

CylancePROTECT®

Administrator Guide





Product: CylancePROTECT®

Document: CylancePROTECT® Administrator Guide. This guide is a succinct resource for analysts, administrators, and customers who are reviewing or evaluating the product.

Document Release Date: 2.1 rev34, July 2020

About BlackBerry Cylance®: BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

Copyright: © 2020 BlackBerry Cylance Inc. All Rights Reserved.

Global Headquarters

400 Irvine Spectrum Drive, Irvine, CA 92618

Professional Services Hotline

+1-877-97DEFEND • +1-877-973-3336

Corporate Contact

+1-914-CYLANCE • +1-914-295-2623

Email

sales@cylance.com

Website

<https://www.cylance.com>

To Open a Support Ticket

<https://support.cylance.com> — Click on **Submit a Ticket**

To View Knowledge Base and Announcements

Login to <https://support.cylance.com>

To Request a Callback from BlackBerry Cylance Support

+1-866-699-9689

Table of Contents



Contents

Table of Contents	3
Contents	4
Overview	11
How It Works	12
About This Guide	13
Communications	13
CylancePROTECT Domain Descriptions	14
Additional Domains Required for Console Navigation Descriptions	14
What's New in CylancePROTECT	15
Login	15
Password requirements	15
Console Configuration	17
Device Policy	17
Policy Best Practices	17
File Actions	20
Memory Actions	23
Protection Settings	29
Application Control	31
Agent Settings	34
Script Control	37
Device Control	43
Apply a Policy to a Device	47
Clone a Device Policy	48
Zones	49
About Zone Priority	49
Zone Management Best Practices	50
Zone Properties	53
Zone Rules	53
Zones Device List	56
Agent Installation	59
Download the Install File	59
Install the Agent from the Application Page	59

Install the Agent from the Deployments Page	60
Windows Agent	61
System Requirements	61
Install the Agent — Windows	66
Windows Installation Parameters	67
Windows Installation Verification	70
Uninstall the Windows Agent	70
CylancePROTECT + CylanceOPTICS Windows Agent	73
Install CylancePROTECT + CylanceOPTICS	74
CylancePROTECT + CylanceOPTICS Installation Parameters	79
Uninstall CylancePROTECT + CylanceOPTICS	82
macOS Agent	83
System Requirements	83
Install the Agent — macOS	85
Installation — System Management	86
Install the Agent from the Command Line	87
Optional Installation Parameters	87
macOS Installation Parameters	88
macOS High Sierra – Secure Kernel Extension Loading	89
Use Mobile Device Management	90
macOS Installation Verification	91
Uninstall the macOS Agent	92
Linux Agent	92
System Requirements	92
Linux Installation	95
Install the RHEL/CentOS Agent Automatically	98
Install the RHEL/CentOS Agent Manually	98
Install the Ubuntu Agent Manually	100
Install the Amazon Agent Automatically	101
Install the Amazon Agent Manually	101
Amazon Linux Commands	102
Install the SUSE Agent Automatically	102
Install the SUSE Agent Manually	103
Start the UI (Ubuntu and SUSE 12)	103

Installation — System Management	104
Set an Unauthenticated Proxy Server - Linux	104
Set an Authenticated Proxy Server - Linux	105
Kernel Driver	107
Logging - Linux	108
Re-register a Linux Agent	110
Stop or Start the Linux Service	110
Upgrade the Linux Agent	110
Uninstall the Linux Agent	111
Agent Update	112
Zone-Based Updating	112
Rollback Agent Version	112
Password-Protected Uninstall	114
To Create an Uninstall Password	115
Agent Service	116
Agent User Interface	117
Agent UI Notifications	117
Threats Tab	121
Events Tab	121
Scripts Tab	121
Agent Menu Options	122
Enable Agent User Interface Advanced Options	123
Virtual Machines	124
Enable Submitting Helpdesk Tickets	124
Changing the Help / FAQ Link in the Agent UI	126
Device Management	128
Device Threats & Activities	129
Threats	129
Exploit Attempts	130
Application Control	130
Agent Logs	130
Script Control	131
External Devices	131
Duplicate Devices	132

Example Using Microsoft Excel	132
Threat Management	134
Dashboard	134
Threat Statistics	135
Protection Percentages	135
Threats by Priority	135
Threat Events	138
Threat Classifications	138
Top Ten Lists	139
Priority of Threat Actions	140
Threat Protection	140
Unsafe and Abnormal Files	141
Cylance Score	141
File Classification	142
View Threat Information	145
Save a Filter	148
Threat Details	149
Addressing Threats	154
Protection — Script Control	158
Protection — External Devices	160
Global List	161
Safe List Scripts by Hash	163
Safe List by Certificate	163
Reports	166
CylancePROTECT Overview Report	166
Threat Event Summary Report	167
Device Summary Report	169
Threat Events Detail Report	170
Devices Detail Report	170
Export Reports	171
Administration	172
Application	172
Invitation URL	172
Syslog/SIEM Settings	172

