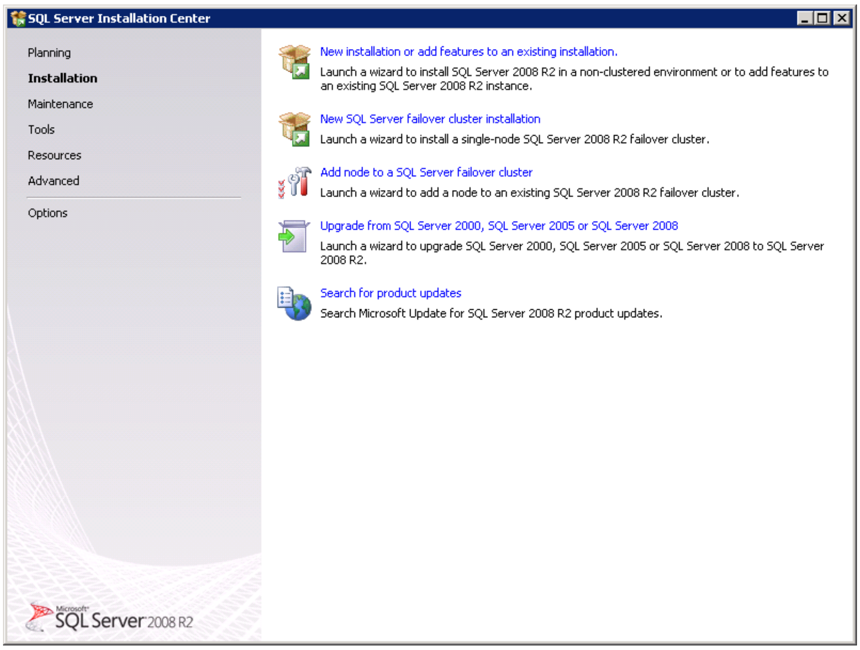
Install Microsoft SQL Server

Install MS SQL Server as follows:

1 Run **setup.exe**.

2 Select **Installation**.

3 Select **New installation or add features to an existing installation**.



New installation or add features to an existing installation.
Launch a wizard to install SQL Server 2008 R2 in a non-clustered environment or to add features to an existing SQL Server 2008 R2 instance.

New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2008 R2 failover cluster.

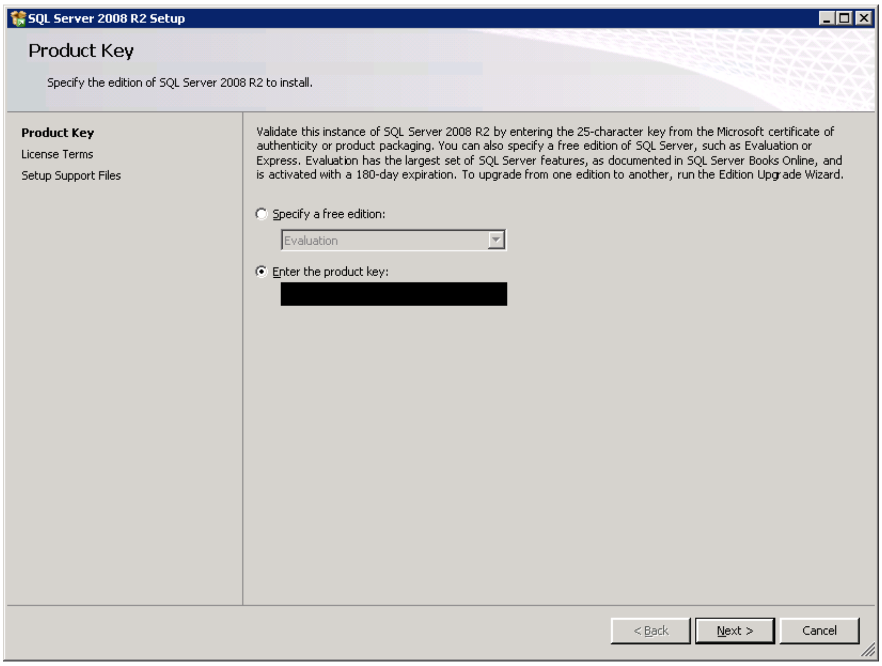
Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2008 R2 failover cluster.

Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008
Launch a wizard to upgrade SQL Server 2000, SQL Server 2005 or SQL Server 2008 to SQL Server 2008 R2.

Search for product updates
Search Microsoft Update for SQL Server 2008 R2 product updates.

Fig. 2-1: SQL Server Installation Center - Start Dialog

4 Enter the Product key or specify an Evaluation:



SQL Server 2008 R2 Setup

Product Key

Specify the edition of SQL Server 2008 R2 to install.

Validate this instance of SQL Server 2008 R2 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server, such as Evaluation or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. To upgrade from one edition to another, run the Edition Upgrade Wizard.

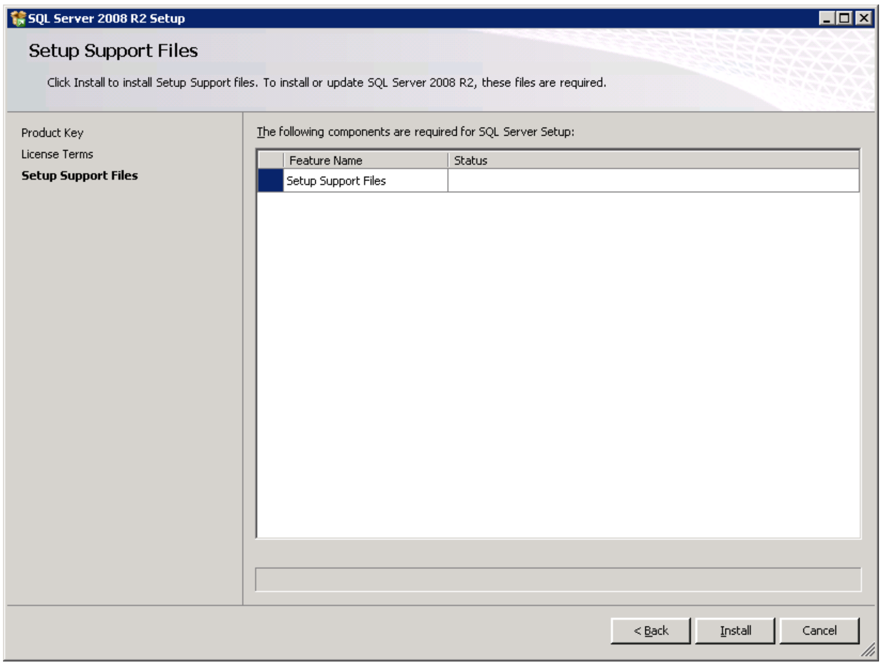
○ Specify a free edition: Evaluation

● Enter the product key: [redacted]

Fig. 2-2: SQL Server Installation Center - Product Key Validation

5 Press **Next** and accept terms.

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



SQL Server 2008 R2 Setup

Setup Support Files

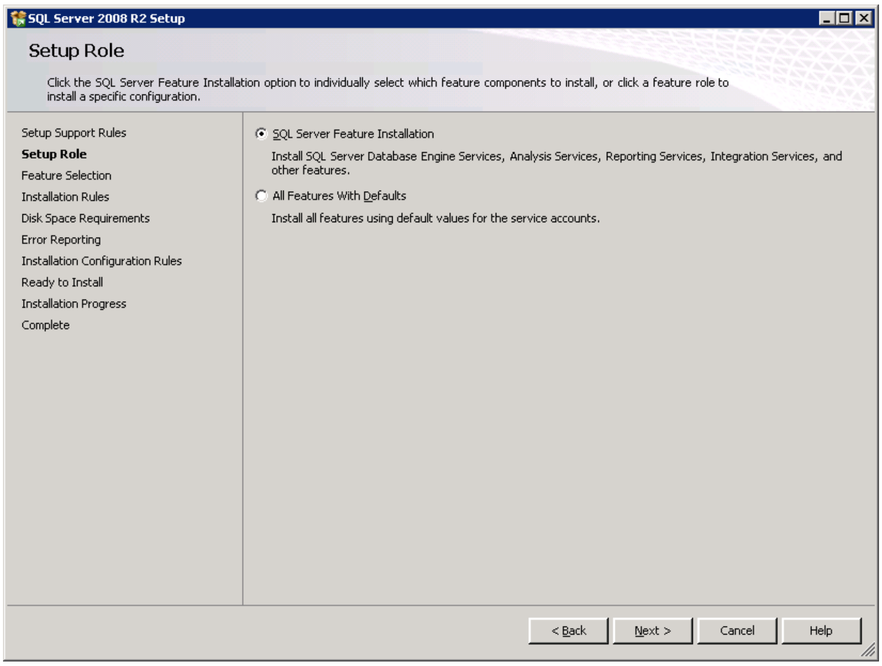
Click Install to install Setup Support files. To install or update SQL Server 2008 R2, these files are required.

The following components are required for SQL Server Setup:

Feature Name	Status
Setup Support Files	

Fig. 2-3: SQL Server Installation Center - Support File Setup

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



SQL Server 2008 R2 Setup

Setup Role

Click the SQL Server Feature Installation option to individually select which feature components to install, or click a feature role to install a specific configuration.

Setup Support Rules
Setup Role
Feature Selection
Installation Rules
Disk Space Requirements
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete

● SQL Server Feature Installation

Install SQL Server Database Engine Services, Analysis Services, Reporting Services, Integration Services, and other features.

○ All Features With Defaults

Install all features using default values for the service accounts.

