



ChromLab Software Security Edition

User Guide
Version 6.1



ChromLab Software, Security Edition

User Guide

Version 6.1



Bio-Rad Technical Support Department

The Bio-Rad Technical Support department in the U.S. is open Monday through Friday, 5:00 AM to 5:00 PM, Pacific time.

Phone: 1-800-424-6723, option 2

Email: Support@bio-rad.com (U.S./Canada Only)

For technical assistance outside the U.S. and Canada, contact your local technical support office or click the Contact us link at www.bio-rad.com.

Notice

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage or retrieval system, without permission in writing from Bio-Rad.

Bio-Rad reserves the right to modify its products and services at any time. This guide is subject to change without notice. Although prepared to ensure accuracy, Bio-Rad assumes no liability for errors or omissions, or for any damage resulting from the application or use of this information.

BIO-RAD is a trademark of Bio-Rad Laboratories, Inc.

All trademarks used herein are the property of their respective owner.

Copyright © 2020 by Bio-Rad Laboratories, Inc. All rights reserved.

Table of Contents

Chapter 1 Introduction	7
U.S. FDA 21 CFR Part 11 Compliance	7
Finding Out More	8
Chapter 2 Preparing to Share the ChromLab Database	9
Preparing Your Site	12
Site Requirements	12
System Requirements	13
Chapter 3 Preparing the Central Computer and NGC Systems	15
Preparing the Central Computer and NGC Systems	16
Backing Up and Restoring ChromLab Data to the Central Computer	17
Setting a Static IP Address on Each NGC System	20
Verifying Each NGC System Name Is Unique	22
Verifying that All NGC Systems Can Reach the Central Computer	23
Chapter 4 Activating Security Edition on the Central Computer	25
Creating an NGC Database Backup Folder	26
Changing the ChromLab Default Password	27
Activating Security Edition on the Central Computer	29
Next Steps	33
Creating Users	33
Uninstalling ChromLab Software on the Central Computer	33

Chapter 5 Connecting Remote Computers to the Central Computer	35
Locating the Date and Time Settings on ChromLab Computers	36
Creating an NGC Database Backup Folder	37
Exporting Existing ChromLab Data	38
Changing the ChromLab Default Password	39
Activating ChromLab Software Security Edition on Remote Computers	41
Importing Existing ChromLab Data	44
Rules for Sharing ChromLab Data	46
Chapter 6 The Security Edition Workspace	51
ChromLab Administration	52
Menu Commands	52
The Security Edition Home Window	54
Security Edition Menu Commands	55
Home Window	55
System Control Window	55
Method Editor Window	55
Evaluation Window	55
Chapter 7 Using ChromLab Software Security Edition	57
Electronic Records	57
Uncontrolled Data Files	57
Controlled Data Files	58
Signed Data Files	58
Identifying Data File Status	59
Signing Data Files	59
Importing Electronic Data Files	62
Exporting Electronic Data Files	62
Backing Up and Restoring the Security Edition Database	63

Audit Logs	64
General Audit Log	65
Run Audit Log	66
Analysis Audit Log	67
Viewing Audit Logs	68
Signed Reports	72
Signed Method Reports	72
Signed Run Reports	73
Signed Analysis Reports	74
Appendix 8 Connecting Multiple ChromLab Computers to One NGC System	75
Rules for Managing Access to NGC Systems	75
Taking Control of an NGC System	76
Chapter 9 Setting Up ChromLab Users and Roles	77
Users and Roles	77
Reviewer Attribute	78
Role Permissions	78
Managing ChromLab User Accounts	87
Adding User Accounts	87
Editing a User Account	90
Deleting a User Account	92
Setting Password Options in Security Edition	93
Setting Password Options	93
Starting ChromLab Software Security Edition	95
Appendix A Troubleshooting Shared Database Connection Issues	97
Possible Causes for Shared Database Connection Issues	97
Solutions for Shared Database Connection Issues	100

Table of Contents

Changing the Location Parameters of Shared Database	100
Restarting the NGC Database Service	101
Uninstalling Microsoft SQL Server on the Central ChromLab Computer	102
Changing the Connection Parameters to the Central Computer	104
Manually Adding Inbound Firewall Rules	105
Appendix B Configuration Checklists	107
Preparing Your Site	107
Setting Up the Shared Environment	109

Chapter 1 Introduction

U.S. FDA 21 CFR Part 11 Compliance

ChromLab software, Security Edition enables ChromLab users to meet the Food and Drug Administration's regulations on good laboratory practices in the pharmaceutical and biotechnology industries.

When enabled, Security Edition provides the necessary features to permit ChromLab to operate in compliance with Title 21 of the U.S. Code of Federal Regulations Part 11 (21 CFR Part 11) within a *closed system*. A closed system is defined as "an environment in which system access is controlled by the persons who are responsible for the content of electronic records that are on the system" (Section 11.3 (b) (4)).

Note:

- The security controls built into ChromLab must be properly configured and administered by the ChromLab administrator(s) in your organization in order to be secure and in compliance with 21 CFR Part 11.
- Bio-Rad makes no claim that ChromLab software, Security Edition is CFR-compliant in and of itself, nor does the company guarantee compliance for the user. Your organization must establish policies and standard operating procedures that work in conjunction with the tools provided by Bio-Rad to ensure compliance with 21 CFR Part 11.

Finding Out More

After you install NGC Chromatography Systems and ChromLab Software documentation from the NGC Chromatography Systems Software USB drive, you can access installed NGC guides and tutorials on the Help menu in any ChromLab view.

More information about the NGC chromatography systems and ChromLab software is available from the following sources.

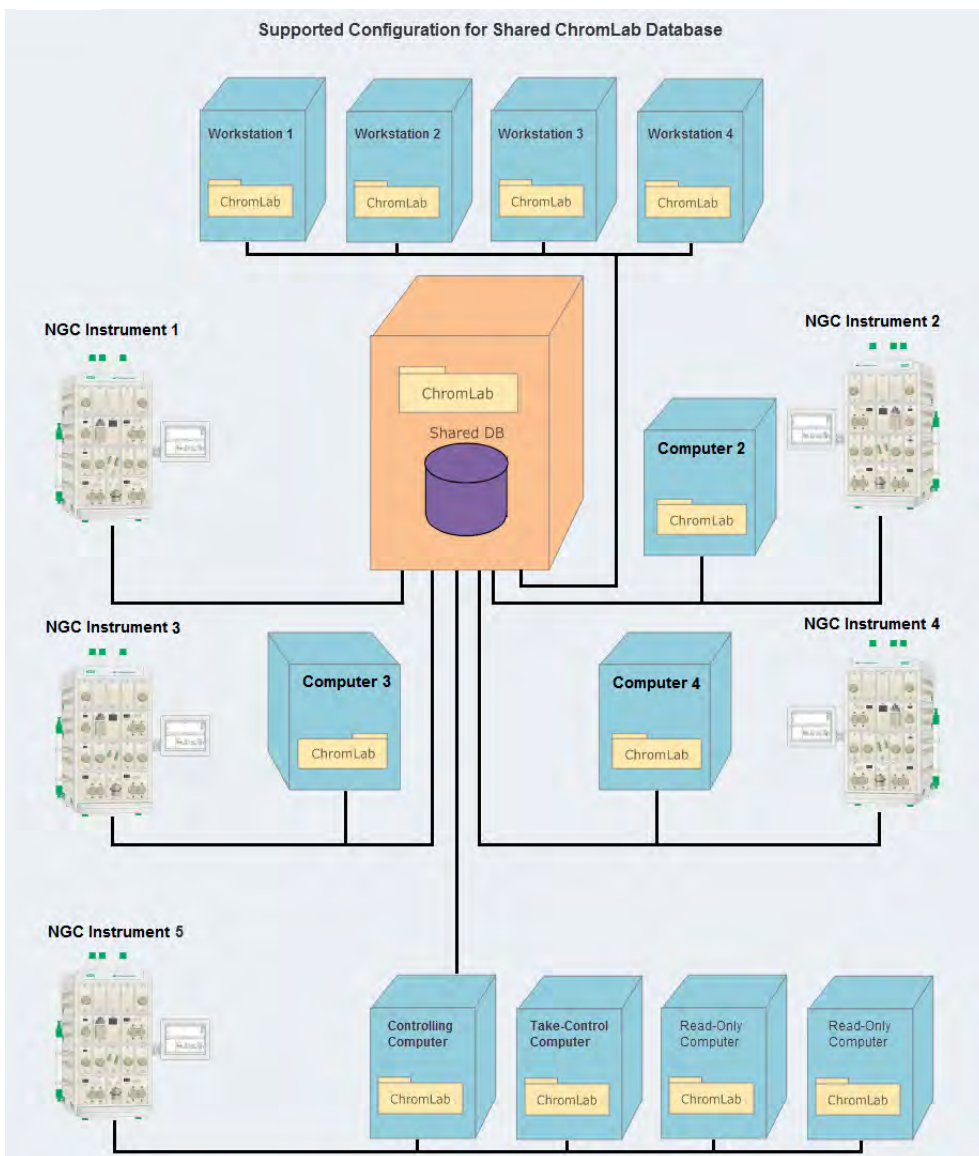
- The NGC Chromatography Systems and ChromLab Software Installation Guide is available on the NGC Chromatography Systems Software USB drive. This document explains how to set up your environment, set up and install the NGC instrument in the lab, and install ChromLab software and connect ChromLab to the NGC system.
- The NGC Chromatography Systems and ChromLab Software Instrument Guide is available on the NGC Chromatography Systems Software USB drive. This document details the modules that comprise the NGC instrument and includes information about priming, plumbing, troubleshooting, and maintaining the NGC system.
- The NGC Chromatography Systems and ChromLab Software User Guide is available on the NGC Chromatography Systems Software USB drive. This document explains how to use ChromLab software to control the NGC instrument, run protein separations and other operations manually, program methods to automate purification runs, evaluate the results, and print experiment reports.

Note: Click the Bio-Rad logo in the upper right corner of any ChromLab window to launch the Bio-Rad website.

Chapter 2 Preparing to Share the ChromLab Database

You can install ChromLab software on a central computer on your local network and share data among multiple users, ChromLab computers, and NGC systems.

The following diagram illustrates supported shared ChromLab database configurations.



In the shared environment, one installation of ChromLab software is designated as the host of the shared database. The shared database can serve any of the following configurations.

- **Multiple ChromLab workstations**

A ChromLab workstation has ChromLab Software, Security Edition installed but is not connected to an NGC system. From this computer you can create methods and save them to the shared database. You can also access, view, and edit ChromLab data files that are saved on the shared database.

- **One NGC system connected to the central ChromLab computer**

Data from the connected NGC system are saved to the shared database and are accessible to users from any computer running ChromLab software.

- **Multiple ChromLab computers and NGC systems**

Computers running ChromLab software (known in this document as ChromLab computers) and the NGC systems can access and use the shared database. Each ChromLab computer can connect to any available NGC system on the network, operate it, and save data to the shared database. Data from the NGC systems are also saved to the shared database.

- **Multiple ChromLab computers connected to one NGC system**

Multiple ChromLab computers can simultaneously connect to the same NGC system. A user assigned the Advanced User role can log into any computer and take control of the system. This is useful in the event that the controlling computer is locked or the user performing a run is not available and there is an immediate need to stop the instrument. In this environment, only one ChromLab computer can control an NGC system at a time. All other NGC computers have View access to the system.

Note: Any user can take control of the NGC system using the system's touch screen. The touch screen is never in View mode.

Important: Preventing unauthorized users from accessing the NGC system's touch screen is the responsibility of the customer.

Preparing Your Site

Note: You can upgrade ChromLab software standard or Security Edition from version 3.x or higher to version 6.1. If you are running an earlier version of ChromLab software, you must first upgrade to one of these versions before you can upgrade to ChromLab 6.1.

Preparing your site to share a ChromLab database requires the following tasks:

1. Verify the site requirements for the central computer.
See the next section, [Site Requirements](#).
2. Verify that the central computer meets the hardware and software requirements.
See [System Requirements on page 13](#).
3. Install or upgrade ChromLab software on the central and remote computers.

For detailed instructions about installing or upgrading ChromLab software and connecting to the NGC system, see the NGC Chromatography Systems and ChromLab Software Installation Guide.

Site Requirements

The room and power requirements for installing NGC systems and ChromLab software in a shared database environment are the same as those for local installations.

Note: Ensure that the network hosting the ChromLab computers and NGC systems supports Internet Protocol version 4 (IPv4).

For specific information, see the chapter Preparing the ChromLab Computer in the NGC Chromatography Systems and ChromLab Software Installation Guide.

System Requirements

The system requirements for the central ChromLab computer or server are very similar to those for the local and remote installation of ChromLab with the differences bolded in this table.

