



# CylancePROTECT<sup>®</sup> Home Edition

User Manual



CYLANCE™



# CylancePROTECT Home Edition User Manual

**Product:** CylancePROTECT Home Edition User Manual

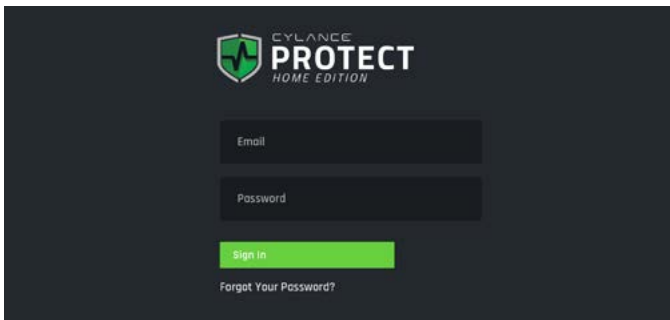
**Document Release Date:** v1.0, August 2017

**About Cylance®:** Cylance is the first company to apply artificial intelligence, algorithmic science, and machine learning to cybersecurity to improve the way companies, governments, and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated math and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit [cylance.com](http://cylance.com).

# Contents

<b>Overview</b> . . . . .	4	<b>Threat Detail</b> . . . . .	8
System Requirements . . . . .	4	Affected Devices (Under Threat Information) . . . . .	9
<b>Getting Started</b> . . . . .	4	<b>Device Protection Settings</b> . . . . .	10
<b>Web Portal</b> . . . . .	4	<b>Global Lists</b> . . . . .	10
<b>Install and Add Devices</b> . . . . .	5	Safe List. . . . .	10
Download the Installation File . . . . .	5	Quarantined List . . . . .	11
Installing on a PC or Mac . . . . .	5	<b>Appendix A – Glossary</b> . . . . .	11
User Interface on a PC or Mac . . . . .	5	<b>Appendix B – Threat Classifications</b> . . . . .	12
<b>Uninstalling from a PC or Mac</b> . . . . .	5	UNKNOWN (Blank Entry) . . . . .	12
Removing a Device from the Web Portal . . . . .	6	Trusted — Local . . . . .	12
<b>My Devices</b> . . . . .	6	Malware . . . . .	12
List of Devices. . . . .	7	PUP . . . . .	13
<b>Device Detail</b> . . . . .	7	Dual Use . . . . .	14
Threat Activity (Under Device Detail) . . . . .	8		





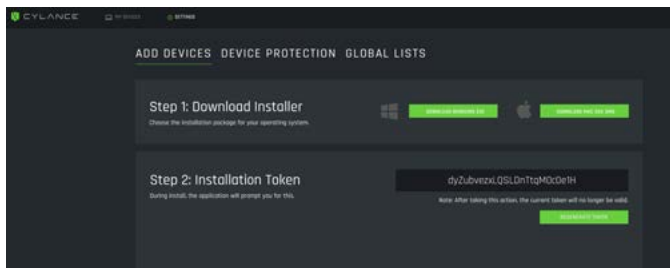
## Install and Add Devices

CylancePROTECT Home Edition must be installed on each system you want to protect (Windows or Mac device). You can install CylancePROTECT Home Edition on up to 10 devices that belong to your household, family, and loved ones.

### Download the Installation File

You can download the installation file for Windows or Mac systems. The installation file works with 32-bit and 64-bit operating systems.

1. Login to the Console.
2. Go to Settings, then Add Devices.
3. Click the Download Windows EXE or Download Mac DMG button to download the installation file.



### Installing on a PC or Mac

1. On the system you want to protect, double-click the installation file. Make sure you are using the correct installation file (Windows or Mac) on the correct operating system.
2. Follow the installer's instructions.
3. Type or copy/paste the Installation Token into the installer.
4. Continue with the installation.
5. Once the installation of CylancePROTECT Home Edition on a device (PC or Mac) is completed, the device name is automatically added to My Devices in the Web Portal.

