

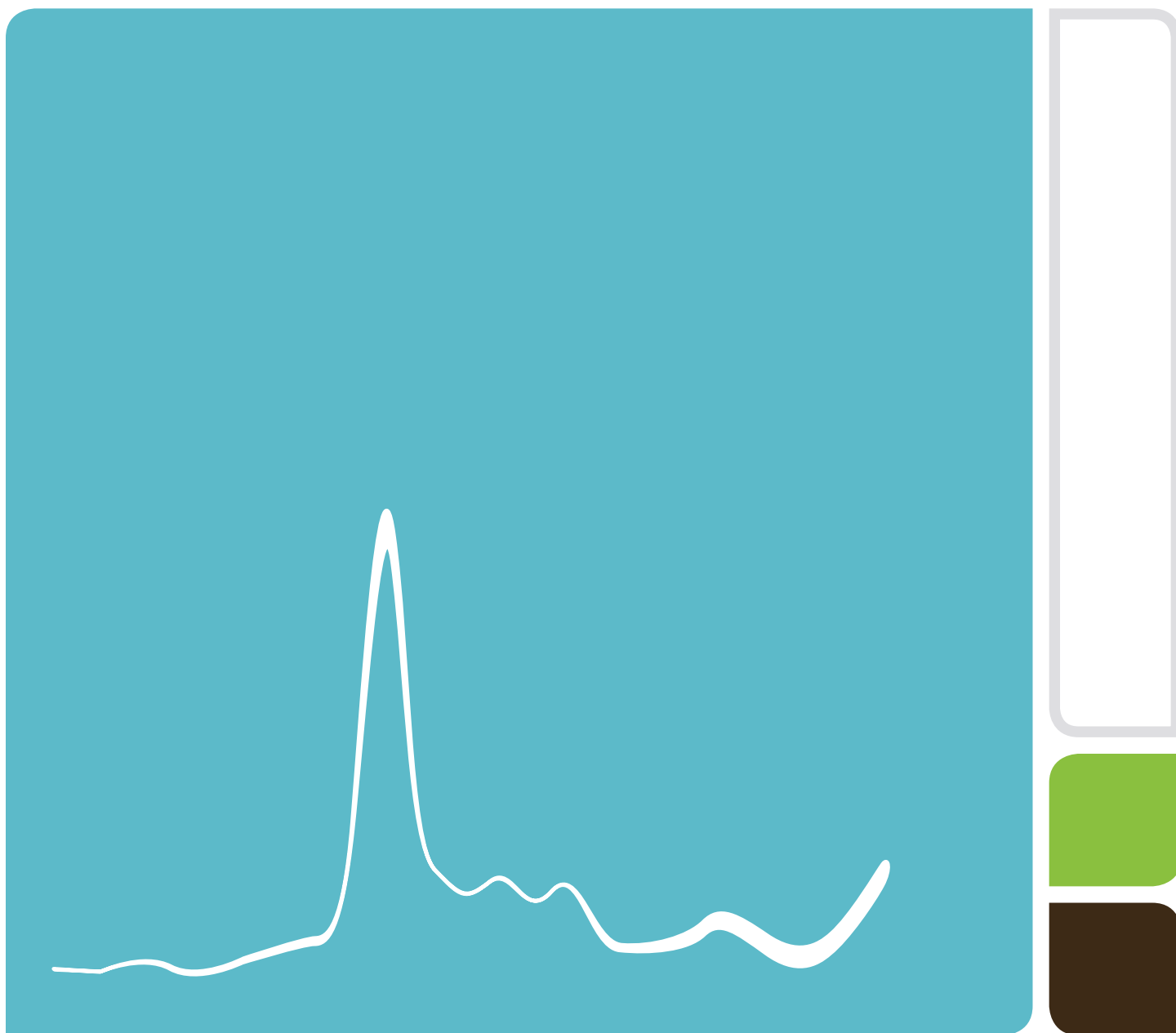


Image Lab Software
Security Edition User Guide
Version 6.1



Image Lab Software Security Edition

User Guide

Version 6.1



Legal Notices

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.

Technical Support

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

Web: www.bio-rad.com

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

For technical assistance outside the U.S. and Canada, contact your local technical support office.

Table of Contents

Chapter 1 Setting Up Image Lab Software	5
System Requirements	5
Installing Image Lab Security Edition	6
Chapter 2 Setting Up Image Lab Security Edition	11
Enabling and Disabling Image Lab Secure Mode	11
Setting Security Preferences	14
Renaming Security Groups	15
Using Groups on a Local Domain	16
Changing Security Preferences	16
Deactivating Image Lab Security Edition	17
Chapter 3 Using the Security Edition	19
21 CFR Part 11	19
ChemiDoc Touch and 21 CFR Part 11 Compliance	19
Administering Security Controls	19
Establishing Policies and Procedures for Compliance	20
Standard Mode versus Secure Mode	20
User Names, Groups, and Roles	21
Role Restrictions	22
Starting Image Lab Security Edition	23
Electronic Records	23
Unsecured Documents	23
Secure Documents	24
Modifying Secure Documents	24
Signing Documents	25
Document Logs	26
Viewing the Document Log	27
Appendix A Setting Up Users and Groups	29
User Accounts	29

Table of Contents

User Authentication and Group Membership	30
Finding Your Authentication Domain Name	31
Specifying the Domain Name	32
Configuring Users and Groups on a Local Computer	32
Configuring Users and Groups on a Network Domain	36
Password Security	38
Password Policy Setting Examples	40
Account Lockout Policy Setting Examples	40
Auditing Windows Event Logs	40
Other Security Measures	41

Chapter 1 Setting Up Image Lab Software

Image Lab Software Security Edition is available to help organizations comply with US FDA 21 CFR Part 11 regulations.

Note: The Security Edition can be installed and activated on a computer running the Microsoft Windows operating system only.

Important: To enable secure mode, Image Lab Administrator role privileges must be in place. You must create the required groups and assign the Image Lab roles to users in those groups before you install Image Lab software.

- For information on required Image Lab roles, groups, and users, see [Configuring Users and Groups on a Local Computer on page 32](#).
- For information about setting up groups, user names, and passwords, see [Configuring Users and Groups on a Network Domain on page 36](#).

System Requirements

The amount of memory required for running Image Lab depends on the size of the images you scan and analyze. Images scanned at high resolution can be quite large. For this reason, Bio-Rad recommends that you archive images on a network file server or on removable storage media.

Tip: Bio-Rad can provide an appropriate computer for use with your imaging system. Contact your local Bio-Rad representative for details.