Table 1. Minimum system requirements for a shared ChromLab database

Hardware and Software	Minimum Requirement
Operating system	One of the following: <ul style="list-style-type: none"> ■ Microsoft Windows 7 SP1 Pro (64-bit only) ■ Microsoft Windows 10 Pro (64-bit only) ■ Microsoft Windows 10 Enterprise (64-bit only) ■ Microsoft Windows Server 2008 R2 SP1 ■ Microsoft Windows Server 2012 R2 ■ Microsoft Windows Server 2016
Processor	Intel Pentium IV with EM64T support or equivalent, 3.0 GHz minimum
RAM	8 GB
Hard disk space	500 GB minimum Note: ChromLab installs Microsoft SQL Server 2014 Express. This application requires 6 GB of disk space.
File system	NTFS (New Technology File System)
Optional peripherals (Required only if an NGC system is connected to the central computer.)	USB 3.0 high speed ports (2 minimum) Mouse Keyboard 2 gigabit ethernet port (1 minimum)

Table 1. Minimum system requirements for a shared ChromLab database, continued

Hardware and Software	Minimum Requirement
<p>Important: Do not install Security Edition on a Windows Server computer that you plan to upgrade to, or that has, a newer version of Microsoft SQL Server installed.</p>	

Chapter 3 Preparing the Central Computer and NGC Systems

To ensure that the NGC systems can successfully connect to the central ChromLab computer, they all must have access to the subnet on which the central computer resides.

Important: If an NGC system is connected by an ethernet communication cable to a ChromLab computer that is not the central computer, disconnect the cable from the ChromLab computer and connect the NGC system to the network. See the NGC Chromatography Systems and ChromLab Software Installation Guide for information about connecting your NGC system to the network. Ensure the network can access the subnet on which the central computer resides.

Before setting up the shared database, determine which computer will host the shared database. Choose a clean computer (one that does not have an existing installation of ChromLab) to host the shared database.

Notes:

- Bio-Rad strongly suggests that you host the shared database on a dedicated computer or server that is regularly backed up.
- Ensure that all remote computers and NGC systems have access to that computer.
- If installing on a Windows Server computer, ensure that it is dedicated to the ChromLab installation. ChromLab requires and installs Microsoft SQL Server 2014 and is not supported on any other version of this software.

Preparing the Central Computer and NGC Systems

Preparing the central computer and the NGC systems requires the following tasks. This chapter explains these tasks in detail.

1. Install ChromLab software on the central computer and all remote computers and NGC systems.

See [NGC Chromatography Systems and ChromLab Software Installation Guide](#).

2. Verify that all NGC systems and remote ChromLab computers can access the subnet on which the central ChromLab computer will reside.

See your system or network administrator for information about subnets and setup.

3. Assign a static IP address to the central ChromLab computer.

See your system administrator for information about assigning a static IP address to the central computer.

4. Verify or assign a unique system name to each NGC system.

See [Verifying Each NGC System Name Is Unique on page 22](#).

5. Verify or assign a static IP address to each NGC system.

See [Setting a Static IP Address on Each NGC System on page 20](#).

6. Verify that the central computer can access each NGC system.

See [Verifying that All NGC Systems Can Reach the Central Computer on page 23](#).

Backing Up and Restoring ChromLab Data to the Central Computer

Bio-Rad recommends that you activate ChromLab Software, User Management Edition on a clean computer (one that does not have ChromLab installed). After you install ChromLab software on the clean computer and upgrade your existing ChromLab databases to version 6.1, use ChromLab Administration to back up your largest database and restore it onto the central computer. You can also use ChromLab Administration to set a reminder to back up the NGC database on a daily, weekly, or monthly basis.

Important: Restoring backup data overwrites existing ChromLab data. Perform this task only once, and carefully select the database to back up and restore.

Backing Up ChromLab Data on the Remote Computer

Perform the backup procedure on the remote ChromLab computer.

To back up a ChromLab database

1. Verify that you have upgraded ChromLab to version 6.1.
2. On the remote computer, determine the size of the NGC database.
 - a. Navigate to C:\ProgramData\Bio-Rad\NGC\Database.
 - b. Right-click on the Database folder and select Properties.
 - c. On the General tab, note the Size value.

Ensure that the disk on which you plan to save the backup zip file has free disk space that is at least equal to the size of the NGC database.

3. On the Start menu, select ChromLab > ChromLab Administration and log into ChromLab Administration.
4. In ChromLab Administration, select the Backup and Restore tab.

5. In the Backup section, click Browse to browse to a location into which to save the NGC backup (.sbk) file.

Note: Ensure that the central computer can access the target location.

6. Click Backup.

ChromLab displays a status bar of the backup progress. Depending on the size of your database, the backup can take some time.

7. When the backup completes, close ChromLab Administration.

Setting a Backup Reminder on the Remote Computer

You can set a reminder to back up the central database. The reminder appears on the ChromLab computer at the time interval you set. From the ChromLab Administration Backup Reminder dialog box, you can open ChromLab Administration and perform the backup.

Alternatively, you can close the reminder dialog box and perform the backup at another time.

To set a reminder to back up the central database

1. Open ChromLab Administration and select the Backup and Restore tab.
2. In the Backup Reminder section, verify the Set Reminder checkbox is selected.
3. Use the up and down arrows to set the numeric interval for the reminder and select either Daily, Weekly, or Monthly from the dropdown list.
4. Click Apply.

To stop receiving reminders to back up the database

- ▶ In the Backup Reminder section, clear the Set Reminder checkbox and click Apply.

Restoring ChromLab Data to the Central Computer

Important: Restoring backup data overwrites existing ChromLab data. Ensure the central computer does not have existing ChromLab data.

Perform this task on the central ChromLab computer. Ensure the computer has free disk space that is at least equal to the size of the backup file.

To restore ChromLab data to the central ChromLab computer

1. Verify that you have installed ChromLab 6.1 on the central computer.
2. On the Start menu, select ChromLab > ChromLab Administration.
3. In the Restore section, click Browse to browse to the location where you saved the NGC backup (.bak) file.
4. Click Restore.

ChromLab displays a status bar of the restore progress. Depending on the size of your database, the restore can take some time.

5. When the restore completes, close ChromLab Administration.

Setting a Static IP Address on Each NGC System

Note: Bio-Rad strongly recommends that you set a static IP address on each NGC system that connects to the central computer. Alternatively, you can record and use its system name to verify its connection to the central computer.

Important: The NGC system must restart to apply the IP address changes.

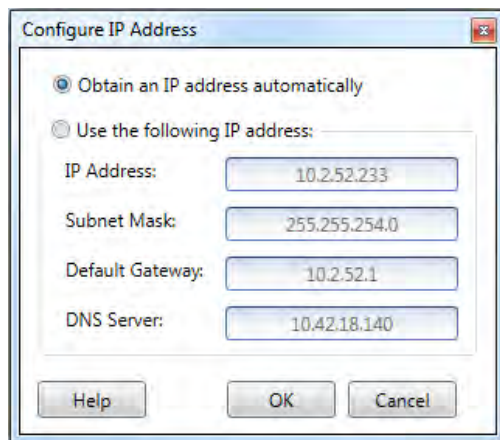
To set a static IP address on the NGC system

1. On the instrument touch screen, select System Information on the dropdown menu.

The System Information dialog box appears.

2. In the General tab, click Configure beside System IP Address.

The Configure IP Address dialog box appears.



3. In the Configure IP Address dialog box, select Use the following IP address and provide the IP address, subnet mask, default gateway, and DNS server information specific to your site.

Tip: See your system or network administrator for the appropriate IP settings.

- IP address — the specific numeric address for the NGC system.
 - Subnet mask — the numeric filter used to define the subnet to which the IP address belongs.
 - Default gateway — (required only if you plan to install the shared ChromLab database on a separate subnet or access the NGC system from ChromLab computers that are on another subnet) this is the IP address of the node that allows communication between the subnets.
 - DNS Server — the IP address of the node that translates a server name to its IP address.
4. Click OK.

A message appears explaining that the NGC system must restart.

5. Click Yes to save the changes and restart the system.

The NGC system shuts down and restarts.

6. To verify that the IP address changed successfully, open the System Information dialog box from the dropdown menu and view System IP Address in the General tab.

Verifying Each NGC System Name Is Unique

Each NGC system that connects to the central ChromLab computer must have a unique system name. Locate the NGC system's name and, if necessary, change the name so that it is unique.

To locate the NGC system name

1. On the instrument touch screen, select System Information on the dropdown menu.
The System Information dialog box appears displaying the General tab.
2. Locate and record the system name and system IP address information in the General tab.
3. Close the System Information dialog box.
If two or more NGC systems have the same name, you must change one name so that each is unique.

To change the NGC system name

1. On the instrument touch screen, select System Settings on the dropdown menu.
The System Settings dialog box appears.
2. Select the System Name tab.
3. On the System Name tab, type a new name for the system and click OK to save the change and close the System Settings dialog box.
4. To verify that the name changed successfully, open the System Information dialog box from the dropdown menu and view System Name in the General tab.

Verifying that All NGC Systems Can Reach the Central Computer

To verify that all NGC systems can reach the central computer

1. On the central ChromLab computer, open a command prompt window.
2. At the prompt, type

```
> ping <NGC_IP_address>
```

If the NGC system can reach the central computer, a response similar to the following appears:

```
Pinging <NGC_system_name>
```

```
Reply from <data from local IP Address> time<1ms
```

3. Perform [Step 2](#) for each NGC system and remote computer you plan to connect to the central computer.
4. Exit the command prompt window.

Important: If you experience a problem accessing an NGC system from the central computer, contact your system or network administrator and verify the network configuration, routing, firewall, and antivirus settings are correct. See [Appendix A, Troubleshooting Shared Database Connection Issues](#) for more information.

Chapter 4 Activating Security Edition on the Central Computer

When ChromLab is installed, by default it is set to run in standard mode (that is, only the local database is available). It continues to run in this mode until a user with ChromLab Administrator privileges activates ChromLab Software, Security Edition.

The workflow for activating Security Edition on the central computer consists of the following tasks. This chapter explains these tasks in detail.

1. Create an NGC database backup folder on the central computer.
See [Creating an NGC Database Backup Folder on page 37](#).
2. Change the default admin password in ChromLab Administration.
See [Changing the ChromLab Default Password on page 39](#).
3. Activate Security Edition on the central computer.
See [Activating Security Edition on the Central Computer on page 29](#).
4. Create ChromLab users on the central computer and assign access levels to NGC systems.
See [Next Steps on page 33](#).

Important: In order to use ChromLab after Security Edition has been activated on the remote computers, users must log in to the shared database. This requires each user to have a valid user name and password. You must create users after you activate Security Edition on the central computer. For more information, see [Chapter 9, Setting Up ChromLab Users and Roles](#).

Creating an NGC Database Backup Folder

ChromLab automatically backs up the existing NGC database when you activate Security Edition. If you have not previously backed up your NGC database, consider creating the database backup folder at this time.

Note: Even if you are installing ChromLab for the first time, the system backs up the empty NGC database. A new, empty NGC database requires approximately 75 MB of free disk space.

Perform this task on all computers on which you plan to activate Security Edition.

To create the NGC database backup folder

1. Determine the size of the NGC database.
 - a. Navigate to C:\ProgramData\Bio-Rad\NGC\Database.
 - b. Right-click the Database folder and select Properties.
 - c. On the General tab, note the Size value.

Ensure that the disk on which you plan to save the backup zip file (the target disk) has free disk space that is at least equal to the size of the NGC database.

2. On the backup computer, right-click the target folder and select New > Folder.
3. Rename the new folder, for example, NGC Database Backup.

Changing the ChromLab Default Password

You activate Security Edition through the ChromLab Administration tool. The first time you launch ChromLab Administration on each computer you must change the default admin password before continuing.

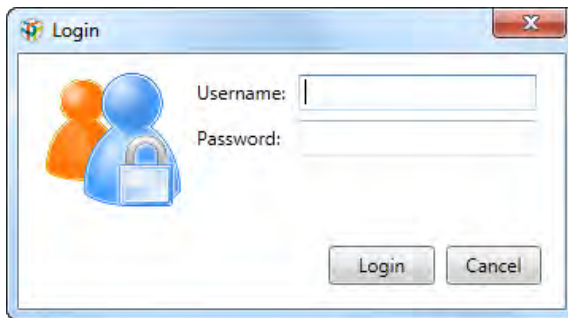
Note: You cannot activate Security Edition while either ChromLab software or the NGC system is in use. Close ChromLab and shut down the system before launching ChromLab Administration.

Important: You will perform this task on each remote ChromLab computer as well as the central ChromLab computer. Ensure that the Administrator password for each ChromLab computer is unique. Keep the Administrator passwords for all ChromLab computers in a secure place.

To change the default admin password

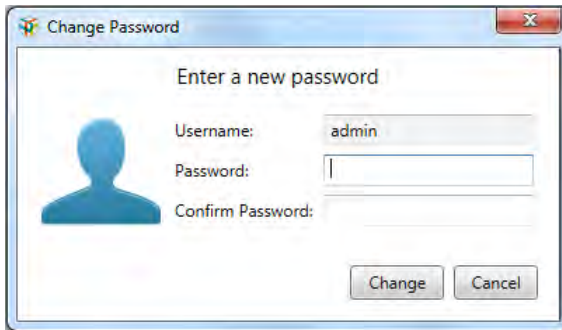
1. On the Start menu, select ChromLab > ChromLab Administration.

The Login dialog box appears.



2. Type the word admin for both the user name and password and click Login.

The Change Password dialog box appears.



3. Type a new password for the ChromLab administrator in the Password field, type it again in the Confirm Password field, and click Change.

