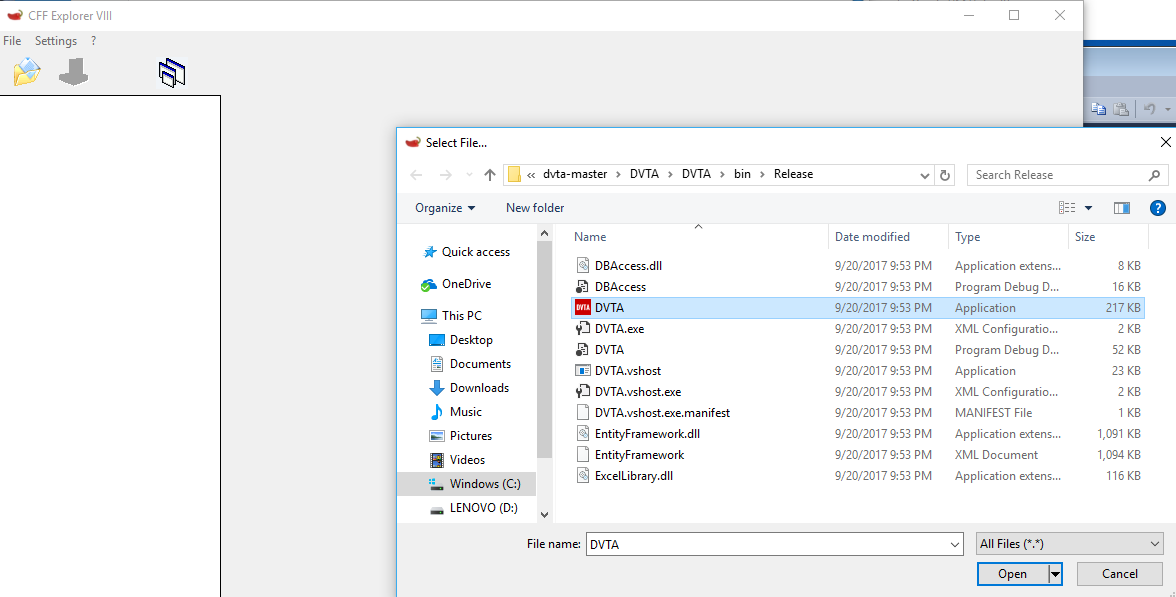
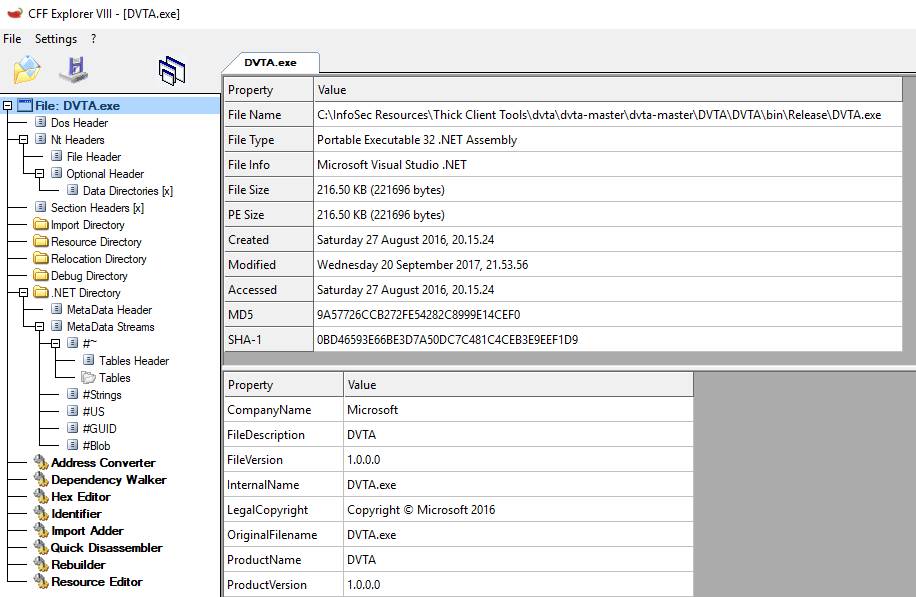
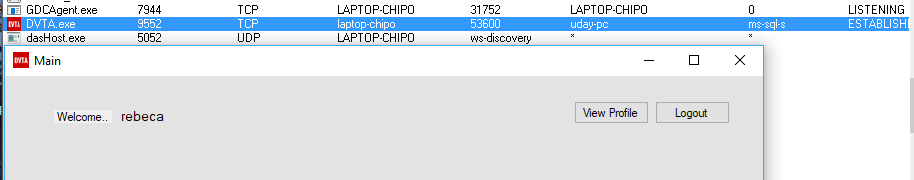
Understanding how the application is built is very useful and one way to do it is to reverse the binary using a tool such as CFF Explorer. CFF Explorer can be downloaded from <http://www.ntcore.com/exsuite.php>

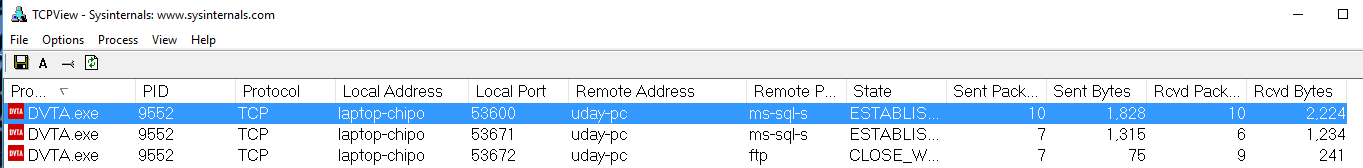
Install CFF Explorer and open the DVTA application..