**NOTE:** The Device Name that is displayed in the Web Portal is automatically taken from the Computer Name of the device on a Windows or Mac device.

### User Interface on a PC or Mac

When the Agent is installed, a Cylance icon is added to the system tray. There are three states in which you will find the Agent icon - Protected, At Risk, or Offline.

## Uninstalling from a PC or Mac

Uninstalling CylancePROTECT Home Edition from a PC or Mac will remove all malware protection capabilities from the device and will leave it vulnerable to malware attacks.

**NOTE:** After uninstalling from the PC or Mac, the device should also be removed from your CylancePROTECT Console.

#### Windows 8.1 and 10

1. Right-click the Start button in the bottom-left corner of the screen.
2. Select Control Panel.
3. Select Programs and Features.
4. Double-click CylancePROTECT Home Edition and follow the instructions to uninstall the program.

#### Windows 7

1. Click the Start button in the bottom-left corner of the screen.
2. Select Control Panel.
3. Select Uninstall a Program.
4. Double-click CylancePROTECT Home Edition and follow the instructions to uninstall the program.

## Mac OS X and macOS

1. Open a Finder window and select Applications.
2. Open the Cylance Folder.
3. Run the Uninstall CylancePROTECT application.

## Removing a Device from the Web Portal

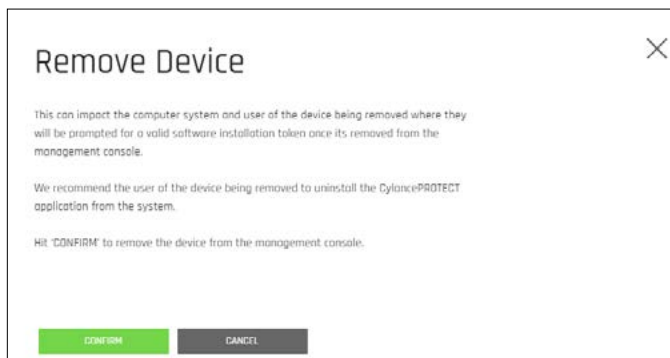
Removing a device from the Web Portal removes it from the My Devices list. This does not uninstall CylancePROTECT Home Edition from the device, but only unregisters the device from the Web Portal.

**NOTE:** *If the device is removed from the Web Portal before CylancePROTECT Home Edition is uninstalled from the PC or Mac, the user of the device will be prompted for a new Installation Token.*

- If you want to fully remove CylancePROTECT Home Edition from the device, follow the Uninstalling from a PC or Mac instructions.
- If you do not want to fully remove CylancePROTECT Home Edition from the device, simply re-enter the Installation Token on the device and it will reconnect to the Web Portal.

### To Remove a Device from the Web Portal

1. Login to the CylancePROTECT Home Edition Web Portal using a supported web browser.
2. From My Devices, click on the Device Name of the device to be removed to go to Device Details.
3. Click the Remove This Device button.
4. CylancePROTECT Home Edition will ask to confirm the removal of the device.



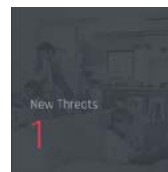
## My Devices

My Devices gives an overview of the safety or risk of all your devices protected by CylancePROTECT Home Edition. To view the My Device page, login to the Web Portal. You can install CylancePROTECT Home Edition on up to 10 devices that belong to your household, family, and loved ones.



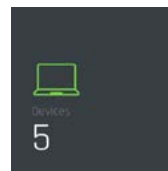
Environment SAFE displays if all your devices are free of running malware. This means that CylancePROTECT Home Edition automatically quarantined any detected malware, and therefore prevented it from running, or no malware was detected. All devices will show PROTECTED next to the device name.

**NOTE:** *If any threats are not quarantined, then New Threats # will display and include the number of threats.*

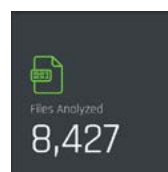


New Threats # displays the number of threats currently running on one or more of your devices. This can happen if any of the Auto Protect settings are Disabled. Action should be taken immediately to quarantine the threats on the infected devices. Devices that are infected will show AT RISK next to the device name.

