Vermont Oxford Network – eNICQ 6 Documentation

eNICQ 6 System Administrator's Guide

Release 1.0

Published August 2019

Vermont Oxford NETWORK

eNICQ 6 System Administrator's Guide

Introduction

eNICQ has been created to be a true client/server application using Microsoft® SQL Server® or SQL Server Express® as a database back end. This requires that the client application eNICQ can communicate over the network to this back end database and that this back end database provides a service to the network. This document is intended to help Systems Administrators secure the eNICQ 6 installation and to help deploy eNICQ 6 in a more manageable way. There are 5 sections outlined below:

This guide is intended for System Administrators. It is intended to provide supplementary information necessary to install eNICQ 6 in diverse environments. Throughout this guide it is expected that the reader has a base level of technical knowledge required to implement Microsoft® Windows® networks, support Microsoft® SQL Server®, configure firewalls, perform network level scripting and make security related decisions.

Technical Assistance

If any assistance is needed or if you have questions, you can contact Vermont Oxford Network's eNICQ Technical Support Team in one of the following ways:

EMAIL: support@vtoxford.org

Phone: 802-865-4814 (extension 240, or ask the operator for eNICQ Technical Support)

System Requirements

eNICQ 6 Client Software, installed locally

- Supported Operating Systems: Windows® 7, Windows® 8.1*, Windows® 10*
- Microsoft® .NET Framework version 4.6.1*
- At least 400 MB of free disk space
- At least 1 GB of RAM
- Installer and client require Internet connection open to vtoxford.org and all subdomains on ports 80 and 443. This connection must accommodate a RESTful API web service (.svc)

*Depending on configuration, Windows® 8.1 and Windows® 10 may require installation of .NET Framework 4.6.1.

Microsoft® SQL Server® Express 2012, installed locally

- Supported Operating Systems: Windows® 7, Windows® Server 2008 R2, Windows® Server 2008 Service Pack 2, Windows® 10
- 32-bit systems
  - Computer with Intel or compatible 1GHz or faster processor (2 GHz or faster is recommended.)
- 64-bit systems
  - 1.4 GHz or faster processor
- Minimum of 512 MB of RAM (2 GB or more is recommended.)
- 2.2 GB of available hard disk space
- For more information on SQL Server® Express 2012, please visit the Microsoft® site: https://www.microsoft.com/en-us/download/details.aspx?id=29062

-or-

Microsoft® SQL Server® 2012 or higher, existing Standard or Enterprise Edition

- Supported SQL Server® Versions: 2012 or higher
- Maximum anticipated database size of 1 GB

Protected Health Information and HIPAA

Confidential patient data items are stored in your local eNICQ 6 database. Patient identifiers are protected health information as specified in the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations implementing HIPAA. eNICQ 6 has been designed to ensure that patient identifiers cannot be sent to Vermont Oxford Network ("VON") unless the submitting member has the appropriate agreement(s) in place with VON. Hospitals in the US must implement measures to protect protected health information from unauthorized access, as specified in the HIPAA Privacy and Security regulations. Users of eNICQ software should be sure to comply with local hospital policies and good information security practices to protect data in the eNICQ database. Hospitals outside of the US should work with their legal and information security departments to determine the appropriate safeguards required in their jurisdiction(s).

To avoid access to the eNICQ 6 tables by unauthorized personnel, system administrators should review the security options available in this guide and ensure that the application is implemented to be accessible only to hospital staff members who have permission to access the data.

If you are unsure about the sufficiency of your information security safeguards, or have any difficulty implementing the instructions in the guide, please consult your IT department or a qualified information security professional for assistance, in order to avoid and prevent HIPAA violations and potential breaches of information security.

Chapter 1: Authentication and User Roles

There are two levels of authentication to eNICQ 6: client authentication and database authentication. Application access depends on successful authentication at both levels.

Client Authentication

Authentication to the eNICQ 6 client can be managed in one of two ways. One option is for your VON Services Administrator would assign either the eNICQ User or eNICQ Admin role to users from the Manage Users page in the Member's Portal on our website, https://admin.vtoxford.org/.

It is also possible to set up the eNICQ 6 client authentication to use your Active Directory. In order to use your Active Directory user or group accounts for login to eNICQ 6, create an eNICQ User and an eNICQ Admin group in your Active Directory for each center added to the database:

- Enicq User – This level of access provides users with all the functionality needed to enter new records, view existing records, and submit data to Vermont Oxford Network.
- Enicq Admin – This level of access provides users with full application functionality, along with access to some additional tools.

You can call the groups whatever fits your naming conventions although they cannot have any spaces in the names. The installer will ask you for the group names if you select to use Active Directory logins. It will also ask you for AD group names whenever you add a new Center to the database using the client application from the Center Management window in the eNICQ 6 Client Application. You can edit the group names by rerunning the installer, by editing the Center in the Center Management page in the application, or by editing the **ADAdminGroup** or the **ADUserGroup** fields on tbl.Center in the eNICQ 6 database.

Once you have created both of the eNICQ 6 Active Directory groups, add existing Active Directory users or user groups to provide the level of access appropriate for each of your eNICQ 6 application users. After you have completed this setup, when users who have been added to an eNICQ 6 Active Directory group launch eNICQ 6, they will be logged in based on their Active Directory credentials, and will not need to manually log in to eNICQ 6.

Removing access privileges requires removing the user's account from the eNICQ 6 Active Directory group.

Database Authentication

In eNICQ 6, the front-end application communicates with the SQL Server® or “back end.” This requires authentication. By default, the installation uses SQL Server® authentication to connect to the back end.

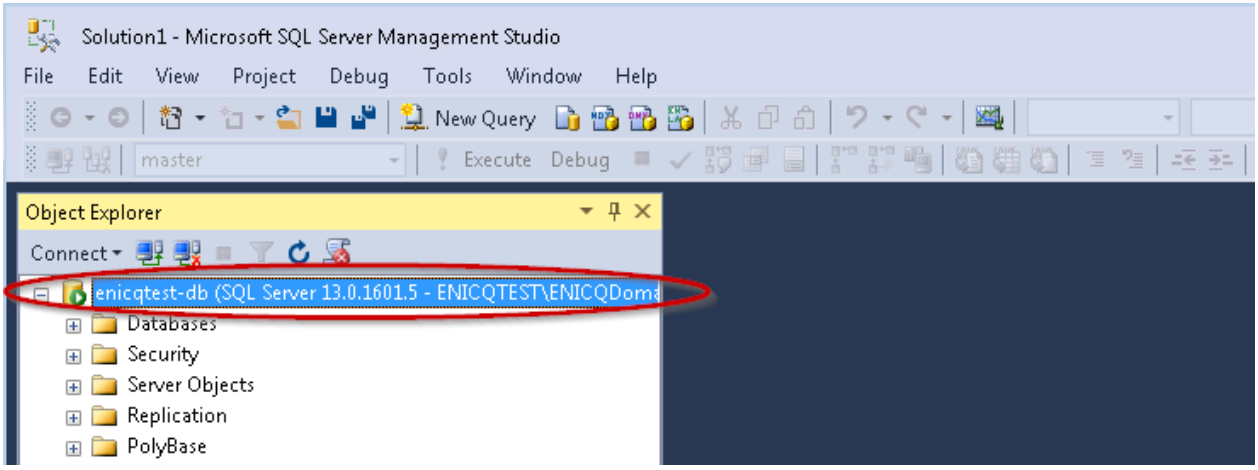
There are many ways to secure authentication. This guide describes what needs to be secured and provides instructions for implementing security measures using standard practice in a pure Microsoft® Windows® environment. You may need to adjust these instructions to fit your environment. These instructions assume that all computers are in the same domain, or if multiple domains are used, it assumes that the domains have trust relationships that allow for authentication to cross domains. If you are running the full version of SQL Server® 2012 or higher, these authentication settings may already be in place, but this documentation should still be reviewed by the SQL Server® Administrator.

Set SQL Server for Windows® Only Authentication

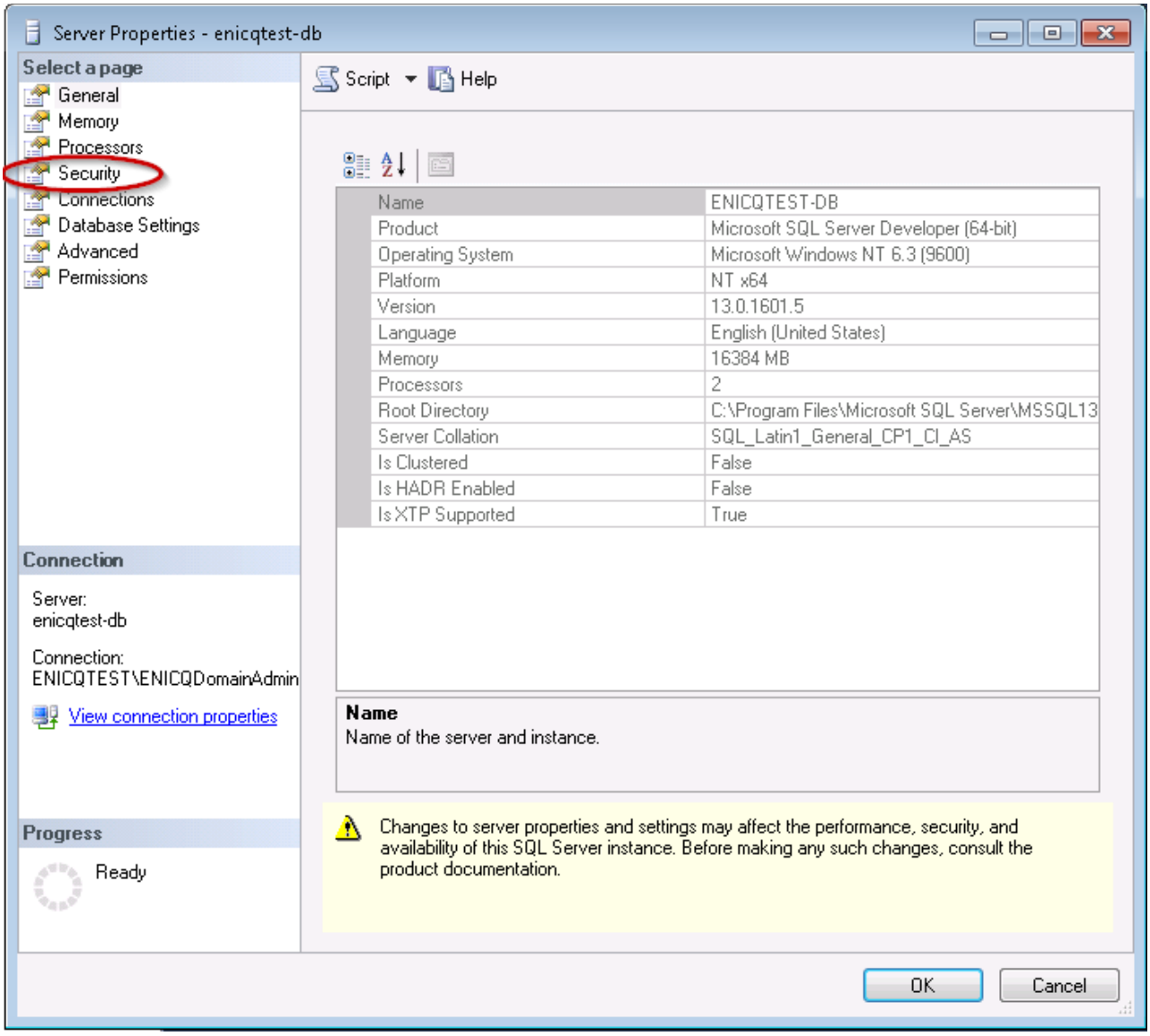
The first thing that we recommend is to set SQL Server® to use only Windows® Authentication. There are two possible authentication mechanisms for SQL: Windows® Authentication, or SQL Authentication and Windows® Authentication. By default, the SQL Server Express® Database is set to use both SQL Authentication and Windows® Authentication. If you set the authentication mode to Windows® Authentication only, the system will use all of your Microsoft® Windows® domain settings to authenticate the user. When set properly, these settings can greatly enhance the security of any network. Please see the Microsoft® knowledge base for more information regarding authentication in a Microsoft® Windows® environment.

To set the server to use only Windows® Authentication, open the SQL Server® Management Studio Express as an administrator and connect via Windows® Authentication to the computer that runs the SQL Server Express® Database.

