

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Purpose . . . . .	3
1.2	Target audience . . . . .	3
1.3	Overview . . . . .	3
<b>2</b>	<b>System requirements</b>	<b>5</b>
2.1	Hardware requirements . . . . .	5
2.1.1	Minimum hardware requirements . . . . .	5
2.1.2	Recommended hardware configuration . . . . .	5
2.2	Operating system . . . . .	6
2.3	Microsoft .NET Framework 2.0 SP2 . . . . .	7
2.4	Microsoft .NET Framework 3.5 SP1 . . . . .	7
2.5	Microsoft Visual C++ 2010 Redistributable . . . . .	7
2.6	Microsoft XML 6.0 SP1 . . . . .	7
2.7	Windows Installer 4.5 . . . . .	7
2.8	Permissions . . . . .	8
2.9	Security software . . . . .	8
2.9.1	Anti-Virus . . . . .	8
2.9.2	Firewall and proxy servers . . . . .	8
<b>3</b>	<b>Installation procedure</b>	<b>11</b>
3.1	Installing a new BioNumerics instance . . . . .	11
3.1.1	Prerequisites . . . . .	11
3.1.2	Existing instances detected . . . . .	12
3.1.3	Welcome dialog . . . . .	12
3.1.4	Software End User License Agreement . . . . .	12
3.1.5	Customer information . . . . .	13
3.1.6	Setup Type . . . . .	14
3.1.7	Choose destination location . . . . .	14
3.1.8	Select features . . . . .	15
3.1.9	Database Engine properties . . . . .	17
3.1.10	NetKey+ connection settings . . . . .	18
3.1.11	Confirm installation . . . . .	19
3.1.12	NetKey+ configuration . . . . .	19
3.1.13	Setup INI XML file . . . . .	19
3.2	Updating a BioNumerics instance . . . . .	20
3.2.1	Welcome dialog . . . . .	20
3.2.2	Software End User License Agreement . . . . .	20
3.2.3	Customer information . . . . .	21
3.2.4	Choose destination location . . . . .	22
3.2.5	Select features . . . . .	22
3.2.6	NetKey+ connection settings . . . . .	24
3.2.7	Confirm update . . . . .	25

3.3	Maintenance installation . . . . .	25
3.3.1	Select instance to maintain . . . . .	25
3.3.2	Maintenance options . . . . .	26
3.3.3	Modify maintenance mode . . . . .	26
3.3.4	Repair maintenance mode . . . . .	27
3.3.5	Remove maintenance mode . . . . .	28
3.4	Installing Protection Keys . . . . .	28
3.4.1	Protection Key Types . . . . .	28
3.4.2	Install Protection Key Driver . . . . .	29
3.4.3	Activate Sentinel HASP SL key . . . . .	29
3.5	Setup log . . . . .	35
3.6	Silent installation . . . . .	38
3.6.1	Purpose . . . . .	38
3.6.2	Installation procedure . . . . .	38
3.6.3	Setup INI XML file format . . . . .	39
<b>4</b>	<b>NetKey+ configuration</b>	<b>41</b>
4.1	Introduction . . . . .	41
4.2	Installing and starting the NetKey+ service on the server . . . . .	41
4.3	Configuring licenses . . . . .	45
4.4	Running sessions on the clients . . . . .	49
4.5	Monitoring sessions . . . . .	49
4.6	Logging data . . . . .	51
4.7	Resetting the NetKey+ settings . . . . .	51
4.8	Repairing the NetKey+ service . . . . .	52
4.9	Overview of configuration rights . . . . .	53
4.10	Usage statistics . . . . .	53
4.10.1	Usage information parse tool . . . . .	53
4.10.2	Example . . . . .	55
<b>5</b>	<b>Installation process</b>	<b>59</b>
5.1	Overview . . . . .	59
5.2	Setup dialog list . . . . .	59
5.3	Setup processes . . . . .	59
5.3.1	Read command line options . . . . .	59
5.3.2	Read global variables . . . . .	60
5.3.3	Write global variables . . . . .	60
5.3.4	Save Setup INI XML file . . . . .	60
5.3.5	Read requested features . . . . .	60
5.3.6	Save Setup Log . . . . .	61
5.3.7	OnMoveData . . . . .	61
5.3.8	Feature functions . . . . .	61
5.4	Setup Process list . . . . .	64
<b>6</b>	<b>Command line options</b>	<b>67</b>
6.1	Running BioNumerics from the command line . . . . .	67
6.2	Running the startup program from the command line . . . . .	68
<b>7</b>	<b>Granting access to BioNumerics databases</b>	<b>69</b>

## NOTES

### SUPPORT BY APPLIED MATHS

While the best efforts have been made in preparing this manuscript, no liability is assumed by the authors with respect to the use of the information provided.

Applied Maths will provide support to research laboratories in developing new and highly specialized applications, as well as to diagnostic laboratories where speed, efficiency and continuity are of primary importance. Our software thanks its current status for a part to the response of many customers worldwide. Please contact us if you have any problems or questions concerning the use of BioNumerics<sup>®</sup>, or suggestions for improvement, refinement or extension of the software to your specific applications:

#### **Applied Maths NV**

Keistraat 120  
9830 Sint-Martens-Latem  
Belgium  
PHONE: +32 9 2222 100  
FAX: +32 9 2222 102  
E-MAIL: [info@applied-maths.com](mailto:info@applied-maths.com)  
URL: <http://www.applied-maths.com>

#### **Applied Maths, Inc.**

8834 N. Capital of Texas Hwy, Suite 280  
Austin, Texas 78759  
U.S.A.  
PHONE: +1 512-482-9700  
FAX: +1 512-482-9708  
E-MAIL: [info-US@applied-maths.com](mailto:info-US@applied-maths.com)

### LIMITATIONS ON USE

The BioNumerics<sup>®</sup> software, its plugin tools and their accompanying guides are subject to the terms and conditions outlined in the License Agreement. The support, entitlement to upgrades and the right to use the software automatically terminate if the user fails to comply with any of the statements of the License Agreement. No part of this guide may be reproduced by any means without prior written permission of the authors.

**Copyright ©1998, 2014, Applied Maths NV. All rights reserved.**

BioNumerics<sup>®</sup> is a registered trademark of Applied Maths NV. All other product names or trademarks are the property of their respective owners. BioNumerics<sup>®</sup> includes the Python<sup>®</sup> 2.6 release from the Python Software Foundation (<http://www.python.org/>) and a library for XML input and output from Apache Software Foundation (<http://www.apache.org>). The BLAST sequence search tool is based on the NCBI toolkit version 2.2.10 (<http://www.ncbi.nlm.nih.gov/BLAST/>).



# Chapter 1

## Introduction

### 1.1 Purpose

---

The purpose of this document is to provide understandable and detailed information on how to install the various features of BioNumerics. These features include the application software, sample and tutorial data, the NetKey+ server program and the Sentinel drivers.

### 1.2 Target audience

---

The target audience for this document is anyone who is responsible for installing and configuring BioNumerics or the NetKey+ licensing server program. This document assumes that the person who will install BioNumerics or the NetKey+ service has a basic knowledge on how to administer a Windows client computer.

### 1.3 Overview

---

The BioNumerics Setup program is an InstallShield installation wizard that allows a person with Administrator privileges to install the BioNumerics application or the NetKey+ licensing server program on a target computer. In addition, the Setup program will optionally install the *Database Engine* and install or upgrade the Sentinel and HASP drivers.

The BioNumerics Setup package is regularly updated and can be delivered on CD-ROM, or can be downloaded from the Applied Maths website (<http://www.applied-maths.com/download/software>).



## Chapter 2

# System requirements

### 2.1 Hardware requirements

---

#### 2.1.1 Minimum hardware requirements

---

The minimum hardware requirements for running the BioNumerics application are the cumulative requirements needed to run the Operating System, the BioNumerics application, the optional **Database Engine** and any third-party software that will run concurrently (e.g. Microsoft Office).

The typical minimum hardware requirements for a computer running Windows Vista, Microsoft Office 2003 and the BioNumerics application are:

- **Processor:** 1.6 gigahertz (GHz) processor or higher
- **Processor Type:** Intel Pentium Dual Core or higher compatible processor
- **Memory:** 2 GB or higher (1 GB if the **Database Engine** feature will not be installed)
- **Hard disk:** 2 GB of free disk space (application files only)
- **Display:** WXGA (1280 x 800) or higher resolution monitor, True Color (32 bit)
- **USB port:** Depending on the license type a free USB port may be required

For *standalone licenses*, each computer that will run BioNumerics must have an available USB port for connecting the Sentinel hardware security key. For *network licenses*, the computer that will be running the NetKey+ server program must have a free USB port for attaching the hardware security key. *Internet licenses* do not require a hardware security key, hence an USB port is not needed.

A 64-bit processor and Windows version are required for systems with more than 4 GB of RAM installed.



The actual hardware requirements will largely depend on the features that will be used in BioNumerics, the database platform used to store the BioNumerics data and the size of the data. For example, the Power Assembler feature of the Sequence data module requires a 64-bit processor and a minimum of 8 GB installed memory.

#### 2.1.2 Recommended hardware configuration

---

The recommended hardware configuration for a computer running the latest Windows and Office versions, and the BioNumerics application are:

- **Processor:** 1.8 gigahertz (GHz) processor or higher
- **Processor Type:** Intel Core 2 Duo Processor or higher compatible processor
- **Memory:** 2 GB or higher
- **Hard disk:** 2 GB of free disk space (application files only), fast hard drive for storing database files (e.g. 7200 RPM SATA drive)
- **Display:** WXGA+ (1440 x 900) or higher resolution monitor, True Color (32 bit), graphics card with dedicated video memory

When purchasing a new computer that will run BioNumerics, make sure that you choose a 64-bit Windows version to allow for future memory expansion. At least 4 GB of RAM should be installed when purchasing a new system.

A recent graphics card with dedicated video memory is recommended. Choosing a basic Windows theme instead of a Windows 7 or Vista Aero theme may be required if the computer is not equipped with sufficient dedicated video memory.



Some features of BioNumerics may require hardware specifications that exceed the above recommendations. For example, the Power Assembler feature of the Sequence data module requires a 64-bit processor, a minimum of 8 GB installed memory and a fast storage system (SSD).

## 2.2 Operating system

---

Generally Applied Maths will support installing BioNumerics on Windows operating system versions for which the Microsoft Extended Support Phase (see <http://support.microsoft.com/gp/lifeselect>) has not been retired. This will allow you to obtain support and security updates from Microsoft for the target operating system.

- Windows XP (with Service Pack 3) Note that the Microsoft Extended support for Service Pack 3 will end on the 8th of April 2014.
- Windows Vista (with Service Pack 2)
- Windows 7
- Windows 8
- Windows 2003 Server (with Service Pack 2)
- Windows 2008 Server (RTM with Service Pack 2 or R2)

Applied Maths recommends installing BioNumerics on a workstation or server with the latest Microsoft service packs installed. BioNumerics can be installed on 64-bit versions of Windows if the WoW64 (Windows 32-bit On Windows 64-bit) subsystem is installed and enabled.

The NetKey+ licensing server program should preferably be installed on a computer running Windows Server 2008 or 2003. If a Windows Server computer is not available, then the NetKey+ program can be installed on a Windows XP or later client operating system.



## 2.3 Microsoft .NET Framework 2.0 SP2

---

The Microsoft .NET Framework 2.0 Service Pack 2 is required to be able to run the BioNumerics Setup. New installation functions have been added to the AppliedMaths.SetupFramework.dll .NET assembly, and this library requires the Microsoft .NET Framework 2.0 runtime.

The Setup will install the Microsoft .NET Framework 2.0 SP2 on Windows Vista, Windows Server 2008 RTM and older Windows versions.

Note that the Setup will attempt to install the Microsoft .NET Framework 3.5 Service Pack 1 Windows feature on Windows 7, Windows Server 2008 R2 and later versions, instead of installing Microsoft .NET Framework 2.0 SP2.

## 2.4 Microsoft .NET Framework 3.5 SP1

---

Microsoft .NET Framework 3.5 Service Pack 1 is a cumulative update that contains many new features building incrementally upon .NET Framework 2.0, 3.0, 3.5, and includes .NET Framework 2.0 Service Pack 2 and .NET Framework 3.0 Service Pack 2 cumulative updates.

The BioNumerics *Database Engine* feature is dependent on the Microsoft .NET Framework 3.5 Service Pack 1 runtime. The *Database Engine* feature installs a BioNumerics instance of Microsoft SQL Server 2008 R2 SP1 Express Edition; hence the corresponding prerequisites must be installed prior to installing this feature.

Note that the Setup will attempt to install the Microsoft .NET Framework 3.5 Service Pack 1 Windows feature on Windows 7, Windows Server 2008 R2 and later versions, even if the BioNumerics *Database Engine* feature was not selected for installation.

## 2.5 Microsoft Visual C++ 2010 Redistributable

---

The Setup will install the Microsoft Visual C++ 2010 Redistributable package on the target computer prior to installing any application files. The redistributable is required to be able to run C++ applications like BioNumerics.

On 32-bit computers only the x86 version will be installed. On 64-bit computers the x86 and x64 versions of the Microsoft Visual C++ 2010 Redistributable will be installed.

## 2.6 Microsoft XML 6.0 SP1

---

The Microsoft Core XML Services (MSXML) 6.0 are required to be able to run the BioNumerics Setup. This version has been included with Windows XP Service Pack 3. All other supported operating systems also include Microsoft XML 6.0.

The BioNumerics Setup uses the "Msxml2.DOMDocument.6.0" COM object for reading and writing to the Setup INI and log files. Hence MSXML 6.0 must be installed before running the BioNumerics Setup.

## 2.7 Windows Installer 4.5

---

The BioNumerics Setup will install Windows Installer 4.5 on Windows XP SP2, Windows Server 2003 SP1 and Windows Server 2008 or newer Windows versions, if the required Windows Installer version is not

installed.

The **Database Engine** feature (Microsoft SQL Server 2008 R2 Express Setup) requires Microsoft Windows Installer 4.5 or a later version.

Windows Installer version 4.5 is included with Windows Vista SP2 and Windows Server 2008 SP2. Windows Installer version 5.0 is included with Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012. Hence the BioNumerics Setup will not install Windows Installer on these operating systems.

## 2.8 Permissions ---

The user running the BioNumerics Setup package must have full Administrator privileges on the computer(s) where the Setup program will run. In addition the user must have MODIFY NTFS folder permissions and FULL CONTROL share permissions (if applicable) on the database home directory, for example when this folder will be located on a file server and will be accessed via a file share.

## 2.9 Security software ---

### 2.9.1 Anti-Virus ---

To optimize the performance of the BioNumerics Setup program it is recommended to temporarily disable the real-time protection or on-access scanning features while running the installer. More specifically anti-virus software may considerably slow down the installation of the **Database Engine** feature.

Anti-virus software may also affect the performance of the BioNumerics application. If you notice a significant difference in responsiveness when the anti-virus tool is enabled compared to when the tool is disabled, it may be recommended to exclude the anti-virus tool from scanning the BioNumerics executables (bn-start.exe and bn.exe), the DLL and BXT sub-folders and specific file extensions (\*.dll, \*.mdb, \*.bpl) in the application and database folders.

In addition, the anti-virus software must be properly configured to be compatible with the database platform used to host the BioNumerics databases. Most database software vendors require that the directories containing data and log files are excluded from anti-virus scanning.

If the **Database Engine** feature has been selected for installation the following exclusions should be configured in the anti-virus software:

- Do not scan files with the \*.mdf, \*.ldf, \*.ndf and \*.bak file-name extensions
- Exclude the Microsoft SQL Server 2008 R2 Express process from virus scanning: Program Files \Microsoft SQL Server \MSSQL10\_50.BioNumerics \MSSQL \Binn \sqlservr.exe

For Microsoft SQL Server, please check the following article for more details: "Guidelines for choosing anti virus software to run on the computers that are running SQL Server", <http://support.microsoft.com/kb/309422>.

### 2.9.2 Firewall and proxy servers ---

For BioNumerics internet and evaluation licenses, network filtering software and firewall devices may need to be configured to allow access to TCP port 80 on the Applied Maths license servers.

Currently, the following license servers are active to verify internet licenses:

- license1.applied-maths.com (81.246.4.66)
- license2.applied-maths.com (81.246.4.69)
- license3.applied-maths.com (71.42.72.154)
- license4.applied-maths.com (71.42.72.154)

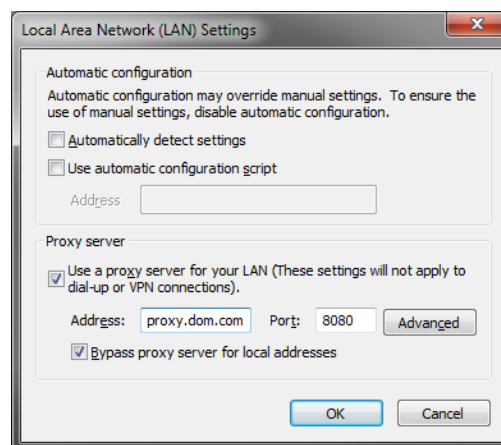
The BioNumerics application requires access to the above internet domain names and public IP addresses to be able to validate internet and evaluation licenses. Note that the IP addresses of the license servers may change in the future, hence firewall exception rules based on the internet domain name should be preferred.

In addition, several BioNumerics plugins require access to specific internet domains to be able to download relevant data:

- .applied-maths.com
- .pubmlst.org (for the *MLST online plugin*)
- .pasteur.fr (for the *MLST online plugin*)
- .mlst.ucc.ie (for the *MLST online plugin*)
- .ridom.de (for the *Spa typing plugin*)

If applicable for your configuration, you may need to grant the BioNumerics application internet access to the above domain names.

If internet access is only allowed through a proxy server, the corresponding settings must be properly configured for the Microsoft Internet Explorer browser (see Figure 2.1). The BioNumerics application will use the same settings when connecting to the internet. In other words, if an automatic configuration script (\*.pac file) or a static proxy server address has been configured for Internet Explorer, BioNumerics will inherit these LAN settings to connect to the internet.



**Figure 2.1:** The *LAN Settings* dialog box.

Network licenses of BioNumerics require that a NetKey+ server has been configured to manage the license sessions. All computers running BioNumerics must be configured to allow access to the listening TCP port on the NetKey+ server computer. Also, the server computer must allow incoming access for the TCP ports used by the NetKey+ server program. For details please check 4.



## Chapter 3

# Installation procedure

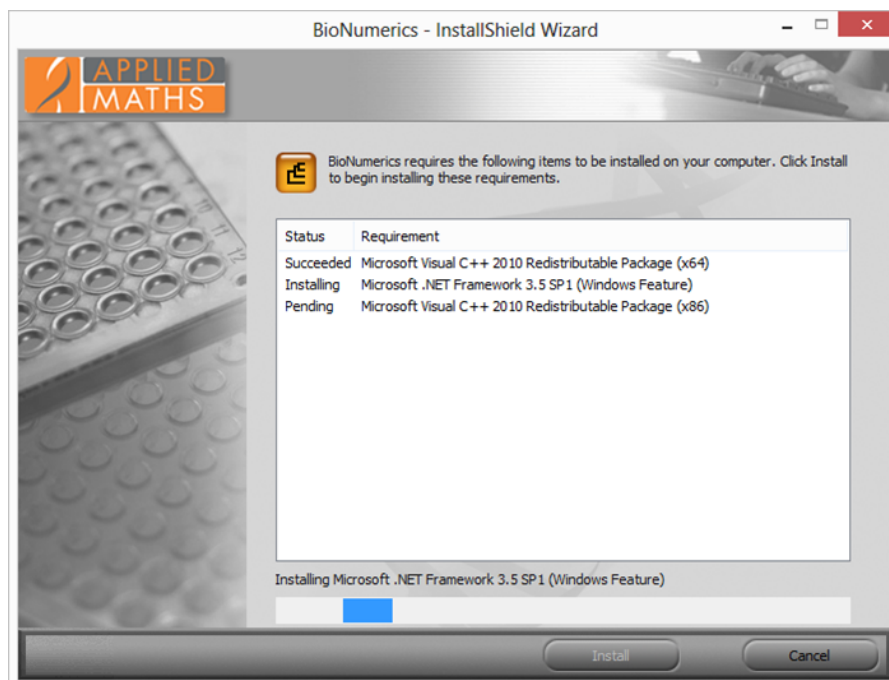
### 3.1 Installing a new BioNumerics instance

---

#### 3.1.1 Prerequisites

---

The *Prerequisites dialog* shows the items that are required to be installed on the local computer before any of the BioNumerics features can be installed (see Figure 3.1).



**Figure 3.1:** The *Prerequisites dialog*.

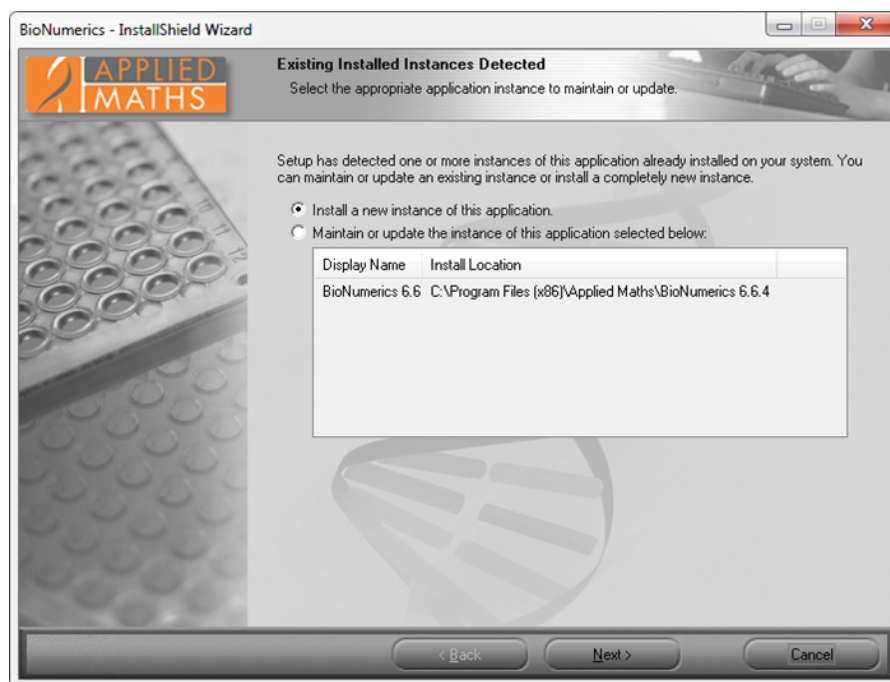
Click on the <**Install**> button to start the installation of the missing prerequisites.