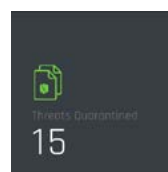
**NOTE:** *If you trust a file on a device, you can Allow the file to run on the device or add it to the Exclusion list to allow it to run on any of your devices.*



Devices # shows the total number of CylancePROTECT Home Edition devices you are managing



Files Analyzed # shows the total number of files analyzed on all the CylancePROTECT Home Edition devices you are managing.



Threats Quarantined # shows the total number of threats detected and quarantined on all the CylancePROTECT Home Edition devices you are managing. When a threat is quarantined by CylancePROTECT Home Edition, it is not allowed to run on your devices.

**NOTE:** If there is a file you trust that has been quarantined, you can go to the Threat Activity page, select the Quarantined tab, and then Allow the file to run on that device. You can add the file to the Exclusion list to allow it to run on any of your devices.

## List of Devices

**CylancePROTECT Home Edition** provides a list of the devices you are managing, including the status of each device, PROTECTED or AT RISK.

**Device Name** is the Computer Name from each device. Next to the Device Name, is its current Risk Status. If the device is free of malware, it will have a status of PROTECTED. If the device is infected with malware, it will have a status of AT RISK.

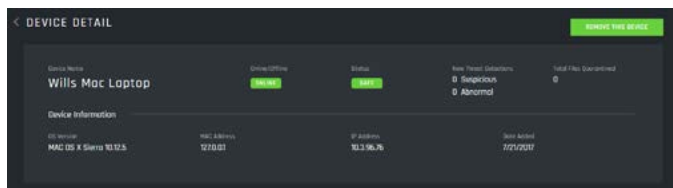
**Online/Offline** indicates whether the device is connected to the Internet and able to communicate with the Web Portal.

**Quarantined Threats** indicates the number of threats that have been quarantined on the device.

**New Threats Detected** indicates the number of threats detected on the device, but that have not been quarantined. This device is most likely infected with actively running malware. Action should be taken immediately to quarantine the threat, or allow the file if you trust it.

## Device Detail

Device Detail displays details about a **CylancePROTECT Home Edition** device, including any threat activity. To view details about a device, go to the My Devices page, and then click on a device name.



**Device Name** is the Computer Name of the device.

**NOTE:** If two or more devices have the same Computer Name, check the MAC Address or IP Address to identify the device.

**Online/Offline** indicates whether the device is connected to the Internet and able to communicate with the Web Portal.

**Status** indicates the risk status of the device. If the device is free of malware, it will have a status of PROTECTED. If the device is infected with malware, it will have a status of AT RISK.

**New Threat Detections** indicates the number of threats detected (suspicious or abnormal) on the device that are not quarantined or allowed.

**Total Files Quarantined** indicates the number of threats that have been quarantined on the device.

**OS Version** shows the specific Operating System (OS) that is used by the device.

**MAC Address** stands for Media Access Control Address and is a unique identifier (12 characters separated by dashes) assigned to the Network Interface Controller (NIC) hardware on the device. The MAC Address should be unique to that specific device and rarely changes unless the NIC hardware is changed.

**IP Address** stands for Internet Protocol Address and is a unique identifier (four to 12 numbers separated by dots) assigned to every device to allow the device to communicate with the Internet. Each device in the environment should have a different IP Address, however, the IP Address for the device could change.

**Date Added** indicates the date that **CylancePROTECT Home Edition** was installed on the device and added to the Web Portal.

**Remove This Device** removes and disconnects the device from the Web Portal. It does not uninstall **CylancePROTECT Home Edition** from the device. Please see the section on Uninstalling from a PC or Mac.

Please note:

- Once a device is removed from the Web Portal, it is no longer protected by **CylancePROTECT Home Edition**, even if the product is not uninstalled from the device. The device owner will be prompted for an Installation Token to reconnect the device to the Web Portal.
- If **CylancePROTECT Home Edition** is uninstalled from a device, but is not removed from the Web Portal, the device status will display as Offline.