Table 1. System requirements

System Element	Minimum Requirement
Operating system	Microsoft Windows 7 (64-bit) Microsoft Windows 10 (64-bit)
Processor	Intel Core i3 or equivalent
Hard disk space	60 GB
Memory (RAM)	4 GB

Table 1. System requirements, continued

System Element	Minimum Requirement
Ports for connecting instrument	1 USB 2.0 port
Screen resolution	1280 x 1024 or higher, 128 MB video RAM

Installing Image Lab Security Edition

Image Lab Security Edition requires you to enter a license code during installation. Before you install Security Edition, locate the 18-digit license code on the back of this user guide.

Important: Only a user assigned the role or group of Image Lab Administrator can enable and disable secure mode. A user assigned the role of Image Lab Administrator does not have to be the network or IT administrator.

To install Image Lab Security Edition on a Windows PC

1. Do one of the following:

- **To install from a USB flash drive**

Insert the Image Lab software USB flash drive into a USB port on the computer. When the contents appear, double-click the icon. Two folders appear, Mac and Windows. Open the Windows folder and double-click ImageLabSetup.exe. Go to Step 2.

- **To install from the website**

Enter the following URL into a web browser:

<https://www.bio-rad.com/ImageLab>

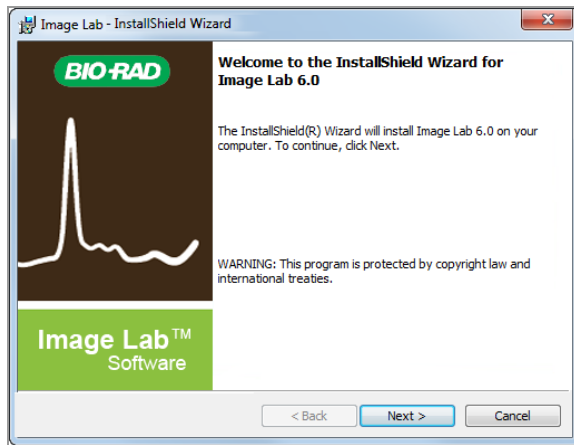
When the Image Lab page appears, click Log In/Register in the upper-right corner.

Do one of the following:

- ☐ If you have an account, enter your user name and password, and then click Sign In.
- ☐ If you do not have an account, click Register Today and complete the fields under Registration and Contact Information. When your account is verified, enter your user name and password, and then click Sign In.

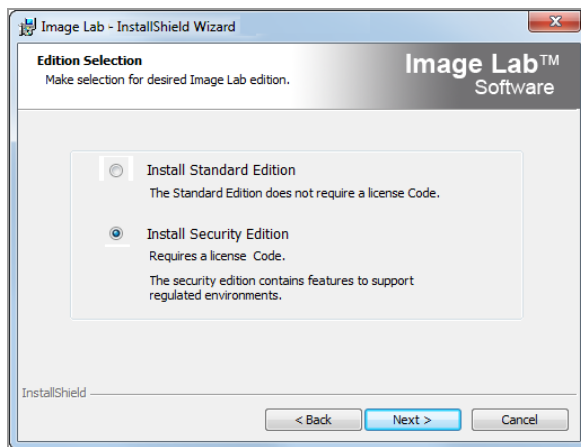
Click the Image Lab Software link, and then click Learn More. Select the Download tab, and then click the Software Download button for Image Lab Software for Windows.

The Image Lab installer wizard opens.

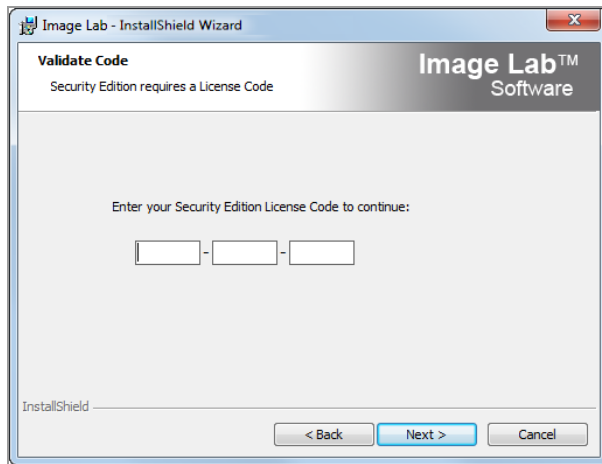


2. On the Welcome screen, click Next.
3. Accept the license agreement and click Next.

The Edition Selection dialog appears.

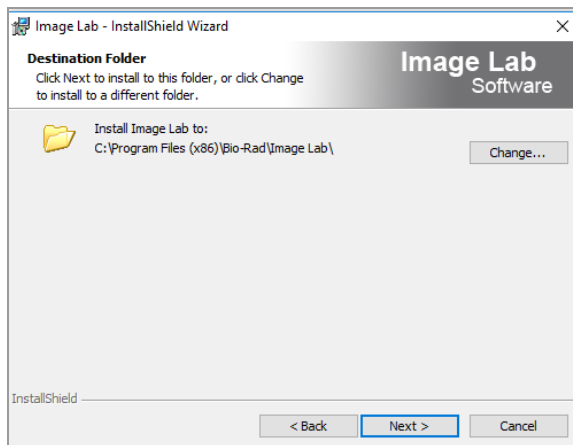


4. On the Edition Selection screen, select Install Security Edition and click Next.
5. The Validate Code screen appears.



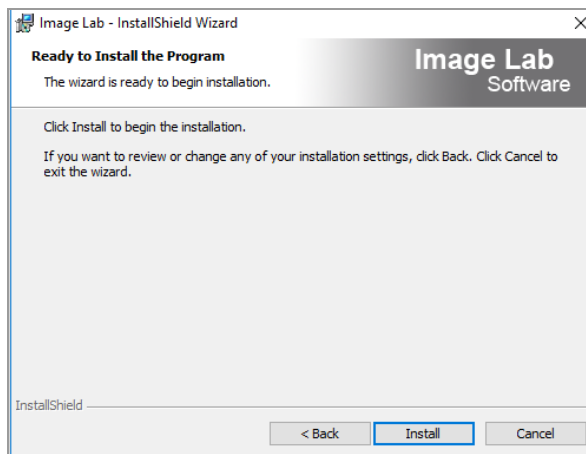
6. Enter your 18–digit license code in the Validate Code screen.
7. Click Next.

The Destination Folder screen appears.



