

Vermont Oxford Network – eNICQ 6 Documentation

eNICQ 6 Local Installation Guide

Documentation Release 1.2
Published April 2024

eNICQ 6 Local Installation Guide Table of Contents

Introduction	2
eNICQ 6 Features	2
User Features	2
Technical Features	2
eNICQ 6 Installation Planning	3
eNICQ 6 Installation Options Overview	4
SQL Server® Standard or Enterprise Edition installed on server (Recommended).....	4
SQL Server® Express Edition installed locally.....	4
eNICQ 6 Logins	5
System Requirements	6
eNICQ 6 Client Software, installed locally.....	6
Microsoft® SQL Server® Express 2019, installed locally	6
Microsoft® SQL Server® 2014 or higher, existing Standard or Enterprise Edition.....	6
Download Installer	6
eNICQ 6 License Key.....	6
Diagram: SQL Server® Express Edition installed locally	7
eNICQ 6 Web Services.....	7
Protected Health Information and HIPAA.....	8
eNICQ 6 Installation Support	8
Local Installation of eNICQ 6 Using SQL Server® Express	9
SQL Server® Management Studio Server-Side Actions	16
Appendix A: Multi-Center Installations	23
Option 1: Hosting multiple centers in the SAME database (Recommended).....	23
Option 2: Hosting multiple centers in separate databases on the same server and installing multiple eNICQ applications on SEPARATE client machines	24
Option 3: Hosting multiple centers in separate databases on SEPARATE servers and installing multiple eNICQ applications on SEPARATE client machines	26

eNICQ 6 Local Installation Guide

Introduction

Welcome to the eNICQ 6 Infant Data Entry System. The software has been developed to assist your hospital enter, store, and submit the data for Vermont Oxford Network's reporting. It will allow users to manage data entry, submissions, and corrections, plus users will be better able to check data for completeness and accuracy. This guide is intended for users with limited or no IT support, or if there is not an existing Standard or Enterprise edition of SQL Server on which to install the database.

If you have an existing SQL Server where the database can be installed, we strongly recommend following the instructions in the [Guide for Installing eNICQ 6 on an Existing SQL Server](#) as the database will be safer, easier to backup, and more secure than on a local workstation. The database will contain personal patient information.

eNICQ 6 Features

User Features

- Immediate feedback on errors and warnings as data items are entered
- The ability to browse, correct, and complete data entry without printing
- Context-sensitive help, including data item definitions and ranges embedded within the data entry form
- The ability to sort, filter, and group records on the Patient Log
- Administrative settings automatically configured when you enter your center information during eNICQ 6 setup
- The capability to enter and submit data for multiple Vermont Oxford Network centers in the same database
- Allowance for multiple concurrent users in a network environment
- Continuous data submission regardless of record status
- Continuous updates of rules and data entry items
- Integrated security model
- Consolidated form with a single status code
- Highly interactive data fields - fields will only display if they are required
- Streamlined process to get a Still Hospitalized status
- Current Disposition has been consolidated
- Streamlined navigation

Technical Features

- Built on the Microsoft® .NET Framework
- SQL Server® database, either using SQL Server® Express or your own SQL Server® installation (recommended)
- Use of Windows® installer technology in all installations and upgrades
- Functionality supporting ongoing data interface from your electronic medical record system
- Secure data submission to the Vermont Oxford Network through streaming XML over HTTPS

eNICQ 6 Installation Planning

The eNICQ 6 Infant Data Entry System consists of a Windows client and a SQL Server database. This design offers many benefits. For example, the database can be installed on a central computer or server for security and backup. Another benefit is once the eNICQ 6 database is made available over the network, the client software can be installed on as many computer workstations as you need.

Discuss an installation plan with your hospital's IT or IS department to determine where the database will be installed, how many workstations will have the client software installed, and how database backups will be accomplished. We recommend that your center installs the eNICQ 6 database on an existing instance of SQL Server® if possible.

If no SQL Server instance is available, a copy of SQL Server® Express 2019 is packaged in the eNICQ 6 installer. **This guide is intended for hospitals where there is no existing SQL Server on which to install the database, or when there is no IT support available to assist with its installation. If either of these conditions is true, please see the [Guide to Install eNICQ 6 Using an Existing SQL Server®](#).**

For detailed descriptions of each installation option, please read the next section of this guide. More information on database installation and security can be found in the [eNICQ 6 System Administrator's Guide](#).

eNICQ 6 Installation Options Overview

This overview describes the available installation options and the technical skill, and permissions required for each scenario. Vermont Oxford Network recommends using an existing Standard or Enterprise Edition SQL Server installation to host the database for the additional security, stability, and extensibility that option offers.

If you do not have the resources or IT staff to support a server hosted database, the installer contains a free version of SQL Server Express 2019 which can be installed locally on a workstation computer with the client application.

SQL Server® Standard or Enterprise Edition installed on server (Recommended)

The eNICQ 6 client application can be installed on one or more workstations. The eNICQ 6 database is hosted by your existing SQL Server® Standard or Enterprise Edition.

Advantages:

- No risk of data loss if the local machine is damaged, upgraded, replaced
- Backups can be managed at the server level by a Database Administrator
- Security of PHI data can be managed at the server level
- Can have multiple client machines for data entry

Disadvantages:

- Requires professional IT support to implement

SQL Server® Express Edition installed locally

The eNICQ 6 client application and SQL Server® Express database are installed on a single workstation.

Advantages:

- Easy to install, can often be implemented with minimal IT support

Disadvantages:

- Risk of data loss if the local machine is damaged, upgraded, replaced
- Establishing a reliable backup protocol will require additional IT support
- Security of PHI data depends on securing access to the machine itself
- Can only have one client machine for data entry

eNICQ 6 Logins

There are two options for logging into eNICQ 6, the standard logins, which requires an email address and password to be entered each time a user logs in, or Active Directory logins, which will automatically log the user into the program using their Windows credentials.

The standard or VON logins are the same as the user's login for the Member Portal on the VON website. A VON Services Administrator for each center will need to go to the [Manage Users](#) page in the Member Portal to give people either [administrator or user permissions](#) to eNICQ. The eNICQ 6 users will log in using the same credentials as they would to log into our website. ***If you are installing the database locally this is the recommended type of login.***

Active Directory logins will require your System Administrator to create an AD group for users, and one for administrators prior to the installation of eNICQ 6. You can use whatever naming conventions for these groups that work best for your center. When Active Directory is selected during the installation, a screen will ask for the names of the AD groups. They will then get added to the eNICQ 6 database with the appropriate client permissions. You will still need to add the SQL permissions after the database installation.

With multi-center installations users and administrators do not necessarily have access to each center added to the eNICQ 6 database. Users and administrators will need to be given access on a center-by-center basis in the Member Portal. When using Active Directory logins, you will be [prompted to add new AD groups each time a new center is added](#). If you use the same AD groups for each center all users will have access to the Protected Health Information (PHI) of every hospital whose data is hosted on the database.

System Requirements

eNICQ 6 Client Software, installed locally

- Supported Operating Systems: Windows® 10*, Windows® 11*
- Microsoft® .NET Framework version 4.6.2 or higher
- 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 port 443. This connection must accommodate a RESTful API web service (.svc)
- User must have both "Read" and "Read & Execute" permissions to the C:\ProgramData folder

*Depending on configuration, Windows® 10 and Windows® 11 may require installation of .NET Framework version 4.6.2

Microsoft® SQL Server® Express 2019, installed locally

- Supported Operating Systems: Windows® 10*, Windows® 11*, Windows Server® 2016, Windows Server® 2019, and Windows Server® 2022
- 64-bit processor
 - 1.4 GHz (2.0 GHz or faster is recommended)
- Minimum of 512 MB of RAM (1 GB or more is recommended.)
- 6 GB of available hard disk space
- For more information on SQL Server® Express 2019, please visit the Microsoft® site: <https://docs.microsoft.com/en-us/troubleshoot/sql/general/use-sql-server-in-windows>

-or-

Microsoft® SQL Server® 2014 or higher, existing Standard or Enterprise Edition

- Supported SQL Server® Versions: 2014, 2016, 2017, & 2019
- Maximum anticipated database size of 1 GB

Download Installer

The eNICQ 6 installer is available for download on the Vermont Oxford Network website: <https://public.vtoxford.org/enicq/>. It contains both the client installer and database installer in one package.

eNICQ 6 License Key

The eNICQ 6 license key can be found by a user with an account to the Member Portal on our website. The full instructions on locating the license key can be found [in our knowledge base](#).

