Information Security Guidelines for HP® Z2 SFF G9 Workstations

For BD Biosciences products using Microsoft® Windows® 10 IoT Enterprise LTSC 2021

23-24247(01)
2022-09

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
23-24247(01)	2022-09	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 workstations running Microsoft® Windows® 10 IoT Enterprise LTSC (Long-term Servicing Channel) 2021 operating system (OS).

Who should read this guide

All IT system administrators and network administrators of BD 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 our recommendations for maintaining a secure system.

Where to store this guide

Store this guide near your BD 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 technical support representative or supplier. Go to our website, bdbiosciences.com, for up-to-date contact information.

When contacting BD, have the following information available:

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

2

Information Security Guidelines

This chapter includes the following topics:

Software policies

Introduction

This topic describes BD 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 delivers software and workstations that are intended for running the instruments supplied by BD. 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 does not provide any warranty with respect to Windows security updates and hotfixes or their compatibility with BD products, nor does BD make any representation with respect to the workstation remaining virus-free after installation. BD is not liable for any claims related to or resulting from failure to install and maintain Windows security.

BD does not provide any warranty with respect to virus protection software or its compatibility with BD products, nor does BD make any representation with respect to the workstation remaining virus-free after installation. BD 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 CylancePROTECT® versions 3.0.1000.25 (on applicable systems) and Windows® Defender versions 1.371.16.0 (antivirus) and 4.18.2205.7 (client). Testing of BD software applications with enabled BitLocker and AppLocker features of Microsoft® Windows® 10 IoT Enterprise LTSC 2021 was also performed. BD cannot claim that future versions of CylancePROTECT® or 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 with computer workstations featuring the Microsoft® Windows® 10 IoT Enterprise LTSC 2021 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 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 has selected Windows® 10 IoT Enterprise LTSC (Long-term Servicing Channel) to provide our customers with a secure and feature-stable operating system from the Windows family. The workstations that BD provides with our instrument products should be considered a part of that medical device system rather than a general purpose computing workstation. Microsoft® recommends the use of IoT Enterprise LTSC for fixed purpose devices such as medical devices and industrial automation.
- The BD workstation operating system is based on Microsoft® Windows® 10 IoT Enterprise LTSC 2021. 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 enabled such as time synchronization, Internet Information Services (IIS) and AppLocker software whitelisting. Lastly, BD adds certain third-party applications and security solutions to the operating system such as the Google®Chrome browser, Adobe® Reader for PDF files, and CylancePROTECT® anti-malware (for some products).
- To maintain operating compatibility with cybersecurity controls and solutions on BD workstations, BD 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.

More information

- Regarding BD's Product Security policy and framework: bd.com/en-us/support/product-security-and-privacy
- Regarding Microsoft® Windows® 10 IoT Enterprise LTSC 2021: https://docs.microsoft.com/en-us/windows/iot/product-family/what%27s-new-in-windows-10-iot-enterprise-21h2

Malware protection software

Introduction

This topic provides general guidelines for BD workstations running the Microsoft® Windows® 10 IoT Enterprise LTSC 2021 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 software.

Installation

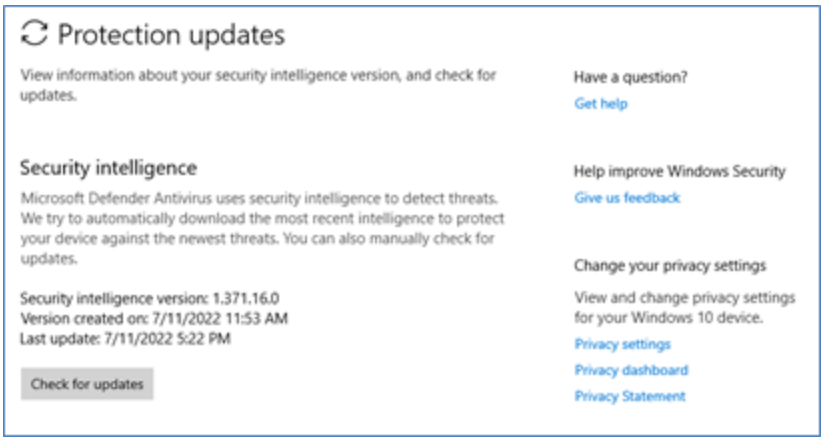
Windows® Defender (and additionally CylancePROTECT® on some products) is preinstalled and preconfigured on BD workstations with Microsoft® Windows® 10 IoT Enterprise LTSC 2021. Windows® Defender is designed to work with third-party anti-malware software and should be left enabled on the workstation even if another protection solution is installed. CylancePROTECT® can be uninstalled if a different third-party anti-malware software is required. From the Windows menu, go to Settings, then Apps, and select Cylance from the applications list to uninstall it. Be sure to reboot the workstation before installing a different third-party anti-malware solution.

The following products have CylancePROTECT® pre-installed in the workstation operating system:

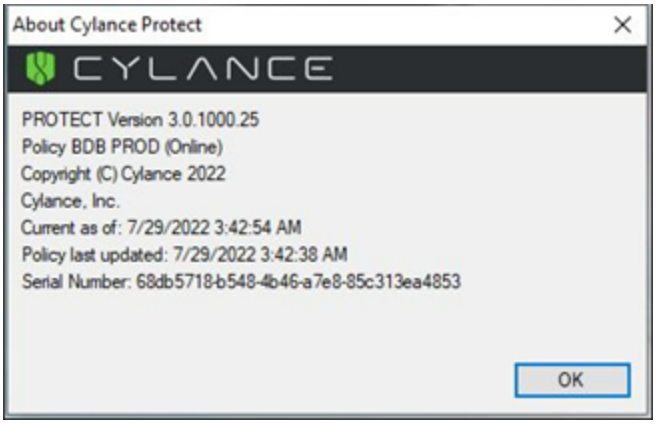
- BD Accuri™ C6 Plus
- BD FACSMelody™ cell sorter
- BD FACS™ Sample Preparation Assistant (SPA)
- BD FACSDiscover™ S8 cell sorter

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.

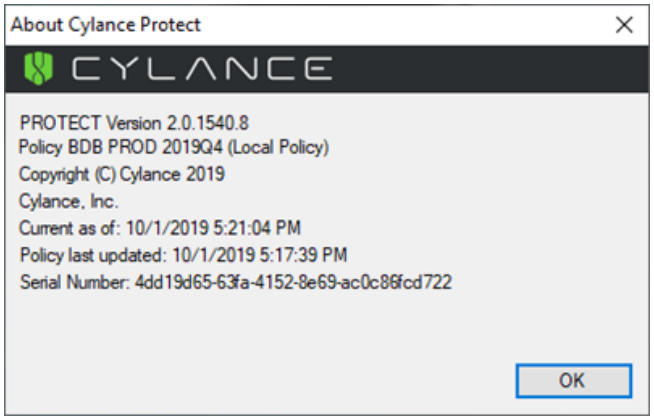


Products with CylancePROTECT® installed will be automatically updated to the BD-approved agent version and the latest device policy if the workstation is connected to a network with internet access. To check the current agent version and device policy, right-click the Cylance icon in the system tray and select **About**. The About dialog displays both the agent version and policy name as well as the update date and time.



If the workstation is not connected to a network, the device policy can be updated from a file using a USB media. Contact your BD Service representative to request the policy file. Use the following steps to apply the policy.

1. Copy the Cylance policy file from the USB media device to the workstation desktop.
2. Rename the file to “Policy.xml”.
3. Copy the file to the folder “C:\Program Files\Cylance\Desktop”.
4. Reboot the workstation.
5. After the workstation has restarted, wait 1-2 minutes for the Cylance icon to appear in the system tray. Right-click the icon and select **About**. The About dialog should display (Local Policy) as shown in the following image.



Scanning guidelines

Third-party malware protection software that performs virus signature-based scanning is processor intensive and could adversely affect the performance of BD software if executing simultaneously. Exclude the following BD folders from on-access scanning for systems running on Windows® 10.

Software	Files and folders
BD Accuri™ C6 Plus software v1.0.34	C:\Windows\BD Accuri C:\Windows\Cytometer Support Files
BD FACSChorus™ software v1.3 or later for BD FACSMelody™ systems	C:\Program Files\BD\FACSChorus C:\ProgramData\BD C:\Program Files\Microsoft SQL Server C:\Program Files (x86)\Microsoft SQL Server
BD FACSuite™ application v1.4 or later	C:\BD Import C:\BD Export C:\ProgramData\BD C:Program Files\Microsoft SQL Server
BD FACSuite™ Clinical application v1.4 or later	C:\BD Import Clinical C:\BD Export Clinical

Software	Files and folders
	C:\ProgramData\BD
	C:Program Files\Microsoft SQL Server
BD FACSCanto™ Clinical Software v4.0	C:\Program Files (x86)\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 17
	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 (x86)\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 17
	C: or D: \BDDatabase
	C:\ProgramData\BD\FACSDiva
	C:\ProgramData\BD\Shared
	C: or D: \BD\FACSDiva\CST
	C: or D: \BDExport
BD FACSChorus™ software v5.0 or later for BD FACSDiscover™ S8 systems	C:\ProgramData\BD
	D:\ProgramData\BD
	C:\Driver
	C:\Program Files (x86)\dotnet
	C:\Program Files (x86)\IIS
	C:\Program Files (x86)\Microsoft Analysis Services
	C:\Program Files (x86)\Microsoft Help Viewer
	C:\Program Files (x86)\Microsoft SQL Server
	C:\Program Files (x86)\ Microsoft SQL server Management Studio 18

Software	Files and folders
	C:\Program Files (x86)\ Microsoft Visual Studio 10.0 C:\Program Files (x86)\Newport C:\Program Files (x86)\teraterm C:\Program Files\BD C:\Program Files\dotnet C:\Program Files\IIS C:\Program Files\Microsoft C:\Program Files\Microsoft Analysis Services C:\Program Files\Microsoft SQL Server C:\Program Files\Microsoft Visual Studio 10.0 C:\Program Files\Microsoft.NET C:\Program Files\StCamSWare

BD is not responsible for data corruption or loss if full-system scanning occurs while BD 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 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 software becomes infected, reinstall it.
- Consult your IT department about whether to delete the infected files.

