GeneXpert®
Powered By CEPHEID INNOVATION

GeneXpert®
Security Guidelines

Cepheid® In Vitro Diagnostic Medical Device IVD CE

301-5760, Rev. D November 2019

Trademark and Copyright Statements

Cepheid®, the Cepheid logo, and GeneXpert® are trademarks of Cepheid.

Microsoft® Windows® are trademarks of Microsoft Corporation. Symantec is a trademark of Symantec Corporation or its affiliates in the U.S. and other countries. McAfee is a trademark of McAfee Corporation or its affiliates in the U.S. and other countries. Trend Micro is a trademark of Trend Micro Inc. or its affiliates in the U.S. and other countries. WebEx and Sourcefire are trademarks of Cisco Systems, Inc. Java is a trademark of Oracle Corporation. Other names may be trademarks of their respective owners.

Preface

Cepheid Headquarters Locations

Corporate Headquarters	European Headquarters
Cepheid 904 Caribbean Drive Sunnyvale, CA 94089-1189 USA	Cepheid Europe SAS Vira Solelh 81470 Maurens-Scopont France
Telephone: + 1 408 541 4191	Telephone: + 33 563 825 300
Fax: + 1 408 541 4192	Fax: + 33 563 825 301
www.cepheid.com	www.cepheidinternational.com

Technical Assistance

Before contacting Cepheid Technical Support, collect the following information:

- Product name
- Serial number of the instrument
- Error messages (if any)
- Software version and, if applicable, Computer Service Tag number

Region	Telephone	Email
US	+ 1 888 838 3222	techsupport@cepheid.com
Australia and New Zealand	+ 1800 130 821 + 0800 001 028	techsupportANZ@cepheid.com
Belgium, Netherlands and Luxembourg	+ 33 563 825 319	support@cepheideurope.com
Brazil and Latin America	+ 55 11 3524 8373	latamsupport@cepheid.com
China	+ 86 021 5406 5387	techsupportchina@cepheid.com
France	+ 33 563 825 319	support@cepheideurope.com
Germany	+ 49 69 710 480 480	support@cepheideurope.com
India, Bangladesh, Bhutan, Nepal and Sri Lanka	+ 91 11 48353010	techsupportindia@cepheid.com
Italy	+ 39 800 902 567	support@cepheideurope.com
Portugal	+ 351 800 913 174	support@cepheideurope.com
Spain	+ 34 919 90 67 62	support@cepheideurope.com
South Africa	+ 27 861 22 76 35	support@cepheideurope.com
United Kingdom	+ 44 3303 332 533	support@cepheideurope.com
Other European, Middle East and African countries	+ 33 563 825 319 + 971 4 253 3218	support@cepheideurope.com
Other countries not listed above	+ 1 408 400 8495	techsupport@cepheid.com

Contact information for other Cepheid offices is available on our website at www.cepheid.com or www.cepheidinternational.com under the **SUPPORT** tab. Select the **Contact Us** option.

🏭

Cepheid

904 Caribbean Drive
Sunnyvale, CA 94089

Tel: + 1 408 541 4191
Fax: + 1 408 541 4192

EC REP

Cepheid Europe SAS

Vira Solelh
81470 Maurens-Scopont
France

Tel: + 33 563 825 300
Fax: + 33 563 825 301

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Overview

Cepheid develops, manufactures, and markets the world's leading on-demand molecular diagnostic systems and tests. Ensuring the integrity of our systems and the business continuity of our customers is a top concern for Cepheid. This *GeneXpert® Security Guidelines* document provides a "best practices" guide to assist our customer's information technology (IT) staff where Cepheid diagnostic products are in use.

1.2 Purpose

These best-practice recommendations are intended to increase the overall security posture of the environment where Cepheid diagnostic systems are installed and operated.

Adherence to these recommendations will reduce the overall risk of security threats to computer-based assets.

1.3 Background

Connectivity creates opportunities and challenges for users.

1.4 Audience

The intended audience for this document includes GeneXpert system users, systems administrator, network administrators, and security personnel.

2 Equipment and Software

2.1 Physical Location Security

GeneXpert computers should be in a location secured with badge access.

GeneXpert computers may be physically secured with a cable lock.

2.2 Operating System Users

Limiting account privileges provides simple but effective protection when working on the GeneXpert system. Standard accounts (sometimes called limited accounts) allow most daily activities but do not allow a user to install software or make certain changes to the computer.

Users may install/upgrade Cepheid software following the instructions provided on the respective installation media:

- GeneXpert Dx Installation Instructions
- GeneXpert Dx Operator Manual

A laboratory technician run tests on the GeneXpert system using a standard user account and can access files in the GeneXpert folder on the desktop.

2.3 Operating System Patches

Microsoft designed Windows 10 to have continuous automatic updates. Cepheid has found that the restart after an automatic update can cause the loss of tests running at the time of the update. Cepheid has the following recommendations to ensure that customers do not lose any data due to an unexpected update or restart.

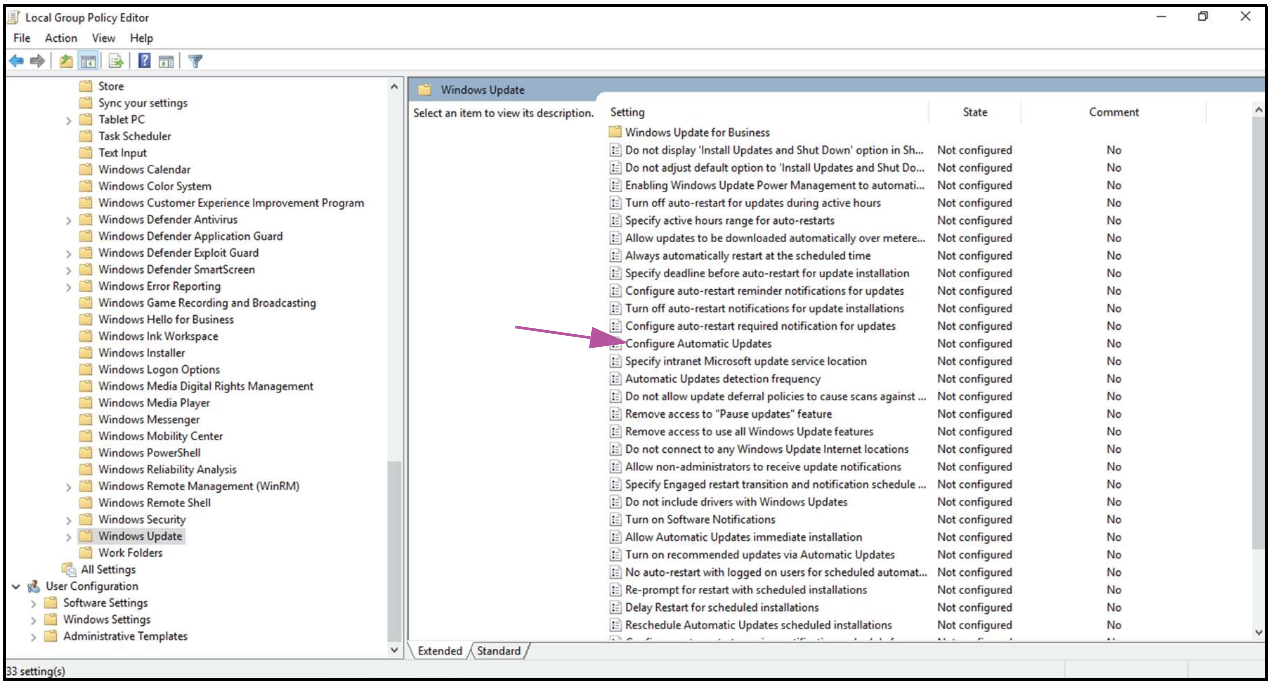
Note If your IT department adds the GeneXpert computer to your company's domain (aka your Active Directory, LDAP, network), then the following changes may get overridden. Please be sure to inform your IT department before proceeding with any of the suggested changes below.

- Section 2.3.1 includes Option A for changing computer settings to avoid loss of tests and data during a computer restart by notifying the customer when to download and install OS patches. Anti-virus updates will continue to download. You will be able to set up notifications for when future updates become available through Microsoft. Finally, this section compiles other available tools to avoid loss of data due to this default Microsoft setting.
- Section 2.3.2 outlines Option B which is highly suggested for customers whose IT departments want to regulate patching internally.

2.3.1 Option A - Edit Group Policy to Notify the Customer When to Download and Install OS Patches

Changing the group policies will prevent inopportune updating and protect your tests. This procedure is intended for customers whose systems are not managed by IT policies.

1. Press Windows key, type **Edit group policy** and click on the result.
2. Double-click **Computer Configuration > Administrative Templates > Windows Components > Windows Update.**
3. Double-click **Configure Automatic Updates.** See Figure 2-1.

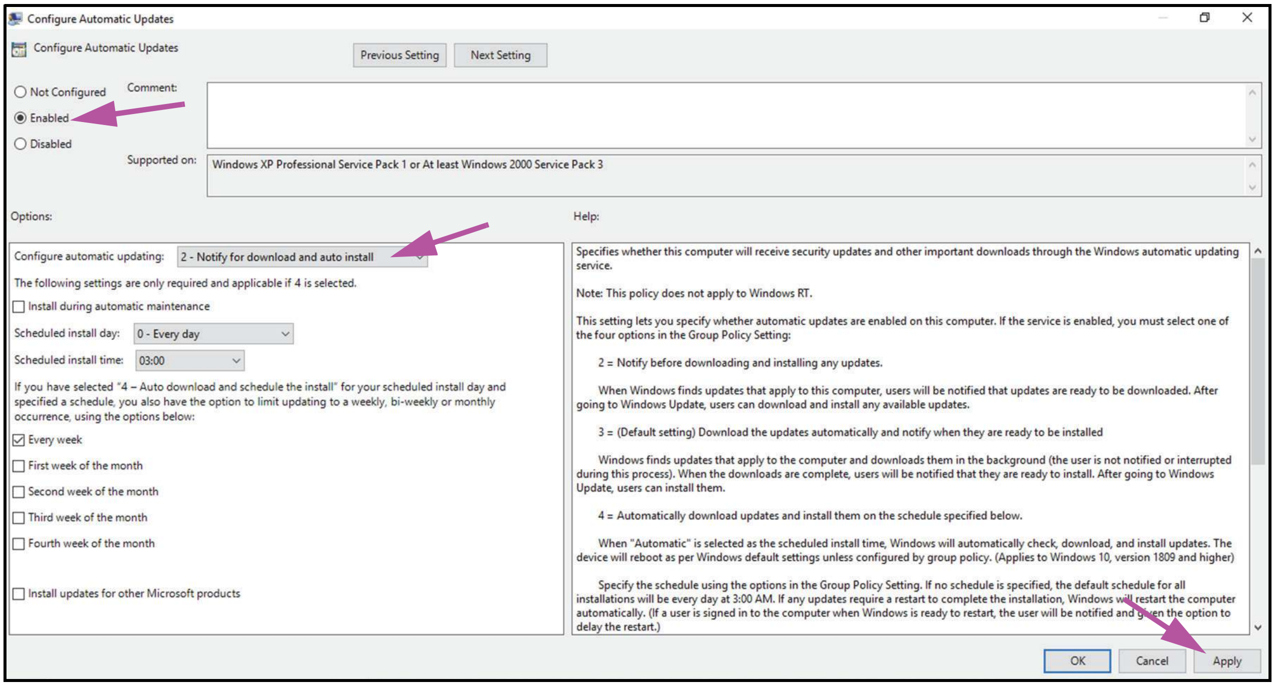


Select an item to view its description.

Setting	State	Comment
Windows Update for Business		
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured	No
Do not adjust default option to 'Install Updates and Shut Do...	Not configured	No
Enabling Windows Update Power Management to automati...	Not configured	No
Turn off auto-restart for updates during active hours	Not configured	No
Specify active hours range for auto-restarts	Not configured	No
Allow updates to be downloaded automatically over metere...	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Specify deadline before auto-restart for update installation	Not configured	No
Configure auto-restart reminder notifications for updates	Not configured	No
Turn off auto-restart notifications for update installations	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure Automatic Updates	Not configured	No
Specify intranet Microsoft update service location	Not configured	No
Automatic Updates detection frequency	Not configured	No
Do not allow update deferral policies to cause scans against ...	Not configured	No
Remove access to "Pause updates" feature	Not configured	No
Remove access to use all Windows Update features	Not configured	No
Do not connect to any Windows Update Internet locations	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Specify Engaged restart transition and notification schedule ...	Not configured	No
Do not include drivers with Windows Updates	Not configured	No
Turn on Software Notifications	Not configured	No
Allow Automatic Updates immediate installation	Not configured	No
Turn on recommended updates via Automatic Updates	Not configured	No
No auto-restart with logged on users for scheduled automat...	Not configured	No
Re-prompt for restart with scheduled installations	Not configured	No
Delay Restart for scheduled installations	Not configured	No
Reschedule Automatic Updates scheduled installations	Not configured	No

Figure 2-1. Local Group Policy Editor

4. Select **Enabled**. See Figure 2-2.
5. Select **2 - Notify for download and auto-install**. See Figure 2-2.



Configure Automatic Updates

Configure Automatic Updates

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Options:

Configure automatic updating: 2 - Notify for download and auto install

The following settings are only required and applicable if 4 is selected.