Fig. 2-4: SQL Server Installation Center - Role Setup

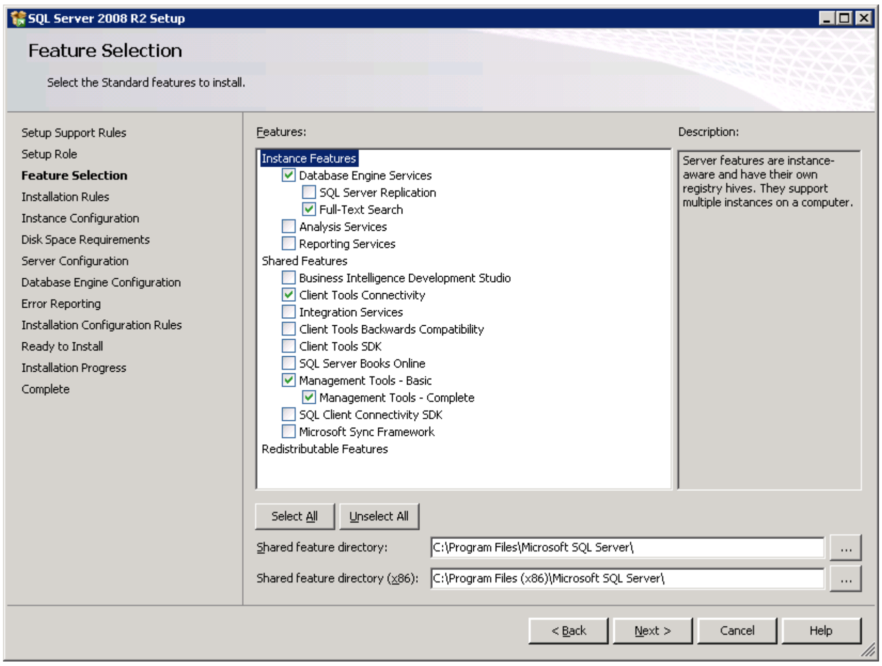
8 From Feature Selection, select the following:

Instance Features

- Database Engine Services
  - Full Text Search

Shared Features

- Client Tools Connectivity
- Management Tools
  - Management Tools Complete



SQL Server 2008 R2 Setup

Feature Selection

Select the Standard features to install.

Setup Support Rules
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete

Features:

Instance Features
- ☑ Database Engine Services
  - ☐ SQL Server Replication
  - ☑ Full-Text Search
- ☐ Analysis Services
- ☐ Reporting Services

Shared Features
- ☐ Business Intelligence Development Studio
- ☑ Client Tools Connectivity
- ☐ Integration Services
- ☐ Client Tools Backwards Compatibility
- ☐ Client Tools SDK
- ☐ SQL Server Books Online
- ☑ Management Tools - Basic
  - ☑ Management Tools - Complete
- ☐ SQL Client Connectivity SDK
- ☐ Microsoft Sync Framework

Redistributable Features

Description:

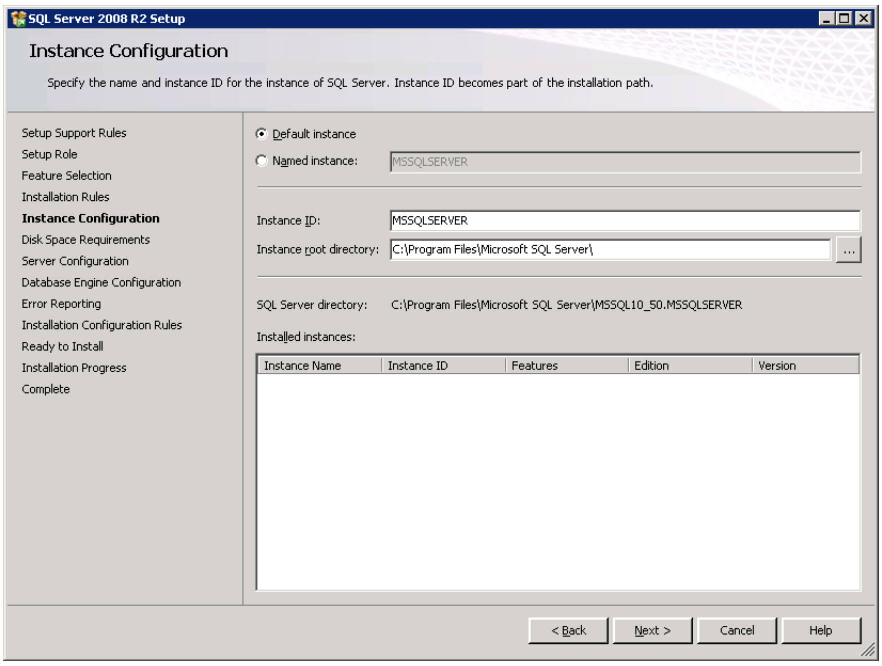
Server features are instance-aware and have their own registry hives. They support multiple instances on a computer.

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

Fig. 2-5: SQL Server Installation Center - Feature Selection

9 Press **Next**.



SQL Server 2008 R2 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

● Default instance

○ Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

Instance root directory: C:\Program Files\Microsoft SQL Server\

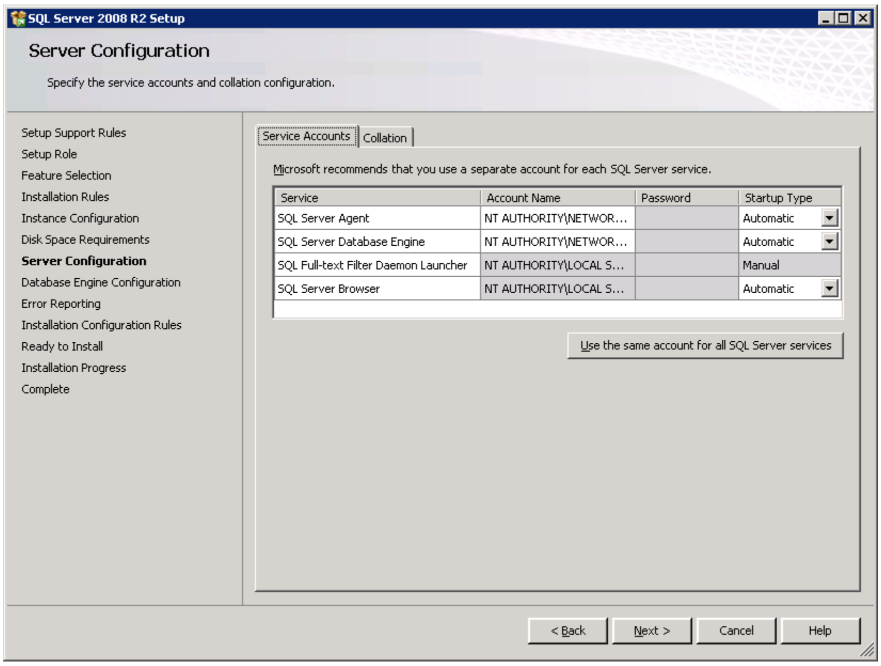
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

Fig. 2-6: SQL Server Installation Center - Instance Configuration

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



SQL Server 2008 R2 Setup

Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

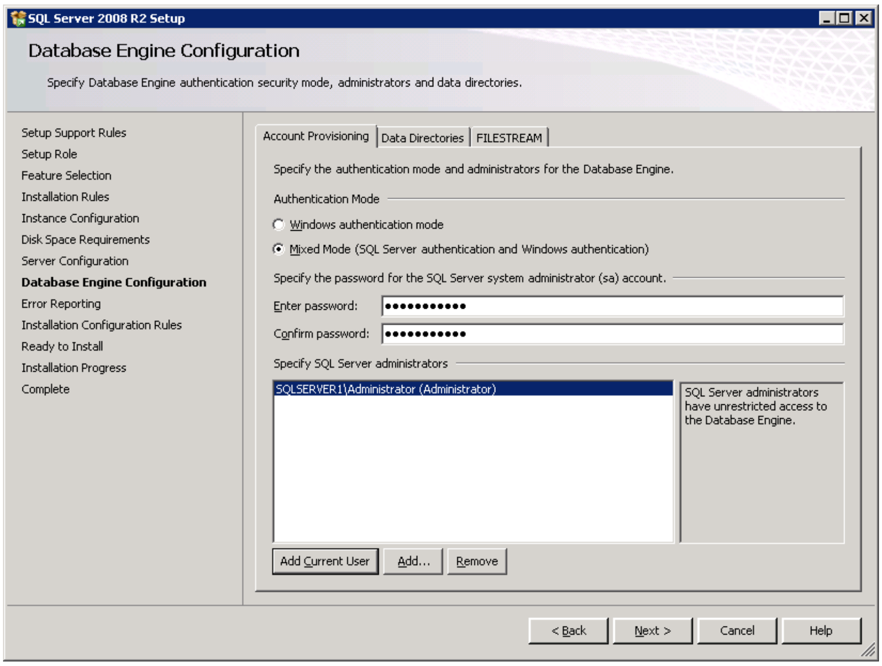
Service	Account Name	Password	Startup Type
SQL Server Agent	NT AUTHORITY\NETWOR...		Automatic
SQL Server Database Engine	NT AUTHORITY\NETWOR...		Automatic
SQL Full-text Filter Daemon Launcher	NT AUTHORITY\LOCAL S...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL S...		Automatic

Fig. 2-7: SQL Server Installation Center - Server Account Configuration

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**



SQL Server 2008 R2 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

Specify SQL Server administrators

SQLSERVER1\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

Fig. 2-8: SQL Server Installation Center - Database Engine Configuration

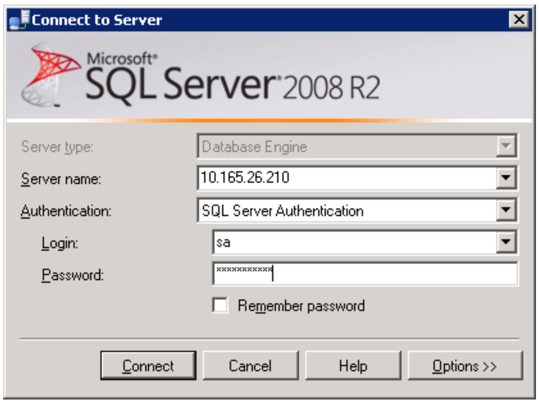
14 Press **Add Current User**.

