

Contents

1	Introduction	3
1.1	Purpose	3
1.2	Target audience	3
1.3	Overview	3
2	System requirements	5
2.1	Hardware requirements	5
2.1.1	Minimum hardware requirements	5
2.1.2	Recommended hardware configuration	5
2.2	Windows operating system	6
2.3	Microsoft XML 6.0	7
2.4	Windows Installer 3.1	7
2.5	Permissions	7
2.6	Security software	7
2.6.1	Anti-virus software	7
2.6.2	Firewall and proxy servers	7
3	Installation procedure	9
3.1	Install a new instance of BioNumerics	9
3.1.1	Welcome dialog	9
3.1.2	Software End User License Agreement	10
3.1.3	Customer information	11
3.1.4	Choose destination location	12
3.1.5	Select features	12
3.1.6	NetKey+ connection settings	14
3.1.7	Confirm installation	15
3.1.8	NetKey+ configuration	15
3.1.9	Setup INI XML file	15
3.2	Updating a BioNumerics instance	16
3.2.1	Welcome dialog	16
3.2.2	Software End User License Agreement	16
3.2.3	Customer information	17
3.2.4	Choose destination location	18
3.2.5	Select features	19
3.2.6	NetKey+ connection settings	20
3.2.7	Confirm update	20
3.3	Maintenance installation	21
3.3.1	Select instance to maintain	21
3.3.2	Maintenance options	22
3.3.3	Modify maintenance mode	22
3.3.4	Repair maintenance mode	23
3.3.5	Remove maintenance mode	23
3.4	Setup log	24

3.5	Silent installation	25
3.5.1	Purpose	25
3.5.2	Installation procedure	25
3.5.3	Setup INI XML file format	26
4	NetKey+ configuration	29
4.1	Introduction	29
4.2	Installing and starting the NetKey+ service on the server	29
4.3	Configuring licenses	33
4.4	Running sessions on the clients	37
4.5	Monitoring sessions	38
4.6	Logging data	39
4.7	Resetting the NetKey+ settings	40
4.8	Repairing the NetKey+ service	40
4.9	Overview configuration rights	41
5	Installation process	43
5.1	Overview	43
5.2	Setup dialog list	43
5.3	Setup processes	43
5.3.1	Read command line options	43
5.3.2	Read global variables	44
5.3.3	Write global variables	44
5.3.4	Save Setup INI XML file	44
5.3.5	Read requested features	44
5.3.6	Save Setup Log	45
5.3.7	OnMoveData	45
5.3.8	Feature functions	45
5.4	Setup Process list	49

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[®], 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
URL: <http://www.applied-maths.com>

Applied Maths, Inc.

13809 Research Boulevard, Suite 645
Austin, Texas 78750
U.S.A.
PHONE: +1 512-482-9700
FAX: +1 512-482-9708
E-MAIL: info-US@applied-maths.com

LIMITATIONS ON USE

The BioNumerics[®] 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, 2010, Applied Maths NV. All rights reserved.

BioNumerics[®] is a registered trademark of Applied Maths NV. All other product names or trademarks are the property of their respective owners. BioNumerics[®] includes the Python[®] 2.6.6 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 or upgrade the Sentinel drivers to the latest version.

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>).

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 and optional database client software and third-party software that will run concurrently (e.g. Microsoft Office).

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

- **Processor:** 1.30 gigahertz (GHz) processor or higher
- **Processor Type:** Intel Pentium 4 or higher compatible processor
- **Memory:** 512 MB or higher
- **Hard disk:** 1 GB of free disk space (application files only)
- **Display:** XGA (1024 x 768) 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 Types 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:** 1.6 gigahertz (GHz) processor or higher
- **Processor Type:** Intel Pentium Dual Core or higher
- **Memory:** 2 GB or higher
- **Hard disk:** 1 GB of free disk space (application files only), fast hard drive for storing database files (e.g. 7200 RPM SATA drive)
- **Display:** SXGA (1280 x 1024) 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 Types module requires a 64-bit processor and a minimum of 8 GB installed memory.

2.2 Windows operating system

Applied Maths NV will support installing BioNumerics on Windows operating system versions for which the Microsoft Extended Support Phase¹ has not been retired. This will allow you to obtain support and security updates from Microsoft for the target operating system.

- Windows XP (SP3 recommended, this includes Microsoft XML 6.0). Note that the Microsoft support for Service Pack 2 has ended on the 13th of July 2010.
- Windows Vista
- Windows 7
- Windows 2003 Server (SP1 recommended, this includes Windows Installer 3.1)
- Windows 2008 Server

Applied Maths NV 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 2003 or 2008. If a Windows Server computer is not available then the NetKey+ program can be installed on a Windows XP or later client operating system.

¹Microsoft Products life cycle information: <http://support.microsoft.com/gp/lifeselect>

2.3 Microsoft XML 6.0

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. If Microsoft XML 6.0 is missing on a Windows XP computer, then upgrading to Service Pack 3 is the recommended option. All other supported operating systems already 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.

2.4 Windows Installer 3.1

Windows Installer 3.1 is a minor update for Windows Installer 3.0 and contains new and improved functionality. Additionally, this version addresses some issues that were found in Windows Installer 3.0. Hence version 3.1 or later is recommended on the computers where the BioNumerics Setup will run.

Windows Installer 3.1 is included with Windows Server 2003 Service Pack 1, and Windows XP Service Pack 3, hence installing these service packs is the recommended option to update the Windows Installer version if the recommended version is not installed. Newer versions of Windows Installer are included with Windows Vista, Windows Server 2008, and later versions of Microsoft Windows.

2.5 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.

2.6 Security software

2.6.1 Anti-virus software

Anti-virus software may considerably affect the performance of BioNumerics. 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 (bnstart.exe and bn.exe), the BXT sub-folder (\BXT *.dll) and specific file extensions (*.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.

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>.

2.6.2 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 two license servers are active to verify internet licenses:

- license.applied-maths.com (217.136.183.96)
- rrcs-71-42-72-154.sw.biz.rr.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 address of the main license server (license.applied-maths.com) 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.

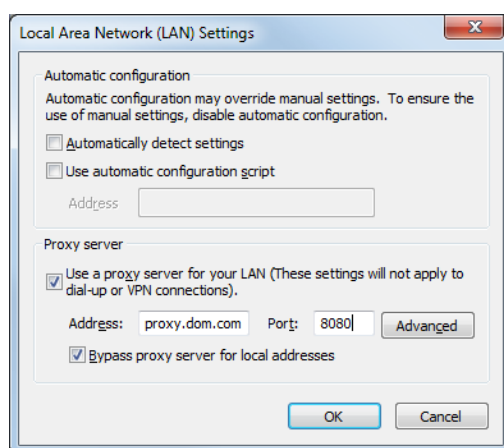


Figure 2.1: The LAN Settings dialog box.

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 Chapter 4.

Chapter 3

Installation procedure

3.1 Install a new instance of BioNumerics

3.1.1 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 (see Figure 3.1). Please verify that you are installing the correct version and click *<Next>* to continue.



Figure 3.1: The *Welcome dialog box*.

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 3.2). 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 perform a side-by-side installation of BioNumerics. For side-by-side installations you must choose a different application installation folder than the one used for the previous installation (see Figure 3.6). This will install a new instance of BioNumerics without upgrading the existing version.