□ Install during automatic maintenance

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

☑ Every week

□ First week of the month

□ Second week of the month

□ Third week of the month

□ Fourth week of the month

□ Install updates for other Microsoft products

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and downloads them in the background (the user is not notified or interrupted during this process). When the downloads are complete, users will be notified that they are ready to install. After going to Windows Update, users can install them.

4 = Automatically download updates and install them on the schedule specified below.

When "Automatic" is selected as the scheduled install time, Windows will automatically check, download, and install updates. The device will reboot as per Windows default settings unless configured by group policy. (Applies to Windows 10, version 1809 and higher)

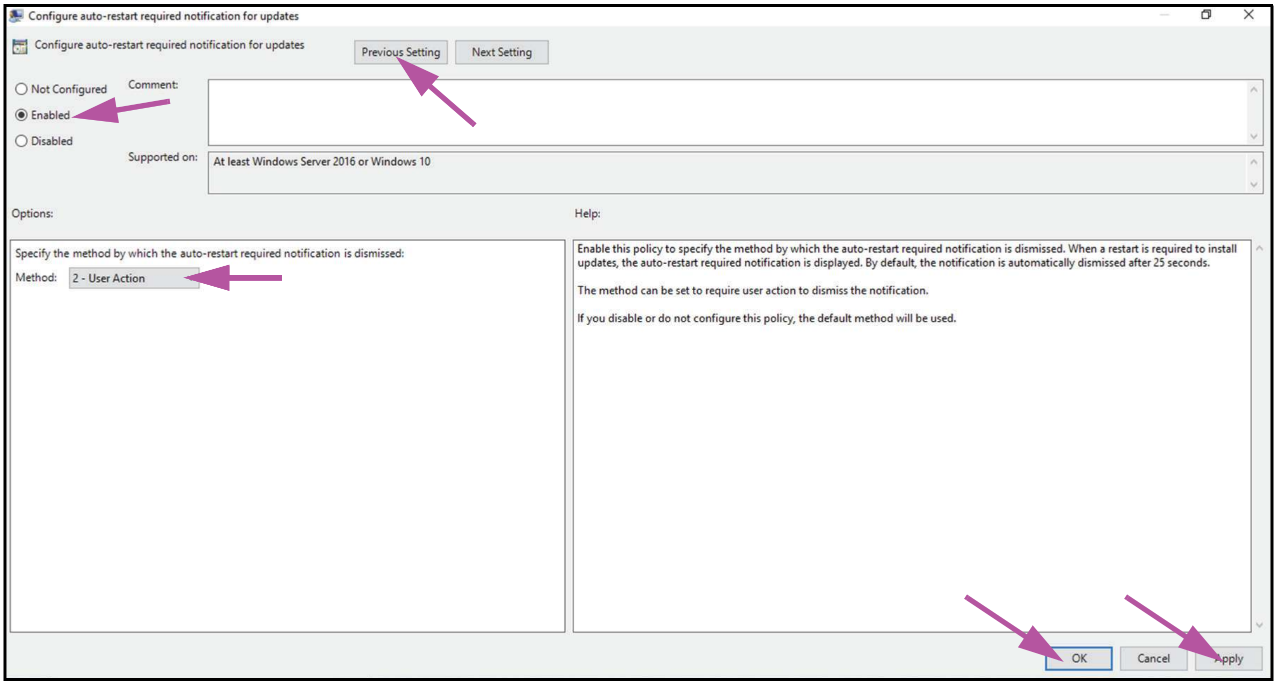
Specify the schedule using the options in the Group Policy Setting. If no schedule is specified, the default schedule for all installations will be every day at 3:00 AM. If any updates require a restart to complete the installation, Windows will restart the computer automatically. (If a user is signed in to the computer when Windows is ready to restart, the user will be notified and given the option to delay the restart.)

OK | Cancel | Apply

Figure 2-2. Configure Automatic Updates

6. Click **Apply.**

7. Click **Previous Setting** (User should be on **Configure auto-restart required notification for updates**). See Figure 2-3.



Configure auto-restart required notification for updates

Configure auto-restart required notification for updates

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016 or Windows 10

Options:

Specify the method by which the auto-restart required notification is dismissed:

Method: 2 - User Action

Help:

Enable this policy to specify the method by which the auto-restart required notification is dismissed. When a restart is required to install updates, the auto-restart required notification is displayed. By default, the notification is automatically dismissed after 25 seconds.

The method can be set to require user action to dismiss the notification.

If you disable or do not configure this policy, the default method will be used.

OK | Cancel | Apply

Figure 2-3. Configure Auto-Restart Notifications

8. Select **Enabled**, select **2 - User Action.** See Figure 2-3.

9. Click **Apply** and then click **OK.**

10. Close Local Group Policy Editor window.
11. Confirm changes:
    A. Click **Start** > **Settings** (Gear icon).
    B. Click **Update & Security.** See Figure 2-4. The user can see if updates are available and ready to download and install. See Figure 2-5.
12. Manually check for updates and only install at a convenient time (not during tests).

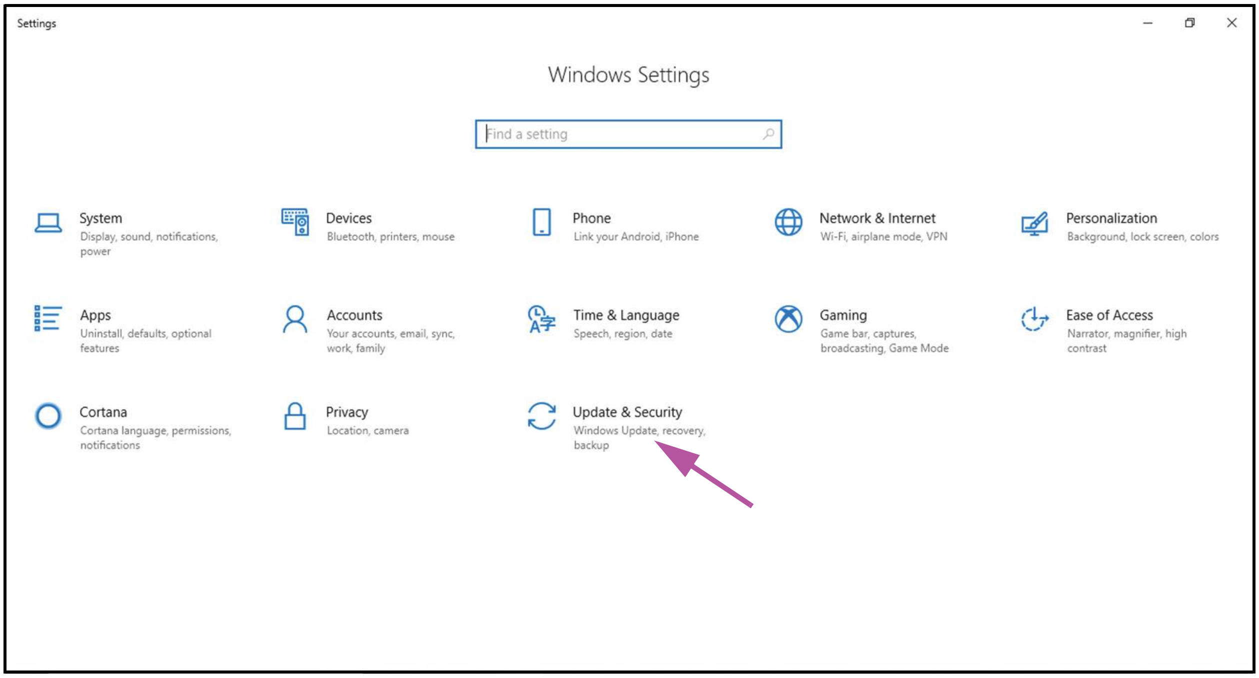
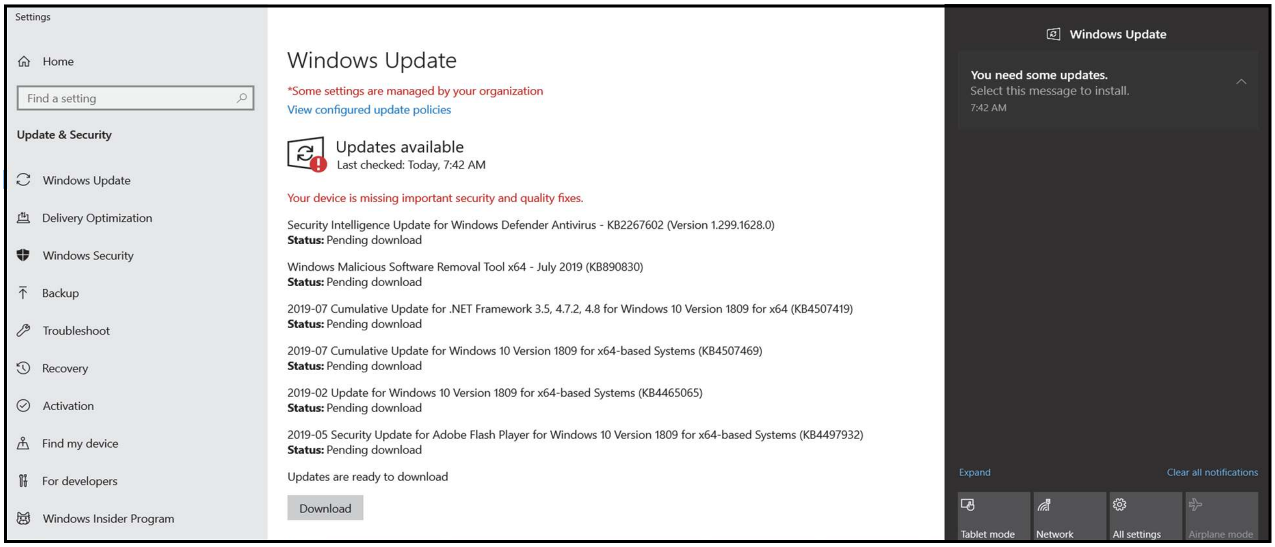

Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Game bar, captures, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Cortana
Cortana language, permissions, notifications
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup

Figure 2-4. Windows Settings



Windows Update

*Some settings are managed by your organization

View configured update policies

Updates available
Last checked: Today, 7:42 AM

Your device is missing important security and quality fixes.

Security Intelligence Update for Windows Defender Antivirus - KB2267602 (Version 1.299.1628.0)
Status: Pending download

Windows Malicious Software Removal Tool x64 - July 2019 (KB890830)
Status: Pending download

2019-07 Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10 Version 1809 for x64 (KB4507419)
Status: Pending download

2019-07 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4507469)
Status: Pending download

2019-02 Update for Windows 10 Version 1809 for x64-based Systems (KB4465065)
Status: Pending download

2019-05 Security Update for Adobe Flash Player for Windows 10 Version 1809 for x64-based Systems (KB4497932)
Status: Pending download

Updates are ready to download

Download

Windows Update

You need some updates.
Select this message to install.
7:42 AM

Figure 2-5. Windows Update Available

Note — **Cepheid** recommends making the following changes so that customers can take control of the patching and restart.

Important — **Lab users should be trained to restart the computer only when the GeneXpert system is not running tests.**

Additional recommendations

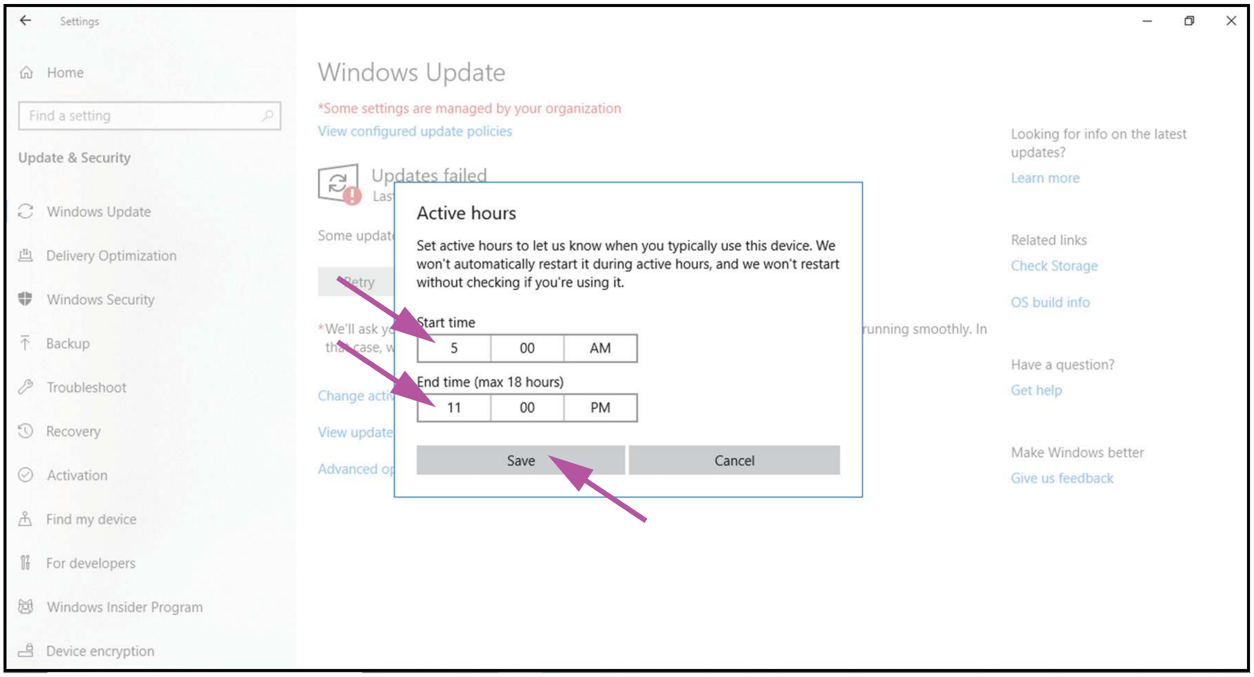
Cepheid recommends implementing the following additional actions to ensure that updates are only installed when the GeneXpert system is not running tests.