Activating Security Edition on the Central Computer

Note: You cannot activate Security Edition while either ChromLab or the NGC system are in use. Close ChromLab and shut down the system before launching ChromLab Administration.

Activating Security Edition requires a license key. This key is located on the back of your Security Edition installation package.

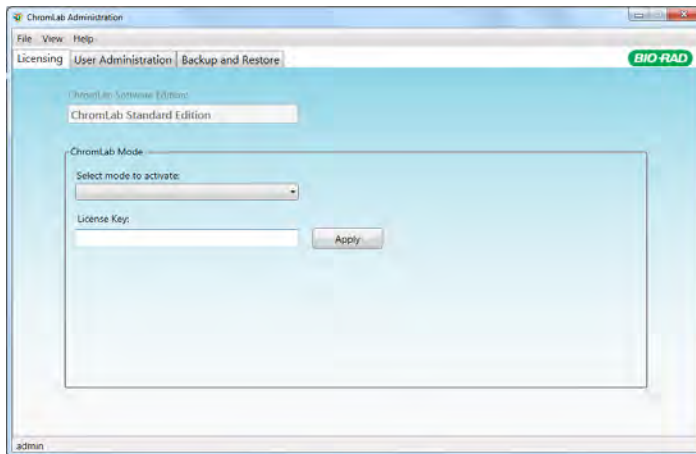
When you activate Security Edition, the system prompts you to select a database location. This section explains how to activate Security Edition on the central computer and designate its database as the shared database.

Important: ChromLab automatically backs up the current NGC database, creates an empty database, and then activates Security Edition. Depending on the size of your current NGC database, this process can take some time.

To activate Security Edition on the central computer

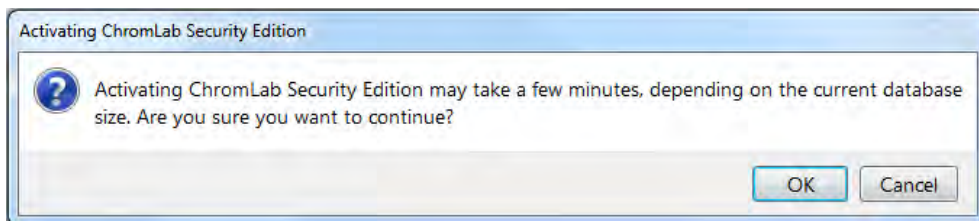
1. On the Start menu, select ChromLab > ChromLab Administration and log in as the ChromLab administrator.

ChromLab Administration opens, displaying the Licensing tab.



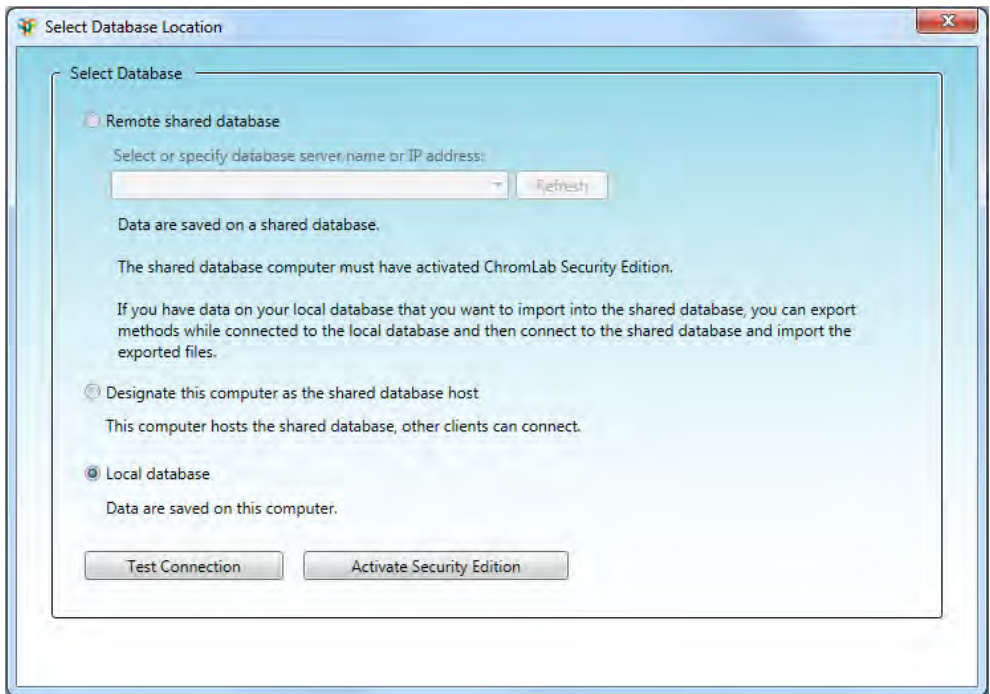
2. Select ChromLab Security Edition from the Select mode to activate dropdown list.
3. In the License Key field, type the 18-character Security Edition license key and click Apply.

The Activating ChromLab Security Edition dialog box appears.



4. Click OK. The Browse For Folder dialog appears.
5. In the Browse For Folder dialog box, select the NGC backup folder that you created and click OK to create and save the NGC backup (.sbk) file.

When the backup completes, the Select Database Location dialog box appears.



6. In the Select Database Location dialog box, select Designate this computer as the shared database host.
7. (Optional) Click Test Connection.
8. Click Activate Security Edition to establish the shared database on this computer.

A message informs you that changing the database to sharing mode requires ChromLab to shut down. ChromLab connects to the shared database when you restart the application.

9. Click Yes to continue the connection process.

ChromLab Administration closes. The next time it is started, ChromLab connects to the shared database on this computer.

Next Steps

After you activate Security Edition on the central computer and before you connect the remote computers to the shared database, Bio-Rad recommends that you create users and assign the relevant roles. Afterwards, you can uninstall ChromLab software from the central computer.

Creating Users

Important: In order to use ChromLab after Security Edition has been activated on the remote computers, users must log in to the shared database. This requires each user to have a valid user name and password. If you have not yet done so, Bio-Rad suggests that you create users before activating Security Edition on the remote computers.

For more information about creating and managing ChromLab user accounts, see [Chapter 9, Setting Up ChromLab Users and Roles](#).

Uninstalling ChromLab Software on the Central Computer

Note: This task is *optional*.

After you activate Security Edition on the central computer, and have created users and assigned roles to them, you can uninstall ChromLab software from the central computer. Although uninstalling removes ChromLab software and ChromLab Administration from the computer, the ChromLab database remains and remote ChromLab computers and NGC systems can access it.

Special Considerations

Uninstalling ChromLab from the central computer removes the Bio-Rad firewall settings and the backup and restore feature in ChromLab Administration. This section lists two important considerations to keep in mind if you choose to uninstall ChromLab software from the central computer.

Creating Inbound Firewall Rules for the ChromLab Database

You must create the following custom inbound firewall rules in order for the SQL Browser and SQL Server services to receive data from the network:

- Bio-Rad NGC SQLServer NG
- Bio-Rad NGC SQLServer Browser

Important: Contact your system or network administrator or Bio-Rad Technical Support for assistance. See [Manually Adding Inbound Firewall Rules on page 105](#) for more information.

Backing Up and Restoring ChromLab Data

You will not be able to use ChromLab Administration to back up and restore the NGC database. You must use SQL Server Management Studio or a 3rd party tool to back up and restore the database. You require the password for the sa user to connect to the NGC instance and perform this task.

For more information, contact Bio-Rad Technical Support.

Tip: You can also reinstall the same version of ChromLab software on the central computer at any time to access ChromLab Administration and perform backup and restore functions.

Chapter 5 Connecting Remote Computers to the Central Computer

When ChromLab is installed, by default it is set to run in standard mode (that is, only the local database is available). It continues to run in this mode until a user with ChromLab Administrator privileges activates ChromLab Software, Security Edition.

The workflow for connecting remote ChromLab computers to the shared database consists of the following tasks. This chapter explains these tasks in detail.

1. Verify that ChromLab 6.1 is installed on each remote computer.
2. (Optional but recommended) Export existing 6.1 ChromLab methods from all computers.

Note: Only ChromLab methods can be imported into the Security Edition database. See [Importing Electronic Data Files on page 62](#) for more information.

3. Verify date and location settings on the remote computers.

See [Locating the Date and Time Settings on ChromLab Computers on page 36](#).

4. Create an NGC database backup folder on all remote ChromLab computers.

See [Creating an NGC Database Backup Folder on page 37](#).

5. Change the local default admin password in ChromLab Administration.

See [Changing the ChromLab Default Password on page 39](#).

6. Activate Security Edition on each remote computer.

See [Activating ChromLab Software Security Edition on Remote Computers on page 41](#).

7. (Optional) Import existing data to the shared database.

Important: In order to use ChromLab after Security Edition has been activated on the remote computers, users must log in to the shared database. This requires each user to have a valid user name and password. If you have not yet done so, Bio-Rad suggests that you create users at this time. For more information about creating and managing ChromLab user accounts, see [Chapter 9, Setting Up ChromLab Users and Roles](#).

Locating the Date and Time Settings on ChromLab Computers

In order for ChromLab to function correctly, the date and time settings on remote computers must be the same as those on the central computer.

Perform this task on the central ChromLab computer first. Verify that the settings on the remote computers are the same as those on the central computer.

To locate the date and time settings

1. On the central ChromLab computer, open the Control Panel and select Date and Time.
2. In the Date and Time dialog box, note the current date, time, and time zone settings.
3. Close the Date and Time dialog box on the central computer.
4. On each remote computer, open the Date and Time dialog box.
5. Note the date, time, and time zone settings.
 - If the time zone is different from that on the central computer, click Change time zone and modify the settings as necessary.
 - If the date or time differ from those on the central computer, click Change date and time and modify the settings as necessary.
6. Close the Date and Time dialog box.

Creating an NGC Database Backup Folder

ChromLab automatically backs up the existing NGC database when you activate Security Edition. If you have not previously backed up your NGC database, consider creating the database backup folder at this time.

Note: Even if you are installing ChromLab for the first time, the system backs up the empty NGC database. A new, empty NGC database requires approximately 75 MB of free disk space.

Perform this task on all computers on which you plan to activate Security Edition.

To create the NGC database backup folder

1. Determine the size of the NGC database.
 - a. Navigate to C:\ProgramData\Bio-Rad\NGC\Database.
 - b. Right-click the Database folder and select Properties.
 - c. On the General tab, note the Size value.

Ensure that the disk on which you plan to save the backup zip file (the target disk) has free disk space that is at least equal to the size of the NGC database.

2. On the backup computer, right-click the target folder and select New > Folder.
3. Rename the new folder, for example, NGC Database Backup.

Exporting Existing ChromLab Data

Important: ChromLab creates a backup of the database that resides on the local computer when you activate Security Edition. Because restoring the backup data overwrites existing data, Bio-Rad strongly recommends that you *export* ChromLab methods from the local ChromLab database that you want to use in the shared environment. Perform this procedure *after* you upgrade to ChromLab 6.1 and *before* you activate Security Edition on remote computers. You can then import the methods into the shared database after you set up the shared environment. This ensures you have access to all your necessary methods.

Note: You can import only methods into Security Edition. You cannot import associated runs with the methods into Security Edition. For more information, see [Importing Electronic Data Files on page 62](#)

To export ChromLab methods

1. Start ChromLab.
2. Select File > Browse to open the Browse Data dialog box.
3. Choose Methods on the View by dropdown list.
4. Select the project that contains the target file in the Projects pane.
5. Right-click the file or files to export in the right pane and select Export <file_type>.

The Browse for Folder dialog box appears.

6. Browse to a target folder or create a destination folder and click OK.

The Exporting NGC Files dialog box appears, showing the status of the export. When the export is complete, Completed appears in the Status column.

7. Click OK to close the dialog box.

Changing the ChromLab Default Password

You activate Security Edition through the ChromLab Administration tool. The first time you launch ChromLab Administration on each computer you must change the default admin password before continuing.

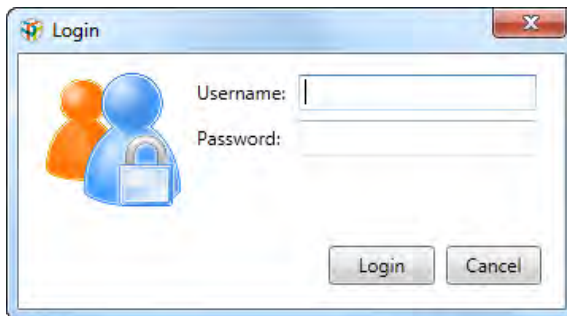
Note: You cannot activate Security Edition while either ChromLab software or the NGC system is in use. Close ChromLab and shut down the system before launching ChromLab Administration.

Important: You will perform this task on each remote ChromLab computer as well as the central ChromLab computer. Ensure that the Administrator password for each ChromLab computer is unique. Keep the Administrator passwords for all ChromLab computers in a secure place.

To change the default admin password

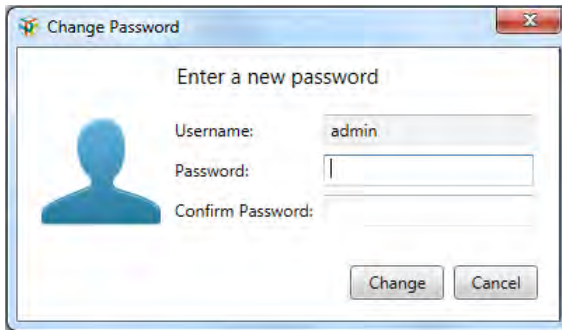
1. On the Start menu, select ChromLab > ChromLab Administration.