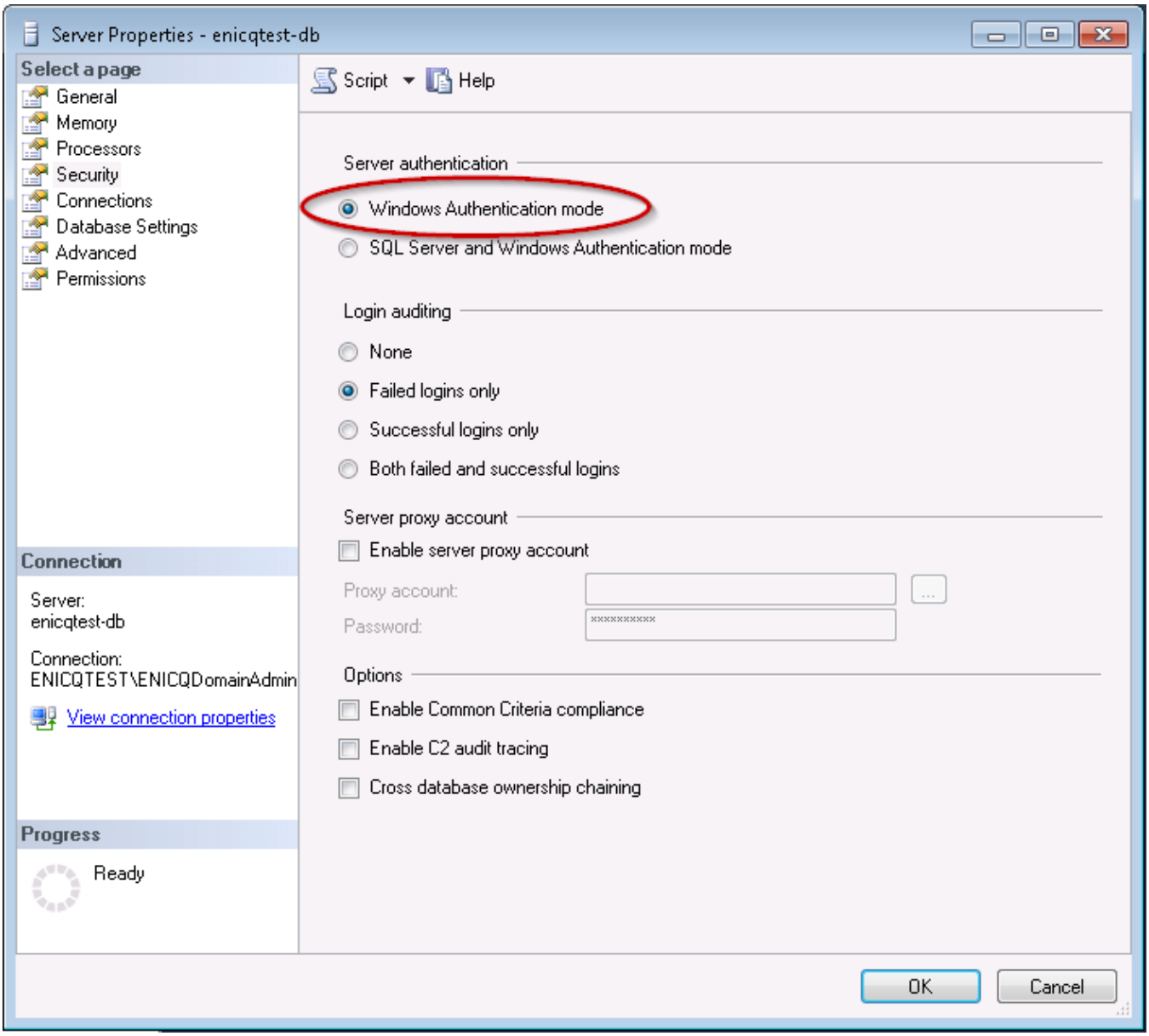
Right-click on the database server (circled in red below), and select **Properties**.



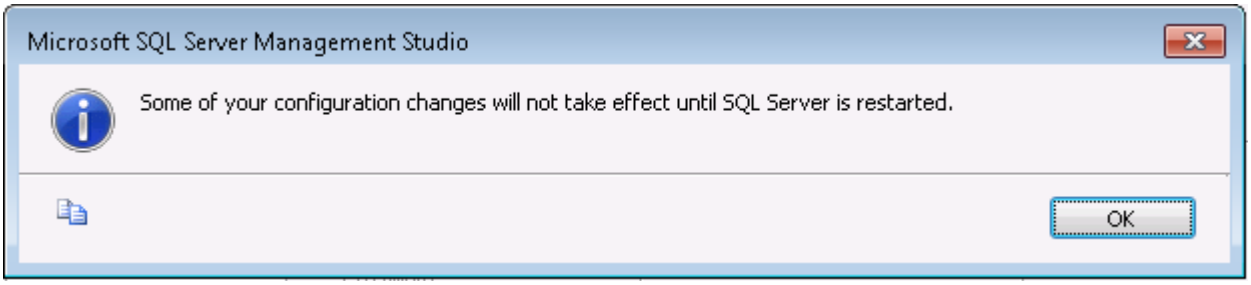
Within the Server Properties settings, choose **Security** from the left sidebar under **Select a page:**



Under **Server authentication**, select **Windows® Authentication mode**.



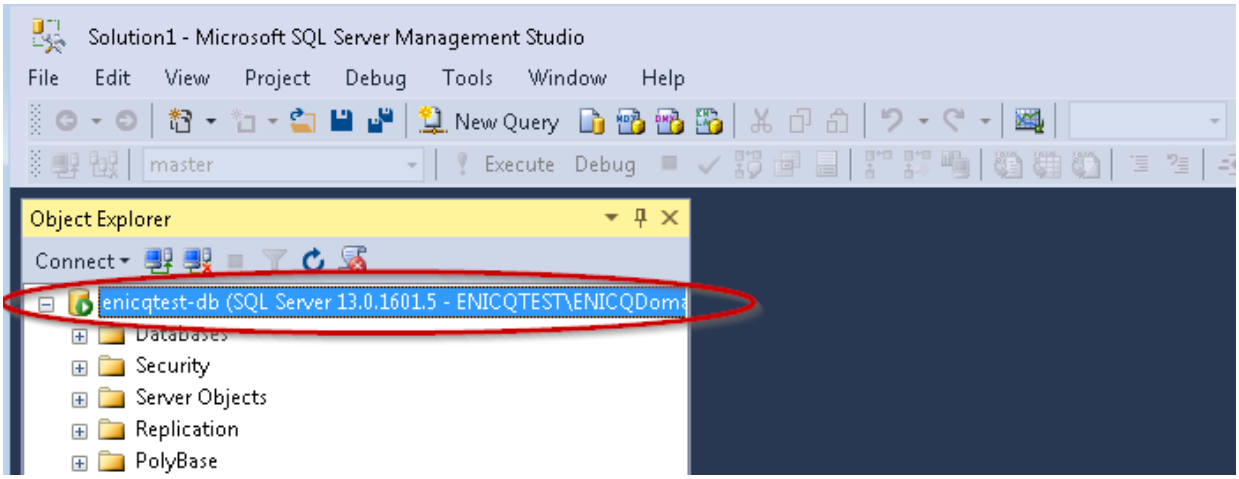
Click **OK**. You will get a message stating that you need to restart the SQL Server®.



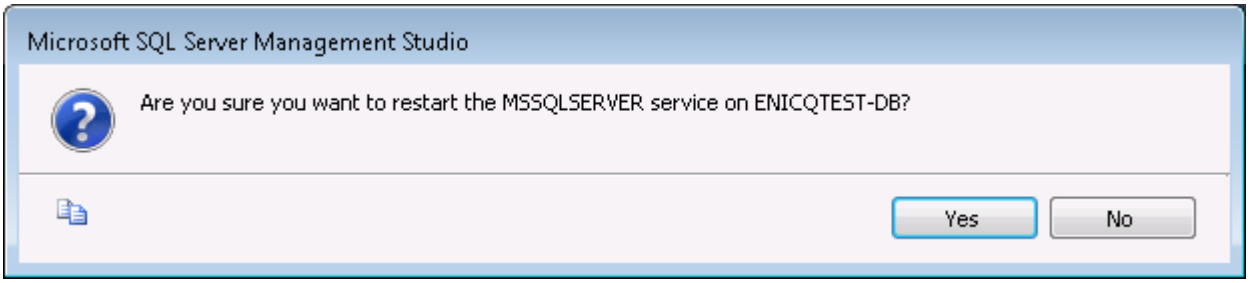
Click **OK**.

Restart the SQL Server® to apply these changes. Since you are in the SQL Server®

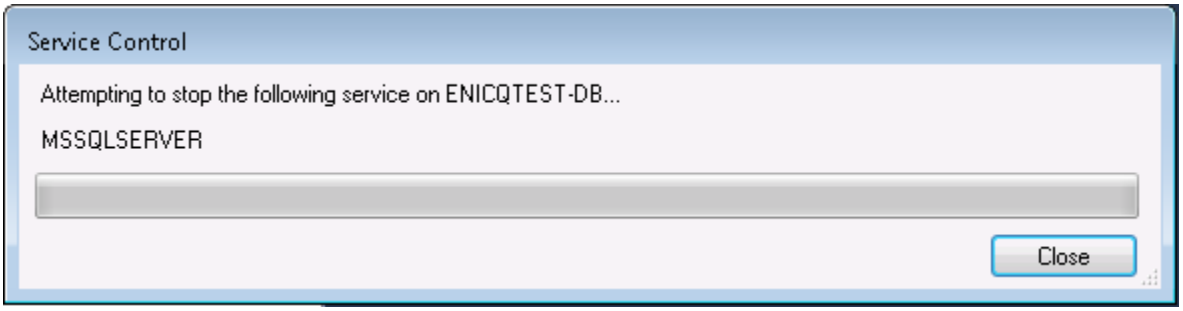
Management Studio, the easiest way to do this is to right-click on the database server again and select **Restart**.



You will get a message asking if you really want to restart. Click **Yes**.



The **Service Control** dialog will show the database restart progress:



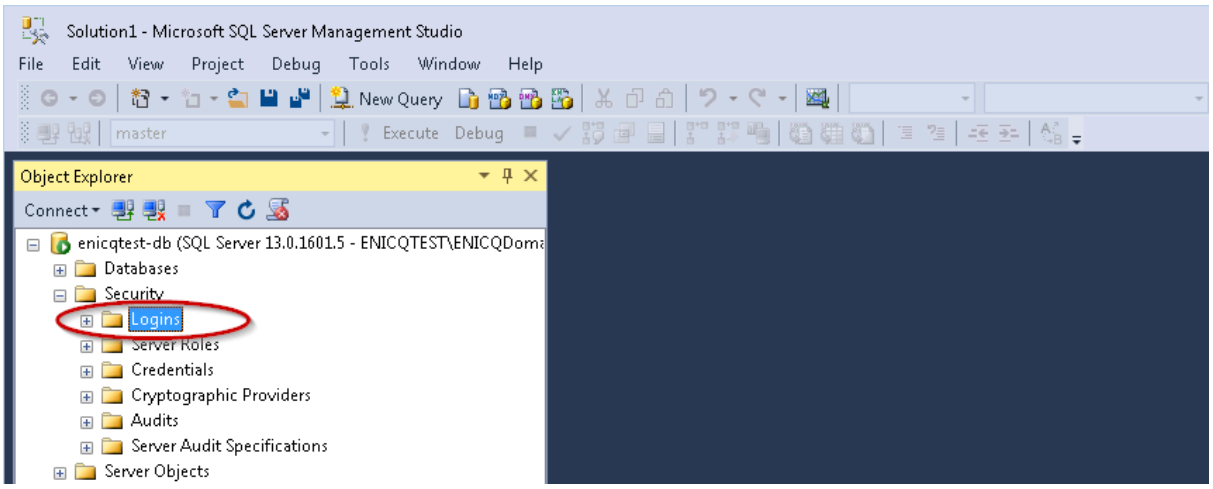
Wait until this task is done. Now the server will be set to use Windows® Authentication only.