## Threat Activity (Under Device Detail)

The Threat Activity list shows all the threats that **CylancePROTECT Home Edition** detected on the device grouped by their status (Detected, Quarantined, or Allowed). Use the checkbox next to the Device Name to select a device and perform an action.

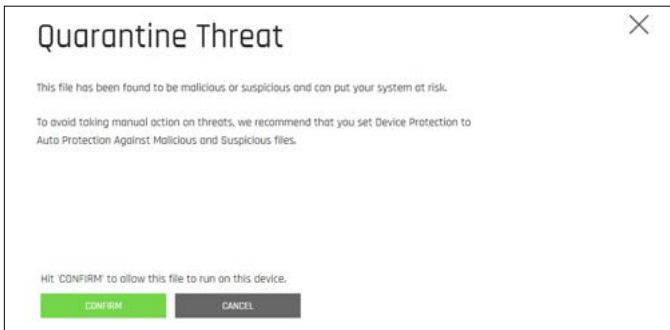


NAME	STATUS	CLASSIFICATION	FIRST FOUND	FILE PATHS
<input type="checkbox"/> <code>cmd.exe</code>	Quarantined	Trusted - Local	5/29/2017	C:\Users\Administrator\Desktop\cmd.exe C:\Users\Administrator\Desktop\cmd.exe
<input type="checkbox"/> <code>cmd.exe</code>	Quarantined	Trusted - Local	5/18/2017	C:\Users\Administrator\Desktop\cmd.exe C:\Users\Administrator\Desktop\cmd.exe

**Detected** shows a list of all the Suspicious and Abnormal files detected on the device that have not been quarantined or allowed. The files are most likely still running on the device. Action should be taken immediately. To act on a file, click the checkbox next to the filename, and then select the action to perform on that file (Quarantine or Allow). The Quarantine and Allow buttons are enabled only when one or more files are selected on the Threat Activity list.

**Quarantined** shows a list of all the threats that have been quarantined on the device. These files are quarantined on this device only. If you want to quarantine these files on all **CylancePROTECT Home Edition** devices you manage, see [Global List – Quarantined List](#).

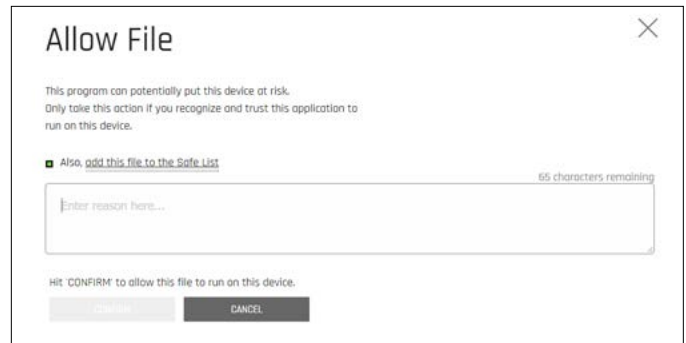
If a file that you trust has been quarantined and you want to allow it to run on the device, you can click the checkbox next to the filename, then click Allow. The Allow button is enabled only when one or more files are selected on the Threat Activity list. A screen will appear to ask you to confirm.



**Allowed** shows a list of all the files that were detected as threats but allowed to run on the device. If you want to allow a file to run on any **CylancePROTECT Home Edition** device you manage, see [Global Lists – Safe List](#).

If you want to quarantine a file you previously allowed, you can click the checkbox next to the filename, then click Quarantined. The Quarantined button is enabled only when one or more files are selected on the Threat Activity list. A screen will appear to ask you to confirm.

In the confirm message, a checkbox asks if you want to “Also, add this file to the Safe List” which will allow the file on all devices in the environment. See section on [Global Lists](#).



**Name** is the filename of the file as seen on the device.

**Status** indicates the current status of the file.

- **Quarantined** means the threat was detected, blocked, and quarantined. A quarantined file will not run on the device.
- **Allowed** means the file was allowed to run.
- **Suspicious** means the file is considered suspicious, was not quarantined, and might be actively running on the device. Suspicious files are malicious, or potentially malicious, and should be quarantined. If the file is one that you trust, you can add it to the Exclusion list to allow it to run on your devices.
- **Abnormal** means the file is considered abnormal, was not quarantined, and might be actively running on the device.