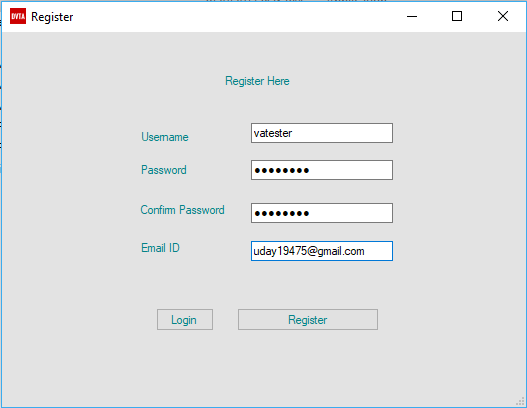




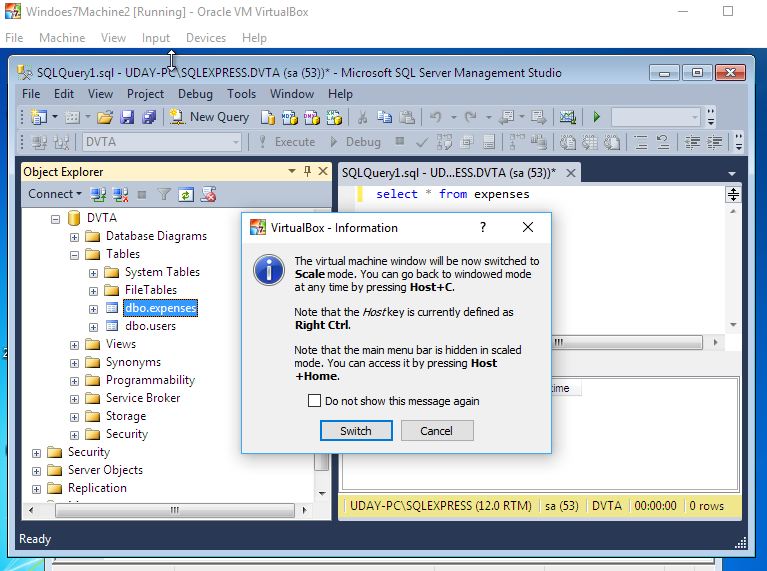


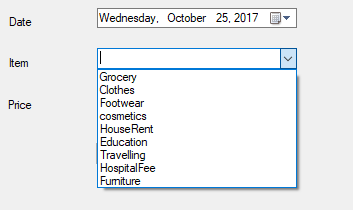


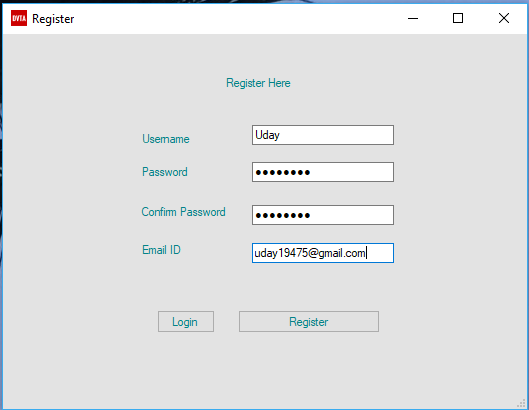
Registering a new user



Pwd: vizag123



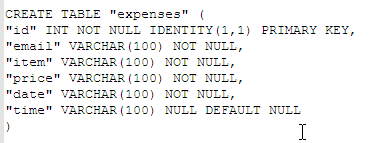


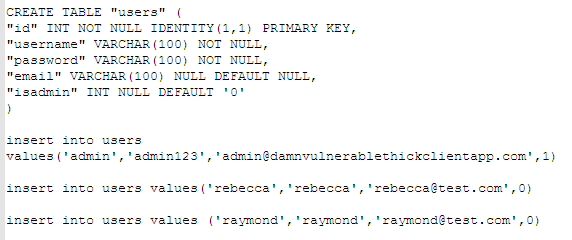


Un: uday

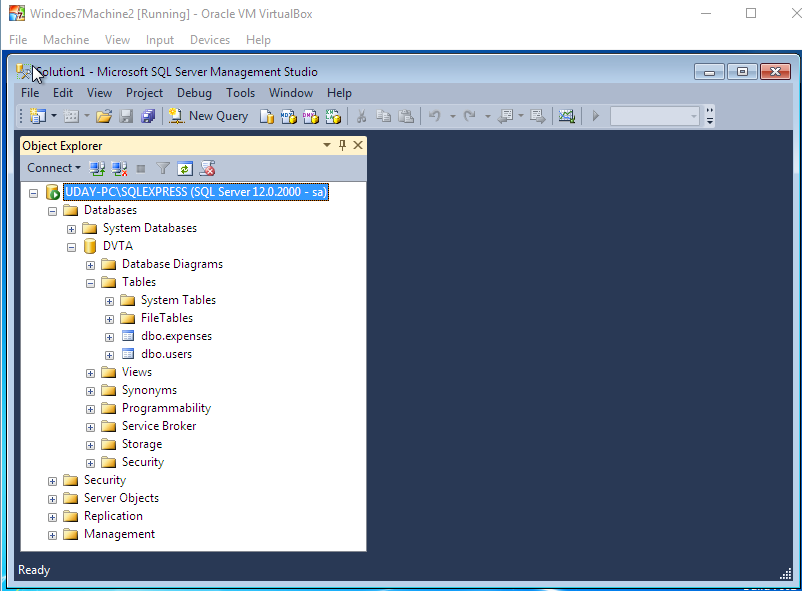
Pwd: vizag123

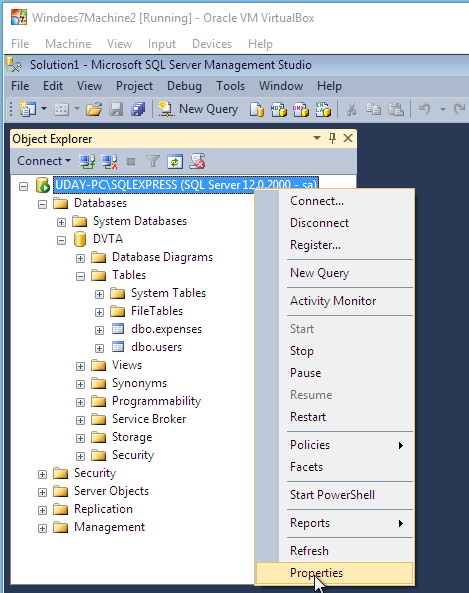
Email: [uday19475@gmail.com](mailto:uday19475@gmail.com)