BD software installation

Temporarily disable third-party anti-malware protection software before installing BD 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 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 workstations without affecting the performance or functionality of BD 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

- Microsoft® Windows® 10 IoT Enterprise LTSC 2021 applies recommended updates for security patches (also known as quality updates) when connected to the internet. These updates can be paused for 7 days at a time when the Pause updates option is selected in the Windows Update section under Settings. The Pause updates option can be used up to five times for a total of 35 days. The Advanced options in the Windows Update section can be used to pause updates until a specific date. This option is limited to a maximum of 35 days. After 35 days, the Pause feature cannot be used again until the available updates have been installed.
- BD 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 recommended and patches that affect product operation are not recommended. Patch testing is performed approximately monthly and patch bulletins are published once per quarter unless critical vulnerability patches are released by Microsoft.
- Your IT system administrator should test and approve the Windows security updates and hotfixes. Only download updates from an official vendor site.

Windows patch testing bulletins

For Windows patch testing bulletins, go to cybersecurity.bd.com/bulletins-and-patches.

Third-party application update guidelines

Introduction

This topic discusses updates of third-party applications that are pre-installed on BD workstations, such as Google® Chrome browser and Adobe® Reader.

Installation

You can update third-party applications by downloading the installer package from a computer with an internet connection and copying the file to USB media for installation. If the BD workstation is connected to the local network, additional configuration and permissions might be necessary to allow internet access. Your IT system administrator might choose to manage these applications and update them as new versions are released. Download updates only from an official vendor site.

Update policy

- BD monitors for security vulnerabilities reported in third-party applications and periodically checks for vendor end of support. Updates might be included in OS security patch testing cycles that include operation of live instruments and execution of standard product quality control methods. Patch testing is performed approximately monthly and patch bulletins are published once per quarter unless critical vulnerability patches are released by Microsoft.
- Your IT system administrator should also review versions of general use applications, such as browsers.

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.

Security permission settings for driver files

If the workstation is connected to a BD FACSAria™ flow cytometer, BD FACSMelody™ cell sorter, and BD FACSDiscover™ S8 cell sorter, 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 setting for user groups

Windows limited user accounts should be members of the BUILTIN\Users Windows Group for proper management through the local group policy.

Security permission settings for folders

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

Software	Folders
BD Accuri™ C6 Plus software v1.0.34	C:\Windows\BD Accuri

Software	Folders
	C:\Windows\Cytometer Support Files
BD FACSChorus™ software v1.3 or later for BD FACSMelody™ systems	C:\Program Files\BD\FACSChorus C:\ProgramData\BD C:\Program Files\Microsoft SQL Server C:\Program Files (x86)\Microsoft SQL Server
BD FACSuite™ application v1.4 or later	All folders and subfolders in the following: C:\ProgramData\BD\FACSuite
BD FACSuite™ Clinical application v1.4 or later	All folders and subfolders in the following: C:\ProgramData\BD\FACSuite Clinical
BD FACSCanto™ Clinical Software v4.0	C:\Program Files (x86)\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 17 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 (x86)\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 17 C: or D: \BDDatabase C:\ProgramData\BD\FACSDiva C:\ProgramData\BD\Shared C: or D: \BD\FACSDiva\CST C: or D: \BDExport
BD FACSChorus™ software v5.0 or later for BD FACSDiscover™ S8 systems	C:\ProgramData\BD D:\ProgramData\BD

Software	Folders
	C:\Driver
	C:\Program Files (x86)\dotnet
	C:\Program Files (x86)\IIS
	C:\Program Files (x86)\Microsoft Analysis Services
	C:\Program Files (x86)\Microsoft Help Viewer
	C:\Program Files (x86)\Microsoft SQL Server
	C:\Program Files (x86)\ Microsoft SQL server Management Studio 18
	C:\Program Files (x86)\ Microsoft Visual Studio 10.0
	C:\Program Files (x86)\Newport
	C:\Program Files (x86)\teraterm
	C:\Program Files\BD
	C:\Program Files\dotnet
	C:\Program Files\IIS
	C:\Program Files\Microsoft
	C:\Program Files\Microsoft Analysis Services
	C:\Program Files\Microsoft SQL Server
	C:\Program Files\Microsoft Visual Studio 10.0
	C:\Program Files\Microsoft.NET
	C:\Program Files\StCamSWare

Security permissions for database restoration

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

Microsoft Windows firewall, IIS, and proxy settings

Introduction

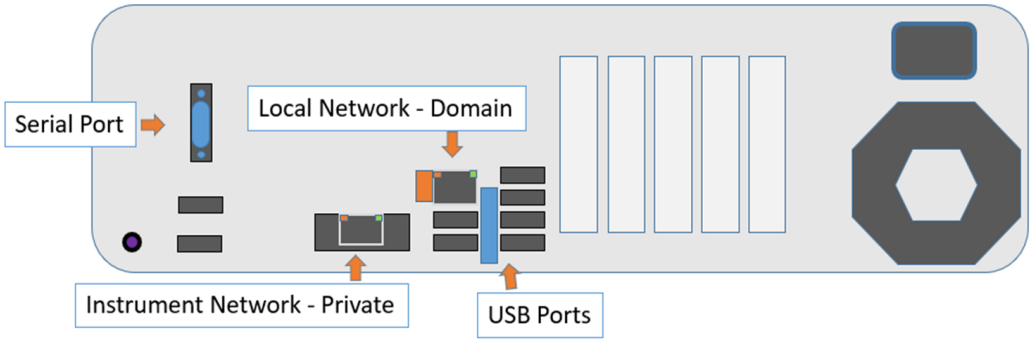
This topic describes how to set the firewall exclusions and proxy settings for the workstation. It also discusses IIS configuration for certain BD instrument products.

Microsoft Windows firewall settings

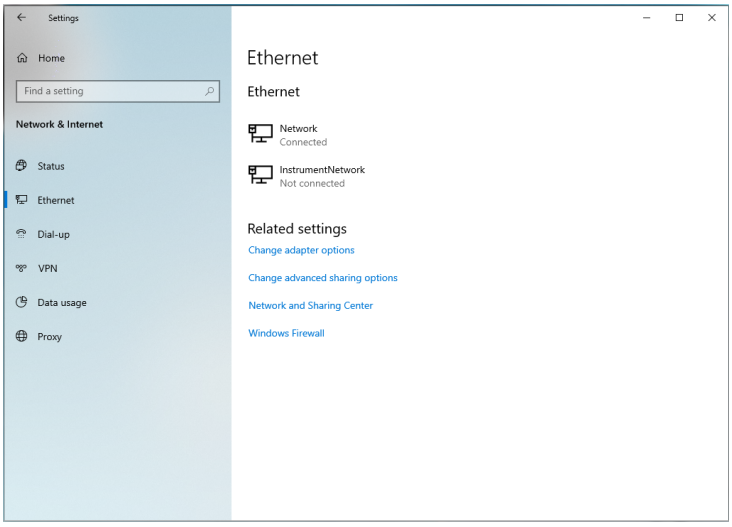
BD workstations ship with the Windows firewall enabled and preconfigured with the necessary firewall exclusions. The workstation has two NIC physical ports: one is provided for connecting the workstation to the local network and the other is dedicated to the instrument connection. This section discusses various aspects of

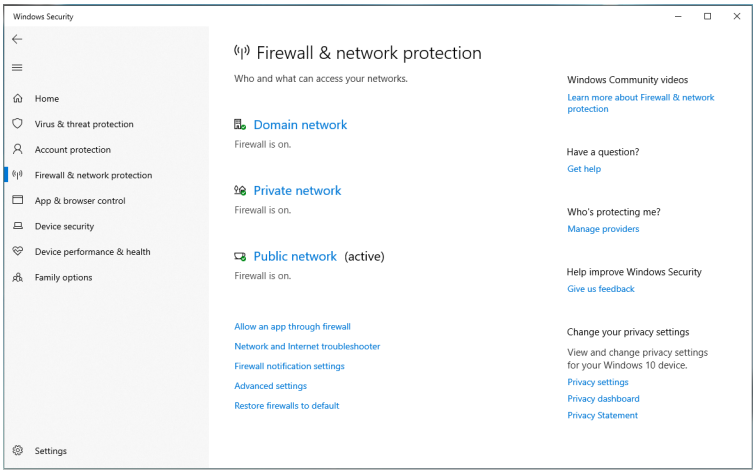
the networking and firewall configuration that are important to maintaining communication between the instrument and workstation.

On the HP® Z2 SFF G9 workstation, the first RJ-45 port is located down low on the left side in a cutout, as illustrated in the following drawing.



This port is configured as Private in the firewall and must be used for the connection to the instrument. The second RJ-45 port is located in a cluster with the USB ports in the lower half of the center area. This port is intended for local network access with the firewall configuration as Public. In the following two illustrations, the first one shows the Ethernet connections and the second shows the Windows® firewall.

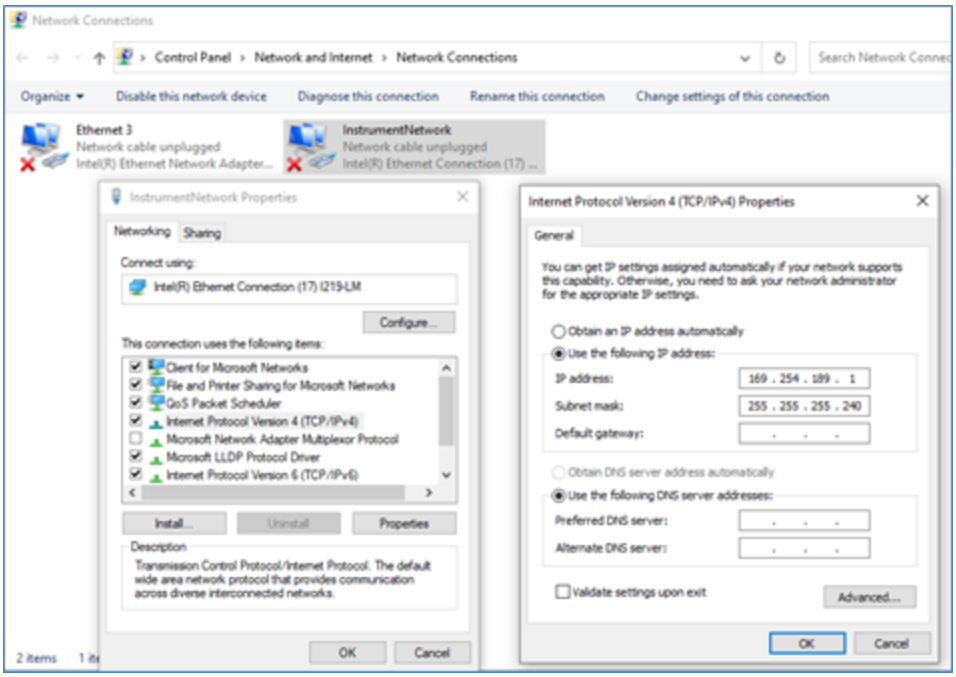




The Instrument Network interface is configured with a static IP address and a subnet mask for the IPv4 protocol. This is the only protocol required for the instrument communication. The other protocols have been disabled for security. The following table provides the information about the static IP addresses and the subnet masks for different BD products:

Product	IP address	Subnet mask
BD FACSDiscover™ S8 systems	169.254.189.1	255.255.255.240
All other products	192.168.2.1	255.255.252.0

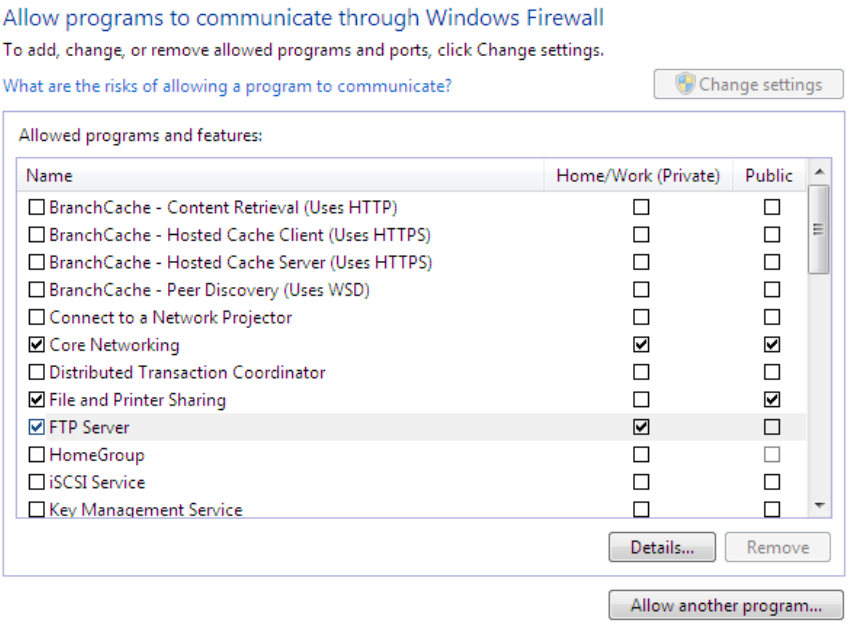
The following illustration shows the InstrumentNetwork connection properties and the IP address settings for the IPv4 protocol.



Internet Information Server configuration

Internet Information Server (IIS) may be configured on the workstation for file transfers to the instrument. The IIS configuration may include either the IIS Management Console or a local FTP service to transfer instrument configuration or firmware updates. For security, connections are configured with a static route only to the instrument NIC address and the instrument network connection is also configured to be Private. These settings are configured to prevent users from changing them through the local security policy.

For systems using a local FTP service, the service 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.



Creating a Microsoft Windows restore point

Introduction

You can create a restore point that you can use to restore the operating system to the state it was in prior to a software change that is causing unexpected behavior. You should create restore points before installations, updates, or other system changes that you have concerns about.

About this task

In addition to the restore points that you manually create, the system automatically creates restore points before the following events:

- Installation of applications that use a System Restore-compliant installer
- Installation of both manual and automatic updates from Windows Update or Auto Update

- System restore operations (so that you can undo a restoration if you selected the wrong restore point)

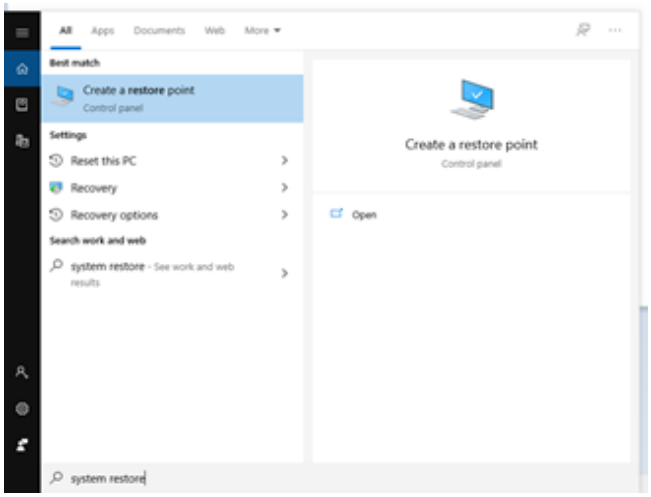
The system protection setting must be turned on for any restore points to be created.

Note: Restore points do not affect files in the Documents folder of a user. Use other methods to back up files in that location.

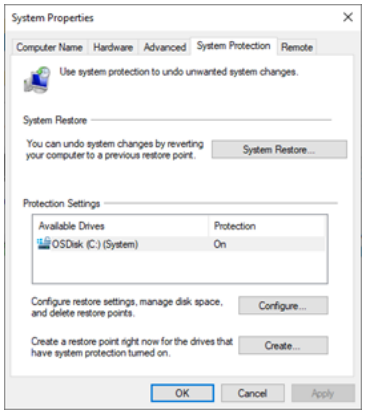
Procedure

To create a restore point:

1. In the taskbar search box, type "system restore" and select **Create a restore point**.

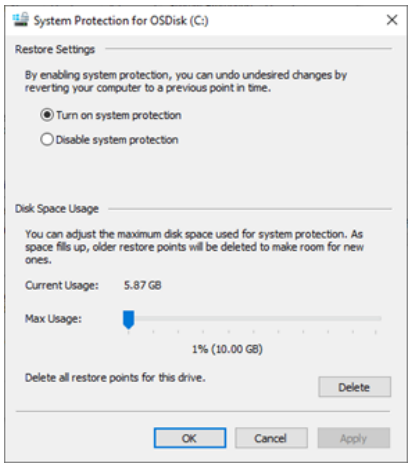


2. In the System Properties dialog, ensure that drive C is selected.



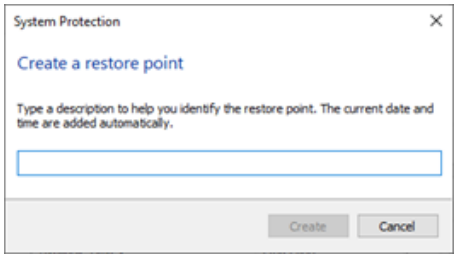
3. If the **Create** button is unavailable, enable system protection:

a. Click **Configure**, and then select **Turn on system protection**.



b. Click **Apply** and **OK**.

4. Click **Create**, type a description to help you identify the restore point, and then click **Create**.



More information

- docs.microsoft.com/en-us/windows/win32/sr/system-restore-portal
- support.microsoft.com/en-us/windows/recovery-options-in-windows-10-31ce2444-7de3-818c-d626-e3b5a3024da5

Restoring the Microsoft Windows system

Introduction

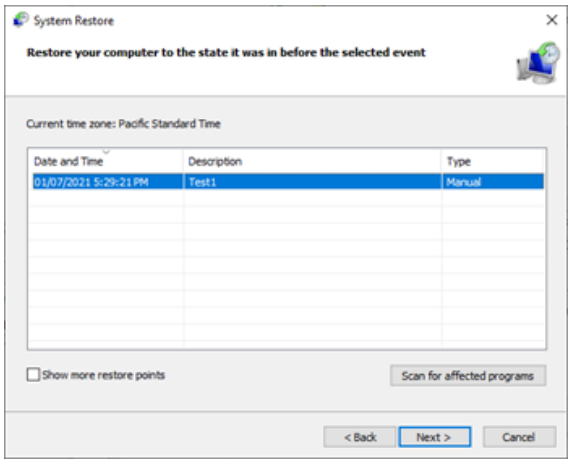
If a change to the operating system is causing unexpected behavior, you can restore the system to a previous state and remove the application or update that is causing the problem.

Procedure

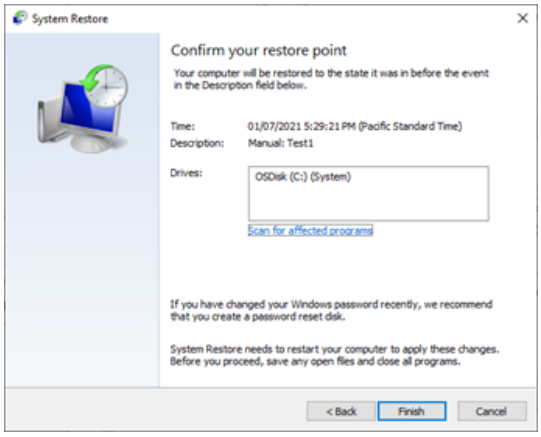
To restore the system:

1. In the taskbar search box, type "system restore" and select **Create a restore point**.
2. In the System Properties dialog, click **System Restore**.

3. Select the restore point that you want from the list, and then click **Next**.



4. Confirm the restore point information, and then click **Finish**.



5. In the warning dialog, read the warning and click **Yes** if you still want to continue.
   The restoration begins and the system restarts.

Sharing files in Microsoft® 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 workstations. At the end of the topic are links to Microsoft support documentation and technical guides.

File sharing basics

Although 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™ flow cytometer and BD FACS™ Sample Preparation Assistant (SPA) systems with the BD FACSLink™ middleware solution.

In the case where the shared folder is located on a network device, it might be more 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 the final steps of the procedure in the next section.

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 32) 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 software applications.

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

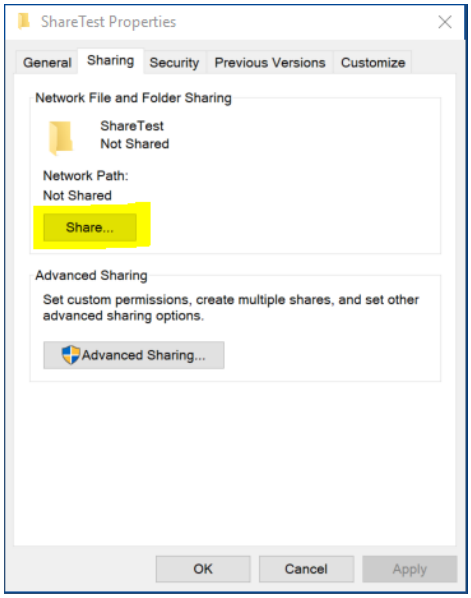
To create a local file share folder:

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.