If an instance of BioNumerics 6.5 or later is already installed, then the *Existing Installed Instances Detected*



Figure 3.2: The *Welcome* dialog box.

dialog box will appear when launching the Setup executable (see Figure 3.3). This dialog allows you to choose between installing a new BioNumerics instance, or changing an existing instance. Choose the *Install a new instance of this application* option to install a new instance of BioNumerics. Pressing the *<Next>* button will display the *Welcome* dialog box.

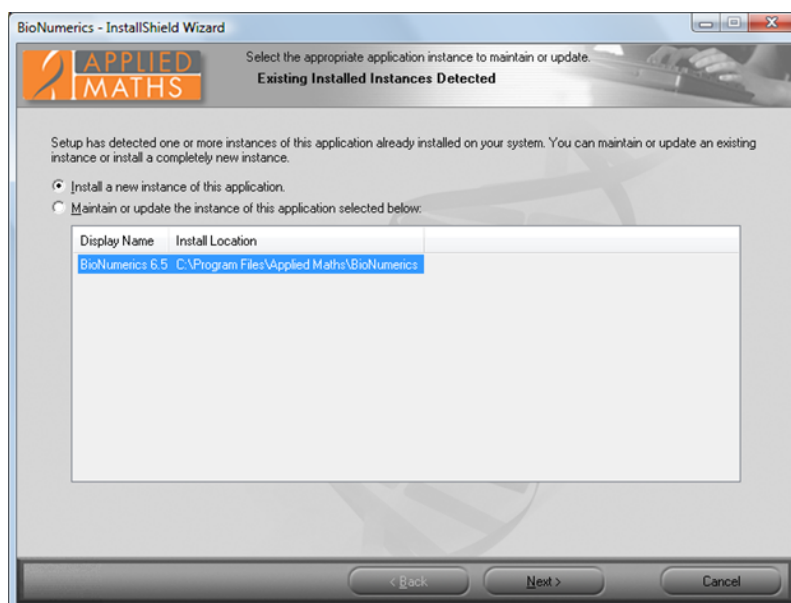


Figure 3.3: The *Existing Installed Instances Detected* dialog box.

3.1.2 Software End User License Agreement

The next dialog will display the Software End User License Agreement (EULA) (see Figure 3.4). 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 3.4: The *License Agreement* dialog box.

3.1.3 Customer information

The *Customer information dialog box* allows you to enter the user and organization names, and the BioNumerics license string (see Figure 3.5). 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.

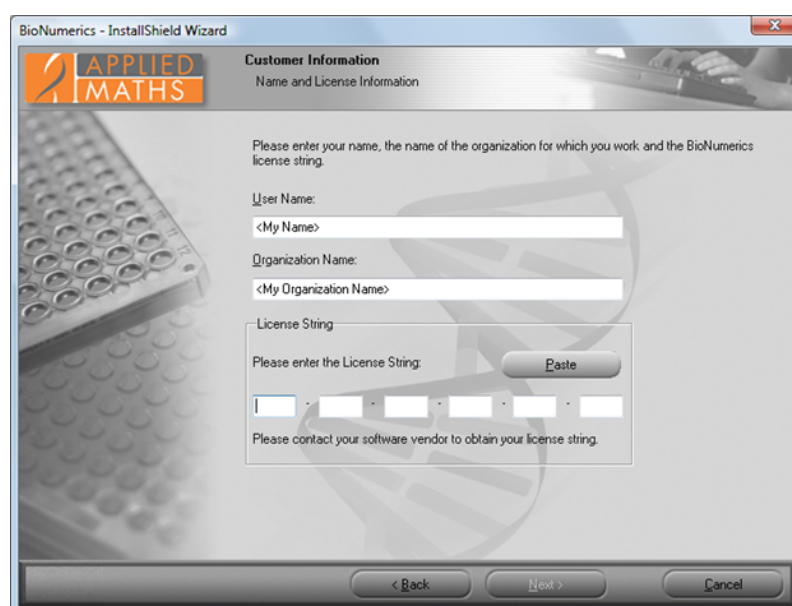


Figure 3.5: The *Customer Information* dialog box.

3.1.4 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.

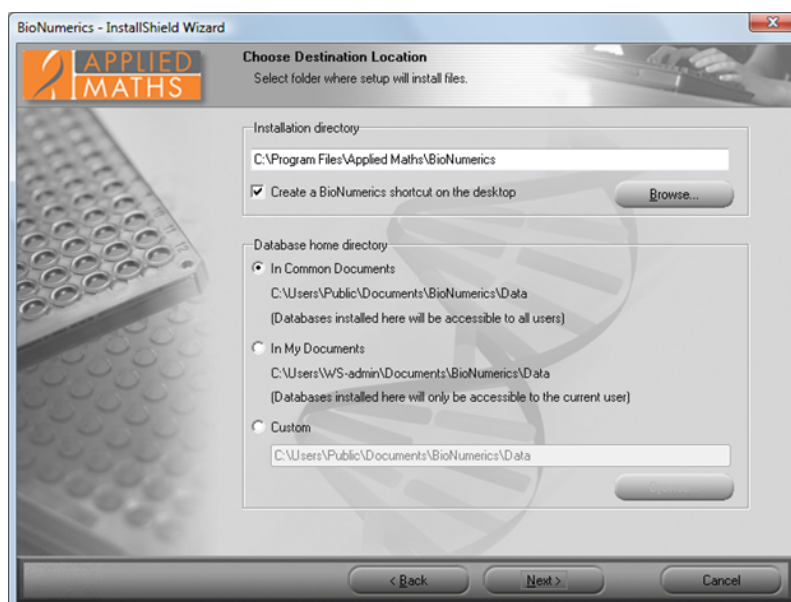


Figure 3.6: The *Choose Destination Location dialog box*.

3.1.5 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.

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

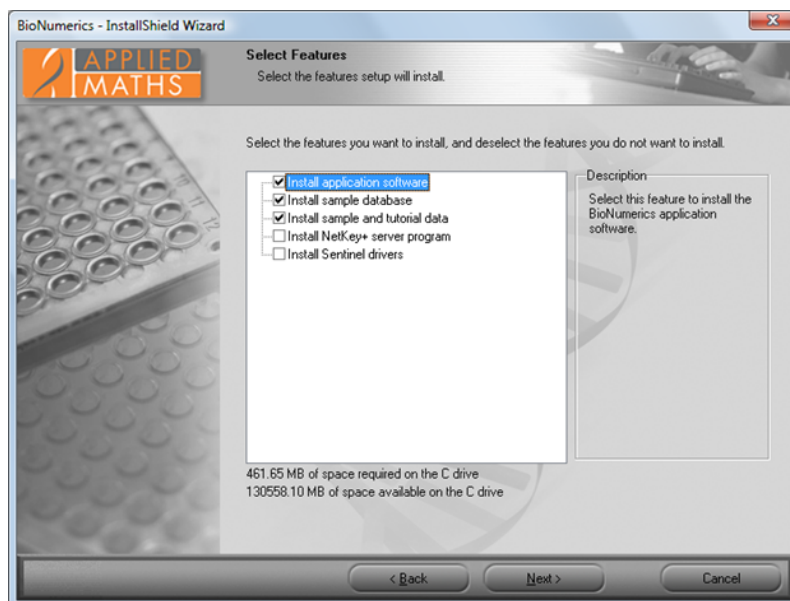


Figure 3.7: The *Select Features* dialog box.

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 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 Quick Guide and 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:

- 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. Since no USB dongle is needed to run an internet license 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 where the hardware security key will be connected to.