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

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:

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



Connect to Server

Microsoft® SQL Server® 2008 R2

Server type: Database Engine

Server name: 10.165.26.210

Authentication: SQL Server Authentication

Login: sa

Password: ***********

□ Remember password

Fig. 2-9: SQL Server Login Dialog

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

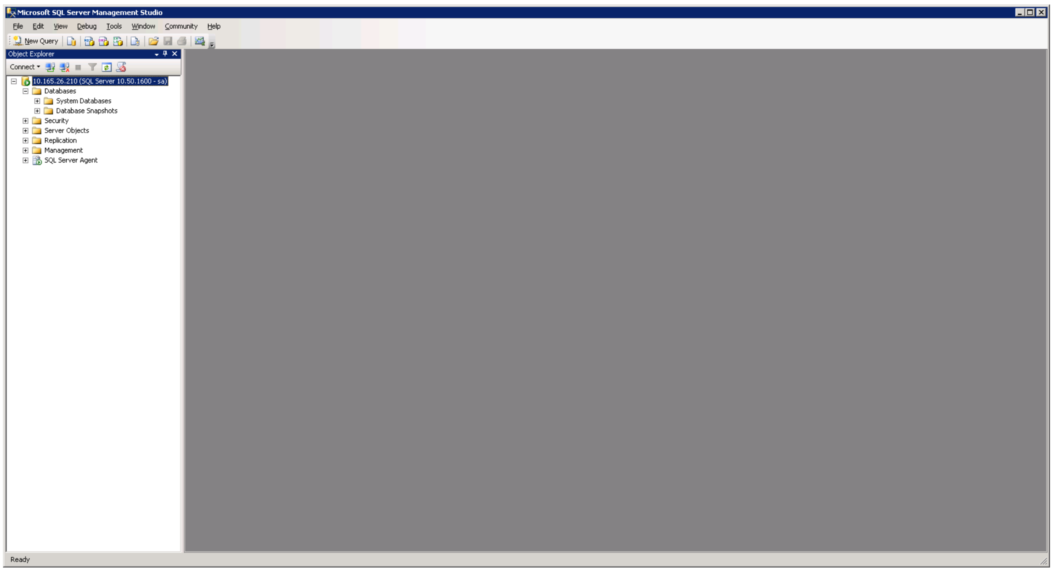


Fig. 2-10: SQL Server Management Studio

Run Scripts to Generate the Database

Before starting, request the **Go! Production Suite Database Setup Scripts** from Technical Support. These are included 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**.

Repeat the above steps for all 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:

Item	Details
Username	admin
Password	quantel@

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

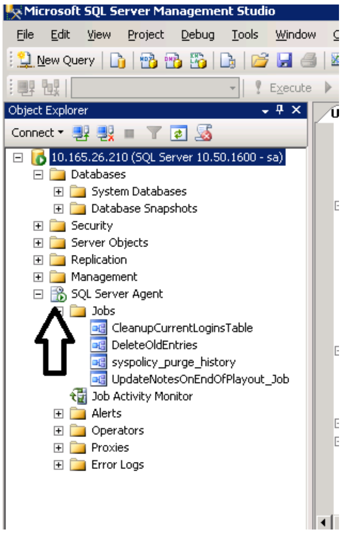


Fig. 2-11: SQL Server Management Studio Showing SQL Server Agent Running

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.

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**.

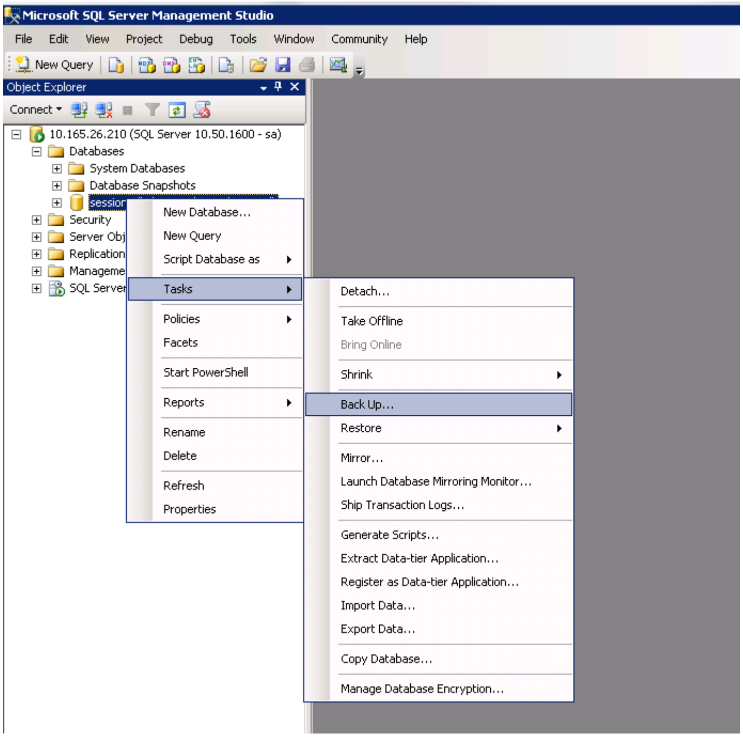
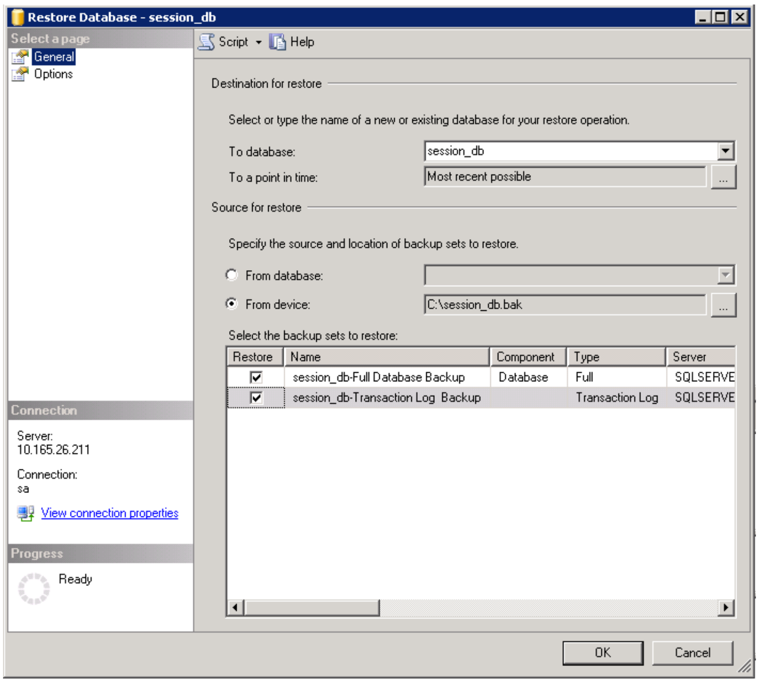


Fig. 2-12: SQL Server Management Studio - Backing up the Session Database

4 Copy the **.bak** file onto 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.



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: session_db

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

○ From database:

● From device: C:\session_db.bak

Select the backup sets to restore:

Restore	Name	Component	Type	Server
☑	session_db-Full Database Backup	Database	Full	SQLSERVE
☑	session_db-Transaction Log Backup		Transaction Log	SQLSERVE

Connection

Server:
10.165.26.211

Connection:
sa

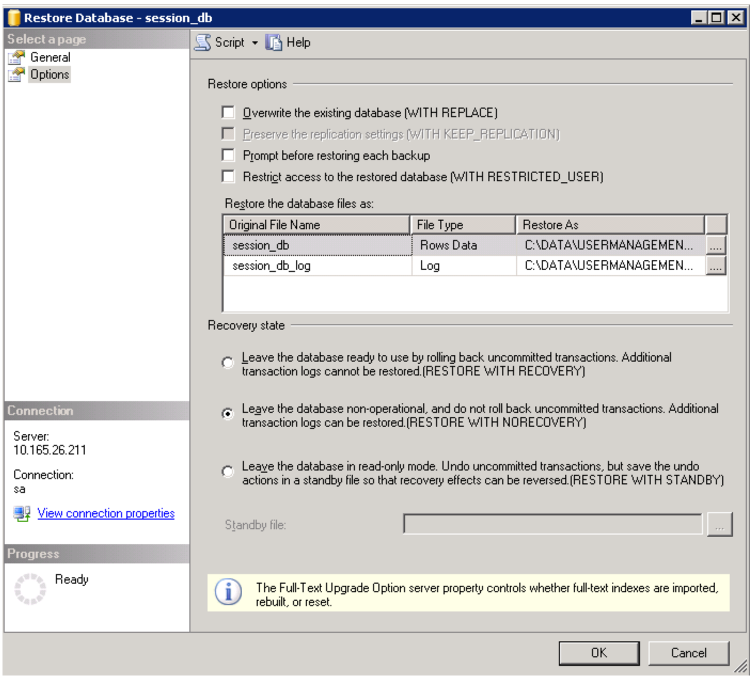
View connection properties

Progress

Ready

Fig. 2-13: SQL Server Management Studio - Restoring the Session Database

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



Restore options

□ Overwrite the existing database (WITH REPLACE)

□ Preserve the replication settings (WITH KEEP_REPLICATION)

□ Prompt before restoring each backup

□ Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As
session_db	Rows Data	C:\DATA\USERMANAGEMEN...
session_db_log	Log	C:\DATA\USERMANAGEMEN...

Recovery state

○ Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.(RESTORE WITH RECOVERY)

● Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored.(RESTORE WITH NORECOVERY)

○ Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reversed.(RESTORE WITH STANDBY)

Standby file:

Connection

Server:
10.165.26.211

Connection:
sa

View connection properties

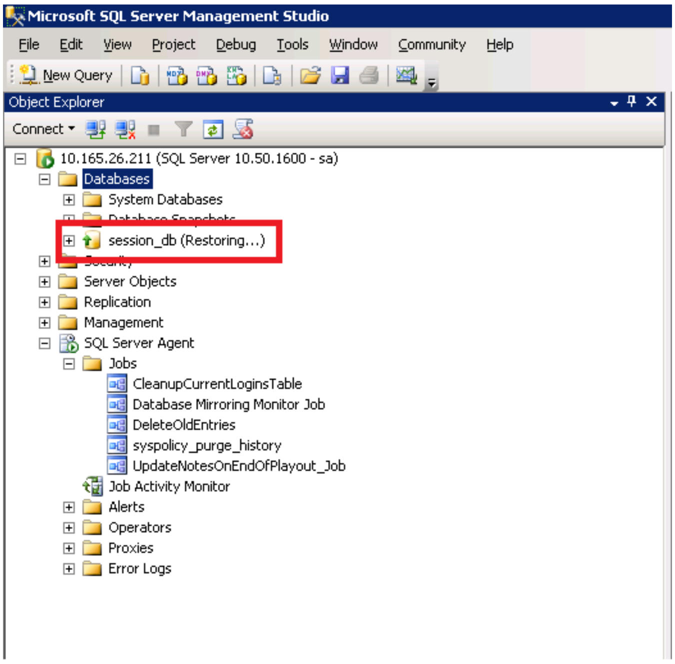
Progress

Ready

The Full-Text Upgrade Option server property controls whether full-text indexes are imported, rebuilt, or reset.

