SIEMENS

FAQ • 11/2015

How to Configure Microsoft SQL Server to Work with RUGGEDCOM CROSSBOW

RUGGEDCOM CROSSBOW

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.industry.siemens.com.

Table of Contents

1 Overview

There are many ways to configure Microsoft SQL Server to work with RUGGEDCOM CROSSBOW, depending on IT resources, the organization of a network, and the planned deployment topology for RUGGEDCOM CROSSBOW.

For example, a user may wish to install a dedicated copy of SQL Server on the same machine as the RUGGEDCOM CROSSBOW server. This is appropriate for single RUGGEDCOM CROSSBOW server installations without redundancy.

Alternatively, a user may wish to install (or may have already installed) a set of SQL Servers on separate machines, providing full redundancy via SQL Server mirroring. Although this topic is beyond the scope of this document, there is information about SQL Server readily available online from Microsoft and other sources.

The purpose of this document is to offer some tips and best practices, and provide basic information on issues directly related to the integration of RUGGEDCOM CROSSBOW and SQL Server.

2 Installing Microsoft SQL Server

In terms of its integration with SQL Server, there are generally two main cases typically encountered when installing the CROSSBOW Server: a simple, single-server installation, and a more complex multi-server installation.

The biggest difference between the two is the manner in which the RUGGEDCOM CROSSBOW server logs into or authenticates itself against the SQL Server. This is simple and straight-forward with a single server installation, but needs extra attention in a multi-server installation.

The RUGGEDCOM CROSSBOW server runs as a set of several services within the Windows operating system on the target machine. Services generally start when a machine is rebooted. Unlike interactive programs that a regular user runs on Windows, an actual user does not need to log into the server for the services to run. However, services do log themselves in when they start. The account they use to log in determines how they authenticate themselves to the operating system, and therefore what access they have to certain system resources, such as the SQL Server database.

By default, on initial installation, RUGGEDCOM CROSSBOW services are configured to run under the *Local System* account. If a single RUGGEDCOM CROSSBOW installation is planned, and the SQL Server instance for the RUGGEDCOM CROSSBOW server is also on the local machine, then this setting can be used with no difficulty.

However, if multiple servers will be used or separate servers for the SQL Server database, and most particularly if SQL Server database mirroring will be used, the *Local System* account should not be used. Instead, it is preferable to create a specific domain user solely for the purpose of running RUGGEDCOM CROSSBOW, and to configure the RUGGEDCOM CROSSBOW services to run as that user. This simplifies the RUGGEDCOM CROSSBOW server authentication against SQL Server databases across different machines. This domain user should be granted administrative rights to the server on which the RUGGEDCOM CROSSBOW server is installed, but does not need to be an administrative user on the SQL Server machine if that machine is separate from the RUGGEDCOM CROSSBOW server.

3 Authentication Under SQL Server

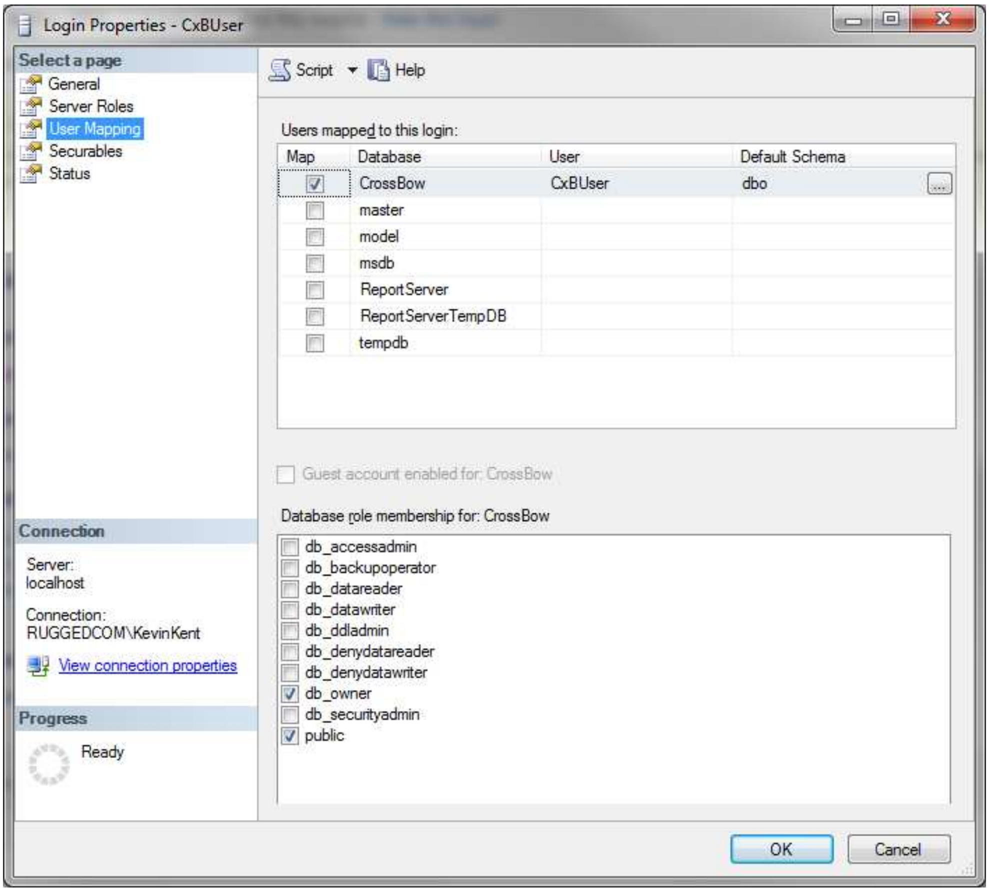
SQL Server supports two methods of authenticating users:

