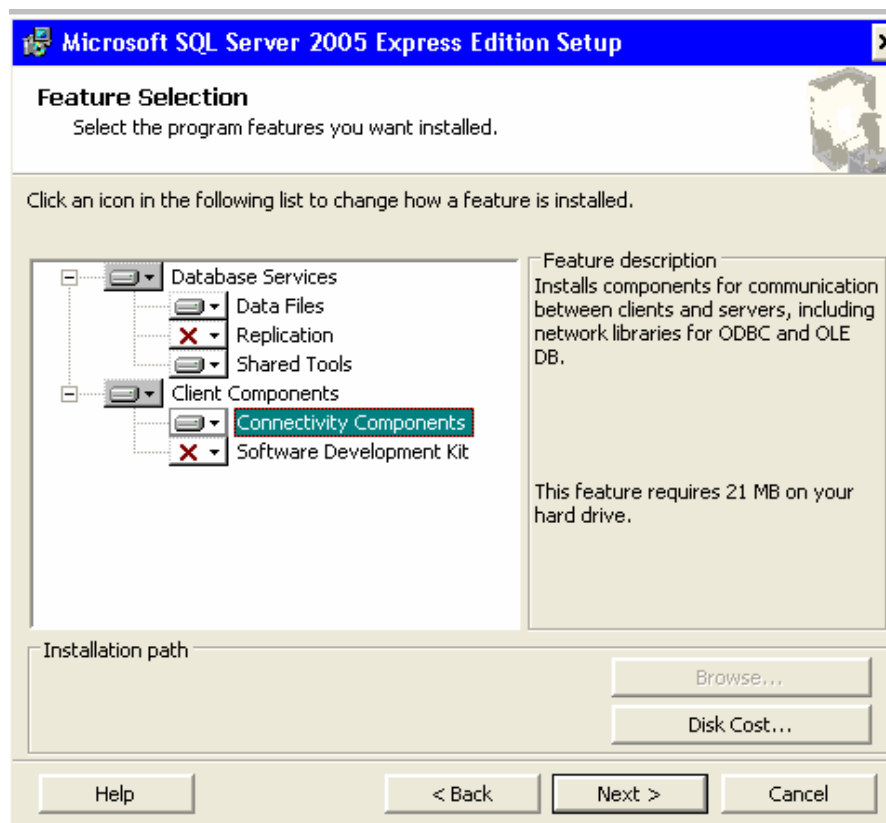


SQL Serveri paigaldus

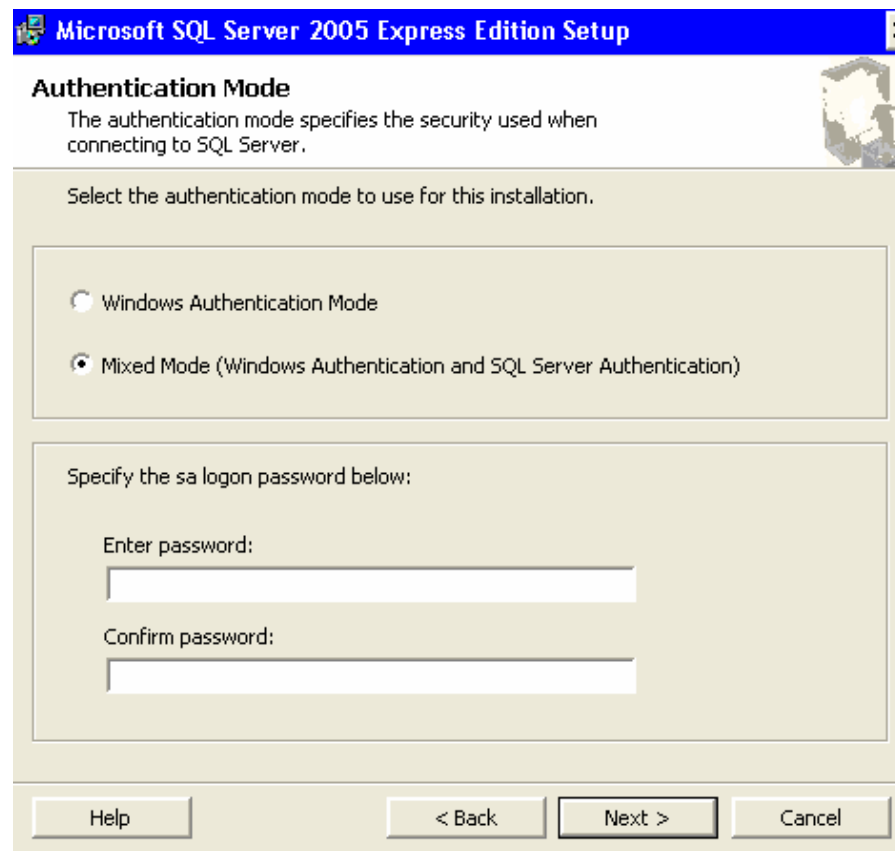
Laadimine: <http://msdn.microsoft.com/vstudio/express/sql/download/>