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 3.5). 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).

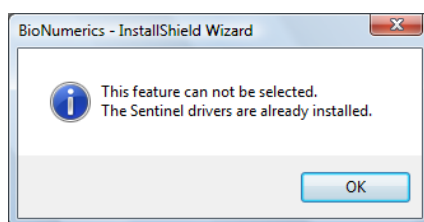


Figure 3.8: Sentinel drivers are already installed.

3.1.6 NetKey+ connection settings

After pressing the *<Next>* button, the *NetKey+ connection settings dialog box* will appear (see Figure 3.9) if a network license string was entered in the *Customer Information dialog box* (see Figure 3.5), and if the BioNumerics application feature was selected for installation (see Figure 3.7).

The *NetKey+ Server name* and *Server port number* connection parameters can be entered in the *NetKey+ connection settings dialog box* (see Figure 3.9). 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.

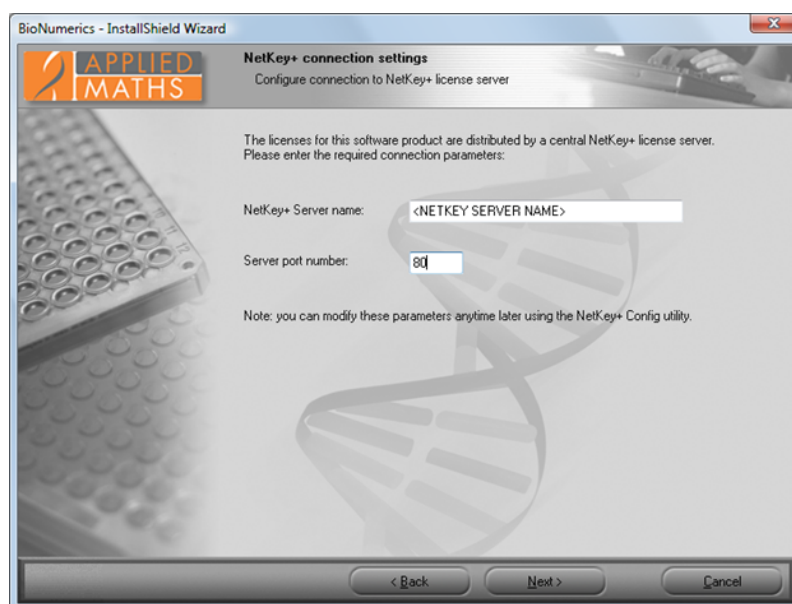


Figure 3.9: The *NetKey+ connection settings dialog box*.

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 +`

3.1.7 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.

3.1.8 NetKey+ configuration

If a network license string has been entered in the *Customer Information dialog box* (see Figure 3.5), 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 3.10). 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 Chapter 4.

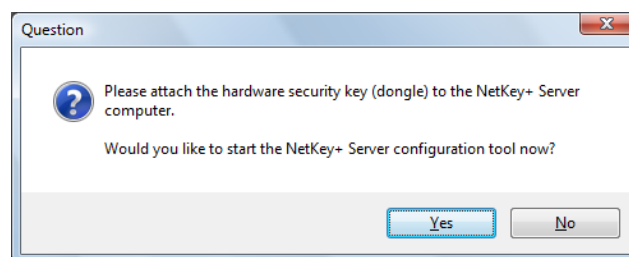


Figure 3.10: Launch the NetKey+ Configuration tool.

3.1.9 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 3.5).

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 3.11). 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 3.11: The *Welcome dialog box*.

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 3.12).

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 3.13). 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.

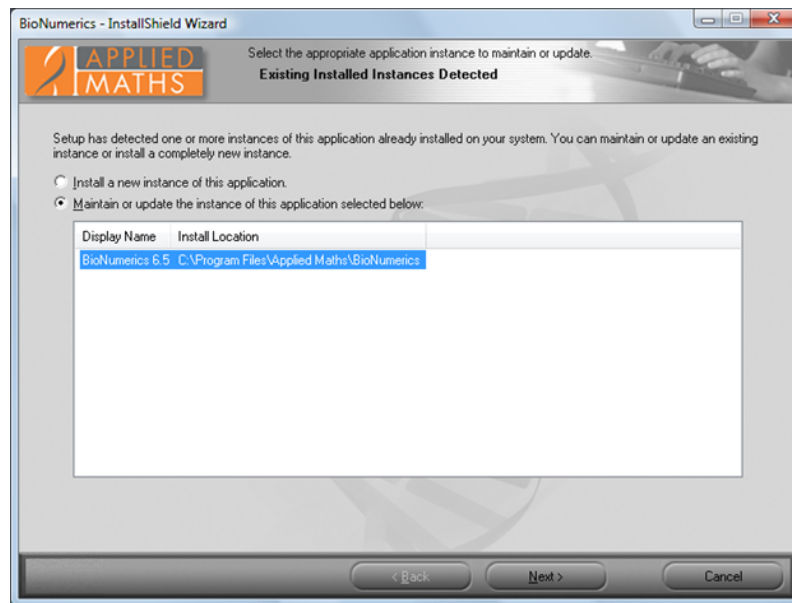


Figure 3.12: The *Existing Installed Instances Detected* dialog box.



Figure 3.13: 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 3.14). 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 6.1.0 to 6.5.0 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.

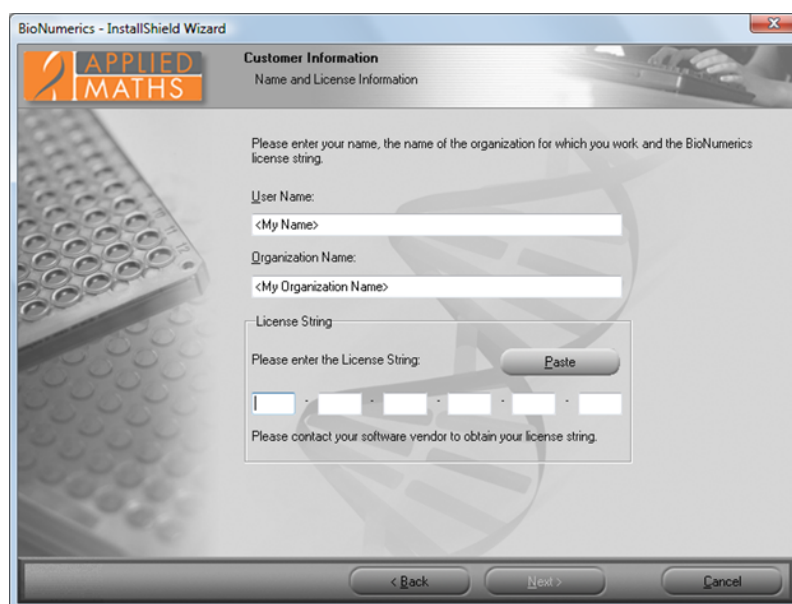


Figure 3.14: The *Customer Information* dialog box.

3.2.4 Choose destination location

The *Choose Destination Location* dialog box (see Figure 3.15) 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.