- *SQL Server Authentication*, which uses a basic username and password
- *Windows Authentication*, which is based on the credentials of the logged-in user who is accessing the database

When SQL Server is installed, the user is asked which method to support. RUGGEDCOM CROSSBOW can use either method, but *SQL Server Authentication* is only appropriate for simple, single-server installations. Use *Windows Authentication* for more complex scenarios preferable with a domain user.

The user chosen to access the RUGGEDCOM CROSSBOW database should be configured as the database owner (dbo). This db_owner role allows the user to perform the administration and maintenance tasks for a given database (e.g. updating fields, changing stored procedures, deleting tables, etc.), but all of those rights exist ONLY for that specific database. Figure 3-1 illustrates setting the db_owner role for a CROSSBOW user.

Figure 3-1: Login Properties -CxBUser



Users mapped to this login:

Map	Database	User	Default Schema
☑	CrossBow	CxBUser	dbo
☐	master		
☐	model		
☐	msdb		
☐	ReportServer		
☐	ReportServerTempDB		
☐	tempdb		

☐ Guest account enabled for: CrossBow

Database role membership for: CrossBow

☐ db_accessadmin
☐ db_backupoperator
☐ db_datareader
☐ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☑ db_owner
☐ db_securityadmin
☑ public

Server:
localhost

Connection:
RUGGEDCOM\KevinKent

View connection properties

Ready

4 Mirroring

The following are tips for setting up SQL Server mirroring for use with RUGGEDCOM CROSSBOW.

NOTE For detailed information about mirror configuration, refer to the Microsoft SQL Server documentation.

Mirroring using domain accounts:

- Make sure SQL Server services on the mirrors are configured to log on with domain accounts, as opposed to running as the local machine account.
- Make sure RUGGEDCOM CROSSBOW Services are configured to log on with domain accounts, as opposed to running as the local machine account.
- Make sure to take a full backup of the Principal database and a Transaction Log Backup of the Principal database.
- Restore the full backup with the **NO RECOVERY** option, then restore the transaction log.
- The mirror database must be in the RESTORING state for mirroring to work. When preparing a mirror database, use **RESTORE WITH NORECOVERY** for every restore operation. Minimally, use **RESTORE WITH NORECOVERY** when creating a full backup of the principal database, followed by all subsequent log backups.
- If a mirrored database is stuck in the RESTORING state and cannot be deleted, run the following SQL statement against the RUGGEDCOM CROSSBOW database:

  ```
  RESTORE DATABASE CROSSBOW WITH RECOVERY
  ```

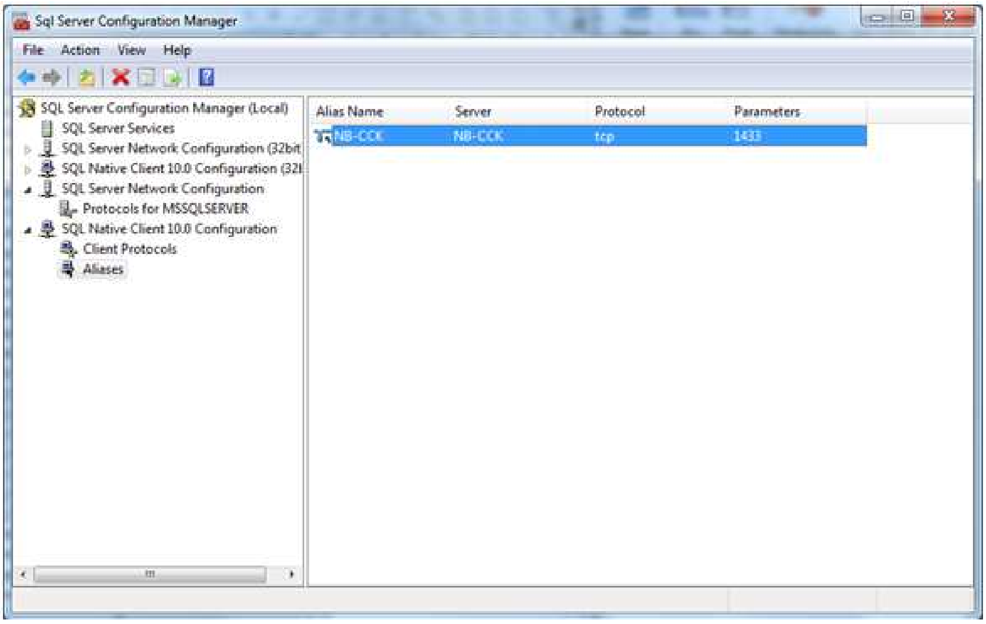
  This will switch the mirror database back to a normal state, which can be deleted.
- If a mirrored database is stuck in the RECOVERY state and cannot be deleted, run the following SQL statement against the RUGGEDCOM CROSSBOW database:

  ```
  ALTER DATABASE CROSSBOW SET PARTNER OFF
  ```