Fig. 2-14: SQL Server Management Studio - Setting Restore Options

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



10.165.26.211 (SQL Server 10.50.1600 - sa)
Databases
System Databases
Database Snapshots
session_db (Restoring...)
Security
Server Objects
Replication
Management
SQL Server Agent
Jobs
CleanupCurrentLoginsTable
Database Mirroring Monitor Job
DeleteOldEntries
syspolicy_purge_history
UpdateNotesOnEndOfPlayout_Job
Job Activity Monitor
Alerts
Operators
Proxies
Error Logs

Fig. 2-15: SQL Server Management Studio - Session Database Restored

As long as SQL Server is installed properly, witness does not require any manual configuration.

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.**

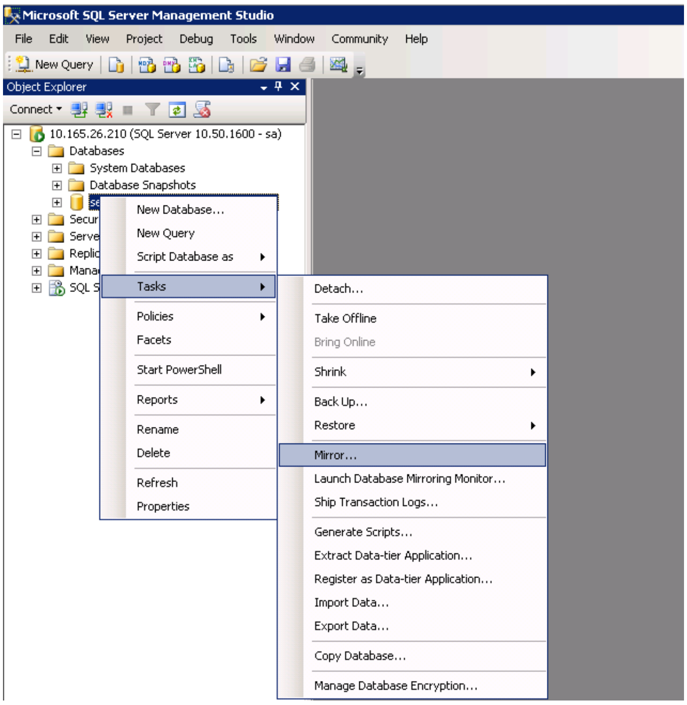
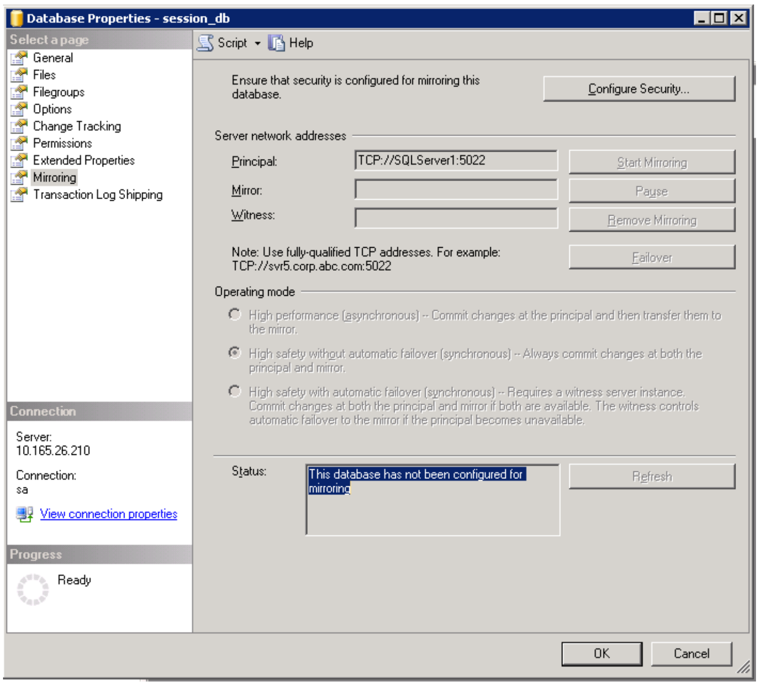


Fig. 2-16: SQL Server Management Studio - Session Database Restored

1. Select **Configure Security**.



Ensure that security is configured for mirroring this database.

Server network addresses

Principal: TCP://SQLServer1:5022

Mirror:

Witness:

Note: Use fully-qualified TCP addresses. For example: TCP://svr5.corp.abc.com:5022

Operating mode

○ High performance (asynchronous) -- Commit changes at the principal and then transfer them to the mirror.

● High safety without automatic failover (synchronous) -- Always commit changes at both the principal and mirror.

○ High safety with automatic failover (synchronous) -- Requires a witness server instance. Commit changes at both the principal and mirror if both are available. The witness controls automatic failover to the mirror if the principal becomes unavailable.

Status: This database has not been configured for mirroring

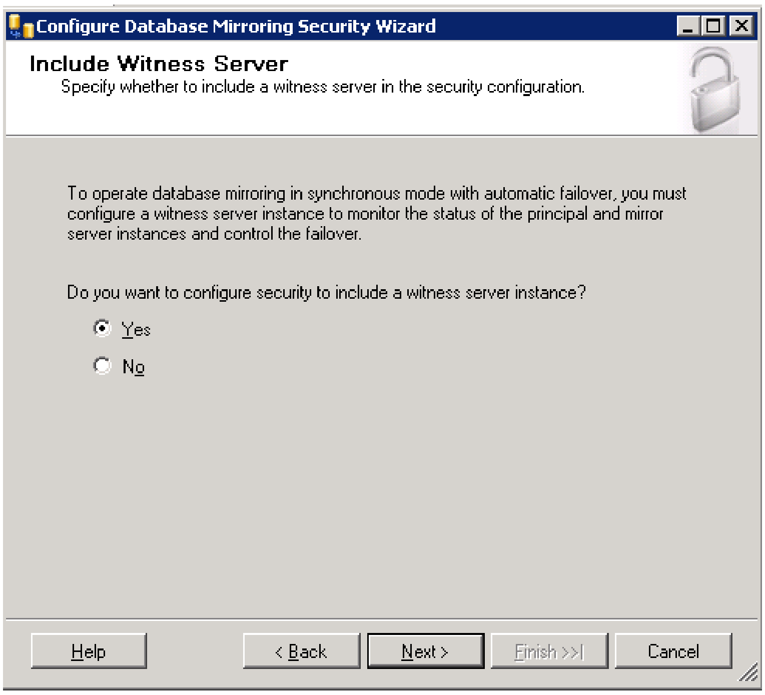
Server: 10.165.26.210

Connection: sa

Ready

Fig. 2-17: SQL Server Management Studio - Session Database Restored

2. Select the **Yes** radio button.



Configure Database Mirroring Security Wizard

Include Witness Server

Specify whether to include a witness server in the security configuration.

To operate database mirroring in synchronous mode with automatic failover, you must configure a witness server instance to monitor the status of the principal and mirror server instances and control the failover.

Do you want to configure security to include a witness server instance?

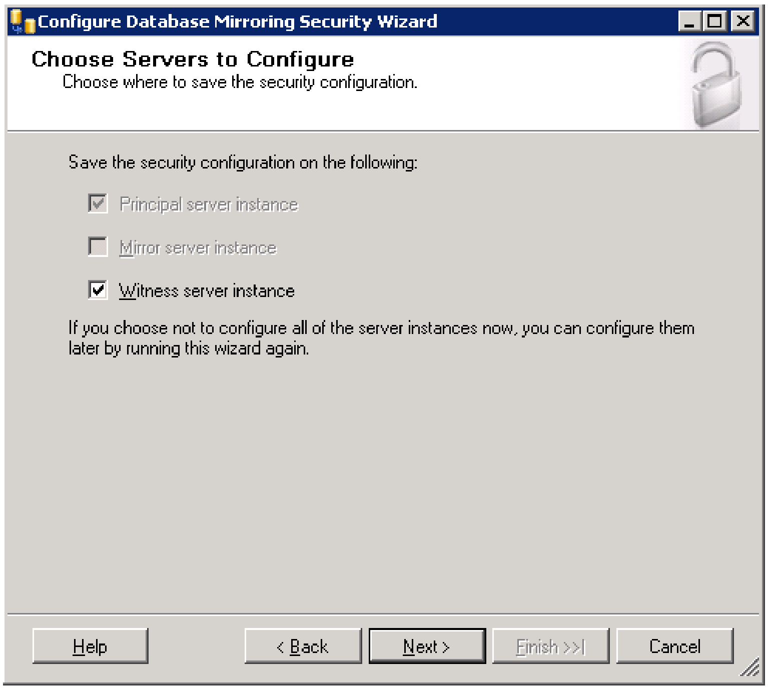
● Yes

○ No

Fig. 2-18: SQL Server Management Studio - Session Database Restored

2 Press **Next**.

3 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:

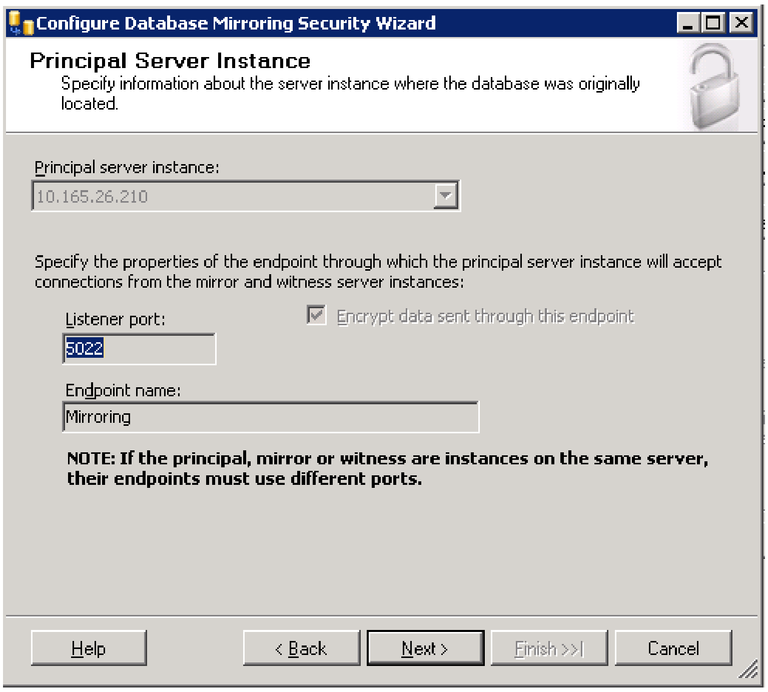
☑ Principal server instance

□ 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.