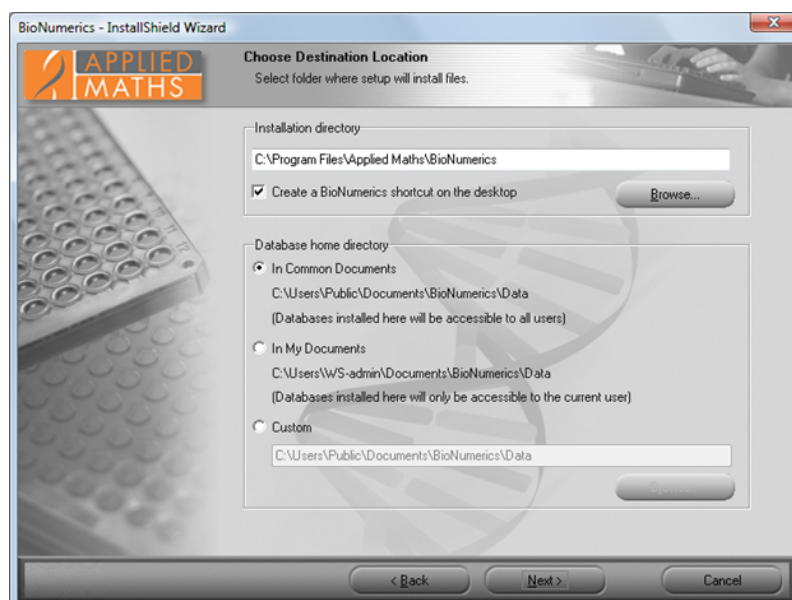


Figure 3.15: The *Choose Destination Location* dialog box.



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 3.16) 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.

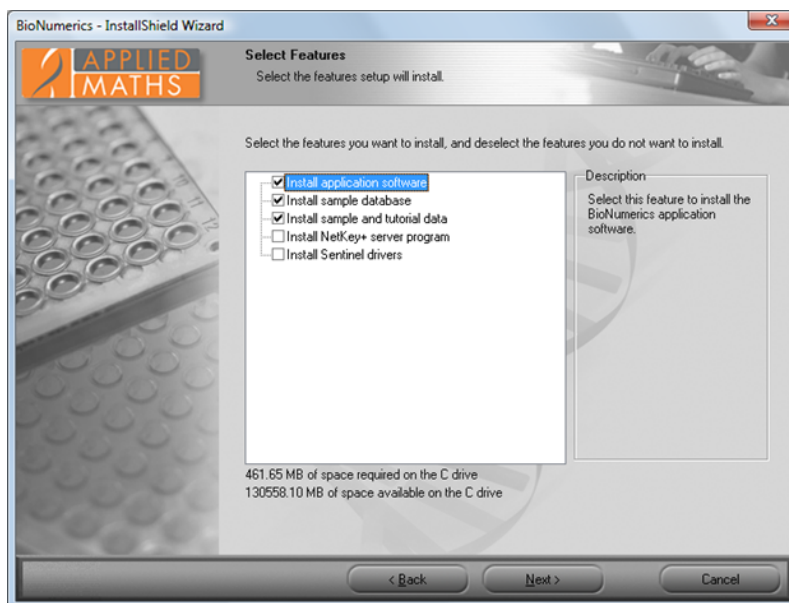


Figure 3.16: The *Select Features dialog box*.

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 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 Quick Guide and 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 3.15).

Install Sentinel drivers:

- 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. Since no USB dongle is needed to run an internet license, 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 where the hardware security key will be connected to.

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 3.14). 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 3.16) 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 3.17). Select **<No>** if you do not want to uninstall the BioNumerics application.

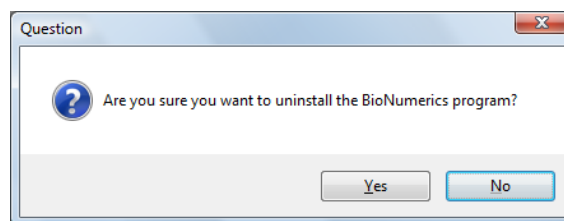


Figure 3.17: Warning message.

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 3.5), 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 *Server port number* connection parameters 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.

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.

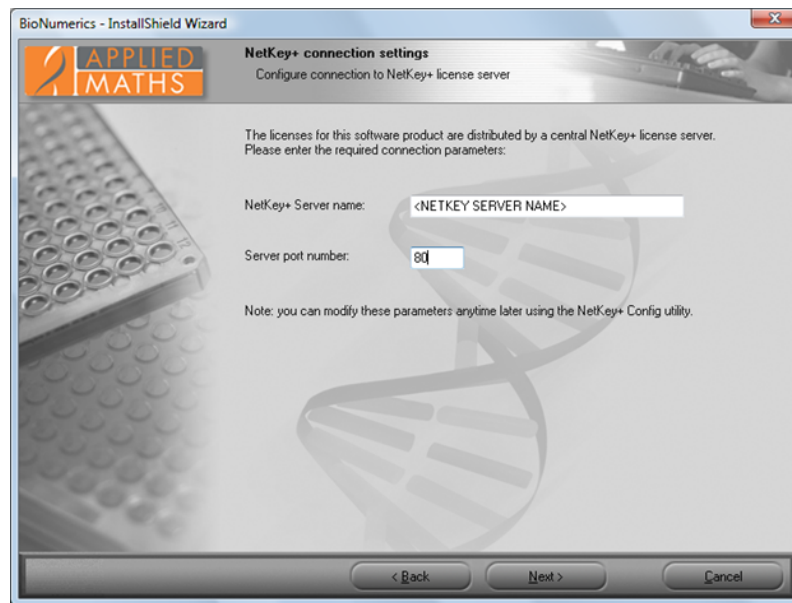


Figure 3.18: The *NetKey+ connection settings* dialog box.

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 3.19).

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.

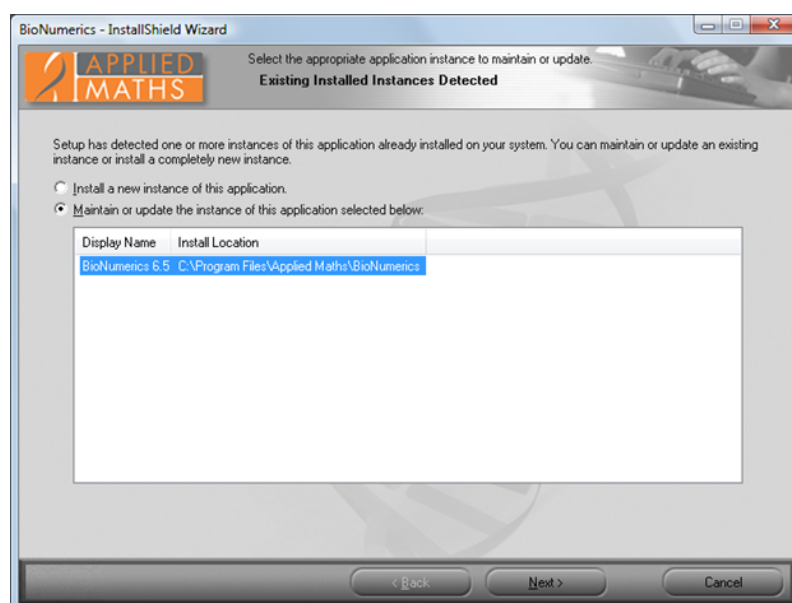


Figure 3.19: The *Existing Installed Instances Detected* dialog box.

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 3.20).

- **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).