Diagram: SQL Server® Express Edition installed locally

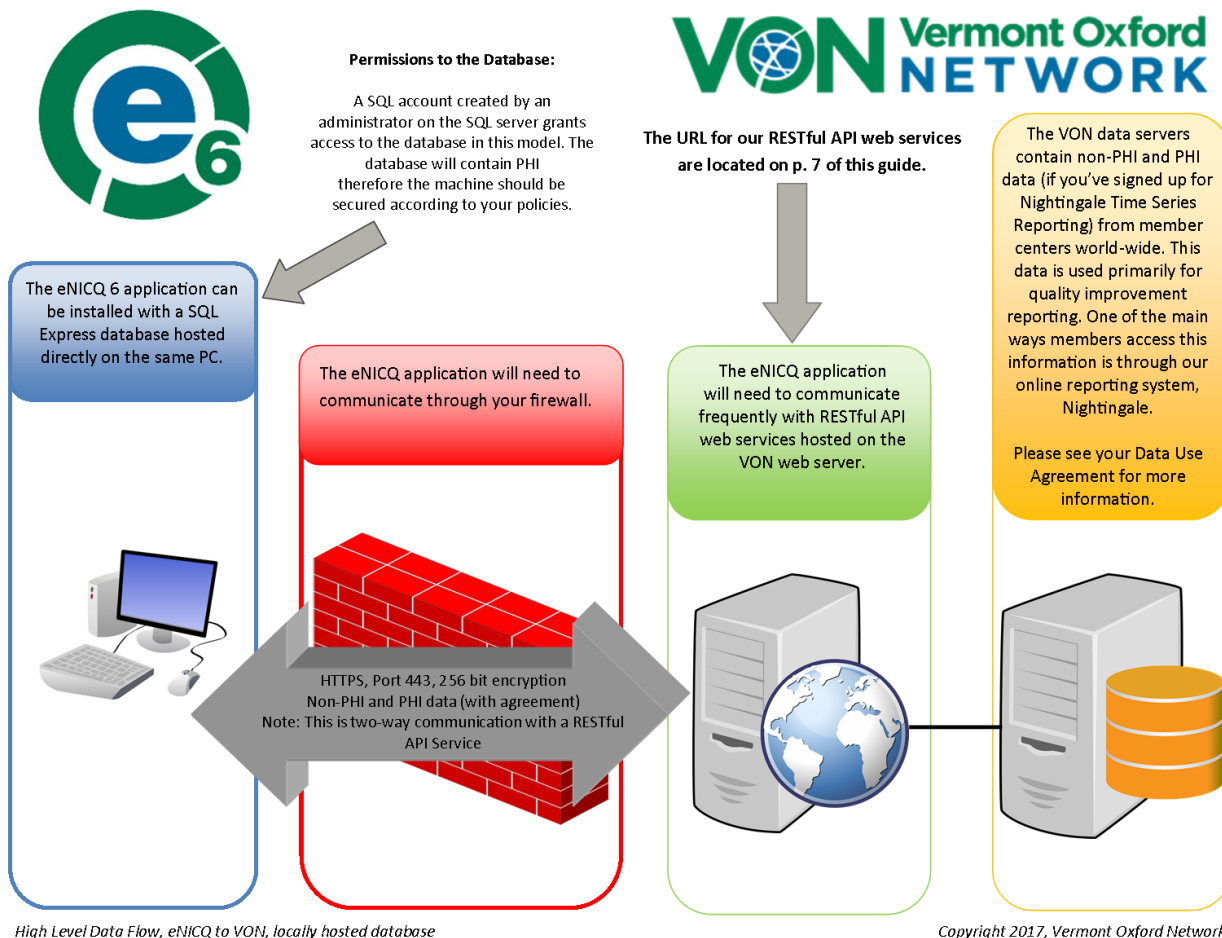


Figure 1 – Data flow diagram

eNICQ 6 Web Services

eNICQ 6 is designed to allow for data fields and definitions to be updated through our web services. It uses RESTful API web services. You may need to update your firewall settings to allow eNICQ 6 to connect with them through the internet.

The specific URLs eNICQ 6 needs to connect with are subject to change with any major revision. The root location <https://services.vtoxford.org> is NOT subject to change. We recommend “safe-listing” the root URL recursively to allow access to any new or renamed services in the future.

If you are having issues connecting with our web services VON offers a Web Services Tester from our Help Center which you can download from the [VON knowledge base](#). There is a complete list of the URLs the eNICQ 6 installer and the client need to connect with on the tester’s instructions page.

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 the [eNICQ 6 System Administrator’s 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.

eNICQ 6 Installation Support

If you have any questions or require any assistance with the installation of the software, you can contact VON Support by emailing us at support@vtoxford.org or calling (802) 865-4814 ex.240. Our business hours are 9:00 am to 5:00 pm Eastern Time, Monday through Friday.

We also have a robust knowledge base containing articles on most issues which has been reported to VON Support. The KB is updated frequently and reviewed annually. You can access the KB at <https://vtoxford.zendesk.com/hc/en-us/categories/200178697-eNICQ-6-Support>.

Local Installation of eNICQ 6 Using SQL Server® Express

NOTES:

- All installation tasks must be performed using an account with local administrator rights.
 - If there will be multiple users logging in with different Windows accounts to use eNICQ 6 the person who does the actual installation will need to install SQL Server Management Studio Express and give each user the EnicqDBUser role on the database using SQL Server Management Studio Express.
 - Because of where the Connection.enicq file, error logs, and import logs are saved all users need to have “Read and end execute” permissions on the C:\ProgramData folder.
1. To begin installation, double-click on **eNICQInstaller.exe**. A warning message may ask if you want to allow the program to make changes to the computer. Click **Yes** and the installer self-extraction process will begin.

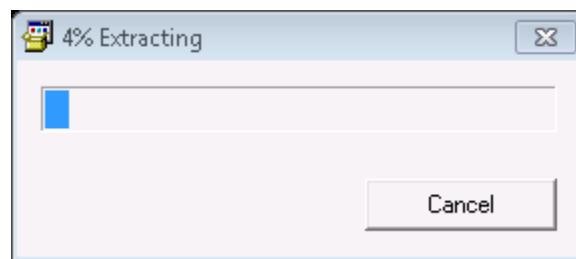


Figure 2 – Windows extracting the installer

2. When the extraction process is complete, a Welcome screen will appear. When installing a new eNICQ 6 database you will not have an existing connection file. Confirm that **No** is selected and click Next.

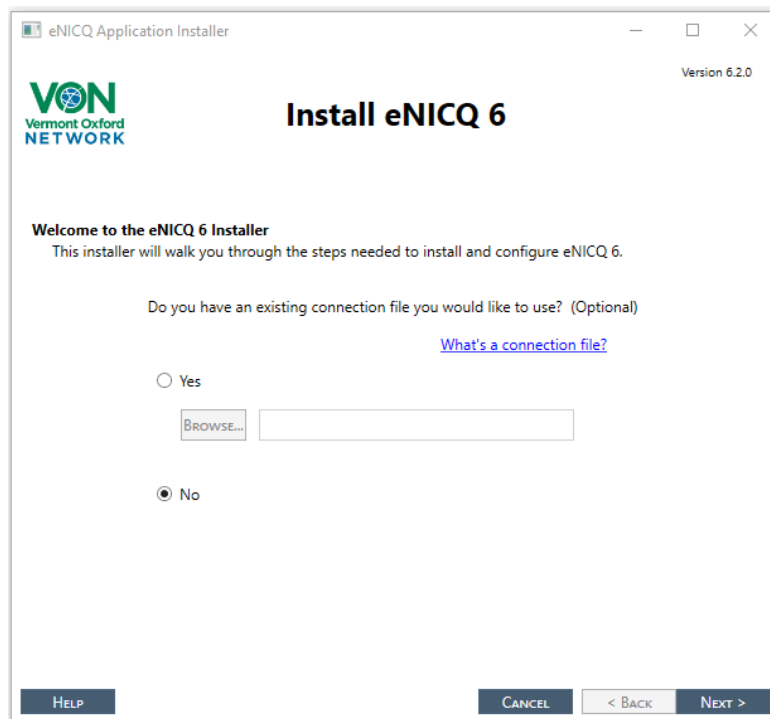


Figure 3 – With new installations you select No to having a connection file, and click Next.

3. Select Normal Install, enter your License Key, and click Next. If you do not know your License Key click the “I don’t have a license key” link for instructions on where to find it.