It is recommend to install the Setup prerequisites as described in 2 prior to launching the Setup in **Silent installation** mode (see 3.6). For example the silent installation will fail if the Setup is not able to download and install the Microsoft .NET Framework 3.5 SP1.

### 3.1.2 Existing instances detected

The BioNumerics 6.5 or later Setup package supports installing multiple instances of the same application side-by-side. Each BioNumerics instance will have a dedicated application installation path, and will have a set of start menu and desktop shortcuts. If an instance of BioNumerics 6.5 or later is already installed then the *Existing Installed Instances Detected* dialog will appear when launching the Setup executable (see Figure 3.2).



**Figure 3.2:** The *Existing Installed Instances Detected* dialog.

This dialog allows you to choose between installing a new BioNumerics instance, and changing an existing instance. Choose the ***Install a new instance of this application*** option to install a new instance of the BioNumerics application.



The above dialog will not appear if BioNumerics 6.1 or older versions are already installed since these applications were installed with a Setup program that was not yet multi-instance aware. In this case the welcome dialog will be displayed with an update message.

### 3.1.3 Welcome dialog

If no instance of BioNumerics is detected on the local computer, the *Welcome dialog box* will display the version number of BioNumerics that is included with the Setup package when launching the Setup executable. Please verify that you are installing the correct version and click **<Next>** to continue.

### 3.1.4 Software End User License Agreement

The next dialog will display the Software End User License Agreement (EULA) (see Figure 3.3). Please read the EULA carefully and click the top ***I accept the terms of the license agreement*** radio button and the **<Next>** button to continue the installation. Click **<Cancel>** if you do not agree with the license agreement; this will abort the installation. The Software End User License Agreement document can be printed to the default printer by clicking the **<Print>** button. The **<Save>** button allows you to browse to a folder where you want to save the Applied Maths EULA.PDF Acrobat document.



Figure 3.3: The *License Agreement* dialog box.

### 3.1.5 Customer information

The *Customer information dialog box* allows you to enter the user and organization names, and the BioNumerics license string (see Figure 3.4). You must enter a valid license string to be able to continue with the installation. In addition, the user and organization names cannot be empty. The license string is provided on the sleeve of the CD-ROM or you may have obtained it electronically.

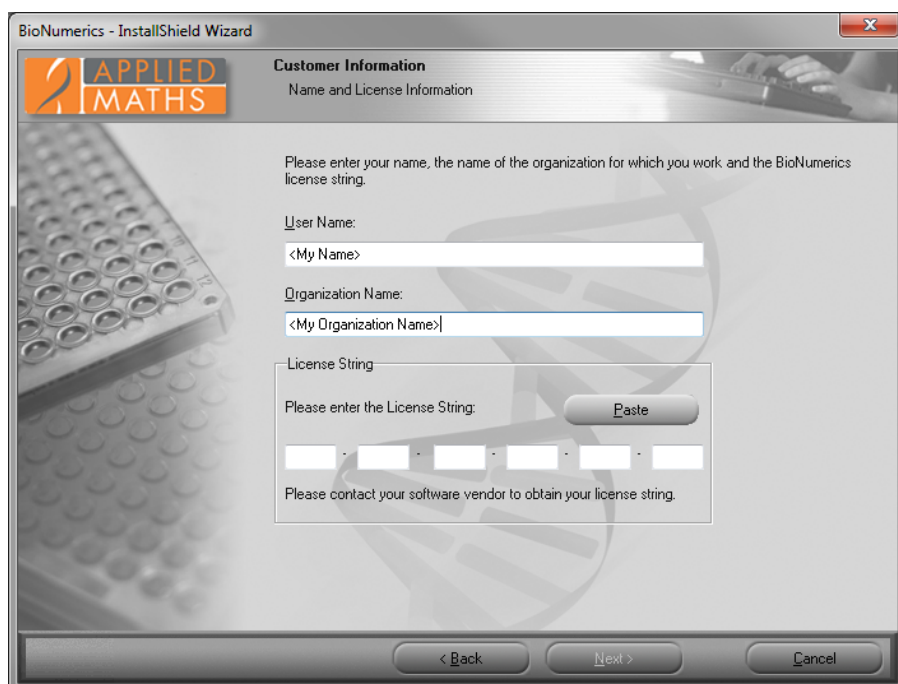


Figure 3.4: The *Customer Information* dialog box.

### 3.1.6 Setup Type

In the *Setup Type* dialog you can choose between a **Default** and a **Custom** setup configuration.

The **Default** setup configuration will install all BioNumerics features with default settings. These settings include the destination paths for the application and data, and the database engine configuration. Note that the **Default** setup configuration does not include the **NetKey+ server program**.

The **Custom** setup configuration allows you to select the features you want to install, choose the target paths for the application and data, and the database engine configuration. The **Custom** setup configuration also allows you to install the **NetKey+ server program**.

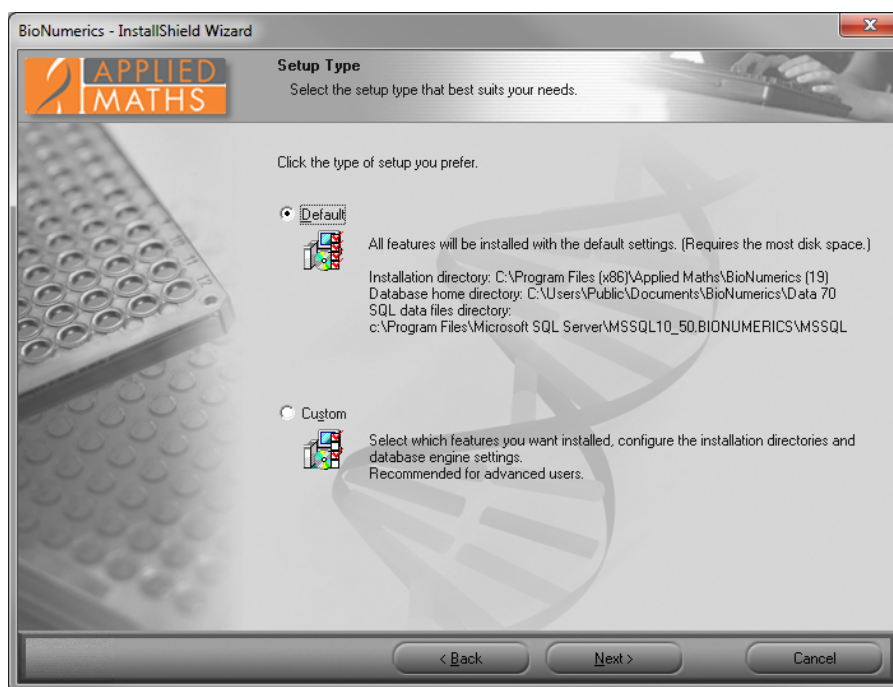


Figure 3.5: Choose setup type.

### 3.1.7 Choose destination location

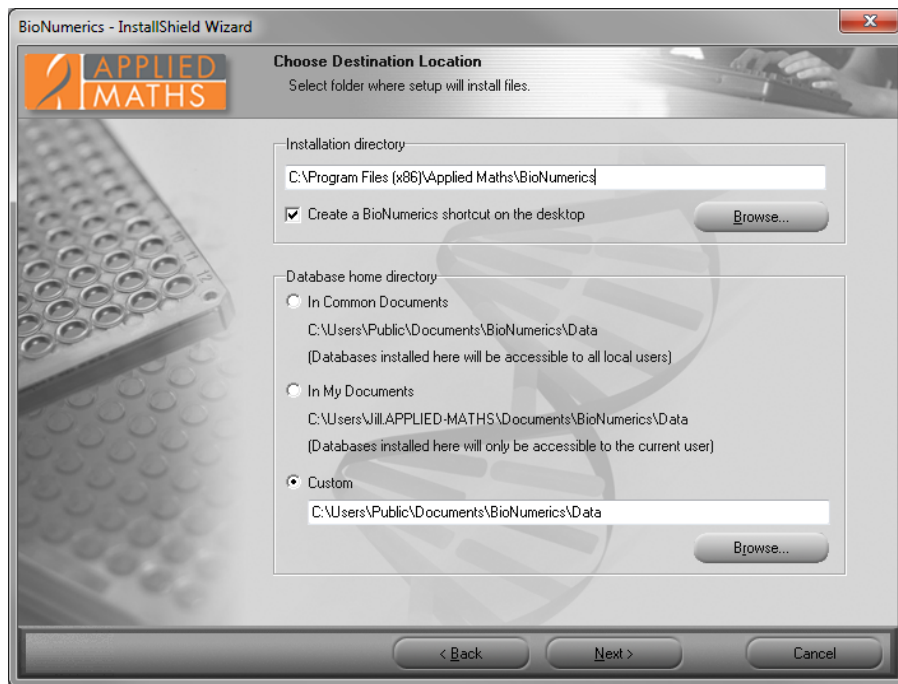
The installation directory for the BioNumerics application and the database home directory can be entered in the *Choose Destination Location* dialog box (see Figure 3.6).

The top **<Browse>** button allows you to navigate to a custom installation path for the BioNumerics application. A BioNumerics shortcut will be created on the desktop when the option **Create a BioNumerics shortcut on the desktop** is checked.

Two default locations can be selected for the database home directory: **In Common Documents** and **In My Documents**. The **In Common Documents** option will store the BioNumerics databases in the public documents folder. As a result, the databases will be available to all users on the local computer. The **In My Documents** option will store the BioNumerics databases in the personal documents folder and by default the databases will only be available to the current user.

The third **Custom** option allows you to enter a path on the local computer or even on a remote file server via a permanent network drive. The lower **<Browse>** button will be enabled if the **Custom** radio button has been selected for the database home directory. Note that all BioNumerics users that will access data in the database home directory must have MODIFY NTFS permissions. In addition, the FULL CONTROL permissions must be granted at the file share level when the directory is located on a remote file server.

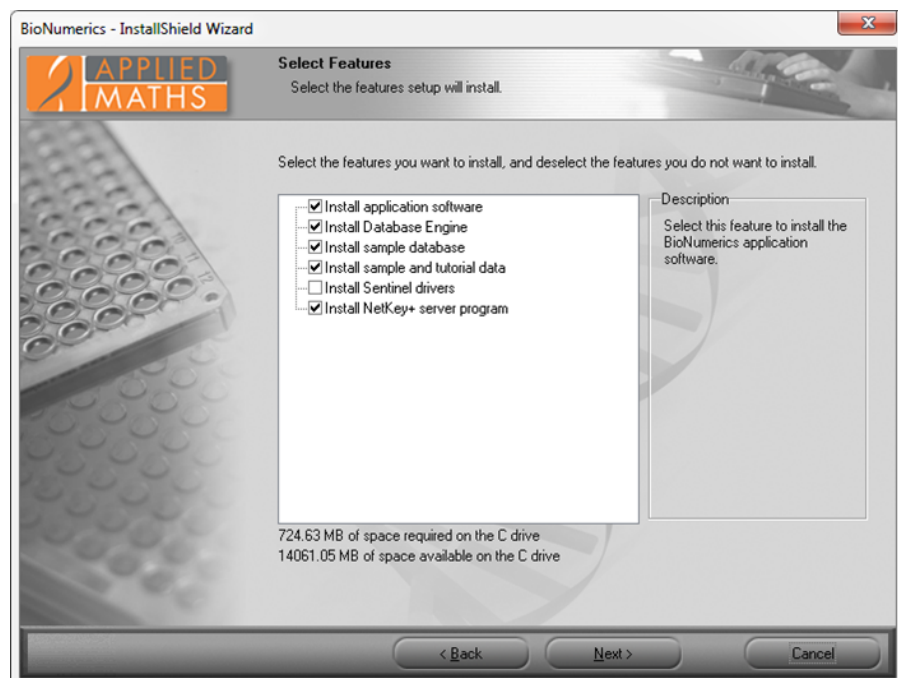




**Figure 3.6:** The *Choose Destination Location* dialog box.

### 3.1.8 Select features

The BioNumerics features that you want to install on the local computer can be selected in the *Select Features* dialog box (see Figure 3.7). Clicking on a feature in the left pane will display a short description in the right pane. Tick the appropriate check boxes for the features you want to install.



**Figure 3.7:** The *Select Features* dialog box.

**Install application software:**

- In case of a *standalone license*, the **Application software** needs to be installed on each computer that you want to use to run the software. Please note that only on the computer where the dongle is attached to, you will be able to work with the software.
- In case of an *internet license*, the **Application software** needs to be installed on the computer that you want to use to run the software. Please note that a permanent and stable internet connection is required to run the internet license.
- In case of a *network license*, the **Application software** needs to be installed on the computers in the network that you want to use to run the software.

#### Install Database Engine:

- Checking this option will install the BioNumerics instance of Microsoft SQL Server 2008 R2 Express SP1 **Database Engine**. The location of the data files can be specified in the next step.

#### Install sample database and Install sample and tutorial data:

- The **Sample database** and **Sample and tutorial data** that are contained in the Setup package are used in the manual to illustrate the features of the software. Selecting these features will install the **Sample database** and **Sample and tutorial data** in the BioNumerics home directory that is specified in the *Choose Destination Location dialog box* (see Figure 3.6).

#### Install Sentinel drivers:

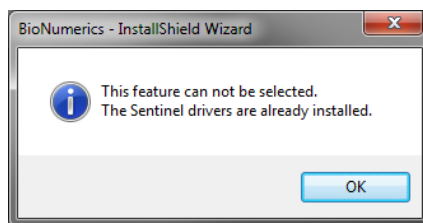
The **Install Sentinel drivers** feature will install version 7.5.7 of the Sentinel System Driver. In addition this feature will also install the Sentinel Run-time Environment (previously known as HASP) version 6.51 if the NetKey+ server program feature has been selected for installation. The Sentinel Run-time Environment will not be installed if a standalone license string was entered in the *Customer Information dialog box*.

- In case of a *standalone license*, the **Sentinel drivers** need to be installed on each computer that you want to use to run the software.
- In case of an *internet license*, you only need an internet connection to run the software. The **Install Sentinel drivers** option does not need to be checked.
- In case of a *network license*, the **Sentinel drivers** only need to be installed on the NetKey+ server computer in the network.

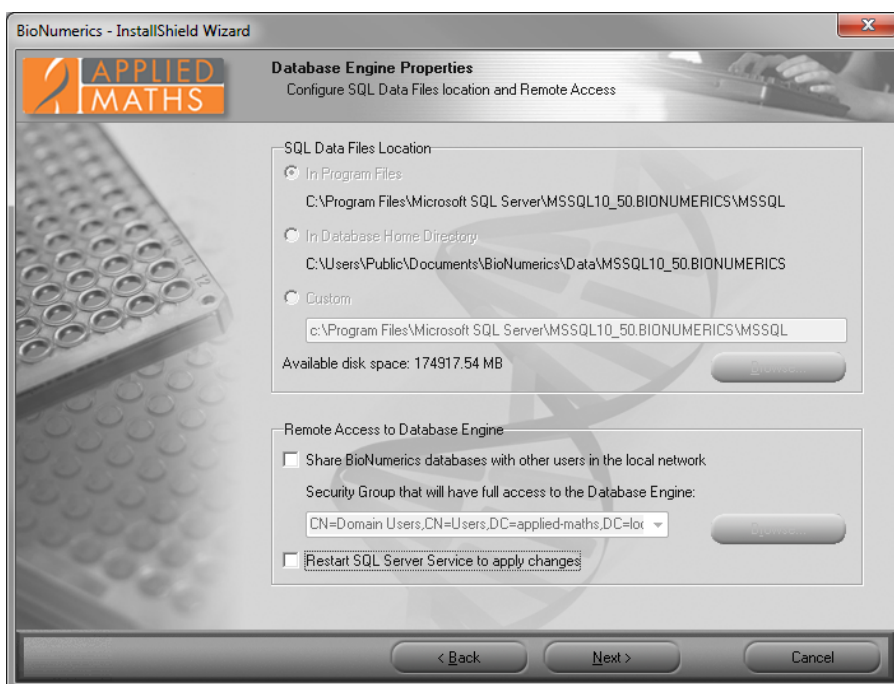
#### Install NetKey+ server program:

- The **NetKey+ server program** feature will only be visible and available for installation if a network license string has been entered in the *Customer Information dialog box* (see Figure 3.4). The **NetKey+ server program** feature must only be installed on the computer in the network where the hardware security key will be connected to.

A message will appear when selecting the **Sentinel drivers** feature and the minimum required version is already installed (see Figure 3.8).



**Figure 3.8:** Sentinel drivers are already installed.



**Figure 3.9:** The *Database Engine Properties* dialog.

### 3.1.9 Database Engine properties

The location of the Microsoft SQL Server 2008 R2 Express data files can be entered in the *Database Engine Properties* dialog (see Figure 3.9). Please make sure to select a local path with sufficient (at least 700MB) free disk space. Network drives and shares are not supported for storing the SQL data files.

In addition this dialog allows you to specify if remote access to the database engine should be enabled. If the BioNumerics databases are shared with other users in the local network then the "Microsoft SQL Server (BioNumerics)" inbound Windows firewall rule will be enabled, and TCP/IP and Named Pipes connections to the database engine will be allowed.

All computers that will be used to access shared BioNumerics databases should be part of the same Active Directory domain. This allows domain users that need to access the shared database engine to be added to an Active Directory security group, and this group can be selected in the *Database Engine Properties* dialog. Subsequently the selected security group will be added to the local BioNumerics Database Administrators Windows group, thus granting full access to the BioNumerics instance of Microsoft SQL Server 2008 R2 Express, and the BioNumerics databases.

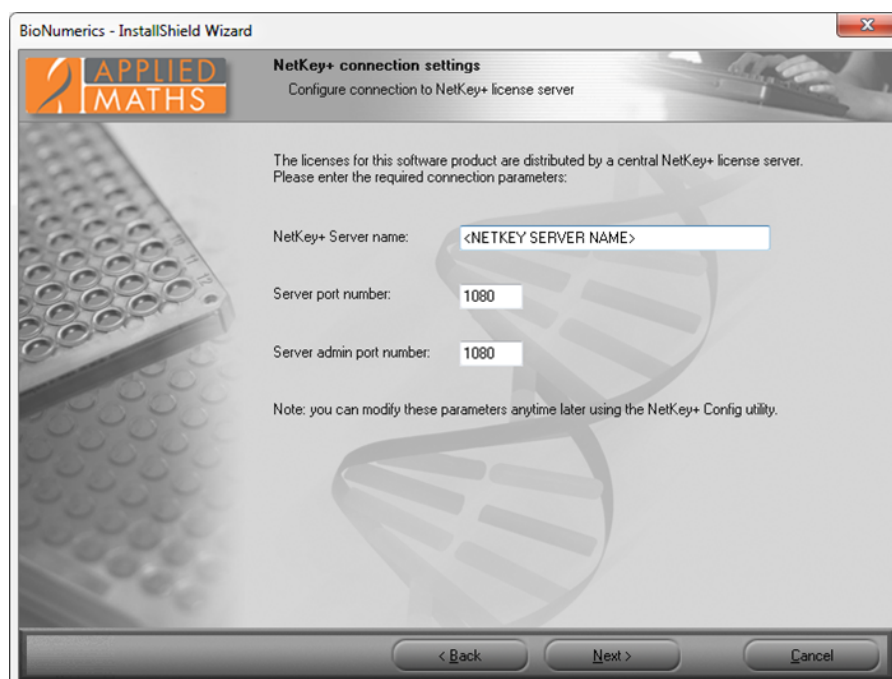
### 3.1.10 NetKey+ connection settings

After pressing the <Next> button, the *NetKey+ connection settings dialog box* will appear (see Figure 3.10) if a network license string was entered in the *Customer Information dialog box* (see Figure 3.4), and if the BioNumerics application feature was selected for installation (see Figure 3.7).

The *NetKey+ Server name*, *Server port* and *Admin port numbers* can be entered in the *NetKey+ connection settings dialog box* (see Figure 3.10). These parameters will allow the BioNumerics application to connect to the NetKey+ server and request a session for the client computer.

- **NetKey+ Server name:** Name of the computer where the NetKey+ license service is running.
- **Server port number:** TCP listening port number of the NetKey+ service running on the NetKey+ server.
- **Server admin port number:** TCP listening port number for configuring the NetKey+ server. This can be the same number as for the Server port, but to increase security a different TCP port number can be configured for administrating the NetKey+ license server. This way the Windows firewall on the NetKey+ server can be configured to only allow remote NetKey+ administration from specific computers.

Please make sure that you enter available TCP port numbers for the NetKey+ Server and admin ports. The Setup will display the following message if the TCP port is already in use: "TCP port 80 is already in use. Please choose an available TCP port".



**Figure 3.10:** The *NetKey+ connection settings dialog box*.

After the BioNumerics application has been installed, the Setup will save the server name and TCP port number to the *NetKey.ini* text file on the client computer. The *NetKey.ini* file is located in the folder containing application data for all users (CommonAppDataFolder). The path of this folder depends on the operating system version.

- Windows Vista or later: C: \ProgramData \Applied Maths \NetKey+

- Windows XP: C: \Documents and Settings \All Users \Application Data \Applied Maths \NetKey+

### 3.1.11 Confirm installation

---

After clicking <Next>, the *Ready to install BioNumerics dialog box* will appear. Click <Install> to start the installation. The <Back> button allows you to review the installation settings, and clicking <Cancel> will cause the installation wizard to exit without modifying your system.

