Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

ISA Server 2006 - Firewall Logging into Microsoft SQL database

Abstract

In this article, I will show you how to log ISA Server 2006 Firewall logging into a Microsoft SQL Server 2005 database.

Let's begin

During a Standard installation of Microsoft ISA Server 2006, ISA will install a local MSDE (Microsoft SQL Server Database Engine) to provide Logging for the Microsoft Firewall- and Webproxy service. It is possible to log the Firewall- and Webproxy service into a local Microsoft SQL Server 2005 database or a remote Microsoft SQL database.

Firewall Lockdown modus

Pay attention when you move the Firewall logging to an external Microsoft SQL Server, because ISA Server use a Firewall Lockdown modus, that deactivates nearly everything functionality of the Firewall when logging could not be enforced. It is possible to disable the Firewall Lockdown modus (I provide a Link how to disable the Firewall Lockdown Modus at the end of this article), but I never recommend to disable this feature.

Installing Microsoft SQL Server 2005 Express Edition

After downloading the SQL Server Express Edition from the Microsoft website, extract the downloaded package and follow the installation instructions.

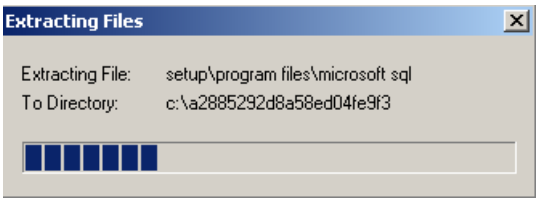

Figure 1: Extracting the Microsoft SQL Server 2005 package

Next, read, understand and accept the license agreement.

Before the Microsoft SQL Server setup can start, the installation wizard installs the Microsoft SQL Native Client and the Microsoft SQL Server 2005 Setup support files.

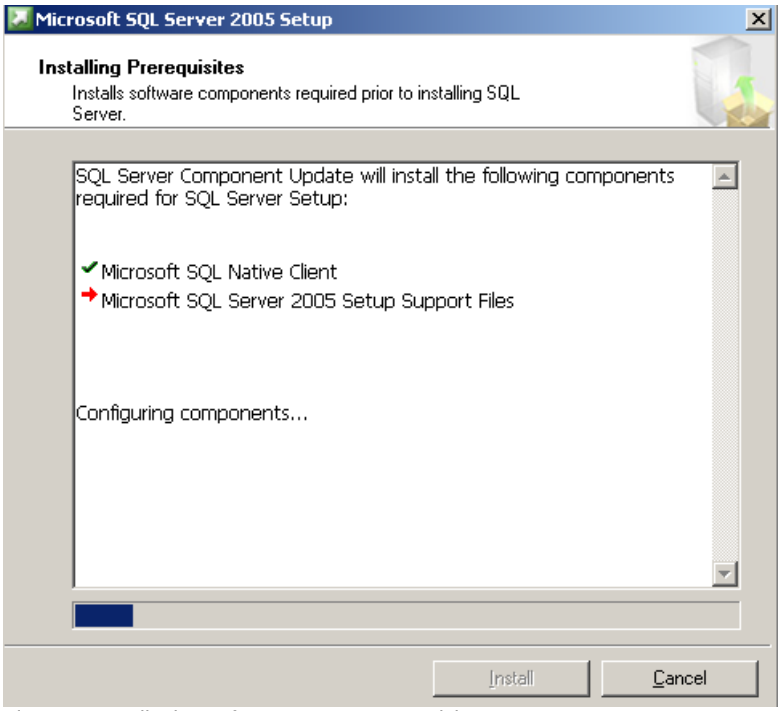

Figure 2: Install Microsoft SQL Server prerequisites

After installing the required setup files, the Microsoft SQL Server Installation Wizard starts.