Add Windows® Account/Group Access to Database

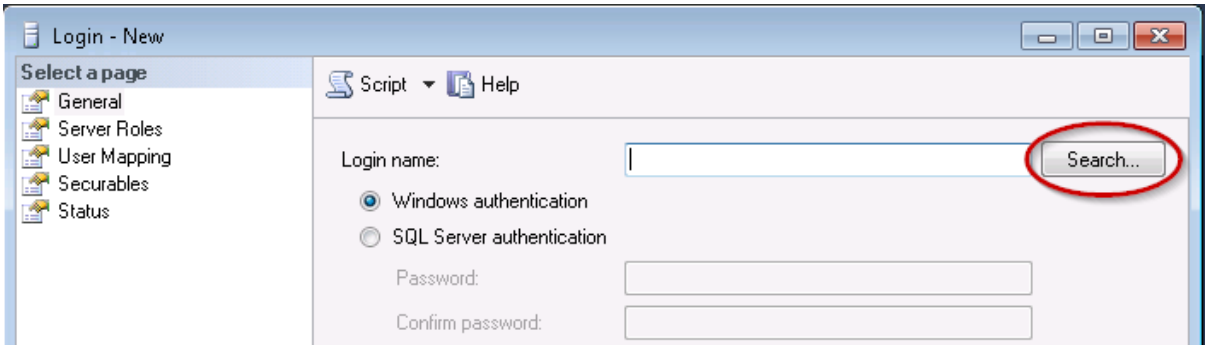
You must now add in the Windows® accounts and/or groups that will use the eNICQ 6 client application and give them the EnicqDBUser permission. You may choose to have a group of users added to a Windows® Group and assign them EnicqDBUser role instead. This may be a better design for your environment. Please check with your System Administrator for advice on Windows® Groups.

It also should be noted that administrative access to the database is now based on which users have administrative access to the local database machine. By default, this would mean that all Domain administrators and any users added to the local administrators account on the database server machine will be administrators of the eNICQ 6 database and therefore have full control of the data.

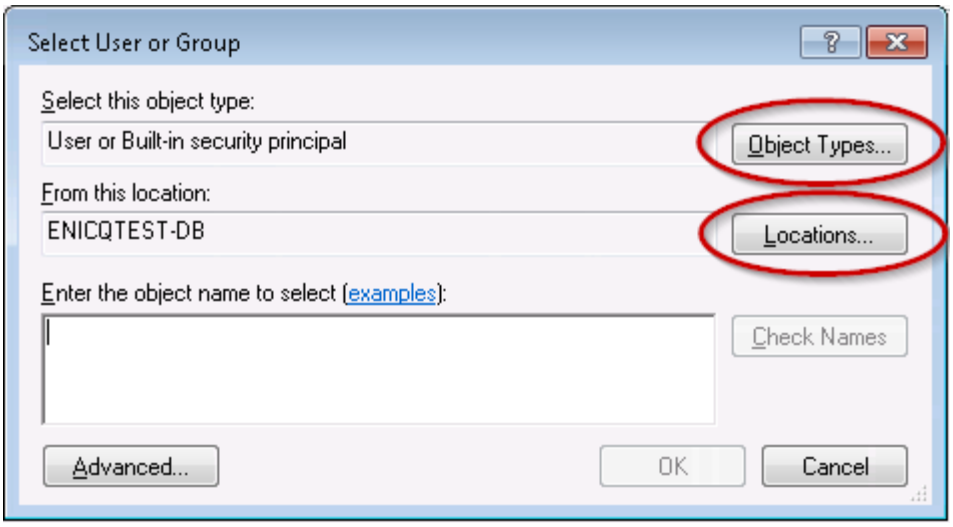
Inside SQL Server® Management Studio Express, go to the **Logins** folder within the **Security** folder (the one that is under the Databases section will not work properly, as you will not be able to see Windows® users from there, so make sure you are in the main security folder as shown below).



Right-click on the **Logins** folder and select **New Login**.

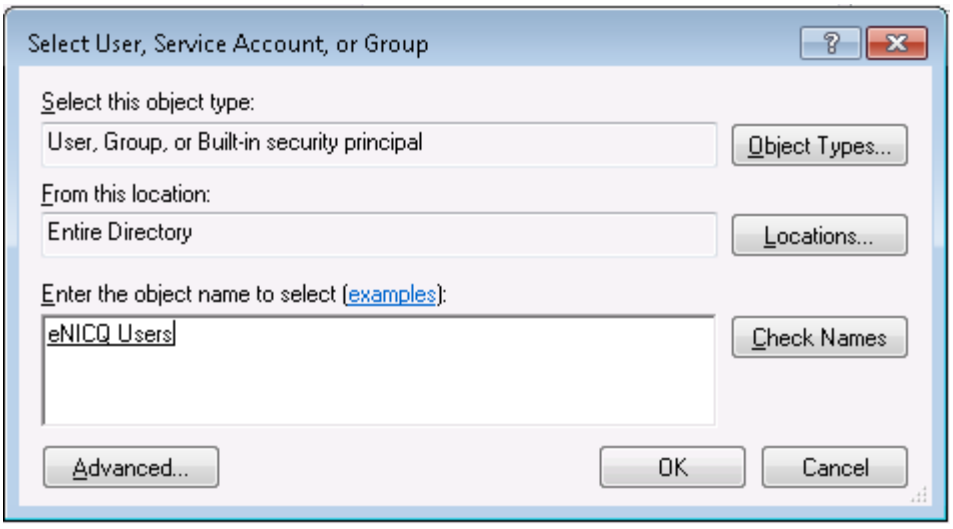


Click **Search**.



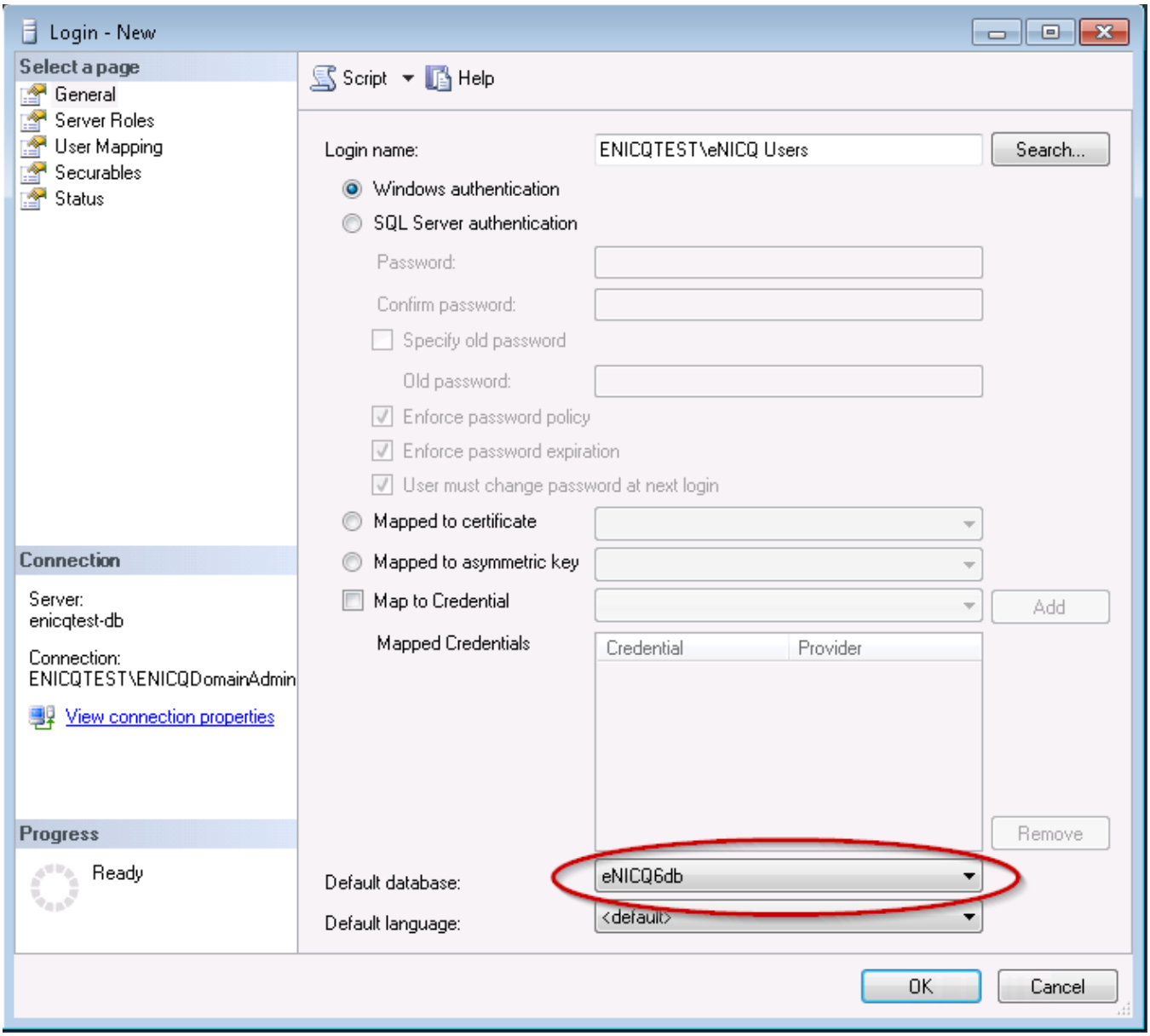
Now you need to find the user/group account that you want to give permissions to. You should note the **Locations** and **Object Types** buttons above; by default, the **Select User or Group** dialog box will query the machine you are logged in to for user accounts. You may have to select a domain instead of the local machine (as your accounts are most likely domain accounts). By default, it will be looking only at user accounts, but not groups. If you want it to look for groups as well you will have to click **Object Types** and check the box next to **Groups**.

You can enter an object name within the textbox, or you can click **Advanced** and click **Find Now** to help you find the user(s) that you are looking for. You can choose only one user at a time, though you could select a group of users here as well. When you click **OK**, the system will verify that it can identify which user/group you are talking about. In this example we will be using a group called “eNICQ Users” that is part of the local machine’s group accounts.



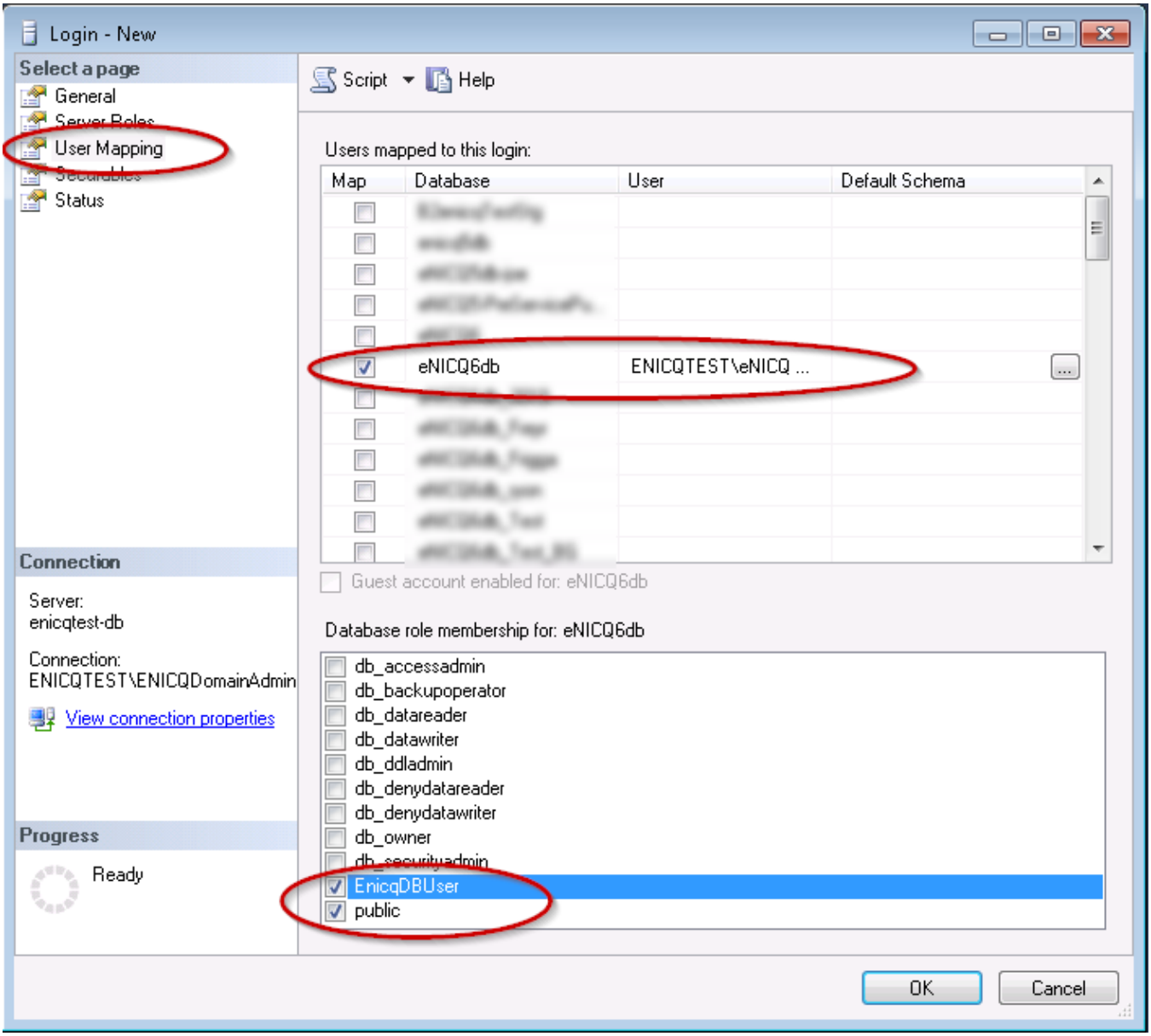
Click **OK**.