Fig. 2-19: SQL Server Management Studio - Session Database Restored



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:

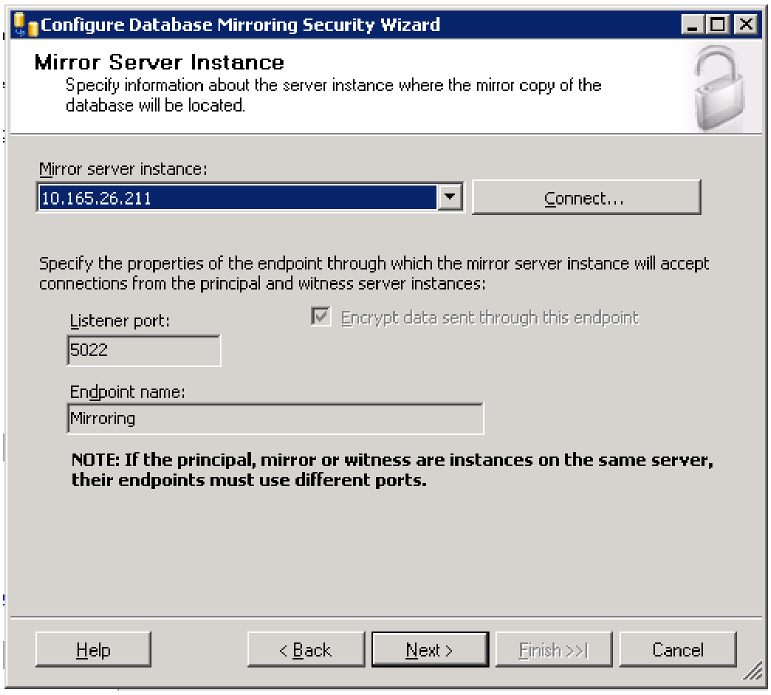
Listener port: 5022

☑ 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.

Fig. 2-20: SQL Server Management Studio - Session Database Restored



Mirror Server Instance

Specify information about the server instance where the mirror copy of the database will be located.

Mirror server instance: 10.165.26.211

Specify the properties of the endpoint through which the mirror server instance will accept connections from the principal and witness server instances:

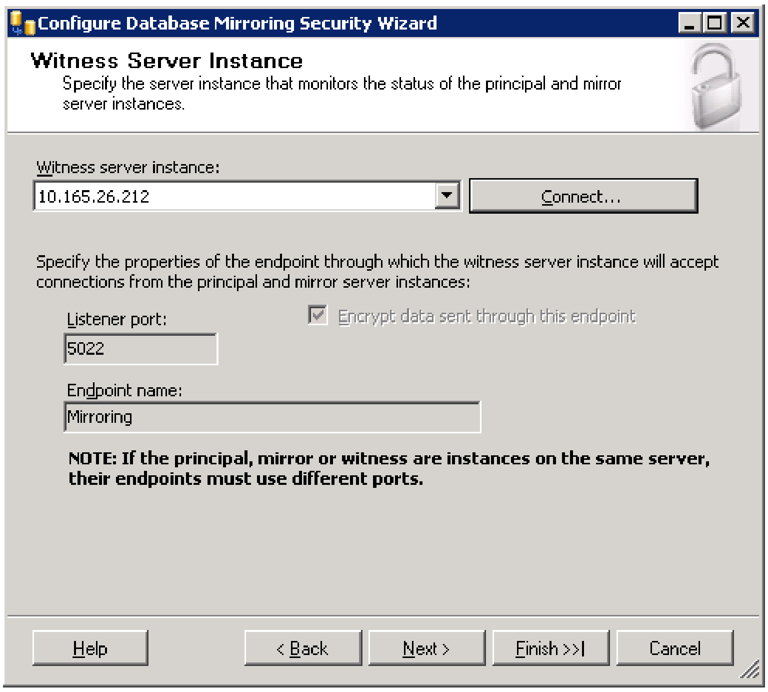
Listener port: 5022

☑ 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.

Fig. 2-21: SQL Server Management Studio - Session Database Restored



Configure Database Mirroring Security Wizard

Witness Server Instance

Specify the server instance that monitors the status of the principal and mirror server instances.

Witness server instance: 10.165.26.212

Specify the properties of the endpoint through which the witness server instance will accept connections from the principal and mirror server instances:

Listener port: 5022

☑ Encrypt data sent through this endpoint

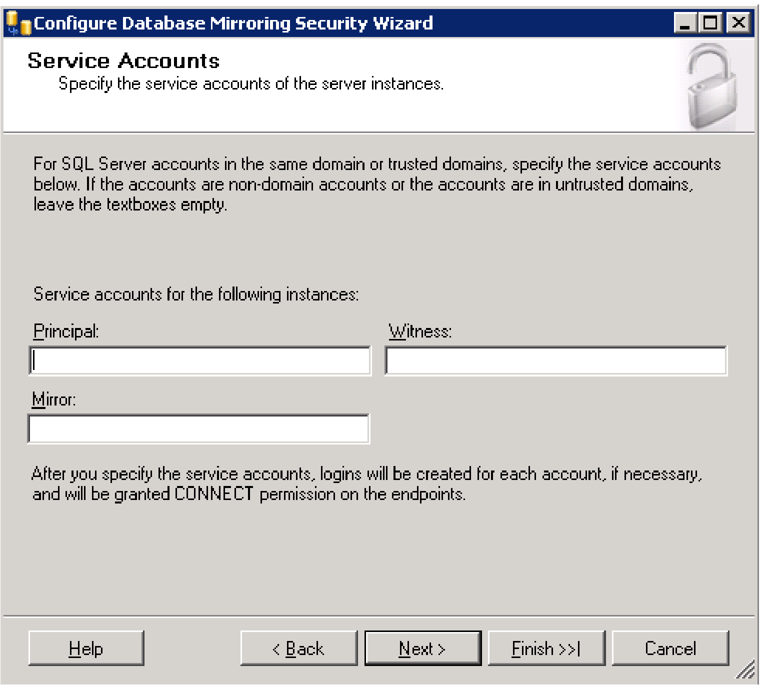
Endpoint name: Mirroring

NOTE: If the principal, mirror or witness are instances on the same server, their endpoints must use different ports.

Fig. 2-22: SQL Server Management Studio - Session Database Restored

4 Press **Finish**.

5 Leave the service accounts fields empty.



Configure Database Mirroring Security Wizard

Service Accounts

Specify the service accounts of the server instances.

For SQL Server accounts in the same domain or trusted domains, specify the service accounts below. If the accounts are non-domain accounts or the accounts are in untrusted domains, leave the textboxes empty.

Service accounts for the following instances:

Principal:

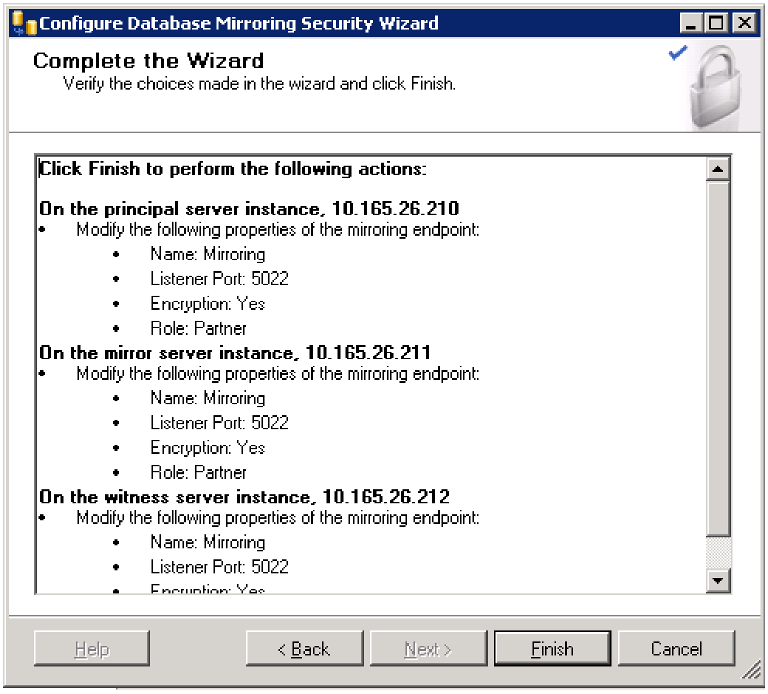
Witness:

Mirror:

After you specify the service accounts, logins will be created for each account, if necessary, and will be granted CONNECT permission on the endpoints.

Fig. 2-23: SQL Server Management Studio - Session Database Restored

6 Press **Next**.


Configure Database Mirroring Security Wizard
Complete the Wizard
Verify the choices made in the wizard and click Finish.

