Information Security Guidelines for HP® Z240 Workstations

For BD® Biosciences products using Microsoft® Windows® 10 Professional

23-22368-00
2/2020

Becton, Dickinson and Company
BD Biosciences
2350 Qume Drive
San Jose, CA 95131 USA

BD Biosciences
European Customer Support
Tel +32.2.400.98.95
Fax +32.2.401.70.94
help.biosciences@europe.bd.com

bdbiosciences.com
ResearchApplications@bd.com

Copyrights

Trademarks

FCC information

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTICE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his or her own expense. Shielded cables must be used with this unit to ensure compliance with the Class A FCC limits. This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numérique de la classe A respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

History

Revision	Date	Change made
23-22368-00	2/2020	Initial release

Contents

1

Introduction

This chapter includes the following topics:

About this guide

Overview

This guide provides recommendations to customers regarding security on BD Biosciences workstations. This includes use of antivirus software, management of Microsoft® Windows® user account settings, firewall settings, and removable media guidelines.

This guide applies to BD Biosciences workstations running Microsoft Windows 10 Professional.

Note: At the time of publication of this document, the testing was performed using the Microsoft Windows Microsoft Windows 10 Professional Version 1809 operating system (OS).

Who should read this guide

All IT system administrators of BD Biosciences instrument workstations should read this guide. Users who are interested in the operation of the computer workstation can read this guide to learn more about BD recommendations for maintaining a secure system.

Guide contents

This guide describes:

- Our recommendations, responsibilities, warranty, and liability regarding the installation and maintenance of virus protection software and Windows security updates and hotfixes.
- Instructions on the setup and use of third-party anti-malware software on BD Biosciences workstations.
- Our policy on the management of Windows limited user account settings on BD Biosciences workstations.
- Our policy on the management of software firewall settings on BD Biosciences workstations.
- Instructions for enabling and managing security features such as BitLocker.
- Our guidelines on the use and management of removable media on BD Biosciences workstations.
- A summary of the operating system hardening configuration applied to the system.

Where to store this guide

Store this guide near your BD Biosciences workstation for reference.

Technical support

Introduction

This topic describes how to get technical support.

Before contacting technical support

Try the following options for answering technical questions and solving problems:

- Read the section of this guide specific to the operation you are performing.
- Read topics about related information, which are listed in the *More Information* section (at the bottom of some topics).

When contacting technical support

If assistance is required, contact your local BD Biosciences technical support representative or supplier. Visit our website, bdbiosciences.com, for up-to-date contact information.

When contacting BD Biosciences, have the following information available:

- Product name, part number, and serial number
- Software application and version number
- Any error messages

This page intentionally left blank

2

Information Security Guidelines

This chapter includes the following topics:

Software policies

Introduction

This topic describes BD Biosciences software policies concerning responsibility, warranty, and liability. It also explains the testing of the information security guidelines using virus protection software.

Responsibility, warranty, and liability

BD Biosciences delivers software and workstations that are intended for running the instruments supplied by BD Biosciences. It is your responsibility to ensure that all workstations are updated with approved Windows security updates and hotfixes. It is your responsibility to install and maintain Windows security updates and hotfixes.

BD Biosciences does not provide any warranty with respect to Windows security updates and hotfixes or their compatibility with BD Biosciences products, nor does BD Biosciences make any representation with respect to the workstation remaining virus-free after installation. BD Biosciences is not liable for any claims related to or resulting from failure to install and maintain Windows security.

BD Biosciences does not provide any warranty with respect to virus protection software or its compatibility with BD Biosciences products, nor does BD Biosciences make any representation with respect to the workstation remaining virus-free after installation. BD Biosciences is not liable for any claims related to or resulting from failure to install and maintain virus protection. It is your responsibility to ensure that all electronic files (including software and transport media) are virus-free. It is your responsibility to maintain up-to-date virus protection software.

Testing

The guidelines in this document are based on tests performed with Windows Defender version 1.233.969.0. Testing of BD Biosciences software applications with enabled BitLocker features of Microsoft Windows 10 Professional were also performed. BD Biosciences cannot claim that future versions of Windows Defender virus

protection software or virus protection software from other vendors will be compatible with these guidelines.

Overview of product

Introduction

This topic provides an overview of the cybersecurity controls and third-party solutions provided by BD Biosciences with its commercial products, in this case computer workstations featuring the Microsoft Windows 10 Professional operating system. It also provides some general recommendations for maintaining the security of the computer system, the BD software applications and data produced by the instrument system.

Summary

- BD Biosciences follows the BD Corporate Product Security policy and framework adopted in 2016. The policy states BD's commitment to providing products to our customers that are designed with security and privacy as fundamental aspects of the product lifecycle. The framework establishes the key activities that align with our global product development system to continuously improve security, incorporate industry best practice, and meet our customer's expectations. These guiding elements help ensure that our products are secure by design, in use and through partnership.
- BD Biosciences has selected Microsoft Windows 10 Professional to support the HP Z240 workstation for migration from Windows 7 to the Windows 10 operating system. This version contains a variety of enhancements to Windows Defender ATP that improve security of the OS environment over previous versions.
- The BD Biosciences workstation operating system is based on Microsoft Windows 10 Professional. The operating system image is configured with security features enabled and unnecessary applications and services removed or disabled. Windows Firewall is enabled and configured to protect the connection to the instrument and close unneeded ports while

allowing for connection of the workstation to the user's local network. Depending on the BD product, additional features of Windows may be added or enabled such as time synchronization and Internet Information Services (IIS). Lastly, BD adds supporting third-party applications to the operating system such as the Adobe Reader for PDF files.