**Classification** indicates the threat classification of the file. Please see [Appendix B — Threat Classifications](#) for more details.

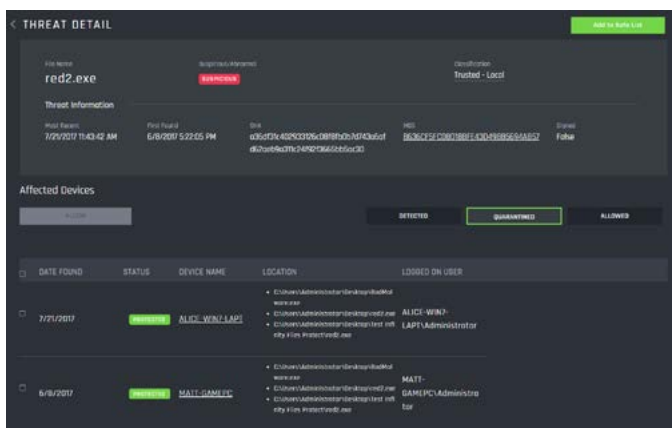
**First Found** indicates the date that the file was found on the device.

**File Paths** indicates the exact location where the file was found in the device’s file system directory.

## Threat Detail

Threat Detail gives insightful information for a specific threat or file that has been detected by **CylancePROTECT Home Edition** and lists all the devices on which the threat was found. After clicking on a specific threat from the Threat Activity list on [Devices Details](#), you will see the Threat Details page.





**File Name** is the name of the file as seen on the device.

**Suspicious/Abnormal** indicates whether the file is considered Suspicious or Abnormal.

- **Suspicious** means CyLancePROTECT Home Edition is highly confident that the file is malware, a potentially unwanted program (PUP), or a dual use file, and the file should be quarantined.
- **Abnormal** means CyLancePROTECT Home Edition has found enough similarities with the file to consider it malware, a PUP, or a dual use file.

**Classification** indicates the threat classification of the file. Please see Appendix B — Threat Classifications for more details.

**Most Recent** indicates the most recent date and time that the file was detected across all the devices that you manage.

**First Found** indicates the first date and time that the file was detected across all the devices that you manage.

**SHA256** is a unique cryptographic hash of the file consisting of 64 characters. Every unique file should have a unique SHA256 hash and is treated like a fingerprint of the file to tell one file apart from another. It could also be used to prove that two files are the same even if they have different filenames.

**MD5** is a unique cryptographic hash of the file consisting of 32 characters. Every unique file should have a unique MD5 hash and is treated like a fingerprint of the file to tell one file apart from another. It could also be used to prove that two files are the same even if they have different filenames.

**Signed** indicates whether the file is digitally signed. Common trusted files are usually signed by the software company that created them. Although malware can pretend to be signed, the absence of a digital signature could imply a lower level of trust for the file.

**Add To Safe List** adds the file to the Global Safe List and allows the file to be run on all devices in the environment. CyLancePROTECT Home Edition will not detect or quarantine the file in the future. See the section on Global Lists for more details.

## Affected Devices (Under Threat Information)

Affected Devices shows all the devices on which the threat was detected by CyLancePROTECT Home Edition. Use the checkbox next to the File Name to select a file and perform an action.

**Detected** shows a list of all the devices on which the threat has been detected, but not quarantined or allowed. The threat is probably still running on the devices. Action should be taken immediately. To act on a file, click the checkbox for the device, and then select the action to perform on that file (Quarantine or Allow). The Quarantine and Allow buttons are enabled only when one or more files are selected on the Affected Devices list.

**Quarantined** shows a list of all the devices on which the threat has been quarantined. If a file that you trust has been quarantined and you want to allow it to run on a device, you can click the checkbox for the device, then click Allow. The Allow button is enabled only when one or more files are selected on the Affected Devices list.