1. Click **Start** > **Settings** (Gear icon) > **Update & Security**
2. Proceed to Change the Active Hours and Change Advanced Options.

Change the Active Hours

Change the active hours in order to reduce the chance of an update installation while the GeneXpert system is running tests.

1. Click **Change active hours**
2. Change the active hours to 5 am-11 pm (maximum of 18 hours). See Figure 2-6.
3. Select **Save.**



*Some settings are managed by your organization

View configured update policies

*We'll ask y... tha case, w... running smoothly. In

Active hours

Set active hours to let us know when you typically use this device. We won't automatically restart it during active hours, and we won't restart without checking if you're using it.

Start time: 5 : 00 : AM

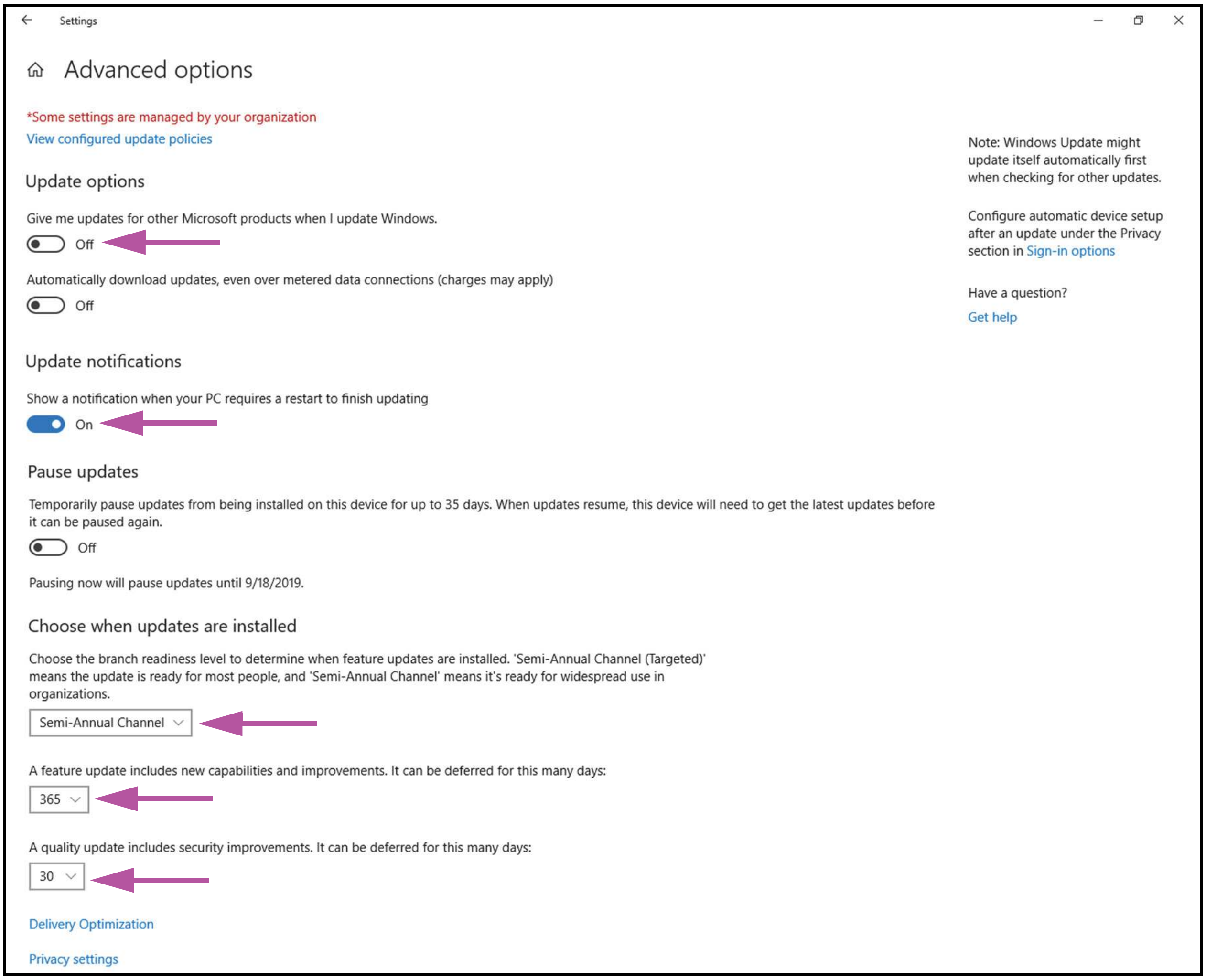
End time (max 18 hours): 11 : 00 : PM

Figure 2-6. Active Hours

Change Advanced Options

The optional advanced settings you can change will further protect you against an unintentional update that could cause data and test losses.

1. Click **Advanced options.**
2. Turn **OFF** the **Give me updates for other Microsoft products when I update Windows** setting. Enabling it will download SQL Server Express updates and the GeneXpert application will stop running. See Figure 2-7.
3. Turn **ON** notifications for updates in **Update notifications.** See Figure 2-7.
4. Choose the **Semi-Annual Channel** for updates that are ready for widespread use in organizations. See Figure 2-7.
5. Defer feature updates (new capabilities and improvements) for up to **365 days**. See Figure 2-7.
6. Defer quality updates (security patches) for up to **30 days.** See Figure 2-7.


Settings

Advanced options

*Some settings are managed by your organization

View configured update policies

Update options

Give me updates for other Microsoft products when I update Windows.

Off

Automatically download updates, even over metered data connections (charges may apply)

Off

Update notifications

Show a notification when your PC requires a restart to finish updating

On

Pause updates

Temporarily pause updates from being installed on this device for up to 35 days. When updates resume, this device will need to get the latest updates before it can be paused again.

Off

Pausing now will pause updates until 9/18/2019.

Choose when updates are installed

Choose the branch readiness level to determine when feature updates are installed. 'Semi-Annual Channel (Targeted)' means the update is ready for most people, and 'Semi-Annual Channel' means it's ready for widespread use in organizations.

Semi-Annual Channel

A feature update includes new capabilities and improvements. It can be deferred for this many days:

365

A quality update includes security improvements. It can be deferred for this many days:

30

Delivery Optimization

Privacy settings

Note: Windows Update might update itself automatically first when checking for other updates.

Configure automatic device setup after an update under the Privacy section in Sign-in options

Have a question?

Get help

Figure 2-7. Advanced Options

2.3.2 Option B - Disable the Windows Update Service

The following steps are appropriate for those customers whose IT departments want to control patching internally.

1. Click **Start > Settings** (Gear icon).
2. Type **Services** in the search field, select **View local services.** See Figure 2-8.

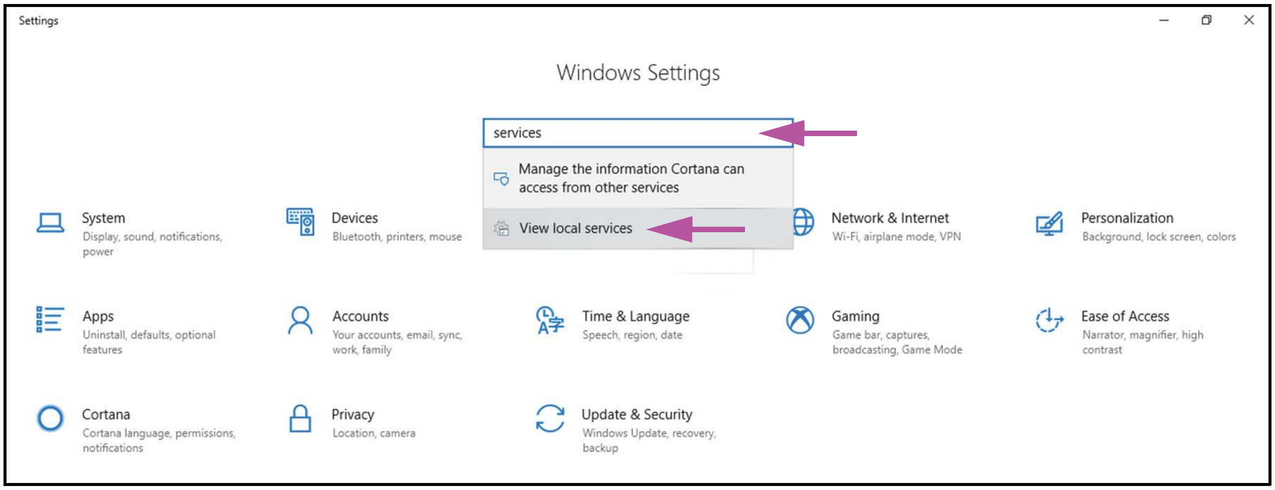
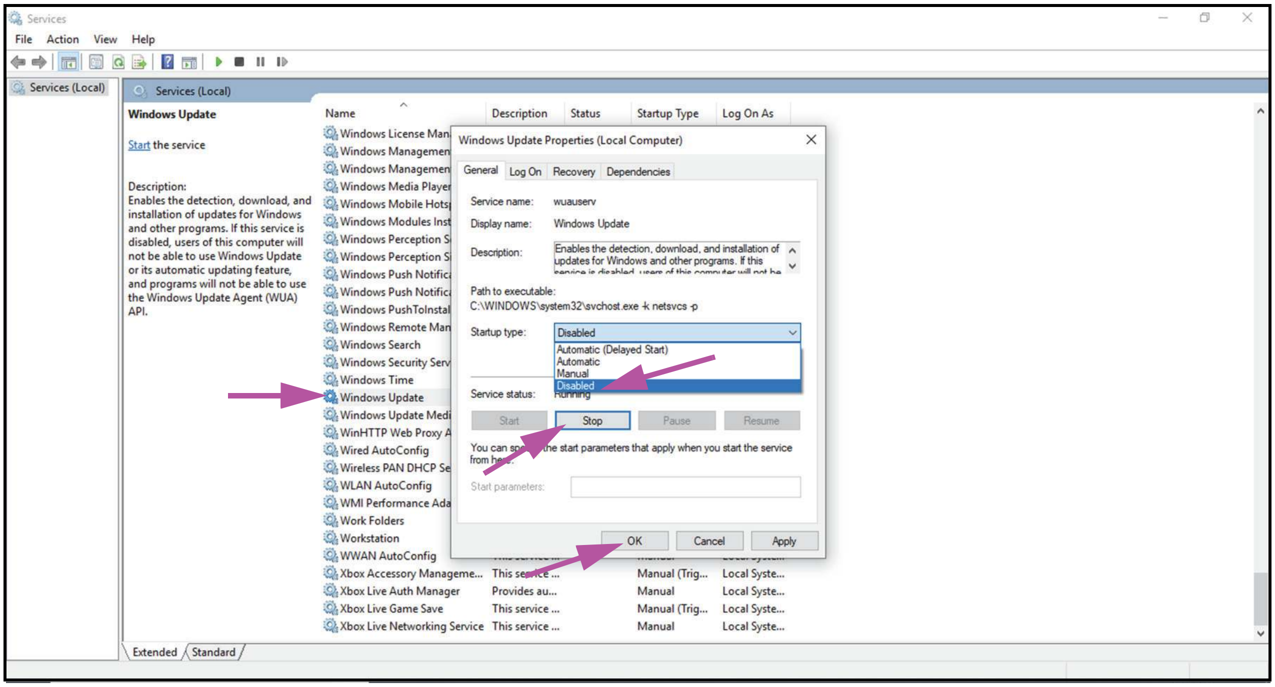

Settings
Windows Settings
services
Manage the information Cortana can access from other services
View local services
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Game bar, captures, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Cortana
Cortana language, permissions, notifications
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup

Figure 2-8. Windows Settings - Services

3. Scroll down to and double-click **Windows Update.**
4. Click the **Stop** button and then change **Startup type** to **Disabled.** See Figure 2-9.



Description:
Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.

Name	Description	Status	Startup Type	Log On As
Xbox Accessory Manageme...	This service ...		Manual (Trig...	Local Syste...
Xbox Live Auth Manager	Provides au...		Manual	Local Syste...
Xbox Live Game Save	This service ...		Manual (Trig...	Local Syste...
Xbox Live Networking Service	This service ...		Manual	Local Syste...