The *Setup Status dialog box* will be displayed after clicking the <Install> button. This dialog will show the name of the feature that is being installed, and the name of the file that is being copied.

The *Install Complete dialog box* will appear after the installation has finished. Click <Finish> to exit the Setup program.

### 3.1.12 NetKey+ configuration

---

If a network license string has been entered in the *Customer Information dialog box* (see Figure 3.4), and the **NetKey+ server program** feature was selected for installation (see Figure 3.7), the Setup will ask if you want to run the NetKey+ Configuration tool (see Figure 3.11). This tool allows you to install and subsequently start the NetKey+ service. Click <Yes> if you want to start the NetKey+ Configuration tool. Click <No> if you do not want to specify the NetKey+ settings at this time. More information about the NetKey+ Configuration tool can be found in 4.

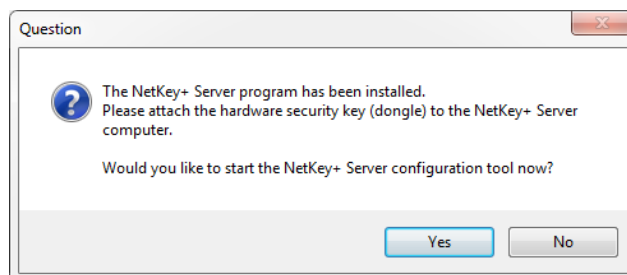


Figure 3.11: Launch the NetKey+ Configuration tool.

### 3.1.13 Setup INI XML file

---

After the dialog sequence, the Setup will record all settings to a Setup INI XML file. This file will be saved to the SetupLogs sub-folder of the BioNumerics installation directory. The file name format is Setup\_x\_ini.XML, where x is a counter to make sure that the file name is unique in the SetupLogs folder.

Each time the Setup program has been launched, and features were installed or removed, a Setup INI XML file will be created. The file will not be created if the Setup was canceled during the initial dialog sequence.

Please attach the Setup log and INI XML files to your e-mail message when reporting Setup issues to the Applied Maths help desk.

After a manual installation of BioNumerics, the Setup INI XML file can subsequently be used to perform silent installations (see 3.6).

## 3.2 Updating a BioNumerics instance

---

### 3.2.1 Welcome dialog

---

#### 3.2.1.1 Updating a 6.1 or older instance of BioNumerics

---

If no existing BioNumerics 6.5 or later instances were detected and an older version of BioNumerics was already installed, then the update *Welcome dialog box* will be displayed when launching the Setup executable (see Figure 3.12). The *Welcome dialog box* will show the version number of the installed instance of BioNumerics and the version that is included in the Setup package.

Click **<Next>** if you want to update the existing version. If you enter the installation directory of the currently installed version in the *Choose Destination Location dialog box*, then the older version will be replaced by the newer version.



Figure 3.12: The *Welcome dialog*.

#### 3.2.1.2 Updating a 6.5 or later instance of BioNumerics

---

If an instance of BioNumerics 6.5 or later is already installed, then the *Existing Installed Instances Detected dialog box* will appear when launching the Setup executable (see Figure 3.13).

Choose the ***Maintain or update the instance of this application selected below*** option to perform an update of the BioNumerics application.

### 3.2.2 Software End User License Agreement

---

The next dialog will display the Software End User License Agreement (EULA) (see Figure 3.14). Please read the EULA carefully and click the top ***I accept the terms of the license agreement*** radio button and the **<Next>** button to continue the installation. Click **<Cancel>** if you do not agree with the license agreement, this will abort the installation. The Software End User License Agreement document can be printed to the



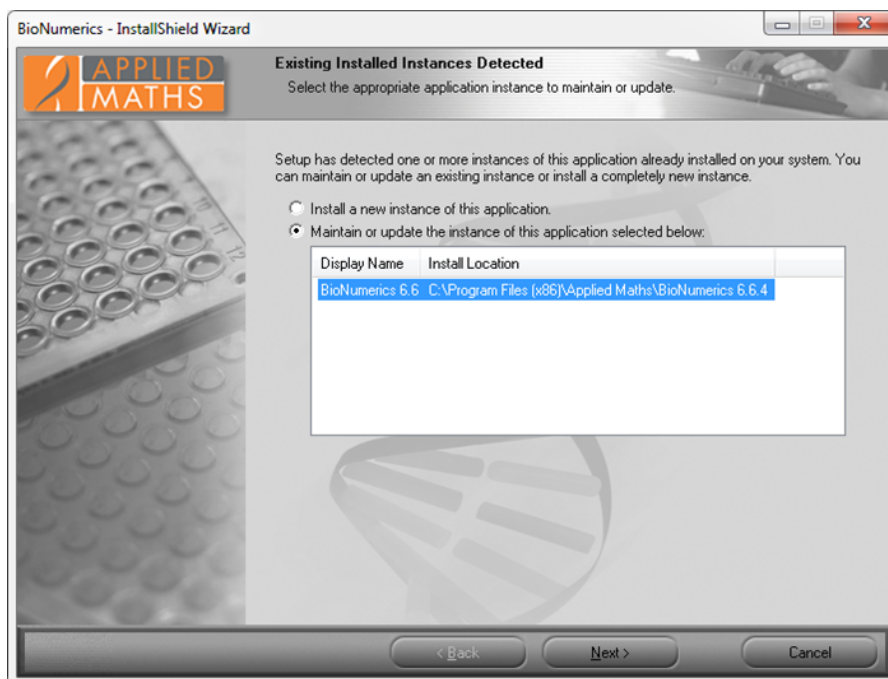


Figure 3.13: The *Existing Installed Instances Detected* dialog box.

default printer by clicking the **<Print>** button. The **<Save>** button allows you to browse to a folder where you want to save the Applied Maths EULA.PDF Acrobat document.

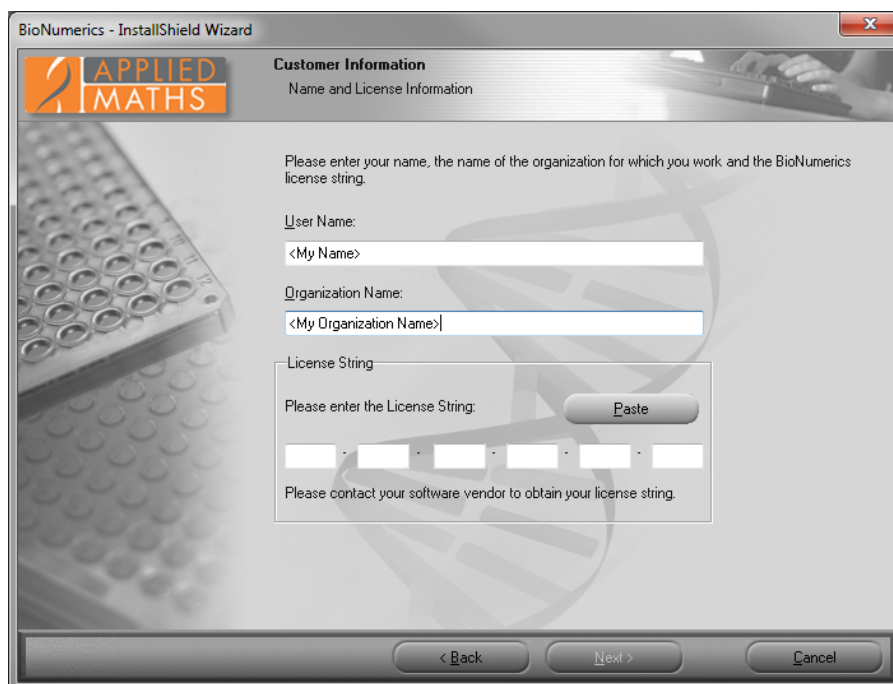


Figure 3.14: The *License Agreement* dialog box.

### 3.2.3 Customer information

If you are installing a new major or minor version of BioNumerics, the *Customer Information* dialog box will be displayed after clicking the **<Next>** button (see Figure 3.15). This dialog allows you to update the

license string for the new version of BioNumerics. By default, a new license string is required for each new minor or major version of BioNumerics. For example, updating version 6.6.4 to 7.0.0 will require a new license string, while updating 6.5.0 to version 6.5.1 will not. You must enter a valid license string to be able to continue with the installation. In addition, the user and organization names cannot be empty.



**Figure 3.15:** The *Customer Information* dialog box.

### 3.2.4 Choose destination location

The *Choose Destination Location* dialog box (see Figure 3.16) will only appear when upgrading a BioNumerics version older than 6.5 (see 3.2.1.1). If you enter the installation directory of the currently installed version, then this version will be replaced by the newer version.



The *Choose Destination Location* dialog box will not appear when upgrading a BioNumerics 6.5 or newer instance (see 3.2.1.2).

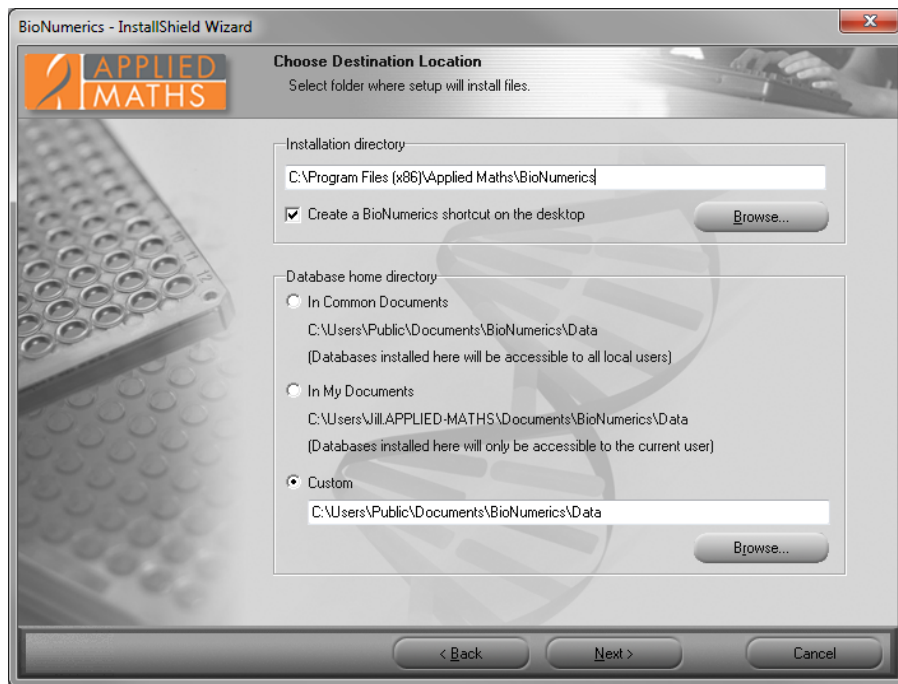
### 3.2.5 Select features

After clicking <Next>, the *Select Features* dialog box (see Figure 3.17) will be displayed allowing you to choose which features to update or to uninstall. Typically you should accept the default feature selection, or select additional features to install.

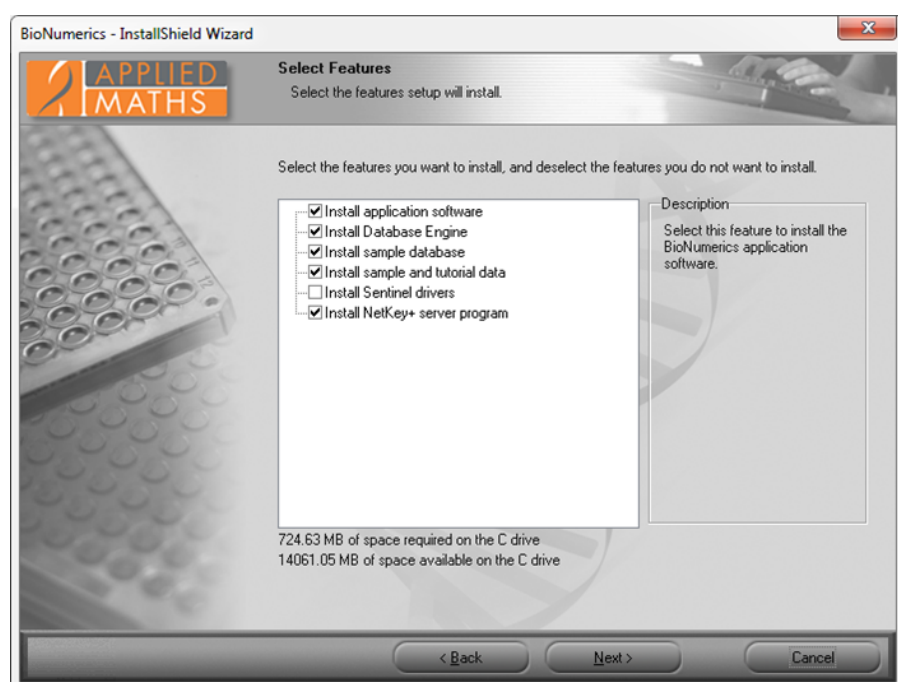
#### Install application software:

- In case of a *standalone license*, the **Application software** needs to be installed on each computer that you want to use to run the software. Please note that only on the computer where the dongle is attached to, you will be able to work with the software.
- In case of an *internet license*, the **Application software** needs to be installed on the computer that you want to use to run the software. Please note that a permanent and stable internet connection is required to run the internet license.





**Figure 3.16:** The *Choose Destination Location* dialog box.



**Figure 3.17:** The *Select Features* dialog box.

- In case of a *network license*, the **Application software** needs to be installed on the computers in the network that you want to use to run the software.

#### Install Database Engine:

- Checking this option will install the BioNumerics instance of Microsoft SQL Server 2008 R2 Express SP1 **Database Engine**. The location of the data files can be specified in the next step.

### Install sample database and Install sample and tutorial data:

- The sample database and sample and tutorial data that are contained in the Setup package are used in the manual to illustrate the features of the software. Selecting these features will install the sample database and sample and tutorial data in the database home directory that is specified in the *Choose Destination Location dialog box* (see Figure 3.16).

### Install Sentinel drivers:

The **Install Sentinel drivers** feature will install version 7.5.7 of the Sentinel System Driver. In addition this feature will also install the Sentinel Run-time Environment (previously known as HASP) version 6.51 if the NetKey+ server program feature has been selected for installation. The Sentinel Run-time Environment will not be installed if a standalone license string was entered in the *Customer Information dialog box*.

- In case of a *standalone license*, the **Sentinel drivers** need to be installed on each computer that you want to use to run the software.
- In case of an *internet license*, you only need an internet connection to run the software. The **Install Sentinel drivers** option does not need to be checked.
- In case of a *network license*, the **Sentinel drivers** only need to be installed on the NetKey+ server computer in the network.

### Install NetKey+ server program:

- The **NetKey+ server program** feature will only be visible and available for installation if a network license string has been entered in the *Customer Information dialog box* (see Figure 3.15). The **NetKey+ server program** feature must only be installed on the computer in the network where the hardware security key will be connected to.



De-selecting already installed features in the *Select Features dialog box* (see Figure 3.17) will cause these features to be uninstalled during the update. A message box will appear if you de-select the main BioNumerics application feature (see Figure 3.18). Select <No> if you do not want to uninstall the BioNumerics feature.

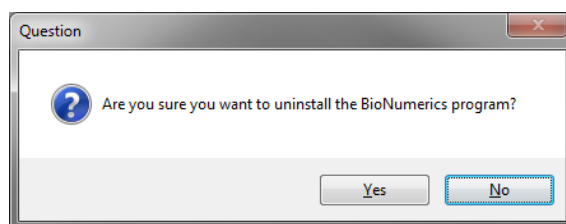


Figure 3.18: Warning message.

### 3.2.6 NetKey+ connection settings

After pressing the <Next> button, the *NetKey+ connection settings dialog box* will appear if a network license string was entered in the *Customer Information dialog box* (see Figure 3.4), and if the BioNumerics application feature was selected for installation (see Figure 3.7).

Typically during an update you can accept the **NetKey+ Server name** and **Port numbers** from the previous installation. These parameters will allow the BioNumerics application to connect to the NetKey+ server and request a session for the client computer.

- **NetKey+ Server name:** Name of the computer where the NetKey+ license service is running.
- **Server port number:** TCP listening port number of the NetKey+ service running on the NetKey+ server.
- **Server admin port number:** TCP listening port number for configuring the NetKey+ server. This can be the same number as for the Server port, but to increase security a different TCP port number can be configured for administrating the NetKey+ license server. This way the Windows firewall on the NetKey+ server can be configured to only allow remote NetKey+ administration from specific computers.

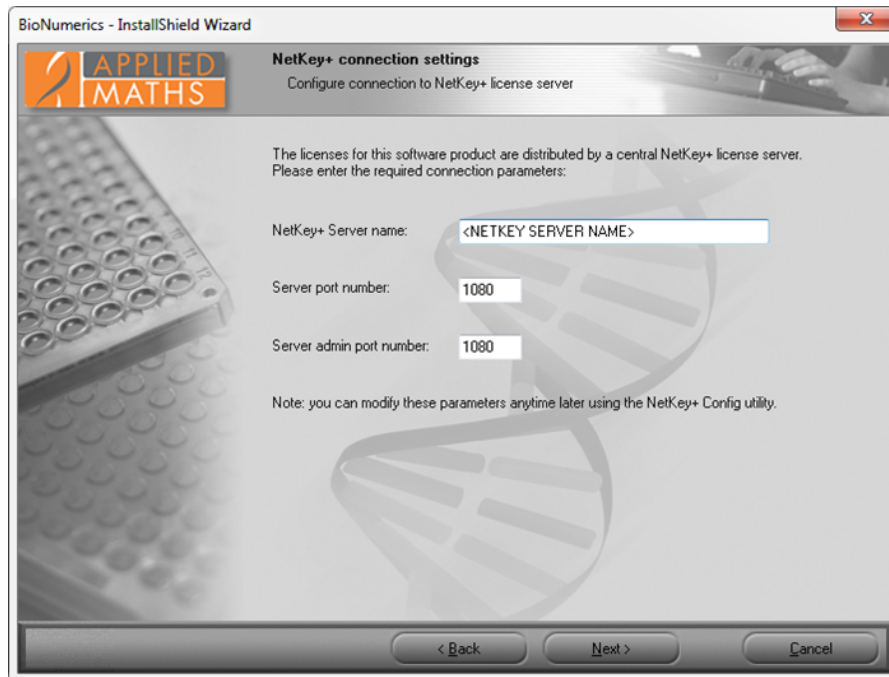


Figure 3.19: The NetKey+ connection settings dialog box.

### 3.2.7 Confirm update

Click *<Next>* to start the update. The *Setup Status dialog box* will be displayed. Newer files will be copied to the target system for the selected features. Any feature that was de-selected will cause the corresponding files and shortcuts to be uninstalled.

The *Update Complete dialog box* will appear after the update has finished. Click *<Finish>* to exit the Setup program.

## 3.3 Maintenance installation

### 3.3.1 Select instance to maintain

If an instance of BioNumerics 6.5 or later is already installed, then the *Existing Installed Instances Detected dialog box* will appear when launching the Setup executable (see Figure 3.20).

This dialog allows you to choose between installing a new BioNumerics instance, or changing an existing instance. Choose the *Maintain or update the instance of this application selected below* option to perform a maintenance of the BioNumerics application.

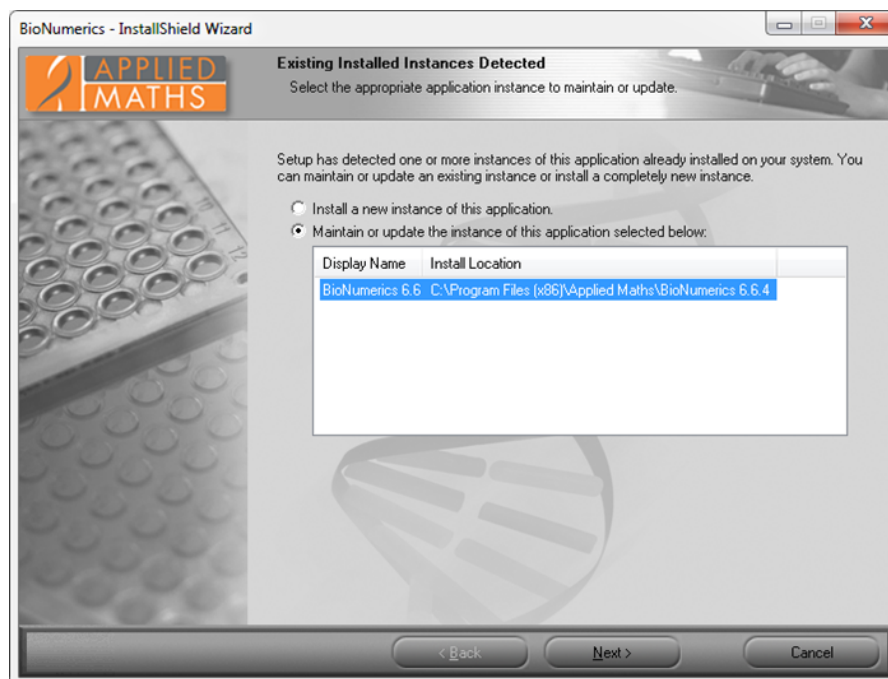


Figure 3.20: The *Existing Installed Instances Detected* dialog box.

### 3.3.2 Maintenance options

After selecting the BioNumerics instance that needs to be modified, the *Welcome dialog box* will display the maintenance options (see Figure 3.21).

- **Modify:** Select **Modify** to install a feature that was not installed during the previous installation (see 3.3.3).
- **Repair:** Choose **Repair** to repeat the previous installation of the BioNumerics application. The same features selected during the previous setup will be re-installed (see 3.3.4).
- **Remove:** Choose **Remove** to remove all BioNumerics files and shortcuts that were created during previous installations of the selected BioNumerics instance (see 3.3.5).

If only one instance of the BioNumerics program is installed then the **Uninstall shared Database Engine feature** check box will be visible. Selecting this option will cause the BioNumerics instance of Microsoft SQL Server 2008 R2 Express to be uninstalled.