Tasub paigaldada kõige lihtsam versioon (SQL Server 2005 Express Edition SP2). Samalt lehelt saab laadida ka Sql Serveri haldamise vahendi (SQL Server Management Studio Express) aga üldjuhul seda vaja ei lähe.

Peale tüüpiliste seadete valimisi jõuate järgmise pildini. Siin on soovitatav valida Connectivity Components ja määrata "Will be installed on local hard drive". Kui on soov muuta ka SQL Serveri andmete asukohta siis võib Data Files real, browse nupule vajutades, valida andmetele sobiv kataloog.



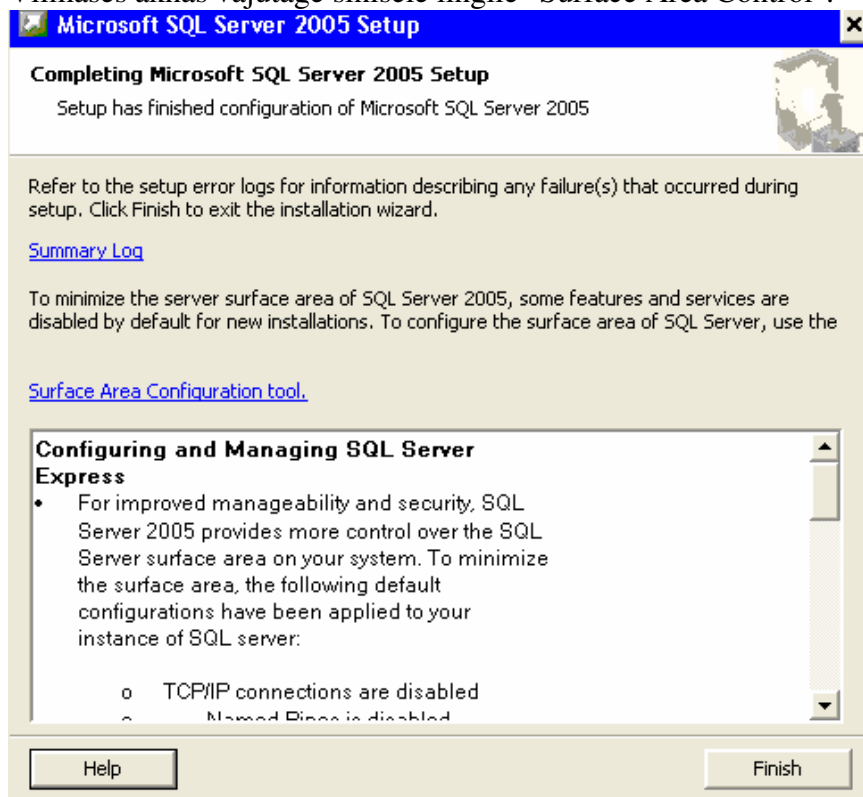
Järgnevalt küsitakse autoriseerimise viisi ja administraatori parooli. Valige Mixed Mode ja kindlasti täitke ära ka administraatori parool. Kui teil on hiljem soov kasutada serverit üle interneti, siis pikk ja keeruline parool on ainus, mis kaitseb teie andmetele ligipääsu internetist.