On the following screen, select the eNICQ 6 database as the Default database. The eNICQ 6 database is named “eNICQ6db” by default, but your center may have given the database a custom name.



Click **User Mapping** under Select a page.

Select “eNICQ6db” database (or use the custom name assigned to the database), and then the “EnicqDBUser” role (see red circles below).



Verify that it says **Database role membership** for “eNICQ6db” (or custom database name).

Click **OK**. You must repeat these steps for every login/group that needs access to eNICQ 6.

Configure the eNICQ 6 clients to use Windows® Authentication

Configuring the eNICQ 6 clients to use Windows® Authentication is done most easily by retrieving your copy of the Connection.enicq file from the C:\ProgramData\VON folder on the computer or server where the installer was first run to install the database and saving it to the same location on other computers where you will be installing other copies of the client application. More detailed instructions for retrieving, editing and distributing your copy of the Connection.enicq file are also located in the section of this document entitled “Deploying eNICQ 6 via Group Policy.”

If for any reason you need to edit your Connection.enicq file you will need to download the eNICQ 6 Connection File Editor from https://vtoxford.zendesk.com/hc/en-us/articles/115015973927-eNICQ-6-Connection-File-Editor. The Connection File Editor can be used to update the Server Name, Database, required ports (if your SQL Server uses dynamic ports, enter port “0”), the Authentication Mode with which to connect to the server, and the proxy server settings if you are using one. If you are using SQL authentication you will need to have a SQL User Name and Password which will log users into the database.

You will need to have “Read and Execute” permissions to the ProgramData folder to use this tool. The users of eNICQ 6 will also need the same permissions otherwise the client application will not be able to read the Connection.enicq file and fail to connect with the database. This would also prevent the creating of the error and import logs as they are also saved to C:\ProgramData\VON.

Chapter 2: Properly Securing eNICQ 6 Data and Auditing

eNICQ 6 was designed to be easy to install and maintain. We have included options in the eNICQ 6 software that allow you to secure it properly, but many of these options are not configured at the time of installation. These options require evaluation and implementation by a qualified IT technician to properly secure eNICQ 6 in a Microsoft® Windows® environment. This section will outline the available options and provide instructions for implementing the various security features. The security options are designed to allow you to enable only the components that you determine are appropriate for your environment

This section assumes that you have a Microsoft® Windows® Domain, and that the installation has already been done for the eNICQ 6 client with a database called eNICQ6db. Your center may have assigned a custom name to the eNICQ 6 database, in which case you will use the custom name instead of “eNICQ6db.”

Auditing:

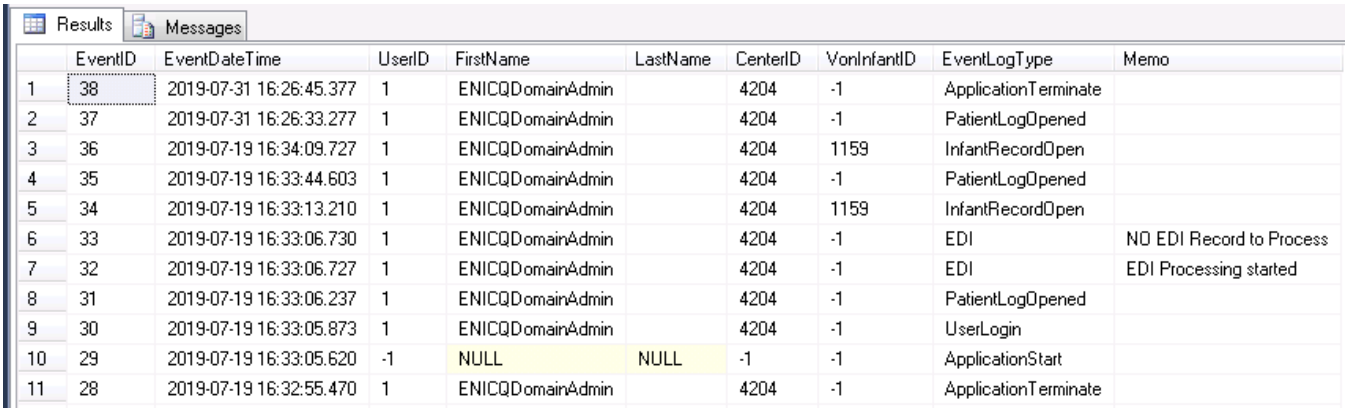
Data should be entered or edited only from within the eNICQ 6 application, never from within the database itself. eNICQ automatically logs time-stamped entries of events that take place within the application.

The Audit log is stored in the table tblEvents, and contains details about the date and time of each event. We have created a view to display the most relevant data. To see this data run the following query:

```
SELECT [EventID]
      ,[EventDateTime]
      ,tblEvents.UserID
    ,tblUser.FirstName
    ,tblUser.LastName
      ,[CenterID]
      ,[VonInfantID]
      ,[EventLogType]
      ,[Memo] from tblEvents left join tblUser on tblEvents.UserID = tblUser.UserID
     Order by EventDateTime desc
```

This will bring up a table that will include the EventID, EventDateTime, UserID, the FirstName and LastName of the user, the CenterID where the event occurred, the VONInfantID of the record edited (if applicable), the EventLogType, and Memo fields.

The results will look similar to this:



Results | Messages

	EventID	EventDateTime	UserID	FirstName	LastName	CenterID	VonInfantID	EventLogType	Memo
1	38	2019-07-31 16:26:45.377	1	ENICQDomainAdmin		4204	-1	ApplicationTerminate	
2	37	2019-07-31 16:26:33.277	1	ENICQDomainAdmin		4204	-1	PatientLogOpened	
3	36	2019-07-19 16:34:09.727	1	ENICQDomainAdmin		4204	1159	InfantRecordOpen	
4	35	2019-07-19 16:33:44.603	1	ENICQDomainAdmin		4204	-1	PatientLogOpened	
5	34	2019-07-19 16:33:13.210	1	ENICQDomainAdmin		4204	1159	InfantRecordOpen	
6	33	2019-07-19 16:33:06.730	1	ENICQDomainAdmin		4204	-1	EDI	NO EDI Record to Process
7	32	2019-07-19 16:33:06.727	1	ENICQDomainAdmin		4204	-1	EDI	EDI Processing started
8	31	2019-07-19 16:33:06.237	1	ENICQDomainAdmin		4204	-1	PatientLogOpened	
9	30	2019-07-19 16:33:05.873	1	ENICQDomainAdmin		4204	-1	UserLogin	
10	29	2019-07-19 16:33:05.620	-1	NULL	NULL	-1	-1	ApplicationStart	
11	28	2019-07-19 16:32:55.470	1	ENICQDomainAdmin		4204	-1	ApplicationTerminate	

To fully audit eNICQ 6, the administrator should also use Microsoft® Windows® auditing to audit process open and close events for the eNICQ application, and follow Microsoft® best practices regarding auditing of Windows® and SQL Server® environments. Following these best practices will ensure end-to-end auditing of all aspects of the environment. Please see the Microsoft® knowledge base for more information regarding auditing in a Microsoft® Windows® environment.

If you need additional assistance with this feature, please contact the eNICQ Technical Support Team.

Data transmission to SQL Server® back end

Data is sent from the client to the server in standard SQL communication. If the communication must be secured, Vermont Oxford Network recommends either an IPSEC connection be made between the computer running the front end software and the SQL server®, or that you enable SSL encryption on the SQL Server® back end. Please see the Microsoft® knowledge base for more information on either of these topics.

Data transmission to Vermont Oxford Network

Most data transferred to and from Vermont Oxford Network through eNICQ 6 is encrypted via SSL. Data that is sent to Vermont Oxford Network from eNICQ 6 is de-identified, and contains no Protected Health Information unless the submitting member center has the appropriate agreements in place with Vermont Oxford Network. Data such as version information may be transmitted without encryption, but all patient data or de-identified data is encrypted.

Data Storage

All data is stored in a SQL Server® database and all backups are done via SQL Server®. None of this data is encrypted by default, and must be secured properly. If encryption is required, Vermont Oxford Network recommends that you use Microsoft® SQL Server® 2012 or higher and use the Transparent Data Encryption option. Please see the Microsoft® knowledge base for more information on setting this up.

Securing access to the computer(s)

Vermont Oxford Network recommends that you physically restrict access to any computer with eNICQ data on it. Anyone who gains physical access to one of these computers may be able to gain access to the eNICQ data. This is especially important for the computer that holds the SQL installation, as administrative rights for the machine allows access to all the data in the database.

Chapter 3: eNICQ 6 Firewall Requirements

This section outlines the requirements for communication from the eNICQ front end application to both the database back end and the Vermont Oxford Network web services.

NOTE: For all operating systems, eNICQ 6 requires that firewall settings allow the client to access the following types of web files: *.aspx, *.svc, *.htm and *.html.

We have included instructions for Windows® 7 and generic instructions for Third Party Firewalls. Vermont Oxford Network has opted not to include instructions for Windows® 10, as it is nearly the same as Windows® 7. Please refer to Windows® 7 instructions for Windows® 10.

The following sections are intended to be followed on the computer hosting the database if you installed the database using the SQL Server Express® installation that came with eNICQ 6. If you are using an existing SQL Server® then you should check with your system administrator to verify these settings.

Windows® 7: Configuring Your Firewall

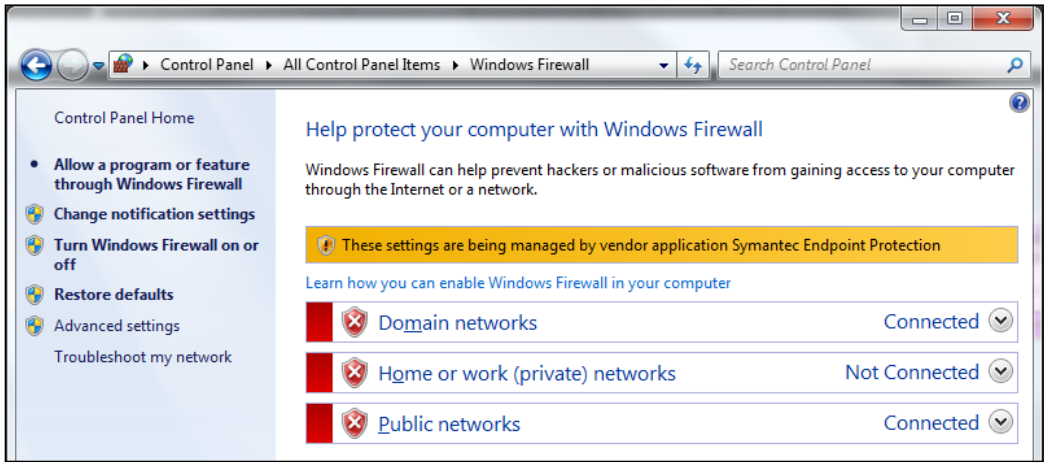
By default, the Windows® 7 Firewall will allow communication to Vermont Oxford Network's web services. The communication required to talk to Vermont Oxford Network's web services for data submission is enabled by default in the Windows® 7 firewall implementation. This document assumes that this functionality has not been removed. You will need administrative privileges to make these firewall changes.

