



# CFX Maestro Software Security Edition



**User Guide**  
Version 2.0





# **CFX Maestro Software, Security Edition**

## **User Guide**

**Version 2.0**



## **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 Laboratories, Inc.

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.

## Revision History

Document	Date	Description of Change
CFX Maestro Software User Guide, Security Edition 2.0 (catalog #10000126765)	June 2020	Ver A, Initial Release



# Table of Contents

Revision History .....	iii
<b>Chapter 1 Introduction .....</b>	<b>7</b>
U.S. FDA 21 CFR Part 11 Compliance .....	7
Finding Out More .....	7
<b>Chapter 2 Activating CFX Maestro Software, Security Edition .....</b>	<b>9</b>
Activating CFX Maestro Software, Security Edition .....	10
Managing Security Edition User Accounts .....	11
Managing Security Edition Users .....	11
Managing Security Edition User Roles .....	13
Starting Security Edition .....	14
<b>Chapter 3 Using CFX Maestro Software, Security Edition .....</b>	<b>17</b>
Using Security Edition on Bio-Rad Supported PCR Instruments .....	17
Using Security Edition on the CFX Maestro Software Computer .....	19
Secure Files .....	19
Audit Trails .....	28

## Table of Contents



# Chapter 1 Introduction

## U.S. FDA 21 CFR Part 11 Compliance

CFX Maestro Software, Security Edition provides the tools to aid CFX Maestro Software 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 CFX Maestro Software 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 CFX Maestro Software must be properly configured and administered by the CFX Maestro Software administrator(s) in your organization in order to be secure and in compliance with 21 CFR Part 11.
- Bio-Rad makes no claim that CFX Maestro 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 installing the Bio-Rad real-time PCR instruments and CFX Maestro Software, Security Edition you can access this guide as well as detailed help topics from the Help menu in any view.

You can also access the CFX Maestro Software User Guide, which describes the software's full features, by logging onto [bio-rad.com](http://bio-rad.com) and searching for catalog #10000126764.

**Note:** Click the Bio-Rad logo in the upper right corner of any CFX Maestro Software, Security Edition window to launch Bio-Rad's website. This site includes links to technical notes, manuals, product information, and technical support. This site also provides many technical resources on a wide variety of methods and applications related to PCR, real-time PCR, and gene expression.



## Chapter 2 Activating CFX Maestro Software, Security Edition

**Important:** CFX Maestro Software, Security Edition uses Microsoft Windows User Authentication to verify users' access to the software. All users who plan to access Security Edition must be able to log in to the CFX Maestro Software computer with their Windows credentials.

By default, CFX Maestro Software, Security Edition (known in this document as Security Edition) starts in standard mode. Security mode is enabled when you insert the Security Edition dongle into a USB port on the CFX Maestro Software computer. CFX Maestro Software remains in security mode until you remove the dongle.

As in standard mode, when security mode is enabled Security Edition detects Bio-Rad's supported PCR instruments and displays them in the Detected Instruments pane.

In security mode, the instruments must be connected to the CFX Maestro Software computer by USB cable. The S1000 thermal cycler must be connected to a C1000 Touch thermal cycler by USB cable.

In security mode, only the following instruments are supported:

- CFX Opus 96 and CFX Opus 384 Real-Time PCR systems
- CFX Touch and CFX Connect Real-Time PCR Detection systems
- S1000 thermal cyclers connected to a CFX Touch thermal cycler via USB cable

**Note:** CFX Maestro Software, Security Edition, 2.0 does not support the MiniOpticon or C1000 thermal cyclers.

## Activating CFX Maestro Software, Security Edition

**Important:** Activating Security Edition requires you to be a member of the Windows Administrators group on the CFX Maestro Software computer. Ensure you meet this requirement before you begin.

This procedure assumes that you have successfully installed the current version of CFX Maestro Software. See the document CFX Maestro Software User Guide for more information.

### To activate Security Edition

1. If you have not already done so, install CFX Maestro Software (known in this document as Standard Edition).
2. Connect a Bio-Rad supported PCR instrument to the CFX Maestro Software computer.  
**Note:** CFX Opus Real-Time PCR systems and CFX Touch Real-Time PCR Detection systems must be connected to the CFX Maestro Software computer by USB cable. The S1000 thermal cycler must be connected to the C1000 Touch thermal cycler by USB cable.
3. Start CFX Maestro Software and verify that the attached instruments appear in the Detected Instruments panel.
4. Shut down CFX Maestro Software.
5. Insert the supplied Security Edition dongle into a USB port on the CFX Maestro Software computer and restart the application.
6. Log in to Security Edition with your Windows credentials.

The software verifies your Windows account and starts in security mode.

After activating Security Edition, you must create a user account for each user who plans to access the software. See [Managing Security Edition User Accounts on page 11](#) for more information.