Service name: wuauserv

Display name: Windows Update

Description: Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be

Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs -p

Startup type: Disabled

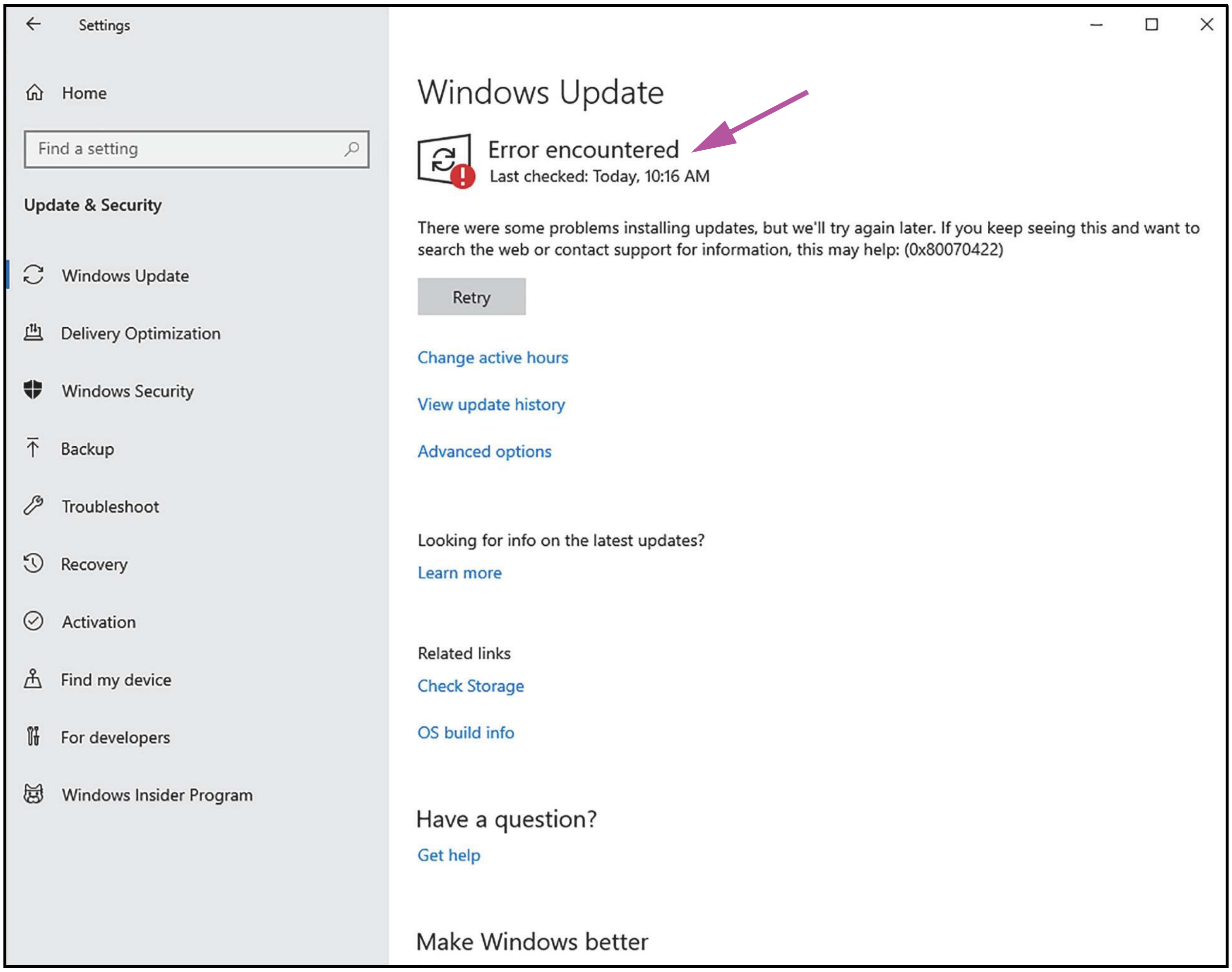
Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 2-9. Windows Update Properties

5. Click the **OK** button to save changes.
6. Confirm changes:
    - A. Click **Start** >**Settings** (Gear icon) > **Update & Security**
    - B. Click **Check for updates**
    - C. User will receive a message titled “Error encountered”. Windows can no longer download updates automatically. This means that the GeneXpert tests will not be interrupted by an unintended Windows restart. See Figure 2-10.



Windows Update

Error encountered

Last checked: Today, 10:16 AM

There were some problems installing updates, but we'll try again later. If you keep seeing this and want to search the web or contact support for information, this may help: (0x80070422)

Looking for info on the latest updates?

Have a question?

Make Windows better

Figure 2-10. Windows Update Error Encountered

2.4 Disk Encryption

Note Before you begin, please keep in mind that encrypting your entire hard disk can be a long process. You will be able to use your computer while encryption takes place in the background, but you will eventually need to restart your computer. Save files frequently and plan accordingly.

BitLocker is an encryption system designed to prevent most offline attacks and malware. It is essential for you to use this feature to protect your data and keep confidential information secure. The procedure for Enabling BitLocker Drive Encryption in Windows 10 is included below.

Cepheid has validated BitLocker disk encryption on GeneXpert computers running Windows 10.

Customers are responsible for enabling BitLocker and setting the encryption key.

Note If your computer includes a Trusted Platform Module (TPM), please skip to Step 10. If your device does not include a Trusted Platform Module (TPM) chip, you will not be able to turn on BitLocker in Windows 10. You can still use encryption, but you will need to use the Local Group Policy Editor to enable additional authentication at startup. Start at Step 1 below.

1. If you are using a tablet or touch screen device, switch to desktop mode.
2. Use the **Windows key + R** keyboard shortcut to open the Run command > type **gpedit.msc** > click **OK**.
3. Under Computer Configuration, expand **Administrative Templates**.
4. Expand **Windows Components**.
5. Expand **BitLocker Drive Encryption** and **Operating System Drives**.
6. On the right side, double-click **Require additional authentication at startup**.
7. Select **Enabled**.
8. Check the **Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)** option.
9. Click **OK** to complete this process.
10. Click **Start > File Explorer > This PC**.
11. Under **Devices and drives**, right-click your system drive (on touch screen devices, press and hold) where Windows 10 is installed, then click **Turn on BitLocker**.
12. Enter a password to unlock your drive. This is important to ensure you can boot the system even if you lose the recovery key.

Note Cepheid recommends a password of 10 characters minimum with a combination of upper/lower case letters, numbers, and symbols.

- Choose how to back up your recovery key:
  - Save to your Microsoft account
  - Save to a USB flash drive
  - Save to a file (not to local hard drive)
  - Print the recovery key

Note Cepheid suggests saving to a USB flash drive and printing the recovery key and archiving the recovery key with your IT department.

13. Choose how much of your drive to encrypt:
    - Encrypt used disk space (faster and best for new PCs and drives)
    - Encrypt entire drive (slower but best for PCs and drives in use)

Note Cepheid recommends encrypting the entire drive.

- Choose which encryption mode to use:
- New encryption mode (best for fixed drives on this device)
- Compatible mode (best for drives to that can be moved from this device)

Note Cepheid recommends that you use the new encryption mode (XTS-AES) since drives do not move from computer to computer.

14. Check the box next to **Run BitLocker system check.**
15. Restart your computer.
16. When prompted, enter your password.
17. After logging into Windows 10, you can check the status of encryption
    - Click **Start > File Explorer > This PC**
    - You will now see a padlock emblem on the system drive.
    - Right-click (press and hold) the drive then select **Manage BitLocker**
    - You will see the current status which should be **C: BitLocker Encrypting**
    - You can continue using your computer while encryption takes place in the background
    - You will be notified when it is complete.

Once BitLocker Encryption is finished, all content and communications will be secured.

2.5 Anti-virus

Customers should run anti virus software on the GeneXpert system computer and ensure that the virus definitions are always up to date.

Customers should schedule anti-virus updates when the system is not in use.

Customers should schedule Quick or Full Scans when the system is not in use.

Table 2-1. Summary of Validated Antivirus Solutions for GeneXpert Dx and Infinity-80/Infinity-48s Systems

Cepheid Systems Software	McAfee Antivirus Plus	Norton Antivirus	Windows Defender Antivirus included as part of Windows 10
GeneXpert Dx 5.1 or higher on Windows 7	X		
GeneXpert Dx 5.1 or higher on Windows 10			X
Xpertise 6.6 or higher on Windows 7		X	
Xpertise 6.6 or higher on Windows 10			X
Cepheid Link 1.0 on Windows 7		X	

2.6 Anti-Virus Exclusions

An anti-virus exclusion is a user-defined configuration that instructs an anti-virus program to exclude certain files from being scanned to avoid performance issues due to file contention and/or file locking.

Table 2-2. Exclusions for Xpertise 4.x on Windows 7

Program	Properties
Javaw, Java	C:\Program Files\Cepheid\GeneXpert 4.0\JRE\bin
Bcserver	C:\Program Files\Cepheid\GeneXpert 4.0\tools\bcserver.exe

Table 2-3. Exclusions for Xpertise 6.x on Windows 7

Program	Properties
Javaw, Java	C:\Program Files\Cepheid\GeneXpert 6.x\JRE\bin
Bcserver	C:\Program Files\Cepheid\GeneXpert 6.x\bin
InfShutdown	C:\Program Files\Cepheid\GeneXpert 6.x\bin

Table 2-4. Exclusions for GeneXpert Dx on Windows 7

Program	Properties
Javaw, Java	C:\Program Files\Cepheid\GeneXpert 4.0\JRE\bin

Table 2-5. Exclusions for Xpress on Windows 7

Program	Properties
Javaw, Java	C:\Program Files\Cepheid\GeneXpert 4.x\JRE\bin

Table 2-6. Exclusions for GeneXpert Dx on Windows 10

Program	Properties
Javaw, Java	C:\Program Files\Cepheid\GeneXpert Dx\JRE\bin

2.6.1 Adding Anti-virus Exclusions in Windows 10

1. Click **Start** > **Settings** (Gear icon) > **Update & Security.** See Figure 2-11.

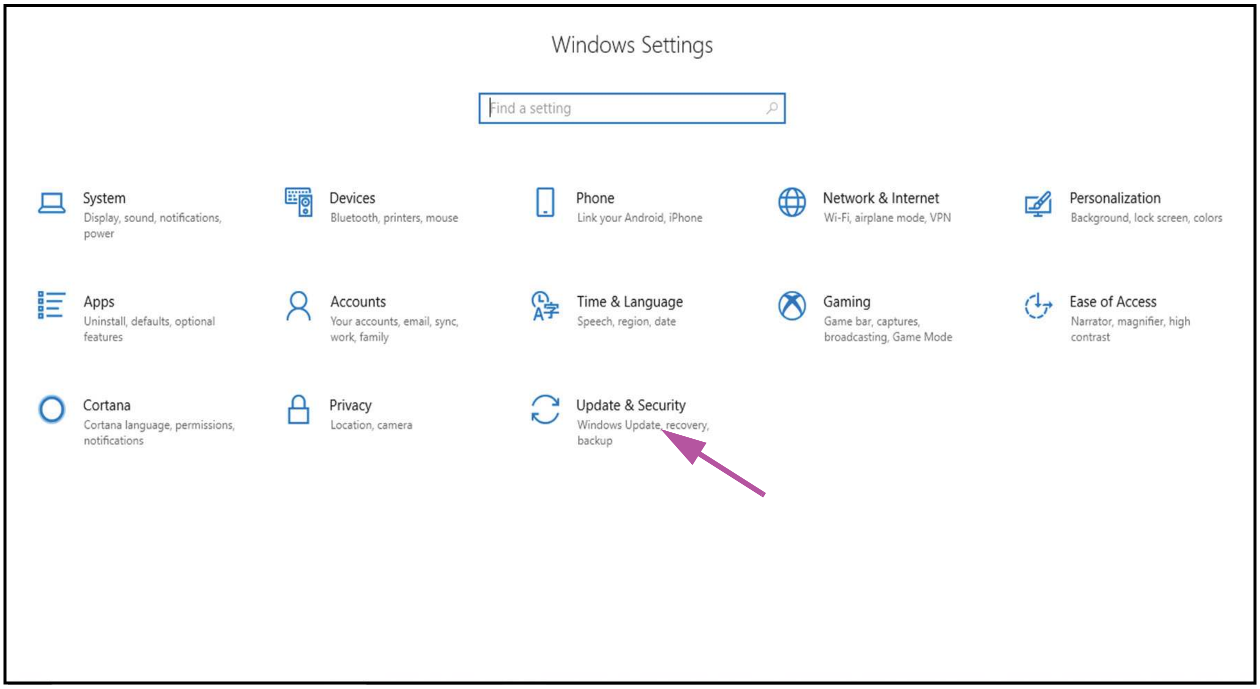
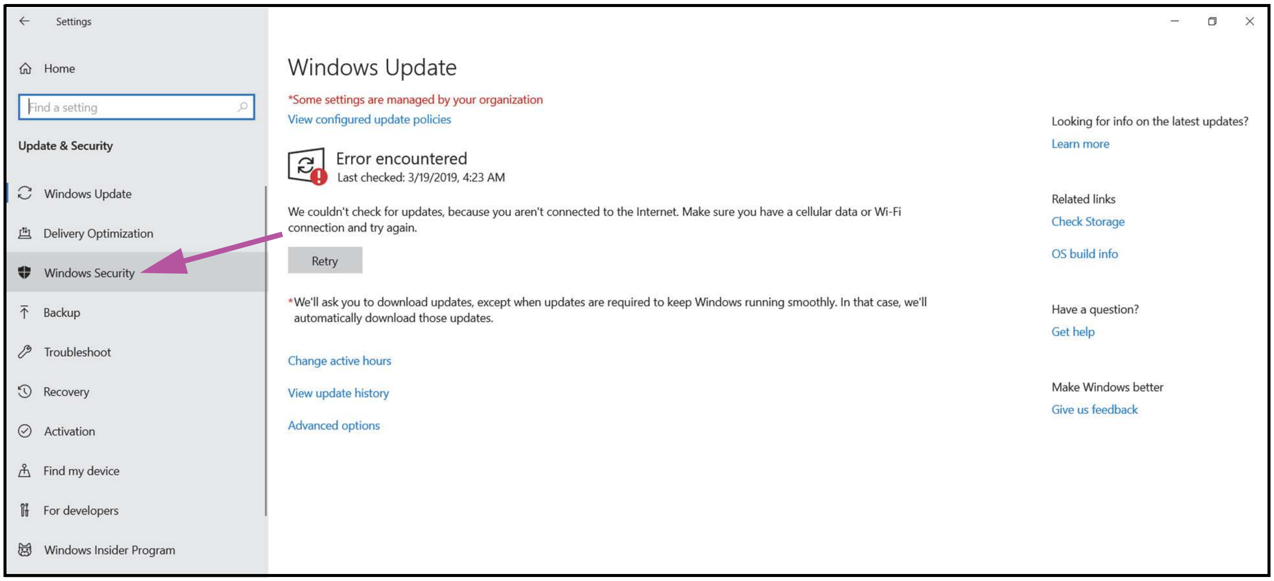

Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Game bar, captures, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Cortana
Cortana language, permissions, notifications
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup

Figure 2-11. Windows Settings

2. Click **Windows Security.** See Figure 2-12.



Windows Update

*Some settings are managed by your organization

Error encountered

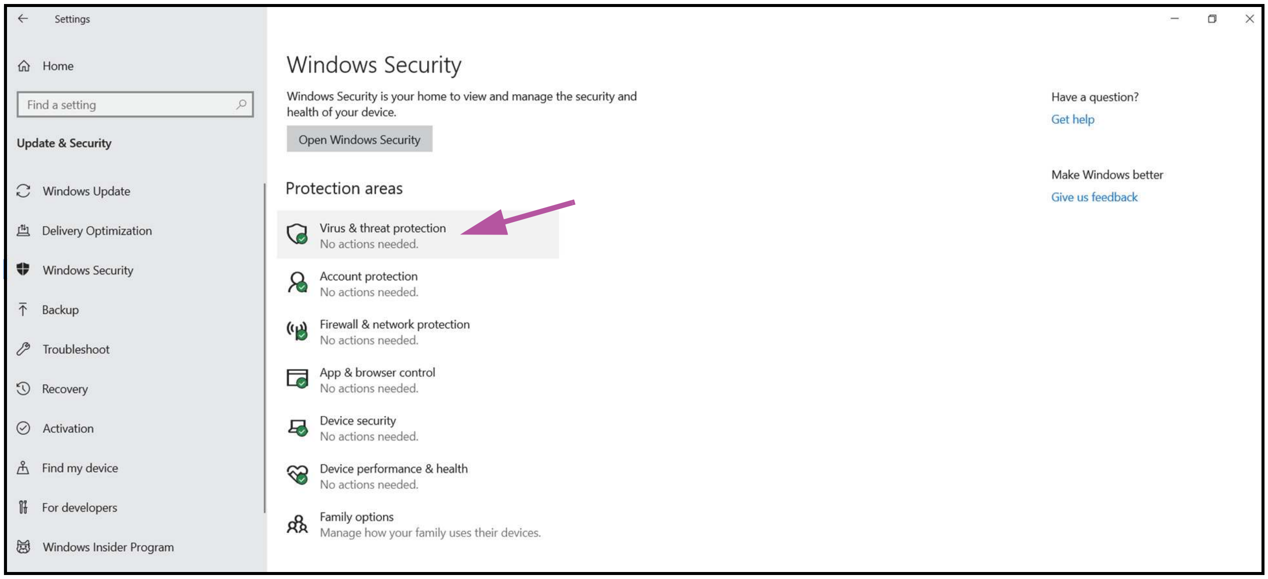
Last checked: 3/19/2019, 4:23 AM

We couldn't check for updates, because you aren't connected to the Internet. Make sure you have a cellular data or Wi-Fi connection and try again.

*We'll ask you to download updates, except when updates are required to keep Windows running smoothly. In that case, we'll automatically download those updates.

Figure 2-12. Windows Security

3. Click **Virus and Threat Protection**. See Figure 2-13.



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

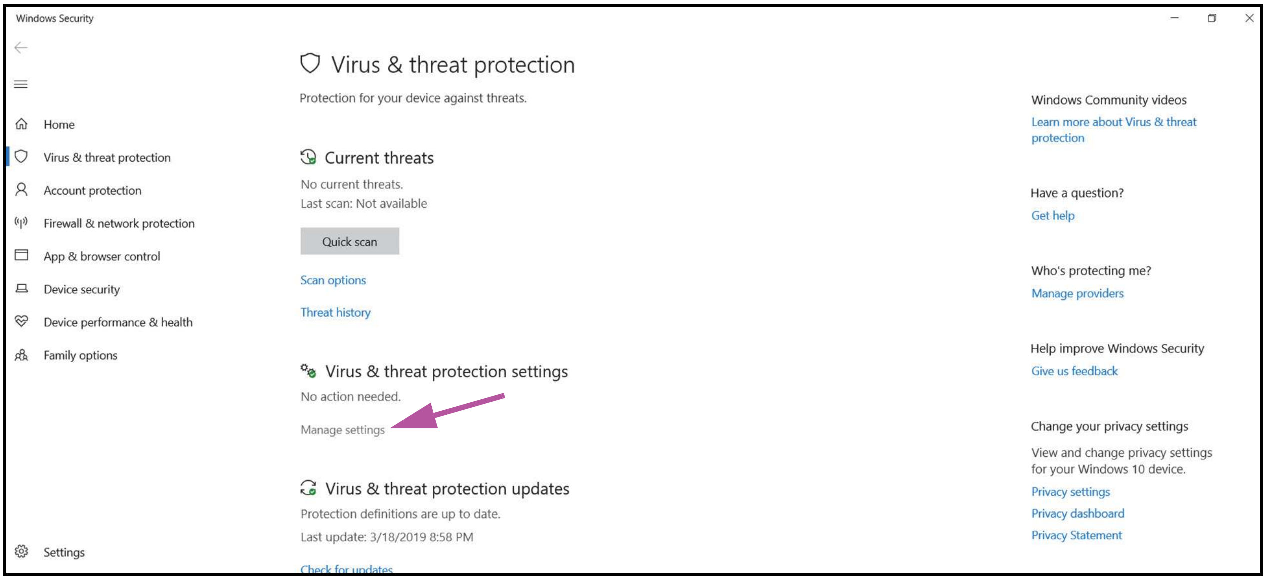
Device security
No actions needed.

Device performance & health
No actions needed.

Family options
Manage how your family uses their devices.

Figure 2-13. Virus & Threat Protection

4. Click **Manage Settings**. See Figure 2-14.



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: Not available

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Protection definitions are up to date.
Last update: 3/18/2019 8:58 PM

Windows Community videos

Learn more about Virus & threat protection

Have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

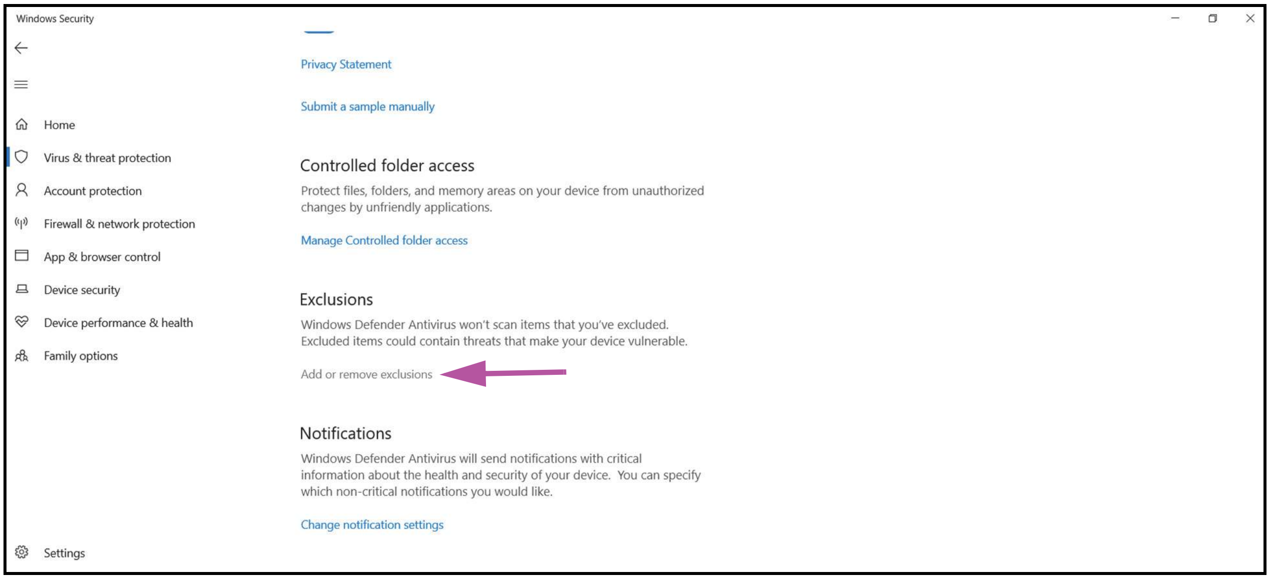
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings
Privacy dashboard
Privacy Statement

Figure 2-14. Manage Protection Settings

5. Scroll down and click **Add or remove exclusions**. See Figure 2-15.



Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

Exclusions

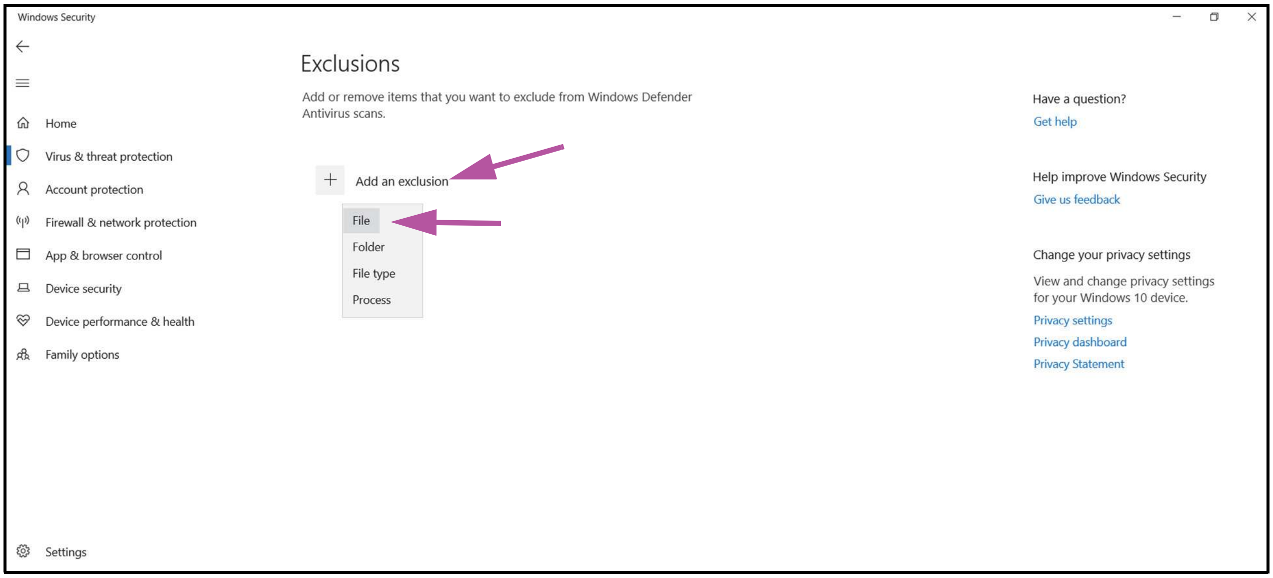
Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.

Notifications

Windows Defender Antivirus will send notifications with critical information about the health and security of your device. You can specify which non-critical notifications you would like.