Step 1: Access Advanced Firewall Settings

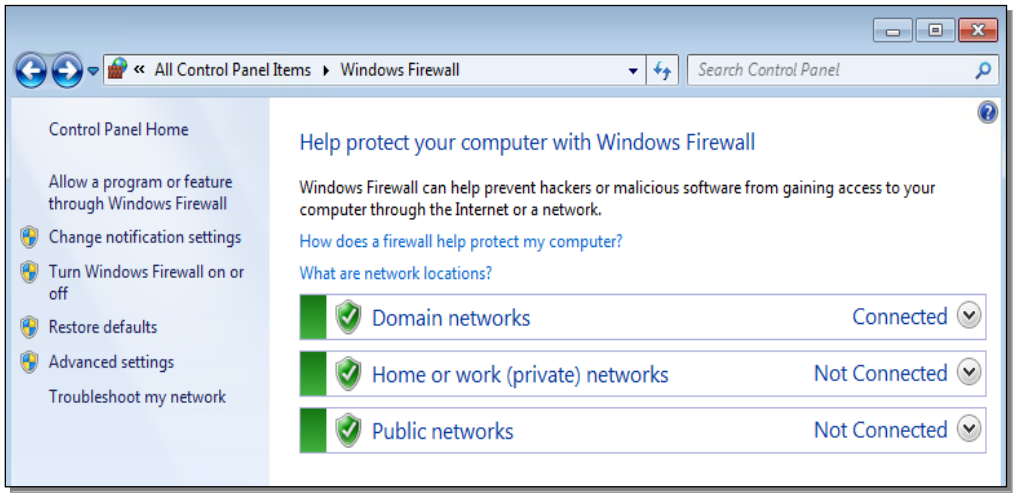
A. Open the **Control Panel**, and then click on **Windows® Firewall**. If **Windows® Firewall** isn't available, change the **View by:** option (in the upper right-hand corner) to **Large icons** or **Small icons**.

First, determine whether your Windows® Firewall is on.

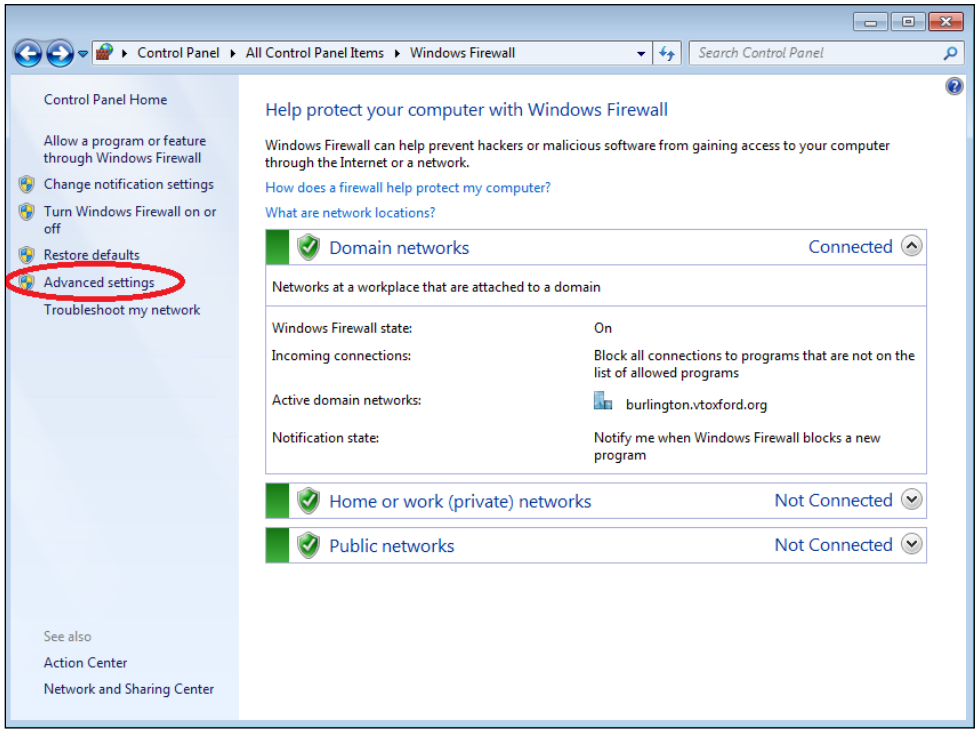
If the icons displayed are red, your Windows® Firewall may be off, or it may be managed by another security vendor (as shown below). If the Windows® Firewall is off or if the settings are disabled, you will need to contact your Systems Administrator to make the necessary changes.



If your Windows® Firewall is enabled and the settings are not being managed by another application, the screen will look similar to the one below. If this is the case, you can use the following instructions to open the ports necessary for the eNICQ clients to communicate with the database server.



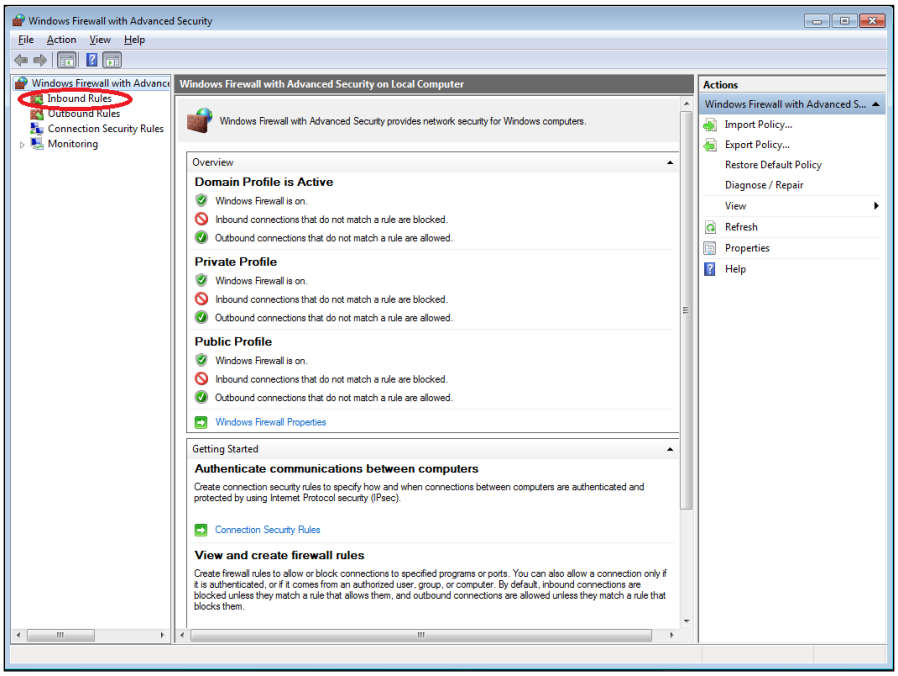
B. Click on **Advanced settings** within the toolbar on the left. At this point, the system may prompt you for administrative credentials.



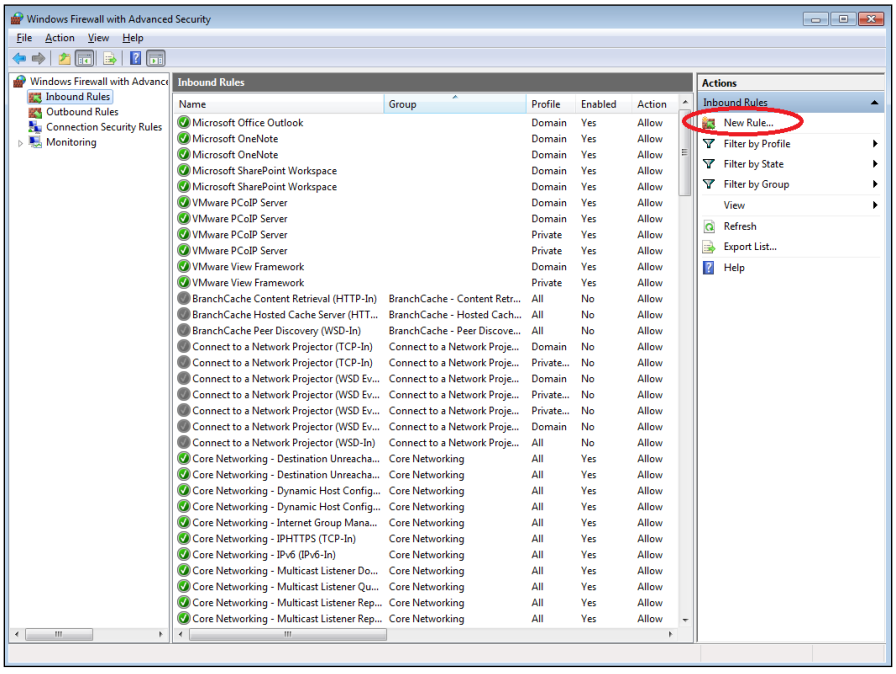
Step 2: Create an “Inbound Rule” to allow TCP port 1433 for SQL Server® Express to listen on.

Note: There are two ways to do this, either through a Port rule or a Program rule. This documentation describes creating this firewall rule using a Port rule, as in order to use a Program rule you would have to have the program installed first. Depending on your environment, this may or may not be acceptable. Please consult your Systems Administrator to determine the correct implementation for your environment. If you choose to create a program rule, you will need to implement a program rule for both “sqlservr.exe” and “sqlbrowser.exe” after installing eNICQ 6.

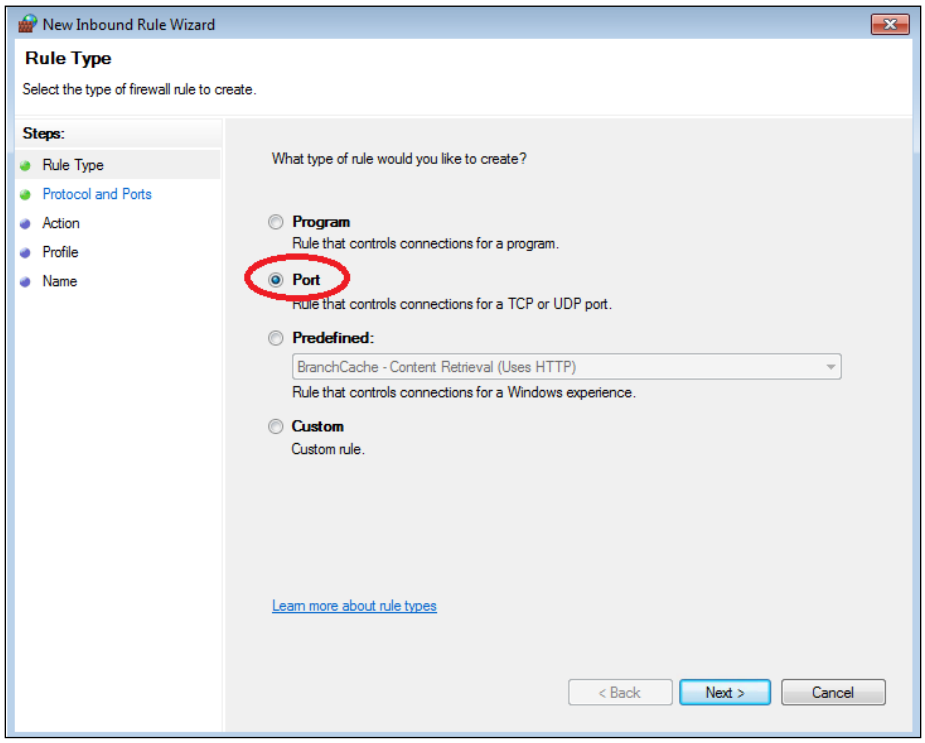
A. Click on **Inbound Rules** to the top left.