Change Syslog Settings	172
Event Types	173
Application Control	173
Audit Log	174
Devices	175
Memory Protection	176
Threats	177
Threat Classifications	178
Security Information and Event Management (SIEM)	178
Protocol	178
TLS / SSL	178
IP / Domain	178
Port	179
Severity	179
Facility	179
Testing the Connection	179
Custom Authentication	179
Threat Data Report	180
User Management	181
Add Users	181
Change User Roles	181
Remove Users	182
Role Management	182
My Account	188
Audit Logs	189
How-To Guide	190
Help and FAQ	190
Language Preferences	190
In Google Chrome	190
In Mozilla Firefox	191
Network Related	191
Firewall	191
Proxy	191
Integrations	192

CylanceOPTICS API	192
Troubleshooting	193
Missing Menu Options, Pages, and Functionality	193
Installation Parameters	193
Performance Concerns	194
Update, Status, and Connectivity Issues	194
Enable Debug Logging	195
Script Control Incompatibilities	195
Enable Support Login	196
Virtual Machines	197
Time Zone Variances	198
Cylance Host URLs	200
North America	200
Asia-Pacific North East	200
Asia-Pacific South East (including Australia)	201
Europe Central	202
South America East	202
SIEM / Syslog URLs	203
Asia-Pacific North East (login-apne1.cylance.com)	203
Asia-Pacific South East (login-au.cylance.com):	203
Europe Central (login-euc1.cylance.com):	203
North America (login.cylance.com):	204
South America (login-sae1.cylance.com):	204
Undeliverable Messages	204
Agent Status Information File	205
Appendix A: VDI Best Practices	210
Malware Prevention	211
Gold Image Preparation	212
Layering in Memory Protection & Script Control	218
Non-Persistent VDI Install Parameter	218
Details for VDI=<X>	219
Details for AD=1	220
Verification	220
VDI Agent Update Process	221

Appendix B: Cylance Exclusions and When to Use Them	222
Policy Safe List (File Actions)	222
Example Scenario:	222
Exclude Executable Files (Memory Protection)	222
Example Scenario:	223
Exclude Specific Folders (Protection Settings)	223
Example Scenario:	223
Folder Exclusions (Script Control)	224
Example Scenario:	224
Appendix C: Glossary	225

OVERVIEW

CylancePROTECT detects and blocks malware before it can affect a device. Cylance uses a mathematical approach to malware identification, using machine learning techniques instead of reactive signatures, trust-based systems, or sandboxes. This approach renders new malware, viruses, bots, and future variants useless. CylancePROTECT analyzes potential file executions for malware in the Operating System and memory layers to prevent the delivery of malicious payloads.

This guide explains using the Cylance Console, installing the CylancePROTECT Agent, and how to configure both. Best practices are included, where applicable.

How It Works

CylancePROTECT consists of a small Agent, installed on each host that communicates with the cloud-based Console. The Agent detects and prevents malware on the host by using tested mathematical models, does not require continuous cloud connectivity or continual signature updates, and works in both open and isolated networks. As the threat landscape evolves, so does CylancePROTECT. By constantly training on enormous, real-world data sets, CylancePROTECT stays one step ahead of the attackers.