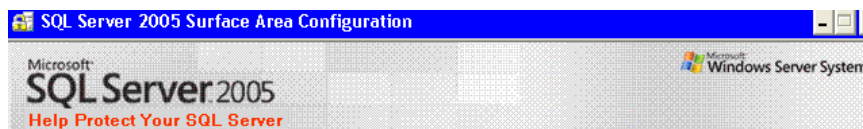
The image shows a screenshot of the 'Microsoft SQL Server 2005 Express Edition Setup' dialog box. The title bar is blue with the text 'Microsoft SQL Server 2005 Express Edition Setup'. The main window has a light beige background. At the top left, the text 'Authentication Mode' is displayed in bold. Below it, a smaller text explains: 'The authentication mode specifies the security used when connecting to SQL Server.' To the right of this text is a small icon of a person's head and shoulders. Below the explanation, the instruction 'Select the authentication mode to use for this installation.' is shown. There are two radio button options: 'Windows Authentication Mode' (which is unselected) and 'Mixed Mode (Windows Authentication and SQL Server Authentication)' (which is selected). Below these options, the text 'Specify the sa logon password below:' is displayed. This is followed by two text input fields: 'Enter password:' and 'Confirm password:'. At the bottom of the dialog box, there are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a dark border.

Järgmised dialoogid jätta nii nagu paigaldusprogramm pakub ja viige paigaldus lõpuni.

Viiimas aknas vajutage sinisele lingile "Surface Area Control".



Sealt vajutage lingile "Surface Area Configuration for Services and Connexion



Minimize SQL Server 2005 Surface Area

SQL Server 2005 improves manageability and security by giving administrators more control over the surface area of local and remote instances of SQL Server 2005. With the SQL Server 2005 Surface Area Configuration tools, you can easily:

- Disable unused services and network protocols for remote connections.
- Disable unused features of SQL Server components.

For new installations, use these tools to enable required features, services, and network protocols that are disabled by default. For upgraded instances, use these tools to identify and disable unused features, services, and protocols.

Users with administrative privileges on Microsoft Windows Vista and later versions will no longer have administrative privileges on this SQL Server installation by default. To explicitly add yourself as a SQL Server administrator, click on the below link:

 [Add New Administrator](#)

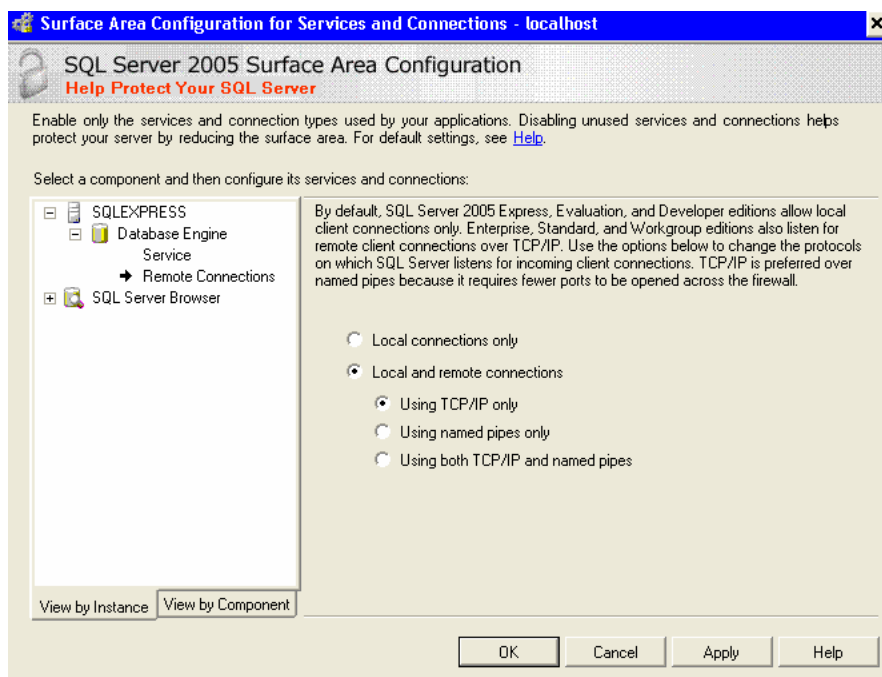
 [Read more about configuring the SQL Server surface area.](#)