## Managing Security Edition User Accounts

In Security Edition, users log in to CFX Maestro Software, Security Edition with their Windows user name and password. The person who installed Security Edition is automatically assigned the role of CFX Maestro Software Administrator and can create and manage Security Edition user accounts and roles. All other users must be assigned a Security Edition user account in order to log into and use the software. This section explains how to manage Security Edition user accounts.

**Important:** Each user must have a Windows account and password on the CFX Maestro Software computer before you can assign a Security Edition user account and role. Users can be members of either the Windows Users group or Windows Administrators group. Members of the Windows Users group can access only their own files and folders (including Security Edition files and folders). Members of the Windows Administrators group can access the files and folders of other users on the computer (including other Security Edition files and folders). Review the Microsoft Windows Administration documentation and see your Windows system administrator for more information before creating Windows accounts.

### Managing Security Edition Users

**Tip:** Only users with the CFX Maestro Software Administrator role can create and remove Security Edition user accounts. The person who installed CFX Maestro Software is automatically assigned the CFX Maestro Software Administrator role. That person can assign the Administrator role to other users.

**Note:** In Security Edition, at least one user must be assigned the Administrator role.

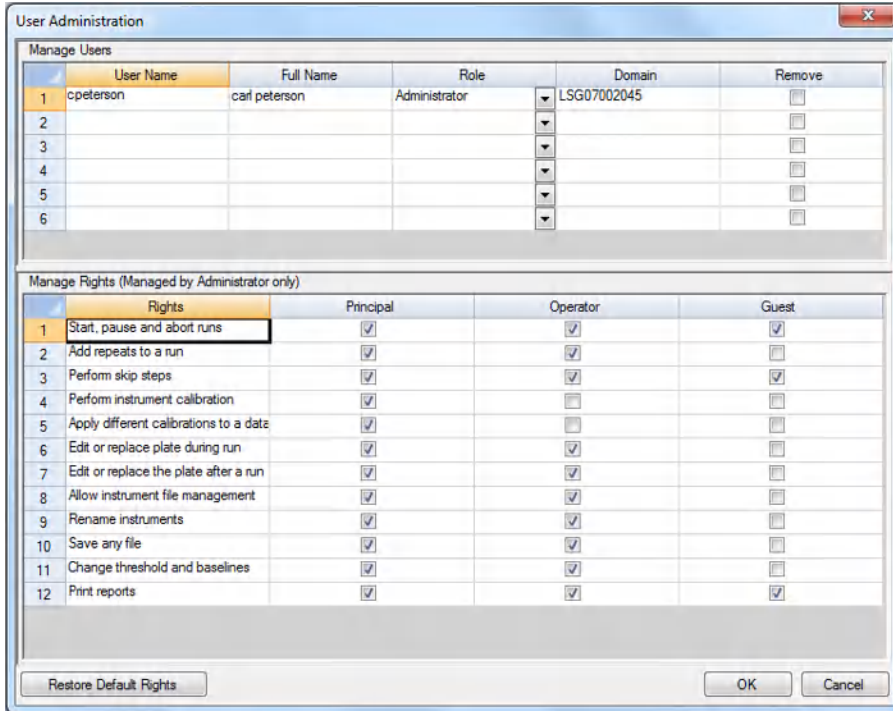
#### To add Security Edition user accounts

1. Verify that each Security Edition user is a member of either the Windows Users group or Windows Administrators group and has a Windows password on the CFX Maestro Software computer.

**Tip:** Review your Microsoft Windows Administration documentation or see your Windows system administrator for information about creating Windows users and groups and setting Windows passwords for each user.

2. Start Security Edition and log in as the software administrator.
3. In the Home window, select User > User Administration.

The User Administration dialog box appears.



- In the Manage Users section, provide the following information for each user:
  - User name** — in Security Edition, this **must** be the user's Windows login user name.
  - Full name** — the user's full name.  
This name appears in the Full User field in the audit trail.
  - Role** — the role to assign to the user.  
**Note:** You can select only one role from the dropdown list. See [Managing Security Edition User Roles on page 13](#) for more information.
  - Domain** — the Windows domain from which the user accesses the software.  
See your Windows system administrator for more information.
- Click OK and then click Yes to save changes and close the User Administration dialog box.

**To remove a Security Edition user account**

1. Start Security Edition and log in as a software administrator.
2. In the Home window, select User > User Administration to open the User Administration dialog box.
3. In the Manage Users pane, select Remove for each user you want to remove.
4. Click OK and then click Yes to save changes and close the User Administration dialog box.

**Managing Security Edition User Roles**

**Important:** Security Edition requires that at least one user be assigned the Administrator role. You can assign this role to more than one user.

Security Edition has four user roles. Each user must be assigned a role in order to access the software. Although users can be assigned only one role, you can change a user's role at any time.

The default rights for roles in security mode are the same as those in standard mode. Except for the Administrator role, you can change the rights assigned to each role. All users assigned a role inherit only the rights of that role.

By default, the rights for each role are as follows:

- Administrator — this role has all rights; you cannot change these rights.
- Principal — this role has all rights.
- Operator — this role has all rights except skipping cycles.
- Guest — this role can only read files.