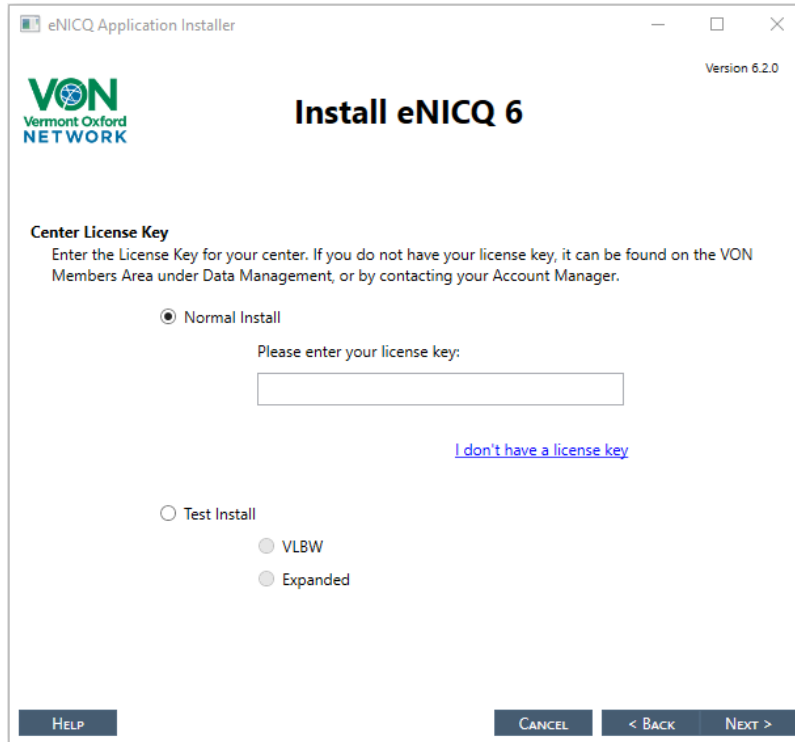


Figure 4 – Select Normal Install, enter [license key](#), and click Next

4. To install the database locally on a workstation (see p.3 of this guide for the advantages and disadvantages of each type of installation) select “On SQL Server Express Edition, installed locally” and click Next.

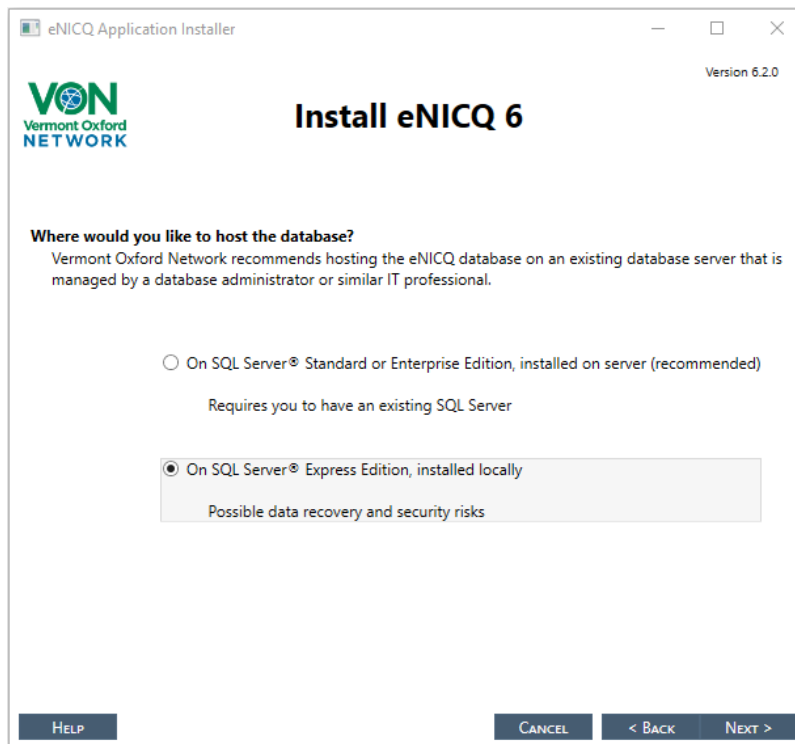


Figure 5 – For a local installation of the database select “On SQL Server Express Edition, installed locally”

5. A window will pop up reminding you of the risks with a local installation of the database. If you are still certain this is what you would like to do click "I understand the risks. Do a local install".

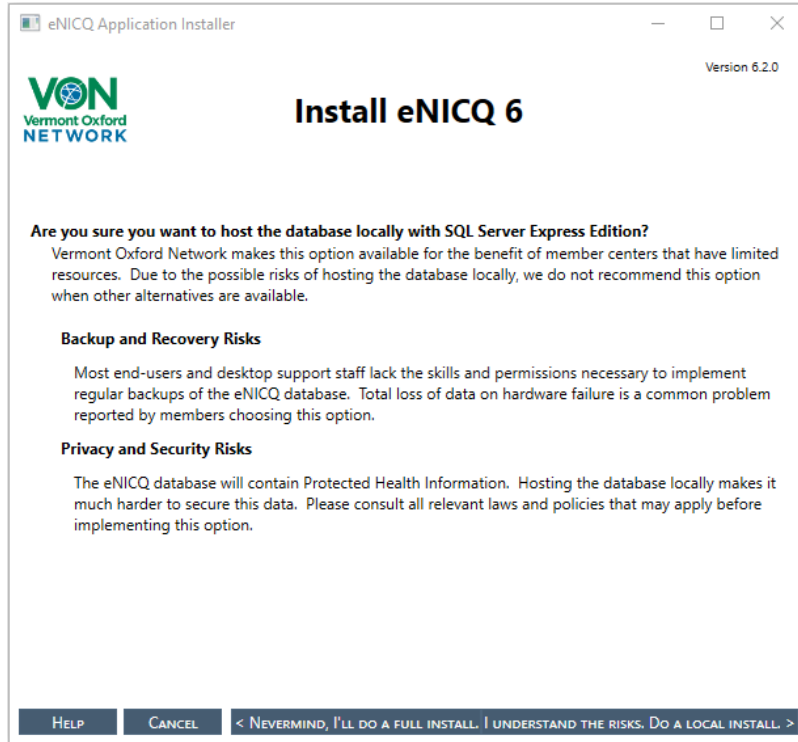


Figure 6 – Please read the warnings about a local installation on SQL Server Express. *There will be PHI saved to this database.*

6. A window will appear while the temporary files are opening, followed by a message asking for you to please wait while the installation of SQL Server® Express 2019 is completed. Do not interrupt.

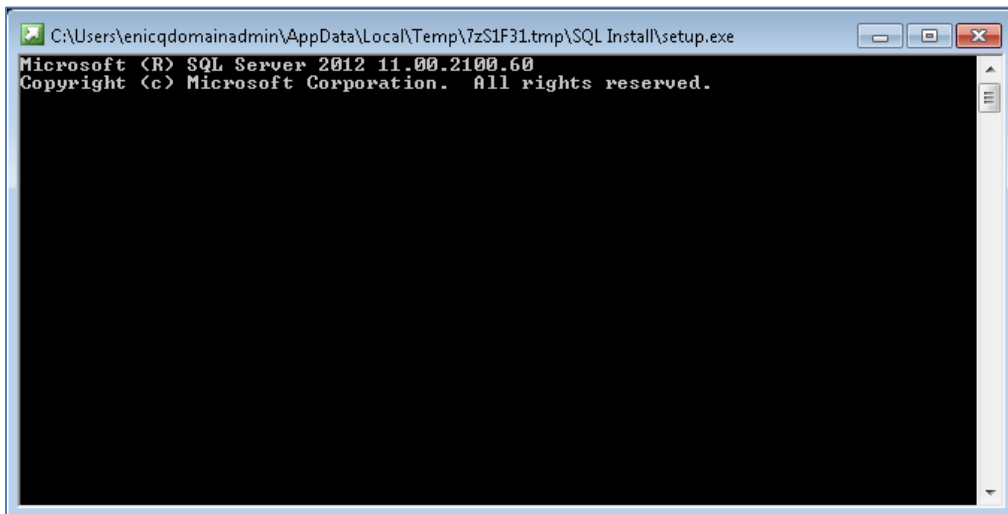


Figure 7 – Temporary files screen

- Next the SQL Server Install Setup Files wizard will appear followed by a series of different windows, including a progress bar. Let this run until completed.