- In order to maintain operating compatibility with cybersecurity controls and solutions on BD Biosciences workstations, BD Biosciences software applications should be installed to the default application path provided during the installation process. Installing applications to a custom path on a BD workstation may cause the software to become quarantined or restricted from access by certain user accounts. BD software applications can be installed to a customized folder path for offline data analysis on user-provided computer workstations.
- Some Windows 10 standard security features are noticeably different from similar features in Windows 7 and may impact user workflows. Two examples are periodic expiration of user account passwords and enabling of the screen saver password lock with an inactivity timeout. The intention of these features is to help prevent unauthorized access due to static passwords and to reduce unintentional exposure to sensitive customer information. Please contact BD Technical Support for recommendations if these features significantly affect you.

More information

- Regarding BD's Product Security policy and framework: https://www.bd.com/en-us/support/product-security-and-privacy
- Regarding Windows 10 Professional version 1809: https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1809
- Regarding specific releases of Windows 10 through the Semi-Annual Channel: https://docs.microsoft.com/en-us/windows/release-information/

Malware protection software

Introduction

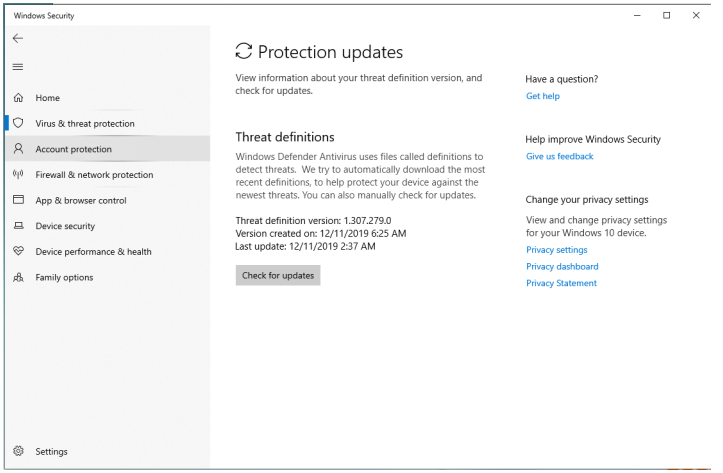
This topic provides general guidelines for BD Biosciences workstations running the Microsoft Windows 10 Professional operating system with third-party antivirus or malware protection software installed by the customer. Follow these guidelines to reduce the risk of impacting the performance and functionality of BD Biosciences software.

Installation

Windows Defender is pre-configured on BD Biosciences workstations with Microsoft Windows 10 Professional. Windows Defender is designed to work with third-party anti-malware software and should be left enabled on the workstation even if another protection solution is installed.

Updates

Products with Windows Defender enabled will be automatically updated with the latest threat definitions if the workstation is connected to a network with Internet access. The threat definition version and date of creation along with the date of the last definition update is shown on the Protection Updates page. It is also possible to manually check for threat definition updates from this page.



Scanning guidelines

Third-party malware protection software that performs virus signature-based scanning is processor intensive and could adversely affect the performance of BD Biosciences software if executing

simultaneously. Exclude the following BD folders from on-access scanning for systems running on Windows 10.

Software	Files and folders
BD FACSChorus™ software v1.3 or later	C:\Program Files\BD\FACSChorus C:\ProgramData\BD C:\Program Files\Microsoft SQL Server
BD FACSuite™ software v1.4 or later	C:\BD Import C:\BD Export C:\ProgramData\BD
BD FACSuite™ Clinical software v1.4 or later	C:\BD Import Clinical C:\BD Export Clinical C:\ProgramData\BD

Software	Files and folders
BD FACSCanto™ Clinical software v4.0 or later	C:\Program Files\BD FACSCanto Software C:\ProgramData\BD\FACSCanto C: or D: \BD\FACSCanto C: or D: \BDFACSCantoFCSFiles C:\Program Files\Java C:\Program Files\SQL Anywhere 12 C:\Program Files\BD FACSDiva Software\CST C:\ProgramData\BD\FACSDiva\CST C:\ProgramData\BD\Shared C: or D: \BD\FACSDiva\CST C: or D: \BDExport
BD FACS™ SPA software v6.0 or later	C:\Program Files\BD FACS SPA Software C:\ProgramData\BD\FACS SPA C:\BD\FACS SPA
BD FACSDiva™ software v9.0 or later	C:\Program Files\BD FACSDiva Software C:\Program Files\Java C:\Program Files\SQL Anywhere 12 C: or D: \BDDatabase C:\ProgramData\BD\FACSDiva C:\ProgramData\BD\Shared C: or D: \BD\FACSDiva\CST C: or D: \BDExport

Caution! BD Biosciences is not responsible for data corruption or loss if full-system scanning occurs while BD Biosciences software is running.

- Schedule full-system scanning when the instrument system is not in use and include all files and folders (BD files and folders as well).
- Schedule automatic updates of virus definitions during times when the instrument is not in use.
- To prevent unnecessary scanning by the on-access scanner, do not insert removable storage media or try to access information on such media while BD Biosciences software is running.

Virus detection

If the software detects a virus:

- Infected files will be moved to a quarantine folder by the protection software.
- If BD Biosciences software becomes infected, reinstall it.
- Consult your IT department about whether to delete the infected files.

BD Biosciences software installation

Temporarily disable third-party anti-malware protection software before installing BD Biosciences software, then enable it again after installation is complete.

Virus protection software upgrades

Upgrading third-party anti-malware software may cause changes in the configuration of the software and the exclusion list for on-access scanning. We recommend that you verify that the configuration settings and exclusion list have not been altered by the software upgrade.

Troubleshooting

If you follow these guidelines, but the performance and functionality of BD Biosciences software is still affected, contact your virus protection software vendor for additional software-specific guidelines.

Microsoft Windows update guidelines

Introduction

This topic describes how to manage Windows 10 updates and hotfixes on BD Biosciences workstations without affecting the performance or functionality of BD Biosciences software.