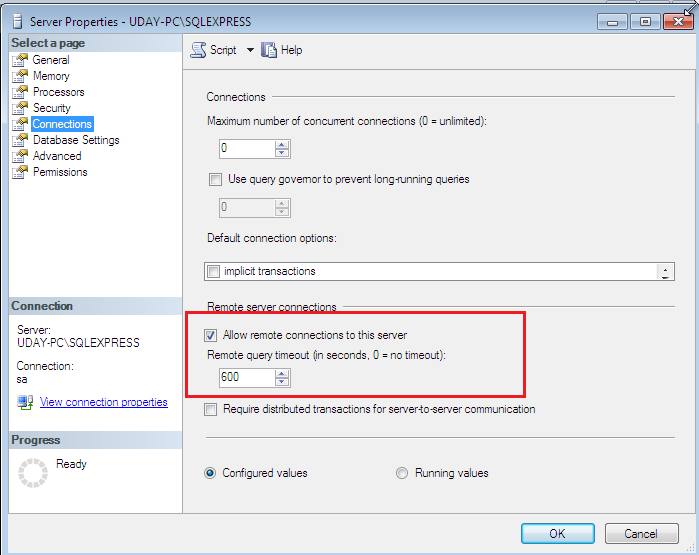




Setting up SQL server to accept connections from other machines:

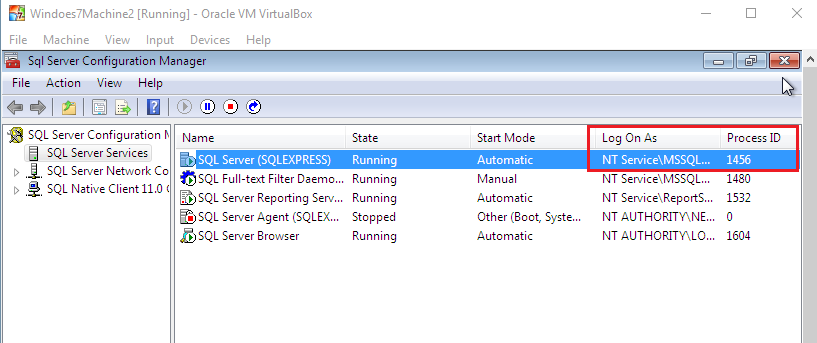




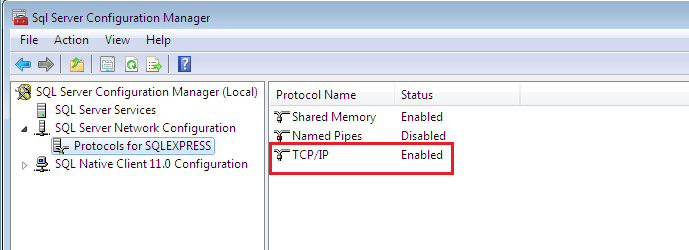


Configure SQL express server to listen on static port

1. Open SQL Server Configuration Manager and click on “SQL Server Services” in the left pane.

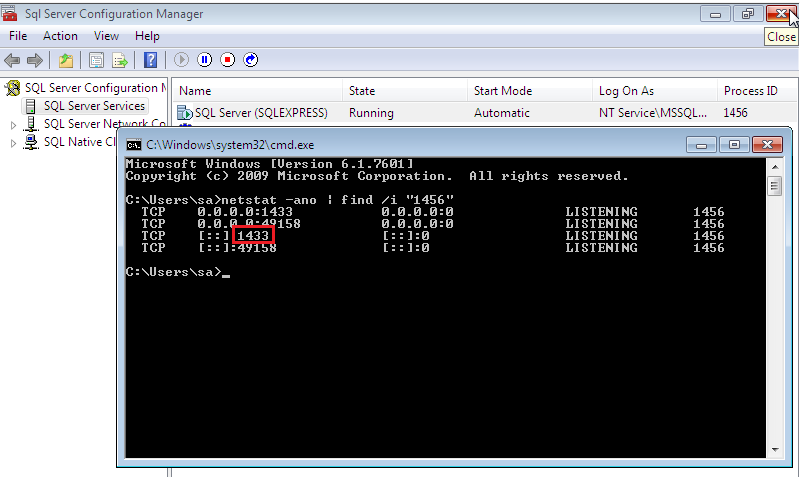


Also, ensure that TCP/IP is enabled for SQLEXPRESS as shown below:

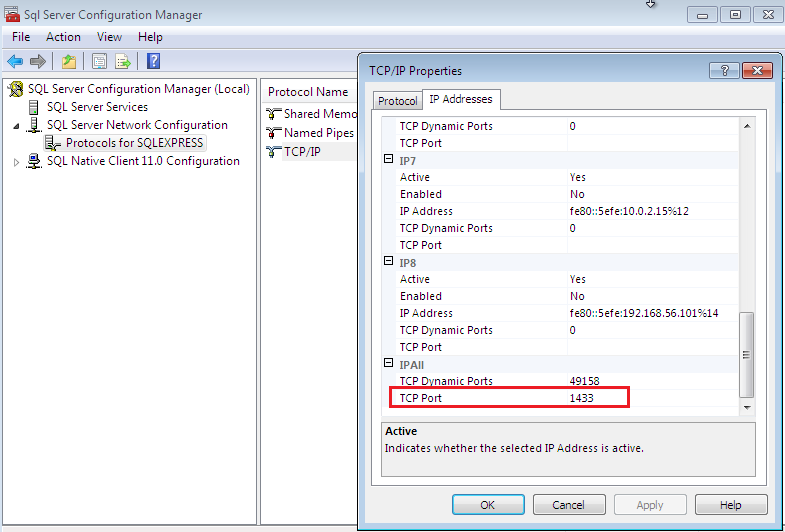


1. In the center pane, is a column that lists the Process ID for each running service. Look for the PID in the row for SQL Server. In our case, the PID for SQL Server is 1456. Identify the port that PID is listening in by typing this into the command prompt:

C:\Users\sa> netstat –ano | find /i “1456”



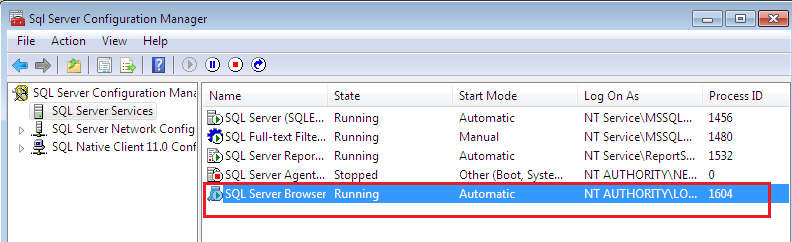
In the SQL Server Configuration Manager, click on SQL Server Network Configuration in the left pane and right-click TCP/IP protocol and select option Properties. Goto IP Address tab and scroll-down to APALL section. Remove value for TCP Dynamic Ports (enter any value except zero) and enter the port 1433 for TCP Port.



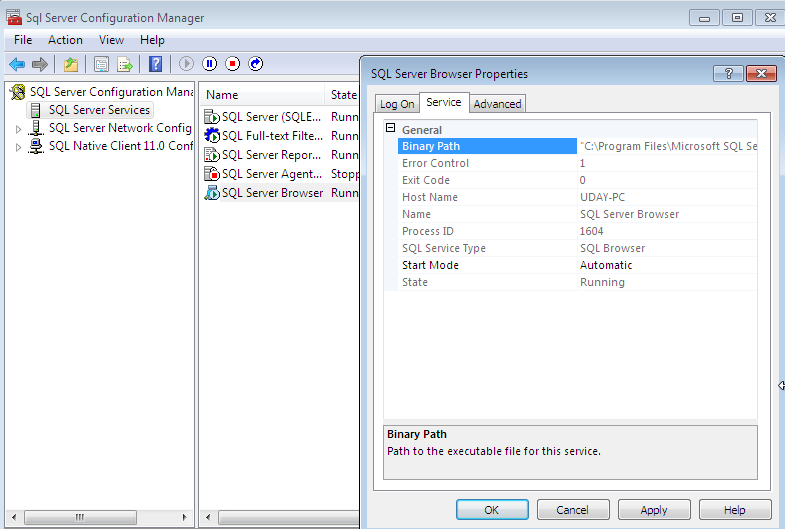
Restart SQL Server to propagate these changes and at this stage, SQL Express is configured to listen on standard port 1433

Next, turn on the SQL Server Browser service:

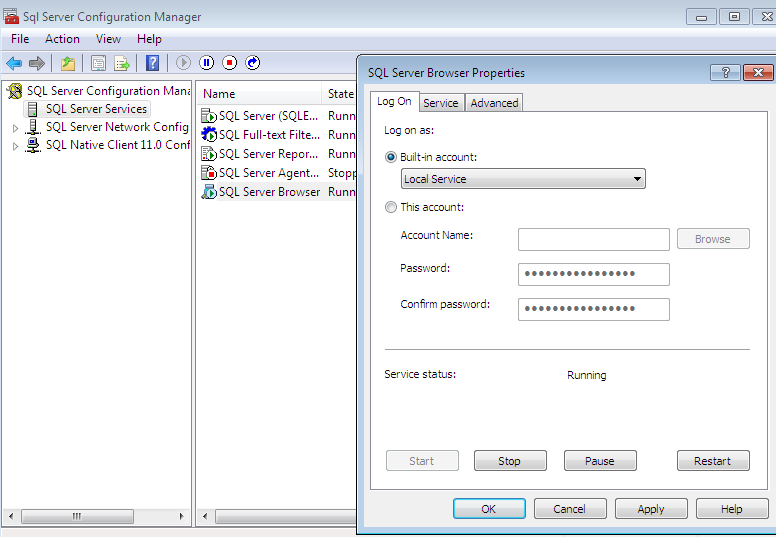
1. Open SQL Server Configuration Manager and click on “SQL Server Services” in the left pane, right-click SQL Server Browser service and select Properties



Go to the Service tab and for Start Mode option change start type to Automatic.