### 3.3.3 Modify maintenance mode

The *Customer Information dialog box* will appear after selecting the **Modify** option and clicking **<Next>** in the *Welcome dialog box* (see Figure 3.21). This dialog allows you to update the user and organization names, and the BioNumerics license string. You must enter a valid license string to be able to continue with the installation.

Next, the *Select Features dialog box* will be displayed, allowing you to choose which features to install or to uninstall.



De-selecting already installed features in the *Select Features dialog box* will cause these features to be uninstalled during the update. A message box will appear if you de-select the main BioNumerics application feature. Select **<No>** if you do not want to uninstall the BioNumerics application.

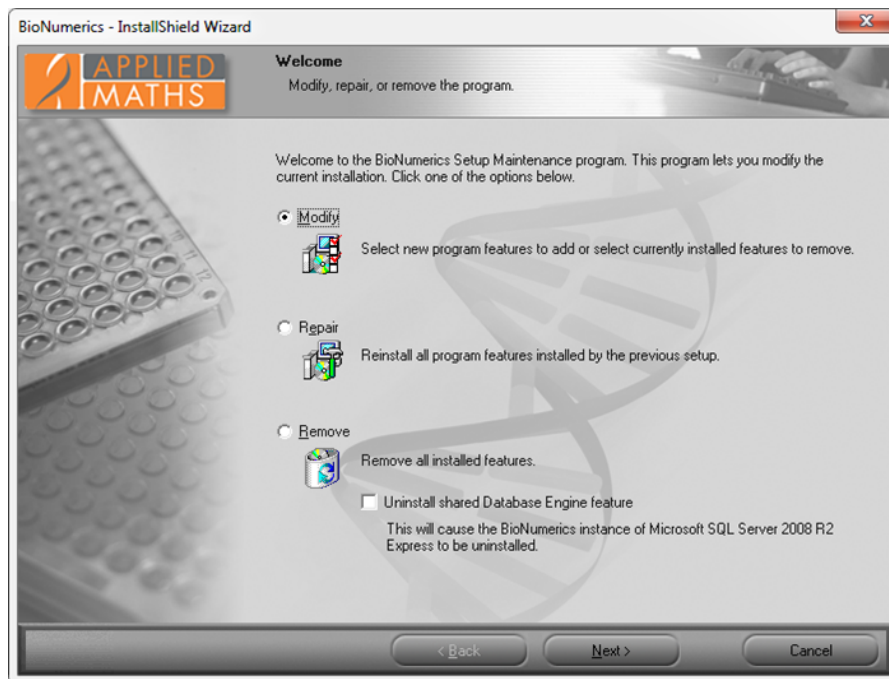


Figure 3.21: The *Welcome dialog box*.



The recommended method for uninstalling an instance of BioNumerics is to choose the **Remove** option in the *Welcome dialog box* (see Figure 3.21). De-selecting the BioNumerics application feature in the **Modify** maintenance mode will uninstall the application, but will not delete any uninstall information from the registry and file system. A message box will appear asking you to confirm that you want to uninstall the BioNumerics application. Other features that remained selected, like the sample database and NetKey+ server features, will not be removed from the target system.

After pressing <**Next**> the *NetKey+ connection settings dialog box* will appear if a network license string was entered in the *Customer Information dialog box*, and if the BioNumerics application feature was selected for installation in the *Select Features dialog box*.

Click <**Next**> to start applying the changes. Files will be copied to the target system for new features that have been selected. Any feature that was de-selected will cause the corresponding files and shortcuts to be uninstalled.

The *Maintenance Complete dialog box* will appear after all changes have been executed. Click <**Finish**> to exit the Setup program.

### 3.3.4 Repair maintenance mode

After choosing the **Repair** option in the *Welcome dialog box* (see Figure 3.21) and clicking <**Next**>, the Setup program will re-install all features that were selected during the previous installation. All corresponding files, shortcuts and registry settings will be re-created on the computer where the Setup is running.

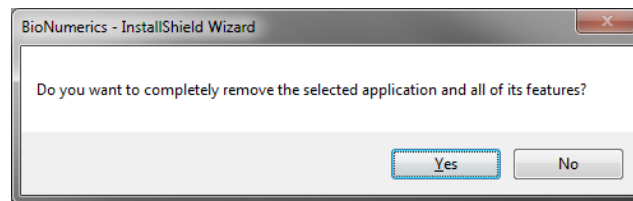
If a network license string has been entered, and the **NetKey+ server program** feature was selected for installation, the Setup will ask if you want to run the NetKey+ Configuration tool. This tool allows you to connect to the NetKey+ server to verify and update the license information. In addition, the tool allows you to repair the NetKey+ service (see 4.7 and 4.8). Click <**Yes**> if you want to start the NetKey+ Configuration tool. Click <**No**> if you do not want to change the NetKey+ settings at this time. More information about the NetKey+ Configuration tool can be found in 4.

The *Maintenance Complete dialog box* will appear after all changes have been executed. Click <**Finish**> to close the Setup program.

### 3.3.5 Remove maintenance mode

The **Remove** option in the *Welcome dialog box* (see Figure 3.21) allows you to completely uninstall the selected instance of BioNumerics. All BioNumerics files and shortcuts that were created during previous installations of the selected BioNumerics instance will be deleted. In addition, the uninstall information for the selected instance will be removed from the computer.

A confirmation dialog will appear, asking you to confirm the removal of the selected BioNumerics instance (see Figure 3.22). Click <**Yes**> to start the deletion of the BioNumerics application. Select <**No**> to return to the previous *Welcome dialog box*.



**Figure 3.22:** Confirm removal of selected features.



Completely uninstalling an instance of BioNumerics which includes the NetKey+ server program may affect other BioNumerics users that use the corresponding NetKey+ service to request license sessions. Make sure that no other users are using the NetKey+ service prior to uninstalling the NetKey+ server program feature, or completely uninstalling the BioNumerics instance.

The *Uninstall Complete dialog box* will be displayed after the selected BioNumerics instance has been removed. Click the <**Finish**> button to exit the Setup program.



The Setup will not delete BioNumerics program folder because it contains the SetupLogs sub-folder holding the log files for each Setup that has been run. Also any file that has been added to the program folder, and which was not originally installed by the Setup program, will not be deleted from the hard drive.

## 3.4 Installing Protection Keys

### 3.4.1 Protection Key Types

Starting from BioNumerics version 7.0 the NetKey+ server supports two types of SafeNet protection keys:

- **SentinelSuperPro** provider: hardware-based Sentinel SuperPro USB protection key. The Sentinel USB dongle is used to protect standalone and network licenses of BioNumerics running on computers either equipped with a physical USB port, or with a network-attached USB hub. The USB dongle has been tested with network-attached USB hubs from Digi (AnywhereUSB) and Silex (USB Device Servers).
- **SentinelHasp** provider: software based Sentinel HASP protection keys. The software-based Sentinel HASP SL key is used to protect network licenses of BioNumerics, more specific to provide a software protection key for the NetKey+ license server program running on a computer that is not equipped



with a free physical USB port. This is particularly useful if the NetKey+ license service is running on a virtualized operating system and a network-attached USB hub is not available.

### 3.4.2 Install Protection Key Driver

The BioNumerics Setup includes the latest version of the SafeNet drivers available at the time of the product release. When installing older BioNumerics versions it is recommended to download and install the latest version of the SafeNet driver before attaching the USB dongle.

The drivers for the Sentinel USB dongle can be downloaded from the following web site: <http://www.applied-maths.com/sentineldriver>.

The Sentinel Run-time Environment for the HASP SL or HL protection keys can be downloaded from the following web site: <http://www.applied-maths.com/haspdriver>.

The above URLs will redirect you to the appropriate download page on the SafeNet Sentinel customer web site.

After installing the drivers and connecting the USB dongle, the protection key should appear under **Universal Serial Bus controllers** in the Windows device manager (see Figure 3.23).

The Windows device manager can be accessed via "Control Panel > System and Security > Administrative Tools > Computer Management".



Figure 3.23: Universal Serial Bus controllers.

If the USB dongle is not listed in Windows device manager then download and install the latest version of the driver from the SafeNet web site and reboot the computer. Please contact the Applied Maths support team ([support@applied-maths.com](mailto:support@applied-maths.com)) if Windows still is unable to detect the protection key after reboot.

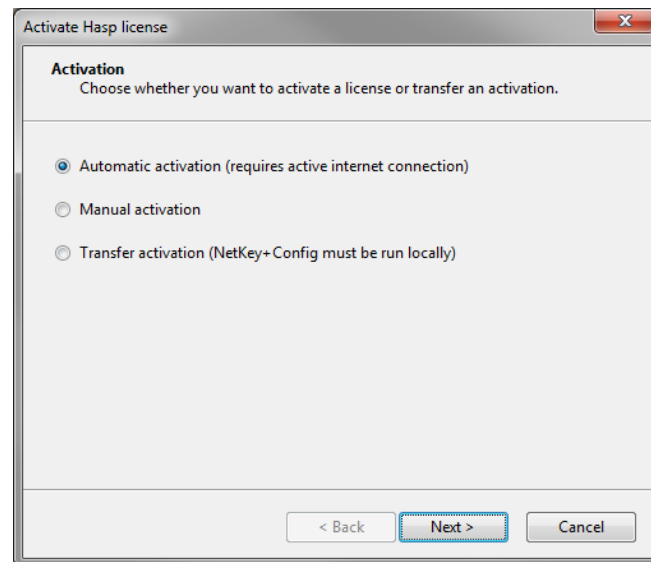
### 3.4.3 Activate Sentinel HASP SL key

#### 3.4.3.1 Introduction

The first step in installing a software-based Sentinel HASP SL key is adding the license string using the NetKey+ configuration tool. If the added license string corresponds with a software lock protection key then the **<Activate>** button (Figure 3.24) will be available, which allows downloading and installing the SentinelHasp key on the NetKey+ server computer. If the license key with the *SentinelHasp* provider is already listed in the NetKey+ configuration tool on the NetKey+ server then the software lock (SL) key is already activated.

Clicking the **<Activate>** button will display the *Activate Hasp license dialog* (see Figure 3.24). It is recommended to activate the software lock (SL) key using automatic activation. This requires an active internet connection on the computer running the NetKey+ configuration tool.

This dialog enables an Administrator to perform an automatic or manual activation of a HASP software lock (SL) license string, or to transfer an existing protection key to another computer. Note that the NetKey+ server never needs an active internet connection for the activation, an active internet connection is recommended for the NetKey+ configuration tool however.

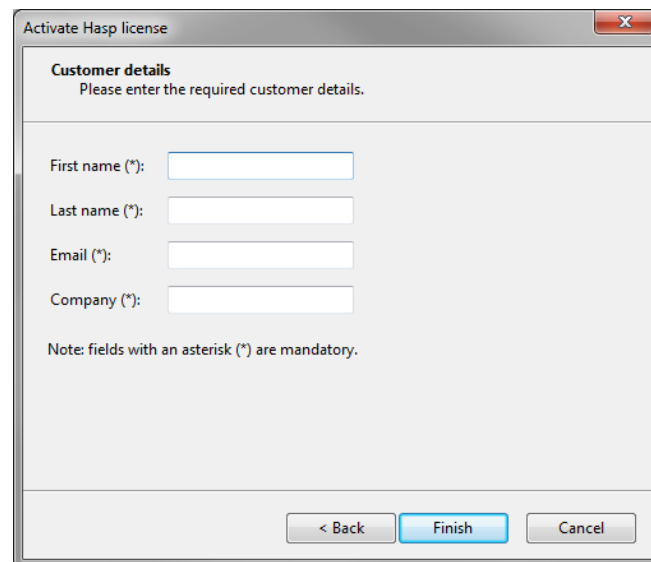


**Figure 3.24:** Activate Hasp license.

### 3.4.3.2 Automatic Activation

It is recommended to activate the software lock (SL) key using automatic activation. This requires an active internet connection on the computer running the NetKey+ configuration tool. Note that the SL key can only be activated once, however it is possible to transfer the lock to a different computer afterwards (see 3.4.3.4).

Click **<Next>** to display the *Customer details dialog*, and enter the contact person's name, email address and organization name you want to use the register the software activation. If possible please use the contact details of the person who ordered the software at Applied Maths NV.



**Figure 3.25:** The *Customer details dialog*.

Click **<Finish>** to start the activation process. The NetKey+ configuration tool will connect to a secured license server to check if there is a SentinelHasp soft lock protection key available for the entered license string. If a protection key is available the NetKey+ configuration tool will connect to a secured activation server to upload a fingerprint of the NetKey+ computer, and subsequently download and install the corresponding soft lock key. Hence the computer running the activation process must be able to access the



following web sites on the internet:

- <https://ssllicense.applied-maths.com>: Secured License Server
- <https://activate.applied-maths.com>: Secured Activation Server

Select **Server** in the left panel of the NetKey+ configuration tool. If the automatic activation was successful the software-based protection key with **SentinelHasp** as the provider should appear within a minute or so in the list of available license keys.

Note that the installed SentinelHasp soft lock key is only valid for a specific target computer, and can by default only be activated once. Afterwards the protection key can be moved to another NetKey+ server, for example when installing a new NetKey+ server computer.

If an error message appears during the activation process, you can look up the NetKeyConfigLog.txt log file in your temp folder, and send the file as an email attachment to activate@applied-maths.com. If receiving the vendor-to-customer (v2c) file from the Applied Maths activation server succeeded, but applying it to the NetKey+ server failed, a backup v2c file is created in the temp folder, with a name formatted like NetKeyConfig\_autoActivate\_backup\_#.v2c. The activation can then be completed manually by using this file and the **Activate with confirmation file** option in the *Manual Activation dialog*.

- License Activation log file path: temp \NetKeyConfigLog.txt
- License Activation backup v2c file: temp \NetKeyConfig\_autoActivate\_backup\_0.v2c



A complete system or full backup scheme must be in place to protect the NetKey+ license server where a soft lock key has been activated. Changing the hardware configuration (e.g. MAC address, CPU, hard drive) will cause the protection key to render invalid; hence the protection key must be transferred to another (intermediate) computer before modifying the hardware, and transferred back to the source computer after the hardware component(s) have been replaced. This also applies to virtual environments, for example moving a virtual NetKey+ server guest image to another host server may invalidate the protection key. Hence the key must be transferred to another (intermediate) computer before moving the guest image to another host server, and transferred back after the virtual guest image has been moved. In case of doubt please contact the support team before changing the hardware configuration of a NetKey+ server that contains a SentinelHasp soft lock protection key.

### 3.4.3.3 Manual Activation

---

If no internet connection is available on the NetKey+ server computer or on any of the computers where the NetKey+ configuration tool is installed, then the **Manual Activation option** can be selected in the *Activate Hasp license dialog* (see Figure 3.24 (It is recommended to activate the software lock (SL) key using automatic activation. This requires an active internet connection on the computer running the NetKey+ configuration tool).

Click <**Next**> to display the *Manual activation dialog*.

Select the **Create activation request file** option in the *Manual Activation dialog*.

Click <**Browse**> to enter the path and file name for the activation request file.

Click <**Finish**> to save the customer-to-vendor (\*.c2v) activation request file, and include the file as an email attachment and send an email to activation@applied-maths.com. If your email system does not allow sending \*.c2v files you can change the file extension to \*.txt.

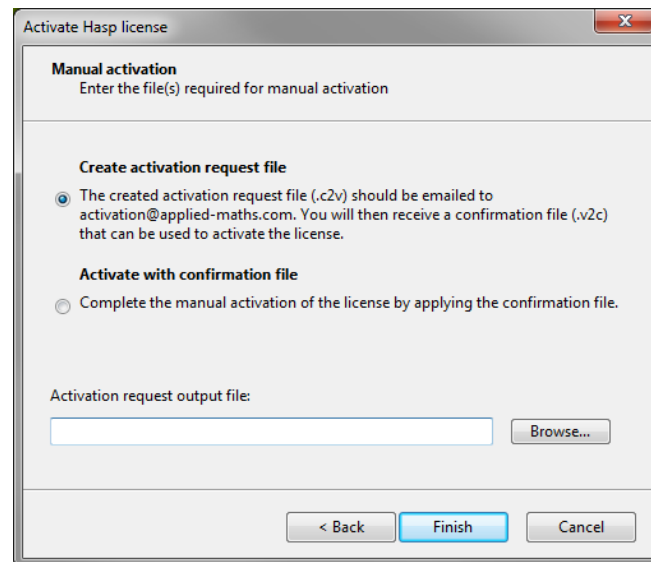


Figure 3.26: The *Manual activation* dialog.

After receiving the vendor-to-customer (\*.v2c) confirmation file from Applied Maths the activation process can be completed:

Select the **Activate with confirmation file** option in the *Manual Activation* dialog.

Click **<Browse>** to select the \*.v2c confirmation file, and click **<Finish>** to install the SentinelHasp soft lock key on the NetKey+ server;

Select **Server** in the left panel of the NetKey+ configuration tool. If the manual activation was successful the software-based protection key with **SentinelHasp** as the provider should appear within a minute or so in the list of available license keys.

#### 3.4.3.4 Transfer Sentinel HASP SL key

To be able to transfer a software-based protection key the NetKey+ server and the configuration tool must be installed on both the source and destination computers, and the NetKey+ configuration tool must be started locally on both computers. A license key with the **SentinelHasp** provider must be listed in the NetKey+ configuration tool on the source NetKey+ server to be able to transfer the key to another NetKey+ server computer.

Transferring the Sentinel HASP SL key is a three-step process:

The first step is creating the protection key request file on the target computer:

1. Start the NetKey+ configuration tool on the target computer.
2. Select **Licenses** in the left pane, select the license string.
3. Click the **<Activate>** button.
4. Select **Transfer activation** in the *Activate Hasp license* dialog (see Figure 3.27 and click **<Next>**).
5. In the top **Computer** section select **NetKey+ is running on the destination computer**.
6. In the **Step** section select **Step 1: Create request file - Destination computer**.
7. Click the **<Browse>** button to enter the path and file name of the protection key request file.

8. Click **<Finish>** to save the protection key request file.

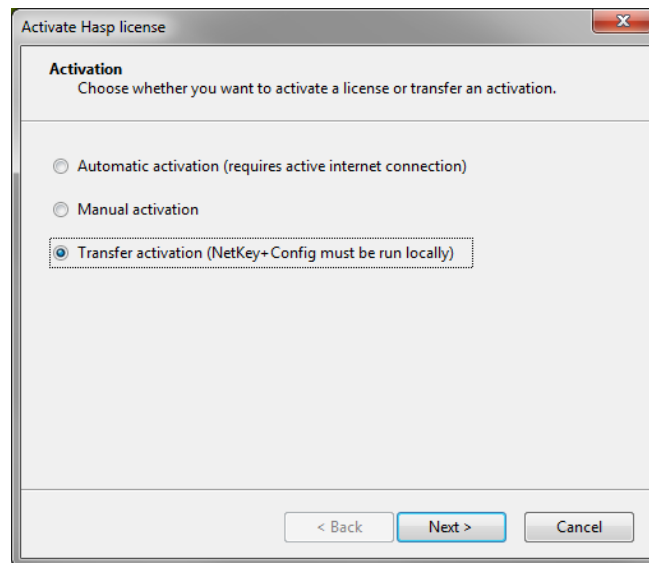


Figure 3.27: Transfer activation.

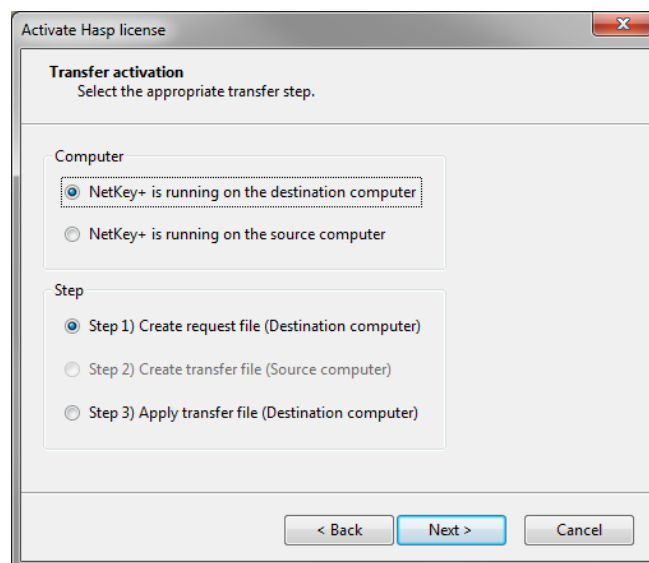
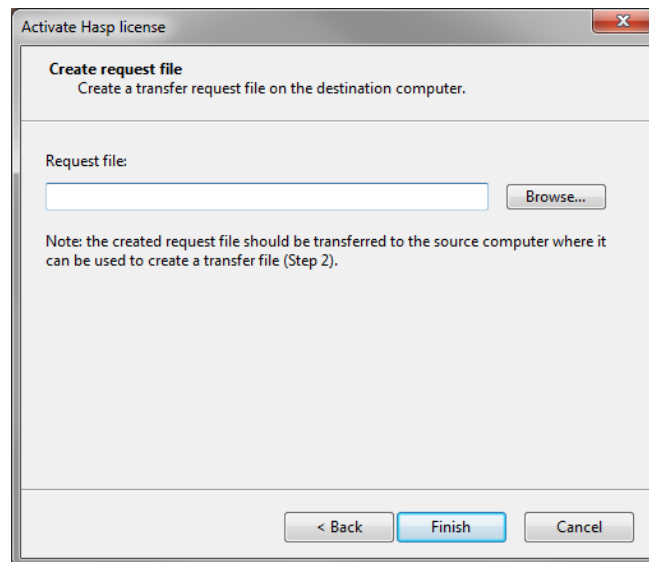


Figure 3.28: Transfer activation.