Before you begin

Contact your company's IT system administrator for the download and installation of Windows security updates and hotfixes on workstations.

Update and hotfixes policy

- Windows 10 initiates mandatory auto-updates (new features and security patches) when connected to the internet. A Defer button instructs the system to defer updates for up to two major OS update releases before Microsoft OS support expires. If the OS is within two versions of the latest, critical patches are applied automatically, even if the Defer button is enabled. Once the system is more than two OS versions out of date, it cannot load critical patches until it is upgraded to an OS within two releases of the latest version. The system continues to work even if the OS updates are expired and there is no Microsoft support.
- BD Biosciences reviews and tests newly released Windows security patches and cumulative rollups from Microsoft. Patch testing includes operation of live instruments and execution of standard product quality-control methods. Patch bulletins are published to the BD.com website and organized by product name. Patches that pass testing are indicated as whitelisted (recommended) and patches which affect product operation are blacklisted (not recommended). Patch testing is performed approximately once per quarter unless critical vulnerability patches are released by Microsoft. Security patch installation is deferred for 30 days on BD workstations to allow for priority testing of critical patches. IT administrators managing BD workstations may need to adjust their patch deployment schedule to allow for BD review.

- Your IT system administrator should test and approve the Windows security updates and hotfixes. Only download updates from an official vendor site.

Auto-update for Java

Do not enable Auto-update in Java v6. When Auto-update in Java is enabled, it will uninstall v6 and install v7, causing issues with BD FACSDiva software.

More information

- For Windows patch testing bulletins: https://www.bd.com/en-us/support/product-security-and-privacy/product-security-patches

Microsoft Windows limited-user-account settings

Introduction

This topic describes how to manage the security permission settings for Windows limited user accounts. Your company's IT system administrator is responsible for ensuring that the Windows limited user accounts have full access permissions to the settings listed in these guidelines. Recommendations for tasks that should not be delegated to limited user accounts are listed.

Limited user account settings

Pre-configured Windows limited user accounts (BDOperator) are created with a default password that expires every 60 days. New passwords must include 1 upper case, 1 lower case, 1 number and 1 symbolic character and must be at least 8 characters in length. Limited user accounts do not have rights to install software or change the OS configuration.

Security permission settings for driver files

If the workstation is connected to a BD FACSAria™ flow cytometer, the Windows limited user accounts must have full access to the following driver files.

- C:\Windows\System32\ipl.dll
- C:\Windows\System32\iplw7.dll
- C:\Windows\System32\Cpuinf32.dll

Security permission

Windows limited user accounts must have full access to the following folders:

Software	Folders
BD FACSChorus™ software v1.3 or later	C:\Program Files\BD\FACSChorus C:\ProgramData\BD C:\Program Files\Microsoft SQL Server
BD FACSuite™ software v1.4 or later	All folders and subfolders in the following: C:\ProgramData\BD\FACSuite

Software	Folders
BD FACSuite™ Clinical software v1.4 or later	All folders and subfolders in the following: C:\ProgramData\BD\FACSuite Clinical
BD FACSCanto™ Clinical software v4.0 or later	C:\Program Files\BD FACSCanto Software C:\ProgramData\BD\FACSCanto C: or D: \BD\FACSCanto C: or D: \BDFACSCantoFCSFiles C:\Program Files\Java C:\Program Files\SQL Anywhere 12 C:\Program Files\BD FACSDiva Software\CST C:\ProgramData\BD\FACSDiva\CST C:\ProgramData\BD\Shared C: or D: \BD\FACSDiva\CST C: or D: \BDExport
BD FACS™ SPA software v6.0 or later	C:\Program Files\BD FACS SPA Software C:\ProgramData\BD\FACS SPA C:\BD\FACS SPA
BD FACSDiva™ software v9.0 or later	C:\Program Files\BD FACSDiva Software C:\Program Files\Java C:\Program Files\SQL Anywhere 12 C: or D: \BDDatabase C:\ProgramData\BD\FACSDiva C:\ProgramData\BD\Shared C: or D: \BD\FACSDiva\CST C: or D: \BDExport

Security permissions for database restoration

Windows limited user accounts do not have the administrative rights required to restore the database in BD FACSDiva software. We recommend that a lab administrator or the IT group perform database restoration if needed.

Microsoft Windows firewall, Internet Information Server (IIS), and proxy settings

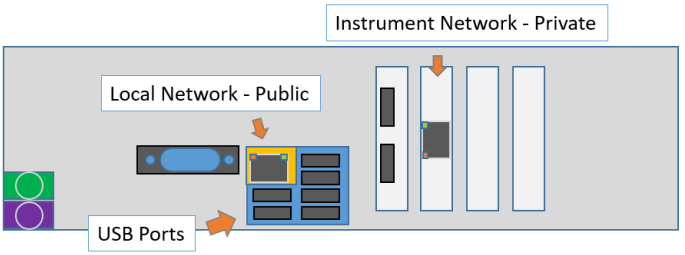
Introduction

This topic describes how to set the firewall exclusions and proxy settings for the workstation. It also discusses IIS configuration for certain BD instrument products.