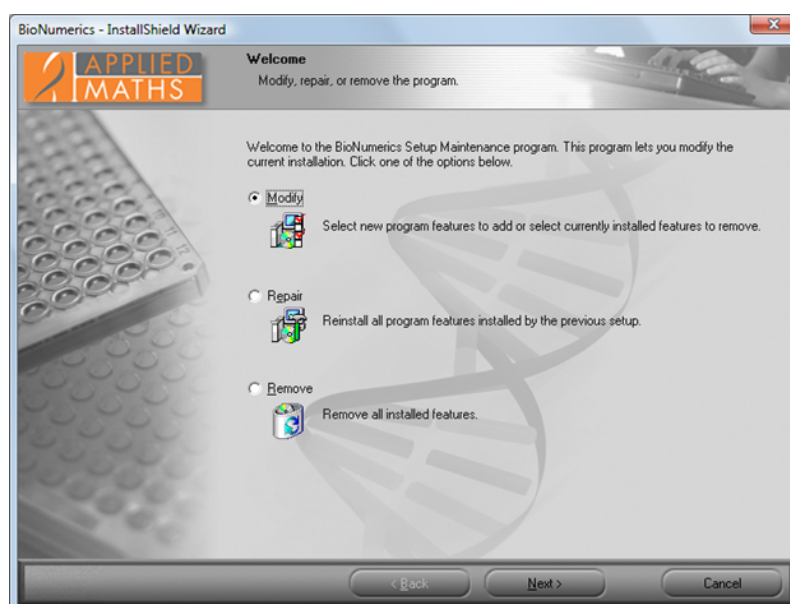


Figure 3.20: The *Welcome dialog box*.

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 3.20). 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.



The recommended method for uninstalling an instance of BioNumerics is to choose the *Remove* option in the *Welcome dialog box* (see Figure 3.20). 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 3.20) 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 Chapter 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 3.20) 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 3.21). Click <Yes> to start the deletion of the BioNumerics application. Select <No> to return to the previous *Welcome dialog box*.

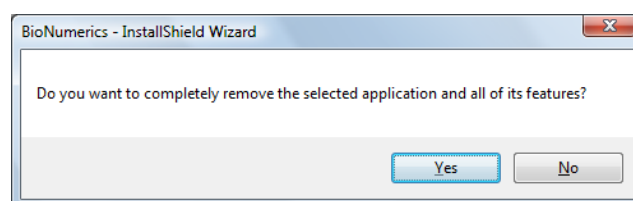


Figure 3.21: Confirm removal of selected features.



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 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.

The Setup log XML file is best viewed with a recent version of the Microsoft Internet Explorer browser (see Figure 3.22). 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 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

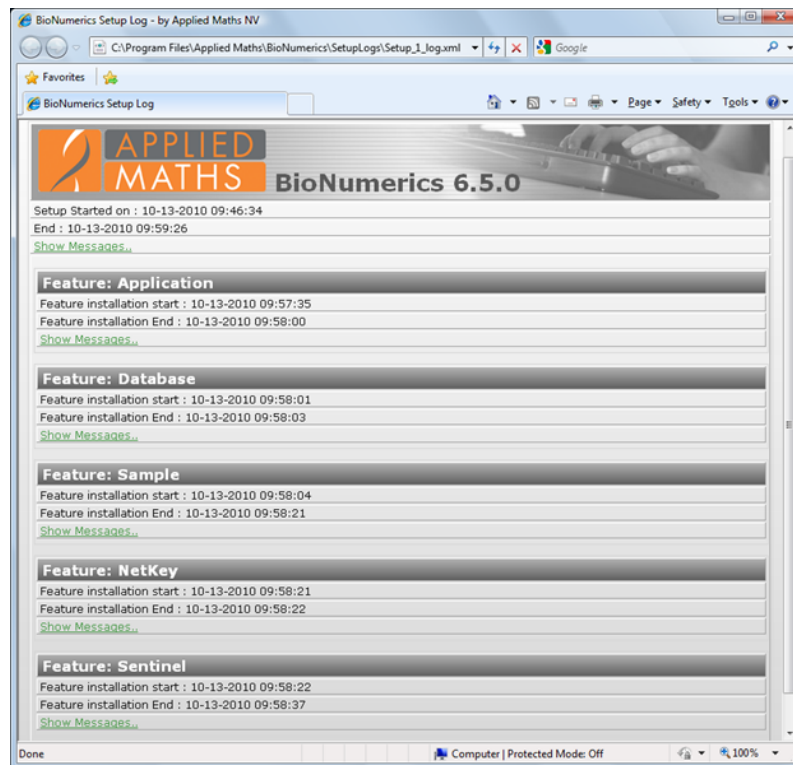


Figure 3.22: The BioNumerics setup log.

3.5 Silent installation

3.5.1 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.

3.5.2 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 3.1.9 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.