Configure Surface Area for localhost [\[change computer\]](#)

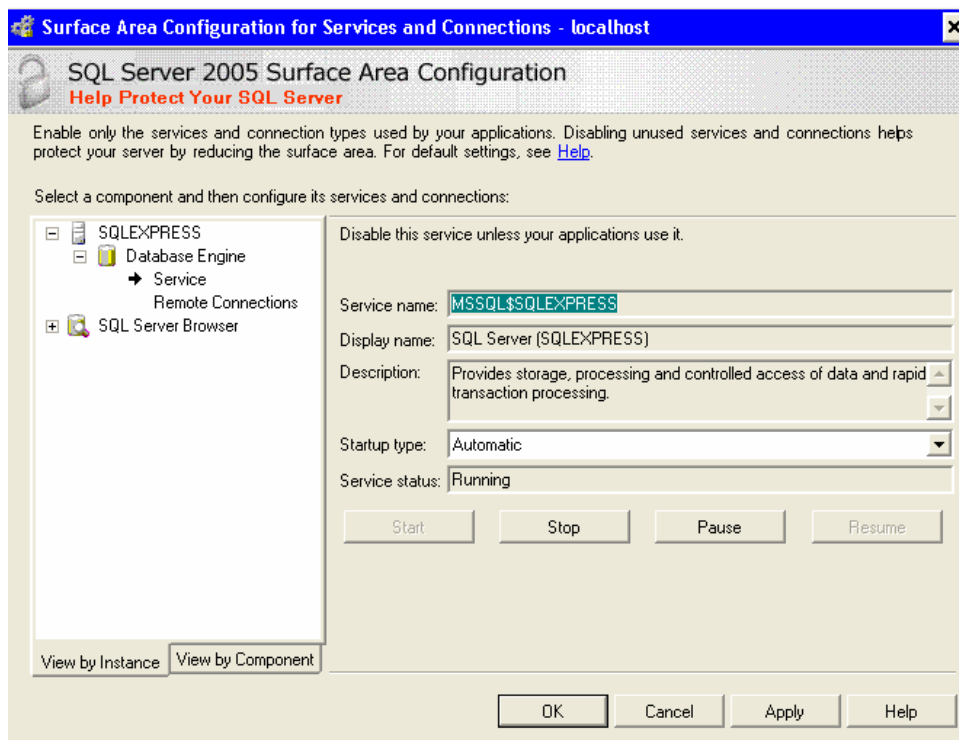
 [Surface Area Configuration for Services and Connections](#)

 [Surface Area Configuration for Features](#)

Avaneb uus aken, kust aktiveerige rida Remote Connection ja määrake: Local and remote connection ning Using TCP/IP only.



Peale OK vajutust programm ütleb, et muudatused ei mõju enne SQL-I uuesti käivitust. Et SQL uuesti käivitada aktiveerige Service link ja seal aknas vajutage Stop ja seejärel Start