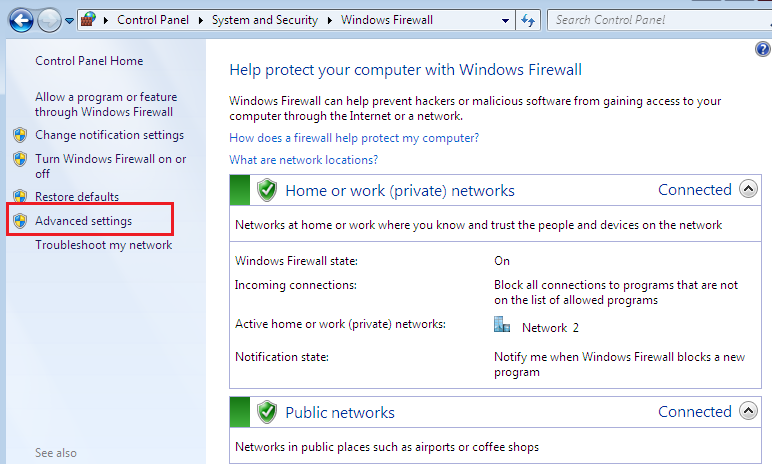
Click the start button to start SQL Browser service and confirm that the SQL Browser is up and running.



Important: According to the SQL server hardening best practices the SQL Browser service should be disabled. This service, which typically isn’t required, responds to requests for SQL Server resources and redirects the caller to the correct port. Keeping the browser service disabled will remove the redirector as an attack vector, helping to obscure the correct entry ways into your SQL Server components.

Configure the firewall to allow network traffic that is related to SQL Server and to the SQL Server Browser service.

Four exceptions must be configured in Windows Firewall to allow access to SQL Server:



A port exception for TCP Port 1433.

In the New Inbound Rule Wizard dialog, use the following information to create a port exception:

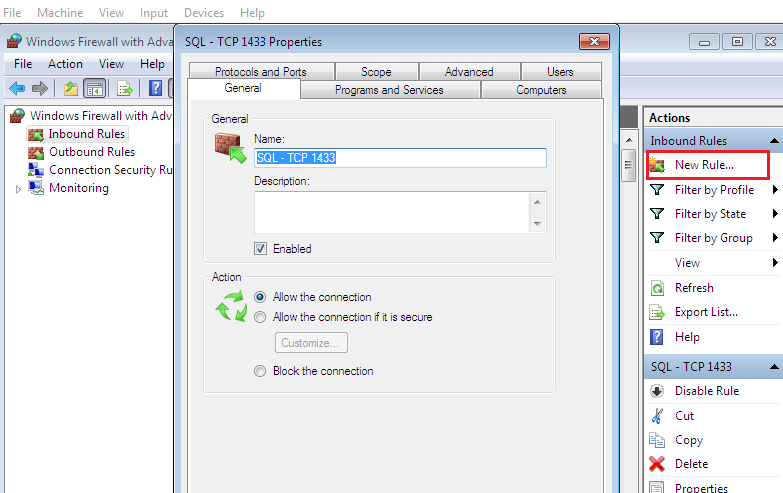
Select Port

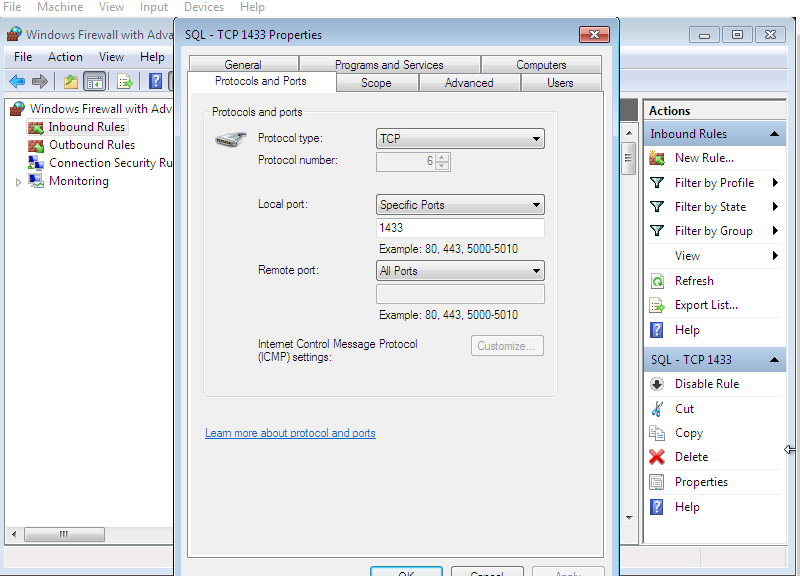
Select TCP and specify port 1433

Allow the connection

Choose all three profiles (Domain, Private & Public)

Name the rule “SQL – TCP 1433”





A port exception for UDP Port 1434. Click New Rule again and use the following information to create another port exception:

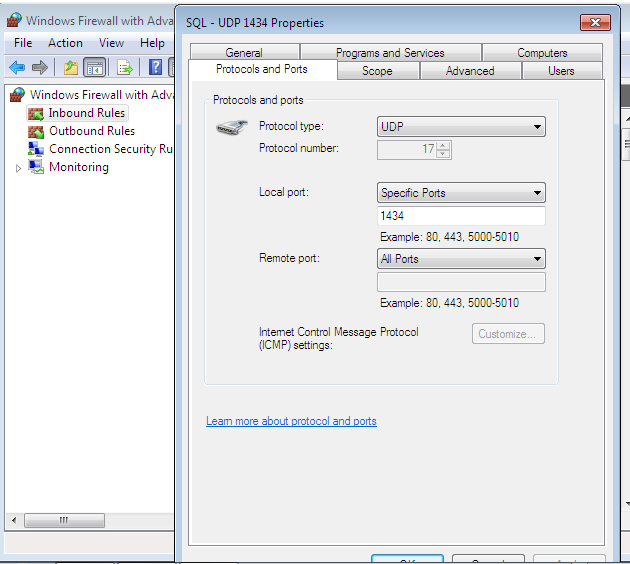
Select Port

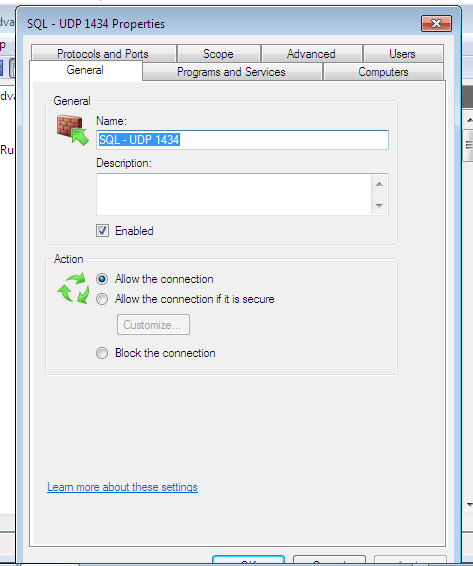
Select UDP and specify port 1434

Allow the connection

Choose all three profiles (Domain, Private & Public)

Name the rule “SQL – UDP 1434





A program exception for sqlservr.exe. Click New Rule again and use the following information to create a program exception:

Select Program

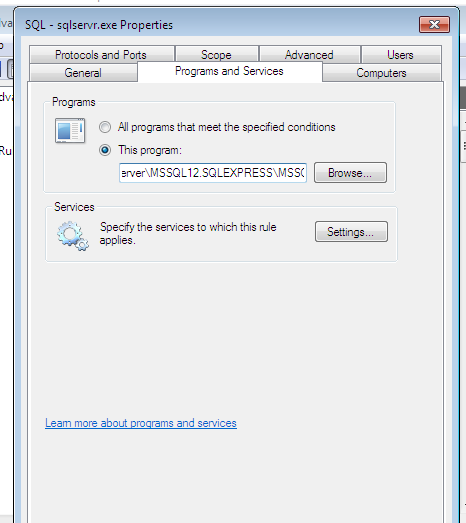
Click Browse to select ‘sqlservr.exe’ at this location:

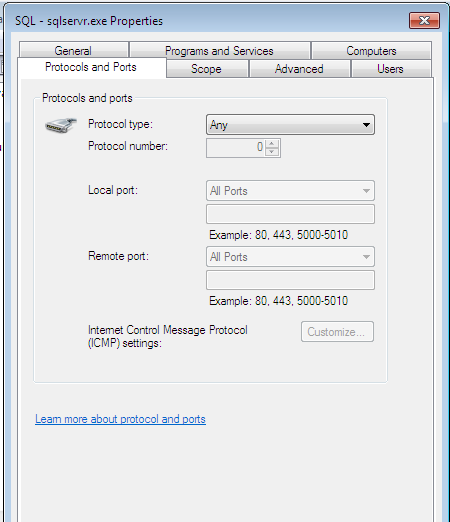
[C:\Program Files\Microsoft SQL Server\MSSQL11.<INSTANCE\_NAME>\MSSQL\Binn\sqlservr.exe] where <INSTANCE\_NAME> is the name of your SQL instance.

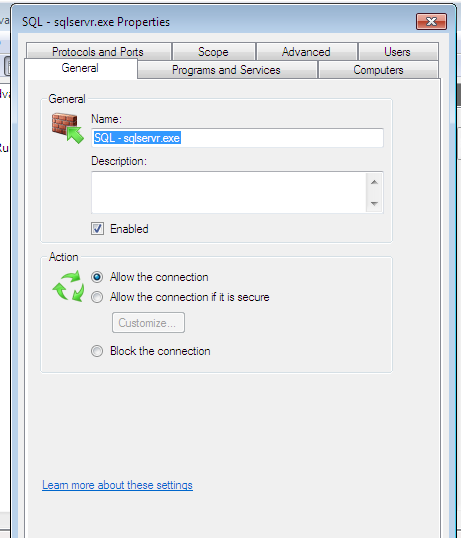
Allow the connection

Choose all three profiles (Domain, Private & Public)

Name the rule SQL – sqlservr.exe







A program exception for sqlbrowser.exe Click New Rule again and use the following information to create another program exception:

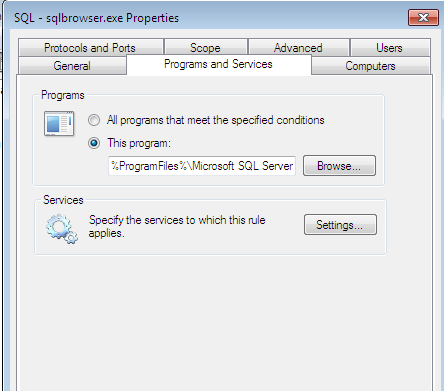
Select Program

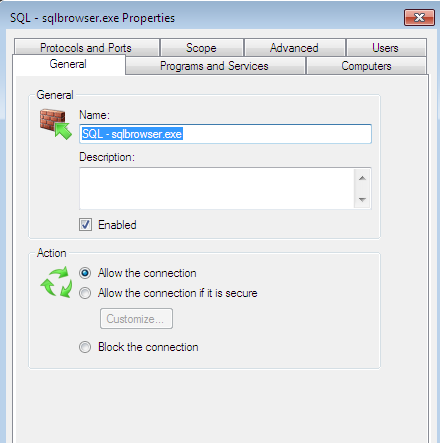
Click Browse to select sqlbrowser.exe at this location: [C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe].