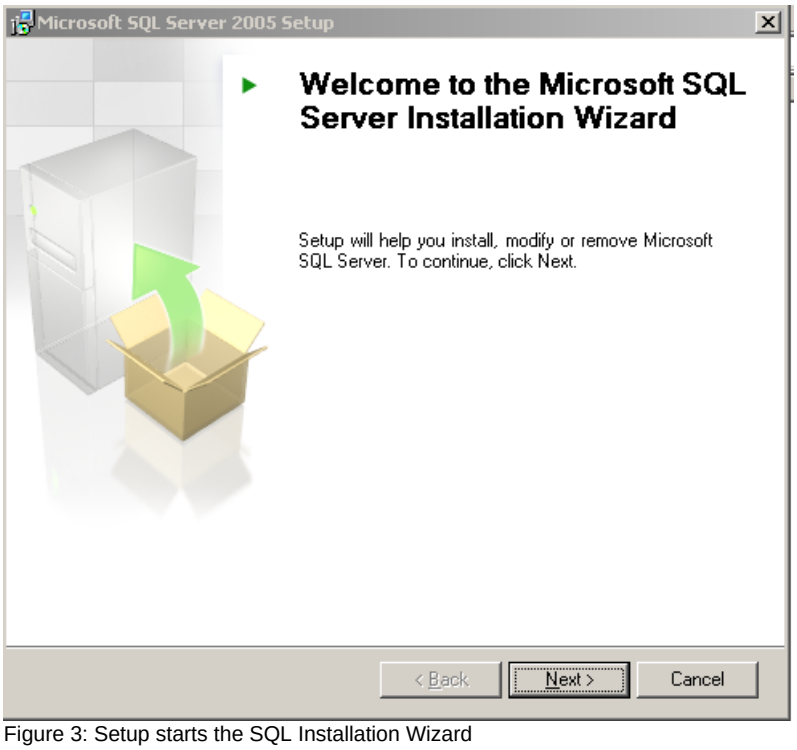

Figure 3: Setup starts the SQL Installation Wizard

Before installing the Microsoft SQL Server database, the installation wizard will do some checks, if the machine provides the necessary configuration for the Microsoft SQL Server 2005 Express Edition.

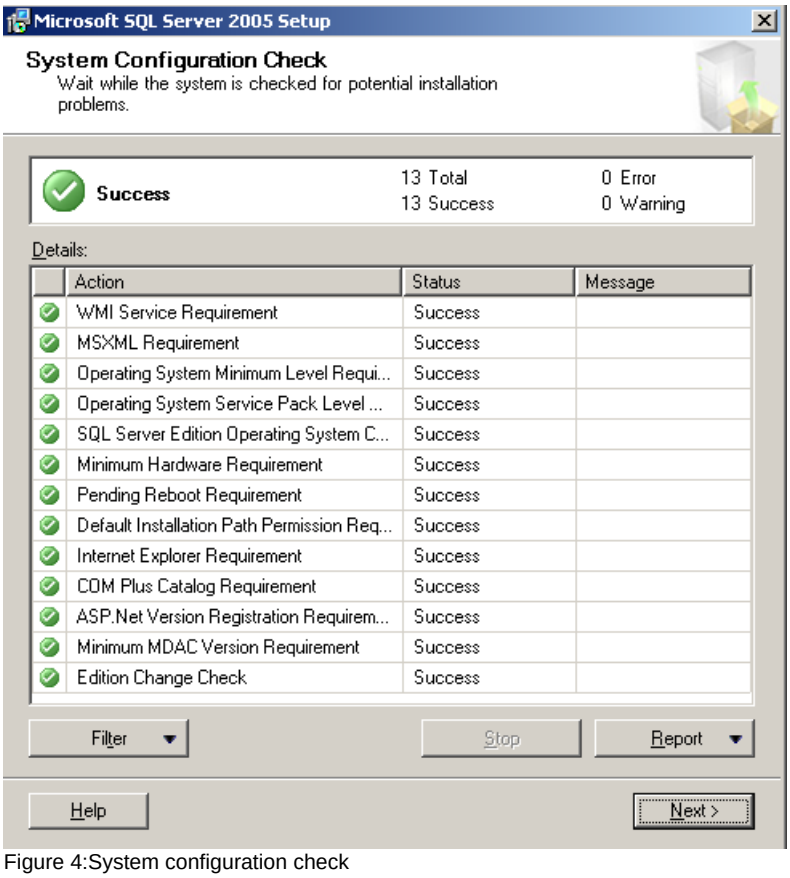

Figure 4:System configuration check

Enter registration information

Select the components you would like to install. The Standard selection is enough to provide reliable database functionalities.

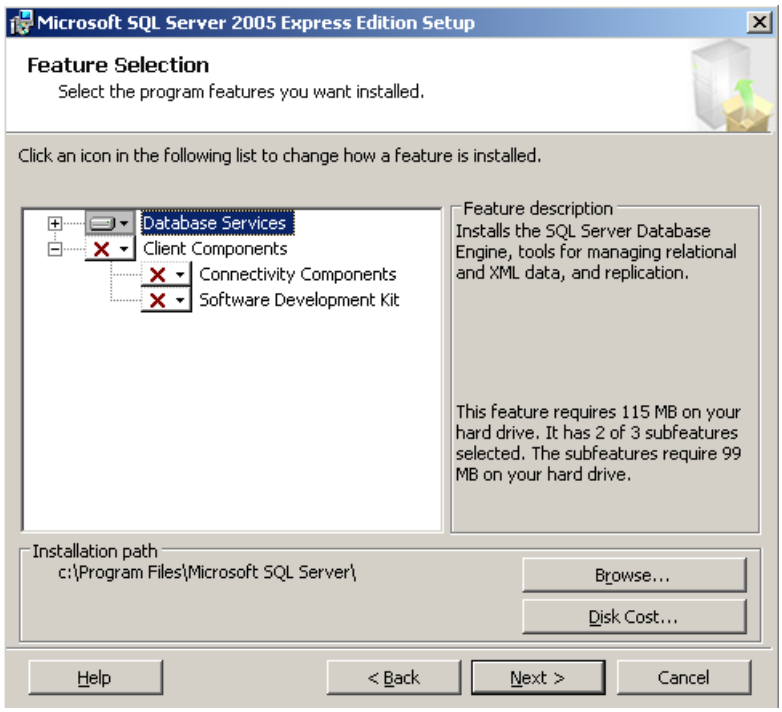

Figure 5: Feature selection

Create a new instance and specify the instance name ISALOG.