Click Finish to perform the following actions:

On the principal server instance, 10.165.26.210
- Modify the following properties of the mirroring endpoint:
  - Name: Mirroring
  - Listener Port: 5022
  - Encryption: Yes
  - Role: Partner

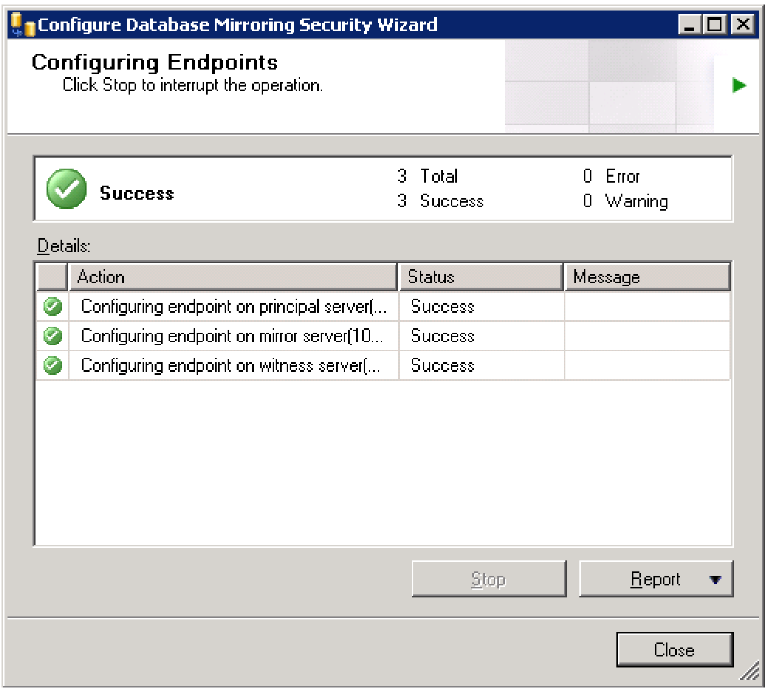
On the mirror server instance, 10.165.26.211
- Modify the following properties of the mirroring endpoint:
  - Name: Mirroring
  - Listener Port: 5022
  - Encryption: Yes
  - Role: Partner

On the witness server instance, 10.165.26.212
- Modify the following properties of the mirroring endpoint:
  - Name: Mirroring
  - Listener Port: 5022
  - Encryption: Yes

Fig. 2-24: SQL Server Management Studio - Session Database Restored

7 Press **Finish**.

The Configuring Endpoint screen displays the status of the configuration.


Configure Database Mirroring Security Wizard
Configuring Endpoints
Click Stop to interrupt the operation.

Success

3 Total
3 Success
0 Error
0 Warning

Details:

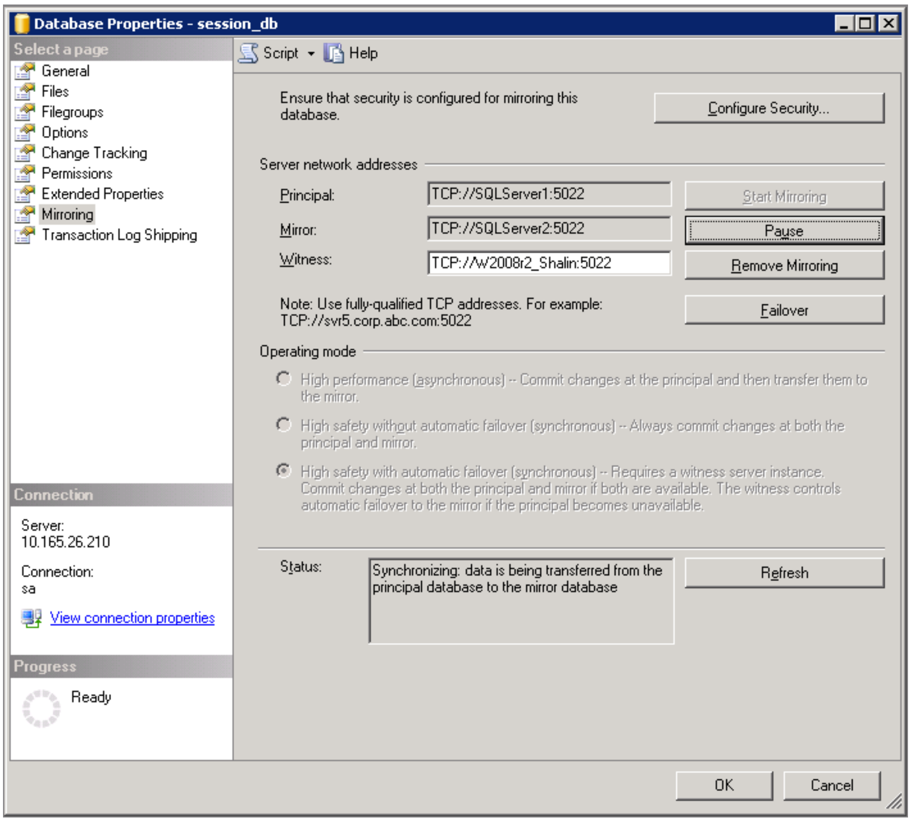
	Action	Status	Message
✓	Configuring endpoint on principal server(...	Success	
✓	Configuring endpoint on mirror server(10...	Success	
✓	Configuring endpoint on witness server(...	Success	

Fig. 2-25: SQL Server Management Studio - Session Database Restored

8 As long as the status indicates 'Success', press **Close**.

9 From the Database Properties screen, press **Start Mirroring**.

Synchronization progresses as shown by the status messages.



Ensure that security is configured for mirroring this database.

Server network addresses

Principal: TCP://SQLServer1:5022

Mirror: TCP://SQLServer2:5022

Witness: TCP://W2008r2_Shalin:5022

Note: Use fully-qualified TCP addresses. For example: TCP://svr5.corp.abc.com:5022

Operating mode

○ High performance (asynchronous) -- Commit changes at the principal and then transfer them to the mirror.

○ High safety without automatic failover (synchronous) -- Always commit changes at both the principal and mirror.

● High safety with automatic failover (synchronous) -- Requires a witness server instance. Commit changes at both the principal and mirror if both are available. The witness controls automatic failover to the mirror if the principal becomes unavailable.

Status: Synchronizing: data is being transferred from the principal database to the mirror database

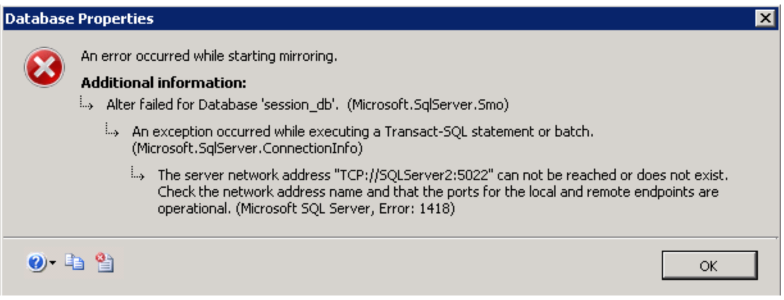
Server:
10.165.26.210

Connection:
sa

Fig. 2-26: SQL Server Management Studio - Session Database Restored

Managing Error Messages

If the following error message displays:



An error occurred while starting mirroring.

Additional information:

Alter failed for Database 'session_db'. (Microsoft.SqlServer.Smo)

An exception occurred while executing a Transact-SQL statement or batch. (Microsoft.SqlServer.ConnectionInfo)

The server network address "TCP://SQLServer2:5022" can not be reached or does not exist. Check the network address name and that the ports for the local and remote endpoints are operational. (Microsoft SQL Server, Error: 1418)

Fig. 2-27: SQL Server Management Studio - Session Database Restored

1 Backup and restore the 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**:

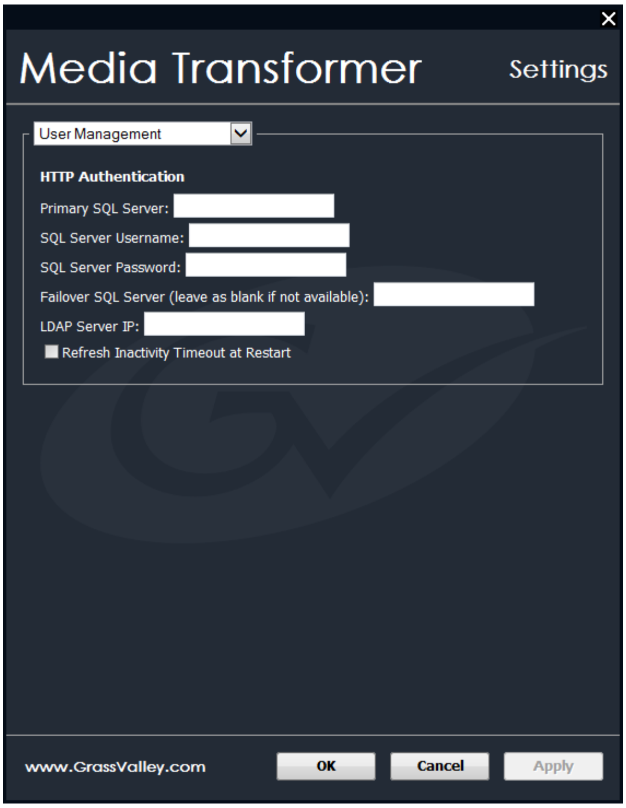
```
CREATE LOGIN [SQLServer1\Administrator] FROM WINDOWS
GO
exec sp_addsrvrolemember @loginname='SQLServer1\Administrator',
@rolename= 'sysadmin'
GO
```

Media Transformer Configuration

Media Transformer Web Server

Each Media Transformer is configured using the Settings menu accessed from the Windows Start menu, select:

Start > All Programs > Grass Valley > Media Transformer V7.3.0 Settings



HTTP Authentication

Primary SQL Server:

SQL Server Username:

SQL Server Password:

Failover SQL Server (leave as blank if not available):

LDAP Server IP:

□ Refresh Inactivity Timeout at Restart

Fig. 2-28: Media Transformer Settings Menu

Use the Settings menu to configure the following:

1 Set credentials for the user management database so that the GV Media Transformer web application can access and authenticate users trying to login.

2 Enter the correct IP address of the SQL Server and set the password to be **0Sam0@1Sam1**

3 Configure a non-resilient database by leaving the **Failover SQL Server** field blank.

4 Restart the Media Transformer after changing the Settings.

Note: Configure each instance of the Media Transformer, including any VMs that may be offline during configuration; run everything up during configuration.