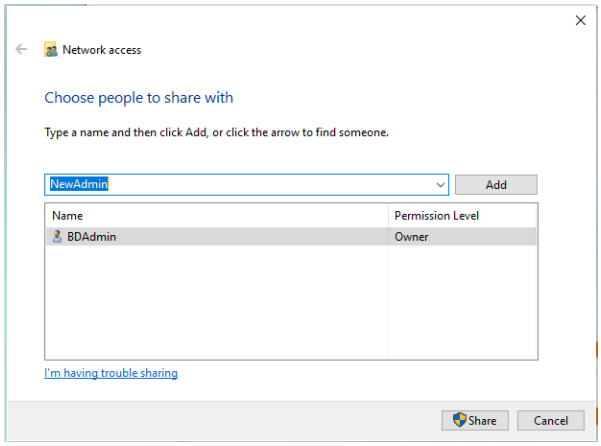
2. Local share folders should be created from the root of the C: drive (or alternatively on the D: drive if present on the workstation). In this example the folder is named ShareTest.

   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 **Share**.

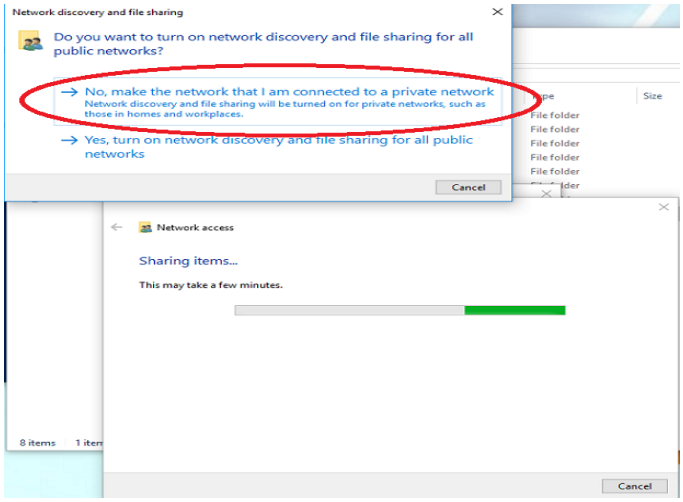


4. In the Network access dialog, enter the account name *NewAdmin* and click **Add**.

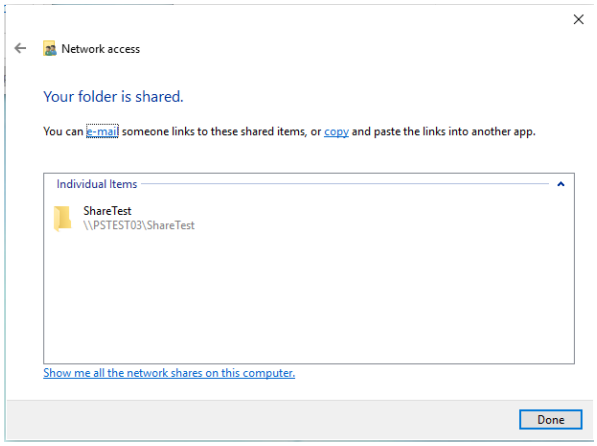


5. The NewAdmin account will appear with Read-only permissions by default. If Read/Write access is required, click the down carat to change the permission level. Click **Share** when you are done.

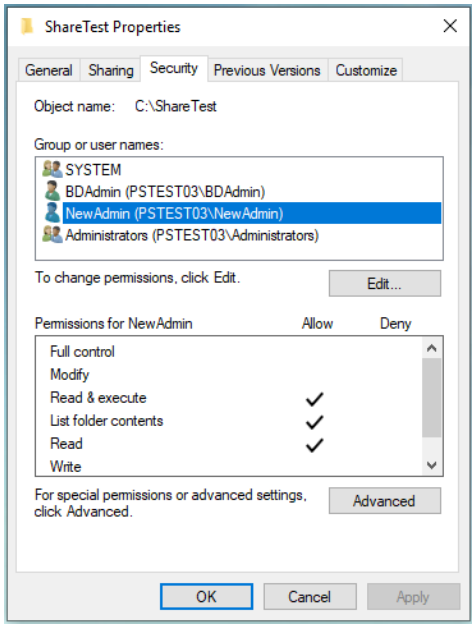
6. The Network discovery and file sharing dialog may open. Be sure to select the option to use settings for Private networks as shown below.



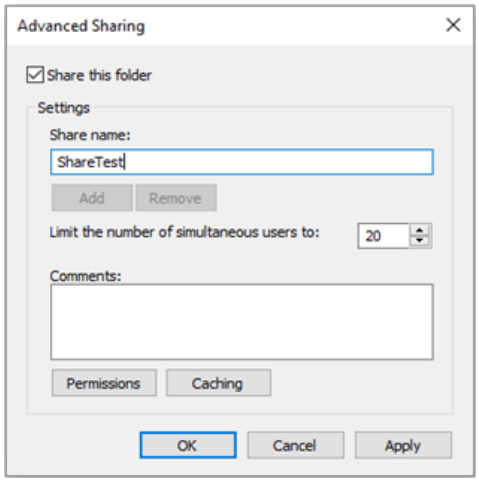
7. The final dialog shows the user accounts with access and the path to use when accessing the folder. Write down the exact path before closing the dialog because it is needed in the following step.



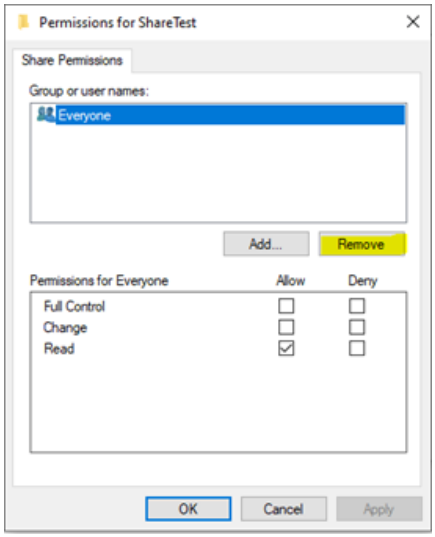
8. The new account will also appear in the Security tab of the folder properties.



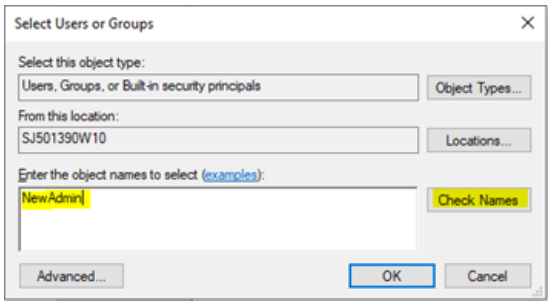
9. On the Sharing tab, under the folder properties, click **Advanced Sharing**.



10. In the Advanced Sharing dialog, click **Permissions**. In the Permissions dialog, select **Everyone** from the list of Group or user names, and then click **Remove**. This will restrict the access to the specific user groups.

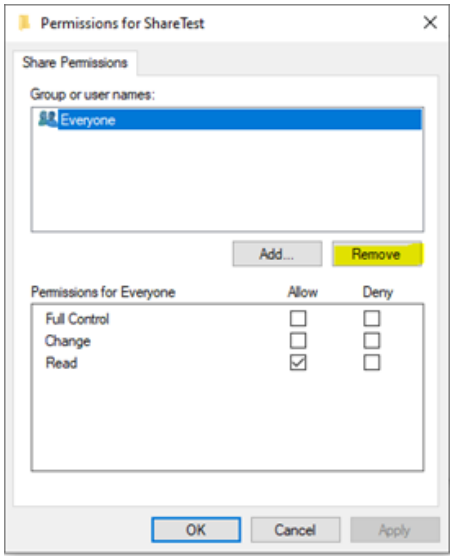


11. If necessary, add additional users by clicking **Add**. Type the user name in the box and select **Check Names** to confirm it exists in the system, and then click **OK**.

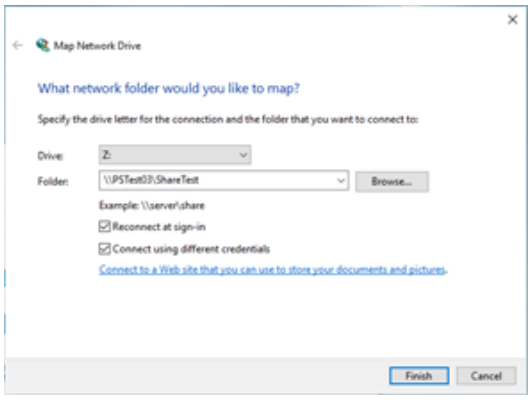


12. Click **OK** as needed to close the dialogs until you return to the Permissions dialog. Review the assigned permissions for each user, and then click **OK**.

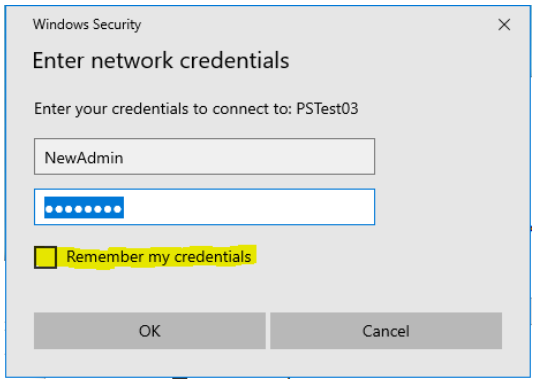
Note: This is minimal configuration when sharing within the LAN or VLAN.