**Allowed** shows a list of all the devices on which the file was detected, but allowed to run on the device. If you want to quarantine a file you previously allowed, you can click the checkbox for the device, then click Quarantined. The Quarantined button is enabled only when one or more files are selected on the Affected Devices list.

**Device Name** is the Computer Name of the device.

**NOTE:** If two or more devices have the same Computer Name, check the MAC Address or IP Address to identify the device.

**Status** indicates the risk status of the device. If the device is free of malware, it will have a status of PROTECTED. If the device is infected with malware, it will have a status of AT RISK.

**Date Found** indicates the date that the threat was found on the device.

**Location** indicates the file path location where the file was found in the device's file system directory.

**Logged On User** displays the username logged on to the device when the threat was found.

# Device Protection Settings

**CylancePROTECT Home Edition** should be installed on every Windows PC or Mac device that you want protected against malware and will notify the user of the device if malware is detected or quarantined.

Controlling what is blocked or allowed is done in the Web Portal. This allows you to manage your devices from one location (even if the device is in a different city or state).

When **CylancePROTECT Home Edition** finds either a Suspicious or Abnormal file, it displays as New Threat Detected and will act on the file based on your Protection Settings. These protection settings apply to all devices you manage and are listed in the Web Portal.

1. Login to the **CylancePROTECT Home Edition** Web Portal.
2. Select Settings.
3. Select Device Protection.
4. Enable or disable the feature you want.
5. **Auto protect against suspicious files** — Automatically prevent suspicious files from executing before they have an opportunity to do any damage to a computer. Suspicious files are files that **CylancePROTECT Home Edition** is highly confident are malware, a PUP, or a dual use file, and should be quarantined.

**NOTE:** *This setting is enabled by default. Cylance highly recommends keeping this setting enabled always to ensure all your devices remain safe. Disabling this setting will allow malware that infects a device to run and could result in loss of personal information and/or data.*

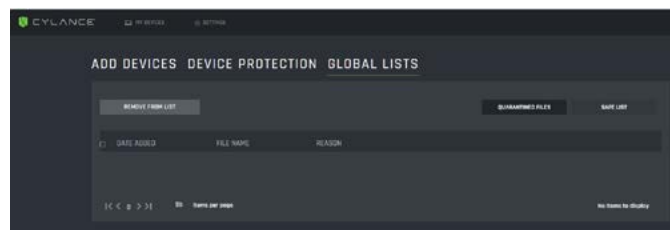
- a. **Auto protect against abnormal files** — Automatically prevent abnormal files from executing before they have an opportunity to do any damage to a computer. Abnormal files are files that **CylancePROTECT Home Edition** has found to have enough similarities to malware, PUPs, or dual use files.

**NOTE:** *This setting is enabled by default. Cylance recommends keeping this setting enabled always to ensure all your devices remain safe. Disabling this setting will allow files that are potentially malware to run.*

- b. **Send file to cloud** — Automatically contribute file samples to the Cylance Cloud to perform deep analysis of the file.

# Global Lists


Global Lists are a list of files you can manage in the Web Portal to quarantine or allow files across all the devices you manage. For files that are identified as Suspicious or Abnormal, you can either add these files to the Quarantined Threat list (meaning these files are moved to a quarantined folder and modified to not execute) or you can add these to the Safe List (meaning these files can run on any of your devices).