8. Accept the default location or click Change and browse to the folder you want.
9. Click Next.

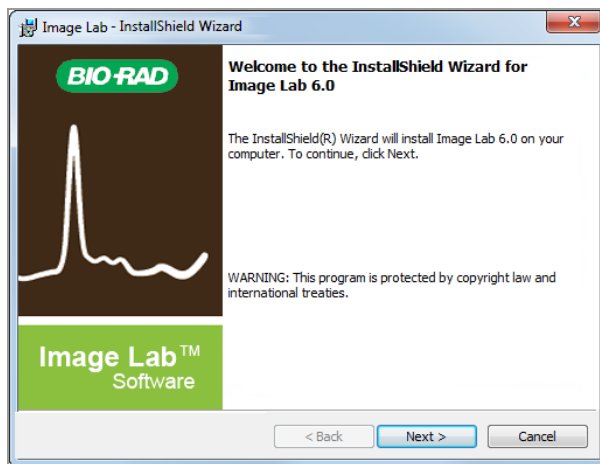
The Ready to Install the Program screen appears.



10. Click Install.

The wizard installs Image Lab.

11. When the installation finishes, a final wizard screen appears, in which you can choose to display the Release Notes, the Windows Installer log, or both.



12. Click Finish to exit the wizard.

The Image Lab icon appears on your desktop.

Chapter 2 Setting Up Image Lab Security Edition

When you install the Security Edition, a Security menu is included on the menu bar. From the Security menu, Image Lab Administrators can do the following:

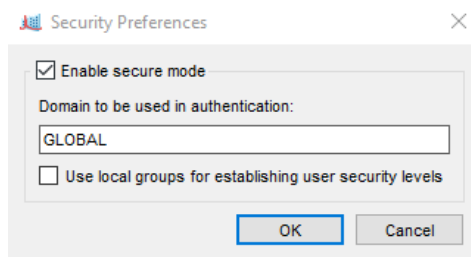
- Enable or disable Secure Mode in Security Preferences
- Rename security groups
- Enable write once support
- Deactivate Security Edition

Enabling and Disabling Image Lab Secure Mode

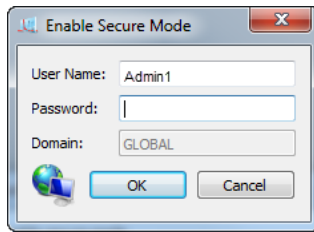
You must have Image Lab Administrator role privileges to switch between Image Lab secure and standard modes.

To enable secure mode

1. On the Security menu, click Security Preferences to display the Security Preferences dialog box.



2. Select the Enable secure mode checkbox.
3. Click OK to display the Enable Secure Mode dialog box.



4. Enter your Image Lab Administrator user name and password.
5. (Optional) If you are working on a Windows network server, type the name of the Windows domain in the Domain box.

Note: By default the name of the domain on which the current Windows user is located appears in the Domain box.

6. Click OK to save your changes.

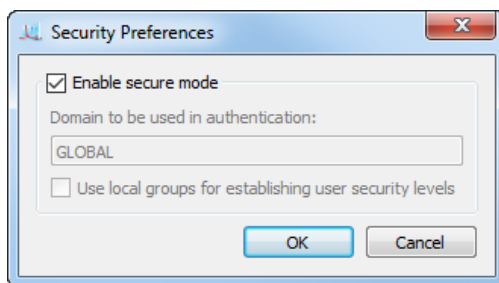
A message instructs you to restart Image Lab.

7. Click OK.

Important: For more information on setting security preferences, see [Setting Security Preferences on page 14](#).

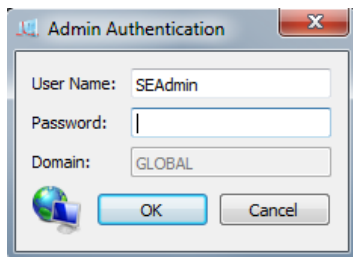
To disable secure mode

1. On the Security menu, click Security Preferences to display the Security Preferences dialog box.



2. Clear the Enable secure mode checkbox.
3. Click OK.

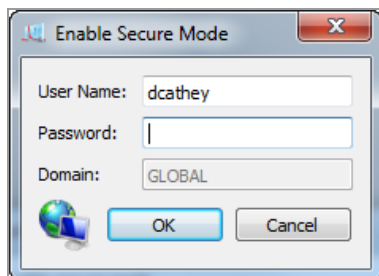
The Admin Authentication dialog box appears.



4. Enter your Image Lab Administrator user name and password.
5. Type the name of the Windows domain in the Domain box.

Note: By default the name of the domain on which the current Windows user is located appears in the box.

6. Click OK to save your changes.



A message instructs you to restart Image Lab.

7. Click OK.

Setting Security Preferences

You must know your network domain name in order to set security preferences. If you do not know this name, see [Finding Your Authentication Domain Name on page 31](#) and follow the instructions to obtain your network domain name.

To set security preferences, you specify the security settings described below.

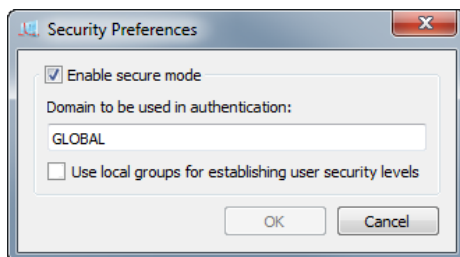
Table 2. Security preferences

Setting	Description
Network domain	A remote domain-controlling computer or system, which ensures that only authorized users with valid credentials can access and run Image Lab. Note: By default, the Security Preferences dialog box displays the name of the domain on which the current user logged in.
Local domain	Local computer on which Image Lab is running, which ensures that only authorized users with valid user credentials can access and run Image Lab.
Credentials	Valid user name and password that allows or prohibits specific user actions

To enable only network domain users to run Image Lab

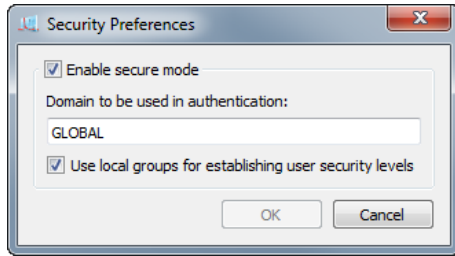
- In the Domain to be used in authentication box, enter the name of your network domain.

Leave the Use local groups for establishing user security levels checkbox unselected.



To enable only domain users who are also valid members of specific local groups to run Image Lab

1. In the Domain to be used in authentication box, enter the name of your network domain.
2. Select the Use local groups for establishing user security levels checkbox.



To enable only local users to run Image Lab

- In the Domain used in authentication box, enter the local computer name.