When assigning roles in security mode, carefully determine the requirements for each user. For example, without the right to save, users assigned the Guest role will not be able to sign a file.

**To modify the rights for a role**

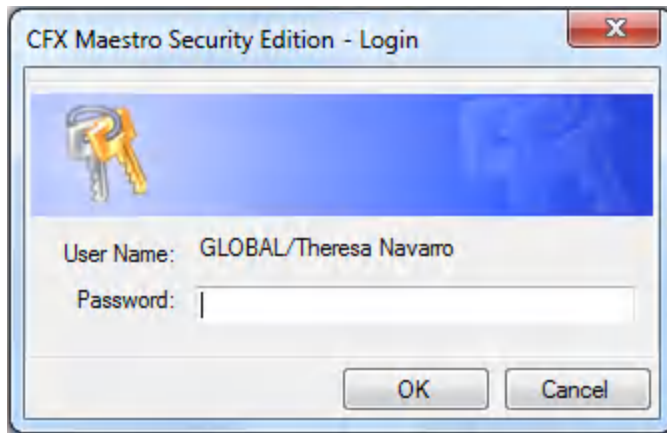
1. Start Security Edition and log in as a software administrator.
2. In the Home window, select User > User Administration to open the User Administration dialog box.
3. In the Manage Rights section, for each role clear or select the checkbox of specific rights as necessary.
4. Click OK and then click Yes to save changes and close the User Administration dialog box.

## Starting Security Edition

To start Security Edition, each user must log in with their Windows user name and password.

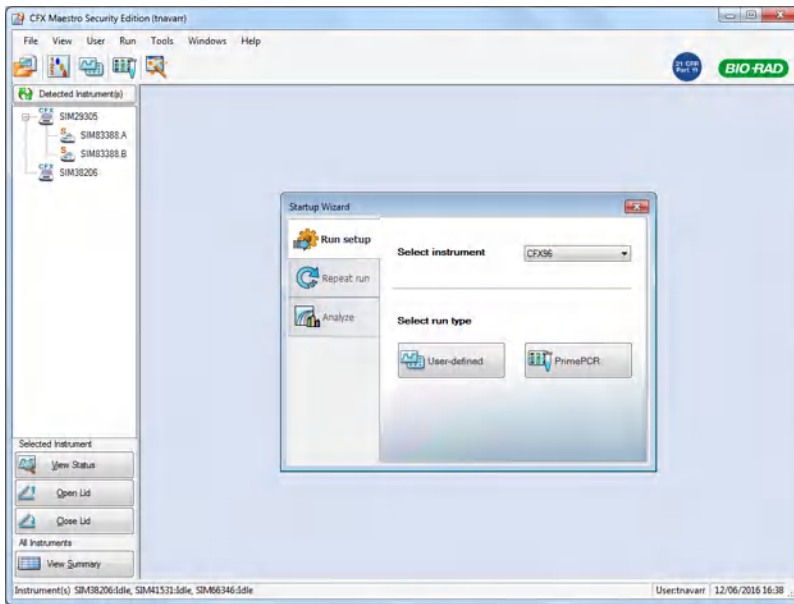
### To start Security Edition

1. Click the CFX Maestro Software shortcut icon to start the application.
2. In the Login dialog box, type your Windows password and click OK.



Security Edition opens to the Home window. The title bar displays the Windows user name of the logged in user, and the menu bar displays a blue sticker indicating the software is 21 CFR Part 11 compliant, for example:







## Chapter 3 Using CFX Maestro Software, Security Edition

When Security Edition is enabled, CFX Maestro Software remains in security mode until you remove the dongle.

**Important:** All files saved in Security Edition are marked as secure files and cannot be opened in Standard Edition.

This chapter explains how to use CFX Maestro Software, Security Edition.

### Using Security Edition on Bio-Rad Supported PCR Instruments

As in standard mode, when security mode is enabled CFX Maestro Software detects the supported instruments and displays them in the Detected Instruments pane. In security mode, only the following instruments are supported:

- CFX Opus 96 and CFX Opus 384 Real-Time PCR Systems
- CFX Touch and CFX Connect Real-Time PCR Detection systems
- C1000 Touch thermal cyclers
- S1000 thermal cyclers that are connected to a C1000 Touch thermal cycler via USB cable

In security mode, the attached instruments are locked. The touch screen displays notification that the system is under remote control.

When the instrument is under remote control, users can do the following:

- View a run in progress.
- View the instrument clock.
- View the status of the plate.
- View the curves for the current run.
- Pause the run.
- Skip a step.

- Select wells on the plate.
- Cancel a run.
- Open the lid.

When the instrument is under remote control, users cannot create plates or protocols and all runs must be initiated from the CFX Maestro Software computer to which the system is attached.

The resulting .pcrd file, which is saved directly onto the CFX Maestro Software computer, is saved as a secure data file. It can be opened only in security mode.