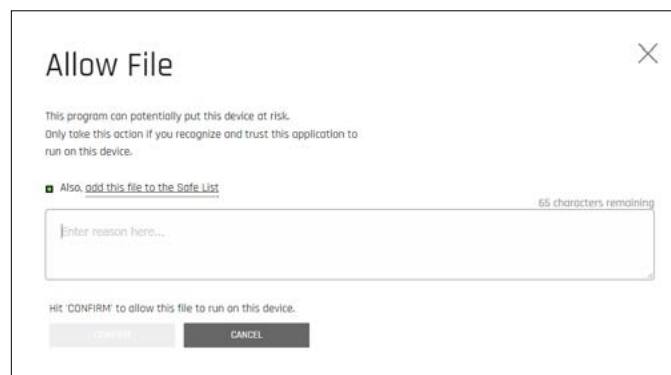


## Safe List

The Global Safe List is a list of files allowed to run on all devices in your environment even if **CylancePROTECT Home Edition** views them as suspicious or abnormal. Sometimes safe files do things that malicious files are known to do, such as pretending to be another file or accessing sensitive areas of your computer. If you are certain a file is trustworthy, it can be added to the Global Safe List and **CylancePROTECT Home Edition** will not detect or quarantine the file in the future.

Adding a file to the Safe List can be done in the following ways:

- From Threat Detail, click on the Add to Safe List button in the upper-right side of the screen.
- 
- From Device Detail, in the Threat Activity section, select a file in the list and click Allow. A confirmation screen will appear. Select Also, add this to the Safe List and confirm.



## Quarantined List

The Global Quarantined List is a list of files that will always be detected and quarantined on all your devices using **CylancePROTECT Home Edition**, even if it did not view them as suspicious or abnormal. It enables you to prevent files you do not want to run on any device in your environment.

## Appendix A – Glossary

**Abnormal** — A file with enough resemblance to a malicious file that it would be safer to block it instead of allowing it to run on your device.

**Allow** — Allow execution of a file locally (on a specific device).

**Audit Log** — Log that records actions performed from the **CylancePROTECT Home Edition** console interface.

**Auto-Quarantine** — Automatically prevent execution of all Suspicious and/or Abnormal files.

**Device Name** — The Computer Name of the Windows or Mac device.

**Environment** — All your devices with **CylancePROTECT Home Edition** installed.

**Global Quarantined List** — Prevent execution of a file globally (across all devices in your environment).

**Global Safe List** — Allow execution of a file globally (across all devices in your environment).

**Installation Token** — A unique ID used when installing **CylancePROTECT Home Edition**.

**Quarantine** — Prevent execution of a file locally (on a specific device).

**Send File To Cloud** — Automatically upload any unknown portable executable (PE) files, detected as Suspicious or Abnormal, to the CylanceINFINITY™ Cloud for analysis.

**Suspicious** — A file that is most likely a malicious file (malware, PUP, or dual use) and should be quarantined.

**Threats** — Potentially malicious files detected by **CylancePROTECT Home Edition**, classified either as Suspicious or Abnormal. Threats include malware, computer viruses, worms, trojans, ransomware, PUPs, adware, etc.

**Web Portal** — **CylancePROTECT Home Edition** website that allows you to download the software, change your protection settings, and manage your devices.

# Appendix B – Threat Classifications

Files that have been analyzed by **CylancePROTECT Home Edition** will be assigned a classification, such as unknown, trusted-local, PUP, dual use, or malware. File classifications can be seen on the Threat Details page or the Device Details page (under Threat Activity). Below is a list of possible classifications for each threat, along with a brief description.

## UNKNOWN (Blank Entry)

The file has not been analyzed by the Cylance research team yet. Once the file is analyzed, the classification for the file will be updated.

## Trusted — Local

The file has been analyzed by the Cylance research team and it is considered safe (not malicious). You can add a file classified as Trusted - Local to your Global Safe List. This will allow the file to run on any of your devices and will not generate any additional alerts.

## Malware

The Cylance research team has definitively identified the file as malware. The file should be removed or quarantined as soon as possible. Malware is also divided into subclasses.