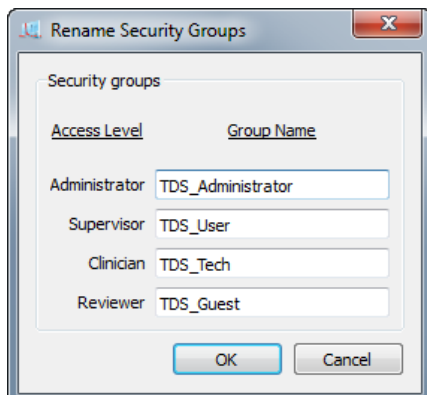
The Use local groups for establishing user security levels option becomes inactive.

Renaming Security Groups

To rename any of the default Security Groups

1. From the main menu, select Security > Rename Security Groups.

This menu option is visible only if the person logged into the local computer is logged in as a member of the Windows Administrators group.



2. Click in any of the Group Name fields.

3. Enter a new name.
4. Click OK to save your changes.

Note: The new user group name must comply with standard Windows Local Users and Groups user names rules.

For more information on setting up security groups, see [Setting Up Users and Groups on page 29](#).

Using Groups on a Local Domain

If you choose not to create or use groups on the network domain, set up local groups. Add the authorized users to the groups on the local domain. In the Security Preferences dialog box, select Use local groups for establishing user security levels.

For information about setting up users and groups for Image Lab Security Edition, see [User Names, Groups, and Roles on page 21](#).

Changing Security Preferences

Changing the domain that is used to authenticate users is a two-step process. You first authenticate on the first domain, then authenticate on the second domain. This change in domains can be performed in either of two ways. It can be performed by one individual assigned the Image Lab Administrator role on both domains, or it can be performed by two individuals, one with the administrator role on the first domain, and the other with the administrator role on the second domain. See [User Authentication and Group Membership on page 30](#) for more information about using this dialog box.

Deactivating Image Lab Security Edition

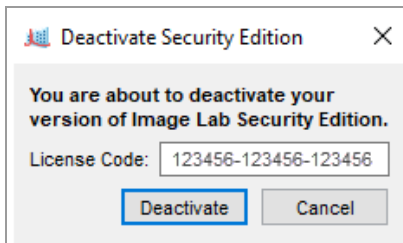
You must have a license for each instance of Image Lab that you install. You can load Image Lab Security Edition on a second computer only if you deactivate the instance on the initial computer first.

You can deactivate Security Edition using the option in the Security menu.

To deactivate Security Edition

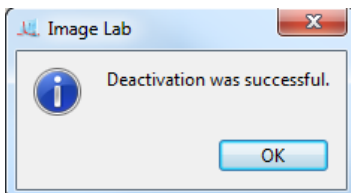
1. From the Menu bar, select Security, and then click Deactivate Security Edition.

The Deactivate Security Edition dialog box appears.



2. Click Deactivate.

Security Edition is immediately deactivated, and a success message appears.



3. Click OK.

Note: To reactivate Security Edition, you must reenter your license code.

Chapter 3 Using the Security Edition

21 CFR Part 11

Image Lab Security Edition is a module in the Bio-Rad's Image Lab software that assists users in meeting the U.S. Food and Drug Administration's regulations on good lab practices in the pharmaceutical and biotechnology industries. The Security Edition enables system administrators to ensure that Image Lab operates in compliance with Title 21 of the Code of Federal Regulations (CFR) Part 11 in 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)).

Important: Image Lab Security Edition is not supported on the Mac.

ChemiDoc Touch and 21 CFR Part 11 Compliance

The ChemiDoc Touch imaging system running Image Lab Touch Software 1.2 or earlier does not support the acquisition of images in secure mode, and any reference to the creation of secure documents does not apply.

However, Image Lab Touch, running on the ChemiDoc Touch, ChemiDoc, or ChemiDoc MP imaging systems, can export secure images but does not support signature or log viewing. Secure files exported to Image Lab Software Security Edition can be opened in secure mode and signed. Logs from these files can be viewed in Image Lab. For more information on this feature, see [Unsecured Documents on page 23](#) and [Signing Documents on page 25](#). For information about the logs that document these actions, see [Document Logs on page 26](#).

Administering Security Controls

The security controls built into Image Lab Security Edition must be properly configured and administered by the system administrator(s) in your organization in order to be secure and in compliance with 21 CFR Part 11.

Establishing Policies and Procedures for Compliance

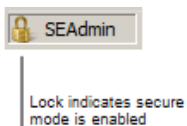
Bio-Rad makes no claim that Image Lab Security Edition software is CFR-compliant in and of itself, nor does the company guarantee compliance for the user. Your organization must establish policies and standard operating procedures that work in conjunction with the tools provided by Bio-Rad to ensure compliance with 21 CFR Part 11.

Standard Mode versus Secure Mode

Image Lab Security Edition can be run in either of the following modes:

- **Standard Mode** — in this mode, there are no restrictions on controlling the instrument, operating the software, or changing the documents.
- **Secure Mode** — in this mode, in addition to the features available in standard mode, security features are enabled, including document signing, the use of Write Once folders, and log creation.

When Image Lab is in secure mode, a padlock symbol appears in the left corner of the status bar. If no padlock is present, the software is running in standard mode.



When Image Lab is installed, by default it is set to run in standard mode. It continues to run in this mode until a user with Image Lab Administrator privileges enables secure mode. This chapter assumes you are running the software in secure mode unless noted.

User Names, Groups, and Roles

To run Image Lab Security Edition in secure mode, you must log in with a user name and password. The Microsoft Windows system administrator usually creates the user names and passwords. The Image Lab administrator defines the groups with which the Security Edition roles will be associated. There are four default roles in Image Lab Security Edition. Each role is associated with one of the four default Image Lab user groups, and each user is assigned a role that gives the user access to specific features in the software.

Note: System administrators can change the user group names, if necessary, to meet their company standards. For more information about setting up groups, user names, and passwords, see [User Accounts on page 29](#).

Table 3. Security Edition groups and roles

User Group	Image Lab Role	Description
TDS_Administrator	Administrator	Administrators can enable or disable secure mode and view log files. They do not have access to other features.
TDS_User	Supervisor	Supervisors have full access to all application features and functions and can also sign files. They cannot enable or disable secure mode.
TDS_Tech	Clinician	Clinicians can perform instrument operations and view log files and sign files. They do not have access to other features.
TDS_Guest	Reviewer	Reviewers can view log files and can also sign files. They do not have access to other features.

Role Restrictions

Your role determines which features of the security edition you have permission to use. If you attempt to perform an action that is not permitted for a user in your role, you will see an error message. In some instances the user's role determines which Security Edition features are visible and/or enabled. Therefore, you might not see all of the features described in this chapter.

[Table 4](#) lists the Image Lab Security Edition functions that each role has permission to perform.