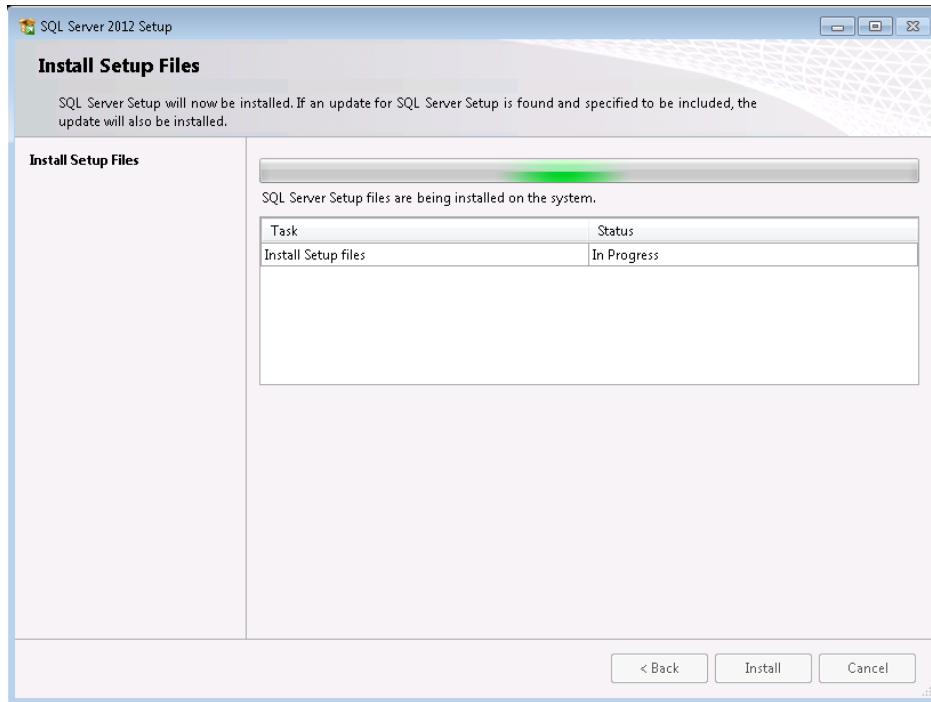


Figure 8 – SQL Server installation window

- When it's finished installing SQL Server® Express 2019 you will then be prompted to select which login type you would like to use (see page 4 for more information on the types of logins). If you select “Use my VON Login” (recommended for this type of installation) skip to step 12.

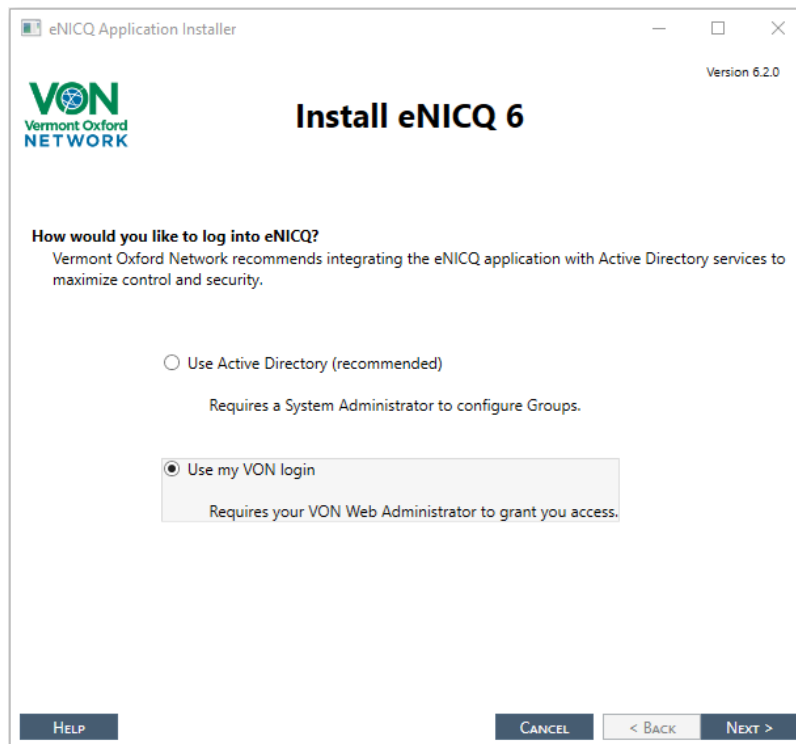


Figure 9 – Select the type of login for the application. VON login is recommended for this type of installation

9. When you choose use Active Directory logins you will get a screen to enter the Active Directory Group names. Your System Administrator should have created the Active Directory groups and provided you with the names prior to performing the installation. Enter the group names into the appropriate fields.



Figure 10 – If Active Directory logins are selected enter the AD group names

10. Next will be a dialog box showing you a progress bar for the eNICQ 6 database.

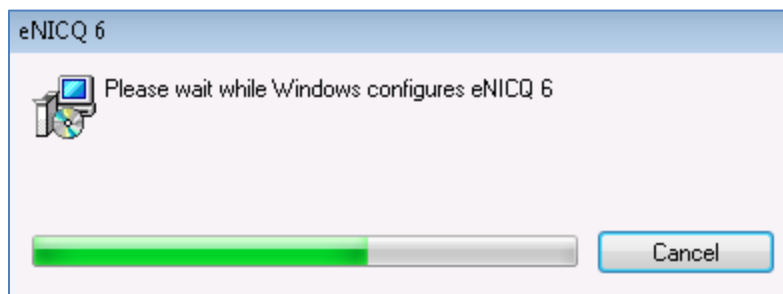


Figure 11 – Installation progress bar

11. When Active Directory is selected the next screen will ask where you would like to install the eNICQ 6 client application (this screen does not appear when VON Logins are selected). Select which option you would like. **If you are planning on having multiple clients connecting with the database you cannot do a local install.** The database will need to be installed on an existing SQL Server® (see the eNICQ 6 Network Installation Guide).

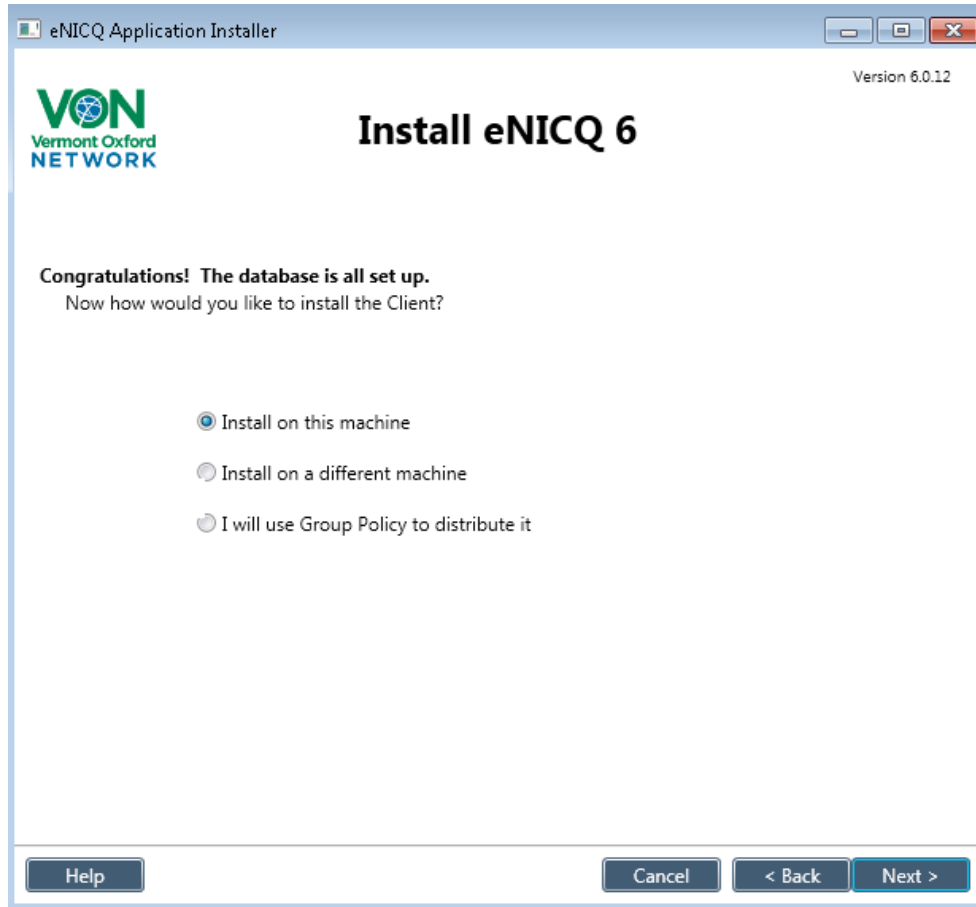


Figure 12 – Database is installed. With a local installation you should select to install on this machine

12. After successfully installing the eNICQ 6 client you will see the “Congratulations!” page of the installer. You can select to simply exit the installer, run eNICQ 6, or to view the help files at this point. The installation is completed at this point.