**Important:** The resulting .zpcr file is not saved as a secure zip file. Users can open the .zpcr file on a computer running CFX Maestro Software in standard mode and can save the .pcrd files as unsecure. Ensure that the computer is running CFX Maestro Software in security mode before opening the .zpcr and saving the data files.

#### **To retrieve the secure data file**

1. Do one of the following:
  - In the software, right-click the instrument in the Detected Instruments pane and select Retrieve Data File.
  - On the instrument, insert a USB drive into the USB port and copy the file to the drive.
2. Save the data file to a shared folder on the CFX Maestro Software computer or to your personal folder.

**Note:** Only Security Edition users with a Windows login and the appropriate role on the CFX Maestro Software computer can open the secure data file.

## Using Security Edition on the CFX Maestro Software Computer

**Important:** Security Edition uses Microsoft Windows User Authentication to verify access to secure CFX data files. Contact your Windows administrator to create an environment that complies with 21 CFR Part 11 requirements.

All features in CFX Maestro Software standard mode are available in security mode. In addition, in security mode users can do the following:

- Sign data and gene study files.
- Password protect data files.
- View and print audit trails.

This section explains these features in detail.

### Secure Files

By default, CFX Maestro Software, Security Edition saves secure files to the logged in user's personal Security Edition folder, which is located at

C:\Users\

Security Edition sets this folder to read-only. However you can share this folder and its contents with others on your team.

**Tip:** Alternatively, your Windows system administrator can create a shared folder and your Security Edition administrator can program the software to save all files to that folder.

In Security Edition, plate, protocol, data, and gene study files are marked as secure when they are saved. You can create these files in standard mode or in security mode. After they are saved in security mode, you can open these files only in security mode.

Security Edition creates an audit trail for all secure data and gene study files (.pcrd and .mgxd files, respectively). The software records all auditable activity in the file's audit trail. For more information, see [Audit Trails on page 28](#).

### Signing Secure Files

After a file is saved in security mode, users can add an electronic signature. To sign a file, the user's role must have the right (or permission) to save a file. For example, by default the Guest role does not have the right to save a file and therefore users assigned this role cannot sign a file.

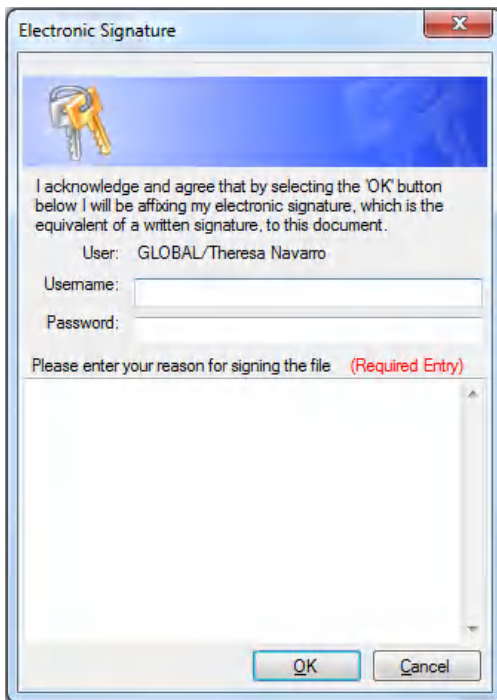
In Security Edition, signed files are not set to read-only. They can be reviewed, modified, and signed multiple times. All changes and signatures are tracked in the file's audit trail. You can sign the following file types:

- Data files (.pcrd)
- Gene study files (.mgxd)

**Note:** Files must be saved in security mode before they can be signed. If you have recently performed a run in security mode, save the resulting data file first.

### To sign a file

1. Log in to Security Edition with your Windows login credentials.
2. Open the secure data file or gene study file to sign.
3. Choose File > Sign. The Electronic Signature dialog box appears.



4. Enter your Windows user name and password and the reason for signing the file.  
The user name and reason for signing are included in the audit trail (for more information see [Audit Trails on page 28](#)).
5. Click OK to submit the signature and close the dialog box.

## Modifying Secure Files

In Security Edition, users can modify secure files, including signed and unsigned data and gene study files. The software prompts you to provide a reason for the change when you save a modified secure data or gene study file. The changes are tracked in the file's audit trail.