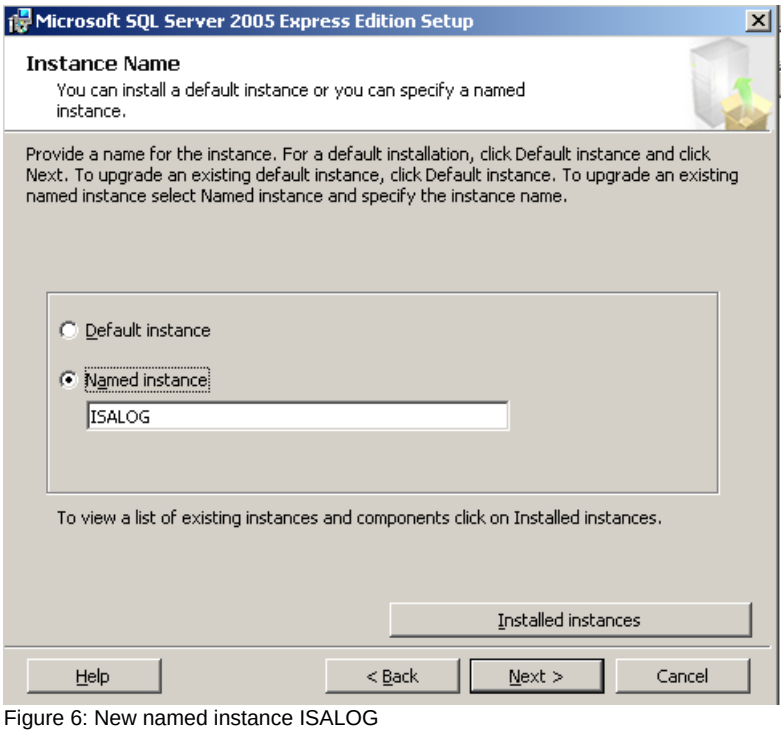

Figure 6: New named instance ISALOG

Specify the Local system account as service account.

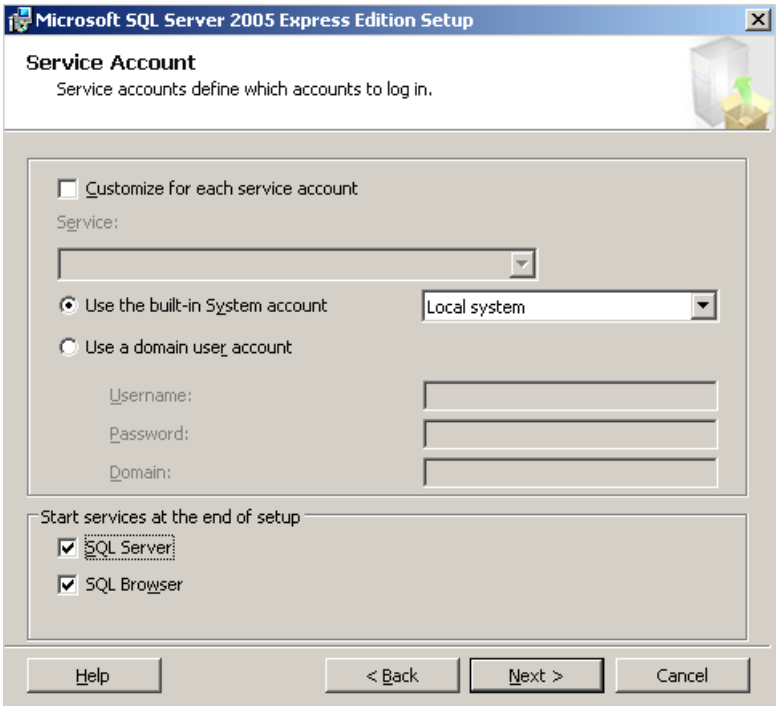

Figure 7: Specify a account for the Microsoft SQL Database

Select Windows as the authentication mode.

Use default collation settings for SQL.

Enable User Instance.