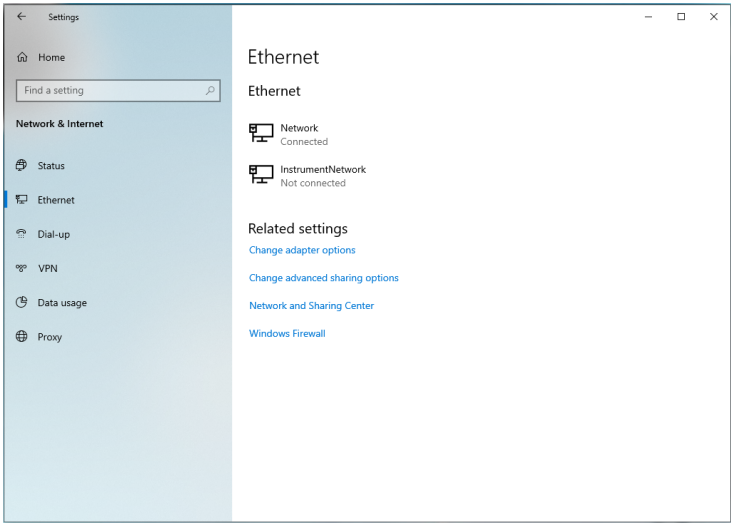
Microsoft Windows firewall settings

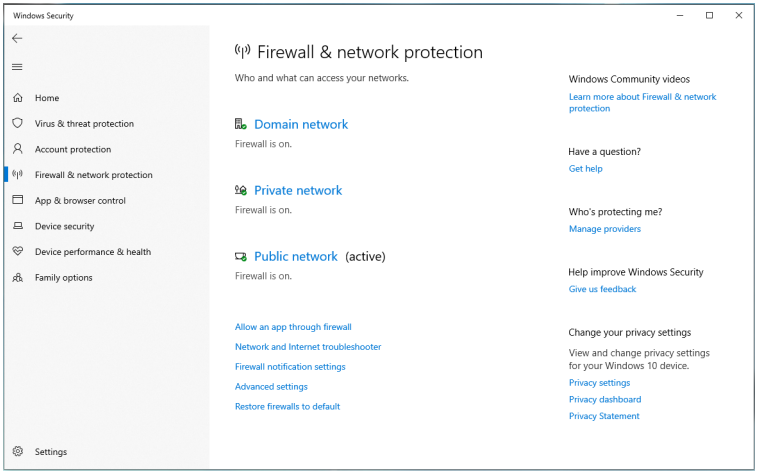
BD Biosciences workstations ship with the Windows firewall enabled and pre-configured with the necessary firewall exclusions. The workstation has two NIC physical ports, one is provided for connecting the workstation to the local network and the other is dedicated to the instrument connection. This section discusses various aspects of the networking and firewall configuration that are important to maintaining communication between the instrument and workstation.

On the HP Z240 workstation, the first RJ-45 port is located near the center of the back panel to the left of the USB port block, as illustrated in the following drawing.

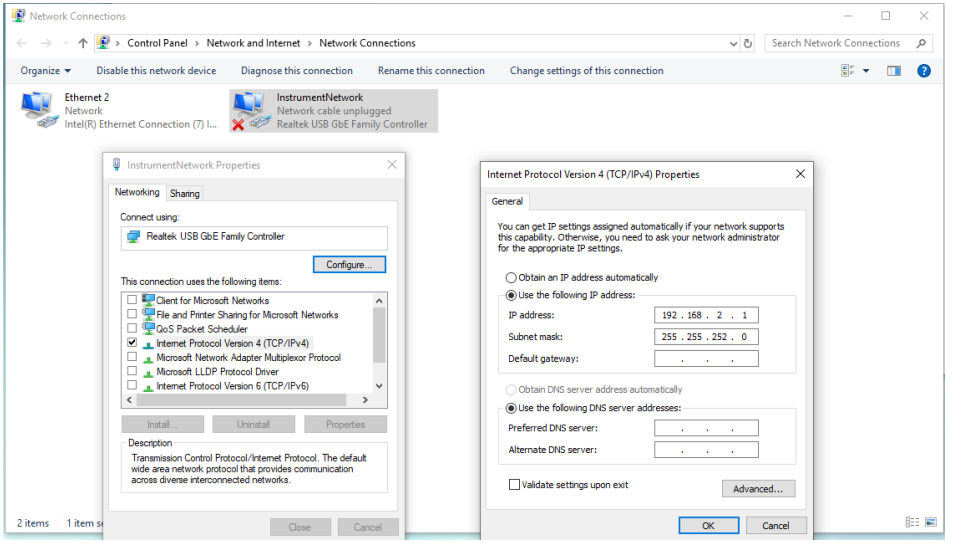


This port is intended for local network access with the firewall configured as Public. The second RJ-45 port is provided by a NIC PCI card in the second expansion slot to the right of the USB ports. This port is configured as Private in the firewall and must be used for the connection to the instrument. The first illustration shows the Ethernet connections and the second shows the Windows firewall.





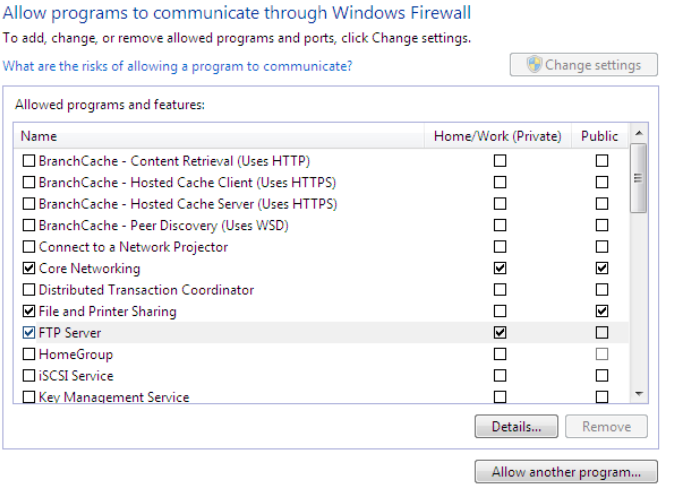
The Instrument Network interface is configured with a static IP address of 192.168.2.1 and subnet mask of 255.255.252.0 for the IPv4 protocol. This is the only protocol required for the instrument communication, the other protocols have been disabled for security.