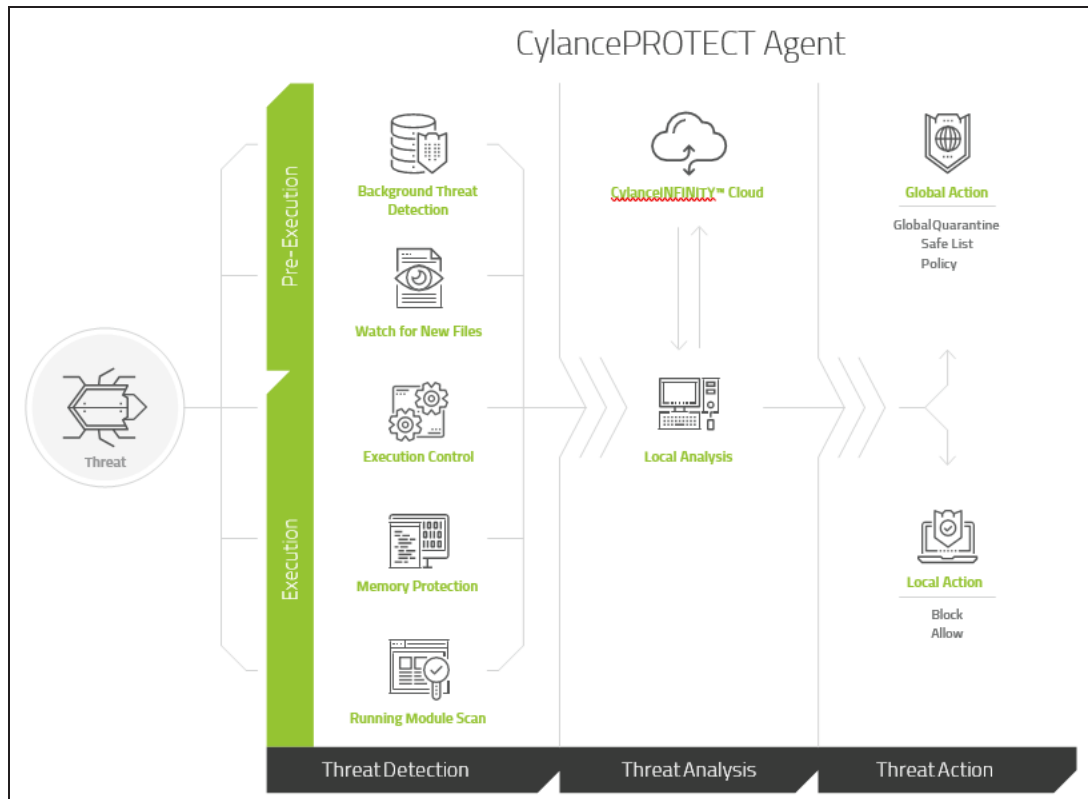


Figure 1: CylancePROTECT Threat Analysis Flowchart

- **Threat:** When a threat is downloaded to the device or there is an exploit attempt (something running in memory that attempts to execute an attack).
- **Threat Detection:** How the Agent identifies threats.
 - **Running Module Scan:** Scans processes running on the device. This is collected after the initial installation of CylancePROTECT and when the Cylance Service starts (example: system boot).
 - **Execution Control:** Analyzes processes upon execution only. This includes all files that run at startup, that are set to auto-run, and that are manually executed by the user.

- **Background Threat Detection:** Scans files on the system, runs in the background, and is designed to consume a small amount of system resources. It is recommended to enable Background Threat Detection and Watch For New Files. If Watch For New Files is enabled, it is recommended to configure Background Threat Detection to Run Once. You need to check existing files one time only if you are also watching for new and updated files.
- **Watch for New Files:** Scans new and updated files for threats. Because this feature only looks for new and updated files, it is recommended to use Background Threat Detection set to Run Once. Background Threat Detection scans all files on the device.
- **Script Control:** Protects users from malicious scripts running on their devices. This includes PowerShell, Active Script, and Microsoft Office Macros.
- **Analysis:** How files are identified as malicious or safe.
 - **Cylance OEM Engine:** The Mathematical Model in the cloud that is used to score files.
 - **Local:** The Mathematical Model included with the Agent. This allows analysis when the device is not connected to the Internet.
- **Action:** What the Agent does when a file is identified as a threat.
 - **Global:** Checks policy settings, including the *Global Quarantine* and *Safe Lists*.
 - **Local:** Checks for files manually *Quarantined* or *Waived*.

About This Guide

Configure the Console before installing the Agent on devices. Understanding how devices are managed should make protecting and maintaining the devices easier.

Example: Zones help group devices in the organization. For example, you can create a Zone Rule that automatically adds new devices to a Zone based on your selected criteria (such as Operating System, Device Name, or Domain Name). This requires some planning before you install any Agents.

Note: Instructions for installing the Agent come after learning about configuring Policies and Zones. Users can start with installing the Agent if needed.

Communications

The Agent reports to and is managed by the Console. Networks with a proxy server or firewall should allow communication with the following sites (over port 443). For a list of Cylance hosts

to allow, based on the region the organization belongs to, see ["Cylance Host URLs" on page 200](#).

Note: The CylancePROTECT Agent-Cloud Communications image displays the Cylance Host URLs for North America. For other regions, the Agents would use the Cylance Host URLs for your region.

Example: login.cylance.com, login-au.cylance.com, login-euc1.cylance.com, and login-apne1.cylance.com are hosts that perform the same function in different regions.

CylancePROTECT Domain Descriptions

Domain	Description
login.cylance.com	Allows users to log in to the Cylance Console. Also used to register and re-register devices.
data.cylance.com	Requests initiated by the Agent for the following information: <ul style="list-style-type: none"> ■ Global Quarantine List ■ Safe List ■ Centroids ■ System Info Report ■ Client Status ■ Events ■ System Threat List Report ■ Policy <p>This is done once an hour at a randomized minute.</p>
protect.cylance.com	Displays the Console user-interface (UI0 after a user logs in).
update.cylance.com	Provides communications for the Agent Updater.
download.cylance.com	Downloads updates for the Agent.
api.cylance.com	Performs threat analysis and cloud scoring (Cylance Score). Also sends unknown files up to the cloud for analysis.