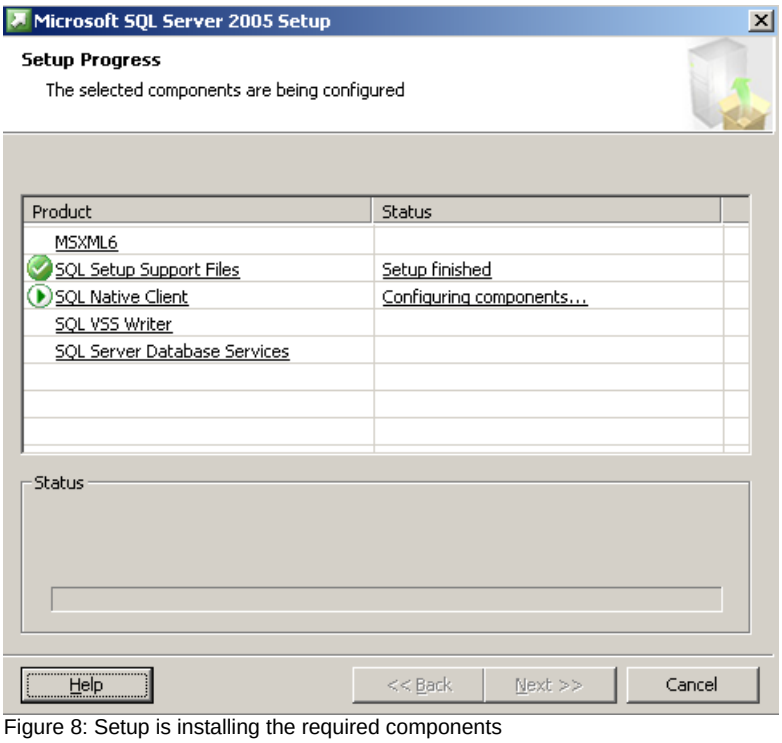

Figure 8: Setup is installing the required components

After setup has finished, restart the Server.

At ISA Server side

Activate the System Policy for Remote SQL Logging. This allows ISA Server access to an internal Microsoft SQL Server database.

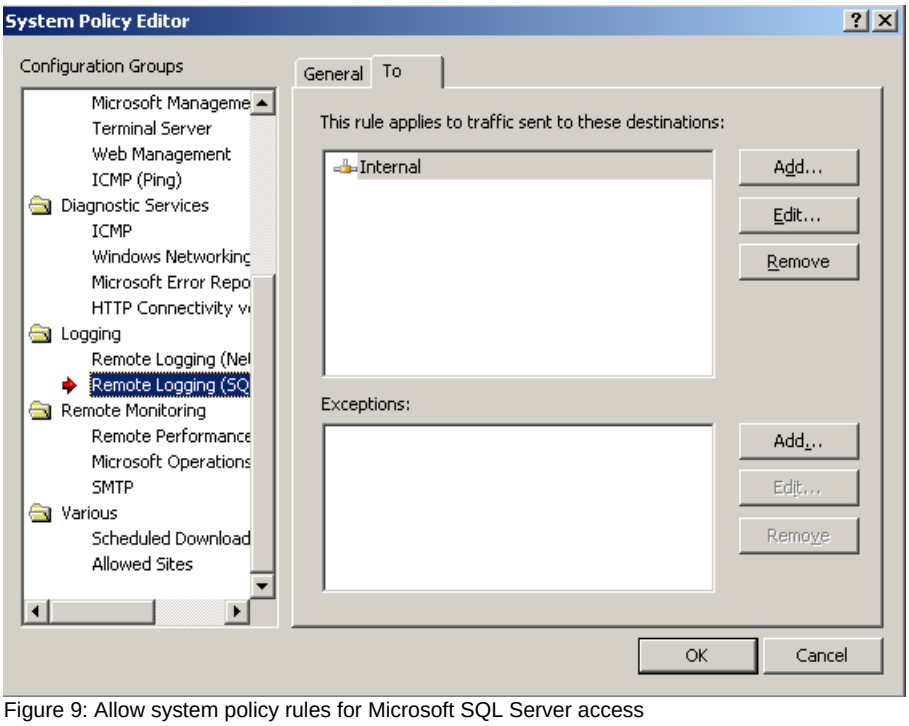

Figure 9: Allow system policy rules for Microsoft SQL Server access

Per default Microsoft SQL Server 2005 Express only allows access from local services to the database. You have to change the setting to allow remote

connections with the help of the Microsoft SQL Server 2005 Surface Area Configuration.