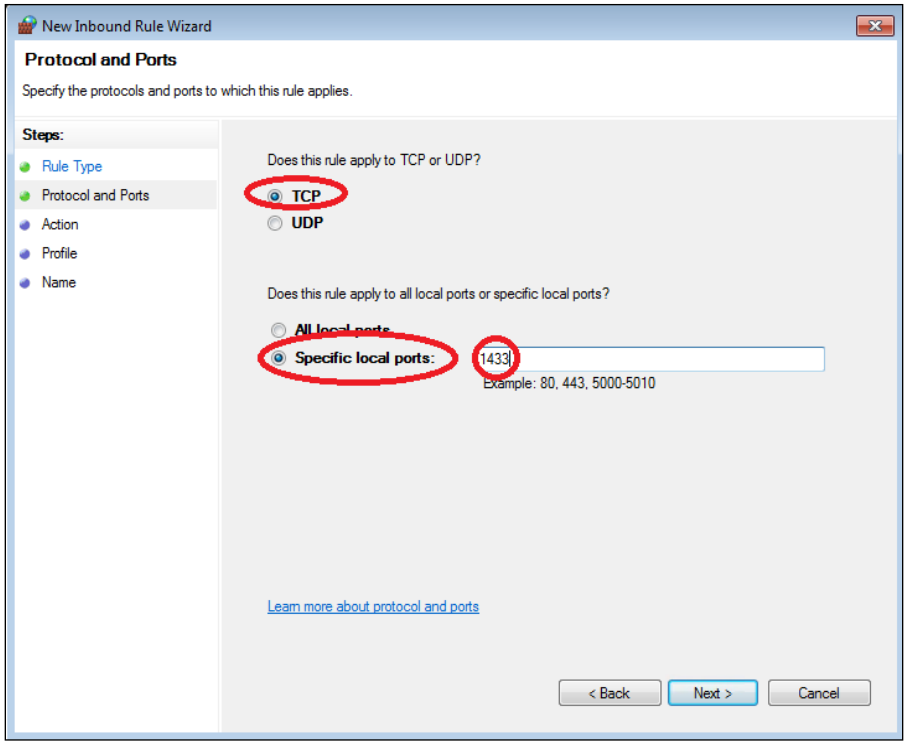
B. Click on **New Rule…** on the right-hand side to create a new rule.



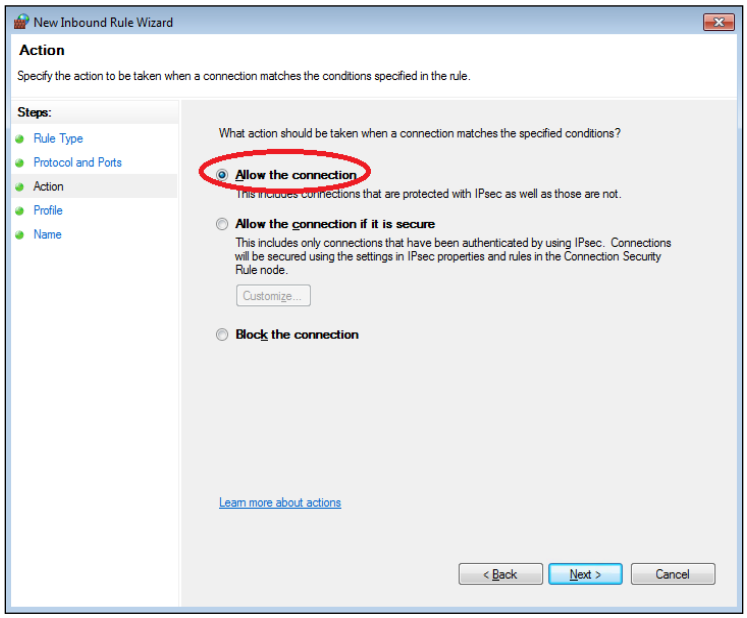
Select **Port**, then click **Next**.



C. Define the Port number and the Protocol to be used. Select **TCP**. Then within the **Specific local ports** text box, enter "1433" and click **Next**.



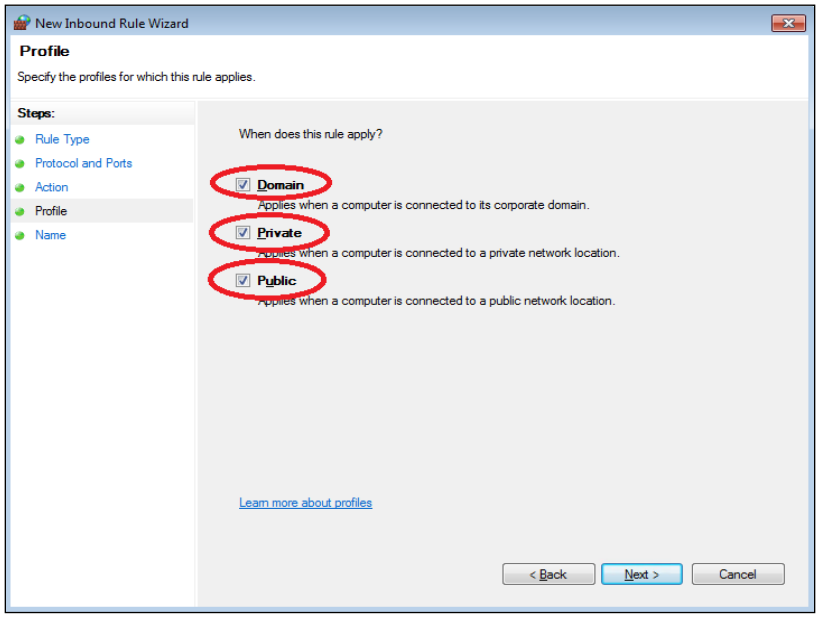
D. To allow traffic on this port, select **Allow the connection**. Again, this may violate your security policy, so contact your Systems Administrator if you are unsure.



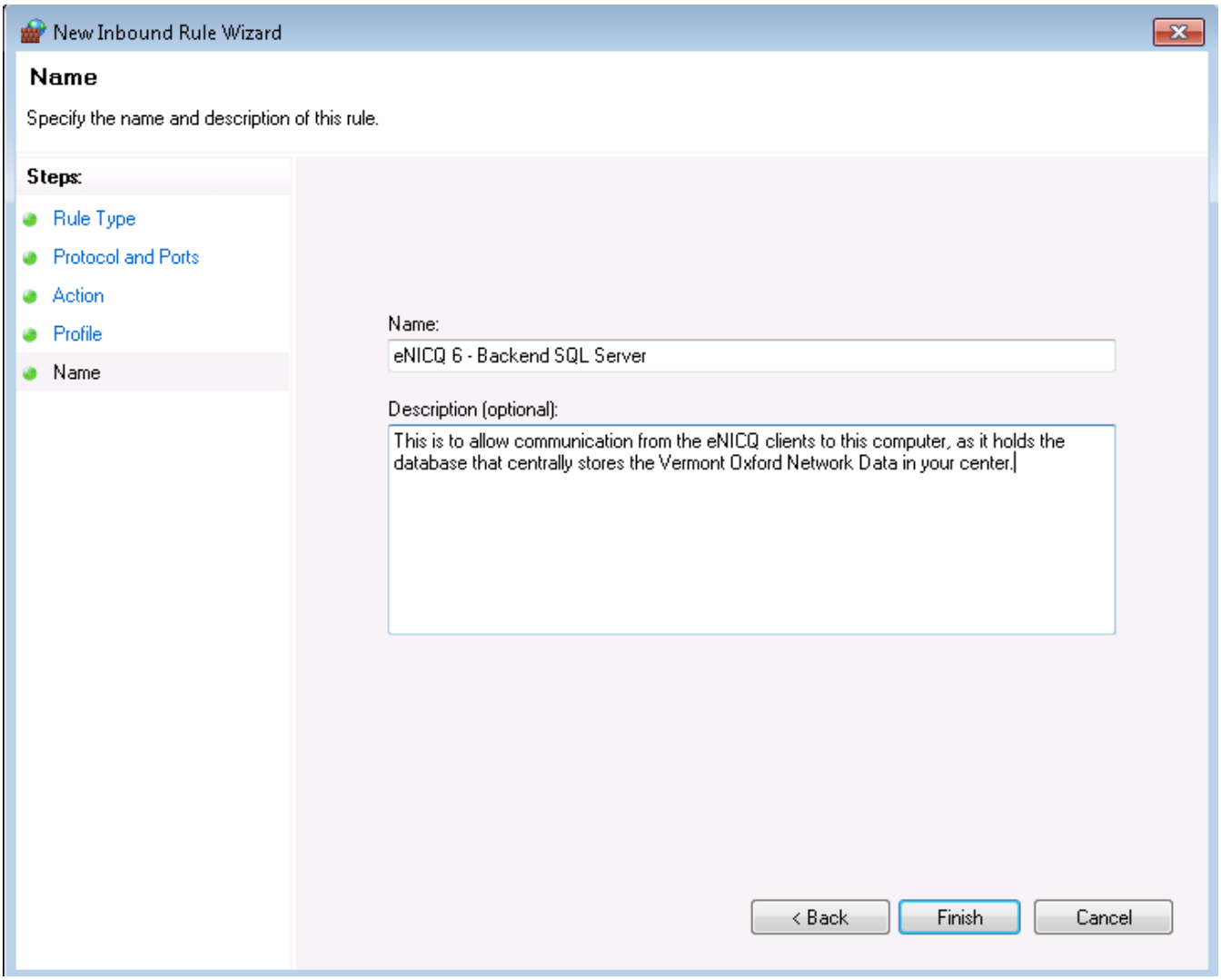
E. Define where the new rule applies. Vermont Oxford Network suggests defining the new rule for all three default profiles: Domain, Private, and Public.

- In the case of a desktop computer, these settings should be appropriate, as the computer will most likely not change networks (though this is not the most secure option).
- In the case of a laptop computer, check off only the profile attached to the network in which the eNICQ software is installed. The premise here is that when you are attached to that profile, this rule will be active. If you are unsure of what you should do here, contact your Systems Administrator for help.

F. Once you have checked the applicable boxes, click **Next**.



G. Choose a name for the new rule. The text here is arbitrary, but to help the eNICQ Technical Support Team assist you during a technical support session, please name the new rule with the starting name of “ENICQ 6” so it is easily found.



H. Click **Finish**.

Third Party Firewall: Configuring Your Firewall

This document cannot cover the settings of every type of firewall software on the market, but the basic requirements are applicable to any firewall software.

First, the eNICQ client needs to be able to send data over HTTP (TCP port 80) and HTTPS (TCP port 443) to any of Vermont Oxford Network's websites. At the very least, each client must be able to communicate to "offsite.vtoxford.org" and "www.vtoxford.org."

Note: These settings are current at the time of writing, but are subject to change.

Limiting network traffic to only these two sites may limit users' abilities to access other services offered by Vermont Oxford Network. It is recommended that the firewall settings allow HTTP/HTTPS traffic to "www.vtoxford.org" and all child domains so that as Vermont Oxford Network introduces new services, there is no maintenance that needs to be done by your center.

Second, the eNICQ client needs to be able to communicate with the machine that is the DB Server. This machine either has SQL Server Express® installed on it using the eNICQ 6 Installer or has SQL Server® installed on it by the Systems Administrator in the center's datacenter. This traffic is sent over TCP port 1433.

Third, the eNICQ installer needs to be able to locate the DB Server using the "Scan for Database" option. In order for this to happen, the UDP Port 1434 must be open and accessible on the DB Server. Without this port open, the "Scan for Database" option will not locate the database and you will have to enter the connection information manually. This may be desired, especially if your DB Server and your clients are on different networks.