Additional Domains Required for Console Navigation Descriptions

Domain	Description
cdn.cylance.com	Used for Content Deliver Network (CDN) communications.
venueapi.cylance.com	Used for the Cylance API.

What's New in CylancePROTECT

To view new updates and releases, login to the Cylance Support Portal at <https://support.cylance.com> and go to the CylancePROTECT Release Notes (requires login).

Login

Upon activation of your account, you will receive an email with your login information for the CylancePROTECT Console. Click the link in the email and go to the login page or go to:

- **Asia-Pacific North East:** <https://login-apne1.cylance.com>
- **Asia-Pacific South East:** <https://login-au.cylance.com>
- **Europe Central:** <https://login-euc1.cylance.com>
- **North America:** <https://login.cylance.com>
- **South America East:** <https://login-sae1.cylance.com>

Password requirements

Your password must meet three of the following requirements:

- A lowercase character
- An uppercase character
- A special character (examples * # \$ %)
- A numeric character
- A Unicode character/data (examples ♥☀☆)

The email address will serve as your account login. Once you have established your password, you will be able to proceed to the Console.

Your login URL depends on the region the organization belongs to:

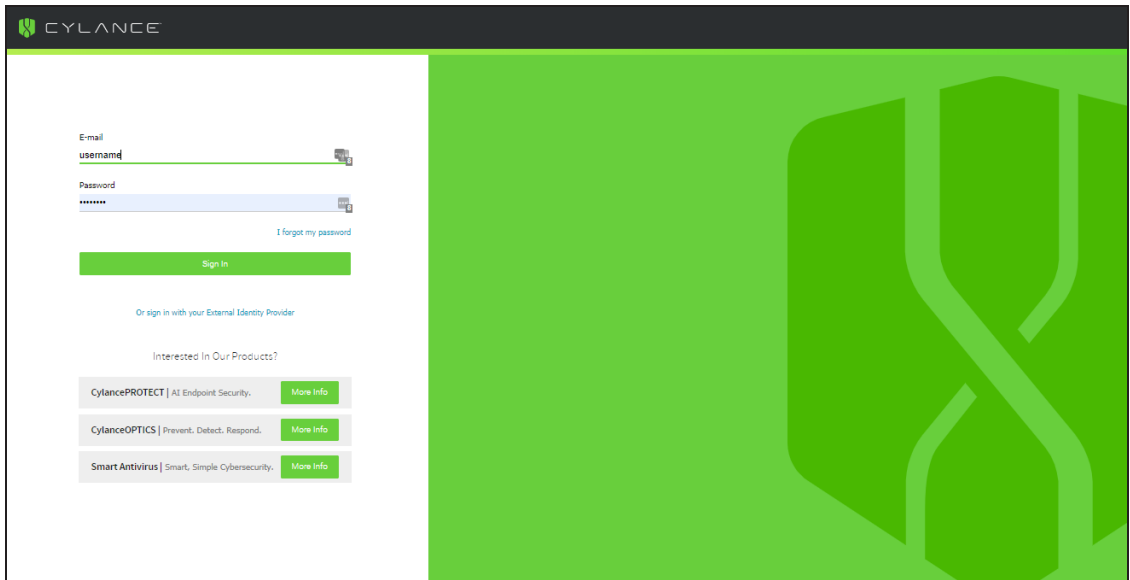


Figure 2: Console Login

CONSOLE CONFIGURATION

The CylancePROTECT Console is a website you log into and view threat information for the organization. The Console makes it easy to organize devices in groups (Zones), configure what actions to take when threats are discovered on a device (Policy), and download the installation files (Agent).

Device Policy

A policy defines how the Agent handles malware it encounters. For example, automatically *Quarantine* malware or ignore it if in a specific folder. Every device must be in a policy and only one policy should be applied to a device. Restricting a device to a single policy eliminates conflicting features (such as blocking a file when it should be Allowed for that device). The device is placed in the Default policy if no policy is assigned.

Only Execution Control is enabled for the Default policy, which analyzes processes upon execution only. This provides basic protection for the device, should not interrupt operations on the device, and provides time to test the policy features before deploying the policy in the production environment.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

To Add a Policy

1. Select **Settings > Device Policy**.
2. Click **Add New Policy**.
3. Enter a Policy Name and select policy options. Descriptions for each policy option are listed below, including Policy Best Practices.
4. Click **Create**.

Policy Best Practices

When you first create policies, you should implement policy features in a phased approach to ensure performance and operations are not impacted. As you understand how Cylance functions in your environment, you can create new policies with more features enabled.