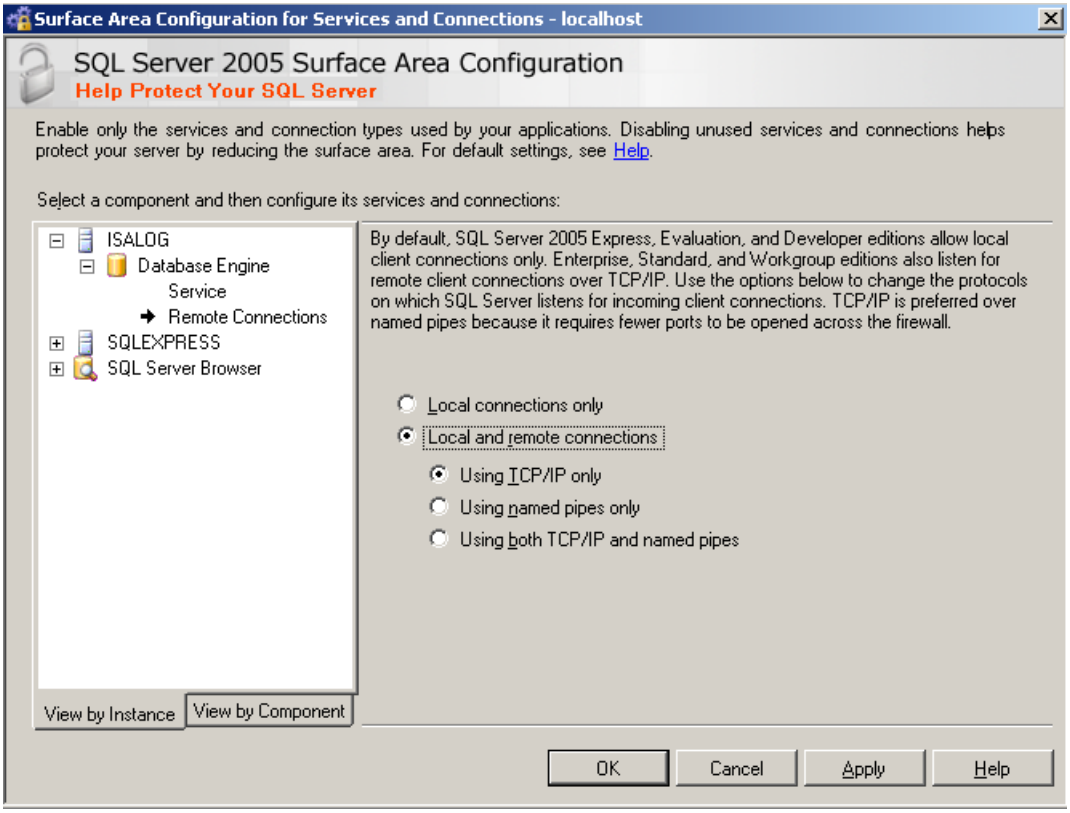

Figure 10: SQL Server attack surface configuration

As a next step, you must check if the TCP/IP protocol is enabled for the ISALOG database and if the Network configuration uses a fixed port for SQL Server (1433)

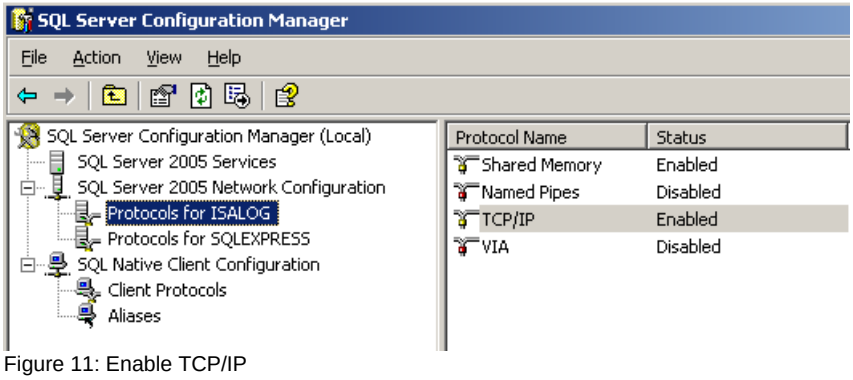

Figure 11: Enable TCP/IP

Disable SQL Server Dynamic TCP Ports (delete the Null value) and specify a fixed port (1433) for all IP addresses.

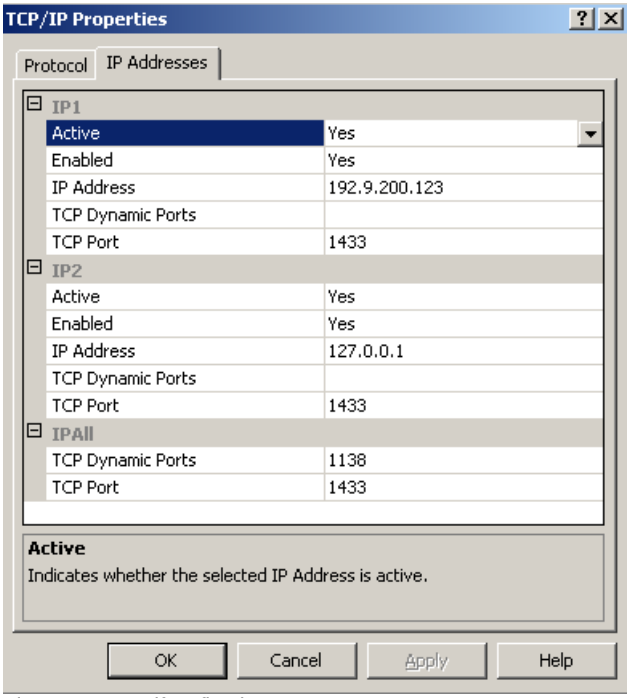

Figure 12: Specify a fixed port

You have to restart the Microsoft SQL Server service after settings are applied.

Installing the Microsoft SQL Server Management Studio Express

Microsoft SQL Server Management Studio Express is the Management console for managing many parts of Microsoft SQL Server. If you are using Microsoft SQL Server 2005 Express Edition, you must download and install the Microsoft SQL Server Management Studio Express separately from the database.