If you are going to run eNICQ 6 you will need to make sure that you are able to login either using Active Directory or with the same login you would use for the Member’s Area. When Active Directory logins are selected as the login type, users will need to log our and back into Windows before the updates to their permissions are updated.

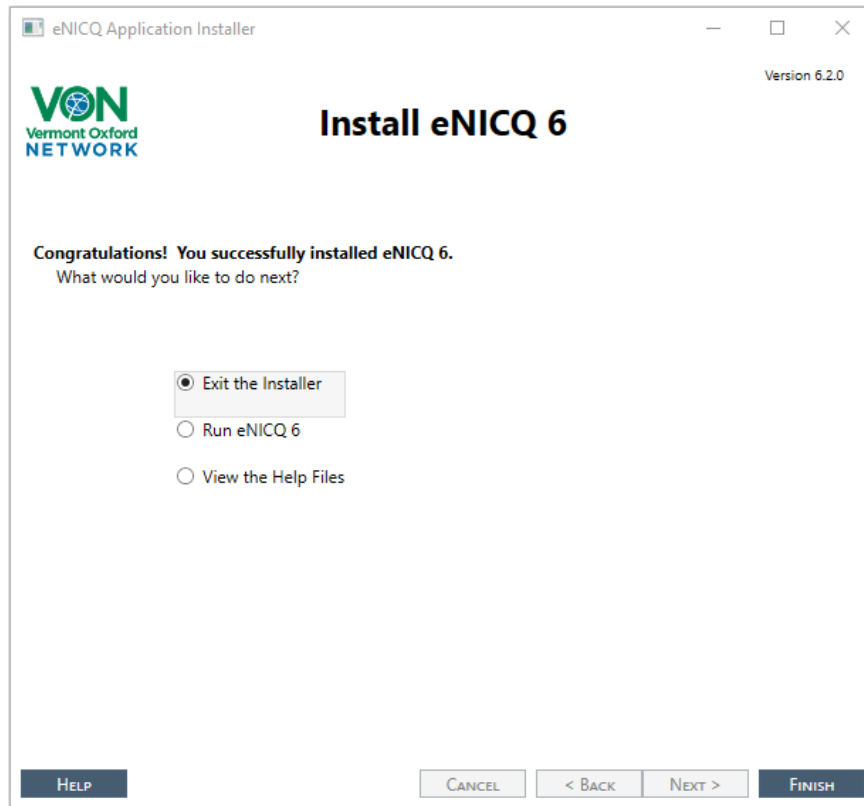


Figure 13 – Installation of eNICQ 6 is complete.

Final Notes:

- Installing the database will create a connection file located C:\ProgramData\VON. ProgramData is a hidden folder so you may need to select to show hidden items before it is visible. **We recommend saving a copy of the connection file in a secure location on your network.**
- The person who does the installation locally using SQL Server© 2019 Express will be the lone Administrator to that installation of SQL Server© Express even if there are other local administrators to this workstation. ***This means nobody else will have permissions to access the database.*** If you installed the eNICQ 6 database following the steps above for only yourself to use then you are done with the installation.

If you are installing this for another user you will need to install SQL Server Management Studio Express and give each user the EnicqDBUser role under User Mapping. Please see your Database Administrator to get the permissions set for each user. The steps for this are included in the next chapter.

SQL Server® Management Studio Server-Side Actions

NOTES:

- The eNICQ 6 application performs database transactions using the following isolation levels: RepeatableRead, ReadUncommitted, Snapshot, ReadCommitted. The SQL Server® database must allow usage of each of these isolation levels.
- To perform the following steps, you will need to have SQL Server® Management Studio (SSMS) installed and connected with the instance of SQL Server® where the eNICQ 6 Database resides. If you do not already have a copy you can download the installer for SQL Server® Management Studio Express from Microsoft's website, <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15>.
- The following instructions should be carried out in SQL Server® Management Studio by a database administrator or IT professional with equivalent skills and permissions. These instructions focus on using Windows Authentication to manage database access. Additional options and tips are available in our documentation on [troubleshooting database connectivity in eNICQ 6](#).

1. Open SQL Server® Management Studio.
2. Locate the **Security** folder at the server level in the object explorer.

Note that there is also a Security folder at the database level under the eNICQ6db database, but that is not the correct Security folder to perform these actions.

3. Expand the **Security** folder. Under the **Security** folder you will see the **Logins** folder.
4. Right-click on the **Logins** folder and choose **New Login...**

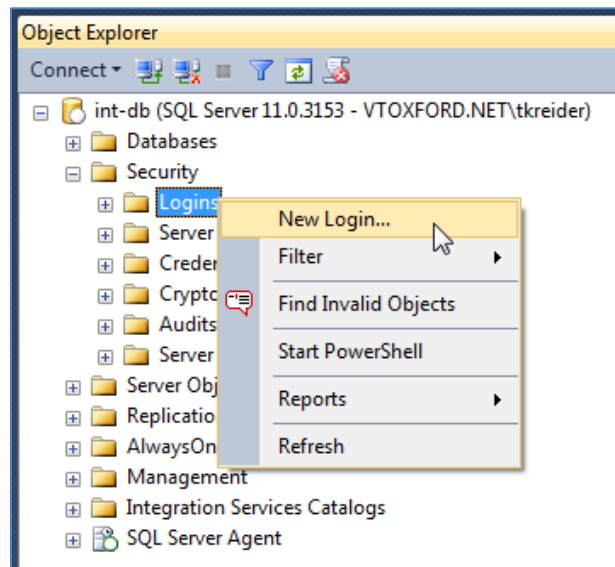


Figure 14 – Right click on the Logins folder located in the server Security folder, and select New Login

If the users have already been given permissions to another database on this server, they will show in Logins already. Right click on them and select **Properties** and skip to step 19.

- At the bottom of the **Login – New** dialogue, set the **Default database** to eNICQ6db unless you named it something other than the default name. In that case select the actual name of the database.

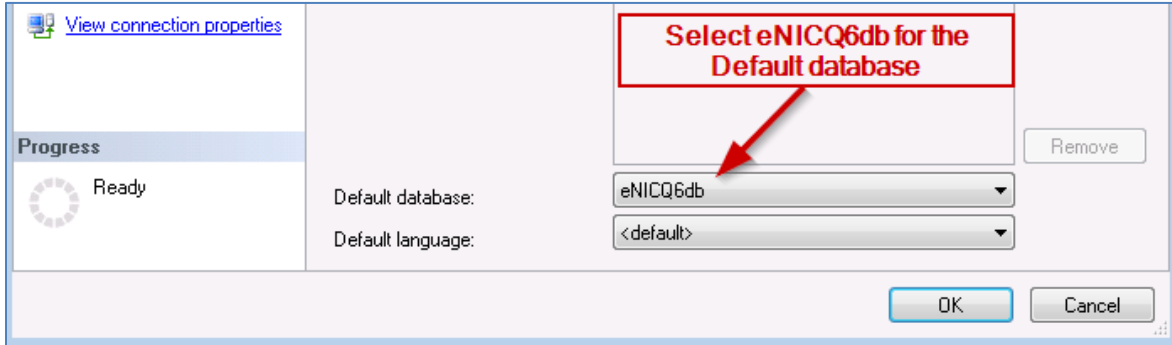


Figure 15 – Select eNICQ6db as the default database

- Select the **Windows authentication** radio button.
- Click the **Search** button



Figure 16 – at the top of the same screen select Windows authentication, and click Search

- Click the **Object Types** button on the **Select User or Group** dialog.