The Login dialog box appears.



2. Type the word admin for both the user name and password and click Login.

The Change Password dialog box appears.



3. Type a new password for the ChromLab administrator in the Password field, type it again in the Confirm Password field, and click Change.

Activating ChromLab Software Security Edition on Remote Computers

Note: You cannot activate Security Edition while either ChromLab software or the NGC system are in use. Close ChromLab and shut down the NGC system before launching ChromLab Administration.

Perform this task on all remote computers that will access the shared database. This includes

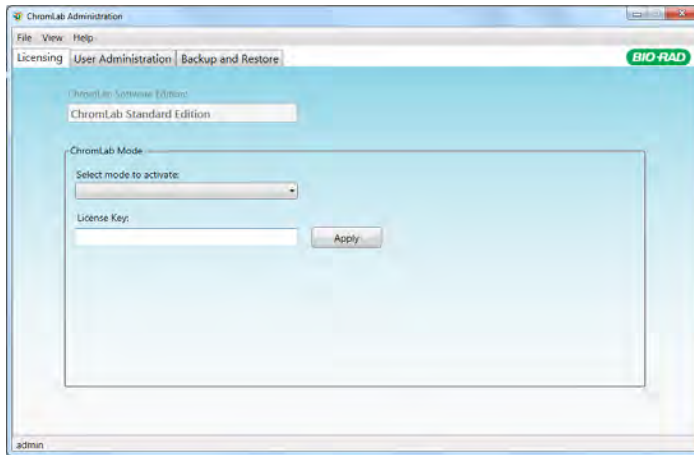
- ChromLab workstations
- ChromLab computers connected to NGC systems, including those in read-only mode

Important: ChromLab automatically backs up the current NGC database, creates an empty database, and then activates Security Edition. Depending on the size of your current NGC database, this process can take some time.

To activate Security Edition on remote computers

1. On the Start menu, select ChromLab > ChromLab Administration and log in as the ChromLab administrator.

ChromLab Administration opens, displaying the Licensing tab.

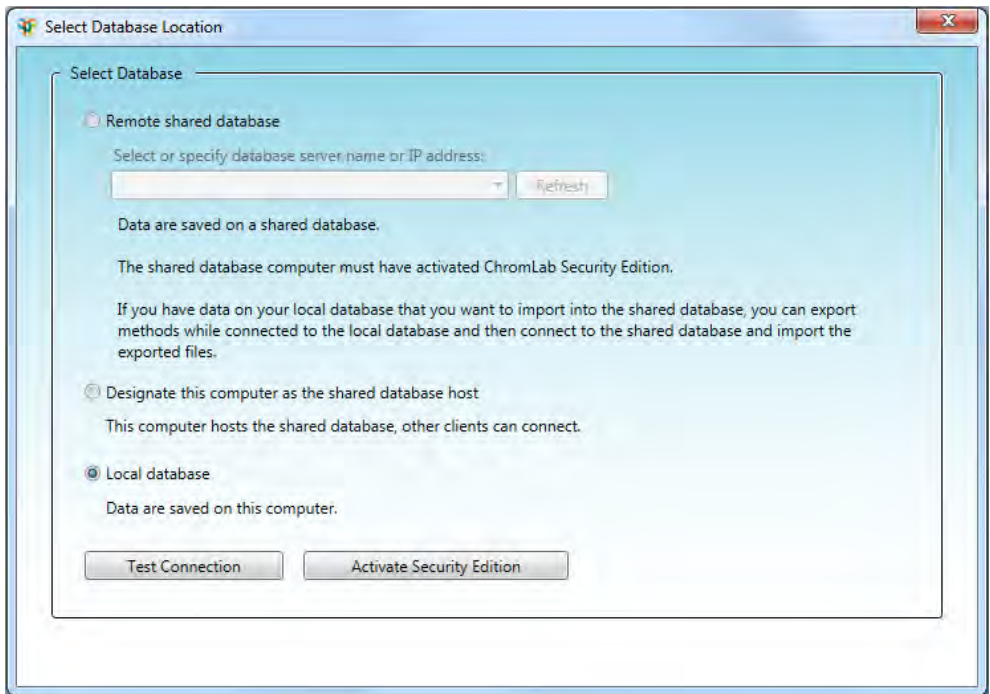


2. Select ChromLab Security Edition from the Select mode to activate dropdown list.
3. In the License Key field, type the 18-character ChromLab Security Edition license key and click Apply.

The Activating ChromLab Security Edition dialog box appears.

4. Click OK. The Browse For Folder dialog appears.
5. In the Browse For Folder dialog box, select the NGC backup folder that you created and click OK to create and save the NGC backup (.sbk) file.

When the backup completes, the Select Database Location dialog box appears.



6. In the Select Database Location dialog box, select Remote shared database.

Tip: Select Local database only if you want to save data to the local ChromLab database.
7. If it does not automatically appear, select the name or IP address of the central computer in the dropdown list. Alternatively, type the central computer's name or IP address in the dropdown list box.

Important: You must use the same connection parameter for all remote computers that will access the shared database. That is, all remote computers should connect to the central computer using either its IP address or its computer

name. Bio-Rad *strongly* recommends that you connect to the central computer using a static IP address.

8. (Optional) Click Test Connection.
9. Click Activate Security Edition to connect to the shared database.

A message informs you that changing the database to sharing mode requires ChromLab to shut down. ChromLab connects to the shared database when you restart the application.

10. Click Yes to continue the connection process.

ChromLab Administration closes. The next time it is started, ChromLab connects to the shared database on the central computer.

Importing Existing ChromLab Data

To ensure that you can access your current data after you set up the shared database and connect to it from the remote computers, import the data from all remote computers into the shared database.

Important: Until the ChromLab administrator has created users on the central ChromLab computer, you will not be able to log in to ChromLab. Ensure that you have a valid user name and password before performing this task.

To import ChromLab methods

1. Start ChromLab and log in as a ChromLab user.
2. Select File > Import and choose NGC File.

The Import NGC File dialog box appears.

3. Click Select.

The Select Project dialog box appears.

4. In the Select Project dialog box, do one of the following:
 - Choose a destination project for the method and click Select Project.
 - Create a new project and click Select Project.
 - Right-click on an existing project and select New Project to create a subproject and then click Select Project.
5. In the Import NGC File dialog box, click Browse to display the Open dialog box.
6. Select the method to import and click Open.
7. (Optional) In the Name box, type another name for the file.

Note: This option is available only when you select a file to import.
8. Click Import. During the import a status dialog box appears. When all methods have successfully imported, the status displays Completed.
9. Click OK to close the dialog box.

The files are imported into the project you selected.

For more information about exporting and importing ChromLab data, see the NGC Chromatography Systems and ChromLab Software User Guide.

Rules for Sharing ChromLab Data

Once the remote computers are connected to the shared database, users can create and modify methods, run methods, and analyze runs. To ensure data integrity, ChromLab enforces the rules noted in [Table 2](#).

Important: The rules in [Table 2](#) are valid for unsigned objects only (signed objects cannot be changed). As well, users must have the required permissions. For example, only users assigned the Advanced User or Service User role can change unsigned methods.

Tip: Remote users can log in to an NGC system while another user's run is in progress. However, only users assigned the Advanced User role can control an NGC system that is in use by another user. Other users must wait until the run completes before they can control the NGC system. As well, the run queue must be cleared of pending runs before other users can control the NGC system. For more information about controlling the NGC system, see [Appendix 8, Connecting Multiple ChromLab Computers to One NGC System](#).

Table 2. Rules for sharing ChromLab data

Action	Rule
Methods	
Add a method to a project that contains another method with the same name	Users are prompted to save the method with a unique name before saving it to the project.

Table 2. Rules for sharing ChromLab data, continued

Action	Rule
Edit and save the same method at the same time (parallel editing)	<p>Changes made by the first user are saved. The next user is prompted to do one:</p> <ul style="list-style-type: none"> ■ Refresh the method then save ■ Save the method with another name ■ Cancel and discard the changes
Edit and save the same method at different times (sequential editing)	Changes made by all users are saved.
Edit a method that was recently deleted by another user	<p>The original method is deleted. The next user is prompted to do one:</p> <ul style="list-style-type: none"> ■ Save the method with another name ■ Cancel and discard the changes
Edit a method that was signed by another user	The action fails. The system displays notification that the signed method cannot be changed.
Run the same method on different systems at the same time	The method is queued and run in parallel.
Method Templates	
Add a method template to the database if another template with the same name exists	Users are prompted to save the template with a unique name before saving.

Table 2. Rules for sharing ChromLab data, continued

Action	Rule
Edit and save the same template at the same time (parallel editing)	<p>Changes made by the first user are saved. The next user is prompted to do one:</p> <ul style="list-style-type: none"> ■ Refresh the template then save ■ Save the template with another name ■ Cancel and discard the changes
Edit and save the same template at different times (sequential editing)	Changes made by all users are saved.
Edit a template that was recently deleted by another user	<p>The original template is deleted. The next user is prompted to do one:</p> <ul style="list-style-type: none"> ■ Save the method with another name ■ Cancel and discard the changes
Runs	
Save a run to the database if another run with the same name exists	Users are prompted to save the run with a unique name before saving it to the project.
Edit the same run at the same time (parallel editing)	Changes made by the first user are saved. The next user is informed the run was changed and the run is reloaded with the changes made.

Table 2. Rules for sharing ChromLab data, continued

Action	Rule
Edit and save the same run at different times (sequential editing)	Changes made by all users are saved.
Edit a run that was recently deleted by another user	The run is deleted. The next user is informed the run was deleted and the window closes.
Edit a run that was signed by another user	The action fails. The system displays notification that the signed run cannot be changed.
Analyses	
Save an analysis to the database if another analysis with the same name exists	Users are prompted to save the analysis with a unique name before saving it to the project.
Edit and save the same analysis at the same time (parallel editing)	Changes made by the first user are saved. The next user is prompted to do one: <ul style="list-style-type: none"> <li data-bbox="817 922 1147 979">■ Save the analysis with another name <li data-bbox="817 995 1157 1019">■ Cancel and discard the changes
Edit and save the same analysis at different times (sequential editing)	Changes made by all users are saved.
Edit an analysis that was signed by another user	The action fails. The system displays notification that the signed analysis cannot be changed.

Table 2. Rules for sharing ChromLab data, continued

Action	Rule
Delete an analysis if another user has it open	<p>The original analysis is deleted. The next user is prompted to do one:</p> <ul style="list-style-type: none"> ■ Save the analysis with another name ■ Cancel and discard the changes
Fluidic Schemes	
Delete a fluidic scheme that was used in a method run by another user	The user is informed that the fluidic scheme is in use and cannot be deleted.
<p>Select or delete a fluidic scheme that was recently deleted by another user</p> <p>Create a new fluidic scheme based on a scheme that was recently deleted by another user</p>	<p>The original fluidic scheme is deleted. The next user is prompted to do one:</p> <ul style="list-style-type: none"> ■ Save the fluidic scheme with another name ■ Cancel and discard the changes

Chapter 6 The Security Edition Workspace

ChromLab Software, Security Edition provides an intuitive interface for developing chromatography methods, operating an NGC instrument, and analyzing data from chromatography runs.

ChromLab software presents four primary workspaces.

- The Home window
- The System Control window
- The Method Editor window
- The Evaluation window

Each workspace and the NGC instrument touch screen are shown and described in detail in the NGC Chromatography Systems and ChromLab Software User Guide.

In Security Edition, you use ChromLab Administration to

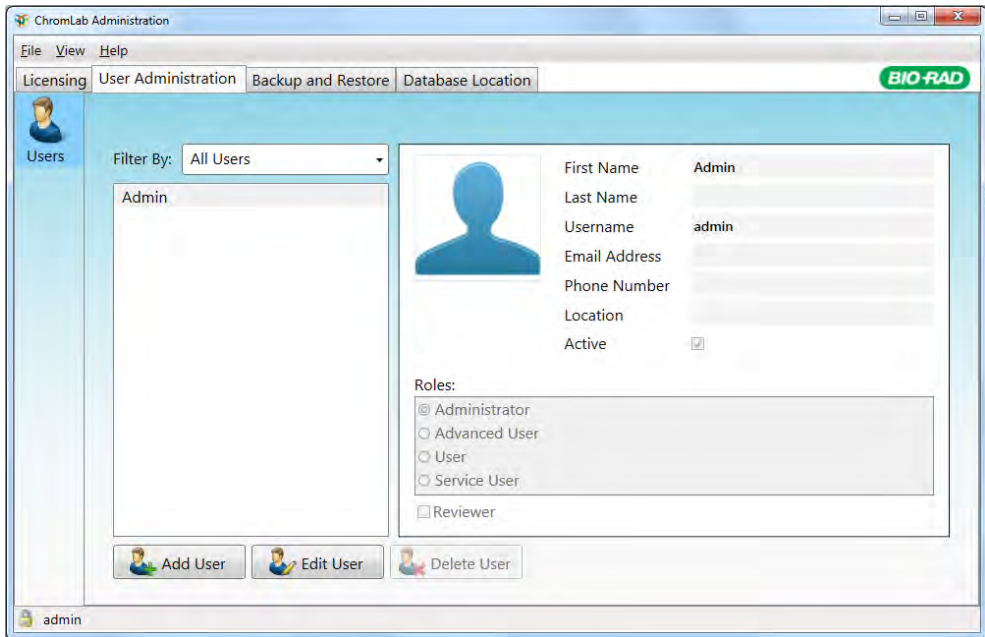
- Activate ChromLab Security Edition
- Create and maintain user accounts
- Back up and restore the NGC database

ChromLab Administration, the Home window, and the additional Security menu item are shown and described in this chapter.