Internet Information Server configuration

Internet Information Server (IIS) may be configured on the workstation for communication with certain instruments including BD FACSCanto, BD FACSAria, and BD FACSMelody™. The IIS configuration includes an FTP service to transfer files to the instrument for configuration and updates. For security, the FTP is configured with a static route only to the instrument NIC address and the instrument network connection is also configured to be Private as mentioned earlier. These settings are configured to prevent users from changing them through the local security policy.

The FTP Server must be allowed to communicate through the Windows firewall, however it should only be allowed to pass through the Private side of the firewall (over the instrument network connection) as shown in the following image. For security reasons the FTP Service should not be exposed on the Public side of the firewall. If the instrument fails to complete the Power On sequence, the FTP Server access through the Private side should be checked.



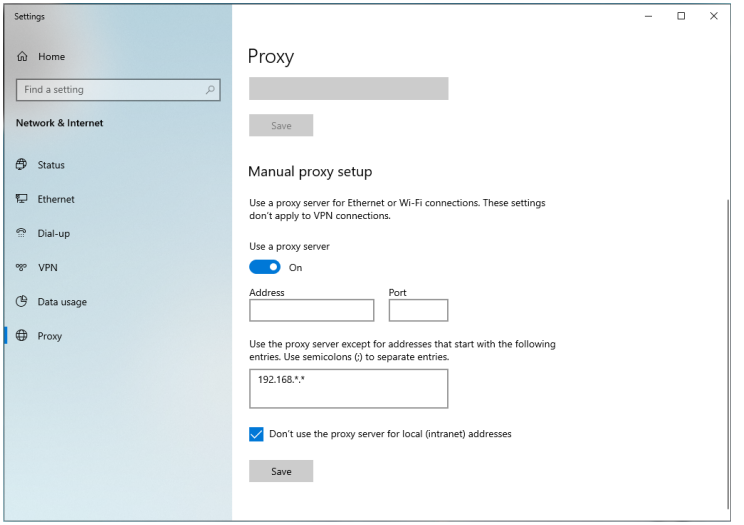
Configuring the Proxy server

If the BD Biosciences workstation is connected to an internal network, and you are using a proxy server, instrument IP requests might get directed to the proxy server. To avoid this, configure exceptions for internal instrument IP addresses.

If you do not have your proxy server or the appropriate exception configured correctly, you might not be able to access the instrument from the application.

Make sure to configure the proxy server and the exceptions in the Windows Network & Internet settings as shown in the following image.

1. In the **Exceptions** field, enter the IP address of the internal instrument network, for example 192.168.*.*.
2. Enable **Don't use the proxy server for local (intranet) addresses**.



File shares in Windows 10

Introduction

This topic provides a brief discussion on sharing files or folders in Windows 10 along with related recommendations from BD and Microsoft for maintaining workstation security. It also presents a procedure for creating a basic shared folder on BD Biosciences workstations. At the end of the topic are links to Microsoft support documentation and technical guides.

File sharing basics

While individual files can be shared in Windows 10, it is more common that specific folders will be shared to support network backups or automated data analysis. The folder can be located on the hard disk of the instrument workstation or it can be on a server or device connected to the local network. Access to the folder and the type of permissions (read /write) are managed by the folder host OS. The steps presented below illustrate the case where the folder is on the workstation, which is the arrangement sometimes used for sharing data from BD FACSCanto and BD FACS SPA systems with the BD FACSLink middleware solution.

In the case where the shared folder is located on a network device, it may be most efficient to create a mapped drive on the BD workstation to automatically reconnect to the drive after rebooting the PC. In addition, creating a drive mapping allows credentials for a different user account to be used when first opening the drive. Creating a mapped drive is illustrated in steps 9-11 of the example below.

Shared folders on Windows 7 workstations or legacy network devices may only support the Server Message Block (SMB) v1 protocol. If you observe errors when attempting to connect to a shared folder from a Windows 10 workstation, see the section on SMBv1 and legacy device support (page 34) near the end of this topic.

Creating a shared folder on the BD workstation

This example is limited to creation of a shared folder on the workstation local drive for remote access using local credentials and does not cover access of network-supported file shares or network storage devices. Access of the local file share using domain-based accounts is also not presented. This procedure can be used to share the common folder BD Export used with several BD Biosciences software applications.

Note: You must be logged into an account with local administrator rights (such as the BDAdmin account) to complete these steps.

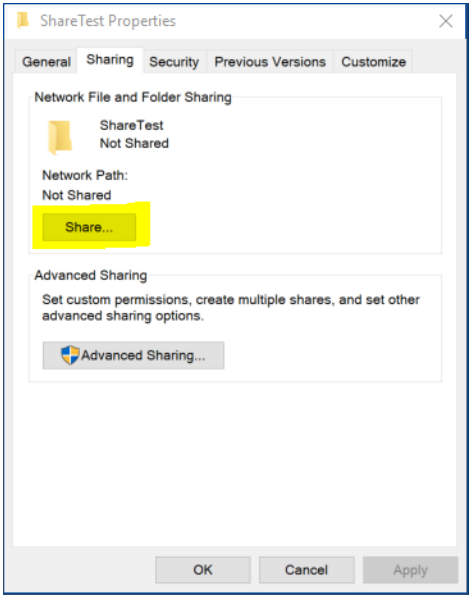
To create a local file share folder, follow these steps.

1. Before starting the procedure, determine if a new local administrator account will be used to authenticate remotely. If so, create that account now and be sure to configure the account appropriately to maintain security of the workstation. Settings such as password expiration interval should be reviewed if the account will be used by automated archiving processes, etc. In this example we named the account NewAdmin.