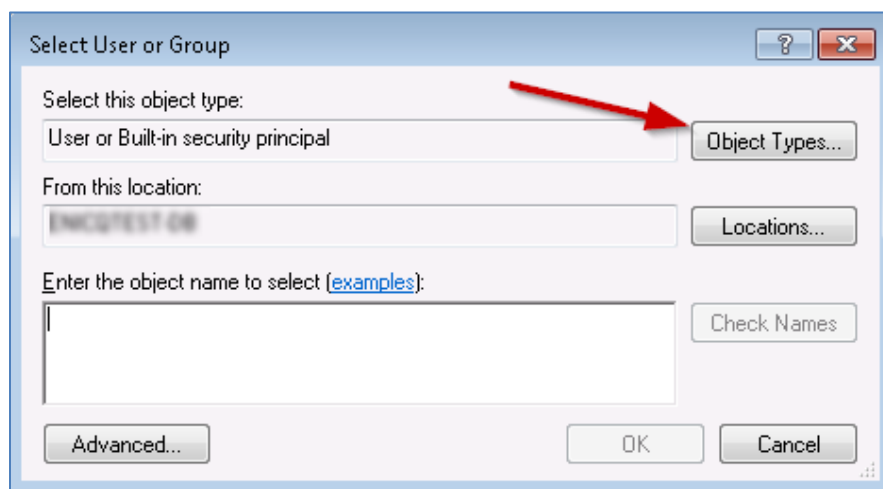


Figure 17 – click the Object Types button

- Uncheck **Built-in security principals and Other Objects**.

10. Check **Groups** and/or **Users**, whichever you are using. For multiple users, managing through group membership is recommended.

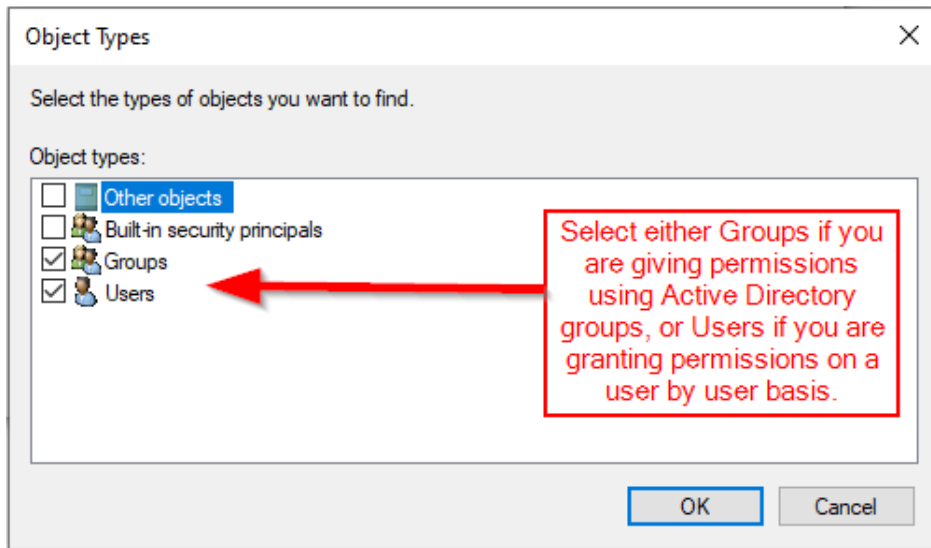


Figure 18 – unselect “Built-in security principals” and “Other objects” then select either Groups or Users

11. Click **OK** to continue.

12. On the **Select User, Service Account or Group** dialog Click **Locations...**

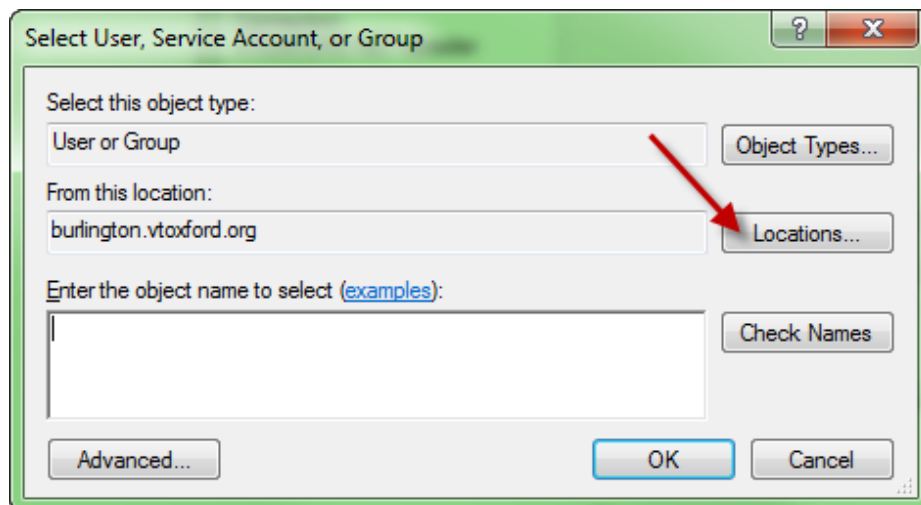


Figure 19 – Click “Locations...”

13. Select the location for the Windows account or group and click ok.

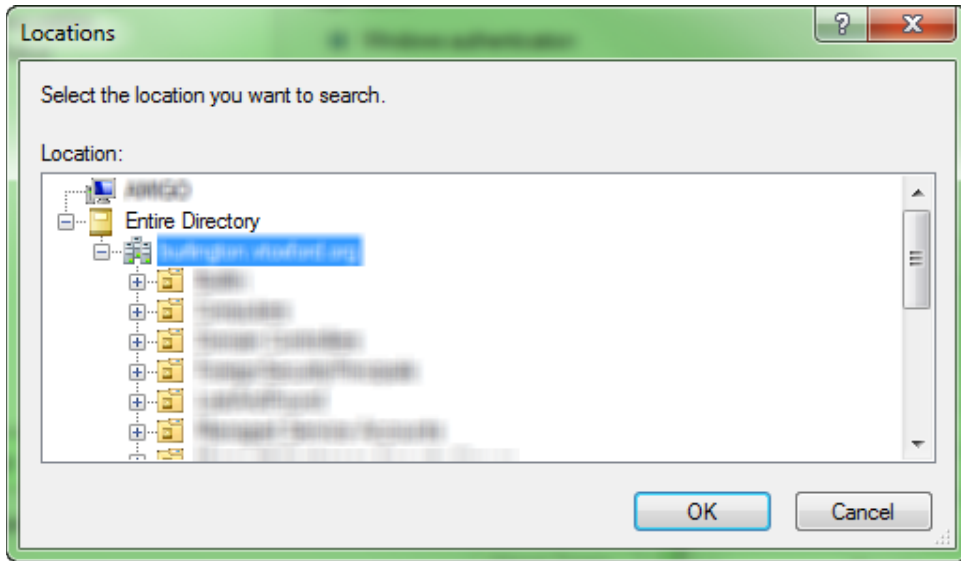


Figure 20 – After selecting the locations to find the user or group click OK

14. Enter the user or group in the space provided and click Check Names.

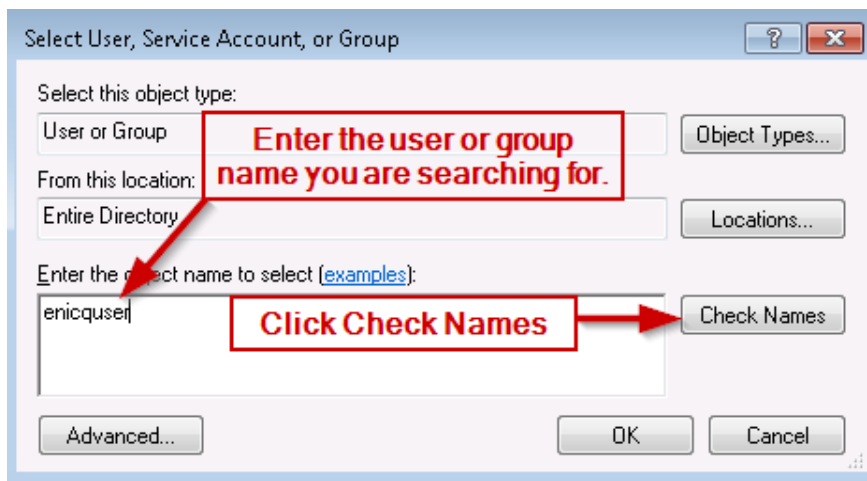


Figure 21 – Enter name of group or user and click Check Names. “enicquser” is only an example and will not be located on your network unless you create this user.

15. If you have been unable to identify the correct user or group, click **Advanced...** on the **Select User, Service Account or Group** dialog for more search options. Otherwise, continue to step 19.