We have included some examples for your reference:

Diagram A - Non-routed flat network where clients and DB Server are in the same network:

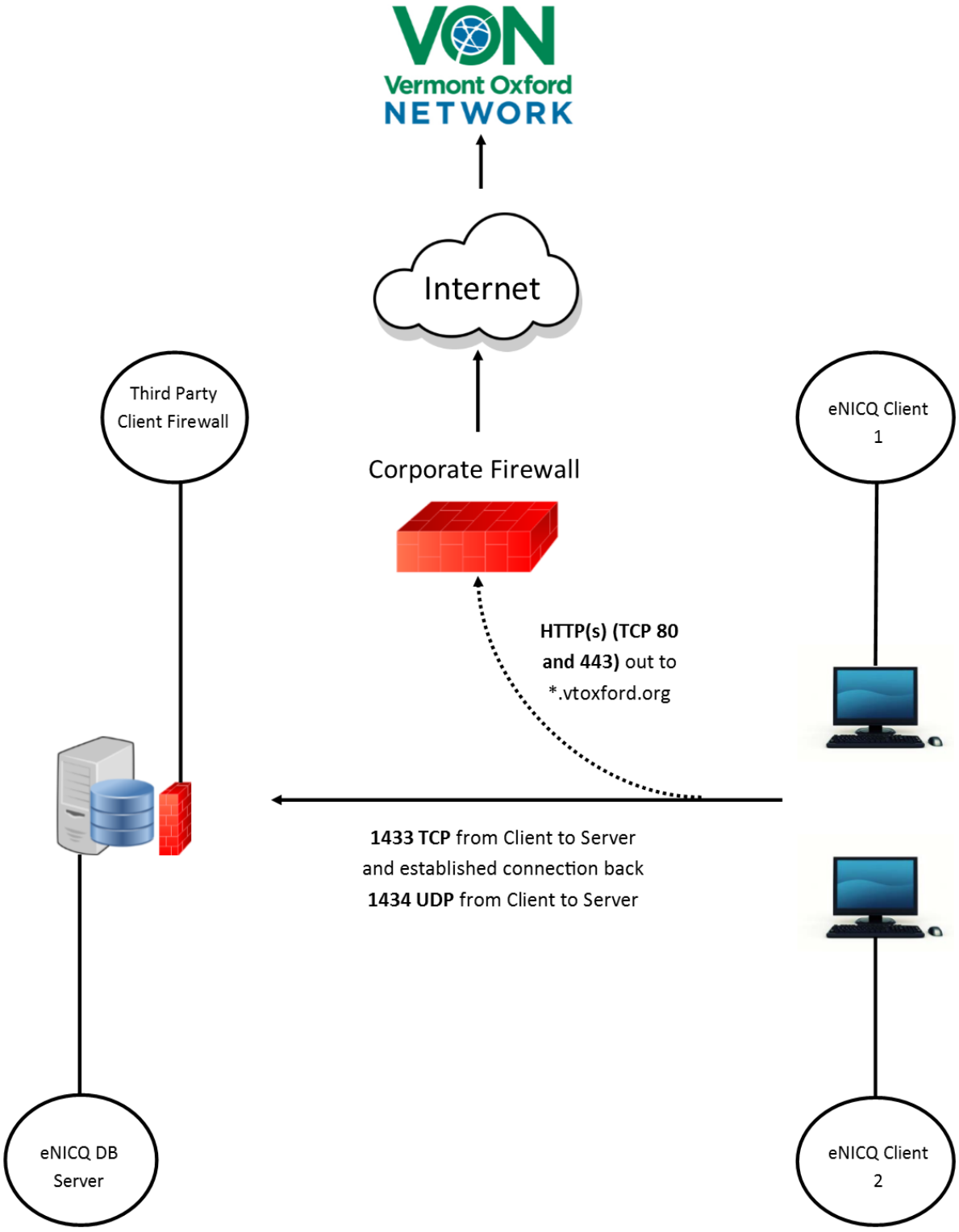
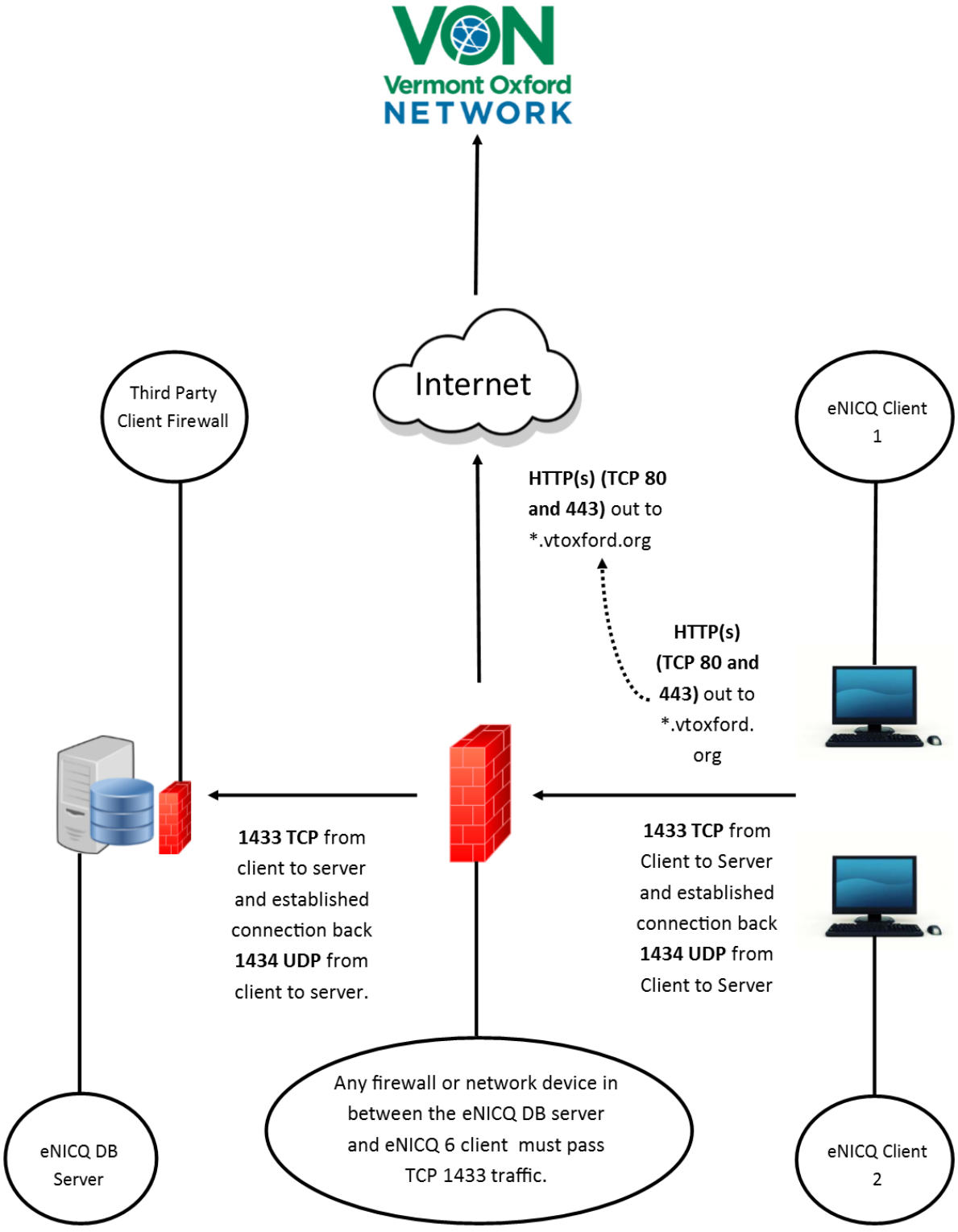


Diagram B - Routed network where DB Server is in a separate network from the clients:



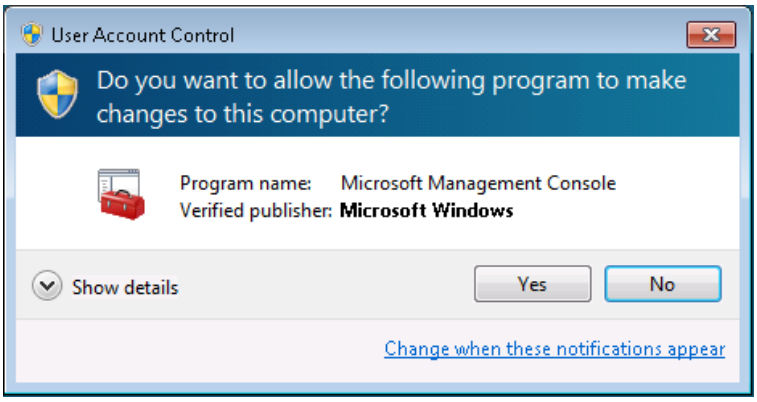
Chapter 4: SQL Server® Service listening port change

This section outlines how you would change the back end database network settings to ensure that the service is provided by a consistent TCP/IP port. Normally this is done automatically via the installer, but this can be done only via Windows® Management Infrastructure. Some organizations have disabled Windows® Management Infrastructure due to security concerns, so the installer would fail to set this static port. This section explains how to do this manually in the case that it is not done automatically.

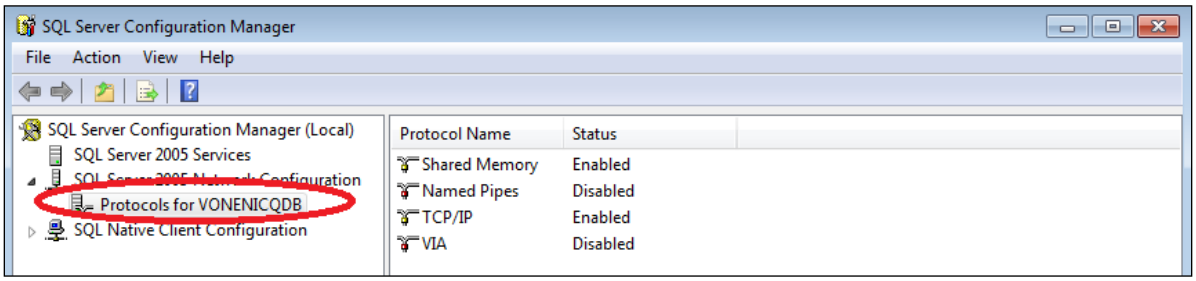
Configuring SQL Server Express® Port Numbers

Changing the SQL Server Express® Port numbers from dynamic to static to ensure connectivity in an environment with host-based firewalls

1. You must have administrative privileges to complete this action. Once you have verified that you have administrative privileges, click on the **Start** menu button, then from **Program Files**, select **Microsoft SQL Server® 2012**, and then **Configuration Tools**. Select **SQL Server® Configuration Manager**.
2. If you are running Windows® 7, you may be prompted by the **User Account Control** dialog as shown below to allow this action. If so, click **Yes**.

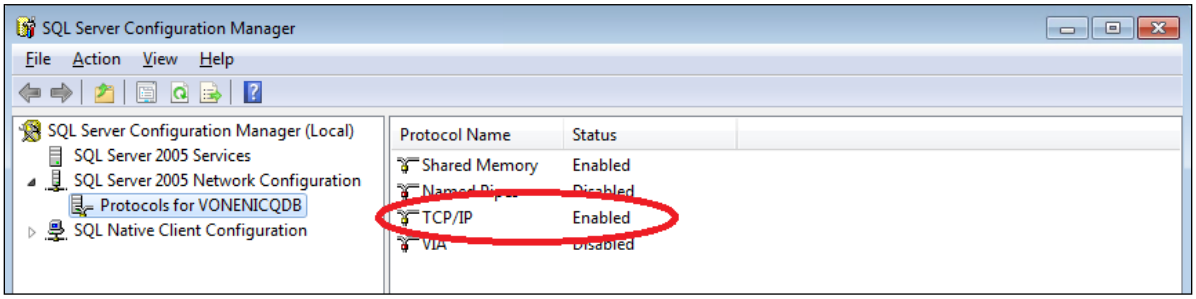


3. With SQL Server® Configuration Manager open, please verify that you have selected the **Protocols for VONENICQ6DB** item.

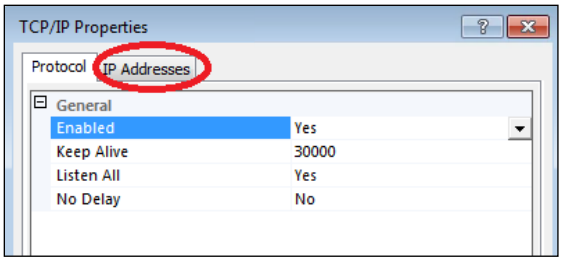


4. Verify that the protocol TCP/IP has the status as **Enabled**.

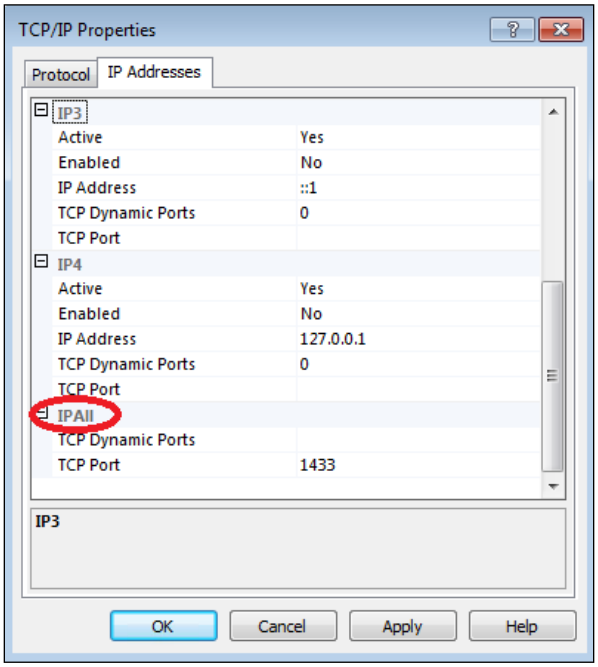
5. Double-click on the enabled **TCP/IP** protocol.