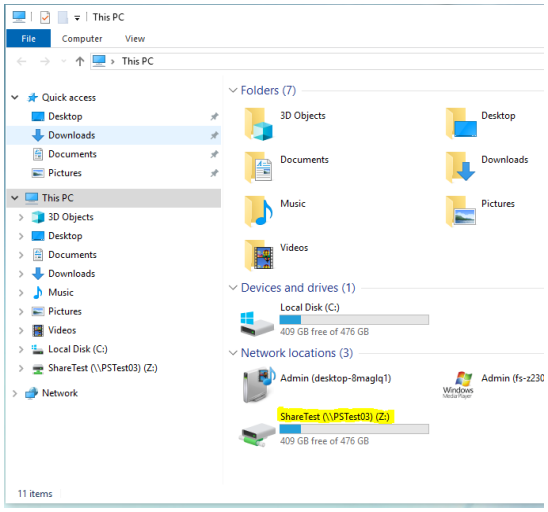
13. On the remote system, double-click on the **This PC** icon to open the Explorer and select **Map Network Drive** from the **Computer** ribbon. Enter the folder path from the previous step in the **Folder** box and check the box **Connect using different credentials**, and then click **Finish**.



14. Log in to the account from step 1. You can select the box to remember the credentials.



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. We recommend 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 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: 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: techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

For general information and troubleshooting, see support.microsoft.com/en-us/windows/file-sharing-over-a-network-in-windows-10-b58704b2-f53a-4b82-7bc1-80f9994725bf

BitLocker® encryption management

Introduction

This topic describes BD guidelines for activating BitLocker® and managing encryption keys. BitLocker® is an integrated feature of Windows® 10 that is used to secure files stored on the workstation local drive. It can also encrypt files on removable media such as USB.

BD cannot claim that future versions of BitLocker® will be compatible with these guidelines.

BitLocker configuration

BD 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.

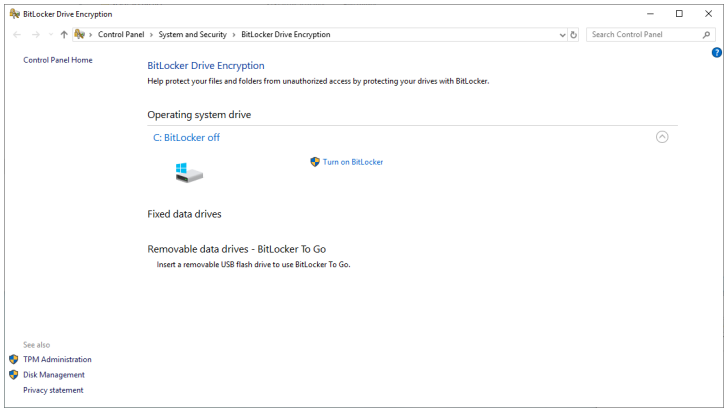
To enable BitLocker®:

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**.

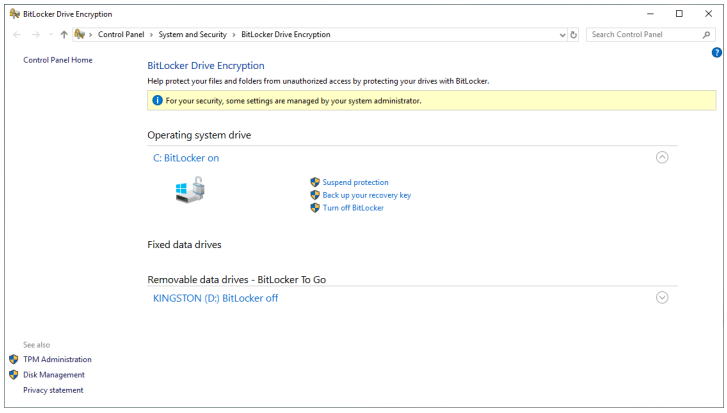
   b. In **How do you want to back up your recovery key**, select **Save to a File**. A file save dialog will open and you can select the USB drive.

   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.

AppLocker Execution Control

Introduction

This topic describes default settings for AppLocker configuration on BD workstations and how to add custom rules for a third-party application installed on a BD configured workstation. AppLocker is an integrated feature of Windows® 10 and is used to manage programs, installers and scripts and prevent execution of malware.

Note: Installing BD software applications to custom paths is not recommended on BD configured workstations.

AppLocker configuration

For BD workstations with AppLocker enabled, the following default rules are configured:

- Allow the BDAdmin and BDFSE user accounts full rights to install software and run software applications from any folder on the local drive and run scripts.
- Allow the BDOperator (and other non-Administrator accounts, if created) to execute programs in the standard Windows folder path (C:\Windows) and the Program Files folder path (C:\Program Files).
- Non-administrator accounts are not allowed to install software, run scripts or run software that is not installed along these folder paths.

As a result, if third-party software is installed by an Administrator on a custom path outside of these standard paths, custom application rules must be created to allow non-administrator user accounts to run the software. The next section, Adding a custom application rule, describes the steps for creating a custom rule for the custom installation path.

Note: Script execution is also restricted by the operating system hardening configuration. For more information, see Operating system hardening (page 43).

Adding a custom application rule

Note: Pre-configured application rules do not need modification. Do not modify these settings as change may affect execution of BD software applications.

To allow execution of third-party software installed to a custom installation path on a BD configured workstation:

1. Determine the folder path for the new application. It is recommended that applications be installed to the default path C:\Program Files\<*Program Name*> where <*Program Name*> is the name of the application or manufacturer of the software.

   For the steps here, we use the example: C:\CompanyX\NewApp.

2. Click **Start** and type *secpol.msc* for Local Security Policy.
3. Go to Security Settings > Application Control Policies > AppLocker and expand the tree.
4. For Executable Rules, follow these steps.

a. Select **Executable Rules** and right-click. Select **Create New Rule...**

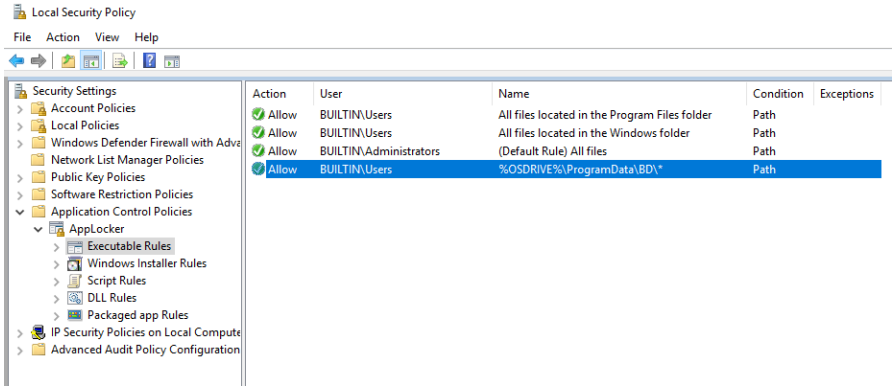
b. Click **Next** on the **Before You Begin** page.

c. On the **Permission** page, in User or Group section, click **Select**, and then click **Advanced**. In the right-hand side, click **Find Now**. In the Search results window, scroll down and select/highlight **Users** and click **OK**. Click **OK** again and click **Next**.

d. On the **Conditions** page, select **Path** and click **Next**.

e. In the **Path** page and in the **Path**: box, type %OSDRIVE%\CompanyX\NewApp*. Then click **Create**.

f. The following screen lists the rules configured. Other category of rules such as Windows Installer Rules, Script Rules and DLL Rules will look similar.



5. For Windows Installer Rules, follow these steps.

a. Select **Installer Rules** and right-click. Select **Create New Rule...**

b. Click **Next** on the **Before You Begin** page.

c. On the **Permission** page, in User or Group section, click **Select**, then click **Advanced**. On the right side, click **Find Now**. In the Search results window, scroll down and select/highlight **Users** and click **OK**. Click **OK** again and click **Next**.

d. On the **Conditions** page, select **Path** and click **Next**.

e. On the **Path** page and in the Path: box, type %OSDRIVE%\ CompanyX\NewApp *. Then click **Create**.

6. For Script Rules, follow these steps.

a. Select **Script Rules** and right-click. Select **Create New Rule...**

b. Click **Next** on the **Before You Begin** page.

c. On the **Permission** page, in User or Group section, click he **Select**, and then click **Advanced**. On the right side, click **Find Now**. In the Search results window, scroll down and select/highlight **Users** and click **OK**. Click **OK** again and click **Next**.

d. On the **Conditions** page, select **Path** and click **Next**.

e. On the **Path** page and in the Path: box, type %OSDRIVE%\ CompanyX\NewApp *. Then click **Create**.

7. For DLL Rules, follow these rules:

a. Select **DLL Rules** and right-click. Select **Create New Rule...**

b. Click **Next** on the **Before You Begin** page.

c. On the **Permission** page, in the User or Group section, click **Select**, then click **Advanced**. On the right side, click **Find Now**. In the Search results window, scroll down and select/highlight **Users** and click **OK**. Click **OK** again and click **Next**.

d. On the **Conditions** page, select **Path** and click **Next**.

e. In the **Path** page and in the Path: box, type %OSDRIVE%\CompanyX\NewApp *. Then click **Create**.

8. Reboot the workstation

Removable media guidelines

Introduction

This topic describes BD 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 possible adverse performance of BD software, install removable media only when the instrument is not analyzing samples.

Restricting user access

BD 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 workstations.

If you want to restrict users from accessing removable media on products featuring Microsoft® Windows® 10 IoT Enterprise LTSC 2021, follow Microsoft's recommendations to prevent users from connecting to USB storage devices. Go to support.microsoft.com.

Workstation power management guidelines

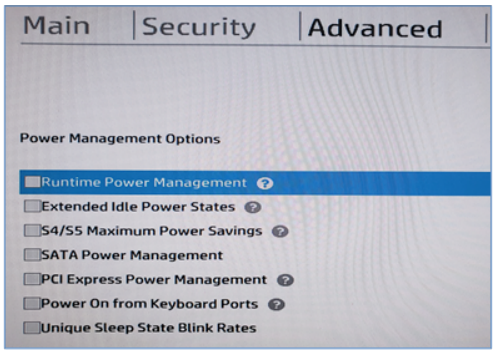
Introduction

This topic describes BD guidelines for workstation power management settings in the Windows operating system and the workstation BIOS.