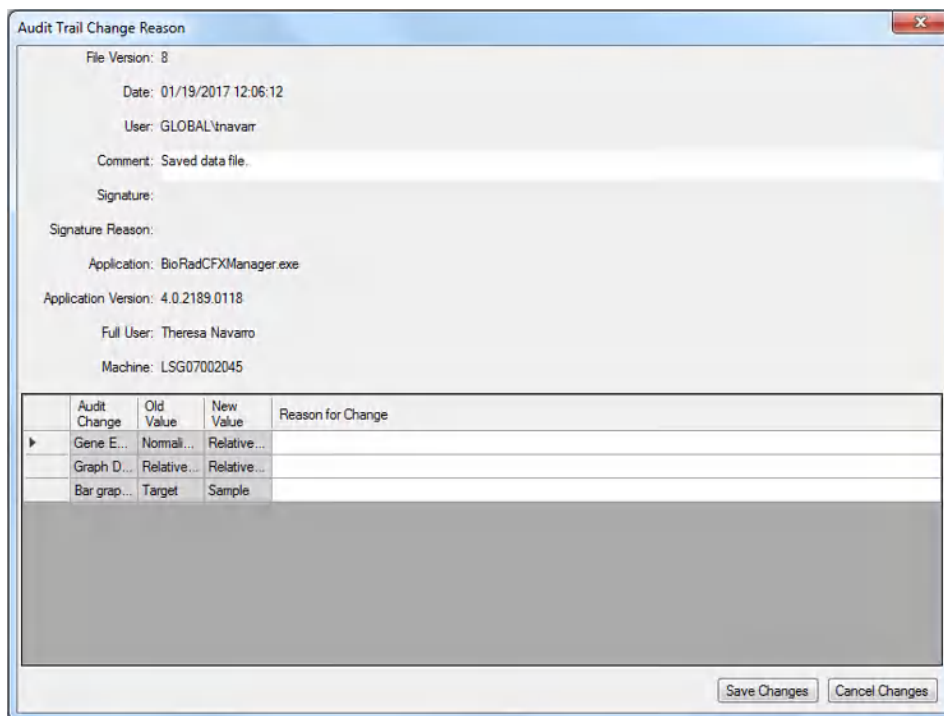
**Tip:** Because the software does not create audit trails for plate or protocol files, you are not prompted to provide a reason when you save changes to these files.

### To save a modified data or gene study file

1. Log in to Security Edition with your Windows login credentials.
2. Open and modify a secure data file or gene study file.

**Tip:** For a list of auditable activities, see [Auditable Events on page 30](#).

3. Choose File > Save. The Audit Trail Change Reason dialog box appears.



This dialog box displays the following information, which is captured in the file's audit trail header for each modification event:

- **Date** — the date on which the change occurred.
- **User** — the Windows domain and user name of the logged in user.

- **Comment** — the last saved comment.
- **Signature** — the electronic signature of the last person who signed the file.
- **Signature reason** — the reason for the signature.
- **Application** — CFX Maestro Software (appears as BioRadCFXManager.exe, which is correct).
- **Application version** — the current version of CFX Maestro Software, Security Edition.
- **Full user** — the full name of the logged in user.  
**Note:** This name appears in the audit trail.
- **Machine** — the computer on which Security Edition is installed.

The change table displays the auditable changes that occurred as a result of the modification. A brief description for the reason of the change might also appear.

**Tip:** You can add or edit descriptions in the Reason for Change column.

4. Review the list of changes. Provide detailed reasons if necessary.
5. Do one of the following:
  - Click Save Changes to save the changes to the file as well as any changes you made to the table and close the dialog box.  
  
The changes to the file and the reasons for the changes appear in the file's audit trail.
  - Click Cancel Changes to revert the file to its previous state and close the dialog box.  
  
The changes are not saved to the file and the audit trail is not updated.



## Password Protecting Secure Files

As an added level of security, Security Edition enables users to set passwords on all secure files. When setting passwords on a secure file, consider the following conditions:

Condition	Action
No password is required.	All users can open, modify, and save the secure file.
File requires the Save password.	All users can open the secure file, and users who know the Save password can modify and save the secure file.
File requires the Open password.	Only users who know the Open password can open, modify, and save the secure file.
File requires both the Open and Save passwords.	Some users can open the secure file, and a subgroup of those users can modify and save the file.

Depending on the user's role, any user can perform Save As to create a new secure file with another name or save a file with the same name in another location as long as one of the following is true:

- The secure file is not password protected.
- The user has the password to open the file.

**Tip:** The new file is saved without password protection. The original file retains its passwords.

Depending on the role, a user can modify and save the original file as long as one of the following is true:

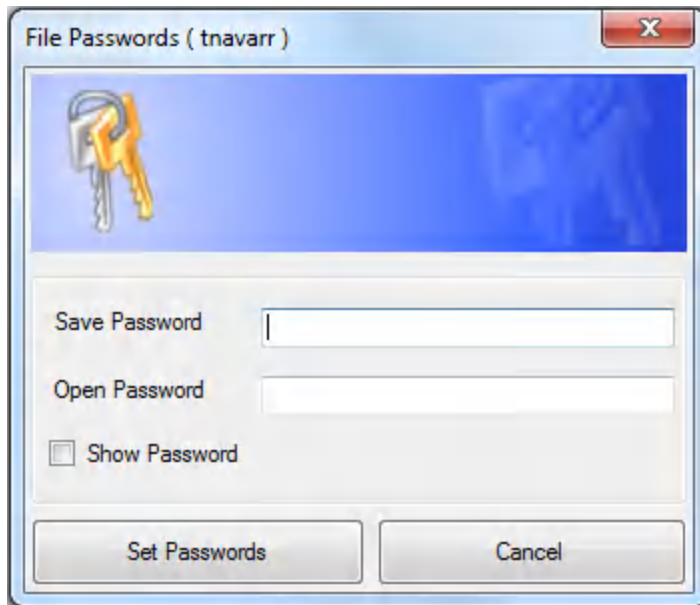
- The file is not password protected.
- The user has the password to open and the password to save the file.