Table 4. User access to features by role

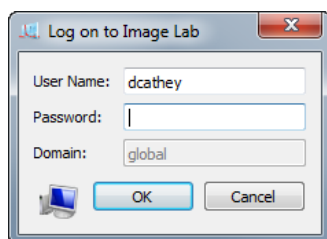
Function	Administrator	Supervisor	Clinician	Reviewer
Enable/disable secure mode	X			
View log files	X	X	X	X
Enable/disable write once support	X			
Set up and recalibrate the instrument		X		
Create new protocols		X		
Open existing protocols		X	X	X
Run protocols		X	X	
Edit protocols		X		
Create new images		X	X	
Open existing images		X	X	X
Edit images		X	X	
Analyze images		X	X	
Sign documents		X	X	X

Starting Image Lab Security Edition

When secure mode is enabled, you are prompted to log on when you start the Image Lab application.

To start Image Lab in secure mode

1. Click the Image Lab icon to start the application.
2. In the Log on to Image Lab dialog box, enter your user name and password.



3. Click OK.

Note: If you have any questions or problems logging on, see your system administrator.

Electronic Records

Image Lab Security Edition enables you to create secure electronic records as defined by 21 CFR Part 11. In Image Lab, the following are electronic records:

- Protocol files
- Image files
- Document log files
- Instrument log files
- System log files

Unsecured Documents

Note: Starting with version 2.0, Image Lab Touch exports secured documents. Information in this section does not apply to imagers running Image Lab Touch 2.0 or later.

Image files created with the ChemiDoc Touch imaging system running Image Lab Touch 1.2 or earlier are unsigned, unsecure documents. Unsecure documents remain unsecure. When you open these files in secure mode, you can make changes to these files and save them without restrictions. A

document log is generated for changes to these files, but the log is not viewable in standard mode. You must log in to secure mode to see the log.

You can also open unsecure documents in secure mode and sign them. You can make changes to these files and save them as secure documents. The original unsecure document remains unsigned and unsecure. The new document is saved as read-only with an incremental revision number and Image Lab generates an audit log. Image Lab will not be able to overwrite the secure file, but it can overwrite the original unsecure file.

Secure Documents

Until ChemiDoc Touch image files created using Image Lab Touch 1.2 or earlier are signed, they are saved as standard files. Once signed, they are they saved with the secure extension (.sscn).

Note: A secure document can be saved unsigned. Likewise, a signed document can be saved as a new, unsigned file. In this case, the saved file is still a secure document. All changes to the document are captured in the document log.

Documents created in secure mode can be signed at any time. When a secure document is signed, it is saved as read-only. Image Lab cannot overwrite the document. You can open signed documents and sign them again. The newly signed file is saved as a second revision, and the new signatures are captured in the document log.

Note: Image Lab can never overwrite a signed file.

You can open secure documents in standard mode of Image Lab. Selecting Save As in the File menu creates an unsecure file. The original file is preserved, and an entry is added to the original log that the file has been reverted to unsecure. Image Lab standard edition can modify the file. A log is generated for the new, unsecure document, and Image Lab no longer checks the file for unauthorized alterations.

Modifying Secure Documents

You can open and change a signed document in Image Lab. The original document is read-only and cannot be overwritten. Saving the revisions opens the Save As dialog box. The changes are saved into a new revision with an incremental revision number.

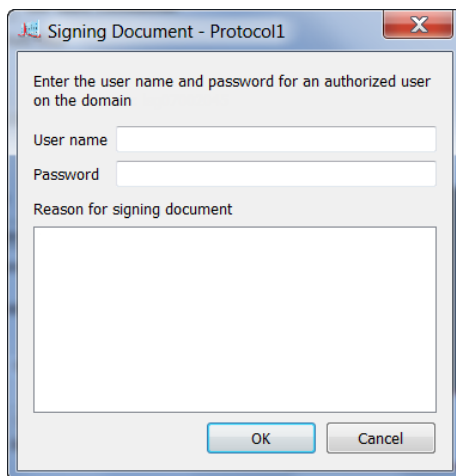
Each time a secure document is modified, you must provide a reason for *each* change before you can sign the document. The modifications are logged in the document log. The new signed document takes with it the entire history of the original document in its log.

Signing Documents

To sign a document

1. Select the protocol or results file.
2. In the Security menu, click Sign Document.

The Signing Document dialog box appears.



3. Enter the user name and password of a user authorized to sign documents.
Note: The user name and password can be for a user other than the current user.
4. Enter a reason for signing the document. Typical reasons include review, approval, responsibility, or authorship.

Note: You must provide a reason in order to sign the document.

The user name, date and time of the signature, and reason for signing are always included in the Signature History section of the image report. For information, see General Tab in the Image Lab User Guide.

5. Click OK.

A Save File dialog box appears.

6. Enter a new name for the file and click Save.

Note: Signed images are saved with an .sscn extension.

Document Logs

Changes made or actions performed on an image file generate a document log that documents each change or action. If you change a file and save it as a new file, of whether you are in secure mode or not, the document log is preserved in the new file. If you are in secure mode, the signature of the previous file is noted as part of the document log.

All major actions and changes are audited (they generate a document log). Examples of auditable actions include

- Signing a file
- Changing the image by cropping or rotating it, for example
- Modifying the analysis. For example, changing the lanes and bands or adding or editing annotations to the images

Minor changes that affect only the display are not audited, such as

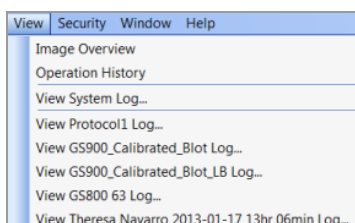
- Selecting different columns in the Analysis Table
- Changing the display options in the Lane Profile
- Annotating or labeling the image using Annotation Tools

Each change you make to a signed image file must be documented in the Reason for Change dialog box.

Viewing the Document Log

The View menu displays a list of logs for each open document. The document log captures information about editing image files. You can view the document log for any open file. This file can be a previously saved file or a newly created image file that is open on your desktop but not yet saved.

If the document was previously saved, the log is identified with its name. If the document has not been saved, the log is identified with the time stamp that shows when the document was created.



The document log includes

- Date and time
- User
- Level — security role of the user
- Type — type of event
- Description — the actual event captured
- Reason — reason for signing a document

For more information about logs, see Software Logs in the Image Lab User Guide.

Appendix A Setting Up Users and Groups

This appendix explains how to set up users and groups to run Image Lab Security Edition software in secure mode.

Note: This task requires System Administrator privileges on the client computers (and possibly their domain) on which Image Lab is installed.

User Accounts

To give users access to Image Lab, Security Edition, you can create new Windows user accounts, add existing user accounts to the four default user groups, or rename any of the four default user groups. Default user groups and roles are defined in [User Names, Groups, and Roles on page 21](#).