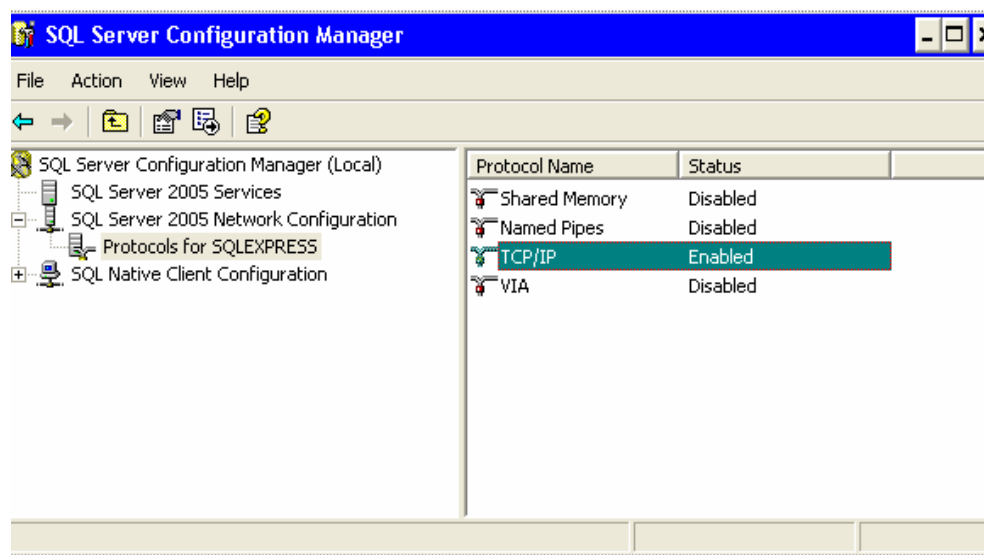


Sulgege nüüd vahepeal avanenud lisaaknad ja vajutage Finish.

Kui soovite SQL serveri andmeid kasutada üle võrgu, siis peate tulemüüris lubama ka 1433 pordi.

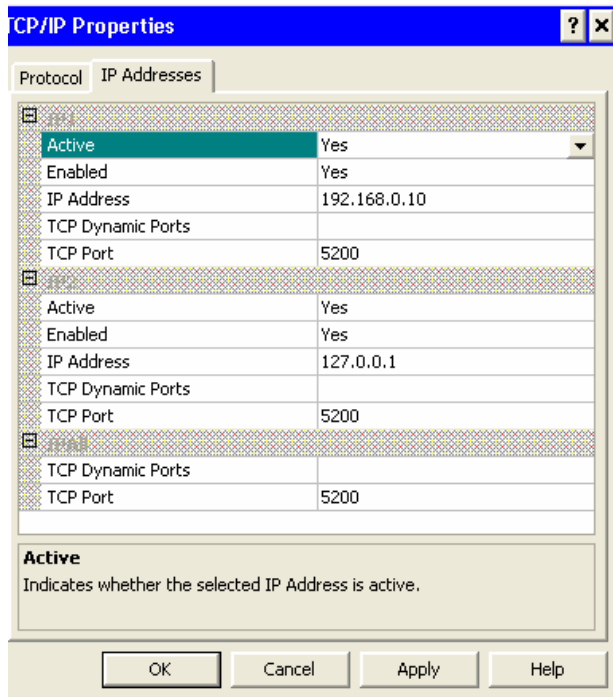
IP pordi muutmine

Avage SQL Server Configuration Manager, valige vasakult SQL Server 2005 Network Configuration ja Protocols for SQLEXPRESS. Paremal tehke TCP/IP real hiirega topeltklõps.



Uues avanevas aknas avage IP Addresses lehekülj ja vaadake et kõigil IP gruppidel oleks Active Yes ja Enabled YES. TCP Dynamic Ports rea peab ära kustutama ja TCP Port reale kirjutama soovitud pordi numbri. Pordi numbrid võivad olla vahemikus 1000 kuni 65536. Nüüd peaks siis tegema SQL service-le restardi ja muutma tulemüüris lubatud pordi ka uueks.