**Note:** The user's role must include the right to save files in order to set passwords. For example, users with the role Guest cannot save files and therefore cannot set passwords on a file.

**Important:** Only Security Edition administrators can reset passwords.

### To password protect a file

1. Log in to CFX Maestro with your Windows credentials.
2. Open the secure file.
3. Choose File > File Passwords. The File Passwords dialog box appears.



4. Enter passwords in the Save Password and Open Password boxes.

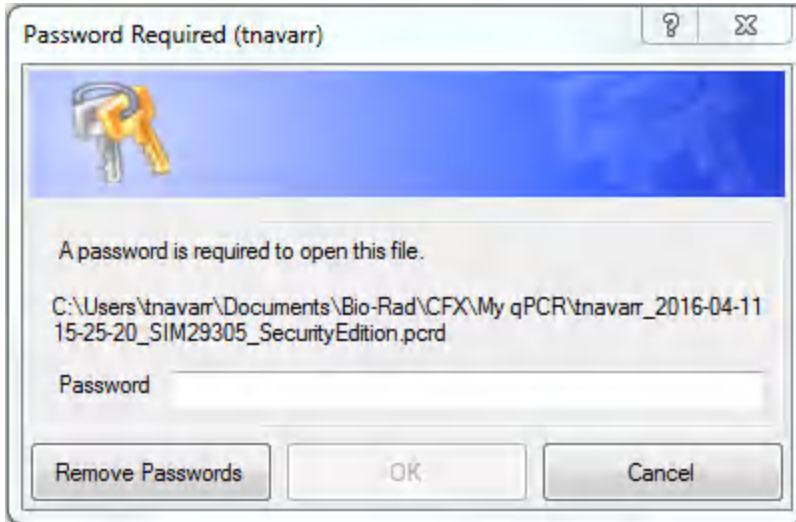
**Tip:** By default, passwords appear as asterisk characters when typed. Select Show Password to display the password as you type it.

**Important:** Passwords are case sensitive. Security Edition does not set limitations on passwords. For best practice, see your system administrator for password requirements at your site.

5. Click Set Passwords to set the passwords and close the dialog box.
6. Choose File > Save to save the changes to the file.

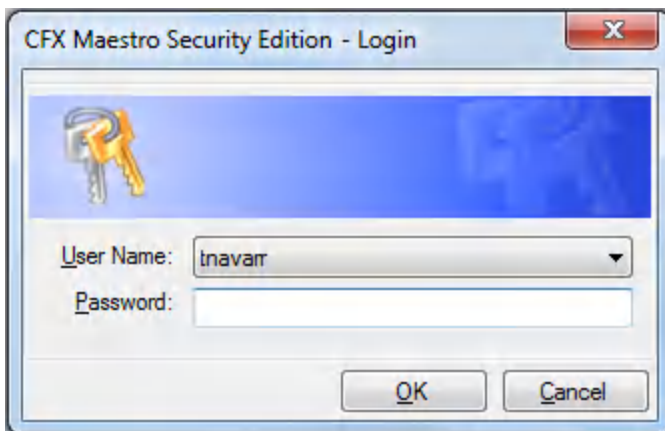
### To remove passwords

1. In the Password Required dialog box, click Remove Passwords.



**Note:** You must be a Security Edition administrator to remove passwords.

The CFX Maestro Security Edition Login dialog box appears.



2. Provide the Windows user name and password for the Security Edition administrator and click OK.

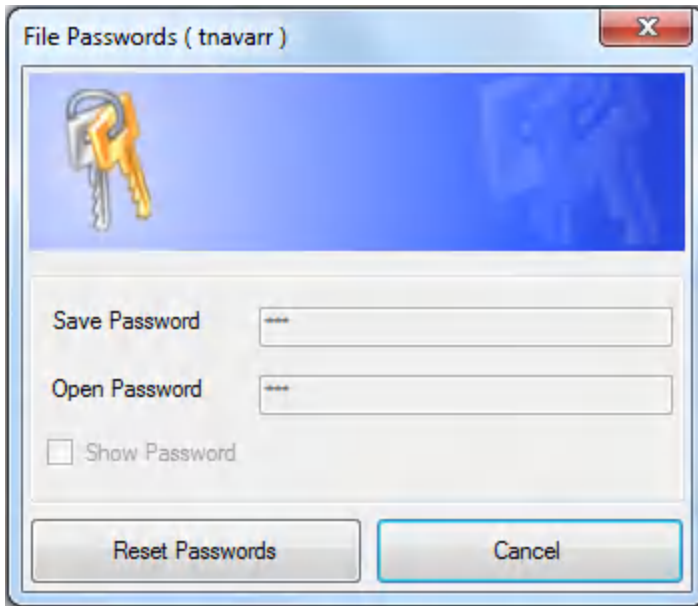
The original data file appears.