- A user account can have any name, but a password must be defined for the account. See [Password Security on page 38](#) for information about setting passwords for maximum security.
- Each user can belong to the Image Lab Administrator group and one other Image Lab user group.

For example, a user can belong to the Administrator group and the Supervisor group, but a user cannot belong to both the Clinician group and the Supervisor group.

User Authentication and Group Membership

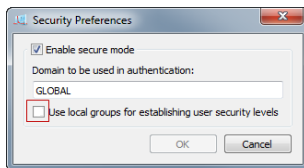
In Image Lab authentication consists of two processes: user authentication and group membership evaluation.

User Authentication

Image Lab matches (authenticates) a user name with permissions assigned to that user name on the authentication domain. The domain can reside on your local computer (a local domain) or on a network server (a network domain). If you (or your network administrator) choose a local domain to be used for authentication, you are considered a local user. If you or your network administrator choose a network domain, you are considered a domain user.

Group Membership Evaluation

Image Lab verifies that a user is a member of one or more of the four default Image Lab user groups (TDS_Administrator, TDS_User, TDS_Tech, or TDS_Guest). The valid members for each of these groups can be specified in one of two places, as defined by the Use local groups for establishing user security levels checkbox on the Security Preferences dialog box.



When this checkbox is selected, only users and groups that are defined on the local computer (on which Image Lab is installed) are recognized. When this checkbox is not selected, only users and groups that are defined on the network domain are recognized.

Finding Your Authentication Domain Name

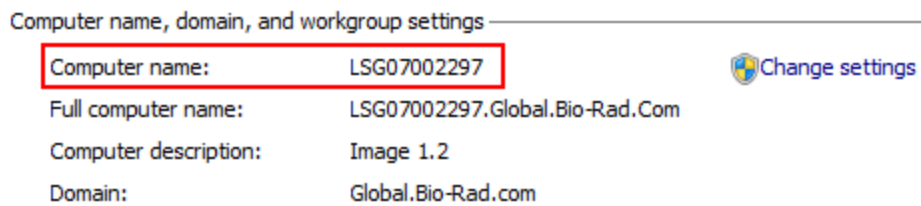
Your authentication domain can be hosted on your local computer (a local domain) or on a network server (a network domain).

To find the name of your local domain

- In Windows, open the Control Panel and click System.

The System window appears.

Under Computer name, domain, and workgroup settings, the name of your local computer is shown as Computer name.

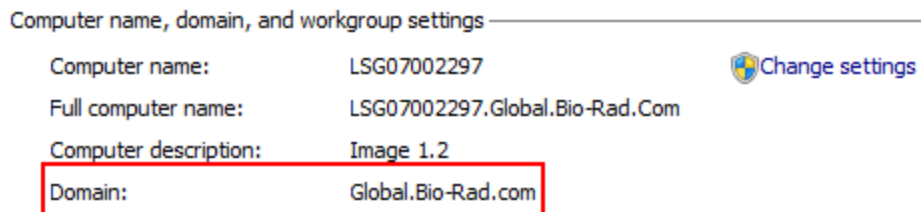


To find the name of your network domain

- In Windows, open the Control Panel and click System.

The System window appears.

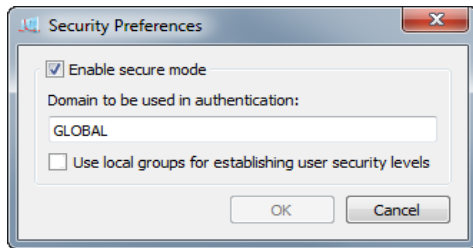
Under Computer name, domain, and workgroup settings, the name of your network domain is shown as Domain.



Specifying the Domain Name

To specify the domain name

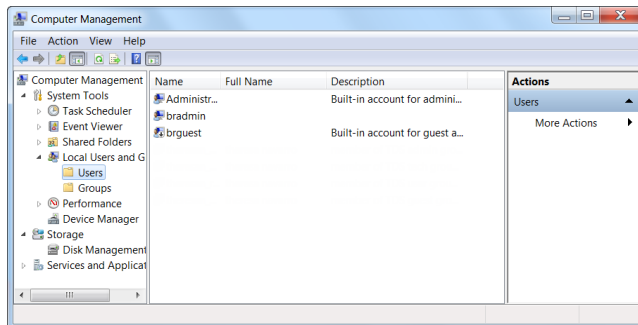
- ▶ In the Security Preferences dialog box, enter the exact name of the local computer or network server you want to designate as the authentication domain.



Configuring Users and Groups on a Local Computer

To access users and groups settings on a local computer

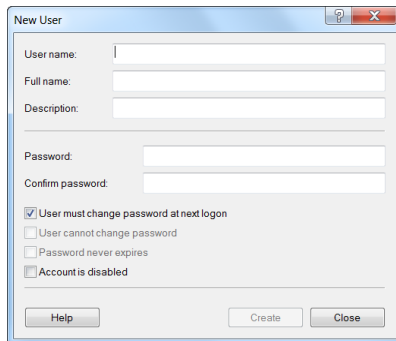
1. In the Windows Control Panel, select Administrative Tools.
2. Select Computer Management.
3. In the Computer Management window, open the System Tools folder, and then open the Local Users and Groups folder.



To create a new user on a local computer

1. Open the Users folder and click Action > New User.

The New User dialog box appears.



The 'New User' dialog box contains the following fields and options:

- User name: [Text box]
- Full name: [Text box]
- Description: [Text box]
- Password: [Text box]
- Confirm password: [Text box]
- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled
- Buttons: Help, Create, Close

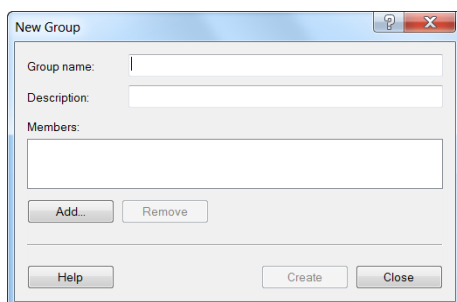
2. Enter information about the user in the following boxes:

- **User name** — must be unique.
- **Full name** — must be unique. Bio-Rad recommends using the user's actual full name, as this name will be shown in the document log and all the log reports. This is a requirement of 21 CFR 11.50a.
- **Description** — required. Bio-Rad recommends entering the user's title as the description.
- **Password** — enter and confirm a password for the user.
- (Optional) To prevent the Windows system administrator from knowing the user's password, you can select the User must change password at next login checkbox. In this case, the user must log on to Windows and change the password before using Image Lab Security Edition. Otherwise, Security Edition will not recognize the user.