IMPORTANT: It is highly recommended that you test on a subset of representative devices in your production environment (not just a clean virtual machine) before a full scale roll-out to identify all programs used in your organization. For example, a group in your organization could

use a custom application that was purchased from a company that has since gone out of business that you are not aware of.

1. When creating initial policies, enable **Auto-Upload** only.

- a. The Agent uses Execution Control and Process Monitor to analyze running processes only.

This includes all files that run at startup, that are set to auto-run, and that are manually executed by the user.

The Agent only sends alerts to the Console. No files are blocked or *Quarantined*.

- b. Check the Console for any threat alerts.

The goal is to find any applications or processes that are required to run on the endpoint that are considered a threat (*Abnormal* or *Unsafe*).

Configure a policy or console settings to *Allow* these to run if this happens (for example, *Exclude* folders in a policy, *Waive* the files for that device, or add the files to the *Safe List*).

- c. Use this initial policy for a day to allow applications and processes that are typically used on the device to run and be analyzed.

IMPORTANT: There may be applications and processes that run periodically on a device (for example, once a month) that might be considered a threat. It is up to you to decide if you want to run that during this initial policy or remember to monitor the device when it runs as scheduled.

2. After Execution Control and Process Monitor are complete, enable **Background Threat Detection — Run Once and Watch For New Files**.

- a. The Background Threat Detection scan can take up to one week, depending on how busy the system is and the number of files on the system that require analysis.

- b. It is recommended to set Background Threat Detection to Run Once. Due to the predictive nature of BlackBerry Cylance's technology, periodic scans of the entire disk are not necessary. You can implement periodic scanning for compliance purposes (example: PCI compliance).

- c. Watch For New Files might impact performance. Check if disk or message processing performance has changed.

- d. Excluding folders might improve performance and ensure that certain folders and files do not get scanned or analyzed by the Agent.

- e. If identified threats include any legitimate applications necessary for business operations, make sure to Waive or Safe list these files. You can also exclude the folder containing the file.
3. Under Protection Settings, enable **Kill Unsafe Running Processes** after Execution Control and Process Monitor are complete.

Kill Unsafe Running Processes and their Sub Processes kills processes (and sub-processes), regardless of state, when a threat is detected (EXE or MSI).
4. Under File Actions, turn on **Auto-Quarantine** and **Memory Protection**, with Violation Type set to **Alert**.
 - *Auto-Quarantine* moves any malicious files to the quarantine folder.
 - Memory Protection set to Alert will send information to the Console but will not block or terminate any processes running in memory.
 - If Memory Protection identifies any legitimate processes necessary for business operations, exclude the executable file. In the policy, include the relative path to the file.
5. After testing Memory Protection set to Alert, change the Violation Type to **Block**.
 - a. Memory Protection set to Block will send information to the Console and will stop any malicious processes running in memory. It will not terminate the file initiating the malicious process.
6. For Device Control, before setting the policy and creating exceptions, administrators should:
 - a. Create or edit a policy used for testing. Make sure a test device is assigned to this policy.
 - b. Enable Device Control and set it to Full Access.
 - c. On the test device, insert a USB device and examine the logs to ensure the right Vendor ID, Product ID, and Serial Number are used in the exception.

Note: Not all manufacturers use a serial number with their products. Some manufacturers use the same serial number for multiple products.
 - d. Once testing is complete, set Device Control to Full Access or Block, and add any exceptions needed.
7. Under Protection Settings, turn on **Script Control** to Alert. **Suggested time: 1-3 weeks**

Script Control protects users from malicious scripts running on their device. The longer the time Script Control is set to alert, the more likely you are to find infrequently run scripts used in the organization.

Users can approve scripts to run for specified folders.

Script Control folder exclusions must specify a relative path of the folder (for example, `\Cases\ScriptsAllowed`).

Note: Enabling Script Control can cause a high-volume of events if your environment uses scripts to manage your Active Directory settings.

Once a device has 0 script control alerts, Script Control can be set to **Block**.

File Actions

Settings > Device Policy > [select a policy] > File Actions

File Actions provide different options for handling files detected by CylancePROTECT as either *Unsafe* or *Abnormal*.

Tip: To learn more about the classification of *Unsafe* or *Abnormal* files, refer to "[Threat Protection](#)" on page 140.