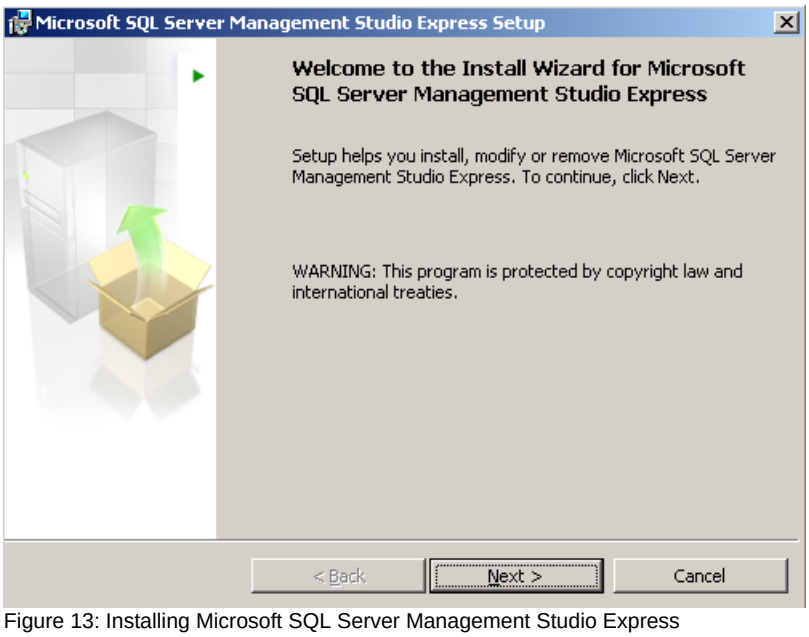

Figure 13: Installing Microsoft SQL Server Management Studio Express

Create a Database

After installing the Microsoft SQL Server Management Studio Express version, start the console and create a new database called ISALOGS.

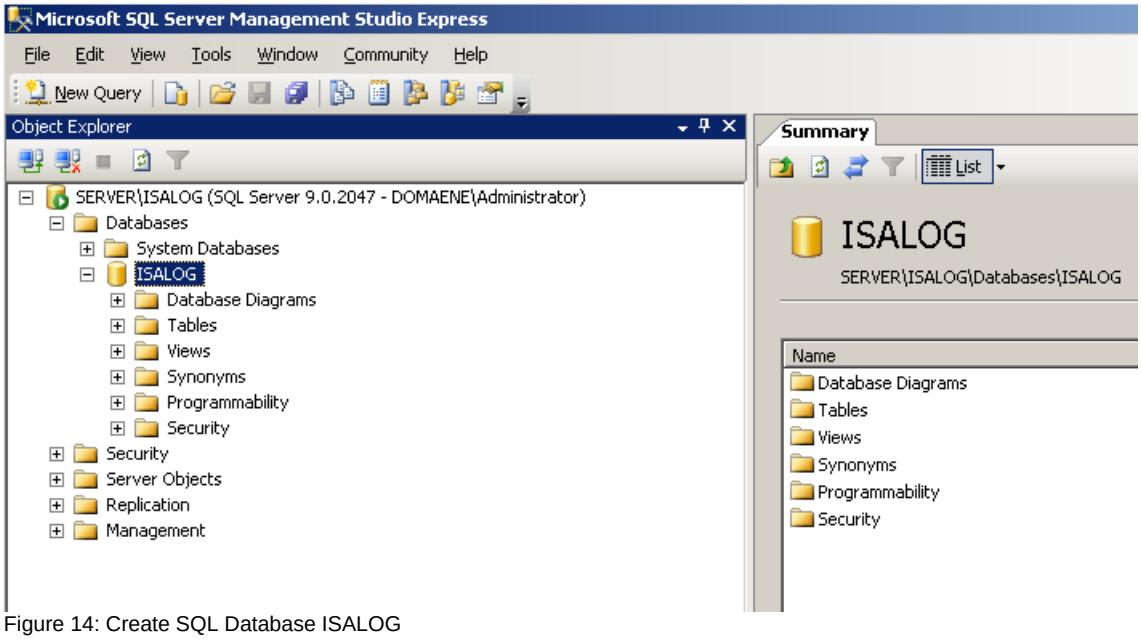

Figure 14: Create SQL Database ISALOG

Create a new account in Active Directory and give this account Domain user rights and additional SQL Server rights to access the ISALOG database. This account will be used in the ISA Server Management Console for direct SQL access.

Create the database tables

The ISA Server 2006 installation CD contains two .SQL files, which can be used to create the required database tables into the ISALOG database.

Open FWSERV.SQL from the ISA Server 2006 program files CD into the Microsoft SQL Server Management Studio Express (File – Open). Before you execute the FWSRV.SQL script, extend the first line with the instruction to use the ISALOG database.