To create a new group on a local computer

1. In the Computer Management window, open the Groups folder and select Action > New Group.

The New Group dialog box appears.



The 'New Group' dialog box contains the following fields and options:

- Group name: [Text box]
- Description: [Text box]
- Members: [List box]
- Buttons: Add..., Remove
- Buttons: Help, Create, Close

2. In the Group name box, enter the name of one of the following default groups: TDS_Administrator, TDS_User, TDS_Tech, TDS_Guest.

3. (Optional) Enter a description in the Description box.

The group does not need special operating-system level privileges.

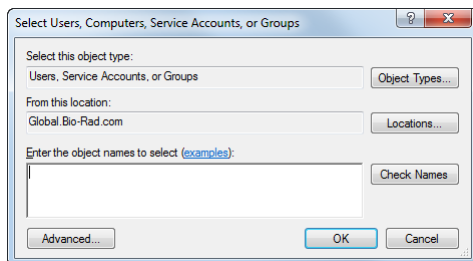
4. Click Create to save the new group.
5. Repeat steps 2–4 to create the remaining groups.

To add a user to a group on a local computer

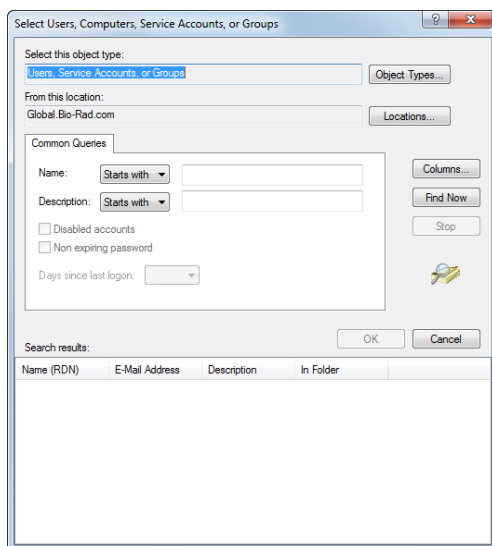
1. Do one of the following:

- In the New Group dialog box, click Add.
- In the Groups folder, double-click an existing group. In the Properties dialog box that appears, and click Add.

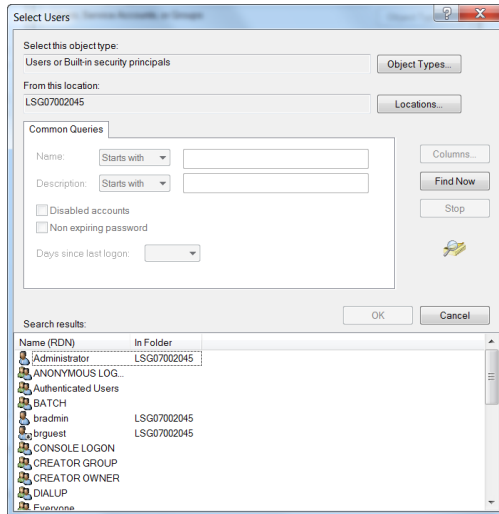
The Select Users dialog box appears.



2. Click Advanced. The Search results box becomes visible.



3. Click Find Now to populate the Search results box with the names of all local computer users.



4. To add users to the group, do one of the following:
 - Select a user name.
 - Select multiple user names: hold down the Ctrl key and select the user names you want.
5. When you have selected all the users to add to the group, do one of the following:
 - To save the users to an existing group click OK and then click OK again to close the Select Users dialog box.
 - To create the new group and save the users to it, click Create to close the New Group dialog box.

Configuring Users and Groups on a Network Domain

Note: The network administrator must know how users and groups are set up using the Windows server software at your site. The following example is used to illustrate the choices.

To locate the users and groups on a Windows server

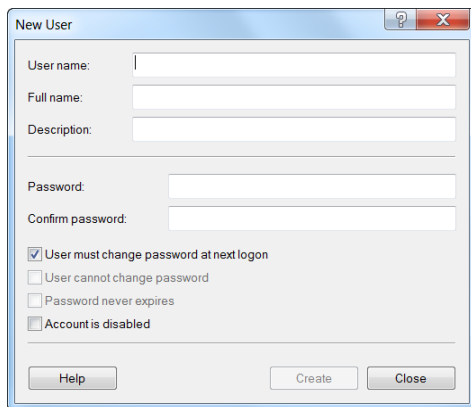
- Open Administrative Tools and select Active Directory.

Note that in the Active Directory window, the Users folder lists groups as well.

To create a new user on a Windows server

1. With the Users folder open, select Action > New User. Alternatively, use the right-click context menu.

The New User dialog box appears.



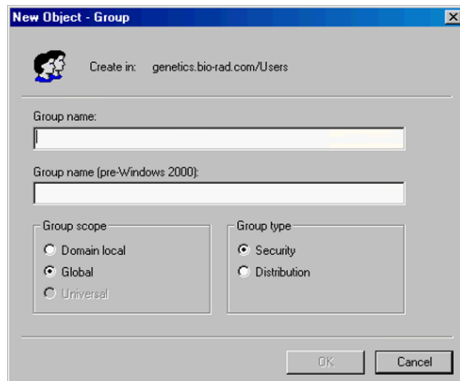
2. Fill in all the boxes:

- **User name** — must be unique.
- **Full name** — must be unique.
- Bio-Rad recommends using the user's actual full name, as this name will be shown in the document log and all the log reports. This is a requirement of 21 CFR 11.50a.
- **Description** — required. Bio-Rad recommends entering the user's title as the description.
- **Password** — Enter and confirm a password for the user.
- (Optional) To prevent the Windows system administrator from knowing the user's password, you can select the User must change password at next login checkbox. In this case, the user must log

on to Windows and change the password before using Image Lab Security Edition. Otherwise, Security Edition will not recognize the user.

To create a new group on a Windows server

1. With the Users folder open, select Action > New Group.



2. In the Group name box, enter one of the following group names: TDS_Administrator, TDS_User, TDS_Tech, TDS_Guest.

Type the name exactly as specified. You can also enter a description for the group in the Description box.

Note: The group does not need special operating-system level privileges.