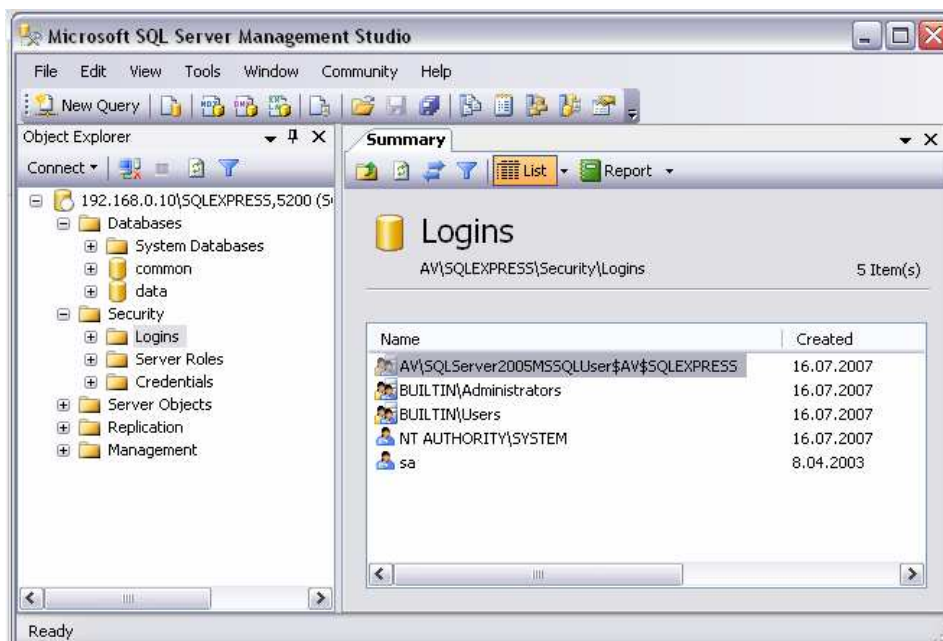
SQL Server Management Studio-s serveriga ühenduseks tuleks serveri nimi kirjutada kujul: 192.168.0.10\SQLEXPRESS,5200



SQL serveri kasutaja lisamine

Joosep suhtleb SQL serveriga kasutades ühte etteantud kasutajanime. Esimesel serveri poole pöördumisel küsitakse kasutajalt SQL serveri kasutajanime ja parooli ning kui need sobivad, siis programm salvestab need kodeeritult common kataloogi sqluser.txt faili. Sellel kasutajal peaksid olema päris suured õigused, et ta saaks uusi andmebaase luua ja vajadusel ka baasidest tabelleid kustutada. Võib kasutada ka algselt SQL Serveri paigaldusel loodud Administraatorit (sa) ja tema parooli, aga turvalisuse huvides on soovitatav luua uus kasutaja ja sa hiljem ümbernimetada.

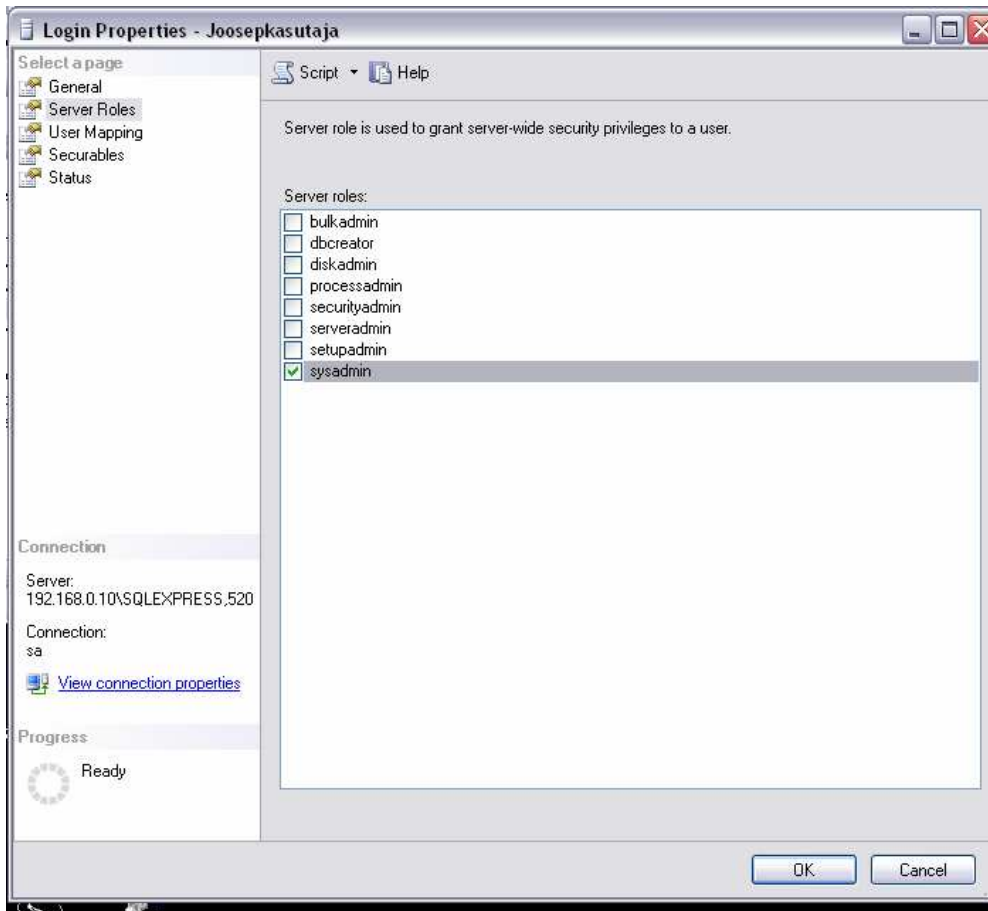
Uue kasutaja lisamiseks avage SQL Server Management Studio, avage Security ja vajutage seal all Logins real hiire paremat nuppu ja valige New Login.