3.5.3 Setup INI XML file format

The information recorded in the `Setup_x_ini.XML` file has the format as displayed in Figure 3.23.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<setup name="\BnSoftwareName" version="6.5.0" date="2010-01-01"
time="00:00:00">
  <start date="1-1-2010" time="00:00:00"/>
  <feature display_name="Install application software">
    <property desktop_shortcut="1"/>
    <property NetKey_server="localhost"/>
    <property NetKey_server_port="2350"/>
    <property NetKey_config_port="2351"/>
    <property NetKey_refresh_rate="30"/>
  </feature>
  <property log_dir="C:\Program Files (x86)\Applied
Maths\BnSoftwareName\SetupLogs"/>
  <property install_dir="C:\Program Files (x86)\Applied
Maths\BnSoftwareName"/>
  <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="Install sample database"/>
  <feature display_name="Install sample and tutorial data"/>
  <feature display_name="Install NetKey+ server program"/>
</setup>
```

Figure 3.23: 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 Chapter 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.

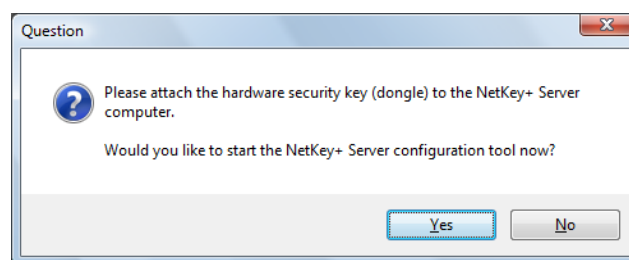



Figure 4.1: Run the NetKey+ Configuration tool.

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".

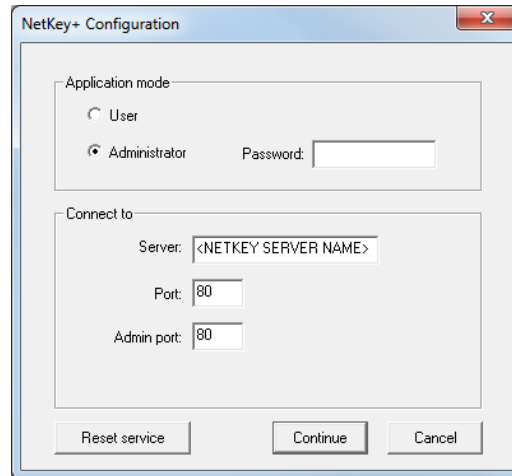


Figure 4.2: The *Login window*.

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 without the DNS domain 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.

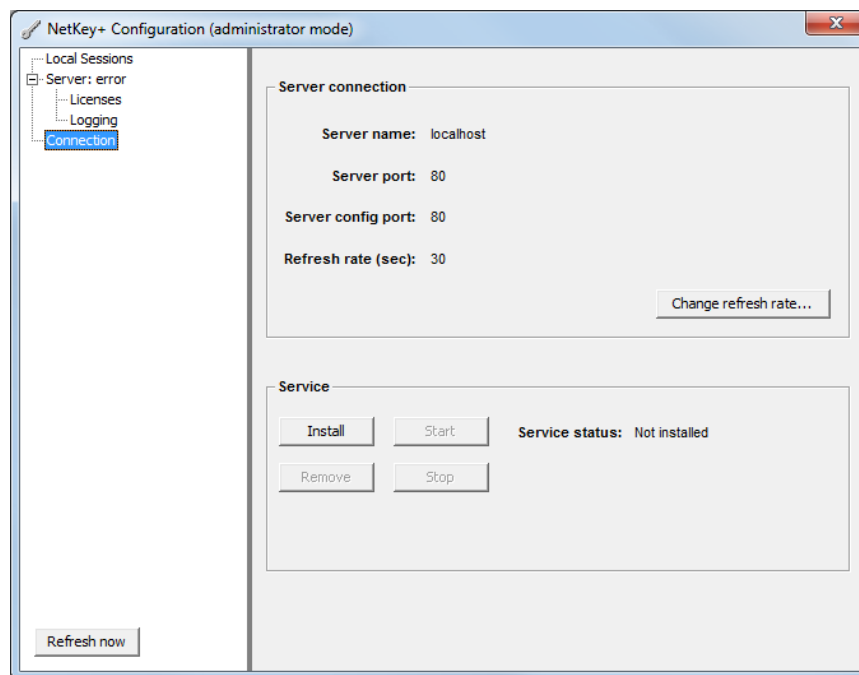


Figure 4.3: The *NetKey+ Configuration tool window*.

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.

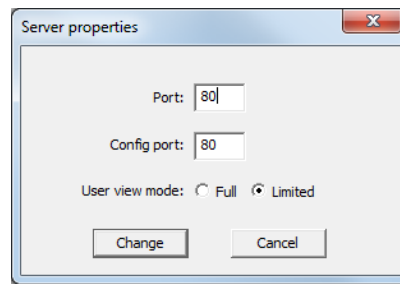


Figure 4.6: Edit the server properties.



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 (USB dongle) 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 **<Change>** button. The **<Remove>** button allows you to remove a string from the list of installed licenses.

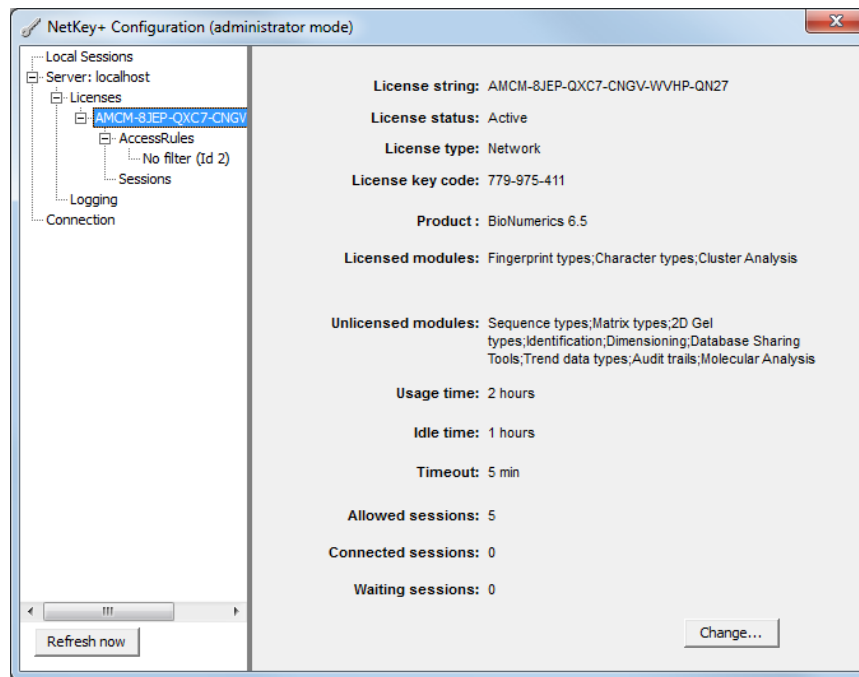


Figure 4.9: License settings.

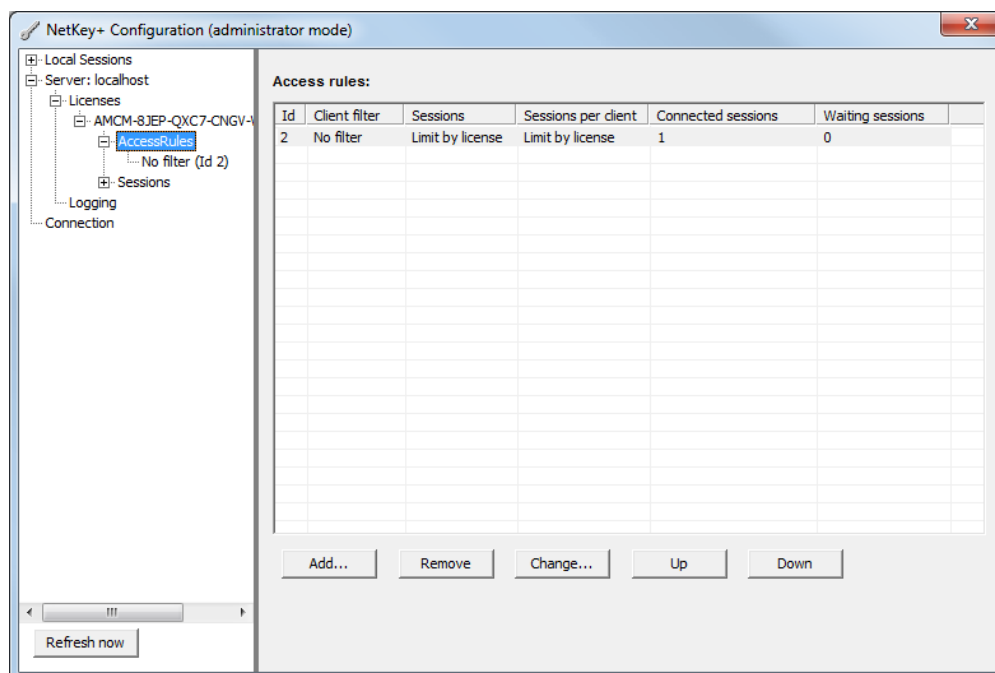


Figure 4.10: Access rules for a license.

- **Filter by ClientId:** Physical Address (MAC) of the client network adapter.
- **Filter by Computer Name:** TCP/IP Host name of the client computer (with or without domain name).
- **Filter by User Name:** Windows login name without domain name.
- **Filter by IP:** Single or a range of IP addresses of client computers.

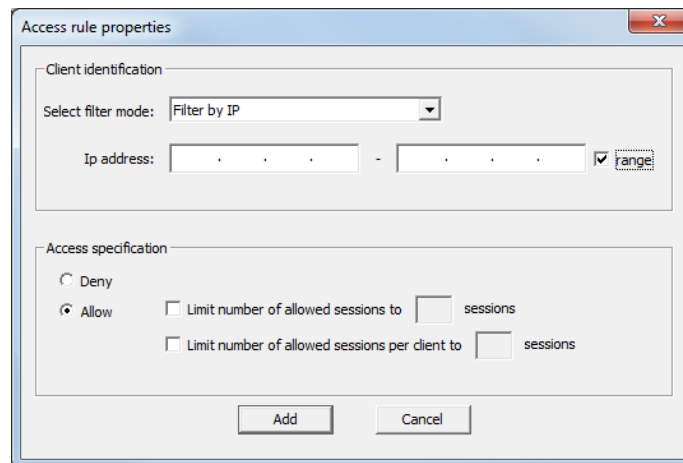


Figure 4.11: The *Access rule properties* dialog box.

A range of IP 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).

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 Chapter 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.

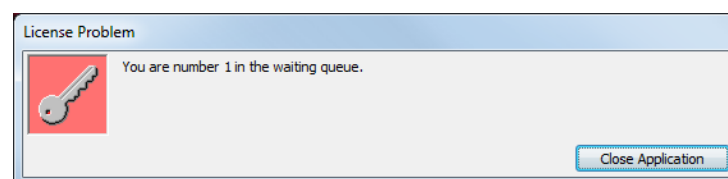


Figure 4.12: Waiting queue.

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 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.