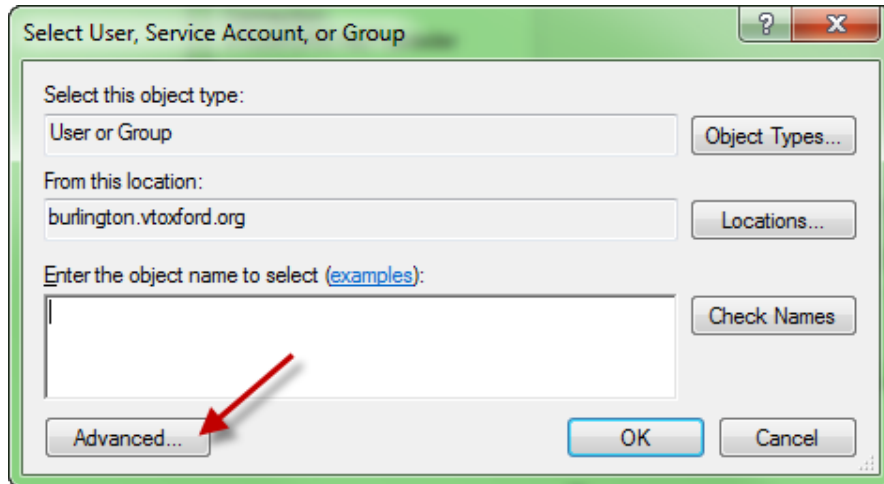


Figure 22 – Click the **Advanced...** button if the user or group is not found in previous step

16. Use the advanced features to find your user or group.

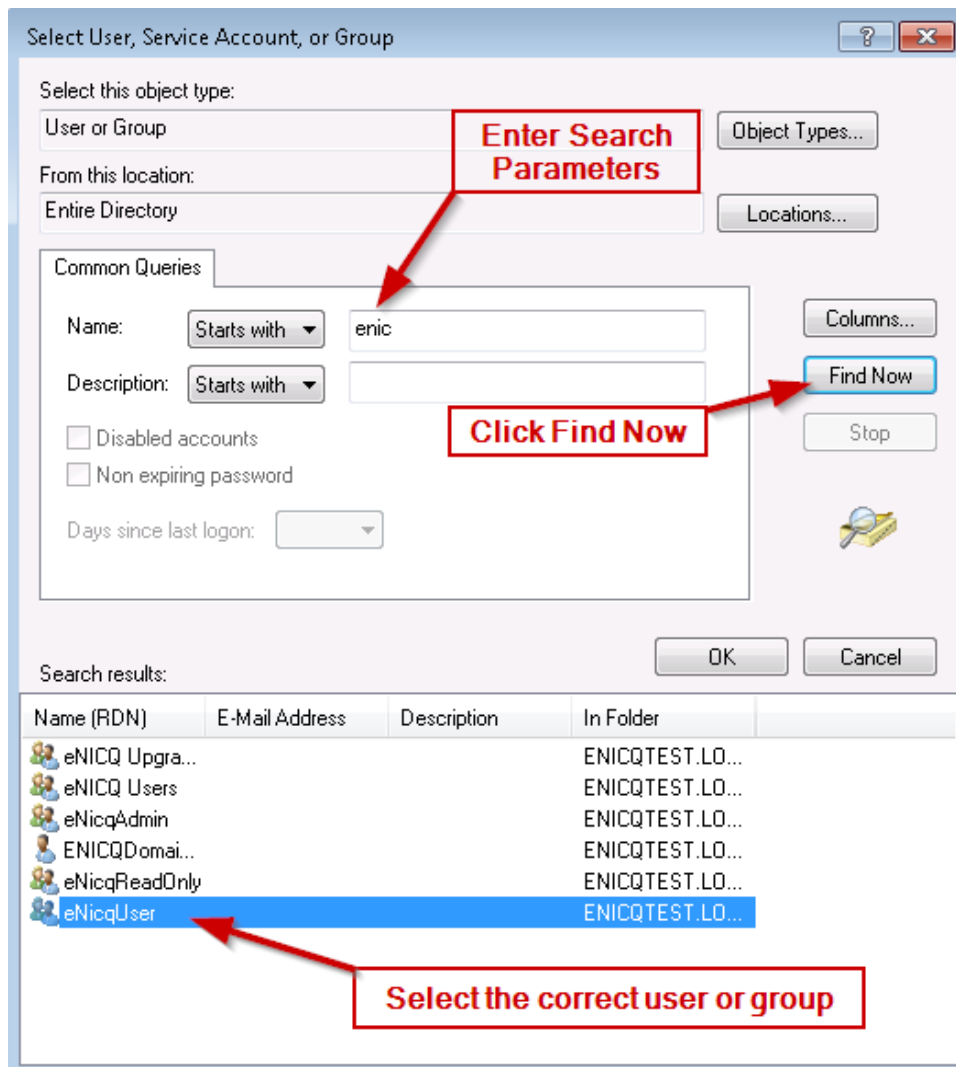


Figure 23 – Use the Common Queries fields to find the user or group, then select them at the bottom.

17. Please contact your System Administration team for assistance if you have difficulty with any of the following:
- Locating the correct user or group.
 - Creating a user or group.
 - Adding or removing users to or from a group
18. On the **Login – New** screen, or the **Login Properties** screen if you are editing an existing user, click the **User Mapping** page.
19. Check the **eNICQ6db** database in the upper panel if you kept the default name. If changed the name to something other than the default look for that in the upper panel and select it.
20. Check the roles **EnicqDBUser** and **public** in the lower panel.

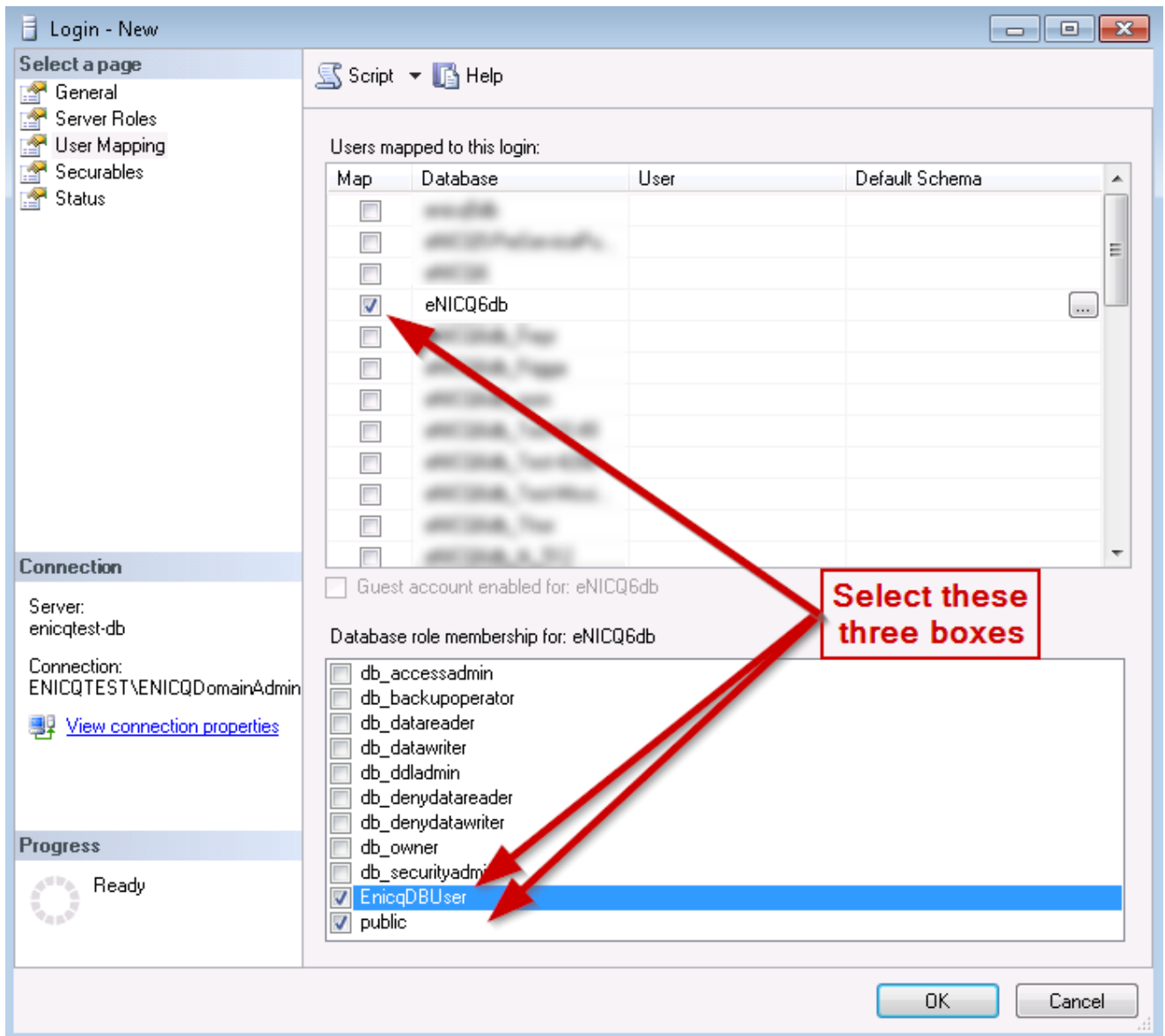


Figure 24 – Select User Mapping on the left. Make sure only the eNICQ 6 database is selected then select EnicqDBUser at the bottom (public should be selected by default already).