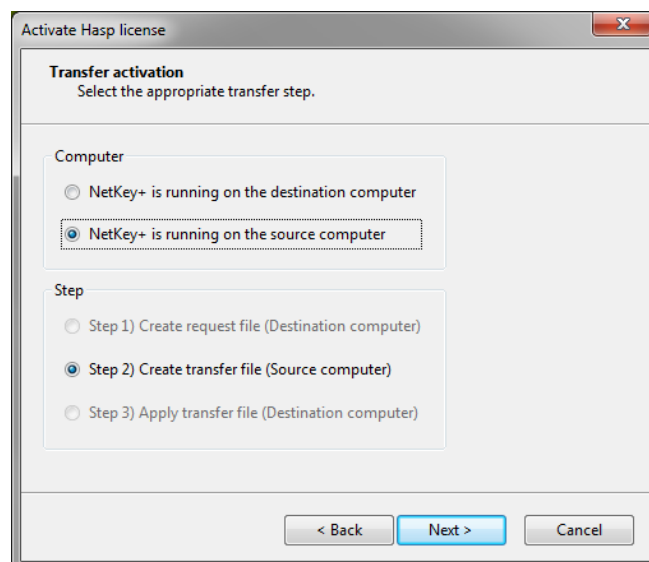
The second step is creating the protection key transfer file on the source computer:

1. Copy the protection key request file from the target to the source computer.
2. Start the NetKey+ configuration tool on the source computer.
3. Select **Licenses** in the left pane, select the license string.
4. Click the **<Activate>** button.
5. Select **Transfer activation** in the *Activate Hasp license dialog* (see Figure 3.27, and click **<Next>**).
6. In the top **Computer** section select **NetKey+ is running on the source computer**.



**Figure 3.29:** Create request file.

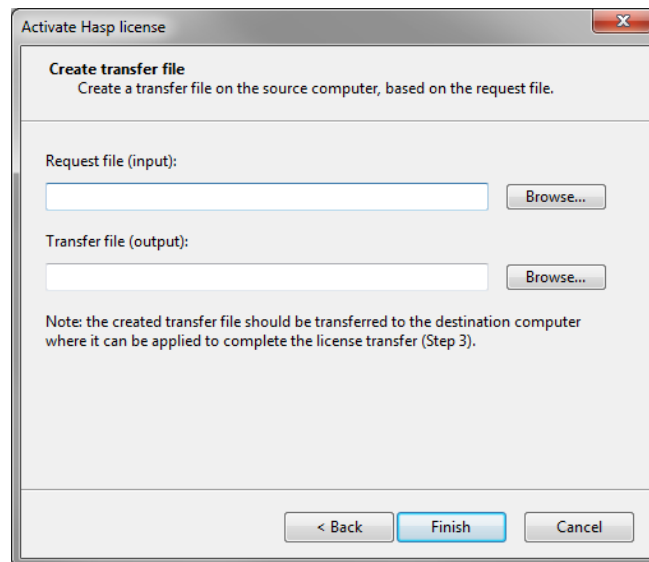
7. In the *Step* section select **Step 2: Create transfer file - Source computer**.
8. Click the first <**Browse**> button to select the \*.id protection key request file.
9. Click the second <**Browse**> button to enter the path and file name of the \*.v2c transfer file.
10. Click <**Finish**> to remove the protection key from the local computer and to save the \*.v2c transfer file.



**Figure 3.30:** Transfer activation.



Upon completion of this step the software lock is effectively removed from the source computer. This means that the license connected to this lock will be deactivated. The software lock has not been transferred to the target computer yet however, at this point the lock can be thought of as "residing in the transfer file". Until the transfer file has been applied on the target computer it is therefore crucial not to accidentally remove it. As a back-up measure a copy of the transfer file is stored in the temp folder, with name e.g. NetKeyConfig\_transferFile\_backup\_0.v2c.



**Figure 3.31:** Transfer activation.

The third and last step is to apply the protection key transfer file on the target computer:

1. Copy the \*.v2c transfer file from the source to the target computer.
2. Start the NetKey+ configuration tool on the target computer.
3. Select **Licenses** in the left pane, select the license string.
4. Click the **<Activate>** button.
5. Select **Transfer activation** in the *Activate Hasp license dialog* (see Figure 3.27, and click **<Next>**).
6. In the top **Computer** section select **NetKey+ is running on the destination computer**.
7. In the **Step** section select **Step 3: Apply transfer file - Destination computer**.
8. Click **<Browse>** and browse to path where the copied \*.v2c transfer file is located and select the file.
9. Click **<Finish>** to install the protection key on the local computer.

## 3.5 Setup log

---

All messages generated while the Setup is running are written to the Setup log XML file. The name of each XML element indicates the message type:

- **<message />**: This is an information message and can safely be ignored.
- **<warning />**: This is a warning message, usually indicating that some user action may be required to resolve the issue.
- **<error />**: This indicates that a severe error has occurred. User action is required to resolve the issue. Severe errors may cause the Setup to abort.

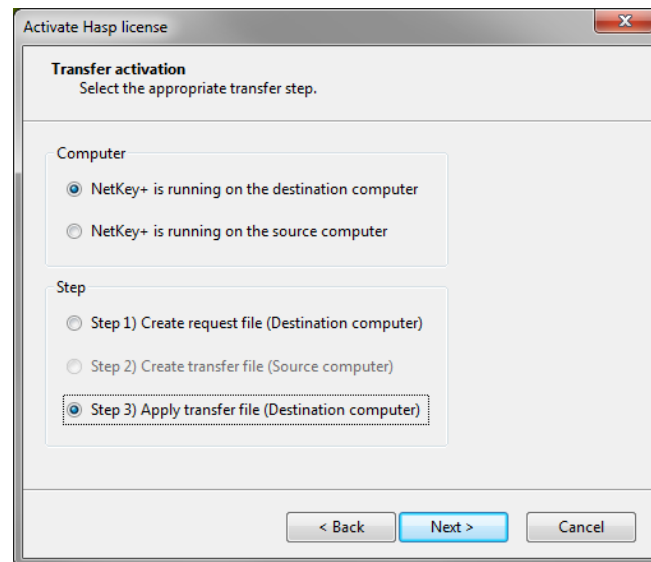


Figure 3.32: Transfer activation.

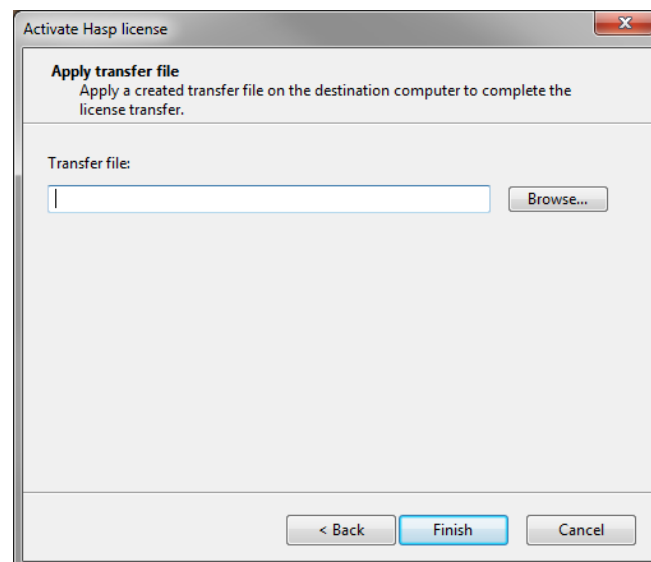


Figure 3.33: Transfer activation.

The Setup log XML file is best viewed with a recent version of the Microsoft Internet Explorer browser (see Figure 3.34). This will allow you to expand and collapse specific message tables in the XML document. Error and warning messages will be expanded by default, and will be displayed at the top of the browser window. Hence you do not need to scroll down to verify if an error has occurred.

A yellow information bar may appear in Internet Explorer with the following message: "To help protect your security, Internet Explorer stopped this site from installing an ActiveX control on your computer. Click here for options". Right-click the information bar and select **Allow Blocked Content...** A *Security Warning message box* will appear. Click <Yes> to confirm that you want to enable the active content in the Setup log XML file.

If the Setup is running in normal (non-silent) installation mode and a warning or error event has occurred, the Setup will automatically display the Setup log XML file in Internet Explorer. Additional messages will continue to be written to the log file, and the file will automatically be updated in Internet Explorer. If you have scrolled down on the Setup log web page, your current position will be lost after the web page has been



Figure 3.34: The BioNumerics setup log.

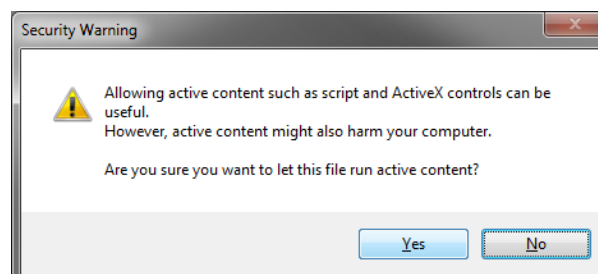


Figure 3.35: Security warning.

refreshed.

The Setup log XML file is located in the SetupLogs sub-folder of the BioNumerics program folder. For example:

- 32-bit platforms: C:\Program Files\Applied Maths\BioNumerics\SetupLogs\Setup\_1\_log.XML
- 64-bit platforms: C:\Program Files (x86)\Applied Maths\BioNumerics\SetupLogs\Setup\_1\_log.XML

## 3.6 Silent installation

---

### 3.6.1 Purpose

---

Running the BioNumerics Setup in "silent installation" mode allows running the BioNumerics Setup program without an end-user interface. No dialogs will be displayed in silent mode, and all messages, including errors, will be logged to the Setup log file. All information required to run the Setup needs to be recorded to a properly formatted Setup\_x\_ini.XML file. This file must subsequently be invoked through Setup.exe command line parameters.

The silent installation mode can be helpful for mass-deployment of BioNumerics, for creating identical configurations and to automate repetitive behavior.

### 3.6.2 Installation procedure

---

Each installation of BioNumerics 6.5 or later not only creates a Setup log XML file, but also a Setup INI XML file (see 3.1.13 for more details). This Setup INI XML file recorded during a manual install of BioNumerics can subsequently be used to perform silent installations.

The Setup INI XML file is located in the SetupLogs sub-folder of the BioNumerics installation directory. The file name is formatted like Setup\_x\_ini.XML. Check the file modification date to determine which INI XML file was created during the latest installation.

The BioNumerics 6.5 or later versions of the Setup program accept the following command line parameters to invoke the silent installation mode:

```
"<path to Setup files>\Setup.exe" /s --ini="<path to Setup_x_ini.XML file>"
```

- The /s command line parameter instructs the InstallShield runtime engine to suppress the *Existing Installed Instances Detected dialog box* if BioNumerics version 6.5 or later is already installed.
- The --ini parameter instructs the Setup script to read the installation settings from the INI XML file, and to hide all dialogs.
- The double hyphen is required to differentiate between InstallShield runtime engine and custom InstallScript command line parameters.
- The slash parameters are used by the runtime engine.
- The double hyphen custom parameters are used by the installation script.
- Optionally the --logdir command line parameter can be specified to override the log\_dir path recorded in the Setup INI XML file.

```
"<path to Setup files>\Setup.exe" /s --ini="<path to Setup_x_ini.XML file>"--logdir="<path to log folder>"
```

Example (all command line parameters should be on a single line):

```
"C:\Users\Public\Documents\Applied Maths\BioNumerics \Setup.exe" /s
--ini="C:\Users\Public\Documents\Applied Maths\Setup_1_ini.XML"
```



```
--logdir="C:\Users\Public\Documents\Applied Maths\SetupLogs"
```

During silent installations, no error or warning messages are displayed when the Setup is running. The installation Administrator should check the Setup log XML file to verify that no errors have occurred, and that no further action is required to complete the BioNumerics installation on the target computer.



The Microsoft .NET Framework 2.0 SP2 or 3.5 SP1 and Windows Installer 4.5 prerequisites described in 2 should be installed prior to launching the Setup in "silent installation" mode. For example the silent installation will fail if the Setup is not able to download and install the Microsoft .NET Framework 3.5 SP1.