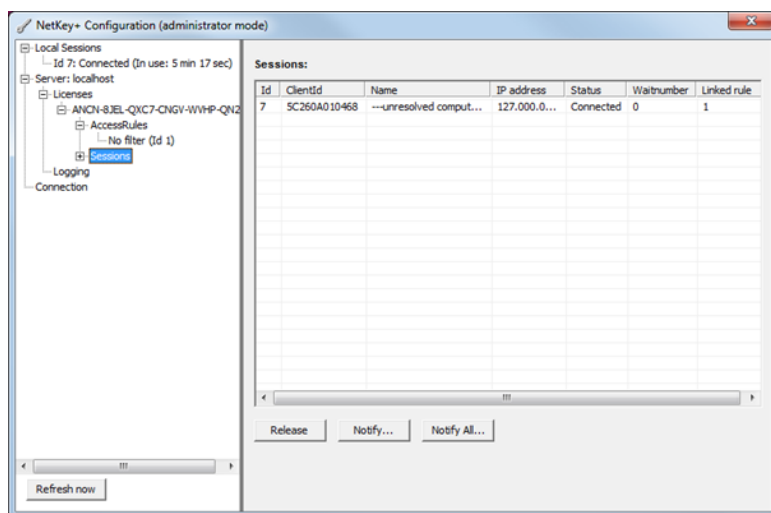


Figure 4.13: List of connected sessions and sessions that are present in the waiting queue.

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.

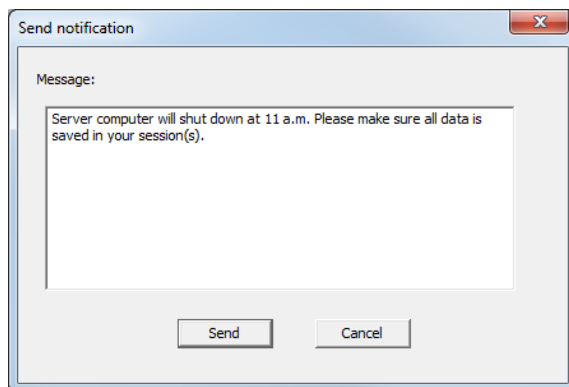


Figure 4.14: Notification message.

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 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 +

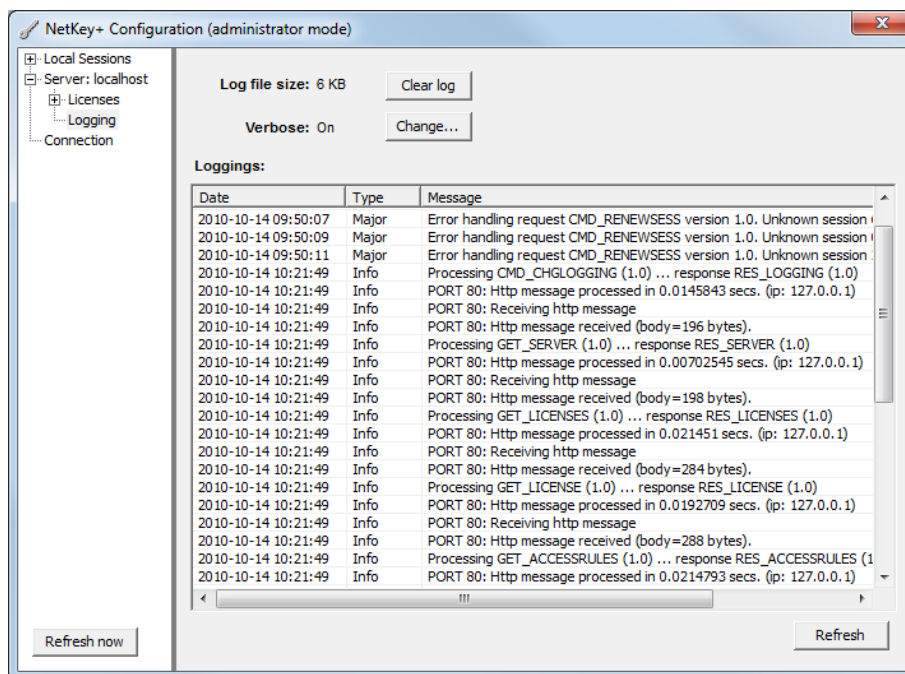


Figure 4.15: Logging information.

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:

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.

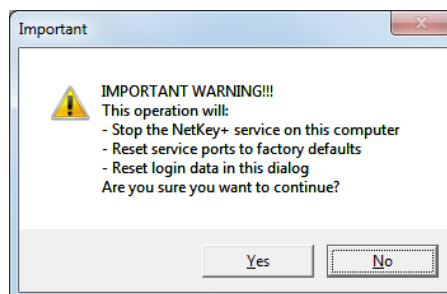


Figure 4.16: Warning message.

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.
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 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.

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

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

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		3.1.1
D2	Dlg_SdWelcome	Figure 3.1	3.1.1
D3	Dlg_Start / SdWelcomeMaint	Figure 3.20	3.3.2
D4	Dlg_SdLicense2		
D5	Dlg_SdSetLicense	Figure 3.5	3.1.3
D6	Dlg_SdPathOptions	Figure 3.6	3.1.4
D7	Dlg_SdFeatureTree	Figure 3.7	3.1.5
D8	Dlg_SdNetKey	Figure 3.9	3.1.6
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 [3.5](#) 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.

5.3.8.1 Application_Installing

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).

5.3.8.2 Application_Installed

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.

5.3.8.3 Application_UnInstalled

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.

5.3.8.4 Sentinel_Installed

The *Sentinel_Installed* event handler function is called by the Setup after the Sentinel drivers place holder 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).

5.3.8.5 NetKey_Installing

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.

5.3.8.6 NetKey_Installed

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.

5.3.8.7 NetKey_UnInstalling

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 then the program folder of the current BioNumerics instance then the service will not be stopped.

5.3.8.8 NetKey_UnInstalled

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 then the program folder of the current BioNumerics instance, then the service will not be removed.

5.3.8.9 Database_Installed

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.

5.3.8.10 DeleteOldFiles

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.

5.3.8.11 IsSentinelInstalled

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.

5.3.8.12 HasDongles

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.

5.3.8.13 CheckLicense

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.

5.3.8.14 LaunchNetKey

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.

5.3.8.15 IsOldNetKeyInstalled