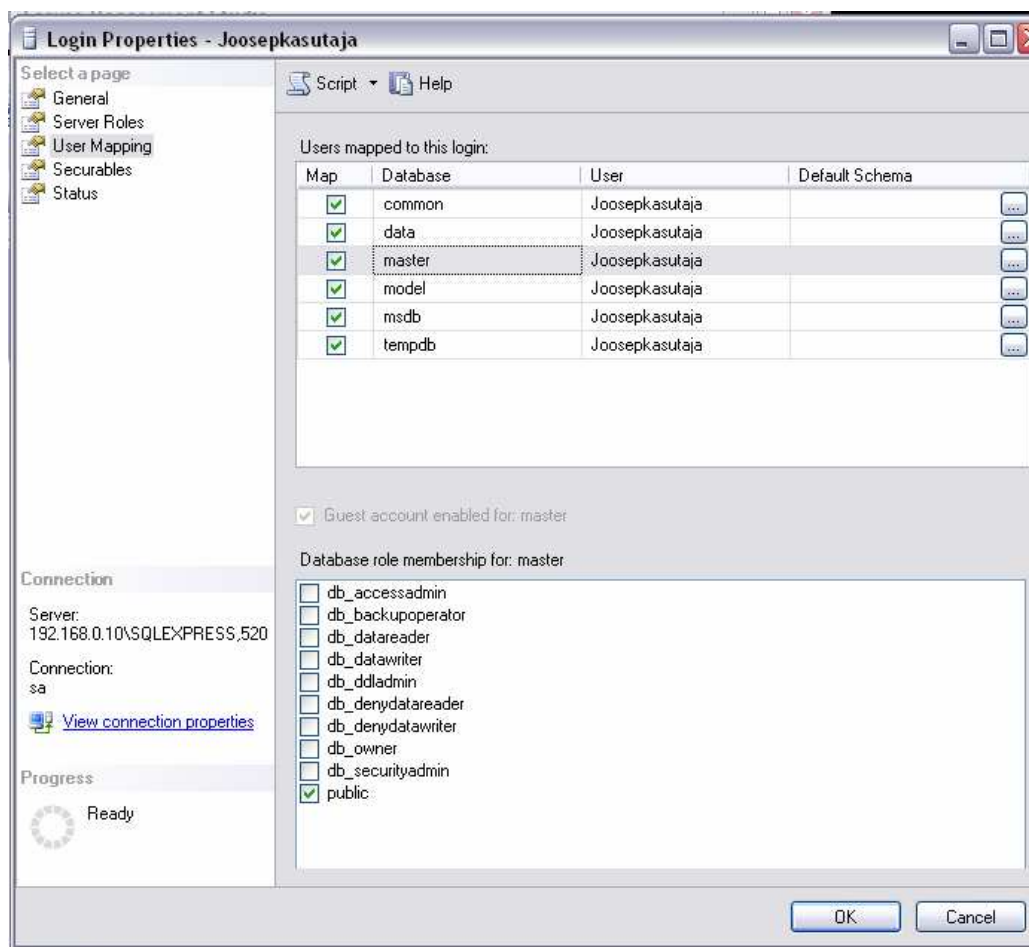
Uue kasutaja lisamise aknas täitke kasutaja nimi (Login name), pange märke "SQL Server authentication" ette ja kirjutage kaks korda soovitud parool. Võtke ka ära linnuke "Enforce password expiration" eest