ChromLab Administration

When ChromLab Administration is launched after Security Edition is activated, it opens displaying the User Administration tab. The application also displays the Licensing, Backup and Restore, and Database Location tabs.

The Licensing, Database Location, and Backup and Restore tabs are available to users with the Administrator role. The User Administration tab is available to all users.



Menu Commands

Each tab has the same menu commands. This section explains the menu commands for ChromLab Administration.

File Menu Command

Close — closes ChromLab Administration.

View Menu Commands

Show Inactive Users — displays currently active and deactivated Security Edition users.

Note: This option is enabled only on the User Administration tab.

Password Options — displays the Password Options dialog box. See [Setting Password Options on page 93](#) for more information.

Note: This option is enabled only for users with the Administrator role.

Show Audit Log — displays the System and User Administration Audit Log.

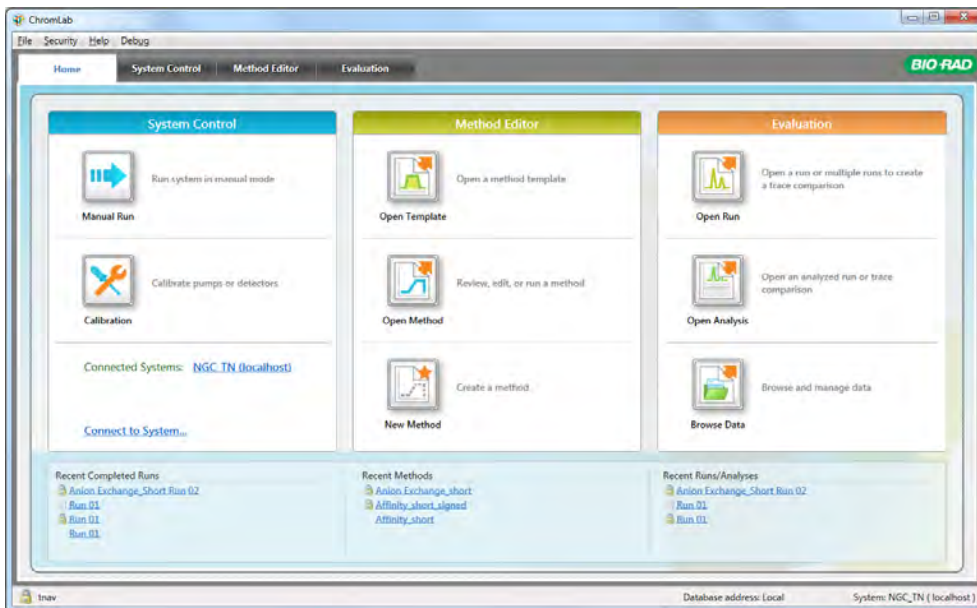
Note: This option is enabled only for users with the Administrator role.

Help Menu Command

About — displays ChromLab Administration copyright and version information.

The Security Edition Home Window

ChromLab Software, Security Edition opens with the Home window, which displays three panes and the System Control tab.



When Security Edition is activated, a lock and the name of the logged in user is displayed in the left corner of the status bar. The status of connection to the NGC instrument is also displayed. Links to recently completed runs, recently created methods, and recently accessed or analyzed runs and analyses appear listed at the bottom of the window.

Tip: A controlled or signed file is identified by a specific icon beside its name, while an uncontrolled file does not have an icon. [Table 3 on page 59](#) shows the icons that identify the status of data files. See [Using ChromLab Software Security Edition on page 57](#) for detailed information about uncontrolled, controlled, and signed files.

Security Edition Menu Commands

Security Edition has the same menu options and menu commands as the standard edition of ChromLab software. Additionally, Security Edition provides the Security menu option on each window. This section describes the menu commands in the Security menu option for all four windows.

Home Window

General Audit Log — displays the General Audit Log.

System Control Window

General Audit Log — displays the General Audit Log.

Method Editor Window

General Audit Log — displays the General Audit Log.

Sign Method — opens the Sign Method dialog box.

Note: Only users assigned the Reviewer attribute can sign methods.

Evaluation Window

General Audit Log — displays the General Audit Log.

Show Run Audit Log — displays the audit log for the displayed run.

Sign Run — opens the Sign Run dialog box.

Note: Only users assigned the Reviewer attribute can sign runs.

Show Analysis Audit Log — displays the audit log for the displayed analysis.

Sign Analysis — opens the Sign Analysis dialog box.

Note: Only users assigned the Reviewer attribute can sign analyses.

Chapter 7 Using ChromLab Software Security Edition

Electronic Records

ChromLab Software, Security Edition enables you to create electronic records as defined by 21 CFR Part 11. In Security Edition, the following data files are considered electronic records:

- Methods
- Runs
- Analyses
- Audit log files

Security Edition data files are either uncontrolled, controlled, or signed. This section defines these terms.

Uncontrolled Data Files

Uncontrolled data files have no audit log. They are not auditable according to 21 CFR Part 11 regulations. The following data files are considered uncontrolled:

- Imported methods
- New, unsigned methods
- Runs created from uncontrolled methods
- Analyses created from uncontrolled runs

- Manual runs
- Column performance runs
- Scout runs

Uncontrolled methods remain uncontrolled until they are signed. At that time, they are considered signed data files. Uncontrolled runs and analyses cannot be signed and remain uncontrolled. Uncontrolled data files can be modified and saved without restrictions.

Controlled Data Files

Controlled data files have an audit log but are not signed. The following data files are considered controlled:

- Unsigned runs based on signed methods
- Unsigned analyses based on controlled or signed runs
- Copies of signed runs or analyses saved as new data files

Actions performed on a controlled file are tracked in its audit log. Controlled files can be modified. Saving modified controlled files overwrites the original file, and the saved file is controlled.

Signed Data Files

Signed data files are controlled files that are signed by a user assigned the Reviewer attribute. The following data files can be signed:

- Uncontrolled methods
- Controlled runs
- Controlled analyses

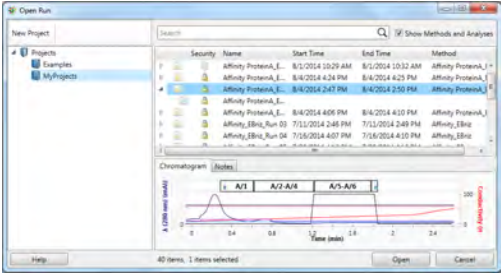


Signed files are read-only. They cannot be overwritten or deleted. Signed runs and analyses can be opened and reviewed, and copies can be saved as a new controlled file using the File > Save As dialog box. The changes are tracked in the audit log.

Important: ChromLab will never overwrite or delete any signed file.

Identifying Data File Status

A controlled or signed file is identified by a specific icon beside its name in the browser and in the open file. An uncontrolled file does not have an icon. [See Identifying Data File Status](#) shows the icons that identify the status of data files.

Table 3. Identifying the status of data files

Icon	Status	Example
	Uncontrolled file	
	Controlled file	
	Signed file	

Signing Data Files

Note: Only users with the Reviewer attribute can sign or re-sign data files.

You can sign the following data files:

- Uncontrolled methods that have not been run

Note: You cannot sign an uncontrolled method that has associated uncontrolled runs. You must save the method with a new name to sign it.

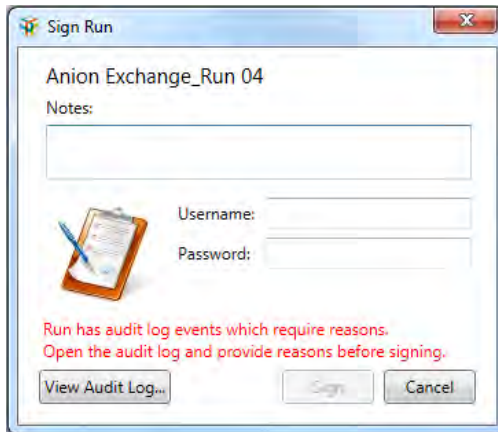
- Controlled runs

Note: You cannot sign a run that was created from an uncontrolled, unsigned method. You must save the method with a new name and sign the new method. Use the signed method to create a signable run.

- Controlled analyses from controlled or signed runs

To sign a file

1. Do one of the following:
 - In the Method Editor, open the method to sign.
 - In Evaluation mode, open the run or analysis to sign.
2. Choose Security > Sign <file>. The signing dialog box appears.



3. (Optional) In the Notes text box, include information about the file or a reason for signing. This information is included in the audit log.
4. Enter the username and password of a user with the Reviewer attribute.

The username, date, and time of the signature are always included in the audit log (for more information see [Audit Logs on page 64](#)).

5. If you manually edited the method during the run, you must provide a reason for each change before you can sign the run.
 - a. Click View Audit Log to open the run's audit log.

Date & Time	Username	Event Type	Event	System Name	Reason
9/15/2015 4:45 PM	sding	Signing	Method 'Anion Exchange_short' signed.		
9/30/2015 2:14 PM	tnav	Run	Run 'Anion Exchange_Run 04' started on system 'NGC_TN'. Method run ...	NGC_TN	
9/30/2015 2:14 PM	tnav	Manual Edit	Flow rate is set to 1.000 ml/min	NGC_TN	Reason required
9/30/2015 2:14 PM	tnav	Manual Edit	Advanced to next step	NGC_TN	Reason required
9/30/2015 2:14 PM	tnav	Manual Edit	Advanced to next step	NGC_TN	Reason required
9/30/2015 2:15 PM	tnav	Manual Edit	BioFrac Advance to Next Fraction	NGC_TN	Reason required
9/30/2015 2:15 PM	tnav	Manual Edit	BioFrac Advance to Next Fraction	NGC_TN	Reason required
9/30/2015 2:15 PM	tnav	Manual Edit	Divert to Waste	NGC_TN	Reason required
9/30/2015 2:15 PM	tnav	Manual Edit	Start Fraction Collection	NGC_TN	Reason required
9/30/2015 2:15 PM	tnav	Manual Edit	Advanced to next step	NGC_TN	Reason required
9/30/2015 2:15 PM	tnav	Run	Run Completed	NGC_TN	

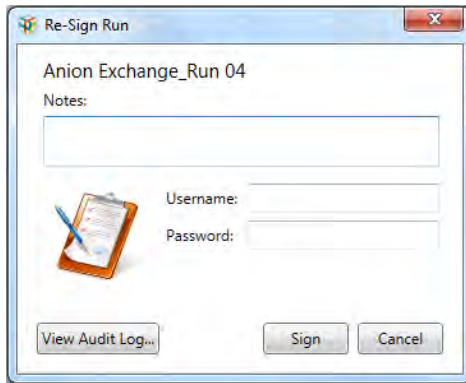
Show full event description

- b. For each manual edit, click the ellipses button beside the highlighted Reason field to open the Add Reason dialog box.
 - c. Provide a reason for each manual edit.
 - d. Click OK and then close the audit log.
6. Click Sign.

The file is saved in the project with the name shown in the signing dialog box.

To re-sign a data file

1. Do one of the following:
 - In the Method Editor, open the method to sign.
 - In Evaluation mode, open the run or analysis to sign.
2. Choose Security > Sign <file>. The re-signing dialog box appears.



3. (Optional) In the Notes text box, include comments about the file or a reason for re-signing.
4. Enter the username and password of a user with the Reviewer attribute.
5. (Optional) Click View Audit Log to see the audit log for this data file.
6. Click Sign.

Importing Electronic Data Files

Only methods exported from the standard edition or the Security Edition of ChromLab software can be imported into Security Edition. These files are uncontrolled. You cannot import runs or analyses into Security Edition.

Exporting Electronic Data Files

You can export any saved data file from Security Edition. Exporting controlled or signed files removes all audit log and signing information. The exported file is saved as an uncontrolled data file.

Backing Up and Restoring the Security Edition Database

Important: In a shared ChromLab database environment, perform this task on the central computer.

Security Edition stores all data (for example, methods, templates, and runs) in a database using Microsoft SQL Server. Bio-Rad highly recommends backing up this database regularly. Backing up the database on a different drive from the one on which Security Edition is running is also recommended.

The backup procedure saves the Security Edition database as a zip (.sbk) file. The .sbk file is approximately the same size as the NGC database itself. Backing up and restoring the database requires the same amount of free disk space as the size of the .sbk file.

Use ChromLab Administration to back up and restore the Security Edition database. ChromLab Administration backs up all NGC data, including all methods, runs, analyses, and audit logs. You can also use ChromLab Administration to set a reminder to back up the NGC database on a daily, weekly, or monthly basis. The reminder appears on the ChromLab computer.