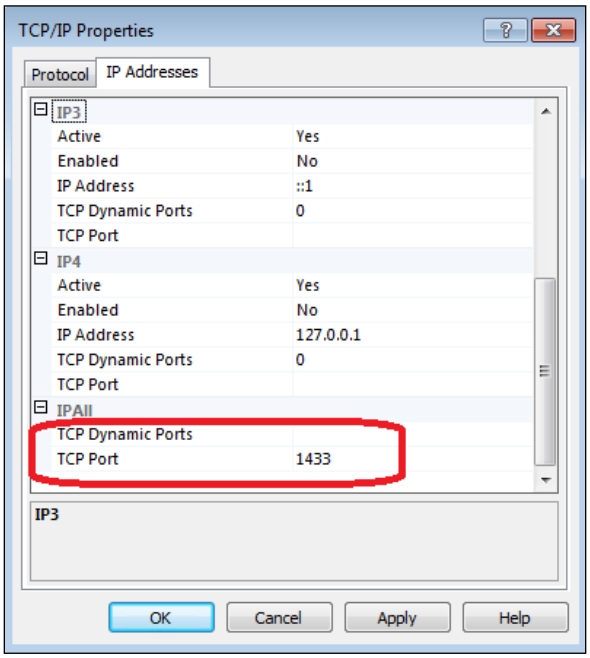
6. Click on the **IP Addresses** tab.



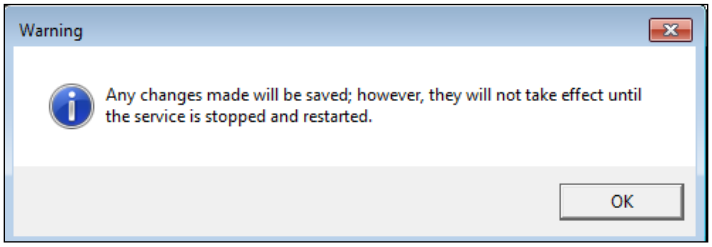
7. Scroll to the bottom where it displays **IPAll**.



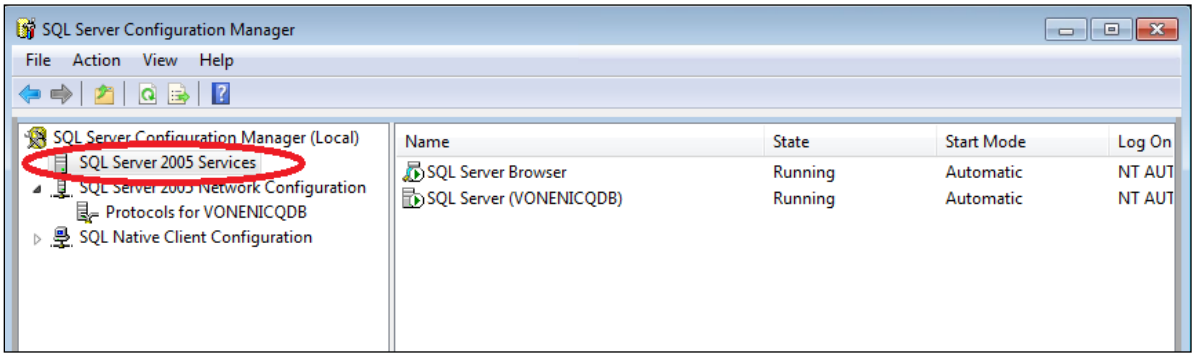
8. Set the TCP Dynamic Ports to be “blank,” and TCP Port to be “1433” as shown below. Click **OK** once these values are set as shown below.



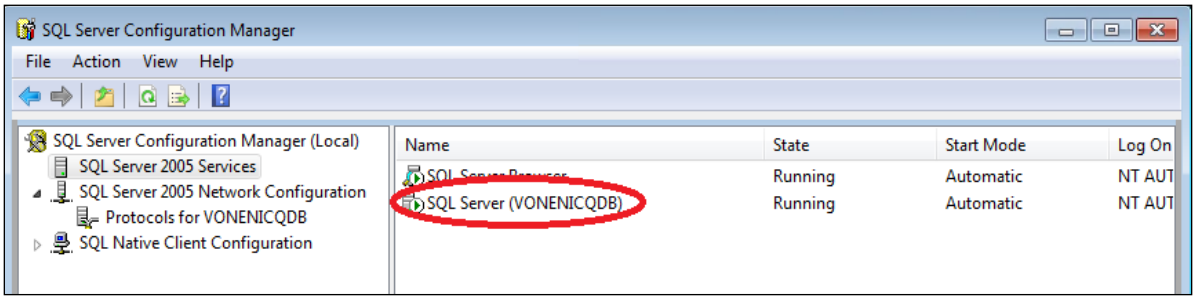
9. You will then be notified that the service will need to be restarted for the changes to take effect. Click **OK**.



- To do this, go back to SQL Server® Configuration Manager and select **SQL Server® 2012 Services**.

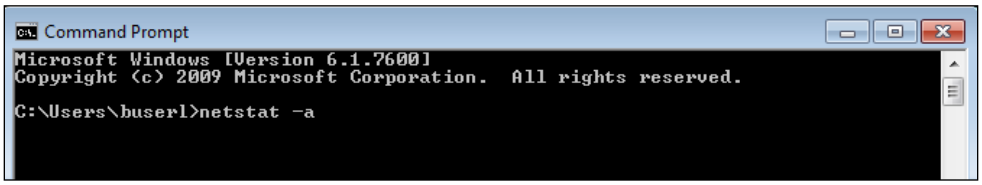


- Right-click on **SQL Server® (VONENICQ6DB)** and choose **Restart**.

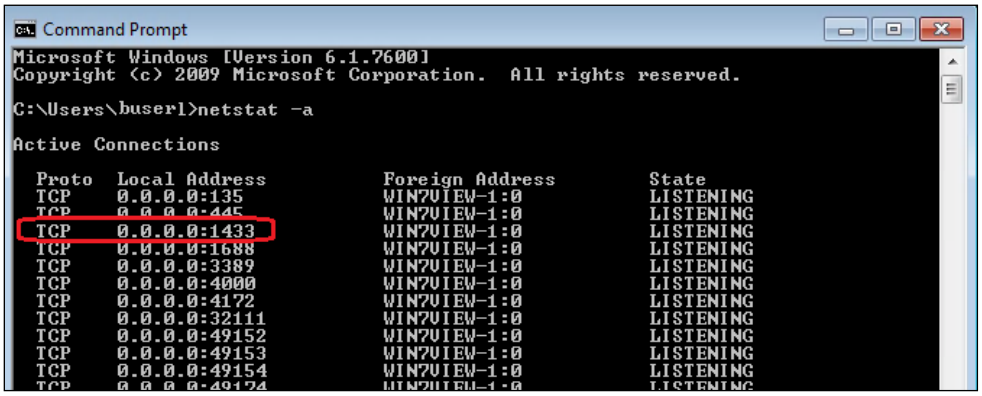


Verifying that service is setup correctly:

1. Once the service has restarted, open a command prompt.
2. Click on the **Start** menu button, and then **All Programs**. Select **Accessories**, then **Command Prompt**. Alternatively, you can open the **Run** program and type “cmd” within the **Run** dialog.
3. Now type “netstat –a” and click **Enter**.



4. You will be looking for a line that says: “TCP 0.0.0.0:1433” that is in the state of “Listening.”



If the above information is displayed, then you have correctly configured the service and you now have the ENICQ SQL Server® “listening” on TCP port 1433.

You will want to ensure that this service is available as often as possible, as it is required for the clients to work properly. You should think of this computer as a server, as it provides a service.

You will also want to refer to the documentation entitled “eNICQ 6 Firewall Settings and Traffic Requirements” to ensure that network communications will not be impeded by any firewalls.

Chapter 5: Deploying eNICQ 6 via Group Policy

This section outlines how you could deploy eNICQ 6 via Group Policy. This would be done in environments where software is maintained only by System Administration staff or in environments where the software will be installed to many workstations.

Before attempting to complete the steps described in this guide, please ensure that the database "eNICQ6db" has been created and is either being hosted by SQL Server Express® (included with the eNICQ 6 installer), or is being hosted by your center's existing SQL Server®. If your center has chosen a custom name for the database instead of "eNICQ6db," use the custom database name in place of "eNICQ6db" when following the instructions below. For more information on installing eNICQ 6, see the eNICQ 6 Installation Guide.

Once you have confirmed that the database has been created, request the eNICQ 6 MSI file from Vermont Oxford Network's Technical Support team at 802-865-4814, ext. 240, or email support@vtoxford.org.

Retrieving the Connection.enicq file

Our software does not ship with the connection information pre-populated, as the connection information is encrypted and will be different for every installation. Your center will need to retrieve your copy of the Connection.enicq file, then either distribute the file via a script (instructions will follow), or add it to the eNICQ 6 MSI file with an MSI utility such as Wise© Installation Studio (MSI repackaging is beyond the scope of this document).

To retrieve your copy of the connection file, log into the computer where the installer was first run to install the database, and go to C:\ProgramData\VON (ProgramData is, by default, a hidden folder so it may not be visible). There you should see the Connection.enicq file.

If you cannot find the connection file you could rebuild one using the eNICQ 6 Connection File Editor which can be downloaded from https://vtoxford.zendesk.com/hc/en-us/articles/115015973927-eNICQ-6-Connection-File-Editor.

Creating a distribution point for eNICQ 6 and deploying via Group Policy

The process of installing software via Group Policy is well documented within the Microsoft® knowledge base. The eNICQ 6 MSI works properly with Group Policy and can be distributed using the standard Microsoft® protocol. Vermont Oxford Network uses this process internally to release the software to our users. The workstation(s) that will have the eNICQ 6 client installed must have "read" permissions to the network location where the MSI is located. For most installations, this is a network share where Domain Computers have "read" access.

Creating a Group Policy Object that runs a script upon installation

For more information on this, please consult the Microsoft® knowledge base. This script will copy the Connection.enicq file to C:\ProgramData\VON.

A variety of languages and techniques may be used to write a script for distributing the Connection.enicq file. (Consult the Microsoft® knowledge base to find out which languages can be executed via a Group Policy computer script.) We have included a sample batch file that you may choose to use as a template.

First, you will need the UNC location of the Connection.enicq file. The workstation computer account will need to have “Read and execute” permissions for this location. (This could easily be the same location as the MSI file referenced above). In the sample below, the UNC location is \\enicqtestsrv\activedirectory.

The first line is: pushd "\\enicqtestsrv\activedirectory"

Pushd will assign an unused drive letter (starting at Z and working back up the alphabet until an unused drive letter is found) to the directory you specify.

The next line is: xcopy /Z /I /E /Y "Z:\Vermont Oxford Network" "c:\ProgramData\VON"

Xcopy is an enhanced copy utility that has some specific features.

In this case we have used the following options:

/Z copies files in restartable mode (so that a network error does not stop the copy operation, it is just tried again).

/I tells Xcopy to assume that the destination must be a directory in case this script is run before eNICQ 6 is installed.

/E copies directories and subdirectories.

/Y suppresses prompting to confirm that you want to overwrite a destination file (so that if you change the file it will be changed on the client).

“Z:\Vermont Oxford Network” is the location that is now mapped. This may differ in your environment. For instance, if z: is already mapped in your environment, another drive letter will be used. Change your script to reflect the appropriate location.

The last line is: popd

Popd removes the temporary drive mapping. This is done to be thorough.

The whole script would look like:

```
pushd "\\enicqtestsrv\activedirectory"
xcopy /Z /I /E /Y "Z:\Vermont Oxford Network" "c:\ProgramData\VON"
popd
```

These steps will need to be modified to match your environment. The script you create should be tested appropriately before deployment. In order to test this script, ensure that the batch file is working on a test machine. To run the script using your user profile, permissions to the source directory may need to be modified. After you have established appropriate permissions, deploy the script via a Group Policy Computer startup script and test it one more time. This will eliminate any Group Policy errors first, as you know you have a good running script.

Once these two Group Policies are created and assigned to the users, eNICQ 6 will be installed and configured for them. The users still may have to go through the initial configuration process for eNICQ 6, but upgrades can now be handled via Group Policy by creating another Group Policy Software Deployment package. The installer technology used by eNICQ 6 will automatically uninstall the previous version. The installer does not remove the Connection.enicq file. If moving the database is necessary, the process will be easier because you will then be able to just recreate the Connection.enicq file and copy it over the existing one to get the clients to connect to the new location.