Configure Authentication in IIS

Configure authentication in IIS as follows:

1 Open **Internet Information Services (IIS) Manager**.

2 Select **Authentication**.

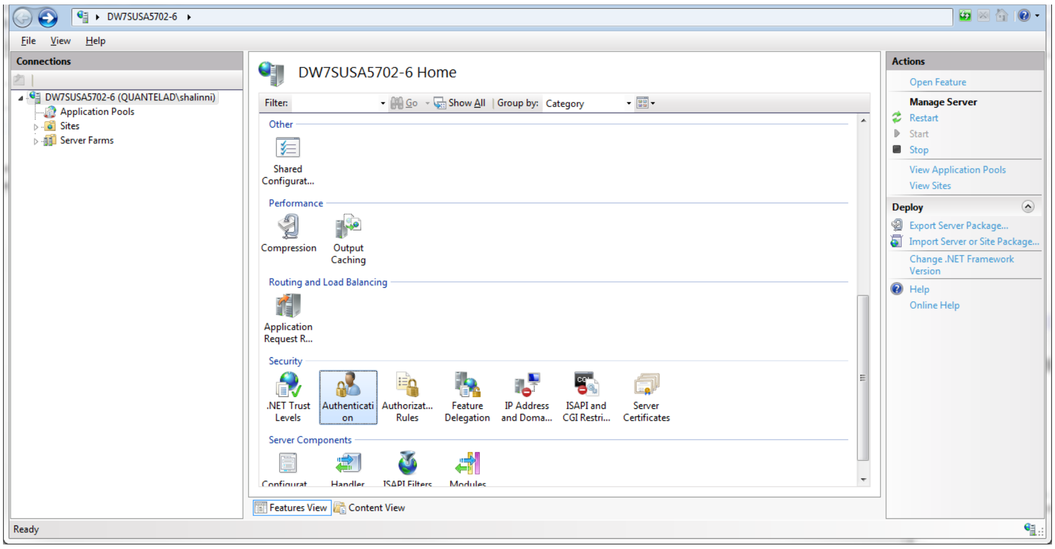
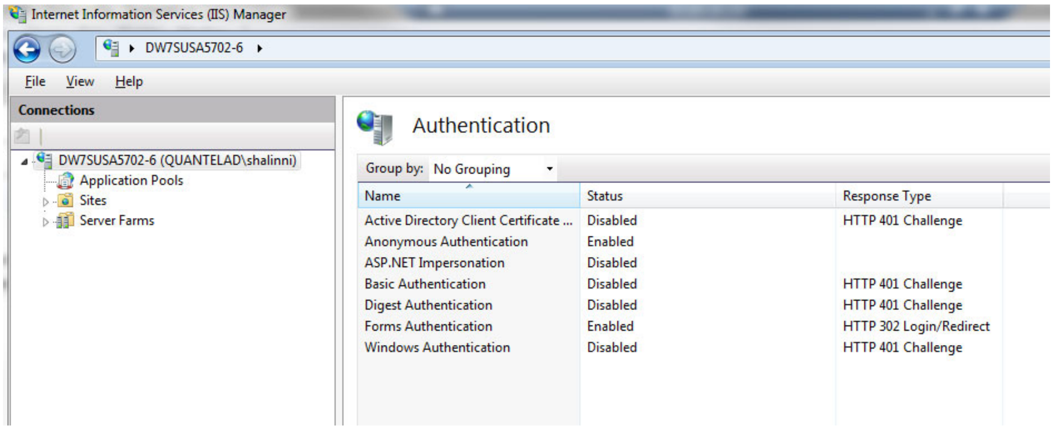


Fig. 2-29: Media Transformer Settings Menu

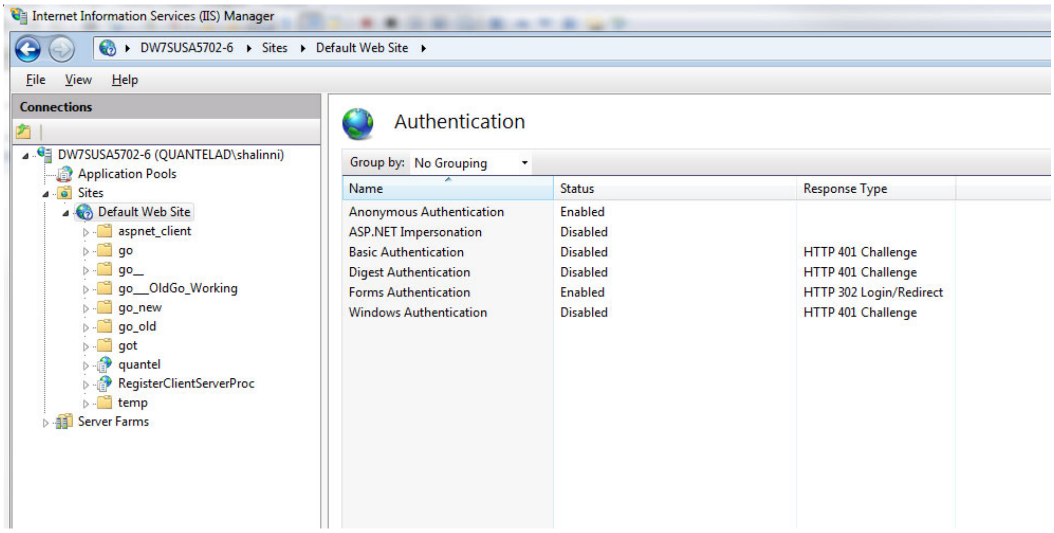
3 Enable **Anonymous** and **Forms** authentication.



Name	Status	Response Type
Active Directory Client Certificate ...	Disabled	HTTP 401 Challenge
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Enabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Fig. 2-30: IIS Manager Authentication Settings

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



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Enabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Fig. 2-31: IIS Manager Default Website Authentication Settings

5 Restart IIS.

6 Run Transformer software.

Disabling User Management

You can choose to disable the Go! user login authentication dialog by adding option **173** to your license.

Add Client Access Licenses (CALs)

Once the Microsoft SQL database engine and User Management is installed, you need to add CALs to enable users to login. At least one CAL Key must be added to the system. This is 1 kB of encrypted text that contains:

- Number of CALs purchased
- System name
- System time zone
- A **valid from** start date and time for the CALs
- An 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 Grass Valley, 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 users 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.

Verify the Installation

From a browser window navigate to http:**//<***Transformer_IP***>/GV/um/Default.aspx** to display the following page:

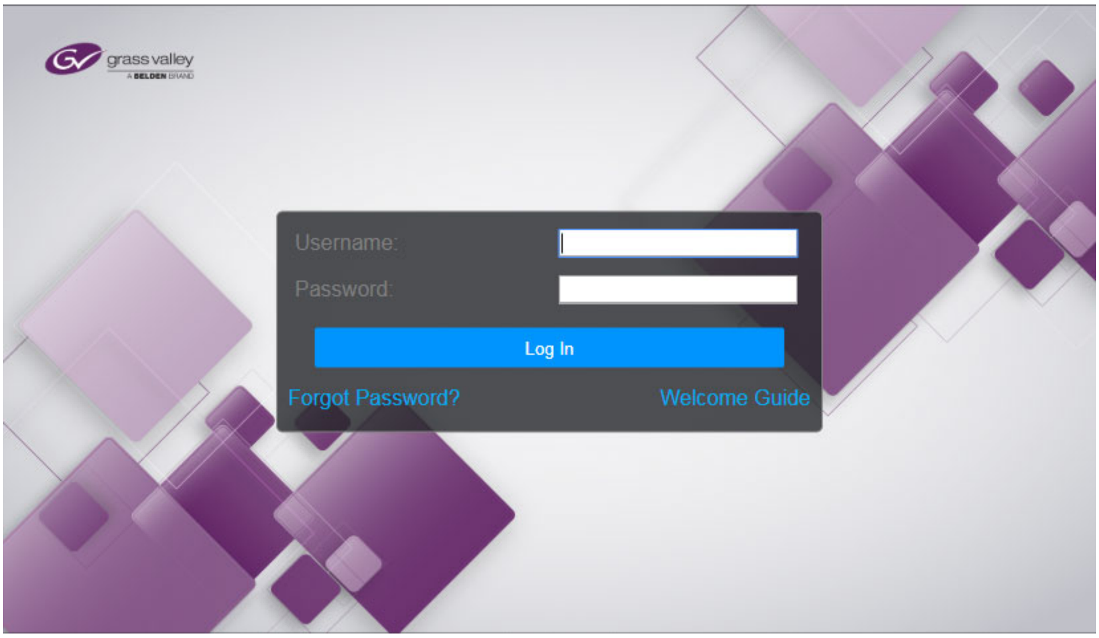
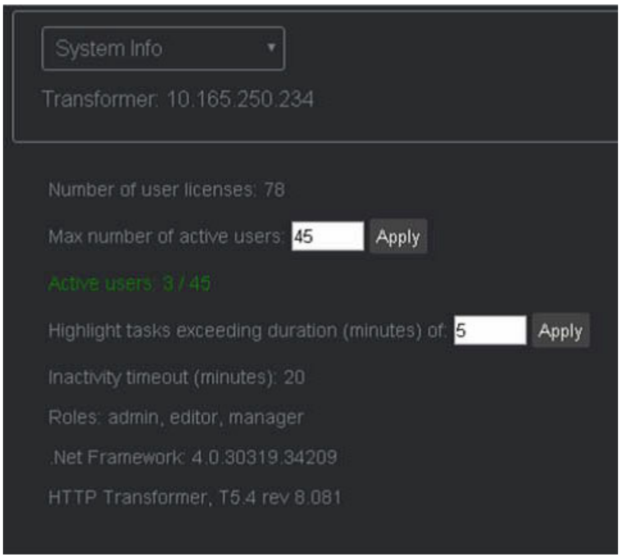


Fig. 2-32: Go! Login Screen

Log in with the following credentials:

Item	Details
Username	admin
Password	quantel@

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



Transformer: 10.165.250.234

Number of user licenses: 78

Max number of active users: 45

Active users: 3 / 45

Highlight tasks exceeding duration (minutes) of: 5

Inactivity timeout (minutes): 20

Roles: admin, editor, manager

.Net Framework: 4.0.30319.34209

HTTP Transformer, T5.4 rev 8.081

Fig. 2-33: Go! Licensing Screen

Anonymous Login in User Management

The anonymous login feature allows standard Go! Editor-level users to access Go! without needing to log in. When enabled, instead of encountering the login page, entitled users are immediately forwarded to Go! and other associated Editor-level pages. If a user attempts to access a Manager-level page (e.g., the Manager Dashboard) or Admin-level page (e.g., Admin Dashboard), then they will be required to login using their named Manager or Administrator account and password. Anonymous login applies only to Editor-level pages.