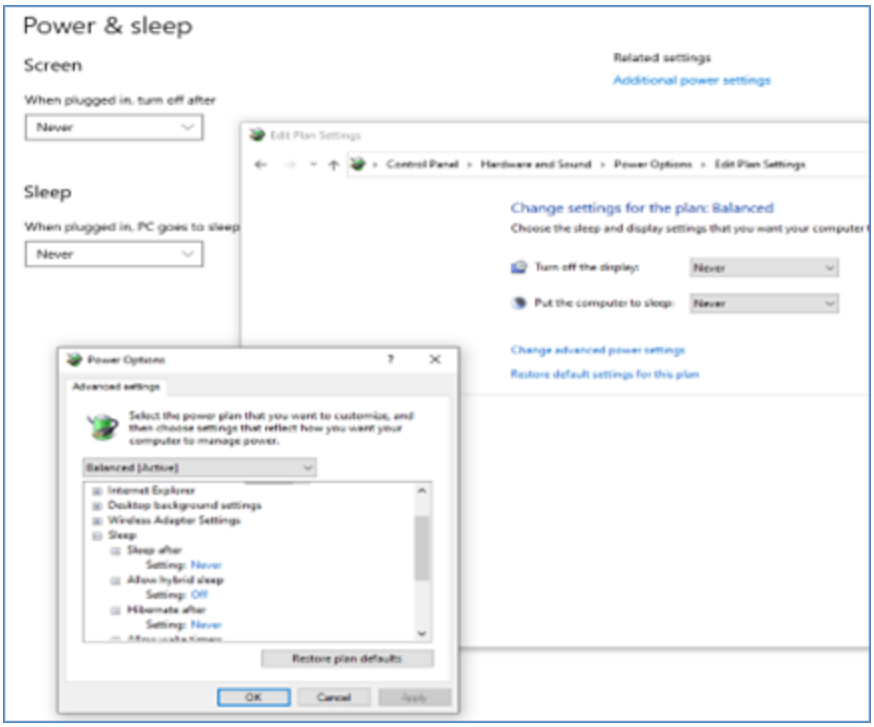
Power management settings and system operation

BD has observed during internal testing that some hardware drivers and PC components do not resume properly from low power or suspended power state, which can cause an interruption in data from the instrument or external devices such as video cameras. To avoid this, the Runtime Power Management and Extended Idle Power States options in the HP® Z2 SFF G9 Bios configuration is not enabled for BD FACSDiscover™ S8 instrument.

Workstations for other BD products might have these options in BIOS, as shown in the following image.



The Windows® 10 operating system also has power management and standby mode settings associated with the display and local hard disk. By default, the HP® Z2 SFF G9 is set to never turn off the displayand never turning off the hard disk or putting the workstation to sleep. The following image shows the Windows 10 power management settings.



Multi-Factor Authentication for Local Administrator Accounts

Introduction

This topic describes configuration of a Multi-Factor Authentication (MFA) hardware token to add additional security for a local administrator account. The instructions presented here uses the YubiKey Series 5 token from Yubico (https://www.yubico.com/). The BD Biosciences products listed have been tested with the YubiKey Series 5 applied to the BDAdmin account during qualification testing of the operating system: BD FACSLyric™, BD FACSCanto™ flow cytometer, and BD Accuri™ C6 Plus.

Even though a YubiKey device is not provided with the workstation, these instructions are provided to guide the user on properly configuring the device for Windows. The YubiKey device supports multiple types of authentication protocols including those used by web services. The instructions here are specific to using the Yubico Windows Login overlay with a local user account.

Adding the YubiKey token to the Windows login for the BDAdmin account requires two stages: first the Yubico Windows Login overlay must be installed so that Windows can recognize the MFA token, second the YubiKey device must be configured and paired with the BDAdmin user account.

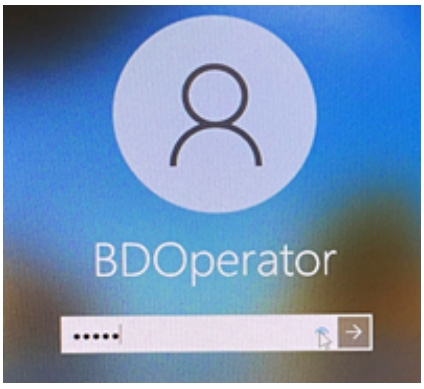
Procedure

Part 1 - Installing the YubiKey Login for Windows® Application

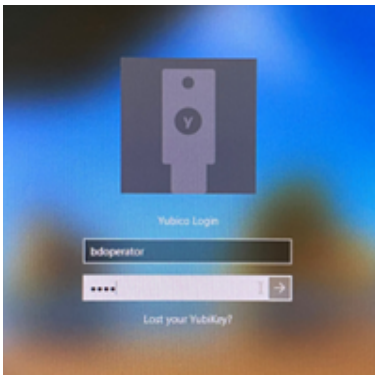
On a PC with Internet access, download the Yubico Login for Windows® 64-bit application from the Yubico download site at https://www.yubico.com/products/computer-login-tools/.

Log in to the instrument workstation where YubiKey is going to be added using the BDAdmin account and copy the file "Yubico-Login-for-Windows-2.0.3-win64.msi" to the desktop. Double-click on the file to launch the installer and follow the prompts using the default options to complete the installation.

Once the Yubico Login for Windows® application is installed, the Windows® login screen will appear different from the default screen. The pictures below show an example of Windows® login screen before and after installation of the Yubico application.



Windows® login screen before installing Yubico application



Windows® login screen after installing Yubico application

The Yubico Login screen adds the following:

- A simple graphic of the YubiKey token above the User ID box with the Yubico Login title.
- The option to unmask the password (blue 'eye' icon in Before screen) is no longer available.
- A link to follow which allows access using the Recovery Code.

Note: The Yubico Login graphic and link for the Recovery Code will appear in the Login screen once the YubiKey Login for Windows application is installed, regardless of whether a YubiKey is configured for any local user account.

Using the Recovery Code

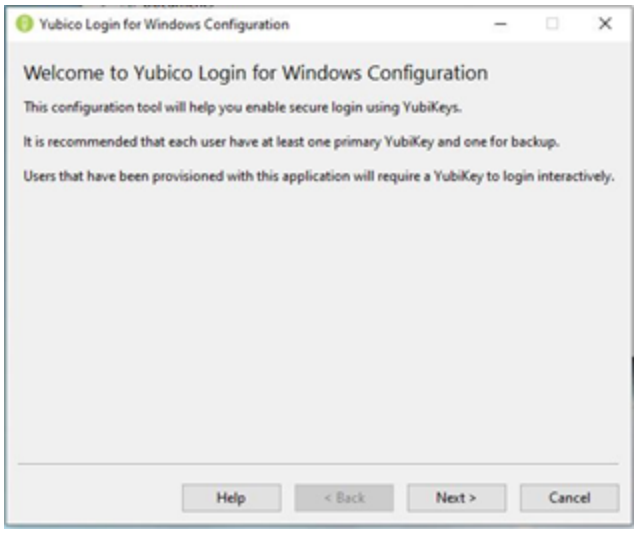
Clicking the 'Lost your YubiKey?' link will display the Recovery code login screen -

Entering the User ID and password with the Recovery Code generated during the YubiKey token configuration will unlock the account. See step 6 in Part 2 below for an example of the Recovery Code shown during the configuration. To return to the Yubico Login screen, select the link 'Use YubiKey instead?'.

Part 2 - Configuring the YubiKey device for the User Account

After the Yubico Login for Windows® application is installed, the YubiKey device can be configured for the BDAdmin account.

1. Launch the Windows® Login Configuration application and on the wizard's landing page, click **Next**.



2. In the 2nd page of the Yubico Login for Windows Configuration:

   a. In the Slots section, select Slot 2.

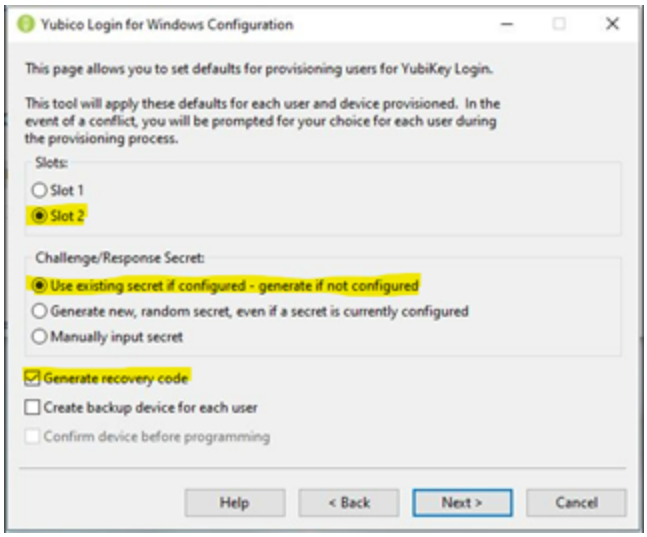
   b. In the Challenge/Response Secret section, select "Use existing secret if configured – generate if not configured."

   c. For the bottom options, select the check the box for "Generate recovery code".

      Leave rest of the boxes blank.

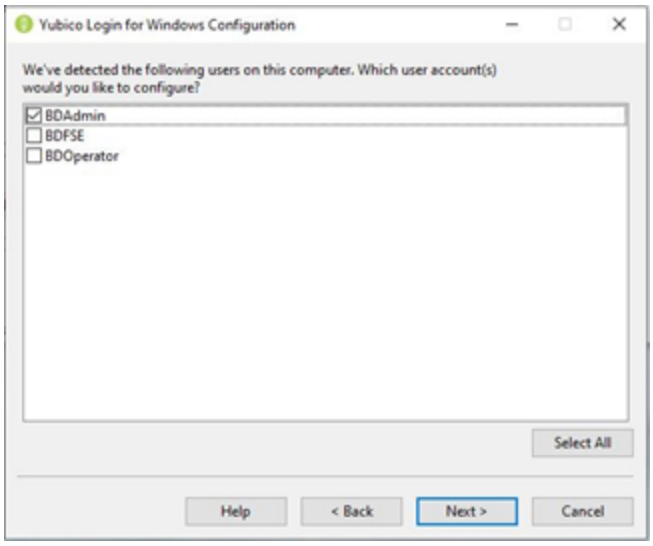
If a 2nd YubiKey is being programmed for backup, select the check box for “Create backup device for each user”.

d. Click **Next**.