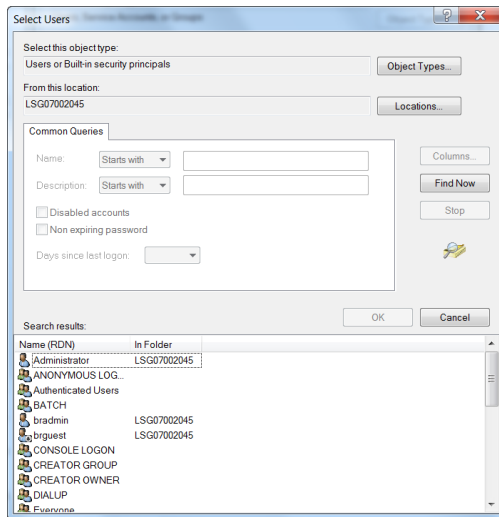
To add a user to a group on a Windows server

1. Do one of the following:
 - In the New Group dialog box, click Add.
 - Double-click an existing group in the User Manager folder to open its Properties dialog box and click Add.

The Select Users dialog box appears.

2. Click Advanced to expand the dialog box.

Appendix A Setting Up Users and Groups



3. Click Find Now to populate Search results with all user names.
4. Click a user name in the list to select it, or press the Ctrl key and click multiple users to select them.
5. When you have selected all the users to add to the group, do one of the following:
 - To save the users to an existing group click OK, and then click OK again to close the Select Users dialog box.
 - To create the new group and save the users to it, click Create to close the New Group dialog box.

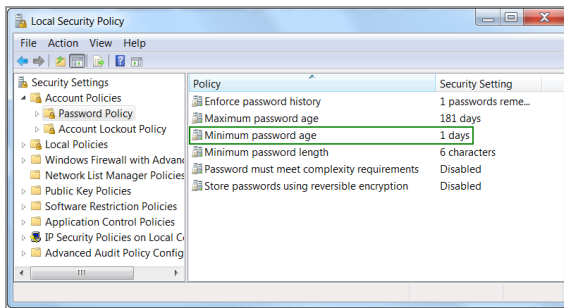
Password Security

21 CFR 11.300 (b) requires that passwords be “periodically checked, recalled, or revised.” Password policies are therefore recommended, although the password duration and rules are up to the system administrator and the organization. For instance, the exact duration between password changes is flexible.

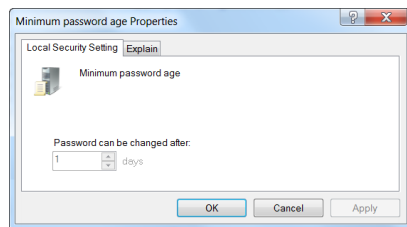
To set password policies on a local computer

1. Open the Control Panel and select Administrative Tools > Local Security Policy.
2. In the left pane of the Local Security Policy window, expand Account Policies and then select Password Policy.

Password policies appear in the right pane.



3. To change password policy settings:
 - a. Right-click the policy and select Properties to open its properties dialog box.



- b. Modify the default setting to meet your company policy.
 - c. Click Apply.
 - d. Click OK to close the Properties dialog box.
4. Close the Local Security Policy window.

To set password policies in Active Directory

1. Open the Control Panel and select Administrative Tools > Domain Controller Security Policy.
2. In the left pane of the Domain Controller Security Policy window, expand Security Settings > Account Policies and select Password Policy.
3. To change password policy settings:
 - a. Right-click the policy and select Properties to open its properties dialog box.
 - b. Modify the default setting to meet your company policy.
 - c. Click Apply.
 - d. Click OK to close the Properties dialog box.
4. Close the Domain Controller Security Policy window.

Password Policy Setting Examples

The following examples are only suggestions. Your organization should establish its own password policy.

- Enforce password history: 12 passwords remembered
- Minimum password age: 5 days
- Maximum password age: 30 days
- Minimum password length: 8 characters
- Password must meet complexity requirements: Enabled
- Store passwords using reverse encryption: Enabled

Account Lockout Policy Setting Examples

- Account lockout duration: 0 (The account is locked out until the administrator unlocks it.)
- Account lockout threshold: 3 login attempts
- Reset account lockout counter after: 30 minutes

Auditing Windows Event Logs

Some global auditing information is stored in the Windows Event logs. It is a requirement of 21 CFR Part 11 that these logs be archived. However, by default, Windows systems automatically remove these data without warning.

Note: It is therefore critical that the event log is reconfigured to generate and preserve all necessary log data. Regular manual intervention is also required to preserve these data.

To open the Event Properties Log

1. Open Administrative Tools and click Event Viewer.
2. Right-click on each log and select Properties.
3. In the section When maximum event log size is reached: select Do not overwrite events (Clear logs manually).
4. Increase the maximum size of the event log to cover any possible messages. The smaller the maximum size of the event log, the more often the system administrator must manually view, archive, and clear the system log.

Auditing information generated by the operating system is recorded in the Security Log. Logon failures in Image Lab Security Edition are recorded in this log.

During the review process, the log should be examined for attempted breaches of security, such as a series of failed login attempts. To avoid the risk of losing data, the size should be very large and this inspection/archive process should occur daily. The Audit Policy should be set as follows:

- Audit account login events — Failure should be checked at a minimum
- Audit account management — both Success and Failure should be checked
- Audit login events — Failure should be checked at a minimum
- Audit policy change — both Success and Failure should be checked

Other Security Measures

Bio-Rad recommends that you use the built-in protections that Windows Server offers in order to protect the computer while the user is absent.

Note: Microsoft continually updates its operating systems in response to security issues. It is critical to keep all components of the Windows operating system, especially domain controllers, up to date.



**Bio-Rad
Laboratories, Inc.**

Life Science
Group

Web site bio-rad.com **USA** 1 800 424 6723 **Australia** 61 2 9914 2800 **Austria** 43 01 877 89019 **Belgium** 32 03 710 53 00 **Brazil** 55 11 3065 7550
Canada 1 905 364 3435 **China** 86 21 6169 8500 **Czech Republic** 36 01 459 6192 **Denmark** 45 04 452 10 00 **Finland** 35 08 980 422 00 **France** 33 01 479 593 00
Germany 49 089 3188 4393 **Hong Kong** 852 2789 3300 **Hungary** 36 01 459 6190 **India** 91 124 4029300 **Israel** 972 03 963 6050 **Italy** 39 02 49486600
Japan 81 3 6361 7000 **Korea** 82 2 3473 4460 **Mexico** 52 555 488 7670 **The Netherlands** 31 0 318 540 666 **New Zealand** 64 9 415 2280 **Norway** 47 0 233 841 30
Poland 36 01 459 6191 **Portugal** 351 21 4727717 **Russia** 7 495 721 14 04 **Singapore** 65 6415 3188 **South Africa** 36 01 459 6193 **Spain** 34 091 49 06 580
Sweden 46 08 555 127 00 **Switzerland** 41 0617 17 9555 **Taiwan** 886 2 2578 7189 **Thailand** 66 2 651 8311 **United Arab Emirates** 971 4 8187300
United Kingdom 44 01923 47 1301