7/7 At 2,5 cm Ln 1 Col 1 REC TRK EXT OVR Estonian

Valige vasakult "Server Roles" ja pange märke "sysadmin" ette.



Seejärel aktiveerige vasakult "User Mapping" ja pange märke kõigi andmebaaside ette. Seejärel vajutage OK.



Nüüd on soovitatav ka sa nimelise kasutaja nimi ära muuta, et .pahatahtlikel sisenede püüdjatel oleks raskem kasutajanime ära arvata. Selleks vajutage sa nimel hiire paremat nuppu ja valige "Rename"

Siiski jääb lahendamata veel see probleem, et andmed liiguvad üle interneti lahtiselt. Selle lahenduseks on kasutada VPN tarkvara, SSH-d või ka SQL serveri enda SSL krüpteerimist. Viimase kohta võib lugeda allpool toodud ingliskeelset teksti. SSL krüpteeringu aktiveerimiseks Avage SQL Server Configuration Manager, valige vasakult SQL Server 2005 Network Configuration ja vajutage real Protocols for SQLEXPRESS hiire paremat nuppu ja määrake avanevast aknast Force Encryption = Yes

SSL in SQL Server 2005 [Il-Sung Lee]

I often receive questions inquiring about the (channel) encryption capabilities in SQL Server 2005. Like SQL Server 2000, 2005 can use SSL (Secure Socket Layer) to secure transmissions over the wire independent of the network protocol used. However, unlike its predecessor, SQL Server 2005 will always make encryption available, even if the administrator hasn't provisioned a SSL certificate on the server machine. For this reason, SQL Server 2005 can and will ensure that the login packet is encrypted even if encryption hasn't been explicitly

turned on. More precisely, unless either the client or the server requests encryption, the channel will not be encrypted beyond the login packet.

How? When initializing SSL support at startup time, the server will use the following order to load a certificate:

1. Use the certificate that the administrator has specified in the SQL Server Configuration Manager (right-click on "Protocols for <instance>" under "SQL Server 2005 Network Configuration" and then select the "Certificate" tab)
2. If no certificate has been specified, the server will search the machine and user's certificate store for an appropriate certificate. The following KB article explains what the server considers a valid certificate, <http://support.microsoft.com/default.aspx?scid=kb;en-us;318605>. (Note that the article was written for SQL Server 2000 but the criteria for a valid server certificate are still employed by SQL Server 2005.)
3. If nothing appropriate can be found, the server will generate a self-signed certificate.

Any other implications? The auto-generation of a certificate is a new feature to SQL Server 2005 and is the reason why encryption will be available even though a SSL certificate has not been provisioned on the server machine. This certificate can be used for full channel encryption but with one caveat. If the client is the one requesting encryption, then it will attempt to perform server validation on the certificate to verify the identity of the server machine. This is a prudent security practice but is impossible to do with a self-signed certificate since it hasn't been signed by a trusted root authority. To overcome this problem, the client may specify the "Trust Server Certificate" flag to override the server validation. Alternatively, you can turn encryption on at the server and leave the client encryption flag off to enable channel encryption.

Conclusion: Whether or not you need channel encryption depends entirely upon your system security requirements and performance tolerance. But one of the nice features of SQL Server 2005 is that it will always be available even if you haven't installed an SSL certificate on the machine (although I still strongly recommend using a certificate signed by a trusted authority whenever possible).