3. In the next page of the wizard, the local users are detected.

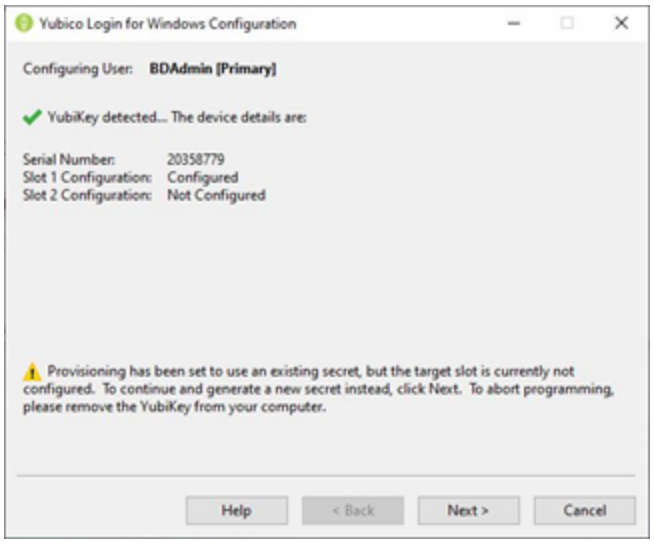
Select the user(s) for the configuration, for example, select the check box for BDAdmin and then, click **Next**.



4. Insert your YubiKey or the wizard will prompt you to insert the YubiKey.

After inserting the YubiKey, in the next page of the wizard, the curent info is displayed and it is ready for programming.

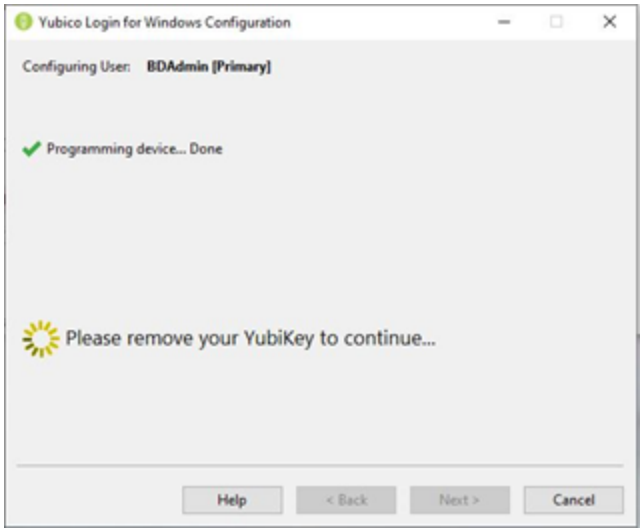
To proceed, click **Next**.



5. In the next page of the wizard, a progress ring displays showing the status of programming.

   When the programming is completed, the status displays as “Programming device... Done”.

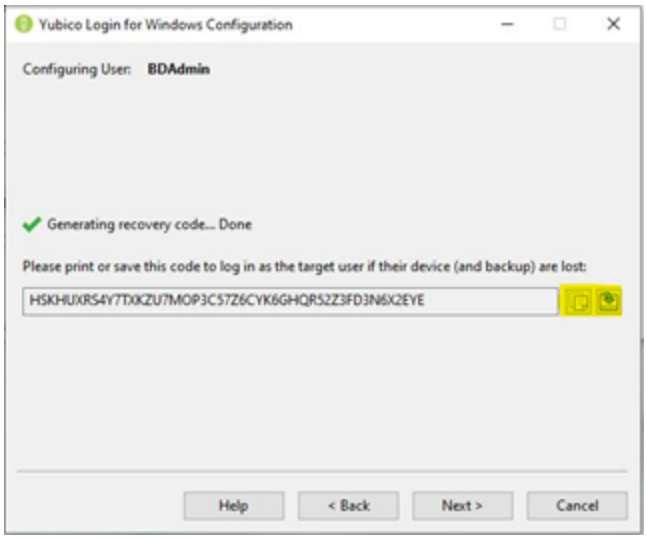
   Remove the YubiKey and click **Next**.



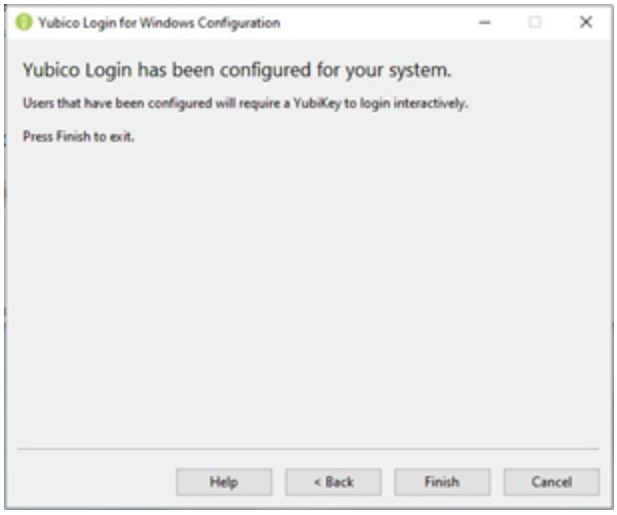
6. In the next page of the wizard, the recovery code is generated.

   You can copy and paste or use the options, buttons next to the code, to save the code.

When you are done, click **Next**.



7. The programming is finished.



Additional references

https://support.yubico.com/hc/en-us/articles/360013708460-Yubico-Login-for-Windows-Configuration-Guide

3

Operating system hardening

This chapter covers the following topic:

Operating system hardening and other guidelines

Introduction

This topic lists the operating system hardening measures and related security configurations applied to BD products using Microsoft® Windows® 10 IoT Enterprise LTSC 2021. These settings are recommended by the Defense Information Systems Agency (DISA) as part of their Security Technical Implementation Guidelines (STIG). This specific set of STIGs has been compiled by the BD Information Security Engineering team for non-server Windows® OS provided with BD products.

For more information regarding security recommendations for operating systems, see the Security Technical Implementation Guides (STIGs) — DoD Cyber Exchange at the following website at public.cyber.mil/stigs/.

Summary of STIGs applied to the OS configuration

The following content lists the STIGs by number and description.

STIG	Description
V-63797	System must be configured to prevent storage of the LAN manager HASH of passwords.
V-63651	Solicited Remote Assistance must not be allowed.
V-63325	The Windows Installer Always install with elevated privileges must be disabled.
V-63667	Autoplay must be turned off for non-volume devices.
V-63673	Autoplay must be disabled for all drives.
V-63671	The default autorun behavior must be configured to prevent autorun commands.
V-63759	Anonymous access to Named Pipes and Shares must be restricted.
V-63745	Anonymous enumeration of SAM accounts must not be allowed.
V-68845	Data Execution Prevention (DEP) must be configured to at least OptOut.
V-68849	(SEHOP) Structured Exception Handling Overwrite Protection (SEHOP) must be turned on.
V-63801	The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.
V-63347	The Windows Remote Management (WinRM) service must not use Basic authentication.
V-63349	Systems must be maintained at a supported servicing level.
V-63749	Anonymous enumeration of shares must be restricted.
V-63335	The Windows Remote Management (WinRM) client must not use Basic authentication.
V-63413	The period of time before the bad logon counter is reset must be configured to 15 minutes. The account lockout feature, when enabled, prevents brute-force password attacks on the system.
V-63411	The enhanced mitigation experience toolkit (EMET) system wide structure exception handler overwrite protection SEHOP must be configured to application opt out.
V-63415	The password history must be configured to 24 passwords remembered.

STIG	Description
V-63419	The maximum password age must be configured to 60 days or less.
V-63795	Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.
V-63711	Unencrypted passwords must not be sent to third party SMB Servers.
V-63713	The SmartScreen filter for Microsoft Edge must be enabled.
V-63719	The Windows SMB server must be configured to always perform SMB packet signing.
V-63723	(SMBPacketSigning_LanManServer) The Windows SMB server must be configured to always perform SMB packet signing.
V-63657	Unauthenticated RPC clients must be restricted from connecting to the RPC server.
V-70639	(SMBv1Disabled) The Server Message Block (SMB) v1 protocol must be disabled on the system.
V-63519	The Application event log size must be configured to 32768 KB or greater.
V-71769	Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.
V-71765	Internet connection sharing must be disabled.
V-71761	The system must be configured to audit Policy Change - Authorization Policy Change successes.
V-63527	The System event log size must be configured to 32768 KB or greater.
V-68817	Command line data must be included in process creation events.
V-63329	Users must be notified if a web-based program attempts to install software.
V-63487	The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.
V-63481	The system must be configured to audit Policy Change - Authentication Policy Change successes.
V-63665	The system must be configured to require a strong session key.
V-63385	The Telnet Client must not be installed on the system.
V-63513	The system must be configured to audit System - Security System Extension successes.
V-63389	The TFTP Client must not be installed on the system.
V-63669	The machine inactivity limit must be set to 60 minutes, locking the system with the screensaver.
V-63467	The system must be configured to audit Logon/Logoff - Logon successes.
V-63707	The Windows SMB client must be enabled to perform SMB packet signing when possible.
V-63705	InPrivate browsing in Microsoft Edge must be disabled.
V-63703	The Windows SMB client must be configured to perform SMB packet signing when possible.
V-63469	The system must be configured to audit Logon/Logoff - Special Logon successes.
V-63701	SmartScreenFilter users must not be allowed to ignore SmartScreen filter warnings for unverified files in Microsoft Edge.
V-63423	Passwords must, at a minimum, be 8 characters.
V-63499	The system must be configured to audit System - Other System Events successes.
V-63559	The system must be configured to prevent IP source routing. Configuring the system to disable IP source