Allow the connection

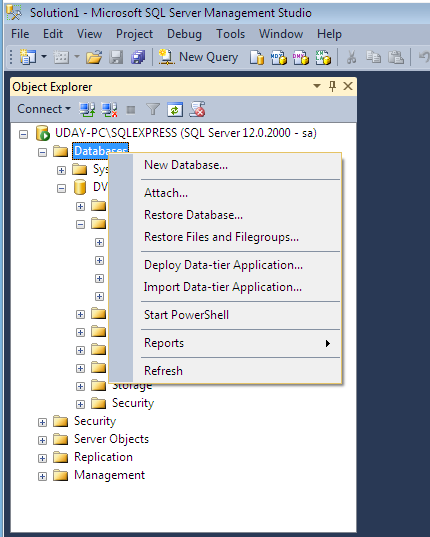
Choose all three profiles (Domain, Private & Public)

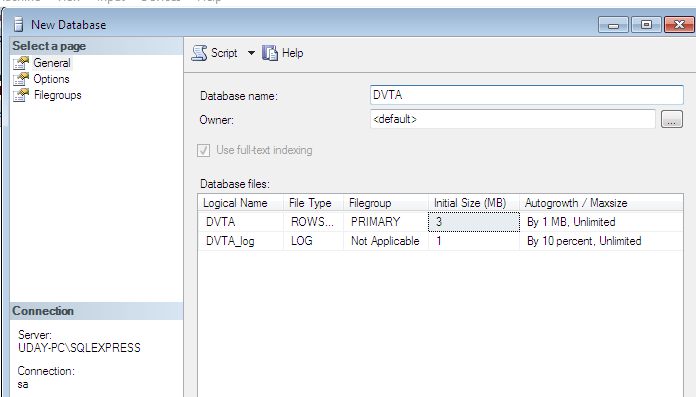
Name the rule SQL – sqlbrowser.exe

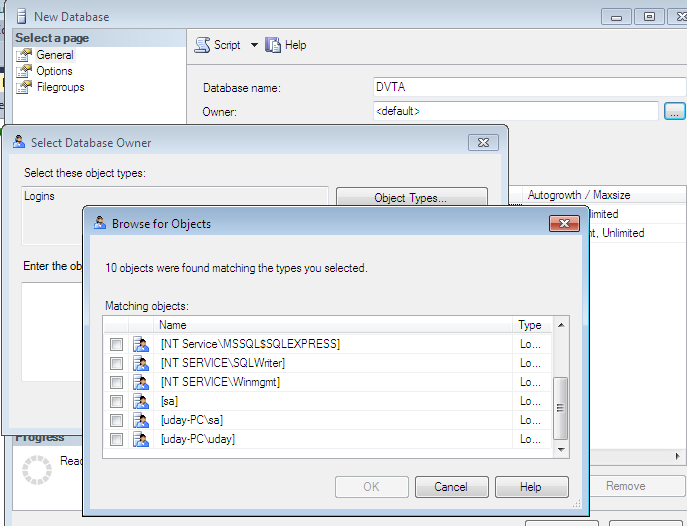


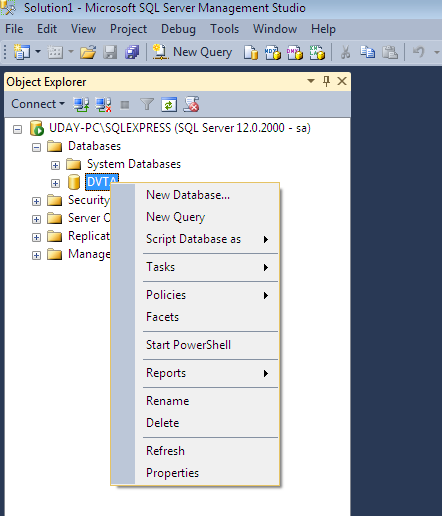


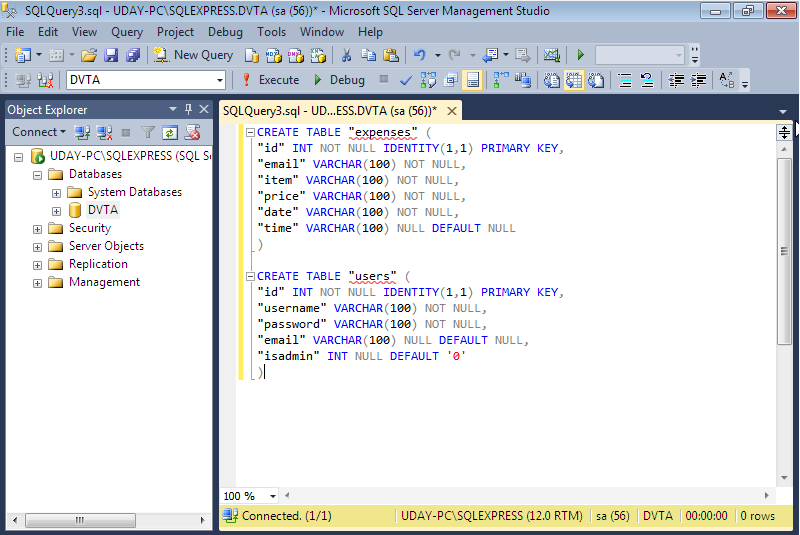
Now that the SQL Server is setup to receive and service requests it is time to create the database.