**Important:** You must save the file in order to remove the passwords.

3. Choose File > Save to save the changes to the file.

### To change passwords

1. Open the secure file.
2. Choose File > File Passwords. The File Passwords dialog box appears.

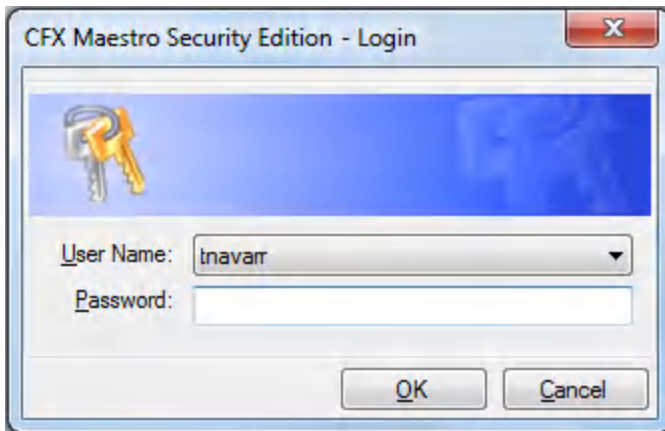


**Tip:** Save Password, Open Password, and Show Password are disabled.

3. Click Reset Passwords.

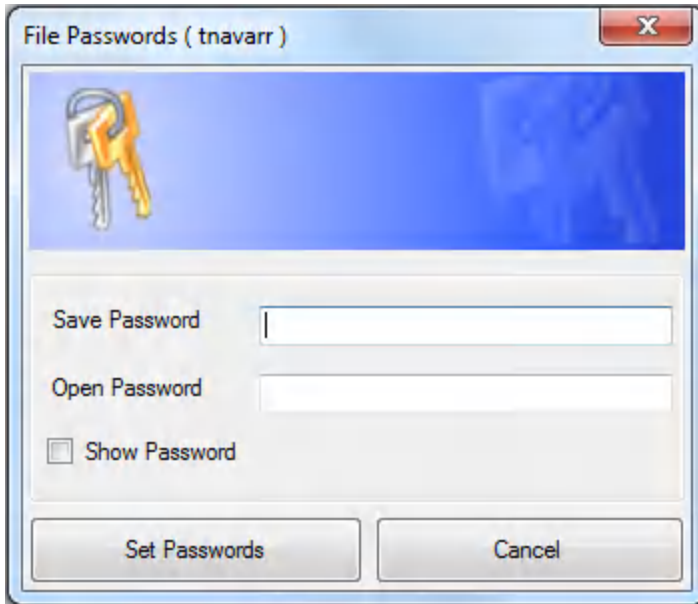
**Note:** Only Security Edition administrators can reset passwords.

The CFX Maestro Security Edition Login dialog box appears.



4. Provide the Windows user name and password for the Security Edition administrator and click OK.

The File Passwords dialog box appears.



5. Do one of the following:
  - To reset password protection, type a new password in the appropriate password box.
  - To remove password protection, clear the password boxes.
6. Click Set Passwords to save the password changes and exit the dialog box.

## Audit Trails

Security Edition creates audit trails for data and gene study files (.procd and .mgxd files respectively). Any changes made to or actions performed on secure data and gene study files are captured in the file's audit trail when the file is saved. Security Edition creates a separate audit trail for each file.

You can choose File > Save As and save secure signed or unsigned data and gene study files into another folder or with another name. The new file inherits the audit trail from the original file. The audit trail for the new file also includes the Save As activity. Changes to or actions performed on the new file are captured in its own audit trail. The original file retains its audit trail, in which further activity is captured.

[Auditable Events on page 30](#) lists the auditable events that the software captures.

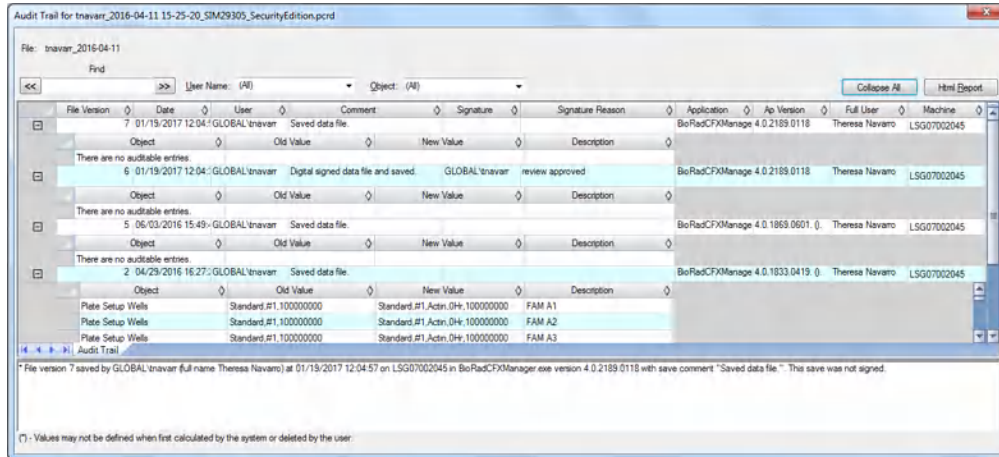
## Viewing Audit Trails

Each audit trail displays the following information:

- Audit header detail
  - File version — the saved version of the file
  - Date — the date of the current auditable event
  - User — the Windows domain and user name of the logged in user
  - Comment — the last saved comment
  - Signature — the electronic signature of the last person who signed the file
  - Signature reason — the reason for the signature
  - Application — CFX Maestro Software
  - Application version — the current version of CFX Maestro Software, Security Edition
  - Full user — the full name of the logged-in user
  - Machine — the computer on which CFX Maestro Software, Security Edition is installed
- Audit change detail
  - Object — the item that was changed (the audited item)
  - Old value — the previous value
  - New value — the new value
  - Description — the description of the change

## To view the audit trail

- ▶ In the open data or gene study file, select View > Audit Trail. The file's audit trail appears.



By default, the data are sorted by date and time, and all events appear in the expanded view. You can filter the view by user name and object, and collapse the expanded view to easily sort by any header field. You can also view the audit trail as an html report.

## To sort by user name

- ▶ Select the target user from the User Name dropdown list.

## To sort by object

- ▶ Select the target from the Object dropdown list.

## To hide the full description of events

- ▶ Click Collapse All.

## To sort data in the change detail table

- ▶ Click the diamond symbol in the data column header to perform an ascending sort (A to Z, smallest number to largest, or earliest to most recent).

## To print the audit trail

1. Click HTML Report to display the audit trail in a web browser.
2. In your browser window, do one of the following:
  - Select File > Print.
  - Right-click the report and select Print.

## Auditable Events

CFX Maestro Software, Security Edition captures the following auditable events in data and gene study files.

### Auditable events during run

- Run Start Time
- Run Time Plate edits
- Run Time Protocol edits
- Run End Time

### Auditable events when a data file is created

- Data file created
- Interpolated Plate Reads added by the system

### Auditable events when a data file is saved

- General
  - Name
  - Signing
  - Plate Setup
  - Display Wells
  - Analyzed fluorophores
  - Plate edits
  - Analysis mode
  - PCR Active Well Group
- Quantification tab
  - Active step
  - Settings —  $C_q$  Determination mode
  - Settings — Baseline Setting
  - Drift correction applied
  - Settings — Cycles to Analyze



- Settings — Analysis Mode
- Settings — Baseline Threshold
- Melt Curve tab
  - Active step
  - Peak type displayed
  - Peak analysis threshold
- End Point tab
  - Active fluorophore/target
  - End cycles to average
  - Tolerance calculation method
  - Percentage of range
- Allelic Discrimination tab
  - X- and Y-axis fluorophore
  - Select cycle number
  - View call map
- Gene Expression tab — All plots
  - Experiment Settings — Target reference
  - Experiment Settings — Sample control
  - Experiment Settings — Auto efficiency
  - Experiment Settings — Efficiency
- Gene Expression tab — Graphing
  - Analysis mode
  - Graph data
  - X-axis
  - Y-axis
  - Scaling option
  - Error bar
  - Error bar multiplier

- P-value threshold
- Gene Expression tab — Clustergram
  - Cluster By
  - Split out replicates
- Gene Expression tab — Scatter Plot
  - Control biological group (previously displayed as "Control sample")
  - Experimental biological group (previously displayed as "Experimental sample")
  - Fold change threshold (previously displayed as "Regulation threshold")
- Gene Expression tab — Volcano Plot
  - Control biological group (previously displayed as "Control sample")
  - Experimental biological group (previously displayed as "Experimental sample")
  - Fold change threshold (previously displayed as "Regulation threshold")
  - P-value threshold
- Gene Expression — Heat Map
  - Control biological group (previously displayed as "Control sample")
  - Experimental biological group (previously displayed as "Experimental sample")
  - Split out replicates
- Gene Expression tab — ANOVA
  - P-value threshold
- Plate Setup — View/Edit Plate
  - Settings — PlateType
  - Settings — Units
  - Editing Tools — Flip Plate
  - Well groups
  - Plate fluorophores
- Plate Setup — Replace Plate and Apply PrimePCR File
  - Plate Setup Import

## Audit Changes for Gene Study Files

### General

- Name
- Study Setup tab
  - Add/Remove data files
- Study Analysis tab
  - Heat map – Selected file