Subclass	Definition	Examples
Backdoor	Malware that provides unauthorized access to a system, bypassing security measures.	Back Orifice, Eleanor
Bot	Malware that connects to a central command and control (C&C) botnet server.	QBot, Koobface
Downloader	Malware that downloads data to the host system.	Staged-Downloader
Dropper	Malware that installs other malware on a system.	
Exploit	Malware that attacks a specific vulnerability on the system.	
FakeAlert	Malware that masquerades as legitimate security software to trick the user into fixing fake security problems at a price.	Fake AV White Paper
Generic	Any malware that does not fit into an existing category.	
InfoStealer	Malware that records login credentials and/or other sensitive information.	Snifula
Ransom	Malware that restricts access to system or files and demands payment for removal of restriction, thereby holding the system for ransom.	CryptoLocker, Cryptowall
Remnant	Any file that has malware remnants post removal attempts.	
Rootkit	Malware that enables access to a computer while shielding itself or other files to avoid detection and/or removal by administrators or security technologies.	TDL, Zero Access Rootkit
Trojan	Malware that disguises itself as a legitimate program or file.	Zeus
Virus	Malware that propagates by inserting or appending itself to other files.	Sality, Virut
Worm	Malware that propagates by copying itself to another device.	Code Red, Stuxnet

## PUP

A PUP is a file that may not be malicious, but can be used in a way that puts you at risk. If you trust the file, you can allow it to run or block it on a per device basis (Allow or Quarantine Threat). You can also add the file to the Safe List to allow it to run on any device you manage. PUPs are divided into subclasses to help you determine if the file should be allowed to run or blocked.

Subclass	Definition	Examples
<b>Adware</b>	Technologies that provide annoying advertisements, such as popups, or provide bundled third-party add-ons when installing an application. This usually occurs without adequate notification to the user about the nature or presence of the add-on, control over installation, control over use, or the ability to fully uninstall the add-on.	Gator, Adware Info
<b>Corrupt</b>	Any executable file that is malformed and unable to run.	
<b>Game</b>	Technologies that create an interactive environment with which a player can play.	Steam Games, League of Legends
<b>Generic</b>	Any PUP that does not fit into an existing category.	
<b>HackingTool</b>	Technologies that are designed to assist hacking attempts.	Cobalt Strike, MetaSp0it
<b>Portable Application</b>	Programs designed to run on a computer independently, without needing installation.	Turbo
<b>Scripting Tool</b>	Any script that is able to run as if it were an executable.	AutoIT, py2exe
<b>Toolbar</b>	Technologies that place additional buttons or input boxes on-screen within a user interface.	Nasdaq Toolbar, Bring Me Sports
<b>Other</b>	A category for things that don't fit anything else, but are still PUPs. There are a lot of different PUPs, most of which aren't malicious but should still be brought to the attention of the System Administrators through our product, usually because they have potentially negative uses or negatively impact a system or network.	

## Dual Use

Dual Use is a file that can be used for malicious and non-malicious purposes. Use caution if you allow this type of file to run on your devices. For example, PsExec.exe is an IT tool that can gain remote access to another computer to help troubleshoot issues, but it can also be used to execute malicious files on another system. If you find PsExec.exe on your devices and you did not intentionally put it there, the file should be quarantined just like malware.

Subclass	Definition	Examples
<b>Crack</b>	Technologies that can alter (or crack) another application in order to bypass licensing limitations or digital rights management protection.	
<b>Generic</b>	Any dual use tool that does not fit into an existing category.	
<b>KeyGen</b>	Technologies that can generate or recover/reveal product keys that can be used to bypass digital rights management or licensing protection of software and other digital media.	
<b>MonitoringTool</b>	Technologies that track a user's online activities without awareness of the user by logging and possibly transmitting logs of one or more of the following: <ul style="list-style-type: none"><li>▪ User keystrokes</li><li>▪ Email messages</li><li>▪ Chat and instant messaging</li><li>▪ Web browsing activity</li><li>▪ Screenshot captures</li><li>▪ Application usage</li></ul>	Veriato 360, Refog Keylogger
<b>Pass Crack</b>	Technologies that can reveal a password or other sensitive user credentials either by cryptographically reversing passwords or by revealing stored passwords.	l0phtcrack, Cain & Abel
<b>RemoteAccess</b>	Technologies that can access another system remotely and administer commands on the remote system, or monitor user activities without user notification or consent.	Putty, PsExec, TeamViewer
<b>Tool</b>	Programs that offer administrative features but can be used to facilitate attacks or intrusions.	Nmap, Nessus, POf