Figure 2-15. Add or Remove Exclusions

6. Click **Add an exclusion**> **File**. See Figure 2-16.



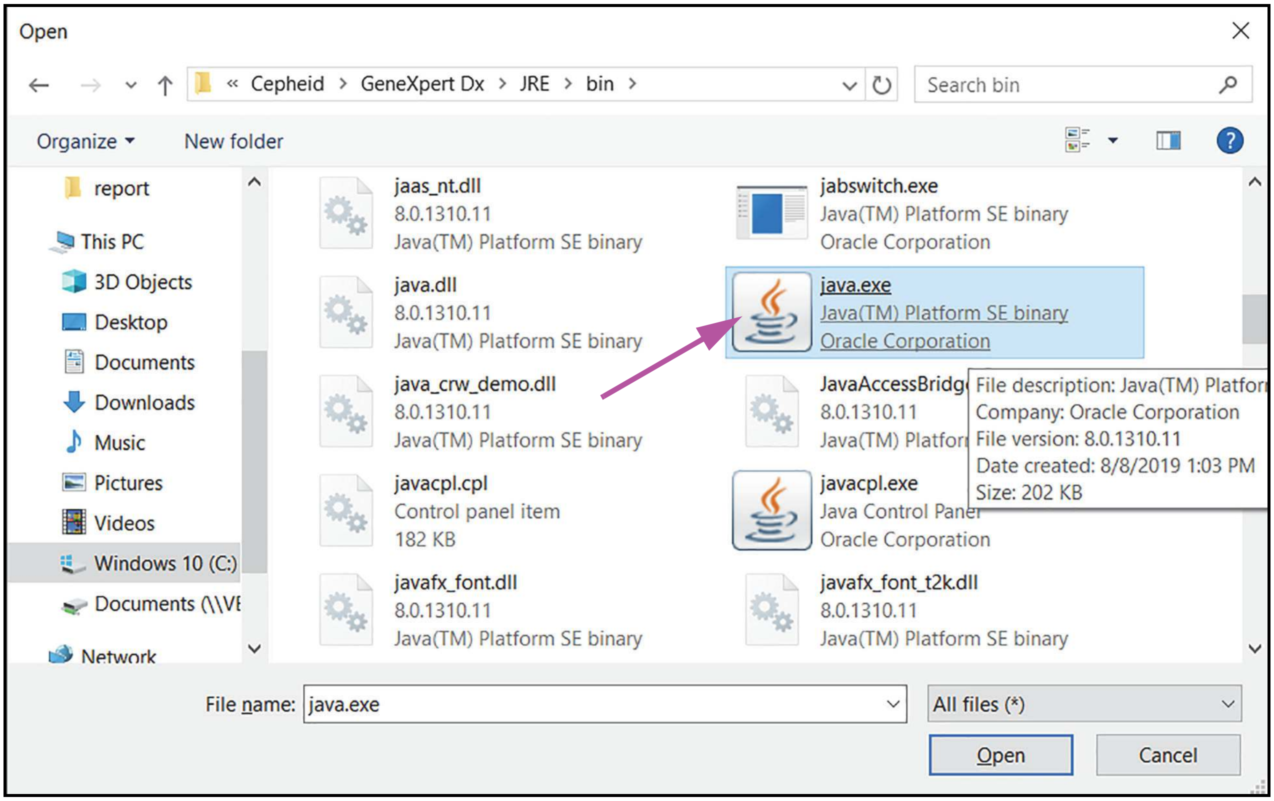
Windows Security

Exclusions

Add or remove items that you want to exclude from Windows Defender Antivirus scans.

Figure 2-16. Add an Exclusion

7. Navigate to **C:\Program Files\Cepheid\GeneXpert Dx\JRE\bin**, click on **java.exe.** See Figure 2-17.



Open

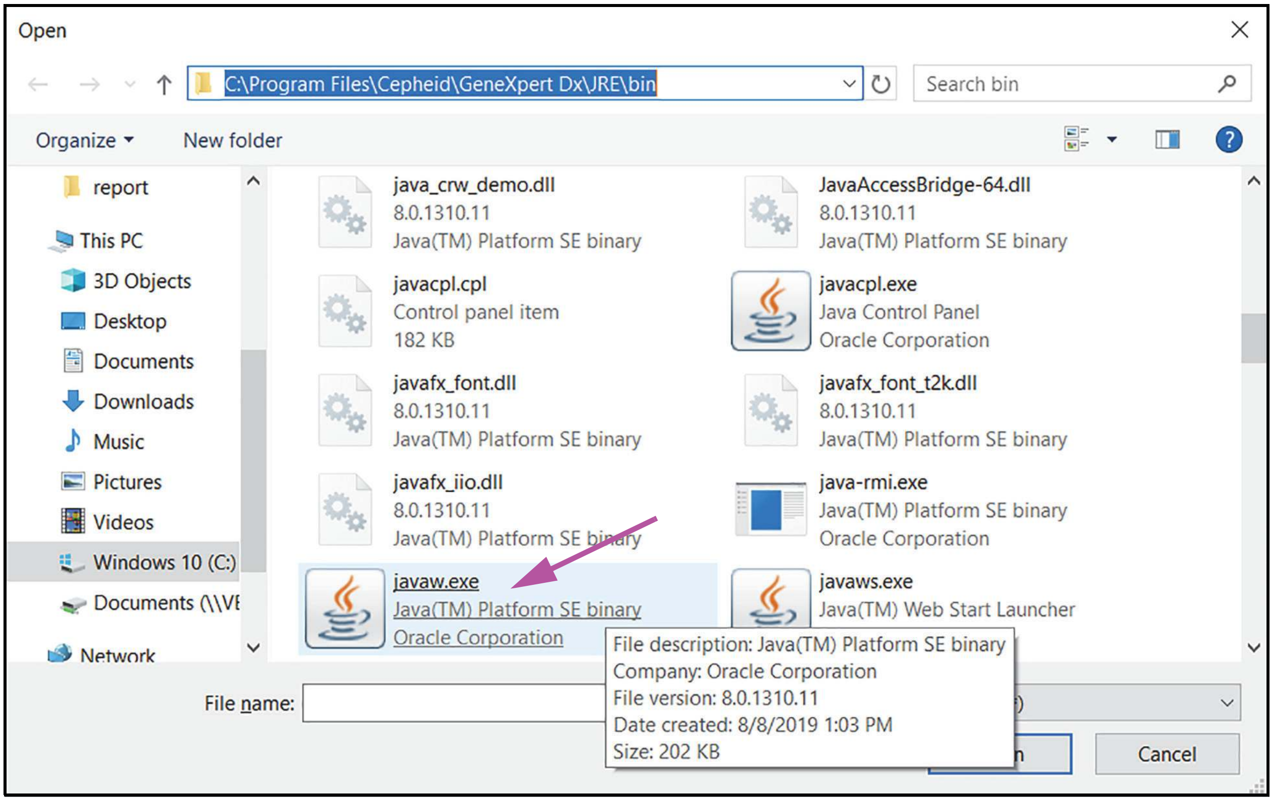
File name: java.exe

File description: Java(TM) Platfor
Company: Oracle Corporation
File version: 8.0.1310.11
Date created: 8/8/2019 1:03 PM
Size: 202 KB

Figure 2-17. Location of Java.exe

8. Click **Add an exclusion** > **File**. See Figure 2-16.

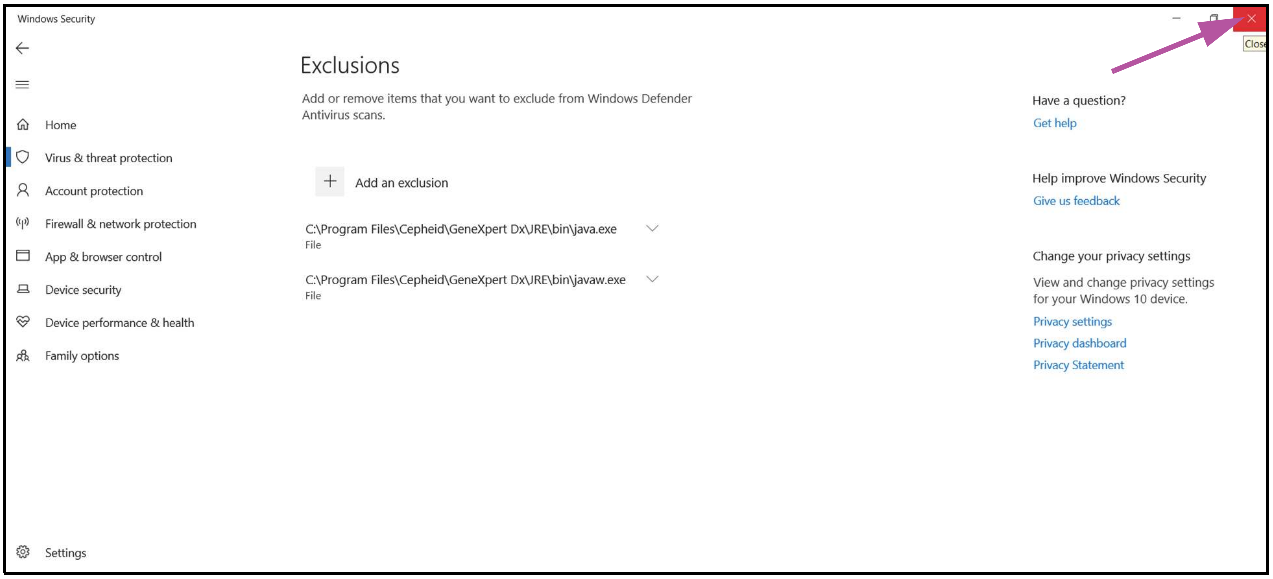
9. Navigate to **C:\Program Files\Cepheid\GeneXpert Dx\JRE\bin**, click on **javaw.exe**. See Figure 2-18.



File description: Java(TM) Platform SE binary
Company: Oracle Corporation
File version: 8.0.1310.11
Date created: 8/8/2019 1:03 PM
Size: 202 KB

Figure 2-18. Location of Javaw.exe

10. Close the window by clicking the **X** in the top right corner. See Figure 2-19.



Exclusions

Add or remove items that you want to exclude from Windows Defender Antivirus scans.

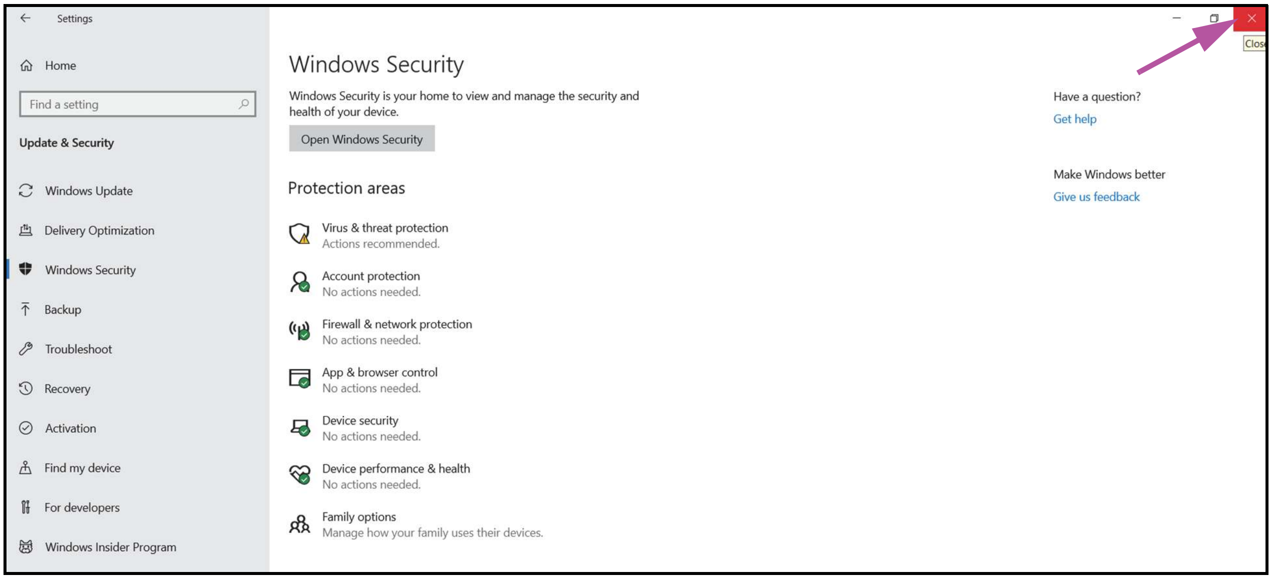
C:\Program Files\Cepheid\GeneXpert Dx\JRE\bin\java.exe
File

C:\Program Files\Cepheid\GeneXpert Dx\JRE\bin\javaw.exe
File

View and change privacy settings for your Windows 10 device.

Figure 2-19. Closing Exclusions Window

11. Close the window by clicking the **X** in the top right corner. See Figure 2-20.



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
Actions recommended.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
No actions needed.

Family options
Manage how your family uses their devices.

Figure 2-20. Closing Windows Security Window

2.7 Firewall Exclusions

Note The following exclusions must be added to the firewall if the customer replaces Norton or McAfee with another Firewall such as Microsoft Windows.