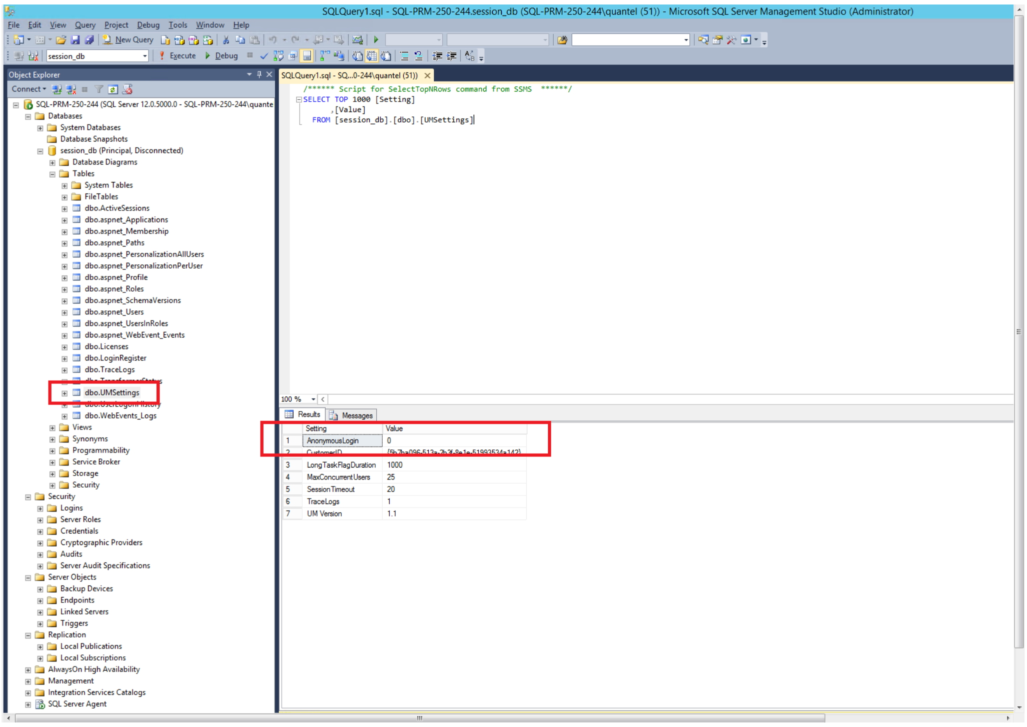
To enable Anonymous logins:

1 Log into the User Management MS-SQL database (session_db).

2 Go to the user management table **dbo.UMSettings**

3 Add a row **AnonymousLogin** with a value of **1**, see Figure 2-34.

If there is no entry for **AnonymousLogin** or if the value is **0**, then anonymous login is disabled.



```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [Setting]
      ,[Value]
  FROM [session_db].[dbo].[UMSettings]
```

	Setting	Value
1	AnonymousLogin	0
2	CustomerID	{5b7ba096-513a-2b3f-8e1e-51993534a142}
3	LongTaskFlagDuration	1000
4	MaxConcurrentUsers	25
5	SessionTimeout	20
6	TraceLogs	1
7	UM Version	1.1

Fig. 2-34: Enabling Anonymous Login in the Database

If named users have already been added to the system (e.g., AndrewSmith@xyz.com, DawnSmith@xyz.com, JohnSmith@xyz.com, etc.) anonymous login will detect the first available *offline* Editor-level user, and assign this login to the physical user.

Note: The person AndrewSmith may not be physically logged-in, but Go! UserManagement will use this account as it is currently unused.

If named users have not been pre-added, Go! UserManagement automatically generates the Editor-level users: anon-1, anon-2, anon-3, etc.

You can still track which pages Editors are visiting (using the Manager and Admin dashboards), however, the system is unable to connect physical users with their online personae.

Note: The UserManagement application polls the Go! MS SQL database for the AnonymousLogin setting only once, at start-up. If you later enable or disable AnonymousLogin in the database, restart UserManagement (by restarting the IIS Service) on all affected Windows computers (e.g., on each Media Transformer in the cluster.)

Control of Default Timeout Period

A new configurable timeout function allows the administrator either to define a period of inactivity after which a user session is timed-out, or to disable the session timeout completely.

A Go! session will currently timeout, by default, after a period of inactivity longer than 20 minutes.

To change the default 20 minute timeout on UserManagement, the system requires the following changes:

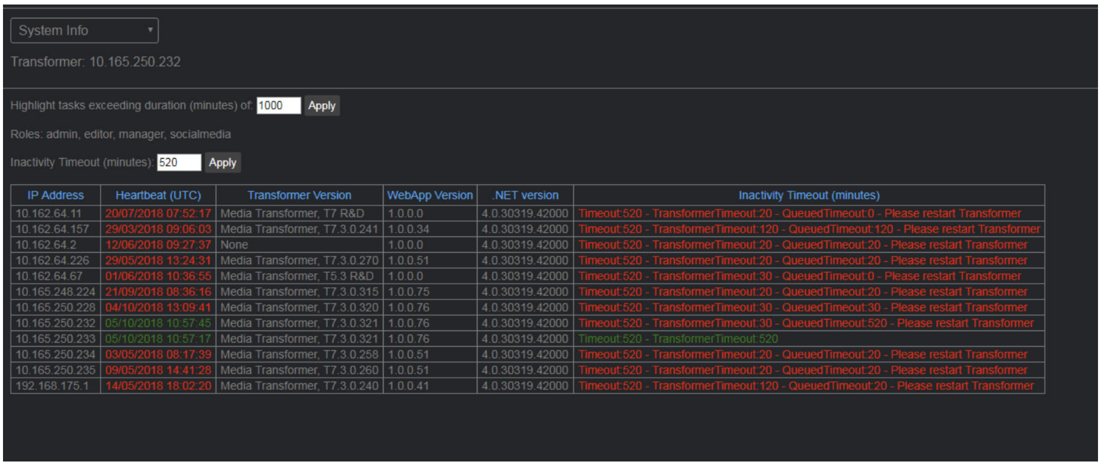
- Modify IIS web.config
- Edit the field **Idle Time-out (minutes)** for that application pool to change
- Restart IIS.

These changes need to be made for each Transformer in the cluster.

To set the timeout duration:

1 Log into the UserManagement console as Administrator.

2 Go to the **System Info** page, see Figure 2-35.



Transformer: 10.165.250.232

Highlight tasks exceeding duration (minutes) of: 1000 Apply

Roles: admin, editor, manager, socialmedia

Inactivity Timeout (minutes): 520 Apply

IP Address	Heartbeat (UTC)	Transformer Version	WebApp Version	.NET version	Inactivity Timeout (minutes)
10.162.64.11	20/07/2018 07:52:17	Media Transformer, T7 R&D	1.0.0.0	4.0.30319.42000	Timeout:520 - TransformerTimeout:20 - QueuedTimeout:0 - Please restart Transformer
10.162.64.157	29/03/2018 09:06:03	Media Transformer, T7.3.0.241	1.0.0.34	4.0.30319.42000	Timeout:520 - TransformerTimeout:120 - QueuedTimeout:120 - Please restart Transformer
10.162.64.2	12/06/2018 09:27:37	None	1.0.0.0	4.0.30319.42000	Timeout:520 - TransformerTimeout:20 - QueuedTimeout:20 - Please restart Transformer
10.162.64.226	29/05/2018 13:24:31	Media Transformer, T7.3.0.270	1.0.0.51	4.0.30319.42000	Timeout:520 - TransformerTimeout:20 - QueuedTimeout:20 - Please restart Transformer
10.162.64.67	01/06/2018 10:36:55	Media Transformer, T5.3 R&D	1.0.0.0	4.0.30319.42000	Timeout:520 - TransformerTimeout:30 - QueuedTimeout:0 - Please restart Transformer
10.165.248.224	21/09/2018 08:36:16	Media Transformer, T7.3.0.315	1.0.0.75	4.0.30319.42000	Timeout:520 - TransformerTimeout:20 - QueuedTimeout:20 - Please restart Transformer
10.165.250.228	04/10/2018 13:09:41	Media Transformer, T7.3.0.320	1.0.0.76	4.0.30319.42000	Timeout:520 - TransformerTimeout:30 - QueuedTimeout:30 - Please restart Transformer
10.165.250.232	05/10/2018 10:57:45	Media Transformer, T7.3.0.321	1.0.0.76	4.0.30319.42000	Timeout:520 - TransformerTimeout:30 - QueuedTimeout:520 - Please restart Transformer
10.165.250.233	05/10/2018 10:57:17	Media Transformer, T7.3.0.321	1.0.0.76	4.0.30319.42000	Timeout:520 - TransformerTimeout:520
10.165.250.234	03/05/2018 08:17:39	Media Transformer, T7.3.0.258	1.0.0.51	4.0.30319.42000	Timeout:520 - TransformerTimeout:20 - QueuedTimeout:20 - Please restart Transformer
10.165.250.235	09/05/2018 14:41:28	Media Transformer, T7.3.0.260	1.0.0.51	4.0.30319.42000	Timeout:520 - TransformerTimeout:20 - QueuedTimeout:20 - Please restart Transformer
192.168.175.1	14/05/2018 18:02:20	Media Transformer, T7.3.0.240	1.0.0.41	4.0.30319.42000	Timeout:520 - TransformerTimeout:120 - QueuedTimeout:20 - Please restart Transformer

Fig. 2-35: UserManagement System Info Screen

3 In the field **Inactivity Timeout (minutes)** set the value to the required timeout period, within the following limits:

- Minimum value: 5 minutes
- Maximum value: 10080 minutes (1 week)

4 Click **Apply**.

5 After applying the new timeout value, restart each Transformer in the cluster.

On restart, the Transformers detect the new timeout value and apply it to their **web.configs** and application pools.

Once the Transformer has been restarted and the new value has been applied, the column **Inactivity Timeout** in the table **SystemInfo**, should change color to green and display the message:

Timeout:50 - TransformerTimeout:50

If the Transformer is not restarted, the column **Inactivity Timeout** in the table **SystemInfo**, will display the following message in red:

Timeout: 50 - TransformerTimeout:20 - QueuedTimeout:50 - Please restart Transformer

Where:

- **Timeout: 50** shows the new timeout value which will be applied at restart
- **TransformerTimeout:20** shows the original timeout value to be removed at restart
- **QueuedTimeout:50** shows the new timeout value, currently queued for application.