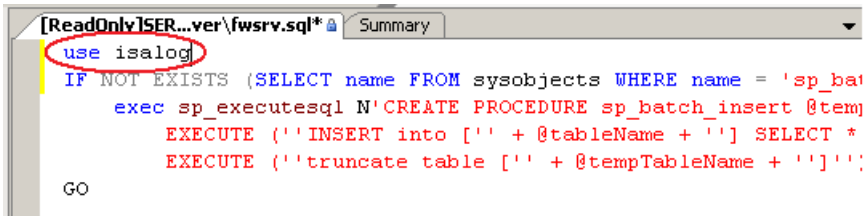

Figure 15: Extend the script to use the ISALOG database

Now it is possible to execute the script. If everything is going fine, the new database table will be created.

```
[ReadOnly]SERVER\...\fwsrv.sql | SERVER\ISALOG...SQLQuery1.sql | Summary

IF NOT EXISTS (SELECT name FROM sysobjects WHERE name = 'sp_bat'
    exec sp_executesql N'CREATE PROCEDURE sp_batch_insert @temp'
        EXECUTE (''INSERT into ['' + @tableName + ''] SELECT *
        EXECUTE (''truncate table ['' + @tempTableName + '']'')
GO

CREATE TABLE FirewallLog (
    [servername]          nvarchar(128),
    [logTime]             datetime,
    [protocol]            varchar(32),
    [SourceIP]            bigint,
    [SourcePort]          int,
    [DestinationIP]       bigint,
    [DestinationPort]     int,
    [OriginalClientIP]    bigint,
    [SourceNetwork]       nvarchar(128),
    [DestinationNetwork]  nvarchar(128),
    [Action]              smallint,
    [resultcode]          int,
    [rule]                nvarchar(128),
    [ApplicationProtocol] nvarchar(128),
    [Bidirectional]       smallint,
    [bytessent]           bigint,
    [bytessentDelta]      bigint,
    [bytesrecvd]          bigint,
    [bytesrecvdDelta]     bigint,
    [connectiontime]      int,
    [connectiontimeDelta] int,
    [SourceProxy]         varchar(32),
    [DestinationProxy]    varchar(32),
    [SourceName]          varchar(255),
```

Figure 16: Table FirewallLog

Now it is time to give the ISA-SQL Account the right to access the ISALOG database.

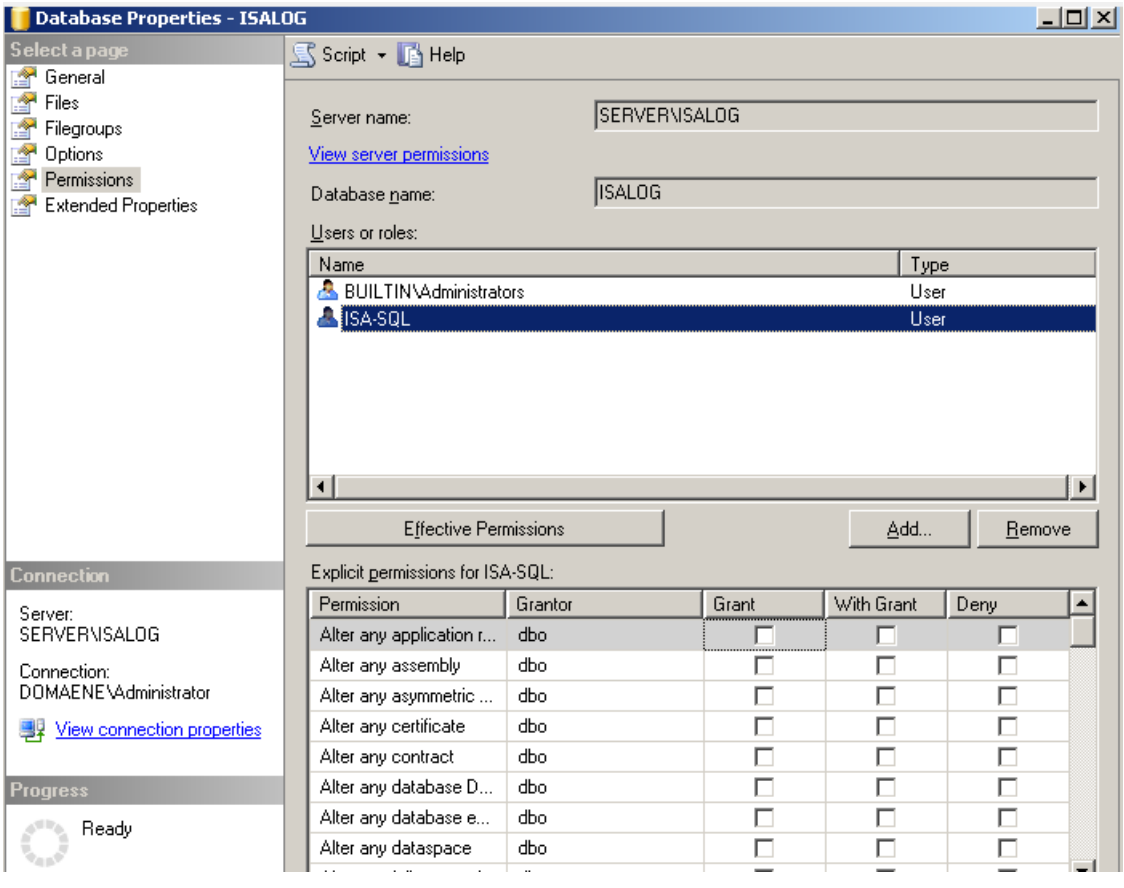

Figure 17: Add the ISA-SQL user to the ISALOG Database

Request a certificate for SQL Server connection encryption

Per default, ISA Server uses a encrypted connection to the Microsoft SQL Server. The connection will be established with the help of a Server Authentication certificate, so you have to install a certificate before establishing the connection. It is possible to use your own CA to create a certificate request or s elf signed certificate. At the end of this article I placed a link with detailed instructions.