Other things to do if there are connectivity issues between the SQL primary and mirror:

- Create an Alias on each of the SQL servers representing the partner machine. Figure 4-1 illustrates an Alias (NB-CCK) of a mirror on the primary instance. The properties of the Alias are illustrated in Figure 4-2.

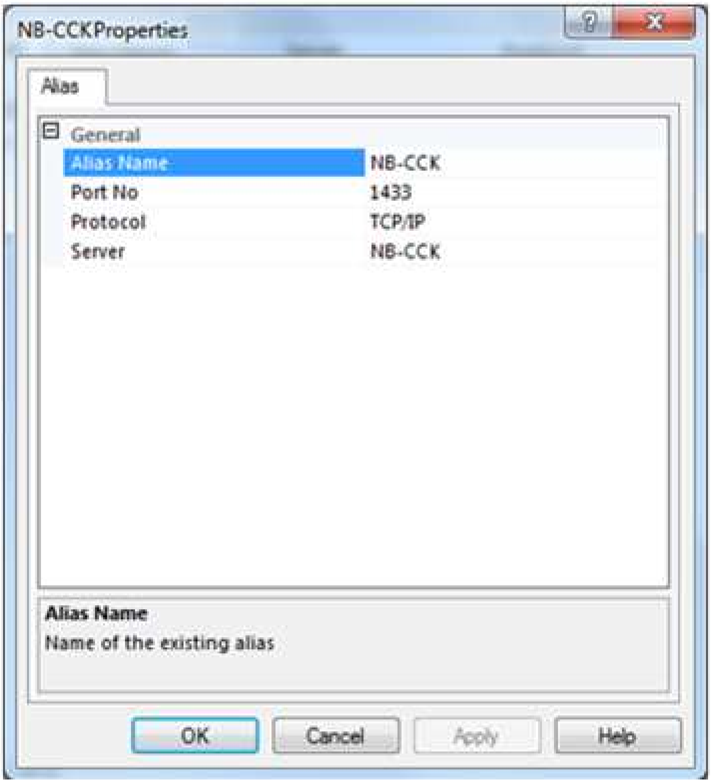
Figure 4-1: SQL Server Configuration Manager



- SQL Server Configuration Manager (Local)
  - SQL Server Services
  - SQL Server Network Configuration (32bit
  - SQL Native Client 10.0 Configuration (32l
  - SQL Server Network Configuration
    - Protocols for MSSQLSERVER
  - SQL Native Client 10.0 Configuration
    - Client Protocols
    - Aliases