### 3.6.3 Setup INI XML file format

The information recorded in the Setup\_x\_ini.XML file has the format as displayed in Figure 3.36.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<setup name="\BnSoftwareName" version="7.0.1" date="2012-12-12" time="00:00:00">
  <start date="12-12-2012" time="00:00:00"/>
  <feature display_name="Install application software">
    <property netkey_server="localhost"/>
    <property netkey_server_port="1080"/>
    <property netkey_config_port="1080"/>
    <property netkey_refresh_rate="30"/>
    <property desktop_shortcut="1"/>
  </feature>
  <feature display_name="Install Database Engine">
    <property enable_remote_access="1"/>
    <property restart_sql_server_service="0"/>
    <property user_database_directory="C:\Program Files\Microsoft SQL Server\MSSQL10_
50.\BNSOFTWARENAME\MSSQL"/>
    <property sysadmin_group="CN=Domain Users,CN=Users,DC=domain,DC=local"/>
  </feature>
  <property log_dir="C:\Program Files (x86)\Applied Maths\BnSoftwareName 7.0\SetupLogs"/>
  <property install_dir="C:\Program Files (x86)\Applied Maths\BnSoftwareName 7.0"/>
  <property database_home_dir="C:\Users\Public\Documents\BnSoftwareName\Data"/>
  <property registered_user="user name"/>
  <property registered_organization="organization name"/>
  <property license_string="license string"/>
  <feature display_name="Microsoft SQL Server 2008 R2 Native Client"/>
  <feature display_name="Microsoft System CLR Types for SQL Server 2008 R2"/>
  <feature display_name="Microsoft SQL Server 2008 R2 Shared Management Objects"/>
  <feature display_name="HPC Pack 2008 MS-MPI Redistributable Package"/>
  <feature display_name="Install sample database"/>
  <feature display_name="Install sample and tutorial data"/>
  <feature display_name="Install Sentinel drivers"/>
  <!-- The NetKey+ service should only be deployed to a single license server computer,
       hence silent deployment of this feature usually is not desired. -->
  <!--
  <feature display_name="Install NetKey+ server program"/>
  -->
</setup>
```

Figure 3.36: Setup INI XML file format.

The root XML node of the Setup INI file is the *setup* node. The attributes in the *setup* node are only used for information purposes, for example to display which BioNumerics Setup version created the Setup INI file. The *setup* node also contains *property* sub-elements, one for each property that is required to configure the Setup.

Setup properties typically contain Setup-related configuration values which are not feature-specific, or which are shared by multiple features.

The *start* XML element contains a time stamp indicating when the file was created.

Each feature that was selected for installation has a corresponding *feature* element with the *display\_name* attribute. The attribute value must match the feature name displayed in the *Select Features dialog box*. The *feature* element may contain *property* sub-elements, one for each property that is required to configure the parent feature.



## Chapter 4

# NetKey+ configuration

### 4.1 Introduction

---

If a network license has been purchased, the *NetKey+ server program* and the *Sentinel drivers* must be installed on a computer where the hardware security will be connected to (i.e. the *server computer*) (see 3).

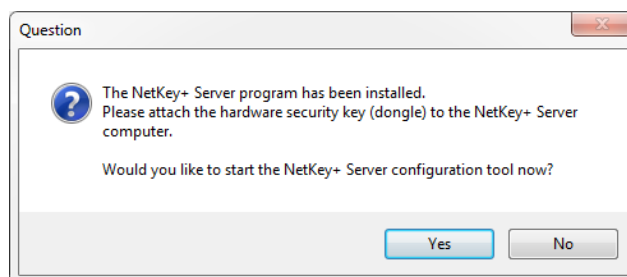
After installation of these features on the server computer, the NetKey+ service needs to be installed and started using the NetKey+ Configuration tool (NetKey+Config.exe) (see 4.2).

Once started, the license(s) can be configured in the NetKey+ Configuration tool (see 4.3) and the NetKey+ service can start distributing sessions to the requesting BioNumerics applications running on the client computers (i.e. the computers with the application software installed) (see 4.4).

### 4.2 Installing and starting the NetKey+ service on the server

---

If a network license string has been entered in the *Customer Information dialog box*, and the NetKey+ server program feature was selected for installation in the *Select Features dialog box*, the Setup will ask if you want to run the NetKey+ Configuration tool (see Figure 4.1). This tool allows you to install and subsequently start the NetKey+ service.




**Figure 4.1:** Run the NetKey+ Configuration tool.

Click <Yes> to start the NetKey+ Configuration tool. This will run the tool with Windows elevated privileges (**Run as administrator**) and the *Login window* will be displayed (see Figure 4.2).



The NetKey+ Configuration tool can also be called by (double-)clicking on the NetKey+Config.exe application in the installation directory of BioNumerics. Alternatively,

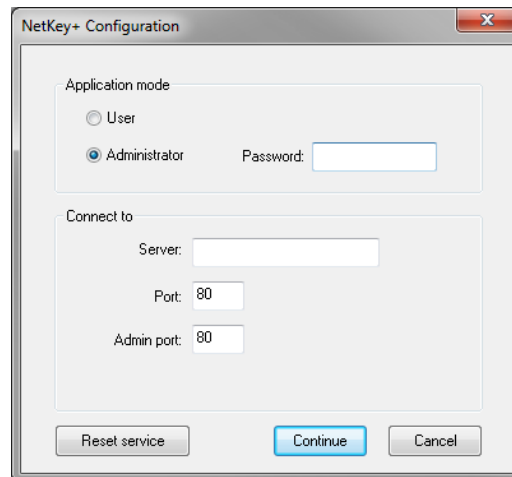
press the <Settings> button () in the startup window of BioNumerics- if the application software has been installed - and select *NetKey+ configuration* from the drop-down list.



The configuration tool can be run as NetKey+ **User** or NetKey+ **Administrator** in combination with or without Windows elevated privileges. An overview of all tools that are accessible in the NetKey+ Configuration program for the four different login options is given in 4.9.



To run a program with Windows elevated privileges in Windows Vista, Windows 7 or Server 2008, right-click on the application and select "Run as administrator".



**Figure 4.2:** The *Login window*.

Choose the **Administrator** mode in the *Application mode panel*. This mode will allow you to install and start the NetKey+ service.

The first time the service will be started, a password will be prompted for. This **Password** is required the next time someone wants to access the configuration program in **Administrator** mode. When the service has not been started yet, the **Password** field can be left empty.

Enter the local computer name or "localhost" as the **Server** name in the *Connect to panel* to indicate that the NetKey+ service will be installed on the computer where the tool is running.

The server **Port** number is an available TCP port number that will be used by the NetKey+ server and clients to exchange session information. The **Admin port** is an available TCP port number that will be used to by the NetKey+ server and configuration tool to configure the service settings. The default suggested TCP port number for both ports is 80. Any other port numbers can be specified.



An HTTP-based protocol is used for the communication between the NetKey+ server, the NetKey+ Configuration tool and the BioNumerics application. Both TCP ports must be enabled on the Windows firewall or any other security tool that may block access to these ports, both on the NetKey+ server computer and on each computer where BioNumerics is installed. The NetKey+ server TCP ports may not be used by any other application or service. For example, no websites should be hosted on the IIS server using a NetKey+ TCP port number.

Clicking the <**Reset service**> button will stop the NetKey+ service on the server computer and will delete all current NetKey+ settings, including the Administrator password (see 4.7 for more information). This operation is not applicable if the service is not already installed.

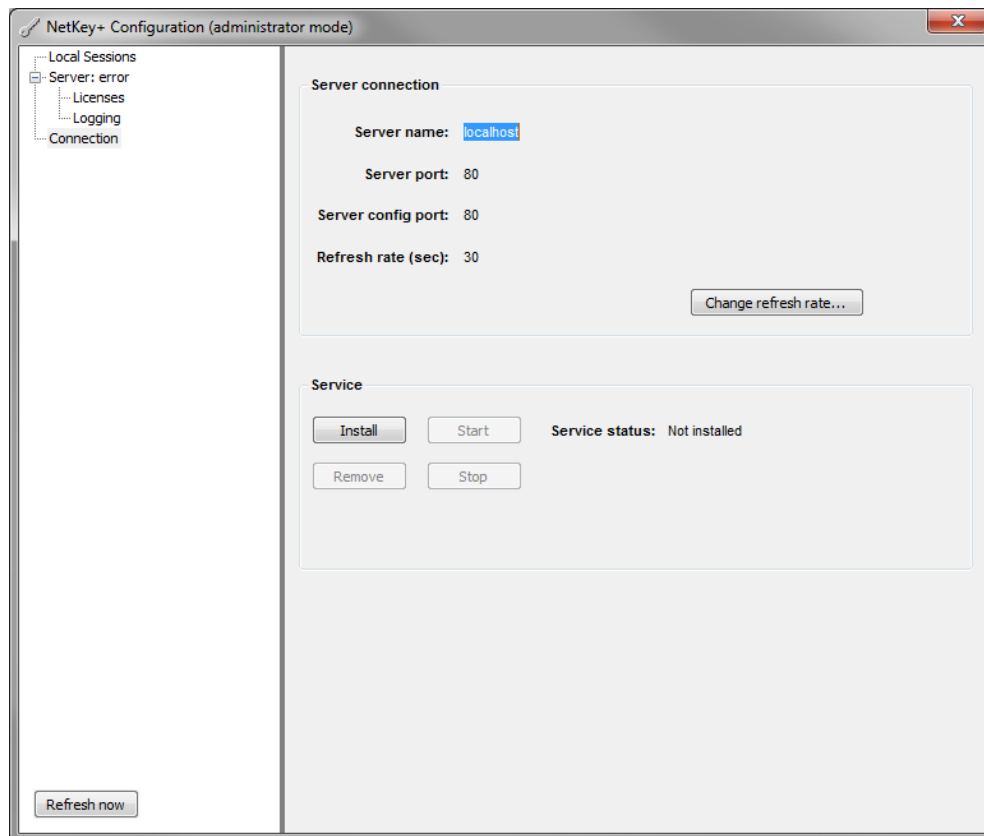
Clicking the <**Continue**> button will save the connection settings to the NetKey.ini text file, and to the NetKey+\_Config.txt XML file. These files are located in the folder containing application data for all users (CommonAppDataFolder). The path of this folder depends on the operating system version.

- Windows Vista or later: C: \ProgramData \Applied Maths \NetKey+
- Windows XP: C: \Documents and Settings \All Users \Application Data \Applied Maths \NetKey+

Select **Connection** in the left panel to display the server connection settings (*Server connection panel*) and service status (*Service panel*) (see Figure 4.3).

The **Refresh rate** determines how often the information displayed in the NetKey+ Configuration tool is updated. The default value is 30 seconds.

The **Service status** text box displays the current status of the NetKey+ windows service. The status should be "Not installed" if this is the first time the BioNumerics Setup is running on the server computer.



**Figure 4.3:** The NetKey+ Configuration tool window.

Click the **<Install>** button in the lower *Service panel* to install the NetKey+ Windows service. Next click the **<Start>** button to start the NetKey+ service.

The *Change server password dialog* will be displayed during a first-time installation of the service, allowing you to enter and confirm a new NetKey+ server password (see Figure 4.4). A user will be required to enter the NetKey+ server password each time the configuration tool is started in **Administrator** application mode. After the user clicks **<Continue>** in the *Login window*, the configuration tool will connect to NetKey+ server via the specified Server config **Port** (or **Admin port**) to verify the credentials.

After clicking **<OK>** in the *Change server password dialog box*, the password is encrypted and stored in the NetKey+\_Config.txt XML file. The Service status will change to "Started" if no error has occurred. In case of error, the NetKey+\_LOG.txt log file can be checked to verify the error message (see 4.6). The log file is stored in the same ProgramData or Application Data folder as the NetKey.ini file, depending on the Windows version.

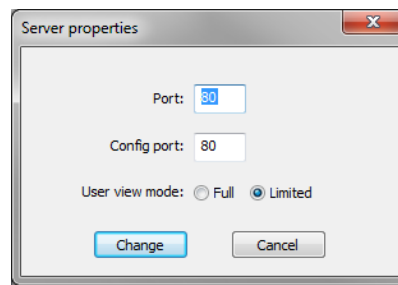
Once the service has been installed and started, the service can be stopped by pressing the **<Stop>** button, and can be removed by clicking the **<Remove>** button in the lower *Service panel*.



The *Service panel* will be disabled (grayed out) if the configuration tool is launched without Windows elevated privileges.



the TCP port numbers.



**Figure 4.6:** Edit the server properties.



If the NetKey+ Configuration tool or the BioNumerics application is unable to communicate with the NetKey+ service through the specified port numbers then check your security settings to make sure that the TCP ports are accessible. For example, if a software firewall has been enabled on the NetKey+ server or on the BioNumerics client computer, then the firewall may need to be configured to allow traffic for the Applied Maths executables and/or the applicable TCP port numbers.

Continue with 4.3 if you want to set up the BioNumerics license string(s) to allow access for the client computers.

Click the "x" sign in the top right corner or press **ALT+F4** to close the NetKey+ Configuration tool. Closing the NetKey+ Configuration tool will not affect the current status of the NetKey+ service. If the service is running, then clients will be able to connect to the NetKey+ server if the configuration was successful.

## 4.3 Configuring licenses

Adding and configuring licenses can only be done by running the NetKey+ Configuration tool in **Administrator** application mode, with or without Windows elevated privileges (**Run as administrator**) (see Table 4.1). After selecting the **Administrator** mode in the *Login window*, the correct NetKey+ server password can be entered in the **Password** field (see Figure 4.2).

The settings in the lower *Connect to panel* correspond with the settings stored in the `NetKey.ini` file. These settings can be changed if the tool was started with Windows elevated privileges. Click the **<Continue>** button to connect to the NetKey+ server.

Select **Licenses** under the **Server** option in the left panel (see Figure 4.7). Click the **<Add>** button to add a new BioNumerics license string to the list of installed licenses.

In the *License properties dialog box*, enter the 6 x 4 characters **License String** in the input fields (see Figure 4.8). Alternatively, use the **<P>** button to paste the contents of the clipboard in the **License** fields. The license string is provided on the sleeve of the CD-ROM or the string may have been delivered electronically. An error message will pop up when attempting to add an invalid license string (e.g. a standalone license string, a second license string for the same key, ...) to the license list.

Press **<Add>** to insert the new license string into the list of installed licenses. The added license string will be displayed in the **String** column (see Figure 4.7). The number of concurrent sessions that are granted to the license is shown in the **Allowed sessions** column. If the corresponding protection key is present in the **Available license keys** list (see Figure 4.5), the state of the license is set to **Active**. If the key is not detected on the server computer, the state is set to **Valid**. The last **Sessions in use** column displays the total number of sessions that are currently in use for this license.

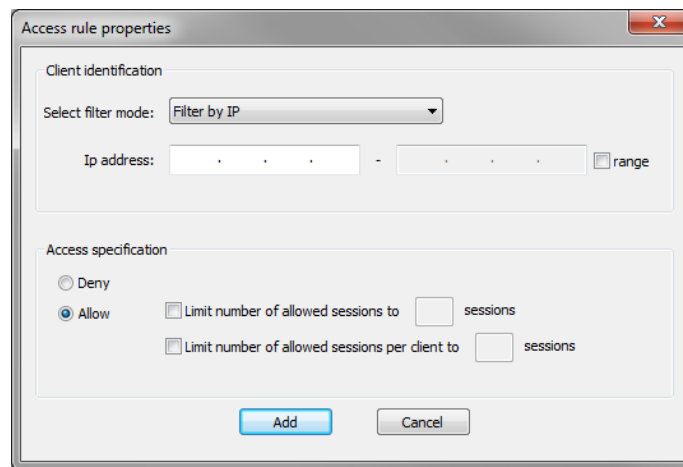
The settings for a specific license can be modified by selecting the corresponding string and clicking the







- **Filter by User Name:** Windows login name without domain name.
- **Filter by IP:** Single or a range of IPv4 addresses of client computers.



**Figure 4.11:** The *Access rule properties* dialog box.

A range of IPv4 addresses can be specified if the **Range** option is checked in the upper *Client identification* panel. Optionally a limit on the number of allowed concurrent sessions can be specified in the lower *Access specification* panel when the **Allow option** is checked (see Figure 4.11). Note that NetKey+ does not support the **Filter by IP** filter mode for IPv6 addresses.

Pressing the **<Add>** button adds the rule to the *Access rules* list (see Figure 4.10). Each access rule is identified by a unique identifier (**Id**). The filter mode is displayed in the **Client filter** column, and the **Sessions** column displays the number of allowed concurrent sessions to all clients. If no limit has been set this column will display **Limit by license**. The **Sessions per client** column displays the number of allowed concurrent sessions for each client. If no limit has been set this column will also display **Limit by license**. Both these sessions columns will display **Deny** if this has been specified as the Access specification. The **Connected** sessions column shows the number of currently connected sessions. The number of sessions that are queued on a waiting list are shown in the last **Waiting sessions** column.

The access properties for a selected rule can be modified by clicking the **<Change>** button. If multiple access rules have been specified for a license, the order of the rules can be changed with the **<Up>** and **<Down>** buttons.

When a client tries to open a session, a *session request* is sent to the server, containing computer information of the client (computer name, Windows user name, IP address, and MAC address) and the license string. The server checks the access rules of the license string that is sent with the session request, and based on the access rules, the server grants or denies the client access to the license. Each session that is granted access to a license is identified by a unique identifier, the *session ID*. The session identifier is sent to the client, and the session is launched on the client computer or the session is put on a waiting list in case the number of allowed sessions (on the client) is reached. The client stores the *session ID* of the session and closes the connection with the server computer. On regular time intervals, a *renew session request* of each connected session and session that is put on hold is sent to the server. Based on these renew session requests, the server keeps track of the status of the sessions on the client computers. The server might disconnect a session if the **Usage time**, **Idle time** or **Timeout** value for a session is reached:

- **Usage time:** The *Usage time* (or *time in use*) of each session that is granted access to a license is recorded by the server program. The usage time is the total connection time for each connected session, or in case of a session present in the waiting queue, the time the session has been put on hold. In case there is a waiting list, a connected session for which the usage time exceeds the maximum

usage time (default 120 min., see Figure 4.8) will be closed in favor of the first session in the waiting list. The usage time of the session that was put on hold, but now is launched by the software, is reset. A session that exceeds the maximum usage time limit will not be closed as long as there is no waiting list.

- **Idle time:** The *Idle time* of each connected session is also recorded by the server program. The idle time starts running as soon as the session is running on a client computer. The status of the session is checked each time a *renew session request* is sent to the server: when the session is in use, the idle time is reset; if no user activity is recorded, the idle time keeps running. A session for which the idle time exceeds the maximum idle time (default 60 min., see Figure 4.8) will be closed in favor of the first session in the waiting list. A session that exceeds the idle time limit will not be closed by the server as long as there is no waiting list.
- **Timeout:** The *Timeout* of a connected session starts running when the server stops receiving *renew session requests* for the session (e.g. caused by a crash, network problems, ...). A session that exceeds the timeout time (default 5 min., Figure 4.8) is closed.

If a session is disconnected by the server, e.g. due to idle time or maximum usage limit, a warning box flashes, warning the client that the session is removed from the list of connected sessions. The session halts automatically after a few seconds.

To change the default suggested *Usage time*, *Idle time* and *Timeout* values for a license, select the license from the list in the left panel and press the **<Change>** button to call the *License properties dialog box* (see Figure 4.8).

## 4.4 Running sessions on the clients

---

After the Setup has finished installing the BioNumerics application, configured with a network license, on the client computers (see 3), the BioNumerics application should start on the client computers if the following conditions are met:

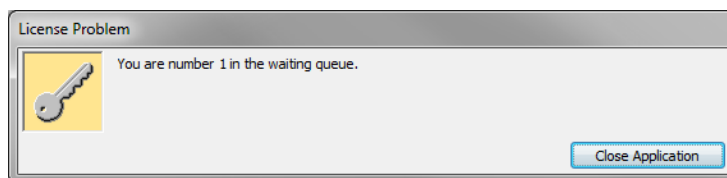
1. The NetKey+ service is running on the NetKey+ server computer (see 4.2).
2. The correct NetKey+ server name and TCP port number have been specified on the client computer.
3. If present, the security software (e.g. firewall) has been configured to allow access to the NetKey+ TCP port.
4. The TCP port is not in use by another application.
5. There is a matching access rule that grants the client access to the license (see 4.3).

If a client is allowed access to the license, but the session limit is reached (see 4.3), the session is added to the waiting queue. A message pops up on the client computer, stating how many sessions have to close before the session can be launched by the software (see Figure 4.12). As soon as one of the connected sessions of the corresponding license is closed on one of the clients, the first session in the waiting list automatically opens on the client computer, and all waiting numbers of the remaining sessions in the waiting queue are updated. Press the **<Close Application>** button if you wish to remove the session from the waiting list.

## 4.5 Monitoring sessions

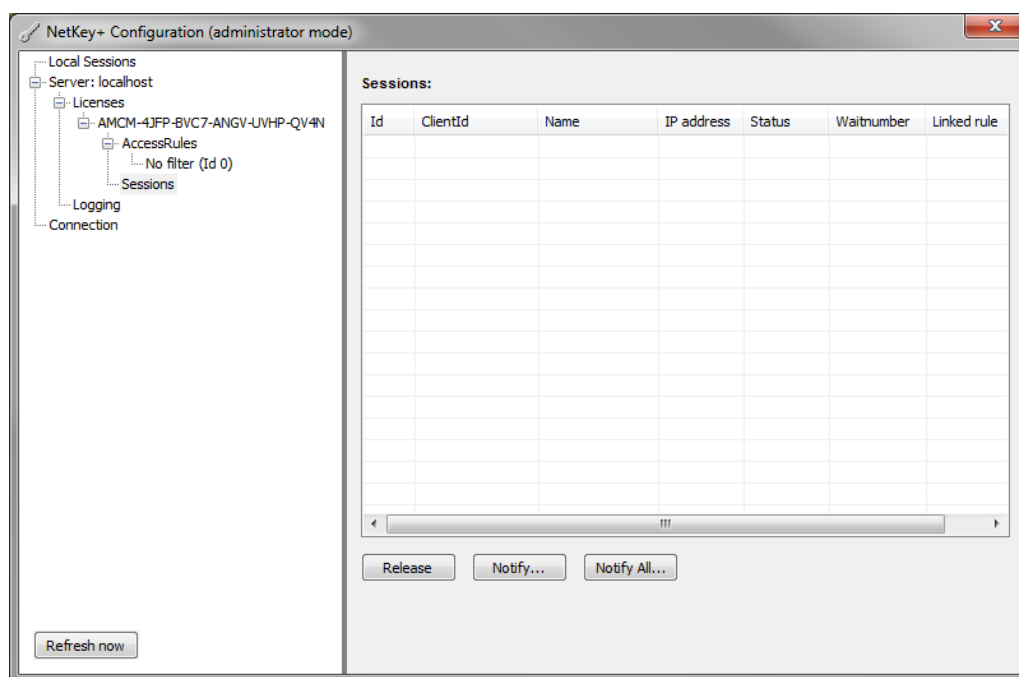
---

A list of all sessions that are running on the client computers and that are put on hold, can be consulted in the *NetKey+ Configuration window* when logged in as **Administrator** or as **User** with **Full** view mode (see



**Figure 4.12:** Waiting queue.

Table 4.1). Selecting the **Sessions** option in the left panel, shows the sessions in the right panel (see Figure 4.13). Each connected session and session present in the waiting queue is identified by a unique *session identifier* (**ID** column). The access rule ID that grants access to the license is displayed in the **Linked rule** column. Information of the associated client computer is shown in the **Client Id**, **Name** and **IP address** columns. The **Status** of each connected session is set to **Connected**. When a session is put on the waiting list (**Waiting** status), the number of sessions that have to close before this session can be launched by the software is displayed in the **Wait number** column. Detailed session information is shown in the right panel when selecting a session in the left panel.

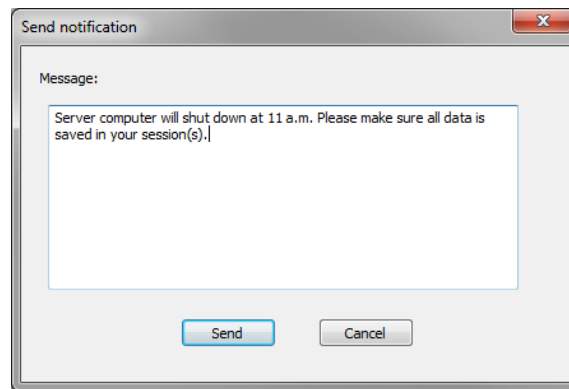


**Figure 4.13:** List of connected sessions and sessions that are present in the waiting queue.

In **Administrator** mode, messages can be sent to any or all connected clients, for example in case the server computer will be shut down or if a session will be disconnected (see Table 4.1). To send a message to a client, select a session of the client in the *Sessions panel* (see Figure 4.13), and press the **<Notify>** button (see Figure 4.13). Alternatively, select the session under the **Sessions** option in the left panel and select the **<Notify>** button. Enter a message string and press **<OK>** (see Figure 4.14). The message is sent to the corresponding client. A message can be sent to all users with **<Notify All>**. All active users will receive the message in a dialog box.

All connected sessions on the clients and sessions present in the waiting queue, can be closed by the **Administrator** (see Table 4.1). To close a session, select the session in the *Sessions panel* (see Figure 4.13), and disconnect the session with **<Release>**. Alternatively, select the session under the **Sessions** option in the left panel and select the **<Release>** button.

A list of all sessions that are running on the *local* computer and that are put on hold, can be consulted in



**Figure 4.14:** Notification message.

the *NetKey+ Configuration window* when logged in as **Administrator** or as **User** with **Full** or **Limited** view mode. Selecting the **Local Sessions** option in the left panel, shows all connected local sessions and local sessions that are present in the waiting queue below the **Local Sessions** option in the left panel (see Figure 4.13). The **Status** (**Connected** or **Waiting**) and **Time in use**, are shown next to each local session. Detailed session information is shown in the right panel when selecting a local session in the left panel.

## 4.6 Logging data

When the NetKey+ Configuration program is launched in **Administrator** mode or in **User** mode with **Full** view, the **Logging** option is displayed in the left panel (see Table 4.1 and Figure 4.15).

Pressing the **Logging** option in the left panel shows all logged information in the right panel. This logged information is stored in a text file called `NetKey+_Log.txt`. This file is located in the folder containing application data for all users (`CommonAppDataFolder`). The path of this folder depends on the operating system version.

- Windows Vista or later: `C: \ProgramData \Applied maths \NetKey+`
- Windows XP: `C: \Documents and Settings \All Users \Application Data \Applied maths \NetKey+`

When *verbose logging* is enabled, additional information messages are logged in the text file (see Figure 4.15). Selecting the **<Change>** button changes the verbose logging status. To clear the log file, press the **<Clear log>** button.



Enabling/disabling verbose logging (**<Change>**) and clearing the log file (**<Clear log>**) is only possible in **Administrator** mode (see Table 4.1).

## 4.7 Resetting the NetKey+ settings

When the NetKey+ Configuration tool is run with Windows elevated privileges (**Run as administrator**), the **<Reset service>** button is displayed in the *Login window* (see Figure 4.2). This button allows you to delete all current NetKey+ settings, including the Administrator password. Furthermore this operation will delete all licensing information and access rules you may have configured previously. Hence the reset service function should be used with caution.

Use the following steps to stop the NetKey+ service and delete the NetKey+ settings:

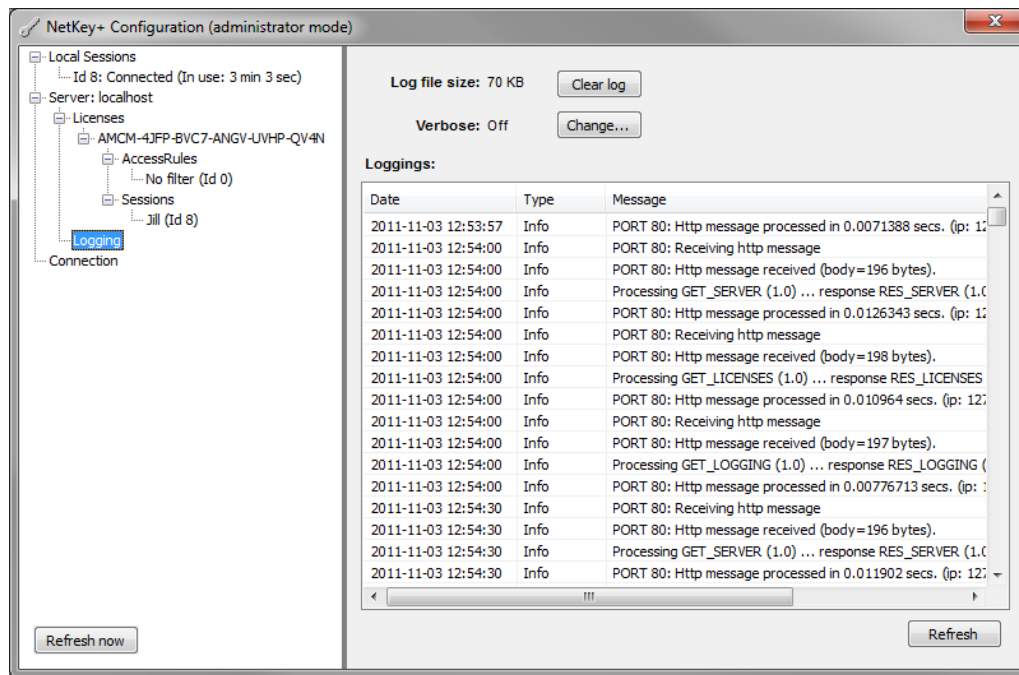


Figure 4.15: Logging information.

1. Click the **<Reset service>** button in the *Login window* (see Figure 4.2).
2. Click **<Yes>** in the confirmation dialog (see Figure 4.16) to delete the current NetKey+ configuration. All NetKey+ settings will be deleted after clicking **<Yes>**.
3. Select the **Administrator** option in the upper *Application mode panel*.
4. Verify and update the **Port** and **Admin port** TCP port numbers if needed. Make sure that the TCP port numbers are not in use on the NetKey+ server computer.
5. Click **<Continue>** and select **Connection** in the left panel to display the **Service** settings.
6. Click **<Start>** in the lower *Service panel*. This brings up the *Change server password dialog*.
7. Enter a secure NetKey+ Administrator password in the **New password** and **Confirm password** text boxes. This password will be required to be able to start the NetKey+ Configuration tool in Administrator application mode.
8. Restart the NetKey+ Configuration tool. Select the **Administrator** option in the upper *Application mode panel* and enter the Administrator **Password** created in the previous step.
9. Click **<Continue>** to connect to the NetKey+ service.

Now you are ready to start configuring the access rules for your BioNumerics license.

## 4.8 Repairing the NetKey+ service

The following steps allow you to repair the NetKey+ service without deleting the current configuration:

1. Select the **Administrator** option in the upper *Application mode panel*.
2. Enter the NetKey+ Administrator **Password** and click the **<Continue>** button.

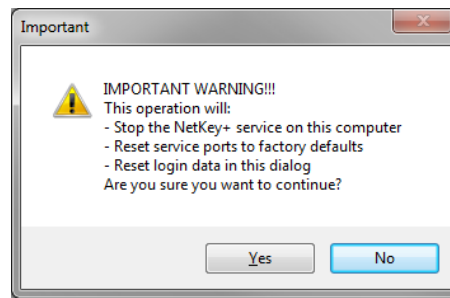


Figure 4.16: Warning message.

3. Select **Connection** in the left panel to display the **Service** settings. Click the **<Remove>** button in the lower **Service panel** to uninstall the NetKey+ Windows service.
4. Click **<Install>** to re-install the NetKey+ service.
5. Next, click the **<Start>** button to start the NetKey+ service.
6. Close the NetKey+ Configuration tool.

## 4.9 Overview of configuration rights

The NetKey+ Configuration program (`NetKey+Config.exe`) is available on the server computer and on all client computers that have the application software installed. This configuration tool can be run as *NetKey+ user* or *NetKey+ administrator*, in combination with or without *Windows elevated rights*. An overview of all rights for the four different login options are shown in the table below.

## 4.10 Usage statistics

### 4.10.1 Usage information parse tool

The NetKey+ server program comes with a standalone command line tool called `ParseUsage.exe`. This tool will transform the NetKey+ log file (see 4.6) to a tab-delimited text file. This text file can easily be imported in MS Excel, which can be used to create usage statistics.

On the NetKey+ server computer, open a command prompt or a Windows PowerShell window and navigate to the NetKey+ installation folder (see 3.1.7).

Enter the command `"ParseUsage "` and press **Enter** to see how to use the `ParseUsage.exe` tool. The result is depicted in Figure 4.17.



For Windows PowerShell, start any command line with `". \ "`. For example, `"ParseUsage "` in a command prompt becomes `". \ParseUsage "` in PowerShell.

Table 4.2 lists all available options for the `ParseUsage.exe` command line tool.

For the `ParseUsage.exe` tool to work, at least the path for the output file should be specified, e.g. `"ParseUsage out=C:\LogFiles\NetKey+.TXT "`.



In case a file path contains one or more spaces, it should be enclosed with double quotes in the Windows command prompt or PowerShell.

The output of `ParseUsage.exe` is a tab-delimited text file with seven fields:

	Windows elevated rights	Windows user rights
NetKey+ admin (password required)	<ul style="list-style-type: none"> <li>• Configure licenses, passwords, logging</li> <li>• Monitor all sessions</li> <li>• View log information</li> <li>• Start/stop service only when run on the server computer</li> <li>• Configure ports</li> </ul>	<ul style="list-style-type: none"> <li>• Configure licenses, passwords, logging</li> <li>• Monitor all sessions</li> <li>• View log information</li> </ul>
NetKey+ user (no password)	<ul style="list-style-type: none"> <li>• Limited user view: Monitor own sessions, Configure ports</li> <li>• Full user view: Monitor own sessions, View session information from other clients, View log information, Configure ports</li> </ul>	<ul style="list-style-type: none"> <li>• Limited user view: Monitor own sessions</li> <li>• Full user view: Monitor own sessions, View session information from other clients, View log information</li> </ul>

**Table 4.1:** Running the NetKey+ configuration tool with different rights.