21. Click **OK** to complete Login creation.
22. Test the end-user's database authentication capability from the client machine by having the end user launch the application once it has been installed.
23. Set up SQL backups and secure your data according to your organization's policies.

END OF SERVER-SIDE ACTIONS

Appendix A: Multi-Center Installations

The eNICQ application is capable of hosting data for multiple centers. There are several ways this can be accomplished:

1. Hosting multiple centers in a single instance of the database (recommended)
2. Hosting multiple centers in separate instances of the database on a common server and multiple copies of the eNICQ application on SEPARATE client machines
3. Hosting multiple centers in separate instances of the database on separate servers and clients

To determine the model that is best suited for your needs, we suggest you consider the following questions:

- Do any of the end users need to have access to more than one center?
- Do any of the end users need have access to more than one center from a single machine?
- Are there any legal or policy impediments to hosting data for multiple centers in a common database?
- Who will be hosting and maintaining the database? Who owns the hardware and employs the staff that will have access to it? Are all necessary legal agreements or releases in place?
- Do your staff members have permission to view data belonging to different centers or are their permissions limited to a single center?
- Who among your staff would be permitted to view data for all centers and manage center data permissions for other staff members?
- Do the centers currently have an eNICQ database in operation? What versions are any existing databases? Where are these databases located?

If you are uncertain of the answers to any of the above questions, work with your team to reach a better understanding of your situation and what you would like to accomplish.

Option 1: Hosting multiple centers in the SAME database (Recommended)

Vermont Oxford Network's recommendation is that whenever possible, data in a multi-center installation be hosted in a single instance of the eNICQ database. This model allows user permissions and security to be centrally managed and provides the most reliable maintenance and annual update options. This model requires co-mingling of data from separate centers in the same database. Access to each center is controlled either by your IT department who will add or remove users from the Active Directory groups or by your VON Services Administrator [who can grant access from the Member's Portal](#) on our website.

Installation

No additional steps are required to install eNICQ under this model. Vermont Oxford Network recommends using a Standard or Enterprise Edition of SQL Server® rather than a local installation using SQL Server® Express and using AD integration for single sign on as described at the beginning of this guide.

Migrating Center Data

New centers can be added to the database easily. The instructions for this process can be found in the “Moving the eNICQ 6 Database” guide, available at <https://vtoxford.zendesk.com/hc/en-us/articles/360018893413-eNICQ-6-Moving-the-Database-Guide>. Use the instructions in the second section titled “Option 2: Moving the Database by XML.” This procedure involves outputting a text file of the infant records, de-registering the database with our support team, adding the center to the new database, archiving the old database, and importing the new data into the combined database. Audit logs from the old database **cannot** be imported to the new database, but they can be output to text file and archived.

If there is no existing data for the new center, add the center by opening the [Advanced Menu Options \(the gear icon in the top right\)...Center Management...Add New Center button](#). eNICQ 6 will ask for the License Key for the center which is being added. If you are using Active Directory logins it will then ask you for the AD group names. eNICQ 6 allows you to use different AD groups for each center even when they are installed on the same database, controlling which centers’ data user will have access to.

Managing User Access

It is possible to activate or deactivate access to each center for each User level account. If you are using VON logins your staff controls access rights for your users through the Member’s Portal on the VON website. If you are using Active Directory, then your IT department would control who has access by adding or removing users from the Active Directory groups. It is up to your centers to determine the access appropriate to each user. The VON Services Administrators for each center will be the ones to [manage the accounts for eNICQ 6 users](#).

Applying Annual Updates

There are no unique requirements for applying updates with this model.

Removing a Center

If it is necessary to later remove a center from the co-hosted model, this can be done by deleting the center. We recommend first outputting the data to a text file for future recovery. See the document “Moving the eNICQ Database” for instructions. After securing an archive copy of the data, remove the center by clicking **Advanced Menu Options (the gear icon in the top right)...Center Management...Deactivate**. This operation requires an Administrator level account in eNICQ. Once this is done you will need to contact VON Support and we will deactivate the registration of the database for that center so they can be added to your other database.

Option 2: Hosting multiple centers in separate databases on the same server and installing

multiple eNICQ applications on SEPARATE client machines

It is possible to set up multiple copies of the database on a single server and connect to them through separate instances of the eNICQ client application. In this model, each client application on each computer will point to only one instance of the eNICQ database that hosts data for a single center. Control of user access under this model is de-centralized and potentially confusing but can be done successfully with appropriate documentation practices.

Installation

This model requires additional steps during installation to bypass safeguards in the installer intended to prevent accidental creation of multiple databases and multiple copies of the client application.

- To create multiple instances of the database, name (or rename if already existing) your database with the convention “**eNICQ6db_**” + **[center number]**. This will allow you to host multiple instances of the database on the same server and to clearly identify those databases by center number.
- When installing the client applications on each machine, it is critical to point the client application to the correct database. You will need to manage the different [connection files](#) for each database carefully as they will all be named “Connection.enicq”. Changing the name of the file will cause the eNICQ 6 client to not be able to connect with whichever database it is supposed to connect with.

Please note that with each eNICQ client pointing to a different database, your encrypted connection files will also be unique and cannot be used interchangeably. Any on-screen tips or tech support advice on reusing or transplanting Connection.enicq files should be ignored.

Migrating Center Data

Introducing new center data to this model can be done with the document “Moving the eNICQ Database.” Use the instructions in the first section titled “Option 1: Moving the Database Using Backup and Restore.” After completing the procedure, rename your database with the convention “**eNICQ6db_**” + **[center number]**.

Managing User Access

This model does not offer centralized management of user access. Each client/database combination must be managed separately for both database access (at the server level) and application access (either with Active Directory groups or by managing the permissions from the Member’s Area of our website depending upon the login type selected during installation).

Please note that the primary means of controlling access to each center with this model begins with whether a copy of the client keyed to the center’s database is installed on a user’s computer in the first place. Secondly, access can be controlled at both the database and application levels. Because these steps will need to be repeated for each separate instance of client and database, access control can potentially become confusing and burdensome under this model. Confusion can be mitigated by maintaining accurate documentation of the model.

Applying Annual Updates

There are no unique requirements for applying updates with this model.

Removing a Center

Because each center is hosted in a separate database instance in this model, a center can be removed first by logging into the client and clicking **Advanced Menu Options (the gear icon in the top right)...Center Management...Deactivate** and then by detaching the database from the server and deactivating the eNICQ instance that pointed to it. Next, uninstall (using Add/Remove Programs) any instance of the application that pointed to the database.

Documentation

It is essential that you document the aspects of your implementation that are unique. This includes your naming of database instances, the client machines that point to those database instances, as well as the names of the end users and the permissions they are to be granted in each instance. The eNICQ application is subject to mandatory annual updates and it will be difficult to perform these updates without a complete understanding of your implementation.

Limitations of Support

If you have implemented this model, please notify Vermont Oxford Network's technical support staff of your alternate implementation on all support inquiries so that our assistance can be tailored to your unique situation. Our technical support staff will not be able to adequately serve you without this information.

Option 3: Hosting multiple centers in separate databases on SEPARATE servers and installing multiple eNICQ applications on SEPARATE client machines

If you intend to host multiple centers on separate servers and access them through separate clients, there is no integration to manage. These are separate installations even if they exist in the same physical facility. No special instructions are needed. Vermont Oxford Network always recommends that your implementation be documented so that IT staff performing maintenance or upgrades can easily determine which servers, databases, and clients are relevant to different centers and end users.

END OF DOCUMENT