Restoring the Security Edition database overwrites the current database. If you have saved any new data since the backup, consider restoring the database onto another computer running Security Edition in order to prevent data loss.

To back up and restore the Security Edition database or set a reminder

- ▶ See Appendix B, Database Management, in the NGC Chromatography Systems and ChromLab Software User Guide.

Each time a secure document is modified, you must provide a reason for **each** change before you can sign the document. The modifications are logged in the document log. The new signed document takes with it the entire history of the original document in its log.

Audit Logs

Any changes made to or actions performed on a controlled run or a controlled analysis are saved to the database and captured in an audit log. Audit logs are created when Security Edition is activated. ChromLab Software, Security Edition has three audit logs:

- **General audit log** — captures user administration events, system and calibration events, and information about changes made to or actions performed on a method, run, or analysis.
- **Run audit log** — captures all major actions and changes for a single run.
- **Analysis audit log** — captures all major actions and changes for a single run or multiple-run analysis.

This section details the events that are captured in the audit logs.

Note: The following objects and events are not captured:

- Runs of uncontrolled methods
- Column performance tests
- Manual runs
- Scout runs
- Annotations
- Analyses of uncontrolled runs
- Run/Traces, Peaks, and Fractions table settings
- Chromatogram settings
- Changes to y-axis ranges
- Trace color and visibility

General Audit Log

The general audit log captures all events included in the run and analysis audit logs. In addition, the general audit log captures the following events:

- System events including
 - System calibration of the following modules:
 - System pumps
 - Sample pumps
 - Column switching valve pressure values
 - Conductivity monitor
 - pH probe
 - Changes to
 - SIM input settings
 - Air sensor settings
 - Control flow rates
 - (In a multiple NGC system environment) User taking control of the NGC system

Note: All system events are captured in the general audit log. All events started from the touch screen are captured in the general audit log while the connection to the ChromLab computer is active. If the connection is inactive, you are notified when you attempt to make changes from the touch screen. System events are logged to the user logged into the ChromLab computer.

- User administration events including
 - Adding/modifying/deleting users
 - Activating/deactivating users

- User logins and exits
- Changes to user profiles

Run Audit Log

In Evaluation mode, all major actions and changes for a single run are audited. The entries appear in the audit log after the run is saved. The run audit log includes the following run events:

- Run start

- Injection point changes

Note: You can change injection points only for controlled unsigned runs. You cannot change an injection point when the run has been signed. You must provide a reason for setting the injection point in the Set Injection Point dialog box before you can click Apply. The reason is included in the audit log.

- Manual edits to method runs including

- Advance to next step
- Change flow rate
- Advance fraction collector
- Collect or waste fraction
- Zero baseline
- Pause/resume run
- Stop/start run
- Hold step

Note: Manual edits to method runs are logged to the user logged into the ChromLab computer. You must provide a reason for each manual edit in the run's audit log before you can sign the run.

- Run completion

Analysis Audit Log

In Evaluation mode, all major actions and changes for a single run analysis are audited. The entries appear in the audit log after the analysis is saved. The analysis audit log includes the following analysis events:

- Automatic peak integration events including
 - Participating traces
 - Integration parameters
 - Peak filtering information
 - Trace deletions
 - Peak deletions
- Manual peak integration events including
 - Peak range changes
 - Peak deletions
 - Peak splits
 - Peak additions
- Undo/redo actions
- Peak table events including
 - Changes to path length
 - Changes to the extinction coefficient column
- Fraction table events including
 - Changes to the extinction coefficient column
 - Changes to pooling that affect child fraction rows

- Injection point changes

Note: You can change injection points only for controlled unsigned analyses. You cannot change an injection point when the analysis has been signed. You must provide a reason for setting the injection point in the Set Injection Point dialog box before you can click Apply. The reason is included in the audit log.

- Trace comparison events including

- Adding a controlled or signed run to a trace comparison
- Removing a controlled or signed run from a trace comparison

- Multiple-run analysis

Note: In Security Edition, trace comparisons and multiple-run analyses can include both signed and controlled runs. Neither a trace comparison nor a multiple-run analysis can be signed if any of the runs are uncontrolled. If the analysis includes controlled but unsigned runs, you will be prompted to sign the runs before you can sign the analysis.

Viewing Audit Logs

The following fields are displayed in each audit log:

- **Date and time** — the local date and time when the event occurred.
- **Username** — the username of the logged in user when the event occurred.
- **Event type** — the type of event, for example run, analysis, calibration, user administration.
- **Event** — an explanation of the event.
- **System name** — the NGC system on which the method was run.
- **Reason** — the reason for the event.

Tip: Until the data file is signed, you can edit this text box. After the file is signed this box is no longer editable.

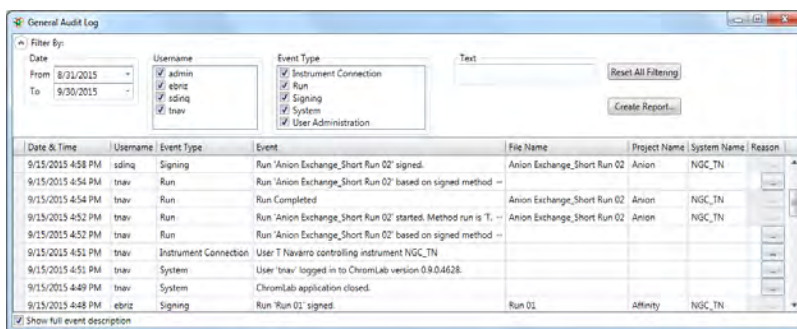
In addition, the following fields are displayed in the general and analysis audit logs:

- **File name** — the name of the method, run, or analysis acted upon.
- **Project name** — the name of the project folder in which the object is located.

Viewing the General Audit Log

To view the general audit log

- ▶ Select Security > General Audit Log. The audit log appears.



By default, the data are sorted by date and time, and the event column displays the full description of the events. You can filter the data by date, username, event type, and text string. You can sort the data by any column, and you can set the event column to display a general description of the events.

To filter data in the general audit log

1. By default, the audit log displays all events performed by all users within the past 30 days. In the Date section, choose the date range of events to view.
2. In the Username section, clear the checkboxes of the users whose events you do not want to include in the filtered view.
3. In the Event Type section, clear the checkboxes of the events you do not want to include in the filtered view.

- In the Text section, type a word or phrase to include in the filtered view.

The audit log displays the results of the filter.

To reset the filter settings in the audit log

- Click Reset All Filtering.

To hide filter options

- Click the Filter By arrow at the top of the window.

Date & Time	Username	Event Type	Event	File Name	Project Name	System Name	Reason
9/15/2015 4:58 PM	sdinq	Signing	Run 'Anion Exchange_Short Run 02' signed.	Anion Exchange_Short Run 02	Anion	NGC_TN	
9/15/2015 4:54 PM	tnav	Run	Run 'Anion Exchange_Short Run 02' based on signed method --				
9/15/2015 4:54 PM	tnav	Run	Run Completed	Anion Exchange_Short Run 02	Anion	NGC_TN	
9/15/2015 4:52 PM	tnav	Run	Run 'Anion Exchange_Short Run 02' started. Method run is T. --	Anion Exchange_Short Run 02	Anion	NGC_TN	
9/15/2015 4:52 PM	tnav	Run	Run 'Anion Exchange_Short Run 02' based on signed method --				
9/15/2015 4:51 PM	tnav	Instrument Connection	User T Navarro controlling instrument NGC_TN				
9/15/2015 4:51 PM	tnav	System	User 'tnav' logged in to ChromLab version 0.0.0.4628.				
9/15/2015 4:49 PM	tnav	System	ChromLab application closed.				

Show full event description

To sort data in the audit log

- Click the heading of the data column you want to sort to perform an ascending sort (A to Z, smallest number to largest, or earliest to most recent).

(Optional) Click the heading again to perform a descending sort.

To display a full description of events

- Select the Show full event description checkbox at the bottom of the dialog box.

To print the audit log

- Click Create Report. A report similar to a method, run, or analysis report appears.

Tip: The general audit log report includes all information displayed on the screen. If you filtered the data, only the results of the filter are printed.

To close the audit log

- ▶ Click the red x at the top of the log.

Viewing the Run Audit Log**To view the run audit log**

- ▶ In the open run, select Security > Run Audit Log. The run audit log appears.

Viewing the Analysis Audit Log**To view the analysis audit log**

1. Do one of the following:
 - Open the run and perform a peak analysis.
 - Open the analysis.
2. Select Security > Analysis Audit Log. The analysis audit log appears.

Signed Reports

The three report formats available in Security Edition make it easy to publish signed method, run, and analysis data in detailed reports. Although only users with the Reviewer attribute can sign reports, all users can view them.

Signed Method Reports

Similar to a method report generated in the standard edition of ChromLab, the signed method report includes all information about the method. It also includes a Signatures table that contains the following fields:

- **Time** — the time of the event.
- **Signed By** — the name of the user who signed the method.
- **Notes** — additional information provided by the user.

The screenshot displays a 'ChromLab™ Method Report - Affinity_Elixir' window. The report is signed by 'BIO-RAD'. It includes a 'Signatures' table with the following data:

Time	Signed By	Notes
16/2014 4:28:19B	D. B. Baird	

The report also features a 'Gradient Graph' showing detector response over time (0 to 4 minutes) and a 'Method Steps' table:

Step	Step No.	Step Description	Step Unit	Step Vol	Flow	Step Parameters
1	1	Preion Column Prep. Step 1 (30 sec)	0	0	Sample Application	Sample Collected at 0.00 min
2	1	Load Inlet Sample	1	0	Sample Application	
2.1	1	Inject Sample	1	0	Sample Application	Sample: Public Inlet Loop
2.2	1	Change Valve (Change Inject Valve)	0	0	Sample Application	Inject Valve: 0.00 min, Sample: Public Inlet Loop

Appendix 8 Connecting Multiple ChromLab Computers to One NGC System

With ChromLab software, multiple ChromLab computers can simultaneously connect to the same NGC system.

In ChromLab Software, Security Edition users assigned the Advanced User role can take control of the NGC system and override another user's control of an instrument. This is useful in the event that the controlling computer is locked or the user performing the run is not available and there is an immediate need to stop the instrument.

Rules for Managing Access to NGC Systems

Important: View mode applies only to users connecting to an NGC system through a ChromLab computer. The NGC system's touch screen is never in View mode. All relevant features are available from the touch screen.

- Users assigned the Advanced User role have Take Control access to all NGC systems. You cannot change this access level for these users.
- The first user connecting to an NGC system from a ChromLab computer has full control of the instrument. The first user's computer retains control until a user assigned the Advanced User role overrides the instrument.
- In a shared database environment a user can take control any time except during system calibration or a Point-to-Plumb operation. Unsaved data from manual runs or current runs are saved to the shared database.

- In a standard environment (one in which each ChromLab computer saves data to its own database), a user cannot take control if any of the following conditions are true:
 - The NGC system has a run in progress
 - The system has queued runs pending
 - The system has unsaved manual data
 - A user is logged into the NGC system

Taking Control of an NGC System

Taking control of an NGC system is useful in the event that the controlling computer is locked or the user performing a run is not available and there is an immediate need to stop the instrument.

Note: Only users assigned the Advanced User role can perform this task. Take Control is disabled during system calibration or Point-to-Plumb actions.

To take control of an NGC system

1. If you have not already done so, connect to the target NGC system.
2. Select File > Take Control.

If successful, ChromLab displays a message informing you that you have control of the system. ChromLab displays a relevant message to the user who lost control.

Chapter 9 Setting Up ChromLab Users and Roles

To access ChromLab Software, Security Edition, each user must have a Security Edition user account. The ChromLab administrator creates the user accounts and assigns each account to predefined ChromLab roles. These roles are defined in the section [Users and Roles](#), which follows.

This chapter explains how to set up and manage ChromLab user accounts and roles.

Note:

- User accounts can have any name or password. See the section [Setting Password Options in Security Edition on page 93](#) for information about setting password rules for maximum security.
- Each user can be assigned only one role.

Users and Roles

Security Edition has four security roles and a Reviewer attribute. Each ChromLab user is assigned a role that provides the user access to specific software features. [Table 4](#) lists the Security Edition roles. [Table 5 on page 79](#) provides a detailed list of permissions for each role.

Table 4. ChromLab Security Edition roles

ChromLab Role	Description
Administrator	This role is designed for the ChromLab software administrator.
Advanced User	This role is designed for users requiring full access to all Security Edition functionality.
User	This role is designed for users requiring limited access to Security Edition functionality.
Service User	This role is reserved for service personnel to troubleshoot and maintain NGC systems.

Reviewer Attribute

Users assigned the Reviewer attribute can sign secure methods, runs, and analyses. The Reviewer attribute can be assigned to any user with the Advanced User or User role. The attribute is not available to users with the Administrator or Service User role.

Role Permissions

Roles determine which features in Security Edition users can access. If a user attempts to perform an action that is not permitted for the assigned role, ChromLab displays an error message. In some instances the user's role determines which Security Edition features are available and/or enabled. Not all features will be available to all users.

Important: Users cannot be assigned multiple roles. Review the permissions carefully before assigning roles.

[Table 5](#) lists the Security Edition functions that each role has permission to perform. See [Using ChromLab Software Security Edition on page 57](#) for detailed information about uncontrolled, controlled, and signed files.