STIG	Description
	routing protects against spoofing.
V-63491	The system must be configured to audit System - IPSec Driver failures.
V-63677	Enhanced anti-spoofing when available must be enabled for facial recognition.
V-63375	The Windows Remote Management (WinRM) service must not store RunAs credentials. Storage of administrative credentials could allow unauthorized access.
V-63679	Administrator accounts must not be enumerated during elevation. Enumeration of administrator accounts when elevating can provide part of the logon information to an unauthorized user.
V-63845	The accounts with the "Access this computer from the network" user right must only be assigned to the Administrators group.
V-63453	The system must be configured to audit Detailed Tracking - Process Creation successes.
V-63549	The display of slide shows on the lock screen must be disabled. Slide shows that are displayed on the lock screen could display sensitive information to unauthorized personnel.
V-63369	The Windows Remote Management (WinRM) service must not allow unencrypted traffic.
V-63441	The system must be configured to audit Account Management - Other Account Management Events successes. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63445	The system must be configured to audit Account Management - Security Group Management successes. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63449	The system must be configured to audit Account Management - User Account Management successes. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63763	Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously. Services using Local System that use Negotiate when reverting to NTLM authentication may gain unauthorized access if allowed to authenticate anonymously vs. using the computer identity.
V-63765	NTLM must be prevented from falling back to a Null session. NTLM sessions that are allowed to fall back to Null (unauthenticated) sessions may gain unauthorized access.
V-63609	Group Policy objects must be reprocessed even if they have not changed. Enabling this setting and then selecting the **Process even if the Group Policy objects have not changed** option ensures that the policies will be reprocessed even if none have been changed.
V-63767	PKU2U authentication using online identities must be prevented. PKU2U is a peer-to-peer authentication protocol. This setting prevents online identities from authenticating to domain-joined systems.
V-63607	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad. Compromised boot drivers can introduce malware prior to protection mechanisms that load after initialization.
V-63725	The use of OneDrive for storage must be disabled. OneDrive provides access to external services for data storage that must not be used. Enabling this setting will prevent such access from the OneDrive app, as well as from File Explorer.
V-63633	Local users on domain-joined computers must not be enumerated. The username is one part of logon

STIG	Description
	credentials that could be used to gain access to a system. Preventing the enumeration of users limits this information to authorized personnel.
V-63577	Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares. Additional security requirements are applied to Universal Naming Convention (UNC) paths specified in Hardened UNC paths before allowing access them.
V-63721	The minimum pin length for Windows Hello for Business must be six characters or greater. Windows Hello for Business allows the use of PINs as well as biometrics for authentication without sending a password to a network or website where it could be compromised.
V-63755	The system must be configured to prevent anonymous users from having the same rights as the Everyone group. Access by anonymous users must be restricted. If this setting is enabled, then anonymous users have the same rights and permissions as the built-in Everyone group.
V-63751	Indexing of encrypted files must be turned off. Indexing of encrypted files may expose sensitive data. This setting prevents encrypted files from being indexed.
V-63517	The system must be configured to audit System - System Integrity successes. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63695	File Explorer shell protocol must run in protected mode. The shell protocol will limit the set of folders applications can open when run in protected mode.
V-63511	The system must be configured to audit System - Security System Extension failures. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63597	Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems. A compromised local administrator account can provide means for an attacker to move laterally between domain systems.
V-63615	Downloading print driver packages over HTTP must be prevented. Some features may communicate with the vendor, sending system information or downloading data or components for the feature.
V-63685	Windows smart screen will help system from program download from the internet that may be malicious.
V-63617	Local accounts with blank passwords must be restricted to prevent access from the network. An account without a password can allow unauthorized access to a system as only the username would be required.
V-63425	The Enhanced Mitigation Experience Toolkit (EMET) Default Actions and Mitigations Settings must enable Anti Detours. Attackers are constantly looking for vulnerabilities in systems and applications.
V-63591	Wi-Fi Sense must be disabled. Wi-Fi Sense automatically connects the system to known hotspots and networks that contacts have shared. It also allows the sharing of the systems known networks to contacts.
V-63459	The system must be configured to audit Logon/Logoff - Logoff successes. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63829	User Account Control must run all administrators in Admin Approval Mode, enabling UAC. User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting enables UAC.
V-63819	User Account Control must run all administrators in Admin Approval Mode, enabling UAC. User Account

STIG	Description
	Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting enables UAC.
V-63321	Users must be prevented from changing installation options. Installation options for applications are typically controlled by administrators. This setting prevents users from changing installation options that may bypass security features.
V-63827	User Account Control must only elevate UIAccess applications that are installed in secure locations. User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized.
V-63825	User Account Control must be configured to detect application installations and prompt for elevation. User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized.
V-63821	User Account Control must automatically deny elevation requests for standard users. User account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized.
V-63569	Insecure logons to an SMB server must be disabled. Insecure guest logons allow unauthenticated access to shared folders. Shared resources on a system must require authentication to establish proper access.
V-71759	The system must be configured to audit Logon/Logoff - Account Lockout failures. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63523	The Security event log size must be configured to 196608 KB or greater. Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel.
V-63743	Attachments must be prevented from being downloaded from RSS feeds. Attachments from RSS feeds may not be secure. This setting will prevent attachments from being downloaded from RSS feeds.
V-63741	Remote Desktop Services must be configured with the client connection encryption set to the required level. Remote connections must be encrypted to prevent interception of data or sensitive information. Selecting **High Level** will ensure encryption of Remote Desktop Services sessions in both directions.
V-63747	Basic authentication for RSS feeds over HTTP must not be used. Basic authentication uses plain text passwords that could be used to compromise a system.
V-63507	The system must be configured to audit System - Security State Change successes. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63621	Web publishing and online ordering wizards must be prevented from downloading a list of providers. Some features may communicate with the vendor, sending system information or downloading data or components for the feature.
V-63585	Connections to non-domain networks when connected to a domain authenticated network must be blocked. Multiple network connections can provide additional attack vectors to a system and should be limited. When connected to a domain, communication must go through the domain connection.
V-63627	Systems must at least attempt device authentication using certificates. Using certificates to authenticate devices to the domain provides increased security over passwords.
V-63629	The network selection user interface (UI) must not be displayed on the logon screen. Enabling interaction with the network selection UI allows users to change connections to available networks

STIG	Description
	without signing into Windows.
V-63421	The minimum password age must be configured to at least 1 day. Permitting passwords to be changed in immediate succession within the same day allows users to cycle passwords through their history database.
V-63837	The screen Saver must be password protected.
V-63831	User Account Control must virtualize file and registry write failures to per-user locations. User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized.
V-63737	The Remote Desktop Session Host must require secure RPC communications. Allowing unsecure RPC communication exposes the system to man in the middle attacks and data disclosure attacks.
V-63439	The system must be configured to audit Account Management - Other Account Management Events failures. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63733	Remote Desktop Services must always prompt a client for passwords upon connection. This setting controls the ability of users to supply passwords automatically as part of their remote desktop connection.
V-63731	Local drives must be prevented from sharing with Remote Desktop Session Hosts. Preventing users from sharing the local drives on their client computers to Remote Session Hosts that they access helps reduce possible exposure of sensitive data.
V-63639	Outgoing secure channel traffic must be encrypted or signed. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted.
V-63637	Signing in using a PIN must be turned off. Strong sign-on must be used to protect a system. The PIN feature is limited to 4 numbers and caches the domain password in the system vault.
V-63635	Audit policy using subcategories must be enabled. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63803	The system must be configured to the required LDAP client signing level. This setting controls the signing requirements for LDAP clients. This setting must be set to Negotiate signing or Require signing, depending on the environment and type of LDAP server in use.
V-63805	The system must be configured to meet the minimum session security requirement for NTLM SSP based clients. Microsoft has implemented a variety of security support providers for use with RPC sessions. All of the options must be enabled to ensure the maximum security level.
V-63807	The system must be configured to meet the minimum session security requirement for NTLM SSP based servers. Microsoft has implemented a variety of security support providers for use with RPC sessions. All of the options must be enabled to ensure the maximum security level.
V-63435	The system must be configured to audit Account Logon - Credential Validation successes. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63341	The Windows Remote Management (WinRM) client must not use Digest authentication. Digest authentication is not as strong as other options and may be subject to man-in-the-middle attacks.
V-63409	The number of allowed bad logon attempts must be configured to 5 or less. The account lockout feature,

STIG	Description
	when enabled, prevents brute-force password attacks on the system.
V-63817	User Account Control approval mode for the built-in Administrator must be enabled. User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized.
V-63813	The system must be configured to require case insensitivity for non-Windows subsystems. This setting controls the behavior of non-Windows subsystems when dealing with the case of arguments or commands.
V-63643	Outgoing secure channel traffic must be encrypted when possible. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted.
V-63641	The system must be configured to block untrusted fonts from loading. Attackers may use fonts that include malicious code to compromise a system.
V-63647	Outgoing secure channel traffic must be signed when possible. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked.
V-63729	Passwords must not be saved in the Remote Desktop Client. Saving passwords in the Remote Desktop Client could allow an unauthorized user to establish a remote desktop session to another system.
V-63645	Users must be prompted for a password on resume from sleep (on battery). Authentication must always be required when accessing a system. This setting ensures the user is prompted for a password on resume from sleep (on battery).
V-63431	The system must be configured to audit Account Logon - Credential Validation failures. Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks.
V-63623	Printing over HTTP must be prevented. Some features may communicate with the vendor, sending system information or downloading data or components for the feature.
V-63333	Automatically signing in the last interactive user after a system-initiated restart must be disabled. Windows can be configured to automatically sign the user back in after a Windows Update restart.
V-70637	WindowsPowerShell - The Windows PowerShell 2.0 feature must be disabled on the system.
V-68819	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.
V-63659	The setting to allow Microsoft accounts to be optional for modern style apps must be enabled. Control of credentials and the system must be maintained within the enterprise.
V-63715	The amount of idle time required before suspending a session must be configured to 15 minutes or less. Open sessions can increase the avenues of attack on a system. This setting is used to control when a computer disconnects an inactive SMB session.
V-63653	The computer account password must not be prevented from being reset. Computer account passwords are changed automatically on a regular basis. Disabling automatic password changes can make the system more vulnerable to malicious access.
V-63419	The maximum age for machine account passwords must be configured to 60 days or less. Computer account passwords are changed automatically on a regular basis. This setting controls the maximum password age that a machine account may have.

STIG	Description
V-63663	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft. Some features may communicate with the vendor, sending system information or downloading data or components for the feature.
V-71771	Microsoft consumer experiences must be turned off. Microsoft consumer experiences provides suggestions and notifications to users which may include the installation of Windows Store apps.
V-63691	Turning off File Explorer heap termination on corruption must be disabled. Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this.
V-63567	The system must be configured to ignore NetBIOS name release requests except from WINS servers. Configuring the system to ignore name release requests, except from WINS servers, prevents a denial of service (DoS) attack.
V-63815	The default permissions of global system objects must be increased. Windows systems maintain a global list of shared system resources such as DOS device names, mutexes, and semaphores.
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.

STIG	Description
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.

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

BD Biosciences
European Customer Support
Tel +32.53.720.600
help.biosciences@bd.com

bdbiosciences.com
ResearchApplications@bd.com