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.

5.3.8.16 SetFilePermissions

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

5.3.8.17 MSI.InstallProduct

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

5.3.8.18 WMI_ServiceStop

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.

5.3.8.19 WMI_ServiceStart

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.

5.3.8.20 CleanUp

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).

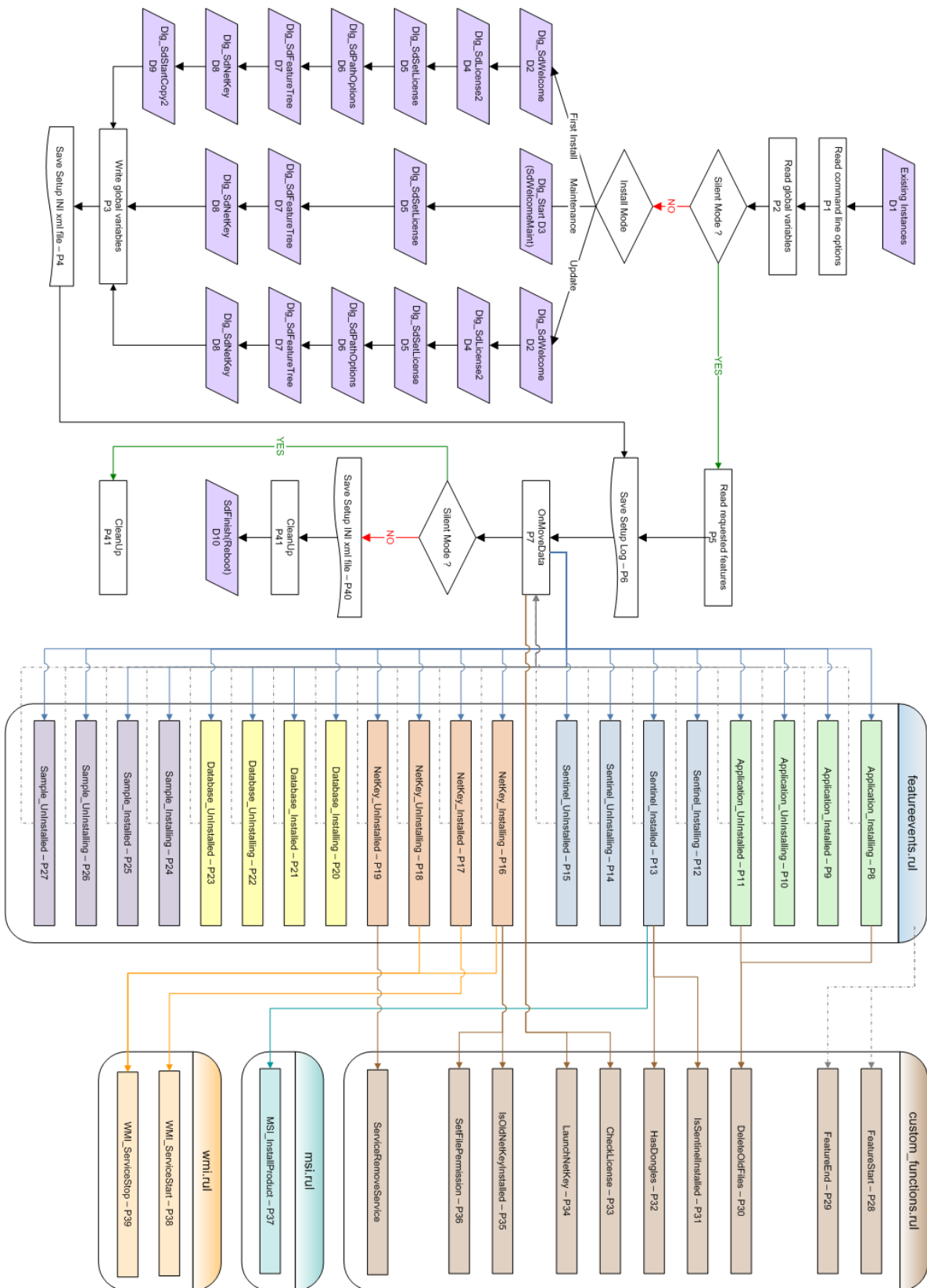


Figure 5.1: The Setup flow diagram.

Process Number	Process Name	Related Section Number
P1	Read command line options	5.3.1
P2	Read global variables	5.3.2
P3	Write global variables	5.3.3
P4	Save Setup INI xml file	5.3.4
P5	Read requested features	5.3.5
P6	Save Setup Log	5.3.6
P7	OnMoveData	5.3.7
P8	Application_Installing	5.3.8.1
P9	Application_Installed	5.3.8.2
P10	Application_UnInstalling	
P11	Application_UnInstalled	5.3.8.3
P12	Sentinel_Installing	
P13	Sentinel_Installed	5.3.8.4
P14	Sentinel_UnInstalling	
P15	Sentinel_UnInstalled	
P16	NetKey_Installing	5.3.8.5
P17	NetKey_Installed	5.3.8.6
P18	NetKey_UnInstalling	5.3.8.7
P19	NetKey_UnInstalled	5.3.8.8
P20	Database_Installing	
P21	Database_Installed	5.3.8.9
P22	Database_UnInstalling	
P23	Database_UnInstalled	
P24	Sample_Installing	
P25	Sample_Installed	
P26	Sample_UnInstalling	
P27	Sample_UnInstalled	
P28	FeatureStart	
P29	FeatureEnd	
P30	DeleteOldFiles	5.3.8.10
P31	IsSentinelInstalled	5.3.8.11
P32	HasDongles	5.3.8.12
P33	CheckLicense	5.3.8.13
P34	LaunchNetKey	5.3.8.14
P35	IsOldNetKeyInstalled	5.3.8.15
P36	SetFilePermissions	5.3.8.16
P37	MSI_InstallProduct	5.3.8.17
P38	WMI_ServiceStart	5.3.8.19
P39	WMI_ServiceStop	5.3.8.18
P40	Save Setup INI xml file	5.3.4
P41	CleanUp	5.3.8.20

Table 5.2: The Setup process list.

Index

- Anti-Virus software, [7](#)
- Database home directory, [11](#), [17](#)
- EULA, [10](#), [16](#)
- Firewall, [7](#)
- Hardware requirements, [5–6](#)
- Idle time, [36](#)
- Installation, [9–26](#)
 - Maintenance, [20–24](#)
 - Modify, [22](#)
 - New instance, [9–15](#)
 - Remove, [23](#)
 - Repair, [23](#)
 - Silent, [24–26](#)
 - Update instance, [15–20](#)
- Installation directory, [11](#), [17](#)
- License string, [11](#), [13](#), [16](#)
- NetKey+, [29–41](#)
 - Access rules, [34](#)
 - Admin port number, [30](#)
 - Configure license(s), [33–37](#)
 - Install NetKey+ service, [31](#)
 - Login window, [30](#)
 - Port number, [30](#)
 - Release session, [38](#)
 - Repair, [40–41](#)
 - Reset, [40](#)
 - Send message, [38](#)
 - Server name, [30](#)
 - Start NetKey+ service, [31](#)
 - Waiting queue, [37](#)
- NetKey+Config.txt file, [31](#)
- NetKey.ini file, [14](#), [32](#)
- Operating system, [6](#)
- Proxy server, [7](#)
- Setup INI XML file, [15](#)
- Setup log XML file, [24](#)
- Timeout, [37](#)
- Usage time, [36](#)
- Windows operating system, [6](#)