Table 2-7. Firewall Exclusions for all GeneXpert Systems

Program	Properties	Scope
GeneXpert Dx /Xpertise	UDP Port: 1207	“Home/Work (Private)” and “Public” and “Domain” (if the computer is defined in domain).
SQL Server Express	TCP Port: 1433	“Home/Work (Private)” and “Public” and “Domain” (if the computer is defined in domain).
InfinityServer (Barcode Scanner)	TCP Port: 2009	“Home/Work (Private)” and “Public” and “Domain” (if the computer is defined in domain).
Infinity Kiosk (Barcode Scanner)	TCP Port: 3009	“Home/Work (Private)” and “Public” and “Domain” (if the computer is defined in domain).
Cepheid Remote Access (Cisco WebEx)	TCP Port: 443	“Home/Work (Private)” and “Public” and “Domain” (if the computer is defined in domain).
Cepheid C360	TCP Port: 80, 443, 8080, 8081	“Home/Work (Private)” and “Public” and “Domain” (if the computer is defined in domain).
Xpert Check	TCP Port: 9096	“Home/Work (Private)” and “Public” and “Domain” (if the computer is defined in domain).

2.8 Browser

Internet browsers are the first target for cyber criminals. Cepheid recommends that users do not use the GeneXpert computer for any purpose other than running tests.

For greater security, Cepheid recommends that the GeneXpert computer be operated without (or with minimal) connectivity to the Internet.

2.9 Java Questions and Answers

Potential security problems with Java

The method of attack is the Java Runtime Environment (JRE) plug-in in the browser. If a user is surfing the internet and comes across some Java code, the JRE will attempt to run it. If the code is malicious, the code might attempt to alter or copy computer files. See Figure 2-21.

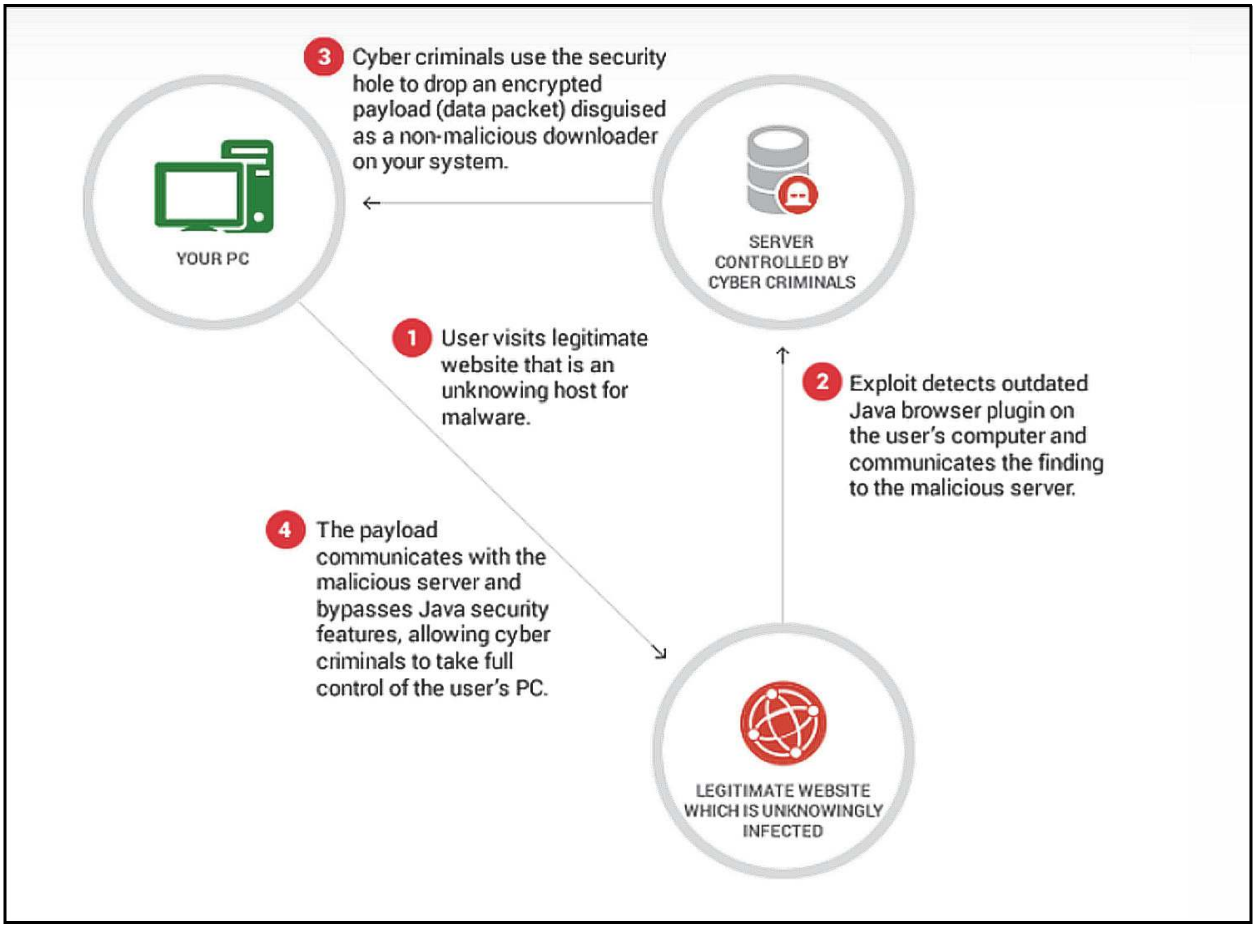

3 Cyber criminals use the security hole to drop an encrypted payload (data packet) disguised as a non-malicious downloader on your system.
YOUR PC
SERVER CONTROLLED BY CYBER CRIMINALS
1 User visits legitimate website that is an unknowing host for malware.
2 Exploit detects outdated Java browser plugin on the user's computer and communicates the finding to the malicious server.
4 The payload communicates with the malicious server and bypasses Java security features, allowing cyber criminals to take full control of the user's PC.
LEGITIMATE WEBSITE WHICH IS UNKNOWINGLY INFECTED

Figure 2-21. Why Java Browser Plug-In can cause security problems[1]

[1] Source: https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/

Why is it OK for Java to be un-patched on a GeneXpert computer?

The Internet Explorer browser that is pre-loaded on the GeneXpert computer does not have the Java plug-in installed. The GeneXpert / Xpertise software runs locally and does not require the internet. Therefore, the risk level is lower if the Java browser plug-in is not installed.

2.10 SQL Server Questions and Answers

In what way are old versions of SQL Server not secure?

Attacks exploit SQL Server where there are existing network connections.

Why is it OK for my SQL Server to be unpatched?

The GeneXpert / Xpertise software communicates with the local database. There is no network traffic to the database. The GeneXpert / Xpertise database has an embedded password that is not known to users.

What if a hot fix or service pack is available through Windows Update?

Do not update SQL Server with hot fixes or service packs until notified by Cepheid Technical Support. If you apply service packs or hot fixes to SQL Server, then the GeneXpert / Xpertise software will not run.

Please contact Cepheid Technical Support to restore the system to its original state working condition if an accidental update has taken place.

2.11 Adobe Questions and Answers

In what way are old versions of Adobe Reader not secure?

GeneXpert systems are preloaded with Adobe Reader IX (validated on Windows XP) or Adobe Reader X (validated on Windows 7) in order to view GeneXpert user documentation provided on the system computer and to view test reports. Adobe Reader IX or X have a known vulnerability through the internet. If a PDF is downloaded and has a web link that points to a malicious site, then Adobe Reader may attempt to download or run malware which could adversely affect the local computer or network.

Why is it OK to use Adobe Reader IX or X and not the latest version?

Adobe Reader is meant for viewing local GeneXpert / Xpertise documentation.

The GeneXpert / Xpertise PDFs do not have web links in them. We recommend that you do not download PDFs from other websites which could have web links in them.

On Windows 10 systems, Cepheid is shipping Adobe Acrobat Reader DC which receives continuous updates if you are connected to the internet.

2.12 Remote Access Questions and Answers

What is Cepheid Remote Access?

Remote Access allows Cepheid Technical Support engineers to securely access GeneXpert systems at customer sites using internet connectivity.

What is Remote Access used for?

Cepheid uses Cisco's WebEx Remote Support to provide:

- Screen Sharing – Cepheid can see what the customer sees.
- Remote Control – Cepheid can take control if the customer authorizes.
- File Transfer – Cepheid can review application logs and archive files.

What is the benefit of Remote Access?

- Remote Access can reduce unplanned service visits.

How can I minimize risk to the GeneXpert computer?

Access to the system is explicitly granted by the customer. Data transport is encrypted and logged. Cepheid can provide official detailed white papers on Cisco WebEx security.

What if a customer wants Cepheid to use another solution such as Secure-Link?

Cepheid will use a customer's preferred method for remote access as long as it can accommodate the following functionalities.

- Screen Sharing
- Remote Control
- File Transfer

2.13 Locked Out Access

In order to make sure customers maintain access to the GeneXpert application and the relevant data stored therein, Cepheid Technical Support has the ability to provide temporary access to a customer's authorized user to unlock the application in case of an inadvertent lock-out.

Cepheid validates authorized users by verifying the institution account details as maintained in Cepheid's ERP system.

2.14 Additional Information

- Please refer to the operator's manual for additional information and please contact Cepheid Technical Support if you have any questions.
- Customers may send IT questionnaires to Cepheid Technical Support.

A Windows Security Updates

The following tables provide a summary of the Windows Operating System updates which were installed for the validation testing of **GeneXpert Dx 6.0**. Reports were generated using the following embedded Windows OS command: **wmic qfe list brief/ format:texttablewsys**

Table A-1. Security Updates - Windows 10 - OS:

Windows 10, OS 1803, Build 17134.345		
Description	**HotFixID**	**Installed On**
Security Update	KB4471331	1/18/2019
Security Update	KB4480979	2/13/2019
Windows 10, OS 1809, Build 17763.253		
Description	**HotFixID**	**Installed On**
Update	KB4100347	1/15/2019
Update	KB4462930	11/29/2018

Table A-2. Security Updates - Windows 7 64-Bit - Service Pack 1

Windows 7 64-bit, SP1		
Description	**HotFixID**	**Installed On**
Update	KB2849697	1/8/2019
Update	KB2849696	1/8/2019
Update	KB2841134	1/8/2019
Update	KB2670838	1/8/2019
Update	KB971033	1/8/2019
Security Update	KB2479943	1/8/2019
Security Update	KB2491683	1/8/2019
Update	KB2506014	1/8/2019
Security Update	KB2506212	1/8/2019
Update	KB2506928	1/8/2019
Update	KB2533552	1/8/2019
Update	KB2545698	1/8/2019
Update	KB2547666	1/8/2019
Update	KB2552343	1/8/2019
Security Update	KB2560656	1/8/2019
Update	KB2563227	1/8/2019
Security Update	KB2564958	1/8/2019
Security Update	KB2579686	1/8/2019
Update	KB2603229	1/8/2019

Table A-2. Security Updates - Windows 7 64-Bit - Service Pack 1

Windows 7 64-bit, SP1		
Security Update	KB2604115	1/8/2019
Security Update	KB2620704	1/8/2019
Security Update	KB2621440	1/8/2019
Security Update	KB2631813	1/8/2019
Update	KB2640148	1/8/2019
Security Update	KB2654428	1/8/2019
Update	KB2660075	1/8/2019
Security Update	KB2667402	1/8/2019
Update	KB2685811	1/8/2019
Update	KB2685813	1/8/2019
Security Update	KB2690533	1/8/2019
Security Update	KB2698365	1/8/2019
Security Update	KB2705219	1/8/2019
Security Update	KB2706045	1/8/2019
Update	KB2719857	1/8/2019
Update	KB2726535	1/8/2019
Security Update	KB2727528	1/8/2019
Update	KB2729094	1/8/2019
Security Update	KB2729452	1/8/2019
Update	KB2732059	1/8/2019
Security Update	KB2736422	1/8/2019
Security Update	KB2742599	1/8/2019
Update	KB2750841	1/8/2019
Update	KB2761217	1/8/2019
Update	KB2763523	1/8/2019
Security Update	KB2770660	1/8/2019
Update	KB2773072	1/8/2019
Update	KB2786081	1/8/2019
Update	KB2791765	1/8/2019
Update	KB2799926	1/8/2019
Update	KB2800095	1/8/2019
Security Update	KB2807986	1/8/2019
Update	KB2808679	1/8/2019
Security Update	KB2813430	1/8/2019
Update	KB2834140	1/8/2019
Security Update	KB2840631	1/8/2019
Update	KB2843630	1/8/2019
Security Update	KB2847927	1/8/2019
Update	KB2852386	1/8/2019
Update	KB2853952	1/8/2019