CREATE TABLE "expenses" (

"id" INT NOT NULL IDENTITY(1,1) PRIMARY KEY,

"email" VARCHAR(100) NOT NULL,

"item" VARCHAR(100) NOT NULL,

"price" VARCHAR(100) NOT NULL,

"date" VARCHAR(100) NOT NULL,

"time" VARCHAR(100) NULL DEFAULT NULL

)

CREATE TABLE "expenses" (

"id" INT NOT NULL IDENTITY(1,1) PRIMARY KEY,

"email" VARCHAR(100) NOT NULL,

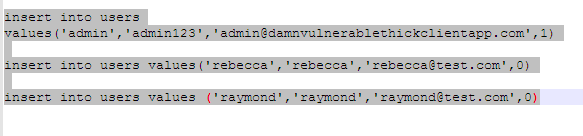
"item" VARCHAR(100) NOT NULL,

"price" VARCHAR(100) NOT NULL,

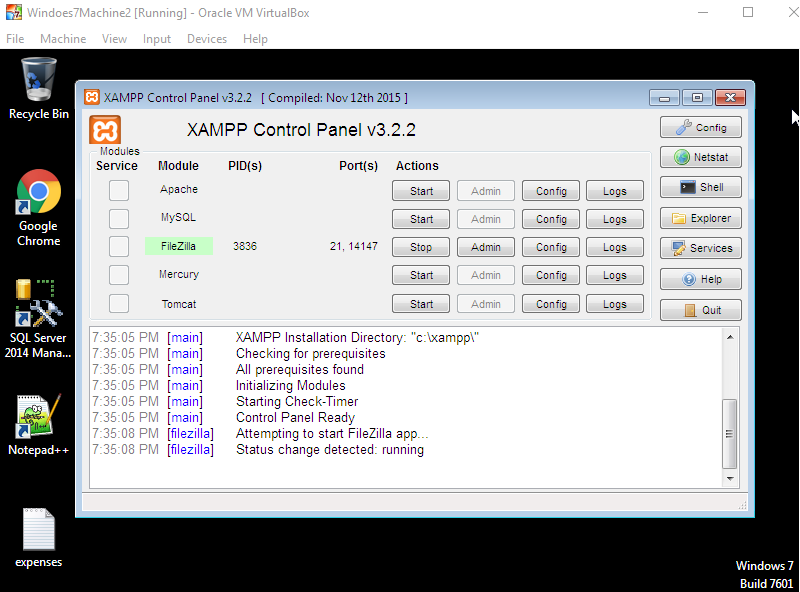
"date" VARCHAR(100) NOT NULL,

"time" VARCHAR(100) NULL DEFAULT NULL

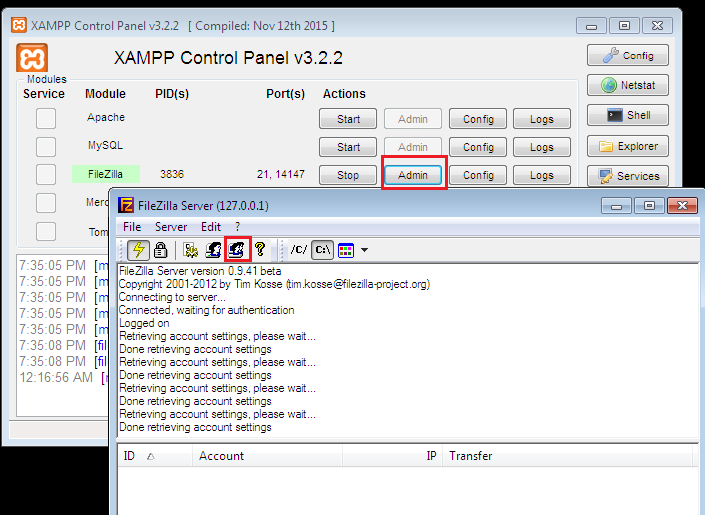
)

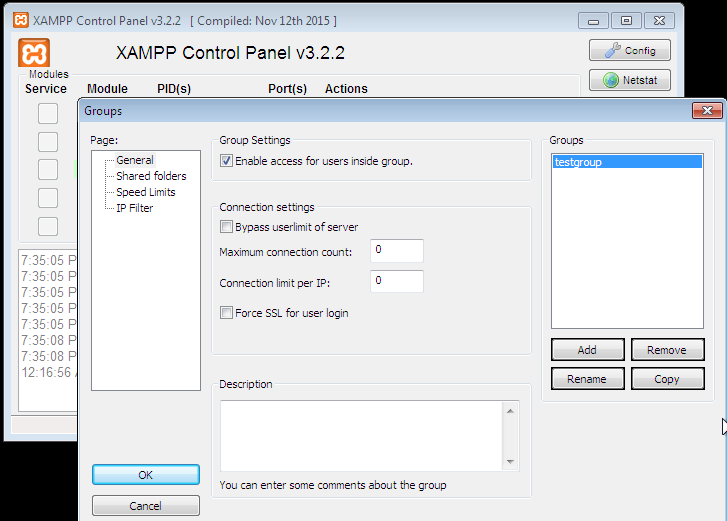


FTP Server Configuration:



Click on Admin and then Groups as shown below and then click on Add and create a group called “testgroup” and select “Enable access for users inside group”.





Next Click on “user” and create a user called “dvta” and with the password “p@ssw0rd” and assign this user to the group membership “testgroup”. Also assign a shared folder on this machine. This is the location where ftped files will be available.