Table 5. ChromLab permissions granted per role

	Administrator	Advanced User	User	Service User
General				
View audit logs	X*	X	X	X
Edit reason text box in audit log (add comments)	X*	X	X	X
* Administrators can see and edit only the ChromLab Administration details in the general audit log.				
Methods				
Create new uncontrolled methods		X		X
View (open) uncontrolled methods		X	X	X
View (open) signed methods		X	X	
Import uncontrolled methods		X		X
Modify (save) methods		X		X
Run uncontrolled methods		X	X	X
Run signed methods		X	X	

Table 5. ChromLab permissions granted per role, continued

	Administrator	Advanced User	User	Service User
Delete uncontrolled methods		X		X
Delete signed methods				
Rename uncontrolled methods		X		X
Rename signed methods				
Sign methods (with Reviewer attribute)		X	X	
Method Templates				
Create new templates		X		X
View (open) templates		X	X	X
Modify (save) templates		X		X
Delete user-defined templates		X		X
Rename templates		X		X

Table 5. ChromLab permissions granted per role, continued

	Administrator	Advanced User	User	Service User
System Control				
Run manually		X	X	X
Run at touch screen		X	X	X
Run uncontrolled methods		X	X	X
Run signed methods		X	X	
Change fluidic scheme		X	X	X
Calibrate NGC system		X	X	X
Delete fluidic scheme		X	X	X
Create fluidic scheme		X	X	X
Method run changes		X	X	X
Map fluidic scheme		X	X	X
Modify system settings		X		X
Take control of NGC system		X		

Table 5. ChromLab permissions granted per role, continued

	Administrator	Advanced User	User	Service User
Runs				
Create manual runs		X	X	X
Open (view) manual runs		X	X	X
Open (view) uncontrolled runs from an uncontrolled method		X	X	X
Open (view) controlled runs from a signed method		X	X	
Open (view) signed runs		X	X	
Modify manual runs (injection point, column performance)		X	X	X
Modify controlled runs from a signed method (injection point)		X	X	
Modify signed runs				
Rename manual runs		X	X	X

Table 5. ChromLab permissions granted per role, continued

	Administrator	Advanced User	User	Service User
Rename uncontrolled runs from an uncontrolled method		X	X	X
Rename controlled runs		X	X	
Rename signed runs				
Delete uncontrolled runs including: <ul style="list-style-type: none"> ■ Column performance runs ■ Scout runs ■ Manual runs ■ Runs based on uncontrolled methods 		X	X	X
Delete controlled runs		X		
Delete signed runs				
Sign runs (with Reviewer attribute)		X	X	
Import runs				

Table 5. ChromLab permissions granted per role, continued

	Administrator	Advanced User	User	Service User
Analyses				
Create analyses		X	X	X
View uncontrolled analyses		X	X	X
View controlled analyses		X	X	
View signed analyses		X	X	
Modify uncontrolled analyses		X	X	X
Modify controlled analyses		X	X	
Modify signed analyses				
Rename uncontrolled analyses		X	X	X
Rename controlled analyses		X	X	
Rename signed analyses				
Delete uncontrolled analyses		X	X	X

Table 5. ChromLab permissions granted per role, continued

	Administrator	Advanced User	User	Service User
Delete controlled analyses		X		
Delete signed analyses				
Sign analyses (with Reviewer attribute)		X	X	
Copy controlled analyses		X	X	
Copy signed analyses		X	X	
ChromLab Administration				
Log into ChromLab Administration	X	X	X	X
Back up and restore the Security Edition NGC database	X			
Set password rules	X			
View password rules	X	X	X	X
User Administration Tasks including:				
■ Add users	X			

Table 5. ChromLab permissions granted per role, continued

	Administrator	Advanced User	User	Service User
■ Delete users	X			
■ Enable/disable users	X			
■ View own user profile	X	X	X	X
■ Change own user password	X	X	X	X
■ Edit own user profile	X	X	X	X
■ View all profiles	X			
■ Change all passwords	X			
■ Edit all profiles	X			

Managing ChromLab User Accounts

To access and use Security Edition, each user must be assigned a role. This section explains how to manage user accounts.

Important: The admin user account is the default Administrator account, which you use to initially log into ChromLab Administration. To comply with 21 CFR Part 11, it is strongly recommended that you create a user account to administer Security Edition. Assign this account the Administrator role and perform all Security Edition administration tasks with this account. Do not use the default admin user account to perform activities other than to log in and create this first account.

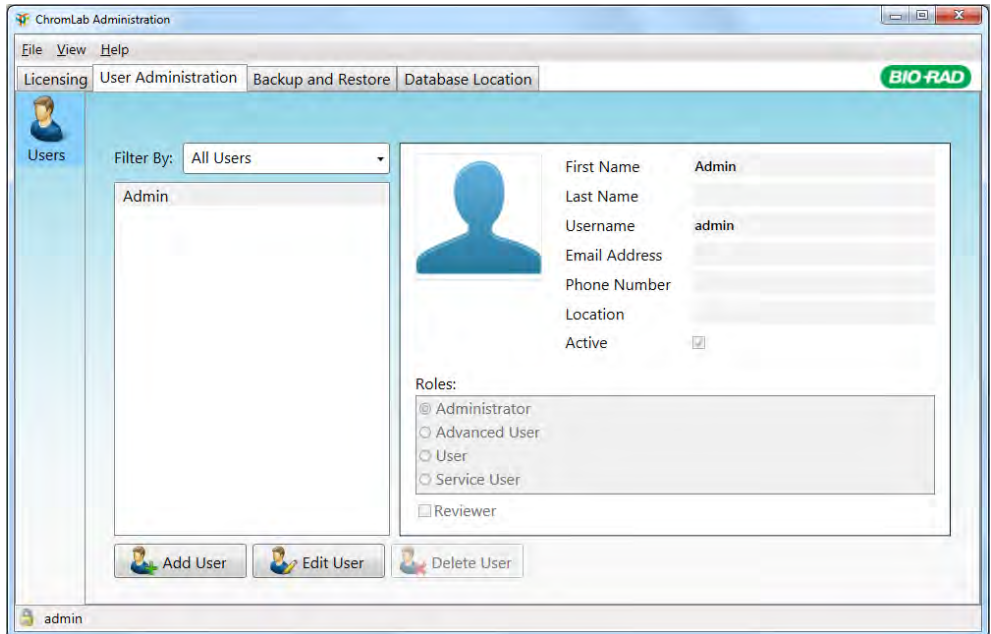
Adding User Accounts

Tip: If you have not yet done so, review the information in the section [Users and Roles on page 77](#)

Important: Each user can be assigned only one role.

To add user accounts to ChromLab

1. On the Start menu, select ChromLab > ChromLab Administration and log in as a ChromLab administrator. ChromLab Administration opens, displaying the User Administration tab.



2. Click Add User. The Add User dialog box appears.

3. Enter identifying information about the user in the text boxes.

Note: Information provided in the first name, last name, and username boxes cannot include the following characters:

"/\ [] ; | = , + * ? < >

- **First name** — required.
- **Last name** — required.

Bio-Rad recommends entering the user’s actual full name, because this name appears in the event logs as required by 21 CFR 11.50a.

- **Username** — required. The username must be unique.
- **Password** — required. The initial password can be generic. Encourage users to change their passwords after they first log in. See [Setting Password Options on page 93](#) for more information.
- **Email address**

- **Phone number**
 - **Location**
 - **Active** — by default, all user accounts are active when first created. Clear this checkbox to remove a user's access to ChromLab.
 - **Administrator** — by default, user accounts are not assigned the administrator role when first created. Select this checkbox to assign this role to the user.
4. Do one of the following:
 - Click OK. The user account is added to the ChromLab database.
 - Click Cancel to close the Add User dialog box without saving the user account to the ChromLab database.
 5. Create additional user accounts for each ChromLab user at your site.
 6. Close ChromLab Administration.

Editing a User Account

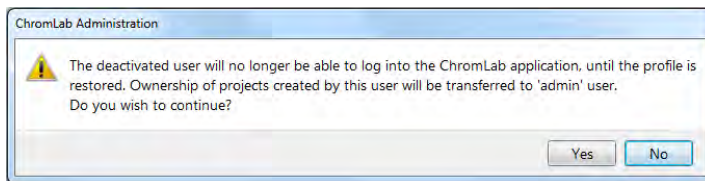
To edit a user account

1. On the Start menu, select ChromLab > ChromLab Administration and log in as a ChromLab administrator.
2. From the list of user accounts in the left pane in the User Administration dialog box, select the user account to modify.
3. Click Edit User.

The Edit User dialog box appears.

4. Do one of the following:
 - Make the required changes to the account and click OK.
 - Click Cancel to close the Edit User dialog box without saving the changes.

Note: If you clear the Active checkbox to deactivate a current user account, the following message appears:



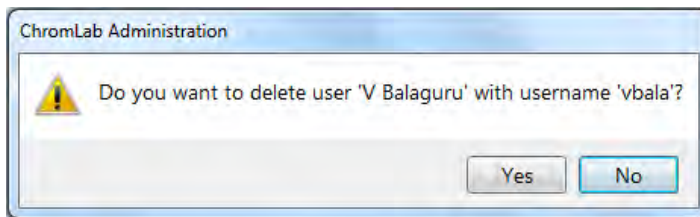
5. Click Yes to continue or No to cancel the action and close the dialog box.
6. Close ChromLab Administration.

Deleting a User Account

Note: You can delete only user accounts for which no data files are stored in the Security Edition database. That is, you cannot delete user accounts that created or modified methods, runs, or analyses. However, you can deactivate these accounts. See [Editing a User Account on page 90](#) for more information.

To delete a user account

1. On the Start menu, select ChromLab > ChromLab Administration and log in as a ChromLab administrator.
2. From the list of user accounts in the User Administration dialog box, select the user account to delete.
3. Click Delete User. A message similar to the following appears.



4. Click Yes to continue or No to cancel the action.
5. Close ChromLab Administration.

Setting Password Options in Security Edition

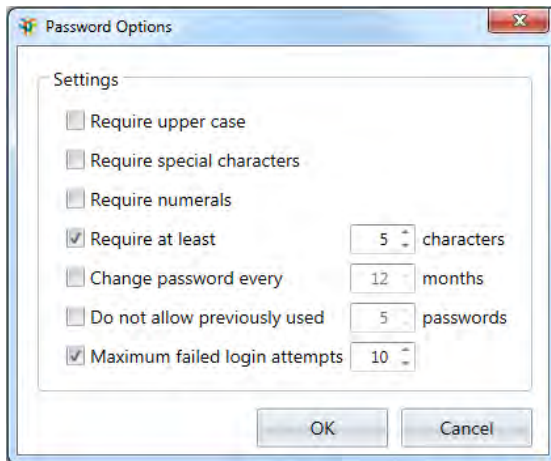
To comply with 21 CFR Part 11, Security Edition gives administrators the ability to set password options.

Setting Password Options

In Security Edition, ChromLab administrators can set password options.

To set password options

1. On the Start menu, select ChromLab > ChromLab Administration and log in as a ChromLab administrator.
2. Select View > Password Options. The Password Options dialog box appears.



3. Select the checkbox to enable the password option.
 - **Require upper case** — the password requires at least one upper case letter.
 - **Require special characters** — the password requires at least one of the following characters:

!	[
@]
%	\
&	?
*	/
(:
)	;
{	_ (underscore)
}	- (hyphen)
.	(dot)

- **Require numerals** — the password requires at least one numeral (0–9).
- **Require at least # characters** — the password requires at least the specified number of characters.
- **Change password every # months** — the password must be changed at least once every specified number of months.
- **Do not allow previously used # passwords** — ChromLab stores the specified number of passwords for the user account and prohibits their reuse.
- **Maximum failed login attempts** — the user can try the specified number of times to log in to the account with this password.

The default is five characters. You can increase or decrease the value.

The default is ten attempts. You can increase or decrease the value.

Note: If the user fails to successfully log in within the specified number of attempts, the account is locked. A message informs the user to contact the ChromLab administrator to reset the password.

4. Select or clear the option checkboxes as appropriate.

The system enforces the selected password options.

5. Click OK to save the password settings and close the dialog box.

Starting ChromLab Software Security Edition

To start ChromLab Software, Security Edition, each user must log in with a valid username and password.

To start Security Edition

1. Click the ChromLab icon to start the application.
2. In the Login dialog box, enter your username and password.
3. Click Login.

Appendix A Troubleshooting Shared Database Connection Issues

This appendix lists potential causes and suggested solutions for resolving connection issues when remote ChromLab computers or NGC instruments cannot access the shared database.

Important: Bio-Rad strongly recommends that you regularly back up the shared ChromLab database and save the backup file in a safe location. For more information about backing up the ChromLab database, see the chapter Database Maintenance in the NGC Chromatography Systems and ChromLab Software User Guide.

Possible Causes for Shared Database Connection Issues

[Table 6](#) lists possible causes and solutions for issues connecting to the shared ChromLab database.