Alias Name	Server	Protocol	Parameters
NB-CCK	NB-CCK	tcp	1433

Figure 4-2: Alias Properties



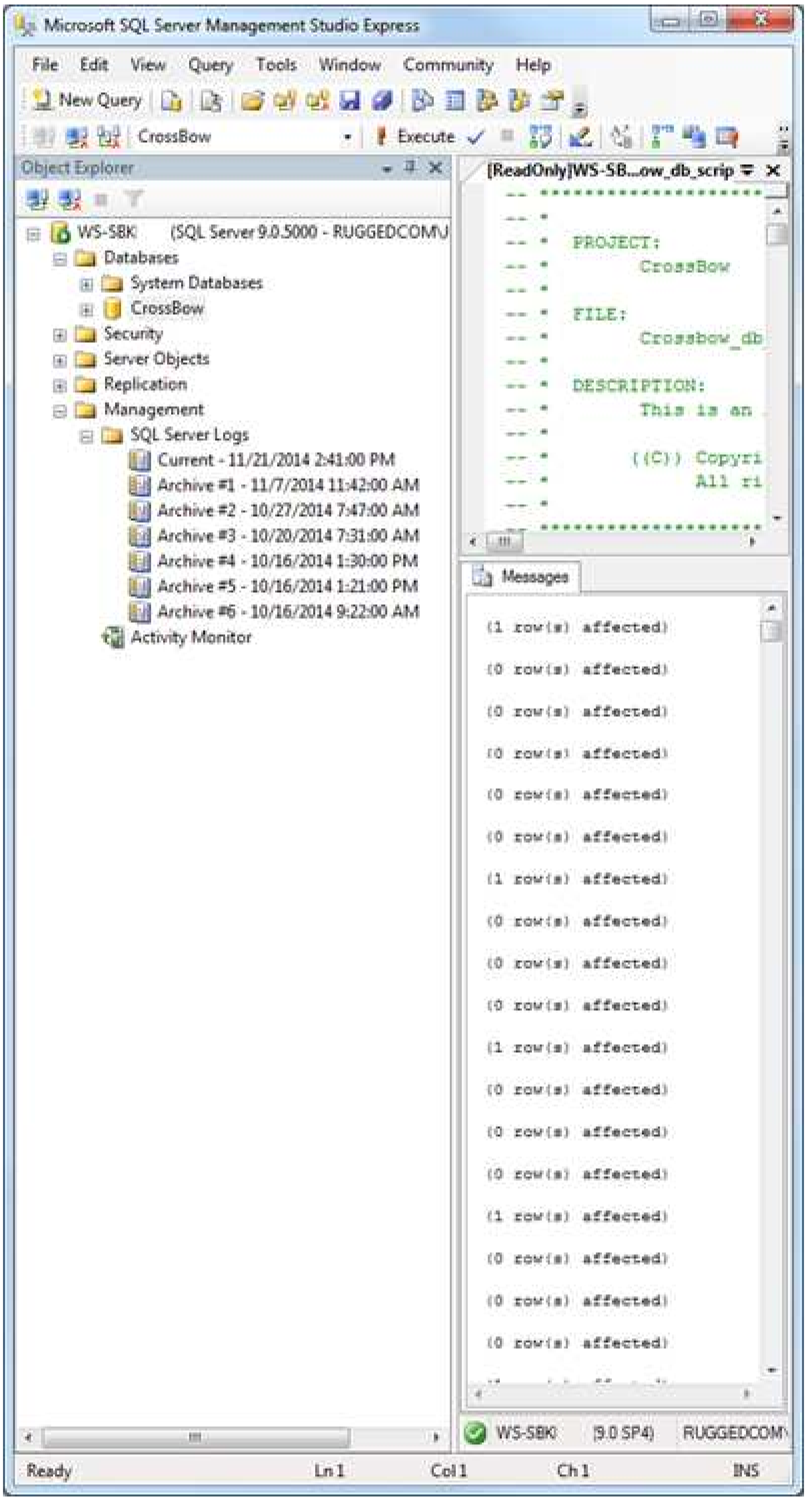
General

Alias Name	NB-CCK
Port No	1433
Protocol	TCP/IP
Server	NB-CCK

Alias Name
Name of the existing alias

Figure 4-3 illustrates the location of the SQL information logs in the SQL Server tree view.

Figure 4-3: SQL Server Management Tree View



Microsoft SQL Server Management Studio Express
File Edit View Query Tools Window Community Help
New Query
CrossBow
Execute
Object Explorer
WS-SBK (SQL Server 9.0.5000 - RUGGEDCOM\
Databases
System Databases
CrossBow
Security
Server Objects
Replication
Management
SQL Server Logs
Current - 11/21/2014 2:41:00 PM
Archive #1 - 11/7/2014 11:42:00 AM
Archive #2 - 10/27/2014 7:47:00 AM
Archive #3 - 10/20/2014 7:31:00 AM
Archive #4 - 10/16/2014 1:30:00 PM
Archive #5 - 10/16/2014 1:21:00 PM
Archive #6 - 10/16/2014 9:22:00 AM
Activity Monitor
[ReadOnly]WS-SB...ow_db_scrip
Messages
WS-SBK (9.0 SP4) RUGGEDCOM\
Ready Ln 1 Col 1 Ch 1 INS

```
-- ********************
-- *
-- *   PROJECT:
-- *           CrossBow
-- *
-- *   FILE:
-- *           Crossbow_db
-- *
-- *   DESCRIPTION:
-- *           This is an
-- *
-- *         ((C)) Copyri
-- *                 All ri
-- *
-- ********************
```

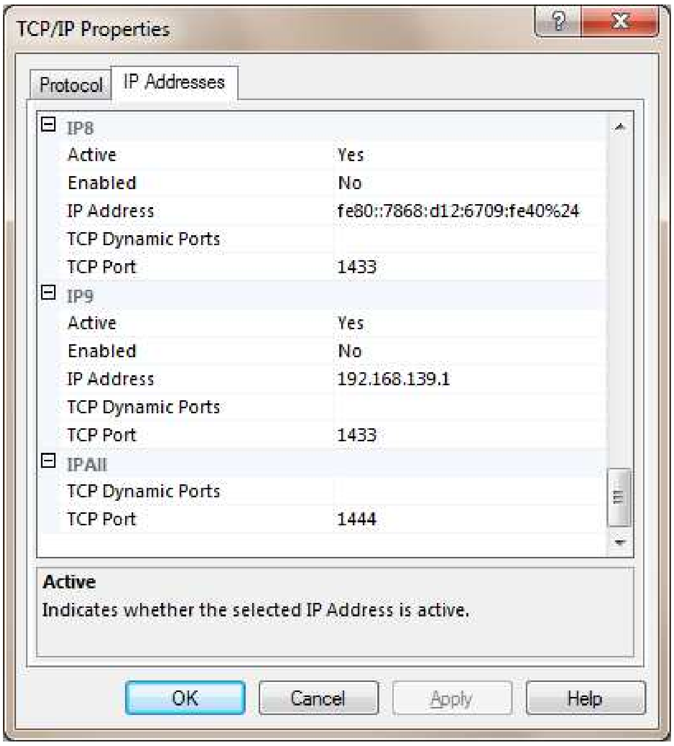
```
(1 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(1 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(1 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(1 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)

(0 row(s) affected)
```