The screenshot displays the 'File Actions' configuration page for a policy named 'aa'. The page includes a navigation bar with tabs for 'File Actions', 'Memory Actions', 'Protection Settings', 'CylanceOPTICS Settings', 'Application Control', and 'Agent Settings'. The 'File Actions' tab is selected and highlighted with a green underline. Below the navigation bar, there are two columns for 'Unsafe' and 'Abnormal' file types. Under each column, there is a table with a header 'File Type' and a row for 'EXECUTABLE'. The 'EXECUTABLE' row has a checkbox and a dropdown menu for each column, both currently set to 'Auto Quarantine with Execution Control'. Below the tables, there is a checkbox for 'Enable auto-delete for quarantined files' with a note 'Available for Agent Version 1430 and higher.' and a text box for 'Set number of days until deletion:' with a value of '14' and a note 'Minimum: 14'. There is also an 'Auto Upload' section with a checkbox for 'Executable'. At the bottom, there is a 'Policy Safe List' section with a note 'Available for Agent Version 1290 and higher.' and buttons for 'Add File' and 'Remove from List'. Below this is a table with columns for 'NAME', 'SHA256 HASH', 'CYLANCE SCORE', 'CLASSIFICATION', and 'TYPE'. The table is currently empty, and the footer shows 'No items to display' and '50 items per page'.

Figure 3: Policy Details > File Actions

Auto Quarantine with Execution Control

This feature *Quarantines* or blocks the *Unsafe* or *Abnormal* file to prevent it from executing. Quarantining a file moves the file from its original location to the *Quarantine* directory.

- **For Windows:** `C:\ProgramData\Cylance\Desktop\q`
- **For macOS:** `/Library/Application Support/Cylance/Desktop/q`
- **For Linux:** `/opt/cylance/desktop/q`

Some malware is designed to drop other files in certain directories. This malware continues to do so until the file is successfully dropped. CylancePROTECT modifies the dropped file so it will not execute to stop this type of malware from continually dropping the removed file.

Tip: Make sure you test *Auto Quarantine* on a small number of devices before applying it to your production environment. This is so you can observe the test results and ensure that no business-critical applications are blocked at execution.

Enable Auto-Delete for Quarantined Files

With Agent 1430 and higher, this feature enables automatic deletion of quarantined files after a specified number of days. This applies to all devices assigned to the policy. The minimum number of days is 14, the maximum is 365.

When enabled, the Agent automatically deletes these files after the designated time. The number of days starts when the file was first quarantined. This action is included in the Agent log file for verification and the file is removed from the quarantine list in the Agent UI. If this feature is not enabled, the quarantined files will remain on the device until the quarantined files are manually deleted.

Note: When a device using Agent 1420 (or lower) is upgraded to Agent 1430 (or higher), files quarantined before the upgrade will start to count the number of days after the upgrade, and will be automatically deleted after the set number of days.

1. Select **Settings > Device Policy**. Create a new policy or edit an existing policy.
2. On the File Actions tab, select **Enable auto-delete for quarantined files**.
3. Set the number of days until the quarantined file is deleted. The number of days can be from 14 days to 365 days.
4. Click **Save**.

File Type	Unsafe	Abnormal
	Auto Quarantine with Execution Control	
EXECUTABLE	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Enable auto-delete for quarantined files Available for Agent Version 1430 and higher.		
Set number of days until deletion: <input type="text" value="14"/> Days <small>Minimum:14</small>		

Figure 4: Auto-delete Quarantined Files

Auto Upload

Make sure that you enable Auto Upload for all available file types. If the Agent finds a file that the Cylance Cloud has never analyzed before, it requests to upload the file for analysis.

If the same unknown file is discovered on multiple devices in the organization, CylancePROTECT uploads one file only from a single device for analysis, not one file per device.

Policy Safe List

You can add files that you consider safe to a Policy.

Using the Policy Safe List means all Agents in that policy will treat the file as Safe, even if the Cylance Score ranks it as *Unsafe* or *Abnormal*.

1. Select **Settings > Device Policy**.
2. Add a new policy or edit an existing policy.
3. Click **Add File** under *Policy Safe List*.
4. Enter the **SHA256** information. Optionally, include the MD5 and File Name, if known.
5. Select a **Category** to help identify what this file does.
6. Enter a reason for adding this file to the *Policy Safe List*.
7. Click **Submit**.

Figure 5: Add a File to the Policy Safe List

Memory Actions

Settings > Device Policy > [select a policy] > Memory Actions

Memory Actions provide different options for handling memory exploits, including process injections and escalations. You can also add executable files to an exclusion list, allowing these files to run when this policy is applied.

VIOLATION TYPE	IGNORE	ALERT	BLOCK	TERMINATE
▶ Exploitation	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stack Pivot	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stack Protect	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Overwrite Code	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
RAM Scraping	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malicious Payload	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ Process Injection	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote Allocation of Memory	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote Mapping of Memory	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote Write to Memory	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote Write PE to Memory	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 6: Policy Details > Memory Actions

Memory Protection

The Agent will scan and monitor running processes to protect devices from malware that attempts to take advantage of software vulnerabilities that exploit running processes or executes

from within memory space. It is recommended that you Block all types of memory violations.