Table A-2. Security Updates - Windows 7 64-Bit - Service Pack 1

Windows 7 64-bit, SP1		
Security Update	KB2861698	1/8/2019
Security Update	KB2862330	1/8/2019
Security Update	KB2862335	1/8/2019
Security Update	KB2864202	1/8/2019
Security Update	KB2868038	1/8/2019
Security Update	KB2871997	1/8/2019
Security Update	KB2884256	1/8/2019
Update	KB2891804	1/8/2019
Security Update	KB2893294	1/8/2019
Update	KB2893519	1/8/2019
Security Update	KB2894844	1/8/2019
Security Update	KB2900986	1/8/2019
Update	KB2908783	1/8/2019
Security Update	KB2911501	1/8/2019
Update	KB2918077	1/8/2019
Update	KB2919469	1/8/2019
Security Update	KB2931356	1/8/2019
Security Update	KB2937610	1/8/2019
Security Update	KB2943357	1/8/2019
Update	KB2966583	1/8/2019
Security Update	KB2968294	1/8/2019
Security Update	KB2972100	1/8/2019
Security Update	KB2973112	1/8/2019
Security Update	KB2973201	1/8/2019
Security Update	KB2977292	1/8/2019
Security Update	KB2978742	1/8/2019
Security Update	KB2984972	1/8/2019
Update	KB2985461	1/8/2019
Hotfix	KB2990941	1/7/2019
Security Update	KB2991963	1/8/2019
Security Update	KB2992611	1/8/2019
Security Update	KB3004375	1/8/2019
Update	KB3006121	1/8/2019
Hotfix	KB3006137	1/8/2019
Security Update	KB3010788	1/8/2019
Security Update	KB3011780	1/8/2019
Update	KB3013531	1/8/2019
Security Update	KB3019978	1/8/2019
Update	KB3020370	1/8/2019
Security Update	KB3021674	1/8/2019

Table A-2. Security Updates - Windows 7 64-Bit - Service Pack 1

Windows 7 64-bit, SP1		
Security Update	KB3023215	1/8/2019
Security Update	KB3030377	1/8/2019
Security Update	KB3035126	1/8/2019
Security Update	KB3037574	1/8/2019
Security Update	KB3045685	1/8/2019
Security Update	KB3046017	1/8/2019
Security Update	KB3046269	1/8/2019
Update	KB3054476	1/8/2019
Security Update	KB3055642	1/8/2019
Security Update	KB3059317	1/8/2019
Security Update	KB3060716	1/8/2019
Security Update	KB3067903	1/8/2019
Update	KB3068708	1/8/2019
Security Update	KB3071756	1/8/2019
Security Update	KB3072305	1/8/2019
Security Update	KB3074543	1/8/2019
Security Update	KB3075220	1/8/2019
Security Update	KB3078601	1/8/2019
Update	KB3078667	1/8/2019
Update	KB3080149	1/8/2019
Security Update	KB3086255	1/8/2019
Hotfix	KB3087873_BF	1/7/2019
Hotfix	KB3087873	1/7/2019
Security Update	KB3093513	1/8/2019
Security Update	KB3097989	1/8/2019
Update	KB3107998	1/8/2019
Security Update	KB3108371	1/8/2019
Security Update	KB3108664	1/8/2019
Security Update	KB3109103	1/8/2019
Security Update	KB3109560	1/8/2019
Security Update	KB3110329	1/8/2019
Security Update	KB3122648	1/8/2019
Security Update	KB3124275	1/8/2019
Security Update	KB3126587	1/8/2019
Security Update	KB3127220	1/8/2019
Update	KB3133977	1/8/2019
Update	KB3137061	1/8/2019
Update	KB3138378	1/8/2019
Update	KB3138612	1/8/2019
Security Update	KB3138910	1/8/2019

Table A-2. Security Updates - Windows 7 64-Bit - Service Pack 1

Windows 7 64-bit, SP1		
Security Update	KB3139398	1/8/2019
Security Update	KB3139914	1/8/2019
Update	KB3140245	1/8/2019
Update	KB3147071	1/8/2019
Security Update	KB3150220	1/8/2019
Security Update	KB3156016	1/8/2019
Security Update	KB3159398	1/8/2019
Update	KB3161102	1/8/2019
Security Update	KB3161949	1/8/2019
Update	KB3179573	1/8/2019
Update	KB3184143	1/8/2019
Update	KB4019990	1/8/2019
Update	KB4040980	1/8/2019
Update	KB4095874	1/8/2019
Update	KB4470641	1/8/2019
Update	KB976902	11/21/2010
Security Update	KB4471318	1/8/2019

Table A-3. Security Updates - Windows 7 32-Bit - Service Pack 1

Windows 7 32-Bit, SP1		
Description	**HotFixID**	**Installed On**
Update	KB2849697	4/8/2015
Update	KB2849696	4/8/2015
Update	KB2841134	4/8/2015
Security Update	KB2479943	11/5/2013
Update	KB2484033	11/5/2013
Update	KB2488113	11/5/2013
Security Update	KB2491683	11/5/2013
Hotfix	KB2496898	11/5/2013
Security Update	KB2503665	3/21/2014
Update	KB2505438	11/5/2013
Security Update	KB2509553	11/5/2013
Security Update	KB2536275	11/5/2013
Security Update	KB2536276	11/5/2013
Update	KB2541014	11/5/2013
Security Update	KB2544893	11/5/2013
Update	KB2545698	11/5/2013
Update	KB2547666	11/5/2013
Update	KB2552343	11/5/2013

Table A-3. Security Updates - Windows 7 32-Bit - Service Pack 1

Windows 7 32-Bit, SP1		
Security Update	KB2560656	11/5/2013
Update	KB2563227	11/5/2013
Security Update	KB2564958	11/5/2013
Security Update	KB2570947	11/5/2013
Security Update	KB2579686	11/5/2013
Security Update	KB2584146	11/5/2013
Security Update	KB2585542	3/21/2014
Hotfix	KB2589986	11/5/2013
Security Update	KB2604115	3/21/2014
Security Update	KB2619339	11/5/2013
Security Update	KB2620704	3/21/2014
Security Update	KB2621440	3/21/2014
Security Update	KB2631813	11/5/2013
Hotfix	KB2639308	11/5/2013
Update	KB2640148	11/5/2013
Update	KB2660075	11/5/2013
Update	KB976902	11/20/2010
Update	KB982018	11/5/2013

Table A-4. Security Updates - Windows XP - Service Pack 4

Windows XP 32-bit, SP4		
Description	**HotFixID**	**Installed On**
Windows	KB968930	8/31/2010
Security Update	(KB954430)	8/31/2010
Security Update	(KB973688)	8/31/2010
Security Update	(KB2758694)	4/14/2015
Security Update	(KB973685)	8/31/2010
Security Update	(KB2510531)	4/14/2015
Update	(KB2598845)	4/14/2015
Security Update	(KB2564958)	4/14/2015
Hotfix	(KB969084)	8/31/2010
Update	(KB898461)	2/18/2011
Security Update	(KB2115168)	4/14/2015
Security Update	(KB2229593)	4/14/2015
Security Update	(KB2296011)	4/14/2015
Update	(KB2345886)	4/14/2015
Security Update	(KB2347290)	4/14/2015
Security Update	(KB2387149)	4/14/2015

Table A-4. Security Updates - Windows XP - Service Pack 4

Windows XP 32-bit, SP4		
Security Update	(KB2393802)	4/14/2015
Security Update	(KB2419632)	4/14/2015
Security Update	(KB2423089)	4/14/2015
Security Update	(KB2443105)	4/14/2015
Update	(KB2467659)	4/14/2015
Security Update	(KB2478960)	4/14/2015
Security Update	(KB2478971)	4/14/2015
Security Update	(KB2479943)	4/14/2015
Security Update	(KB2483185)	4/14/2015
Security Update	(KB2485663)	4/14/2015
Security Update	(KB2491683)	4/14/2015
Security Update	(KB2506212)	4/14/2015
Security Update	(KB2507938)	4/14/2015
Security Update	(KB2508429)	4/14/2015
Security Update	(KB2509553)	4/14/2015
Security Update	(KB2510581)	4/14/2015
Security Update	(KB2535512)	4/14/2015
Security Update	(KB2536276-v2)	4/14/2015
Security Update	(KB2544893-v2)	4/14/2015
Security Update	(KB2566454)	4/14/2015
Security Update	(KB2570947)	4/14/2015
Security Update	(KB2584146)	4/14/2015
Security Update	(KB2585542)	4/14/2015
Security Update	(KB2592799)	4/14/2015
Security Update	(KB2598479)	4/14/2015
Security Update	(KB2603381)	4/14/2015
Security Update	(KB2619339)	4/14/2015
Security Update	(KB2620712)	4/14/2015
Security Update	(KB2631813)	4/14/2015
Security Update	(KB2653956)	4/14/2015
Security Update	(KB2655992)	4/14/2015
Security Update	(KB2659262)	4/14/2015
Security Update	(KB2661637)	4/14/2015
Security Update	(KB2676562)	4/14/2015
Security Update	(KB2686509)	4/14/2015
Security Update	(KB2691442)	4/14/2015
Security Update	(KB2698365)	4/14/2015

Table A-4. Security Updates - Windows XP - Service Pack 4

Windows XP 32-bit, SP4		
Security Update	(KB2705219-v2)	4/14/2015
Security Update	(KB2712808)	4/14/2015
Security Update	(KB2719985)	4/14/2015
Security Update	(KB2723135-v2)	4/14/2015
Security Update	(KB2727528)	4/14/2015
Update	(KB2749655)	4/14/2015
Security Update	(KB2757638)	4/14/2015
Security Update	(KB2770660)	4/14/2015
Security Update	(KB2780091)	4/14/2015
Security Update	(KB2802968)	4/14/2015
Security Update	(KB2807986)	4/14/2015
Update	(KB2813347-v2)	4/14/2015
Security Update	(KB2820917)	4/14/2015
Security Update	(KB2834886)	4/14/2015
Security Update	(KB2847311)	4/14/2015
Security Update	(KB2850869)	4/14/2015
Security Update	(KB2859537)	4/14/2015
Security Update	(KB2862152)	4/14/2015
Security Update	(KB2862330)	4/14/2015
Security Update	(KB2862335)	4/14/2015
Security Update	(KB2864063)	4/14/2015
Security Update	(KB2868626)	4/14/2015
Security Update	(KB2876217)	4/14/2015
Security Update	(KB2876331)	4/14/2015
Security Update	(KB2892075)	4/14/2015
Security Update	(KB2893294)	4/14/2015
Security Update	(KB2898715)	4/14/2015
Security Update	(KB2900986)	4/14/2015
Update	(KB2904266)	4/14/2015
Security Update	(KB2909212)	4/14/2015
Security Update	(KB2914368)	4/14/2015
Security Update	(KB2916036)	4/14/2015
Security Update	(KB2922229)	4/14/2015
Security Update	(KB2929961)	4/14/2015
Security Update	(KB2930275)	4/14/2015
Update	(KB2934207)	4/14/2015
Security Update	(KB2936068)	4/14/2015

Table A-4. Security Updates - Windows XP - Service Pack 4

Windows XP 32-bit, SP4		
Security Update	(KB2964358)	4/14/2015
Hotfix	(KB915800-v4)	8/31/2010
Security Update	(KB923561)	11/3/2009
Hotfix	(KB932716-v2)	8/31/2010
Security Update	(KB938464-v2)	11/3/2009
Hotfix	(KB942288-v3)	1/23/2019
Security Update	(KB946648)	11/3/2009
Security Update	(KB950762)	11/3/2009
Security Update	(KB950974)	11/3/2009
Security Update	(KB951066)	11/3/2009
Security Update	(KB951376-v2)	11/3/2009
Update	(KB951618-v2)	11/3/2009
Security Update	(KB951748)	11/3/2009
Update	(KB951978)	11/3/2009
Security Update	(KB952004)	11/3/2009
Hotfix	(KB952287)	11/3/2009
Security Update	(KB952954)	11/3/2009
Hotfix	(KB953955)	11/3/2009
Hotfix	(KB954434)	11/3/2009
Security Update	(KB954459)	11/3/2009
Hotfix	(KB954550-v5)	11/3/2009
Security Update	(KB954600)	11/3/2009
Hotfix	(KB954708)	8/31/2010
Security Update	(KB955069)	11/3/2009
Update	(KB955759)	8/31/2010
Security Update	(KB956572)	11/3/2009
Security Update	(KB956744)	11/3/2009
Security Update	(KB956802)	11/3/2009
Security Update	(KB956803)	11/3/2009
Security Update	(KB956844)	8/31/2010
Security Update	(KB957097)	11/3/2009
Hotfix	(KB958347)	11/3/2009
Security Update	(KB958644)	11/3/2009
Security Update	(KB958687)	11/3/2009
Security Update	(KB958690)	8/31/2010
Security Update	(KB958869)	8/31/2010
Hotfix	(KB959252)	11/3/2009

Table A-4. Security Updates - Windows XP - Service Pack 4

Windows XP 32-bit, SP4		
Security Update	(KB959426)	11/3/2009
Security Update	(KB960225)	11/3/2009
Security Update	(KB960803)	11/3/2009
Security Update	(KB960859)	11/3/2009
Hotfix	(KB961118)	11/3/2009
Security Update	(KB961371-v2)	11/3/2009
Security Update	(KB961373)	8/31/2010
Security Update	(KB961501)	11/3/2009
Update	(KB961503)	4/14/2015
Security Update	(KB963027)	8/31/2010
Hotfix	(KB967048-v2)	8/31/2010
Update	(KB967715)	11/3/2009
Update	(KB968389)	11/3/2009
Security Update	(KB968537)	11/3/2009
Hotfix	(KB968764)	11/3/2009
Security Update	(KB969059)	8/31/2010
Security Update	(KB969897)	8/31/2010