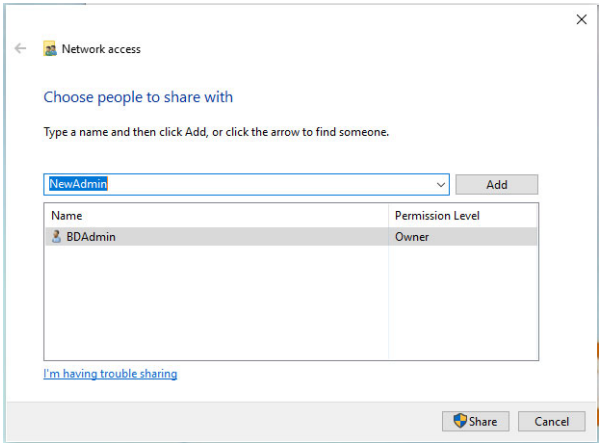
2. Local share folders should be created from the root of the C: drive (or alternatively on the D: drive if present on the workstation). In this example the folder is named ShareTest.

Note: If the shared folder is located deeper in the directory tree, folders above the shared folder may be visible or even accessible to remote users if sharing or security settings are not properly set.

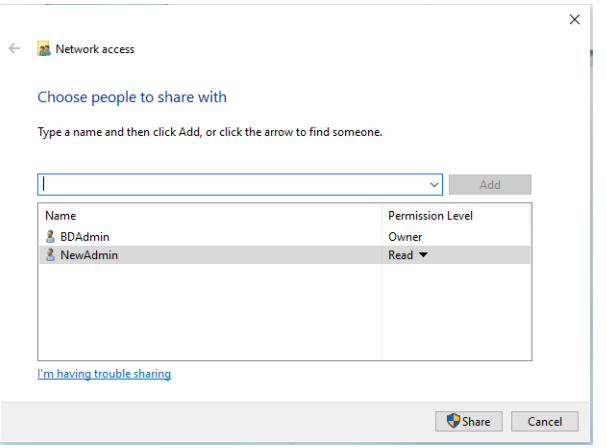
3. After creating the folder, right-click and select **Properties**. Select the **Sharing** tab and click the **Share…** button.



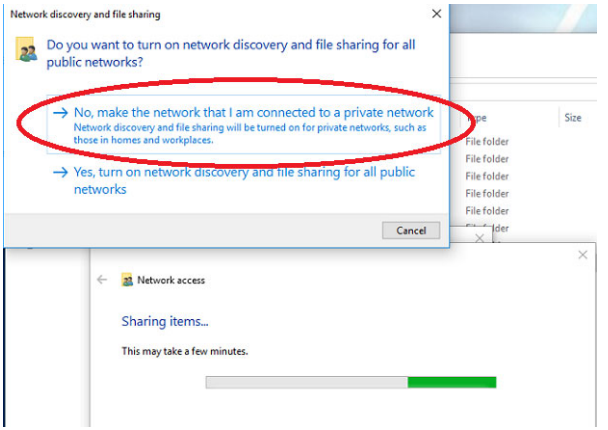
4. In the Network access dialog, enter the account name *NewAdmin* and click **Add**.



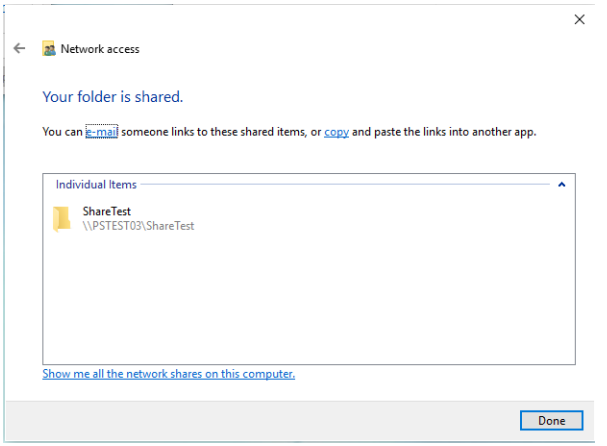
5. The NewAdmin account will appear with Read-only permissions by default. If Read/Write access is required, click the down carat to change the permission level. Click the **Share** button when done.



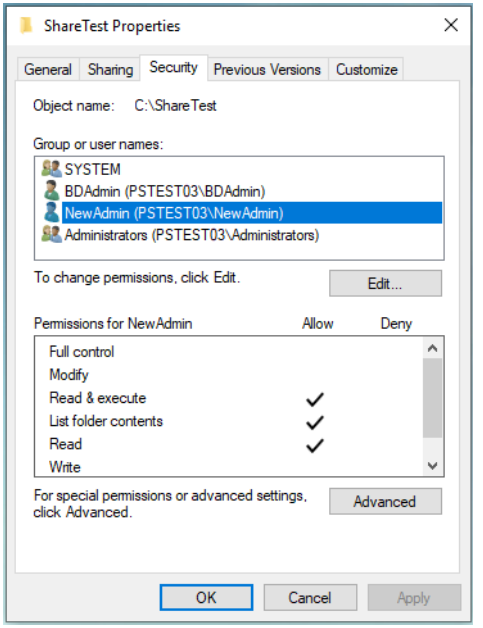
6. The Network discovery and file sharing dialog may open. Be sure to select the option to use settings for Private networks as shown below.



7. The final dialog shows the user accounts with access and the path to use when accessing the folder. Write down the exact path before closing the dialog because it is needed in the following step.