5 Configuring SQL Server to use Non-Standard Ports

NOTE For information about how to use SQL Server Configuration Manager to configure the SQL server to listen on a specific TCP port, refer to Microsoft SQL documentation.

Figure 5-1 illustrates a non-standard port configuration.

Figure 5-1: Non-Standard SQL Port Configuration

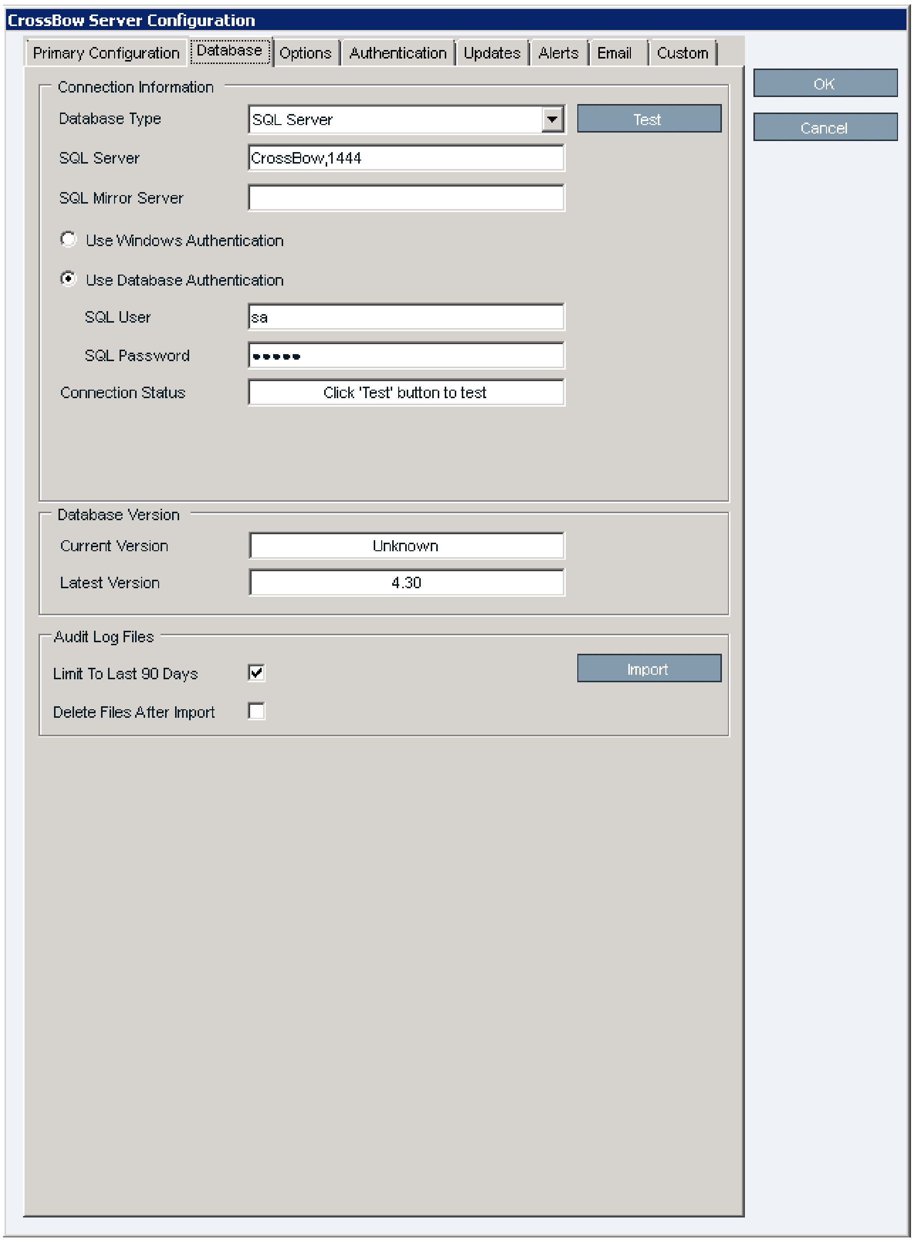


⊟ IP8	
Active	Yes
Enabled	No
IP Address	fe80::7868:d12:6709:fe40%24
TCP Dynamic Ports	
TCP Port	1433
⊟ IP9	
Active	Yes
Enabled	No
IP Address	192.168.139.1
TCP Dynamic Ports	
TCP Port	1433
⊟ IPAll	
TCP Dynamic Ports	
TCP Port	1444

Active
Indicates whether the selected IP Address is active.