Table 6. Possible causes and solutions for shared database connection issues

Possible Cause	Possible Solution
Database server settings have changed	<ul style="list-style-type: none"> Change the database location properties on the central computer and then reconnect each remote computer. <p>See Changing the Location Parameters of Shared Database on page 100.</p>
NGC database service is not started	<ul style="list-style-type: none"> Restart the database service on the central computer. <p>See Restarting the NGC Database Service on page 101.</p>
NGC database service fails to start	<ul style="list-style-type: none"> Uninstall and then reinstall ChromLab on the central computer. <p>See the NGC Chromatography Systems and ChromLab Software Installation Guide for specific information.</p>
	<ul style="list-style-type: none"> Uninstall SQL Server on the central computer. Then reinstall ChromLab on the central computer. <p>See Uninstalling Microsoft SQL Server on the Central ChromLab Computer on page 102.</p>
	<ul style="list-style-type: none"> Contact Bio-Rad Technical Support for assistance.
Network connection fails	<ul style="list-style-type: none"> Your site's DNS server might be down. If you connected to the central computer using its computer name, change the connection parameters to use its IP address. <p>See Changing the Connection Parameters to the Central Computer on page 104.</p>

Table 6. Possible causes and solutions for shared database connection issues, continued

Possible Cause	Possible Solution
	<ul style="list-style-type: none"> ■ Your site's firewall or antivirus tools require specific ports for network communication. SQL Server requires port 1433, which might not be allowed in your firewall environment. <p>See Appendix D, Firewall Configuration in the NGC Chromatography Systems and ChromLab Software Installation Guide for specific information.</p> <p>See Article 287932 on Microsoft's Knowledge Base site for more information: http://support.microsoft.com/kb/287932</p>
	<ul style="list-style-type: none"> ■ You removed ChromLab software from the central computer and must manually add specific firewall rules. <p>See Manually Adding Inbound Firewall Rules on page 105.</p>
	<ul style="list-style-type: none"> ■ The shared database resides on another subnet, which is not accessible from a remote ChromLab computer or an NGC system. Verify that the central computer can ping the remote ChromLab computer or NGC system using ping command line. <p>See Verifying that All NGC Systems Can Reach the Central Computer on page 23.</p> <ul style="list-style-type: none"> ■ Verify that routing between subnets or virtual local area network (VLAN) is configured properly. <p>Contact your system or network administrator for assistance.</p>

Solutions for Shared Database Connection Issues

This section details possible solutions if remote ChromLab computers or NGC systems cannot connect to the shared ChromLab database.

Changing the Location Parameters of Shared Database

If you moved the central ChromLab database to another computer, or changed the name of the computer on which it is located, you must change the connection location properties. You perform this task on the central computer through ChromLab Administration. Then you can reconnect the remote computers to the central computer.

To change the location parameters of the central computer

1. Determine the computer's name:
 - a. On the central computer, right-click the computer's desktop icon and select Properties.

The System Information screen appears.
 - b. Locate and note the computer name and full computer name.
 - c. Close the System Information screen.
2. Determine the computer's IP address:
 - a. Open a command prompt window.
 - b. At the command prompt, type **ipconfig**.
 - c. Note the information on the line IPv4 Address.

Note: Ensure that the computer's IP address is static.
 - d. Close the command prompt window.

3. Launch ChromLab Administration.

Note: If ChromLab Administration fails to connect, the Change Database Server dialog box appears. Use this dialog box to

- Change the server address
- Specify the new settings
- Provide the administrator's login credentials
- Connect to the central computer with the new settings you noted in Steps 1–2.

4. Exit ChromLab Administration.

5. On each remote computer, start ChromLab Administration and reconnect to the central computer.

For more information, see [Chapter 5, Connecting Remote Computers to the Central Computer](#).

Restarting the NGC Database Service

Important: Ensure that ChromLab is not running before you restart the NGC database service.

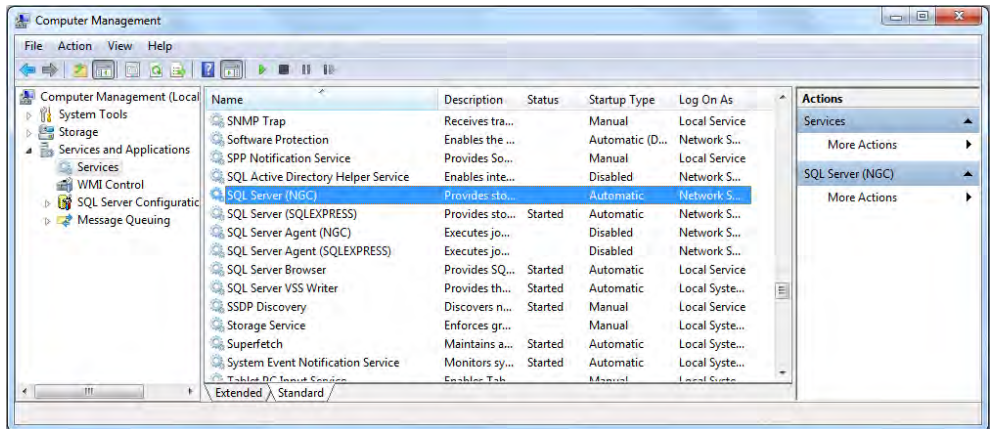
To restart the NGC database service

1. On the central computer's desktop, right-click the computer's desktop icon and select Manage.

The Computer Management dialog box appears.

2. In the Computer Management dialog box, expand Services and Applications in the left pane and select Services.

A list of services appears in the right pane.



3. In the list of services, locate and right-click SQL Server (NGC).
4. Select Start in the list of actions that appears.
5. Close the Computer Management dialog box.

Uninstalling Microsoft SQL Server on the Central ChromLab Computer

Important: You might need to uninstall SQL Server if it is corrupted. Bio-Rad strongly recommends that you back up all SQL Server databases you might have, close all applications that use SQL Server, and uninstall the applications before continuing.

To uninstall Microsoft SQL Server

1. On the central computer, uninstall ChromLab first and then uninstall Microsoft SQL Server:
 - a. Select Start > Control Panel > Programs and Features.
The Uninstall or change a program window appears.
 - b. In the list of installed programs, locate and select ChromLab.

- c. Click Uninstall/Change to uninstall ChromLab.
 - d. In the list of installed programs, locate and uninstall Microsoft SQL Server.
2. When the uninstallation is complete, locate and rename the NGC database folder.

This folder is located at C:\ProgramData\Bio-Rad\NGC\Database. Rename the folder to Database_old.
3. Reinstall ChromLab software on the central computer.

Tip: The ChromLab software installer detects that SQL Server is not installed and installs the application.
4. Activate Security Edition and designate the new database as the shared database.

For more information, see [Activating Security Edition on the Central Computer on page 29](#).
5. If you regularly backed up the original database, restore the data into the new database.
6. Do one of the following:
 - If you changed the name of the ChromLab central computer or its IP address, go to [Step 7](#).
 - If you retained the computer's name and IP address, go to [Step 9](#).
7. On all remote computers, start ChromLab Administration and select the Database Location tab.
8. Provide the required information and click Connect.
9. Start ChromLab on the remote computers and verify connection to the shared database.

Changing the Connection Parameters to the Central Computer

If you selected the central computer's name as the connection parameter when you connected to the shared database, you might need to change the connection parameter to its IP address.

Tip: Skip [Step 1](#) if you know the IP address of the central computer.

To change the connection parameters to the central computer

1. Determine the computer's IP address:
 - a. Open a command prompt window.
 - b. At the command prompt, type **ipconfig**.
 - c. Note the information on the line IPv4 Address.
Note: Ensure that the computer's IP address is static.

For more information about locating the IP address of a computer, see your system or network administrator.
 - d. Close the command prompt window.
2. On each remote computer, open a command prompt window and ping the central computer. For example:

```
> ping <Central_ChromLab_computer_IP_Address>
```

The central computer responds to the ping request if it is available on the network.

Note: See your system or network administrator if the central computer fails to respond to the ping request.

3. On each remote computer, start ChromLab Administration and select the Database Location tab.

4. In the Remote Shared Database dropdown list, select the IP address of the central computer.
5. Click Connect.
6. Start ChromLab and verify the connection to the shared database.

Manually Adding Inbound Firewall Rules

Important: If you uninstall ChromLab from the central computer, you must create custom inbound firewall rules in order for the SQL Browser and SQL Server services to receive data from the network. Contact your system or network administrator or Bio-Rad Technical Support for assistance.

- Bio-Rad NGC SQLServer NG

Enables communication to the NGC database

- Bio-Rad NGC SQLServer Browser

Publishes data about SQL Server and is used during initial connection to the database

[Table 7](#) lists the required firewall settings for these rules. Ensure that your firewall tool follows these rules for the NGC database on the central ChromLab computer or server.

Table 7. Firewall inbound rules for the ChromLab database

Rule	Program	Protocol	Local Port	Remote Port
Bio-Rad NGC SQLServer NG	Any	Any	Any	Any
Bio-Rad NGC SQLServer Browser	Any	Any	Any	Any

Tip: See Appendix D, Firewall Configuration in the NGC Chromatography Systems and ChromLab Software Installation Guide for more information.

Appendix B Configuration Checklists

This appendix comprises checklists that you can use to prepare your site for and set up the shared ChromLab database.

Preparing Your Site

Use this checklist to prepare the computers to use the shared ChromLab database.

Note: Bio-Rad recommends that you set up the shared database on a new computer and connect your existing ChromLab computers to the new database.

Table 8. Site preparation checklist

Task	For Details
<input type="checkbox"/> 1. Determine the computer to host the shared database.	
<input type="checkbox"/> 2. Verify the site requirements for the central computer.	See the NGC Chromatography Systems and ChromLab Software Installation Guide.
<input type="checkbox"/> 3. Verify the central computer meets the system requirements.	See System Requirements on page 13 .

Table 8. Site preparation checklist, continued

Task	For Details
<input type="checkbox"/> 4. Install ChromLab software on all computers.	See the NGC Chromatography Systems and ChromLab Software Installation Guide. Note: You can upgrade ChromLab software standard or Security Edition from version 3.x or higher to version 6.1. If you are running an earlier version of ChromLab software, you must first upgrade to 3.x before you can upgrade to ChromLab 6.1.
<input type="checkbox"/> 5. Prepare the ChromLab central computer and NGC systems.	See Preparing the Central Computer and NGC Systems on page 15 .
<input type="checkbox"/> 6. Prepare the remote computers.	See Connecting Remote Computers to the Central Computer on page 35 .

Setting Up the Shared Environment

Use this checklist to set up the shared ChromLab database and connect to it from the remote computers.

Table 9. Setting up the shared environment

	Task	Computer	For Details
<input type="checkbox"/>	1. Verify that ChromLab 6.1 is installed.	All computers	See the NGC Chromatography Systems and ChromLab Software Installation Guide for details.
<input type="checkbox"/>	2. Create an NGC database backup folder.	All computers	See Creating an NGC Database Backup Folder on page 37 .
<input type="checkbox"/>	3. Change the default admin password in ChromLab Administration.	All computers	See Changing the ChromLab Default Password on page 39 .
<input type="checkbox"/>	4. Activate Security Edition and designate the shared database.	Central computer	See Activating Security Edition on the Central Computer on page 25 .
<input type="checkbox"/>	5. Create ChromLab users and assign roles	Central computer	See Next Steps on page 33 .
<input type="checkbox"/>	6. (Optional) Export existing methods from all computers.	Remote computers	See Exporting Existing ChromLab Data on page 38 .

Table 9. Setting up the shared environment, continued

	Task	Computer	For Details
<input type="checkbox"/>	7. Activate Security Edition and connect to the shared database.	Remote computers	See Connecting Remote Computers to the Central Computer on page 35.
<input type="checkbox"/>	8. (Optional) Import existing methods to the shared database.	Central computer	See Importing Existing ChromLab Data on page 44.



**Bio-Rad
Laboratories, Inc.**

Life Science
Group

Website bio-rad.com **USA** 1 800 424 6723 **Australia** 61 2 9914 2800 **Austria** 00 800 00 24 67 23 **Belgium** 00 800 00 24 67 23
Brazil 4003 0399 **Canada** 1 905 364 3435 **China** 86 21 6169 8500 **Czech Republic** 00 800 00 24 67 23 **Denmark** 00 800 00 24 67 23
Finland 00 800 00 24 67 23 **France** 00 800 00 24 67 23 **Germany** 00 800 00 24 67 23 **Hong Kong** 852 2789 3300
Hungary 00 800 00 24 67 23 **India** 91 124 4029300 **Israel** 0 3 9636050 **Italy** 00 800 00 24 67 23 **Japan** 81 3 6361 7000
Korea 82 2 3473 4460 **Luxembourg** 00 800 00 24 67 23 **Mexico** 52 555 488 7670 **The Netherlands** 00 800 00 24 67 23
New Zealand 64 9 415 2280 **Norway** 00 800 00 24 67 23 **Poland** 00 800 00 24 67 23 **Portugal** 00 800 00 24 67 23
Russian Federation 00 800 00 24 67 23 **Singapore** 65 6415 3188 **South Africa** 00 800 00 24 67 23 **Spain** 00 800 00 24 67 23
Sweden 00 800 00 24 67 23 **Switzerland** 00 800 00 24 67 23 **Taiwan** 886 2 2578 7189 **Thailand** 66 2 651 8311
United Arab Emirates 36 1 459 6150 **United Kingdom** 00 800 00 24 67 23