```

C:\Windows\system32\cmd.exe

C:\Program Files (x86)\Applied Maths\BioNumerics66beta>ParseUsage.exe
Please provide argument 'out'.

ParseUsage out=<filename> [inp=<filename>] [begin=<date>] [end=<date>] [Lic=<license string>] [IP=<ip address>] [User=<user>]

- out: output text file
- inp: optional, input file name, default %ProgramData%\Applied Maths\netkey+\NetKey+ LOG.txt
- begin: optional, begin date in output file, format YYYY-MM-DD
- end: optional, end date in output file, format YYYY-MM-DD
- Lic: optional, filter on specific license string
- IP: optional, filter on specific ip address
- User: optional, filter on specific user

C:\Program Files (x86)\Applied Maths\BioNumerics66beta>_

```

**Figure 4.17:** Windows command prompt with "ParseUsage " executed.

- **Start:** Time stamp for the start of a session.
- **End:** Time stamp for the end of a session.
- **Duration (s):** Total time that the session lasted (in seconds).
- **Lic:** License string used.
- **IP:** IP address (IPv4) of the computer where the session was in use.
- **User:** Windows user name.



Option	Description
out	The location and name of the output file Example: "out=c:\NetkeyReports\usage_Q1_2011.txt "
inp	The location of the NetKey+_LOG.txt file (optional) Default value: "%ProgramData%\Applied Maths\netkey+\NetKey+_LOG.txt " Example: "inp=c:\Logfiles\Netkey+\Netkey+_LOG_2011.txt "
begin	A begin date in the format YYYY-MM-DD (optional) Example: "begin=2011-01-01 "
end	An end date in the format YYYY-MM-DD (optional) Example: "end=2011-03-31 "
Lic	A filter on a specific license string (optional) Example: "Lic=ABCD-82FP-234N-2N8V-VVHP-UR99 "
IP	A filter on a specific client IP address (IPv4) (optional) Example: "IP=192.168.001.010 "
User	A filter on a specific user name (optional) Example: "User=John "

Table 4.2: Options for ParseUsage.exe.

- **ID:** Session ID as generated by the NetKey+ server program.

## 4.10.2 Example

We will illustrate the use of ParseUsage.exe with following (hypothetical) example:

In a research institute there are two types of BioNumerics network licenses, one with all modules (for 3 simultaneous users) and another one with only the Fingerprint data module and the Tree and network inference module (for 5 simultaneous users). The institute has bought this for multiple users belonging to three different labs. Since each lab has its own annual budget, the institute would like to charge the labs for their usage of the different BioNumerics licenses. Invoicing is done after the end of each quarter. The financial department has calculated that the total cost of the 3-user network license is 500 euro per quarter and the cost of the 5-user network license is 350 euro per quarter. Each lab should be billed the respective portion of each license.

- **LAB1 users:** Peter S., Jake, Tim
- **LAB2 users:** Jane, Peter V., Sophie, Anna
- **LAB3 users:** Tom, Catherine, Luke

An example NetKey+ log file, named Netkey+\_LOG\_demo.TXT, can be downloaded from the Applied Maths website (<http://www.applied-maths.com/download/sample-data>, click on "Example NetKey+ log file").

As the NetKey+ server program logs all opened sessions, we will use the ParseUsage.exe tool to create a usage report for the first quarter of 2011.

10.1 On the command line specify: "ParseUsage out=c:\Users\Public\Documents\usage\_Q1\_2011.txt inp=c:\Users\Public\Documents\Netkey+\_LOG\_demo.txt begin=2011-01-01 end=2011-03-31 " and press **Enter**.



Obviously, if the example Netkey+\_LOG\_demo.TXT file is located in a different directory, the command line should be adapted accordingly.



The instructions given below are for Microsoft Excel 2010. For other versions of Excel, we refer to the corresponding user manual.

10.2 Open the usage\_Q1\_2011.TXT file with MS Excel and add a column for the Lab according to the list of lab members shown above (see Figure 4.18 for an example).

	A	B	C	D	E	F	G	H
1	Start	End	Duration(s)	Lic	IP	User	ID	Lab
2	1/01/2011 9:34	1/01/2011 12:24	10182	XYZQ-82XP-134N-2N9V-WWHP-UP99	192.168.001.026	Anna	fbdbce11a39b	LAB2
3	1/01/2011 9:34	1/01/2011 11:24	6574	ABCD-82FP-234N-2N8V-VVHP-UR99	192.168.001.031	Jane	82473553507a	LAB2
4	1/01/2011 9:34	1/01/2011 11:22	6473	XYZQ-82XP-134N-2N9V-WWHP-UP99	192.168.001.016	Luke	8e944d3e9c49	LAB3
5	1/01/2011 9:34	1/01/2011 11:32	7064	ABCD-82FP-234N-2N8V-VVHP-UR99	192.168.001.020	Luke	9ee0fc6cdb16	LAB3
6	1/01/2011 9:34	1/01/2011 11:03	5337	ABCD-82FP-234N-2N8V-VVHP-UR99	192.168.001.032	Tim	13ff03553f56	LAB1
7	2/01/2011 9:34	2/01/2011 10:32	3476	ABCD-82FP-234N-2N8V-VVHP-UR99	192.168.001.010	PeterS	991bb33ad03f	LAB1
8	2/01/2011 9:34	2/01/2011 12:11	9416	XYZQ-82XP-134N-2N9V-WWHP-UP99	192.168.001.033	Sophie	39becb89b6a6	LAB2
9	3/01/2011 9:34	3/01/2011 13:03	12512	ABCD-82FP-234N-2N8V-VVHP-UR99	192.168.001.029	Anna	698505cefb1e	LAB2

Figure 4.18: The parsed usage file in MS Excel.

10.3 Select the whole range that contains data and insert a "PivotTable" with "PivotChart" in Excel.

10.4 Click <OK>.

10.5 Choose 'Lic' and 'Lab' as Category fields (Axis field) and 'Duration (s)' as the Values field (Sum). The result is depicted in Figure 4.19.

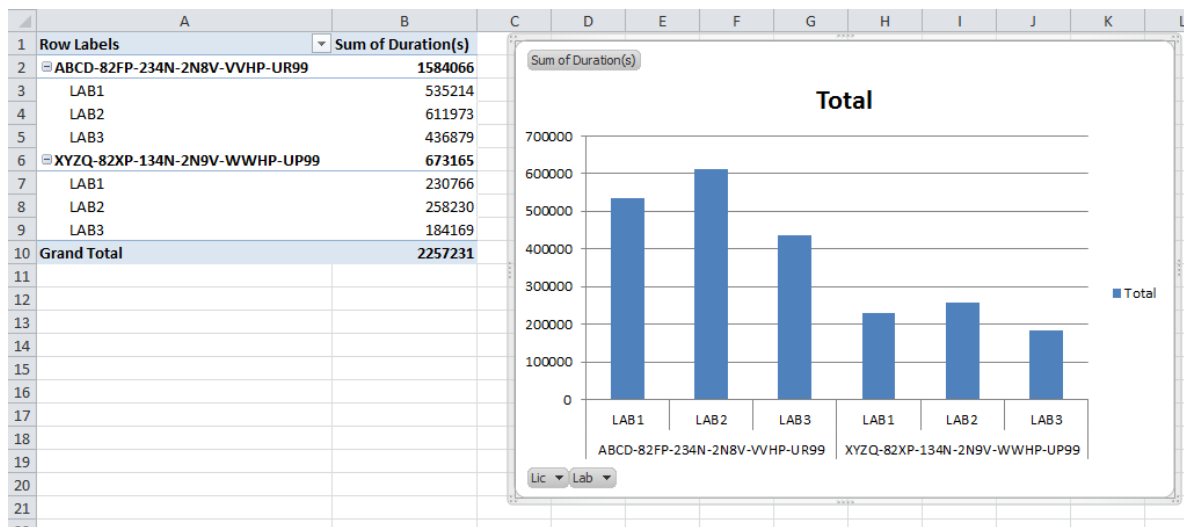


Figure 4.19: Resulting PivotTable and PivotChart in MS Excel.

Currently, usage times are expressed in absolute values (seconds), but we can change the display setting for the "Sum of Duration (s)" to relative values.

10.6 Right-click on the "Sum of Duration (s)" cell and choose "Show values as > % of Parent Total..." with the base field 'Lic'.

10.7 You can then easily add a 'Cost' column to this PivotTable and see the respective value per lab per license (see Figure 4.20).

	A	B	C
1	Row Labels	Sum of Duration(s)	Cost
2	ABC-82FP-234N-2N8V-VVHP-UR99	100,00%	€ 350,00
3	LAB1	33,79%	€ 118,26
4	LAB2	38,63%	€ 135,22
5	LAB3	27,58%	€ 96,53
6	XYZQ-82XP-134N-2N9V-WVHP-UP99	100,00%	€ 500,00
7	LAB1	34,28%	€ 171,40
8	LAB2	38,36%	€ 191,80
9	LAB3	27,36%	€ 136,79
10	Grand Total		

**Figure 4.20:** Calculated license costs per lab and per license.



# Chapter 5

## Installation process

### 5.1 Overview

---

The purpose of this chapter is to provide a general technical explanation on the Setup behavior, and a basic Setup flow diagram of the installation processes. This chapter contains a partial list of the main functions that are applied in the InstallShield installation script. It is not intended to provide a detailed description of all functions implemented in the installation script.

The BioNumerics installation process can be divided into three main blocks: the initial dialog sequence, the feature installation or removal processes and a final sequence running a cleanup process and showing the finish dialog. A subset of dialogs D1 to D9 is displayed during the initial dialog sequence when the Setup is running in normal (non-silent) mode. Next, the *OnMoveData* process will install the selected features, and uninstall the de-selected features.

The Setup will call the appropriate functions for each feature that is being installed or removed: *<feature>\_Installing* and *<feature>\_Installed* during installation, and *<feature>\_UnInstalling* and *<feature>\_UnInstalled* during removal. Each *<feature>\_\** feature function will either call the *FeatureStart* or the *FeatureEnd* function to create the feature node in the Setup log XML file with the proper time stamp elements. The feature nodes contain the information, warning and error messages for a specific feature.

In normal (non-silent) mode the final sequence will display the finish dialog. The *CleanUp* function will display the Setup log file in Internet Explorer if warning or error messages were written to the Setup log file.

### 5.2 Setup dialog list

---

The following table lists the dialogs that are displayed during a normal Setup, and that are invoked by the InstallShield engine and installation script (see Table 5.1). This does not include the dialogs from the NetKey+ Configuration tool.

### 5.3 Setup processes

---

#### 5.3.1 Read command line options

---

When the Setup executable is launched the Setup engine will first attempt to detect if a previous instance of the software is already installed. If the same or another version of the software is already installed the Setup will initially display the *Existing Installed Instances Detected dialog box*. Next, the engine will launch the InstallShield installation script.

Number	Dialog name	Dialog image	Related section
D1	Existing Instances		<a href="#">3.1.3</a>
D2	Dlg_SdWelcome		<a href="#">3.1.3</a>
D3	Dlg_Start / SdWelcomeMaint	Figure <a href="#">3.21</a>	<a href="#">3.3.2</a>
D4	Dlg_SdLicense2		
D5	Dlg_SdSetLicense	Figure <a href="#">3.4</a>	<a href="#">3.1.5</a>
D6	Dlg_SdPathOptions	Figure <a href="#">3.6</a>	<a href="#">3.1.7</a>
D7	Dlg_SdFeatureTree	Figure <a href="#">3.7</a>	<a href="#">3.1.8</a>
D8	Dlg_SdNetKey	Figure <a href="#">3.10</a>	<a href="#">3.1.10</a>
D9	Dlg_SdStartCopy2		
D10	SdFinish / SdFinishReboot		

**Table 5.1:** The Setup dialog list.

One of the first initialization steps in the installation script is to read the optional command line options used to launch the Setup executable. Currently, the Setup supports the `-ini` and `-logdir` command line parameters. See [3.6](#) for more details.

### 5.3.2 Read global variables

After parsing the optional command line parameters the Setup will call the *ReadGlobalVariables* function. This function will:

- Read database home directory from the registry or InstallShield log file.
- Read the Setup INI XML file and check if the file contains a valid license string. The Setup will run in silent mode if the license string is valid. The Setup will abort if a Setup INI XML file has been specified using the `-ini` command line parameter, and the file does not contain a valid license string.
- Read the paths of the Setup log, installation and home directories from the Setup INI XML file.
- Read the requested features listed from the Setup INI XML file. The NetKey+ feature will only be available for installation if a valid network license has been specified in the Setup INI XML file.

### 5.3.3 Write global variables

The *WriteGlobalVariables* function will save the paths of the Setup log, installation and home directories to the Setup INI XML object, if the Setup is running in normal (non-silent) mode. This function will also save the registered user and organization names, and the license string to the Setup INI XML object.

### 5.3.4 Save Setup INI XML file

If the Setup is running in normal (non-silent) mode, the *XML\_SaveIni* function will save the contents of the INI XML object from memory to the Setup INI XML file.

### 5.3.5 Read requested features

In silent mode, the *ReadGlobalVariables* function will read the requested features listed in the Setup INI XML file. The NetKey+ server program feature will only be available for installation if a valid network license has been specified in the Setup INI XML file.

### 5.3.6 Save Setup Log

---

The first time the *XML\_SaveLogFile* function is called the Setup will generate a unique file name for the Setup log XML file. Next, the Setup will copy the following style sheet files to the Setup log folder: *processlogs.xsl*, *applied-maths.css*, *amheader.jpg* and *amlogo.gif*.

Finally, the *XML\_SaveLogFile* function will save the contents of the Setup log XML object from memory to the Setup log XML file.

### 5.3.7 OnMoveData

---

The *OnMoveData* function is the main Setup process that handles the file transfer. First, the function will display the progress bar dialog and create the uninstall information in the registry. Next, the function will call the *CheckLicense* function to check and save the license string to the HKEY\_LOCAL\_MACHINE hive of the registry (if a valid license string was entered).

Subsequently, the *OnMoveData* process will call the *FeatureTransferData* function to install or remove feature files. The *FeatureTransferData* function will launch the *<feature>\_Installing* or *<feature>\_UnInstalling* function before installing or removing a feature. After a feature has been installed or removed the Setup will call the *<feature>\_Installed* or *<feature>\_UnInstalled* function.

Finally, the *OnMoveData* function will call the *LaunchNetKey* function to launch the NetKey+ server configuration tool if the corresponding feature was selected for installation.

### 5.3.8 Feature functions

---

Each feature can be linked to four event handlers:

- The *OnInstalling* event handler responds to the *Installing* event that is generated just before the corresponding feature is installed. This handler is linked to a *<feature>\_Installing* function.
- The *OnUnInstalling* event handler responds to the *UnInstalling* event generated just before the corresponding feature is removed from the target system. This handler is linked to a *<feature>\_UnInstalling* function.
- The *OnInstalled* event handler responds to the *Installed* event that is generated just after the corresponding feature has been installed. This handler is linked to a *<feature>\_Installed* function.
- The *OnUnInstalled* event handler responds to the *UnInstalled* event generated just after the corresponding feature has been removed from the target system. This handler is linked to a *<feature>\_UnInstalled* function.

Each *<feature>\_Installing* and *<feature>\_UnInstalling* function will call the *FeatureStart* function to create a *feature* node and a *start* time stamp element in the Setup log XML file. In addition, each *<feature>\_Installed* and *<feature>\_UnInstalled* function will call the *FeatureEnd* function to create an *end* time stamp element in the Setup log XML file.

The feature event handler functions that call other function in addition to the *FeatureStart* and *FeatureEnd* function are described in the next sections.

The *Application\_Installing* event handler function is called by the Setup just before the main BioNumerics application feature is installed. First, this process will call the *DeleteOldFiles* function to delete legacy files from the BioNumerics program folder, which are no longer included in the current Setup package.

Next, the *Application\_Installing* function will run the *vcredist\_x86.exe* executable to install the Microsoft Visual C++ 2008 Redistributable Package (x86).

The *Application\_Installed* event handler function is called by the Setup immediately after the application feature has been installed. This function will write the database home directory to the HKEY\_CURRENT\_USER hive.

If a network license string was entered, the *Application\_Installed* function will read the NetKey+ server properties from the Setup INI XML file, and create or overwrite the NetKey.ini file in the common application data folder.

Finally, the function will create the shortcuts in the Startup menu and desktop folder.

The *Application\_UnInstalled* event handler function is called by the Setup just after the main BioNumerics application feature has been removed. This function will call the *DeleteOldFiles* function to delete legacy files from the BioNumerics program folder, which are no longer included in the current Setup package.

The *Sentinel\_Installed* event handler function is called by the Setup after the Sentinel drivers placeholder feature has been installed. This process will first call the *IsSentinelInstalled* function to check if the minimum required version of the Sentinel System Drivers is already installed. If the required version is not installed, or in repair maintenance mode, the *Sentinel\_Installed* function will call the *HasDongles* function to check if hardware security keys are connected to the target computer. The appropriate warning messages will appear if existing hardware security keys were detected.

Next, the function will call the *MSI\_InstallProduct* function to install the Sentinel System Driver Windows Installer package (e.g. Sentinel System Driver Installer 7.5.1.msi).

The *NetKey\_Installing* event handler function is called by the Setup just before the NetKey+ server program feature is installed. First, this function will stop the NetKey+ service if it already exists on the target system. This will make sure that existing files are no longer in use, and will allow the Setup to overwrite these files if needed.

Next, the *NetKey\_Installing* process will call the *IsOldNetKeyInstalled* function to delete conflicting versions of the NetKey+ service.

Finally, the function will grant full NTFS permissions to the built-in "NT AUTHORITY\SYSTEM" account for the Applied Maths common application data folder. This way the NetKey+ service running with the SYSTEM account will have sufficient privileges to create and modify files in the NetKey+ sub-folder.

The *NetKey\_Installed* handler function is called by the Setup just after the NetKey+ server program feature has been installed. If the NetKey+ sub-folder in the Applied Maths common application data folder already contains a NetKey+\_CONFIG.txt file, then the Setup will call the *WMI\_ServiceStart* function to start the NetKey+ service.

The *NetKey\_UnInstalling* event handler function is called by the Setup just before the NetKey+ server program feature is removed from the target system. This process will first call the *WMI\_ServiceExists* function to verify if the NetKey+ service exists. If the service exists, then the Setup will check if the path of the service executable matches the program folder configured for the current instance. If both paths are equal then the function will call *WMI\_ServiceStop* to stop the NetKey+ service.

If the running NetKey+ service is installed in a different folder than the program folder of the current BioNumerics instance then the service will not be stopped.

The *NetKey\_UnInstalled* event handler function is called by the Setup just after the NetKey+ server program feature has been removed. This process will first call the *WMI\_ServiceExists* function to verify if the NetKey+ service exists. If the service exists, then the Setup will check if the path of the service executable matches the program folder configured for the current instance. If both paths are equal, then the function will call the built-in *ServiceRemoveService* InstallShield function to remove the NetKey+ service.

If the running NetKey+ service is installed in a different folder than the program folder of the current BioNumerics instance, then the service will not be removed.



The *Database\_Installed* handler function is called by the Setup just after the sample database feature has been installed. This function will set the *Current Database* value in the HKEY\_CURRENT\_USER hive of the registry if the string value does not already exist.

The *DeleteOldFiles* function will delete legacy files from the BioNumerics program folder, which are no longer included in the current Setup package. Only legacy files with the following file extensions will be deleted from the program folder: .BXT,.DLL,.EXE,.AVI,.PYC and .XML.

The *IsSentinelInstalled* function will check the Windows Installer database to verify if the minimum required version of the Sentinel System Driver Installer is already installed. If the USB Driver feature is not installed, then the function assumes that the Sentinel System Driver package is incomplete, and will instruct the Setup to re-install the package.

The *HasDongles* function will launch the setlic.exe executable to verify if hardware security keys or dongles are connected to the target system. The function will check the exit code of the setlic.exe program to verify if dongles were detected.

In silent mode, the *CheckLicense* function will first attempt to read the license string from the Setup INI XML file. Next, the function will read the license string from the HKEY\_LOCAL\_MACHINE hive of the registry if the current string is empty. If the license string is still empty, the Setup will use the license string from the previous installation (in maintenance mode).

If the license string has the correct length, the Setup will launch the setlic.exe tool to get the license type of the entered string. The setlic.exe license tool will return one of the following constants: LIC\_STANDALONE, LIC\_NETWORK, LIC\_INTERNET or LIC\_INVALID.

If the *CheckLicense* function was called by the *OnMoveData* function, and the license type is valid (not LIC\_INVALID), then the Setup will save the license string to the HKEY\_LOCAL\_MACHINE hive of the registry.

The *LaunchNetKey* function is called by the *OnMoveData* function to start the NetKey+ configuration tool after the NetKey+ server program feature has been installed, repaired or updated. The function will use the built-in *LaunchApp* InstallShield function to start the NetKey+Config.exe executable. The Setup will continue after the tool has been launched.

The *IsOldNetKeyInstalled* function will use Windows Management Instrumentation (WMI) queries to verify if other instances of the NetKey+ service are already installed. Optionally, this function can also be used to delete the service if the service name does not match, or if the installation path does not match the current BioNumerics program folder.

The service will not be deleted if the service name is NetKey+, and the path matches with the current BioNumerics program folder.

The *SetFilePermissions* function will use the xcaccls.vbs Microsoft Visual Basic script to grant NTFS folder permissions to a specific user. The Setup will launch the xcaccls.vbs script using the cscript.exe application in the 32-bit version of the Windows system folder.

The *MSI\_InstallProduct* function will use the msixec.exe Windows Installer tool to install an MSI package (e.g. Sentinel System Driver Installer 7.5.1.msi).

The *WMI\_ServiceStop* function will first call the *WMI\_ServiceExists* function to verify that the service exists. The function will attempt to stop the service if the service exists and is running. The *WMI\_ServiceStop* function uses the built-in InstallShield functions to control the service on a local computer.

The *WMI\_ServiceStart* function will first call the *WMI\_ServiceExists* function to verify that the service exists. The function will attempt to start the service if the service exists and is not running. The *WMI\_ServiceStart* function uses the built-in InstallShield functions to control the service on a local computer.

The *CleanUp* function will create the end time stamp element in the setup node of the Setup log XML file and close the progress bar dialog. Next, the *CleanUp* function will call the *XML\_ShowLogFile* function to

save and optionally display the Setup log file in Internet Explorer.

Finally, the *CleanUp* function will unload the *IsGetObj.dll* file from memory and will delete the file from the temporary Setup folder.

## 5.4 Setup Process list

---

Table 5.2 shows the main processes and functions that are used in the installation script, and that are displayed in the simplified Setup flow diagram (see Figure 5.1).

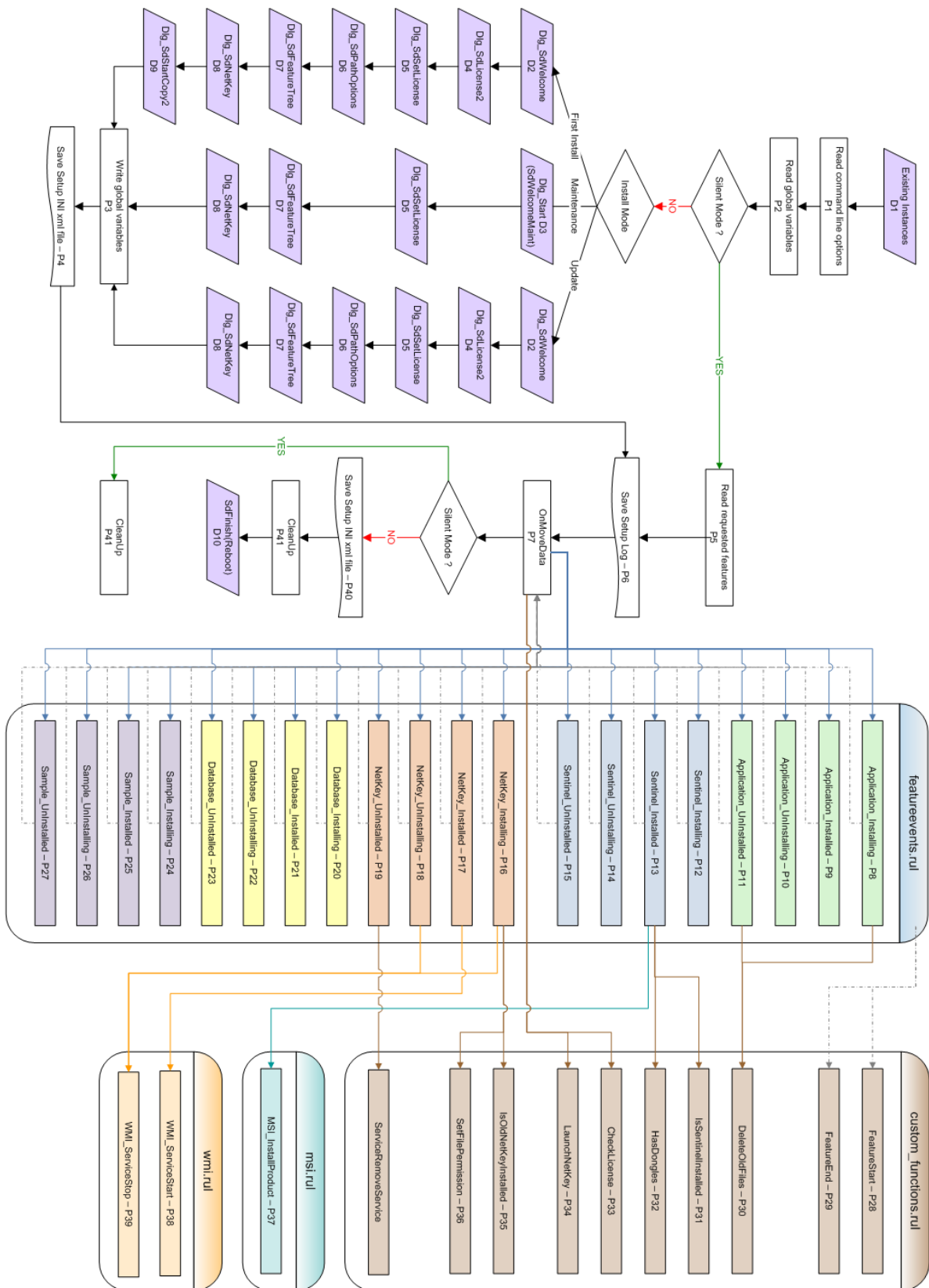


Figure 5.1: The Setup flow diagram.

Process number	Process name	Related section number
P1	Read command line options	<a href="#">5.3.1</a>
P2	Read global variables	<a href="#">5.3.2</a>
P3	Write global variables	<a href="#">5.3.3</a>
P4	Save Setup INI xml file	<a href="#">5.3.4</a>
P5	Read requested features	<a href="#">5.3.5</a>
P6	Save Setup Log	<a href="#">5.3.6</a>
P7	OnMoveData	<a href="#">5.3.7</a>
P8	Application_Installing	<a href="#">5.3.8</a>
P9	Application_Installed	<a href="#">5.3.8</a>
P10	Application_UnInstalling	
P11	Application_UnInstalled	<a href="#">5.3.8</a>
P12	Sentinel_Installing	
P13	Sentinel_Installed	<a href="#">5.3.8</a>
P14	Sentinel_UnInstalling	
P15	Sentinel_UnInstalled	
P16	NetKey_Installing	<a href="#">5.3.8</a>
P17	NetKey_Installed	<a href="#">5.3.8</a>
P18	NetKey_UnInstalling	<a href="#">5.3.8</a>
P19	NetKey_UnInstalled	<a href="#">5.3.8</a>
P20	Database_Installing	
P21	Database_Installed	<a href="#">5.3.8</a>
P22	Database_UnInstalling	
P23	Database_UnInstalled	
P24	Sample_Installing	
P25	Sample_Installed	
P26	Sample_UnInstalling	
P27	Sample_UnInstalled	
P28	FeatureStart	
P29	FeatureEnd	
P30	DeleteOldFiles	<a href="#">5.3.8</a>
P31	IsSentinelInstalled	<a href="#">5.3.8</a>
P32	HasDongles	<a href="#">5.3.8</a>
P33	CheckLicense	<a href="#">5.3.8</a>
P34	LaunchNetKey	<a href="#">5.3.8</a>
P35	IsOldNetKeyInstalled	<a href="#">5.3.8</a>
P36	SetFilePermissions	<a href="#">5.3.8</a>
P37	MSI_InstallProduct	<a href="#">5.3.8</a>
P38	WMI_ServiceStart	<a href="#">5.3.8</a>
P39	WMI_ServiceStop	<a href="#">5.3.8</a>
P40	Save Setup INI xml file	<a href="#">5.3.4</a>
P41	CleanUp	<a href="#">5.3.8</a>

**Table 5.2:** The Setup process list.

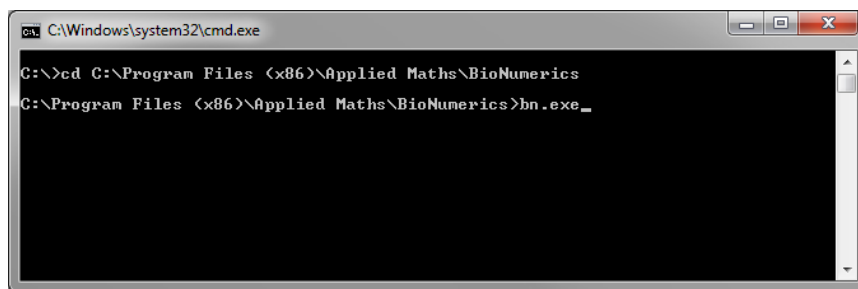
## Chapter 6

# Command line options

### 6.1 Running BioNumerics from the command line

---

The BioNumerics software (bn.exe) can be started from the command line. This can be done by opening a command prompt, navigating to the BioNumerics installation directory (or opening the command prompt immediately in this directory) and entering `bn.exe`. See Figure 6.1 for an example.



**Figure 6.1:** Running BioNumerics from the command line.

When the executable is called without any options, the program will open the last-opened database (as read from the Windows registry). However, the flexibility associated with running BioNumerics from the command line comes with the additional options that can be specified. Following is a list of available options with their values:

- `-database=<DBNAME>`: The BioNumerics database that will be opened, `<DBNAME>` is the name of the database folder (without the path).
- `-homedir=<HOMEDIR>`: The BioNumerics home directory, `<HOMEDIR>` is the full path to the home directory.
- `-bnuser=<USERNAME>`: The BioNumerics database user.
- `-bnpwd=<PWD>`: The password for the specified database user.
- `-licensestring=<LIC>`: The license string (see 4.3) needed to activate the software license.
- `-runbnstart=(0|1)`: Whether or not the startup program should be ran after the main program is closed.
- `-logfile`: Allows to specify a custom log file, different from the default `BNLOG.TXT`. The custom log file needs to reside in the BioNumerics home directory.

- `-id=<ID>`: The ID which should be written in the protection dongle.
- `-script=<PATH>`: Runs a script and does not open the *Main* window by default, `<PATH>` is the full path to the script file.
- `-openmain=(0|1)`: Whether or not the *Main* window should be opened. This option is only valid in combination with the `-script` option.



As always the case with the Windows command prompt, file paths that contain spaces should be enclosed with double quotes.

The command line syntax is quite flexible:

Options can be provided "as is" or they can start with a "-" (hyphen) or "/" (slash). Examples:

```
bn.exe "database=DemoBase"
```

```
bn.exe "-database=DemoBase"
```

```
bn.exe "/database=DemoBase"
```

Options are not case sensitive. Examples:

```
bn.exe "database=DemoBase"
```

```
bn.exe "DataBase=DemoBase"
```

```
bn.exe "DATABASE=DemoBase"
```

Options and their values can optionally be quoted. Examples:

```
bn.exe "database=DemoBase"
```

```
bn.exe database="DemoBase"
```

```
bn.exe database=DemoBase
```

Option names and their values can be separated with ":" or "=". Examples:

```
bn.exe "database=DemoBase"
```

```
bn.exe "database:DemoBase"
```

## 6.2 Running the startup program from the command line

---

The BioNumerics software startup program (BnStart.exe) can be started from the command line. Following options are available:

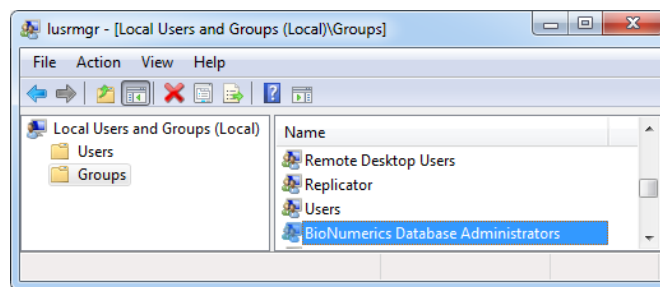
- `-homedir=<HOMEDIR>`: the BioNumerics home directory, `<HOMEDIR>` is the full path to the home directory
- `-licensestring=<LIC>`: the license string (see [4.3](#)), needed to activate the software license

These options will be passed on to `bn.exe` (see [6.1](#)).

## Chapter 7

# Granting access to BioNumerics databases

During the installation of the BioNumerics application, the Setup will create a Windows group named *BioNumerics Database Administrators* (Figure 7.1). This local Windows group has Full control NTFS permissions on the local Database home directory, and if the BioNumerics Database Engine feature is installed members of this group have unrestricted access to the SQL Server databases.



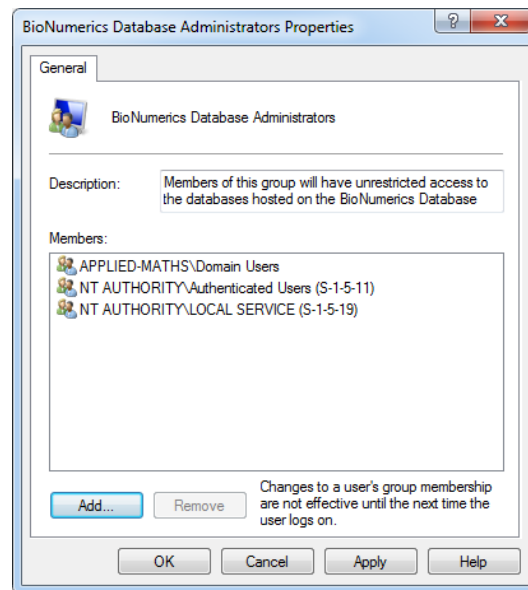
**Figure 7.1:** The BioNumerics Database Administrators Windows group.

By default, the following users and groups are members of the local BioNumerics Database Administrators Windows group:

- User running the BioNumerics Setup
- NT AUTHORITY\Authenticated Users
- Optional Active Directory Security Group selected in the *Database Engine Properties dialog* (see 3.1.9), for example the Domain Users group (Figure 7.2).

The Local Users and Groups management console in Figure 7.1 can be started by running `lusrmgr.msc` on a Windows Command Prompt. Double-click on the BioNumerics Database Administrators Windows group to view the current group members (Figure 7.2). Click the <Add> or <Remove> button to change the group members.

If you do not want all authenticated users to have full access to the BioNumerics Databases you can simply remove the NT AUTHORITY\Authenticated Users group from the BioNumerics Database Administrators group, and replace it with specific users or groups that require database access. For example, you could add all BioNumerics users to an Active Directory Security Group, and add this group to the local BioNumerics Database Administrators Windows group to grant full access to the databases.



**Figure 7.2:** Properties of the BioNumerics Database Administrators Windows group.

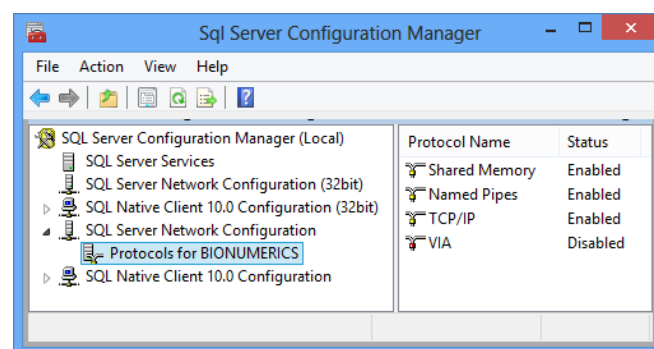
If the Database Engine feature has been installed, then the SQL Server (BioNumerics) service account will also be a member of the BioNumerics Database Administrators Windows group:

- NT AUTHORITY\Local Service (on Windows Vista, Windows Server 2008 or later)
- NT AUTHORITY\Local System (on Windows XP or Windows Server 2003)

The BioNumerics Database Administrators Windows group will also be a member of the *sysadmin* fixed SQL server role on the local BioNumerics instance of the Microsoft SQL Server 2008 R2 SP1 Express database engine. Hence members of this group will be able to perform any activity on the BioNumerics database engine.

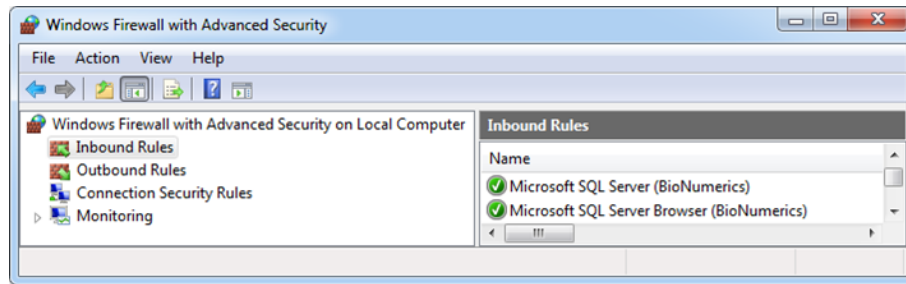
If BioNumerics database sharing has been enabled in the *Database Engine Properties dialog* (see 3.1.9), then the "Microsoft SQL Server (BioNumerics)" inbound Windows firewall rule will be enabled, and TCP/IP and Named Pipes connections to the database engine will be allowed.

To manually enable remote access to the BioNumerics database engine, the appropriate network protocols (TCP/IP) must be enabled in the *SQL Server Configuration Manager tool* (Figure 7.3). In addition, the Microsoft SQL Server (BioNumerics) and the Microsoft SQL Server Browser (BioNumerics) inbound Windows firewall rules will need to be enabled to allow incoming access to the database engine (Figure 45).



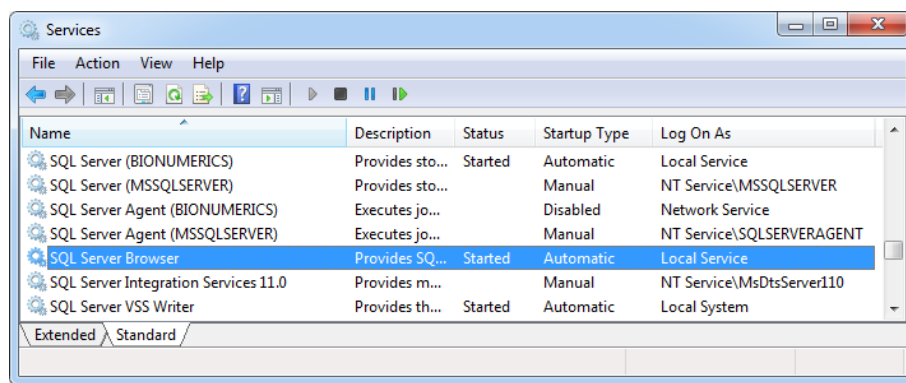
**Figure 7.3:** The SQL Server Configuration Manager tool.





**Figure 7.4:** Windows firewall rules.

By default, the BioNumerics database engine is configured to use dynamic TCP listening ports. Hence the *SQL Server Browser* service should be running, and the Startup Type should be set to "Automatic" to allow client applications to request SQL Server TCP connection information (Figure 7.5).



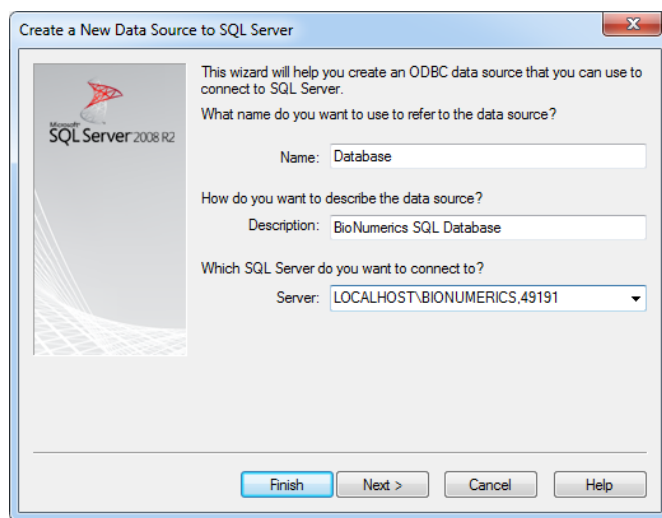
**Figure 7.5:** Windows Services.

If you are unable or not allowed to use *SQL Server Browser* service, then the TCP port number must be specified in the SQL Server instance name when creating a new BioNumerics database (Figure 7.6). In this case, the full SQL Server instance name for the BioNumerics database engine will be formatted like:

<Computer Name>\<SQL Instance Name>,<TCP port number>

For example:

- LOCALHOST\BioNumerics,49191
- SQLSERVER1.domain.local\BIONUMERICS,1445



**Figure 7.6:** Creating a new data source.