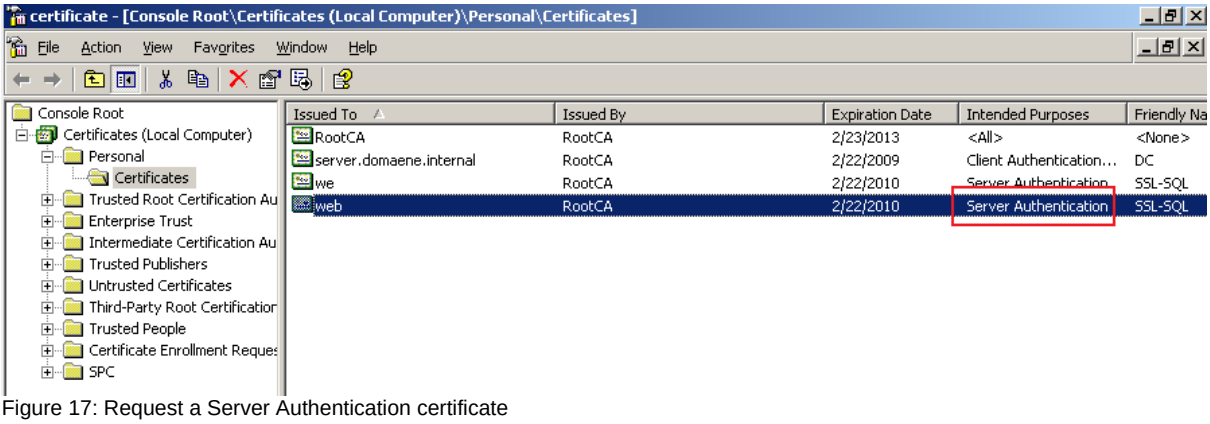

Figure 17: Request a Server Authentication certificate

At ISA side

Now it is time to change the Microsoft ISA Server Logging from MSDE to SQL. Start the ISA Server 2006 Management console, navigate to Logging option and change the logging options for the Microsoft Firewall Service (If you want to change the Logging for the Webproxy Service, the process is similar).

Enter the name of the SQL Server, the Standard SQL port (1433), the Name of the Firewall Table and Windows as the Authentication method. You must also specify the account which will be used to establish a connection. Click *Test* to test the SQL connection.

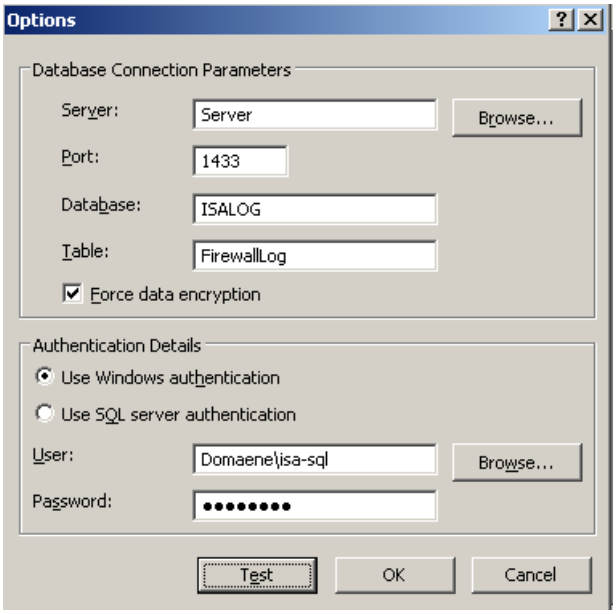

Figure 18: SQL Logging options

After changing the Logging options, click *Apply* to activate the settings and if everything is going fine, ISA Server now use a Microsoft SQL Server database or Firewall and Webproxy Logging.

You can now use all advanced features of Microsoft SQL Server 2005 for your ISA Server database like automatic backups, Database shrinking and many more advanced features.

Conclusion

In this article I tried to show you how to configure ISA Server Firewall Logging into a remote Microsoft SQL Server 2005 Express database. The process for logging into the big brothers database Microsoft SQL Server 2005 is nearly similar, so you can use this article for both versions. In this article I showed you only how to change the logging of the Microsoft Firewall service into a Microsoft SQL Server 2005 database. If you also want to log the Webproxy log into a Microsoft SQL Server 2005 database, you only have to create the Webproxy table for the ISALOG database and change the Webproxy logging in the ISA Management console to Microsoft SQL Server logging.

Related links

Monitoring, Logging, and Reporting Features in ISA Server 2006
http://www.microsoft.com/technet/isa/2006/monitoring.mspx
Best Practices for Performance in ISA Server 2006
http://www.microsoft.com/technet/isa/2006/perf_bp.mspx
Microsoft SQL Server Management Studio Express
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=c243a5ae-4bd1-4e3d-94b8-5a0f62bf7796
How to configure ISA Server 2004 and ISA Server 2006 to log data to an SQL Server database
http://support.microsoft.com/kb/838710/en-us
How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console
http://support.microsoft.com/kb/316898/en-us