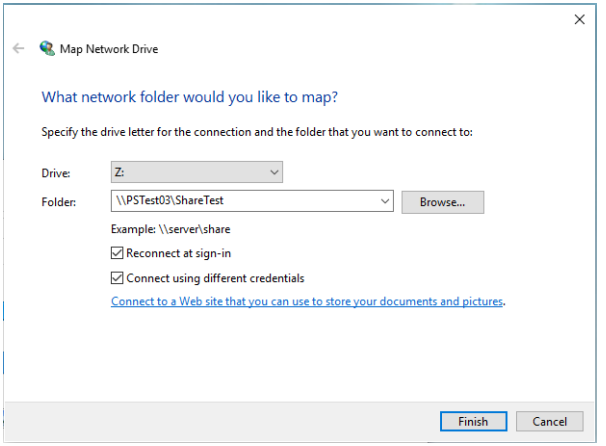


8. The new account will also appear in the Security tab of the folder properties.

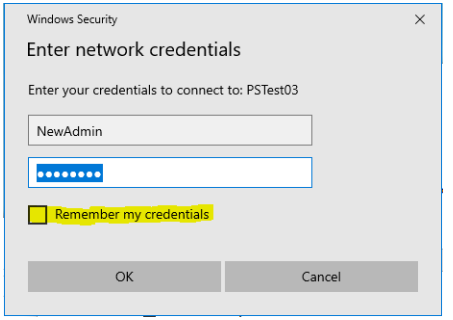


9. On the remote system, double-click the **This PC** icon to open the Explorer and select **Map Network Drive** from the Computer ribbon. Enter the folder path from the previous step

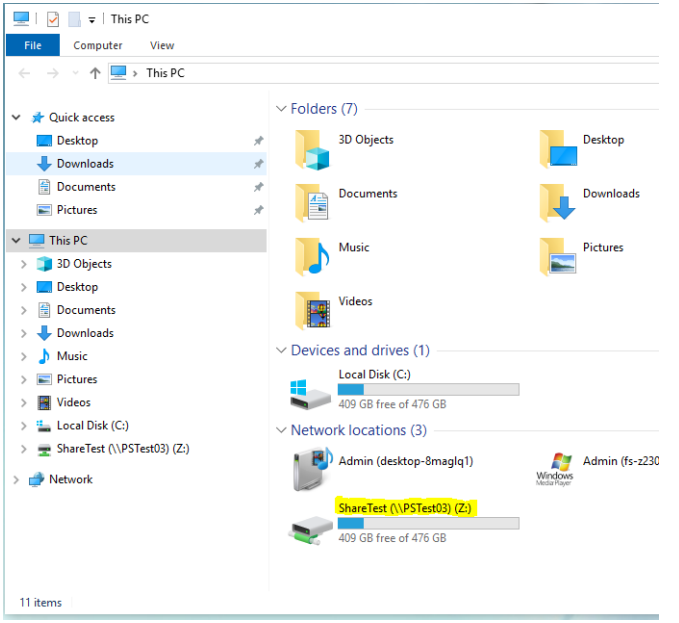
in the Folder box and check the box **Connect using different credentials**. Click the **Finish** button when done.



10. A login dialog appears to request the username and password of the account from Step 1. Optionally, you can check the box to remember the credentials.



11. The mapped drive appears in the section for Network locations.



SMBv1 and legacy device support

SMBv2 (and newer protocols) is the Microsoft recommended protocol for sharing files and folders in Windows 10 operating systems. File / Folder Shares which require SMBv1 protocol are not recommended due to known vulnerabilities with ransomware exploits. You may see various warning messages when trying to connect to devices that support only SMBv1, including 'Unspecified error 0x80004005' or 'The specified network name is no longer available'.

Microsoft deprecated the SMBv1 protocol in 2014 and strongly recommends that SMBv1 not be used. BD recommends that network-based file shares or storage devices which do not support more secure protocols be replaced or upgraded. The vendor of your device may be able to provide a firmware update for the device to support SMBv2 or newer protocols.

If you need to support for network shares that require SMBv1 protocol for access, please contact your BD Service representative for assistance or refer to the Microsoft guidance regarding SMBv1 with Windows 10 at: https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows

The Microsoft Technical Community has also published recommendations to guide users on moving away from SMBv1. Please refer to this article from the Windows Server Storage team at: https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

For general information and troubleshooting regarding file sharing in Windows 10: https://support.microsoft.com/en-us/help/4092694/windows-10-file-sharing-over-a-network

BitLocker Encryption Management

Introduction

This topic describes BD Biosciences guidelines for activating BitLocker and managing encryption keys. BitLocker is an integrated feature of Windows 10 used to secure files stored on the workstation local drive. It can also encrypt files on removable media such as USB. BD FACSChorus software was tested by enabling full-disk encryption with Microsoft BitLocker® version 2.0 for Windows 10. BD Biosciences cannot claim that future versions of BitLocker will be compatible with these guidelines.

BitLocker configuration

BD Biosciences workstations are shipped with BitLocker drive encryption disabled.

Note: You must be logged into an account with local administrator rights (such as the BDAdmin account) to complete these steps.

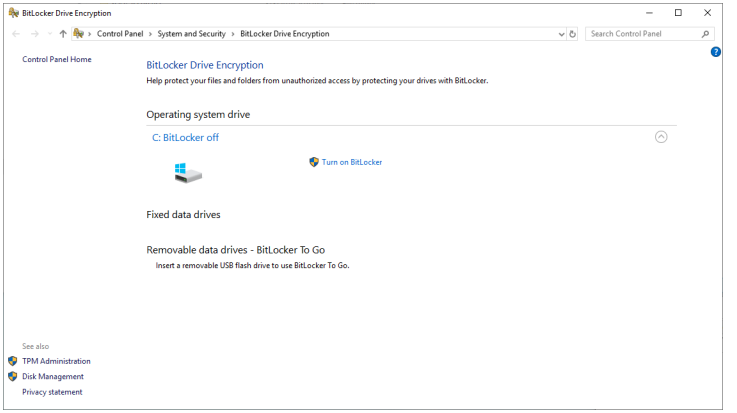
To enable BitLocker, follow these steps.

1. Before starting the drive encryption process, be sure to have a USB drive available to store the BitLocker key.

If the workstation has printer access, the key can be printed instead.

2. Click **Search** on the task bar and type *BitLocker* and select **Manage BitLocker** to open the BitLocker tool from the Control Panel.

3. Insert the USB drive and select **Turn on BitLocker** to start the setup as shown in the following image.



4. The BitLocker setup walks through several options:

   a. In **Choose which encryption mode to use**, select **New encryption mode**.