If the SQL Server has been configured to use a port other than *1433*, the port number will need to be defined in the RUGGEDCOM CROSSBOW server configuration using the following syntax: <ServerName>,<PortNumber>. For an example, refer to Figure 5-2.

Figure 5-2: RUGGEDCOM CROSSBOW Server Database Configuration



CrossBow Server Configuration

Connection Information

Database Type: SQL Server

SQL Server: CrossBow,1444

SQL Mirror Server:

○ Use Windows Authentication

● Use Database Authentication

SQL User: sa

SQL Password: •••••

Connection Status: Click 'Test' button to test

Database Version

Current Version: Unknown

Latest Version: 4.30

Audit Log Files

Limit To Last 90 Days ☑

Delete Files After Import □

For more information about configuring the RUGGEDCOM CROSSBOW database, refer to the *RUGGGEDCOM CROSSBOW User Guide*.

6 Encrypting Communications between CROSSBOW and SQL Server

A user may wish to encrypt the communications between RUGGEDCOM CROSSBOW and SQL Server, particularly in the case where the CROSSBOW Server and SQL Server are on separate machines communicating across a network. This can be done through configuration on the SQL Server machine.

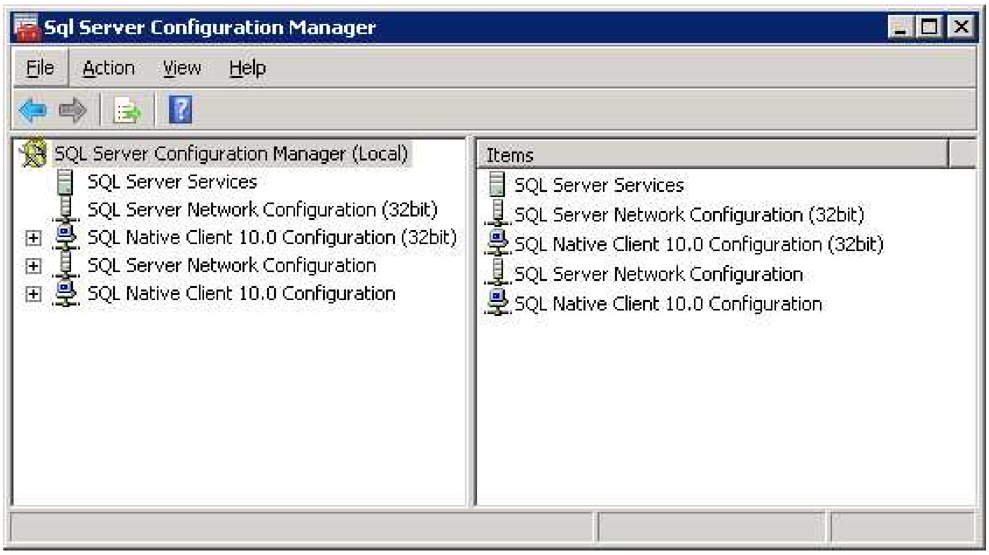
The SQL Server machine must be provisioned with a suitable certificate that the SQL Server service can access. SQL Server requires that this certificate have a Common Name that matches the Fully Qualified Domain Name (FQDN) of the machine that SQL Server is installed on, and that the certificate's Intended Purpose is Server Authentication. It may be that the SQL Server machine already has such a certificate installed, in which case SQL Server can simply be configured to use it. Otherwise, a certificate will need to be generated (typically by an IT department) and installed on the SQL Server machine.

After a suitable certificate is installed, SQL Server can be configured to use encryption through the SQL Server Configuration Manager. This can typically be accessed via the Windows Start menu.

To configure SQL Server to use encryption through the SQL Server Configuration Manager, do the following:

1. Click **Start**, then select **All Programs**, select **Microsoft SQL Server 20xx**, select **Configuration Tools,** and then click **SQL Server Configuration Manager**. The **SQL Server Configuration Manager** window appears.

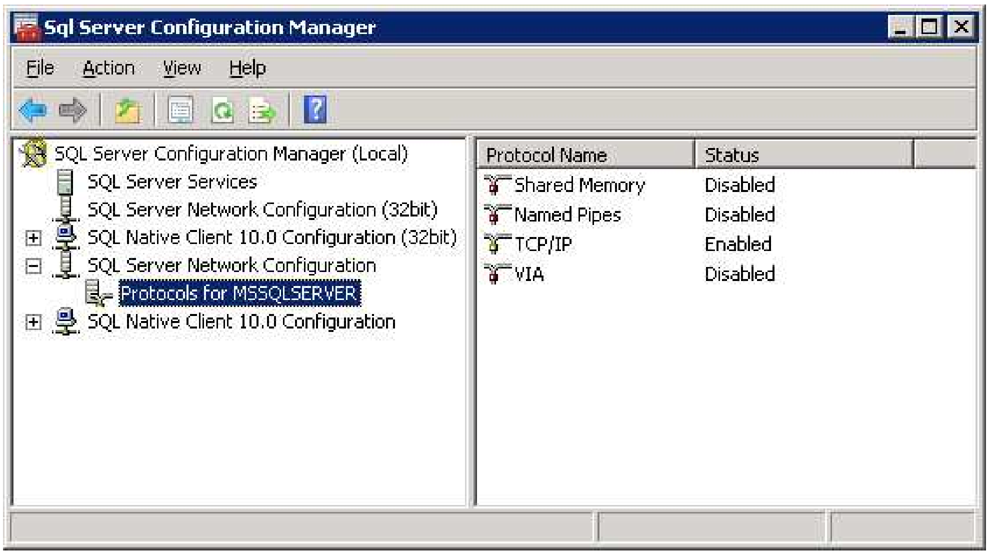
Figure 6-1: SQL Server Configuration Manager



Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
SQL Native Client 10.0 Configuration
Items
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
SQL Native Client 10.0 Configuration

2. Under one of the SQL Server Network Configuration nodes in the tree, find the Protocols for the specific SQL Server instance, depending on the configuration. If there is more than one SQL Server instance on a single machine, this must be the instance that hosts the RUGGEDCOM CROSSBOW database. In the default case it will likely be called MSSQLSERVER. For an example, refer to Figure 6-2.

Figure 6-2: SQL Server Instance Protocols

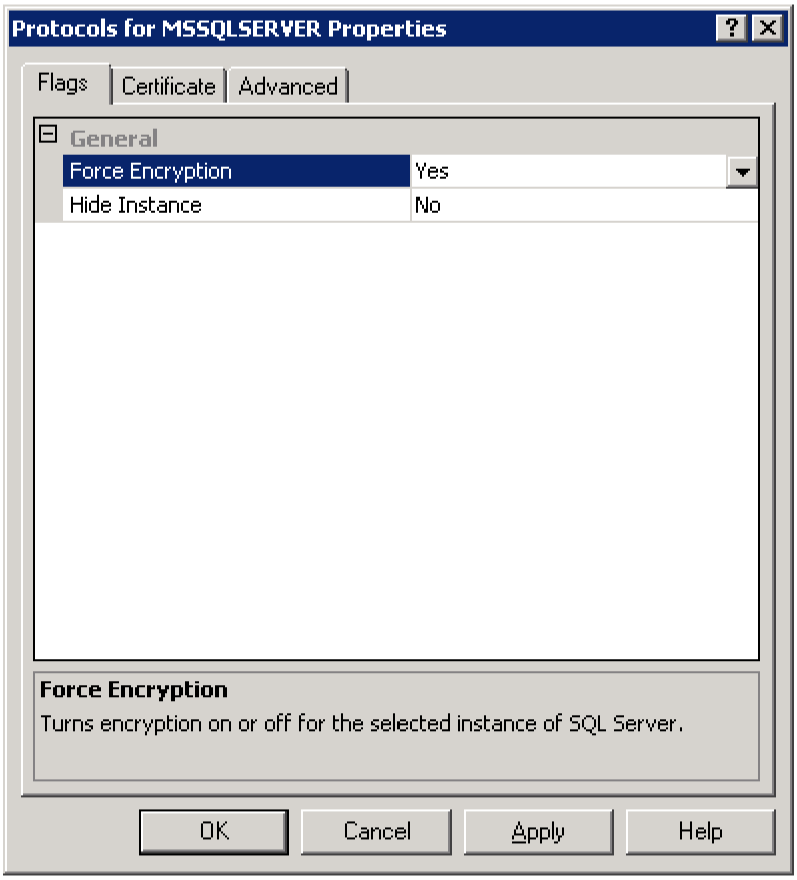


SQL Server Configuration Manager (Local)
- SQL Server Services
- SQL Server Network Configuration (32bit)
- SQL Native Client 10.0 Configuration (32bit)
- SQL Server Network Configuration
  - Protocols for MSSQLSERVER
- SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Disabled
Named Pipes	Disabled
TCP/IP	Enabled
VIA	Disabled

3. For applicable SQL Server instance, right-click the Protocols node and then click **Properties**. The Protocols for MSSQLSERVER Properties dialog box appears.