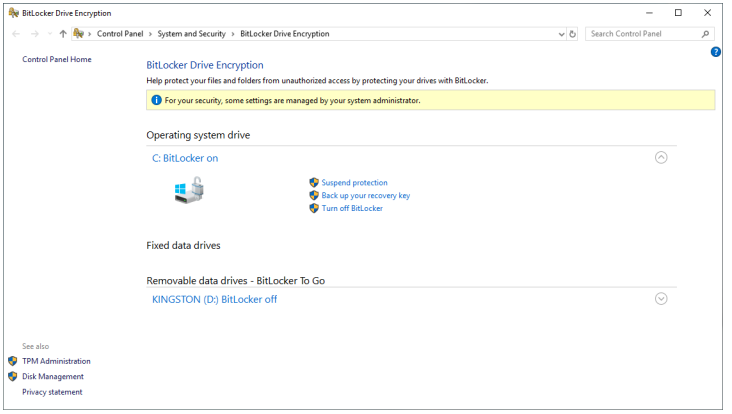
   b. In **How do you want to back up your recovery key**, select **Save to a File**. A file save dialog will open and you can select the USB drive.

   c. In **Choose how much of your drive to encrypt**, select **Encrypt used disk space only**.

5. In the last step of the setup, check the option to **Run BitLocker system check** and click **Continue** to begin the encryption process.

6. The workstation will request to reboot. Close any open applications and restart the workstation.

7. When the process is complete, the BitLocker tool will indicate the drive is encrypted and additional options will be available, including backing up the key as shown in the following image.



Note: Be sure to store encryption keys (either paper or electronic) appropriately to prevent them from being compromised.

Removable media guidelines

Introduction

This topic describes BD Biosciences guidelines for the use of removable media.

Anti-malware protection

Windows Defender is configured with on-access scanning and scheduled full-system scanning of all removable media. To prevent adverse performance of BD Biosciences software removable media, install removable media only when you are not running any BD Biosciences software.

Restricting user access

BD Biosciences workstations require the use of one or more USB ports to connect to the instrument or in some cases to back up data or configurations from the workstation. Do not disable the USB ports on your BD Biosciences workstations.

If you want to restrict users from accessing removable media on products featuring Microsoft Windows 10 Professional, follow Microsoft's recommendations to prevent users from connecting to USB storage devices. Go to support.microsoft.com.

3

Operating System hardening

This chapter covers the following topics:

Operating System hardening and other guidelines

Introduction

This topic lists the Operating System hardening measures and related security configurations applied to BD Biosciences products using Microsoft Windows 10 Professional. These settings are recommended by the Defense Information Systems Agency (DISA) as part of their Security Technical Implementation Guidelines (STIG).

For more information regarding security recommendations for operating systems, see the Defense Information Security Administration web site at http://iase.disa.mil/stigs/Pages/a-z.aspx.

Summary of STIGs applied to the OS configuration

The following content lists the STIGs by number and description.

V-14259	Printing over HTTP must be prevented.
V-26547	The system must be configured to audit Policy Change - Audit Policy Change failures.
V-15722	Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.
V-56511	The Windows Error Reporting Service must be running and configured to start automatically.
V-3470	The system must be configured to prevent unsolicited remote assistance offers.
V-36708	The location feature must be turned off.

V-26578	The Teredo IPv6 transition technology must be disabled.
V-6836	Passwords must, at a minimum, be 8 characters.
V-1097	The number of allowed bad logon attempts must meet minimum requirements, threshold at 5.
V-6840	The maximum password age must meet requirements. [60 days].
V-1098	The period of time before the bad logon counter is reset must meet minimum requirements. [15 minutes for clients].
V-1099	The lockout duration must be configured to require an administrator to unlock an account.
V-3376	The system must be configured to prevent the storage of passwords and credentials.
V-36720	The Windows Remote Management (WinRM) service must not store RunAs credentials.
V-3458	Remote Desktop Services must be configured to disconnect an idle session after the specified time period. [15 minutes].
V-3453	Remote Desktop Services must always prompt a client for passwords upon connection.
V-3457	Remote Desktop Services must be configured to set a time limit for disconnected sessions. [1 minute].

V-3454	Remote Desktop Services must be configured with the client connection encryption set to the required level.
V-26538	The system must be configured to audit Account Management - User Account Management failures.
V-26539	The system must be configured to audit Detailed Tracking - Process Creation successes.
V-57479	The system must be configured to permit the default consent levels of Windows Error Reporting to override any other consent policy setting.
V-36714	The Windows Remote Management (WinRM) client must not use Digest authentication.
V-15666	Windows Peer-to-Peer networking services must be turned off.
V-14254	Client computers must be required to authenticate for RPC communication.
V-4447	The Remote Desktop Session Host must require secure RPC communications.
V-3666	The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.
V-1107	The password uniqueness must meet minimum requirements. [8 previous passwords].
V-1105	The minimum password age must meet requirements. [1 day].

V-21952	NTLM must be prevented from falling back to a Null session.
V-26579	The Application event log must be configured to a minimum size requirement.
V-14235	User Account Control must, at minimum, prompt administrators for consent.
V-63329	Ensure that users are notified before web-based software attempts to install software.
V-63521	Error reports should be kept locally or sent to a corporate server not MS as these could potentially contain PHI.
V-63525	Error reports should be kept locally or sent to a corporate server not MS as these could potentially contain PHI.
V-63529	Error reports should be kept locally or sent to a corporate server over the correct port.
V-63497	Multiple error reports of the same error type are useful in diagnosing potential system configuration issues, as well as intrusion activity.
V-63505	Displaying error messages to users provides them the option of sending the reports. Error reports should be sent silently, unknown to the user.

This page intentionally left blank