Figure 6-3: Protocols for MSSQLSERVER Properties



General

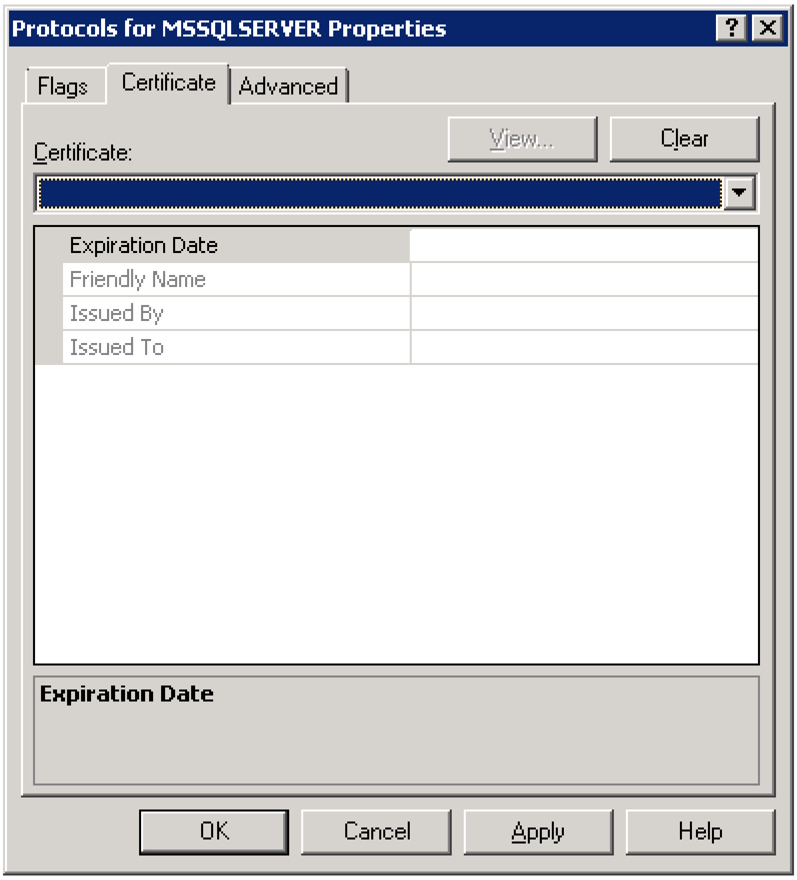
Force Encryption	Yes
Hide Instance	No

Force Encryption

Turns encryption on or off for the selected instance of SQL Server.

4. On the **Flags** tab, set **Force Encryption** to **Yes**.
5. Select the **Certificate** tab and select the applicable certificate from the dropdown list.

Figure 6-4: SQL Server Protocol Certificate

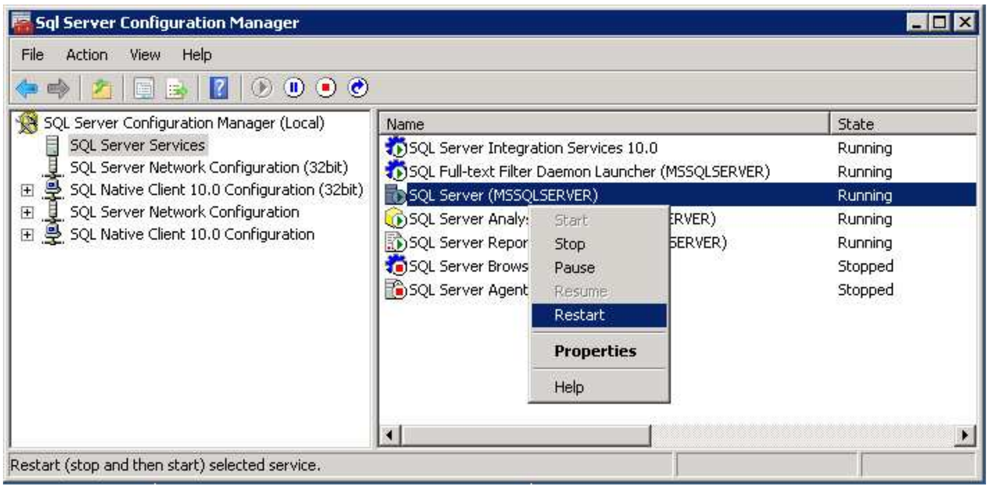


NOTE If no items appear in the Certificate drop-down list, then there is no suitable certificate installed that SQL Server can use for encryption. If there is a certificate installed, it is likely that it either has a Common Name that does not match the Fully Qualified Domain Name (FQDN) for the machine on which the SQL Server instance is installed, or that it does not have an Intended Purpose set to Server Authentication. For more information, refer to the Microsoft SQL Server documentation.

Once the appropriate certificate is selected in the drop-down, its attributes will display in the remaining fields on that tab. These fields are read-only and serve only to provide information about the selected certificate.

6. Click **OK** to close the dialog box.
7. Right-click the SQL Server instance and click **Restart** to apply the changes.

Figure 6-5: SQL Server Restart


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
SQL Native Client 10.0 Configuration
Start
Stop
Pause
Resume
Restart
Properties
Help

Name	State
SQL Server Integration Services 10.0	Running
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Running
SQL Server (MSSQLSERVER)	Running
SQL Server Analy: ERVER)	Running
SQL Server Repor SERVER)	Running
SQL Server Brows	Stopped
SQL Server Agent	Stopped

Restart (stop and then start) selected service.

7 Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, please contact Siemens Customer support through any one of the following methods:

- **Online**

  Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

- **Telephone**

  Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

- **Mobile App**

  Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

  - Access Siemens’ extensive library of support documentation, including FAQs, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community via the forum
  - And much more…

8 History

Table 8-1

Version	Date	Modifications
1	11/2015	Initial release