For descriptions of the different Violation, Process, and Escalation Types, see "[Memory Protection Violation Types](#)" on page 27.

WARNING: Enabling Memory Protection may cause errors if there is another application that also monitors running processes. It is recommended to disable the other application's memory protection before enabling Cylance's. If that is not possible, then leave Cylance's Memory Protection disabled in your policies.

- **Ignore:** The Agent will not take any action against identified memory violations.
- **Alert:** The Agent will record the violation and report the incident to the Console.
- **Block:** If an application attempts to call a memory violation process, the Agent will block the process call. The application that made the call is allowed to continue to run.
- **Terminate:** If an application attempts to call a memory violation process, the Agent will block the process call and will also terminate the application that made the call.

Devices > [select a device] > Exploit Attempts (under Threats & Activities).

- **Exclude Executable Files:** Exclude executable files from Memory Protection by specifying the relative path of the file. On Windows, you can also specify the absolute file path. This will allow the specified files to run or be installed on any device within that policy. After applying the exclusion, all instances of that process must be terminated to stop the driver from injecting into it.

Note: This will exclude any "run.exe" executables inside of a folder named app so use shortened relative path exclusions with caution.

- **Windows Example** — \Application\Subfolder\application.exe
- **Windows Example** — C:\Application\Subfolder\application.exe
- **Linux Example** — /opt/application/executable
- **Linux Example** — exclusion for Dynamic Library Files:
/executable.dylib
- **macOS Example** — exclusion without spaces:
/Applications/SampleApplication.app/Contents/MacOS/executable
- **macOS Example** — exclusion with spaces:
/Applications/Sample Application.app/Contents/MacOS/executable
- **macOS Example** — exclusion for Dynamic Library Files:
/executable.dylib

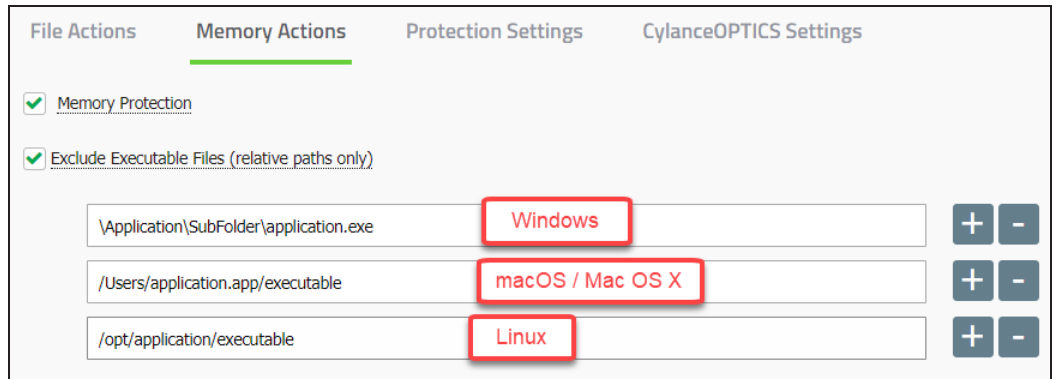


Figure 7: Exclude Executable Files Example

Use Wildcards in Memory Protection Exclusions

Memory exclusions can include the following special characters (all OS):

^ & ' @ { } [] , \$ = ! - # () % . + ~ _

On Windows, the following additional special characters are also supported:

Asterisk (*)

Any letter value followed by colon (C:)

Pattern Syntax for * Wildcard on Windows

Characters	Usage	Details
*	Excluding executables and applications.	Matches zero or more characters, except the platform-specific path separator ('\ on Windows). Notes: <ul style="list-style-type: none"> At this time, "*" escaping is not supported. For example, you cannot exclude a file that contains an asterisk "*" in the file name. Wildcard exclusions for Memory Protection apply only to Windows at this time.
**	Excluding drives and directories. Can be used to include child directories.	Matches zero or more layers of a directory (e.g. "**\"). Note that "***" is not just a double "**", it is a special notation. To avoid confusion, review the following rules when using this special character: <ul style="list-style-type: none"> "**\" is valid if it is at the beginning of pattern, only for Windows. It will match all directories inside all drives. "**\" can appear in the pattern string multiple times, there is no limitation. Note: Wildcard exclusions for Memory Protection apply only to Windows at this time.
Examples	N/A	For the following path:

Characters	Usage	Details
		<p>C:\Application\TestApp\MyApp\program.exe (note that relative paths could also be used)</p> <p>Examples of Correct Exclusions:</p> <ul style="list-style-type: none"> ■ \Application\TestApp\MyApp\program.exe <ul style="list-style-type: none"> • Relative path exclusion without any wildcards. ■ C:\Application**\MyApp\program.exe <ul style="list-style-type: none"> • Would exclude program.exe as long as program.exe is located under "MyApp" child directory in C: drive. ■ C:\Application**\MyApp*.exe <ul style="list-style-type: none"> • Would exclude any .exe extension file as long as the executable is located under "MyApp" child directory in C: drive. ■ C:\Application**\MyApp* <ul style="list-style-type: none"> • Would exclude any executable as long as the executable is located under "MyApp" child directory in C: drive. ■ C:\Application\TestApp**\program.exe <ul style="list-style-type: none"> • Would exclude program.exe as long as program.exe is located under any child directory that belongs to "TestApp" parent directory in C: drive. ■ **\Application\TestApp\MyApp\program.exe <ul style="list-style-type: none"> • Would exclude program.exe as long as program.exe is located under \Application\TestApp\MyApp\ for any drive. ■ **\Application\TestApp\MyApp*.exe <ul style="list-style-type: none"> • Would exclude any .exe extension file as long as the executable is located under \Application\TestApp\MyApp\ for any drive. ■ **\Application\TestApp\MyApp* <ul style="list-style-type: none"> • Would exclude any executable as long as the executable is located under \Application\TestApp\MyApp\ for any drive. <p>Example of Incorrect Exclusions:</p> <ul style="list-style-type: none"> ■ C:\Application\TestA**.exe <ul style="list-style-type: none"> • "*" is used for directories. Use a single asterisk "*" for executables. ■ C:\Application** <ul style="list-style-type: none"> • "*" is used for directories. There is no single asterisk "*" specifying executables to exclude. <p>Not Recommended Exclusions:</p>

Characters	Usage	Details
		<ul style="list-style-type: none"> ■ Correct (but not recommended): C:**** <ul style="list-style-type: none"> ● Would effectively exclude anything in any directory (including child directories) under the C: drive. ■ Correct (but not recommended): *** <ul style="list-style-type: none"> ● Would effectively exclude anything in any directory (including child directories) in any drive.
<p>Note: In a normal wildcard, three asterisks "***" are valid and equal a single asterisk "*". However, three asterisks are not valid for exclusions because it would hide typos. For example, in the pattern "C:***.exe", users might have wanted to type "c:***.exe" but missed one "\". If "****" were treated as a single "*" it could result in different behavior than was intended.</p>		

Memory Protection Violation Types

Exploitation Violation Types	Applies to
<p>Stack Pivot — The stack for a thread has been replaced with a different stack. Generally the system will only allocate a single stack for a thread. An attacker would use a different stack to control execution in a way that is not blocked by Data Execution Prevention (DEP).</p>	Windows macOS Linux
<p>Stack Protect — The memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so usually this means that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt which would otherwise be blocked by Data Execution Prevention (DEP).</p>	Windows macOS Linux
<p>Overwrite Code — Code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP).</p>	Windows
<p>RAM Scraping — A process is trying to read valid magnetic stripe track data from another process. Typically related to point of sale systems (POS).</p>	Windows
<p>Malicious Payload — A generic shellcode and payload detection associated with exploitation has been detected.</p>	Windows
Process Injection Violation Types	Applies to
<p>Remote Allocation of Memory — A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system.</p>	macOS
<p>Remote Mapping of Memory — A process has introduced code and/or data into</p>	Windows

another process. This may indicate an attempt to begin executing code in another process and thereby reinforce a malicious presence.	
Remote Write To Memory — A process has modified memory in another process. This is usually an attempt to store code or data in previously allocated memory (see OutOfProcessAllocation) but it is possible that an attacker is trying to overwrite existing memory in order to divert execution for a malicious purpose.	Windows macOS
Remote Write PE To Memory — A process has modified memory in another process to contain an executable image. Generally this indicates that an attacker is attempting to execute code without first writing that code to disk.	Windows
Remote Overwrite Code — A process has modified executable memory in another process. Under normal conditions executable memory will not be modified, especially by another process. This usually indicates an attempt to divert execution in another process.	Windows
Remote Unmap of Memory — A process has removed a Windows executable from the memory of another process. This may indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution.	Windows
Remote Thread Creation — A process has created a new thread in another process. A process's threads are usually only created by that same process. This is generally used by an attacker to activate a malicious presence that has been injected into another process.	Windows macOS
Remote APC Scheduled — A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process.	Windows
DYLD Injection — An environment variable has been set that will cause a shared library to be injected into a launched process. Attacks can modify the plist of applications like Safari or replace applications with bash scripts, that cause their modules to be loaded automatically when an application starts.	macOS Linux
Escalation Violation Types	Applies to
LSASS Read — Memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.	Windows
Zero Allocate — A null page has been allocated. The memory region is typically reserved, but in certain circumstances it can be allocated. Attacks can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel.	Windows macOS

Protection Settings

Settings > Device Policy > [select a policy] > Protection Settings

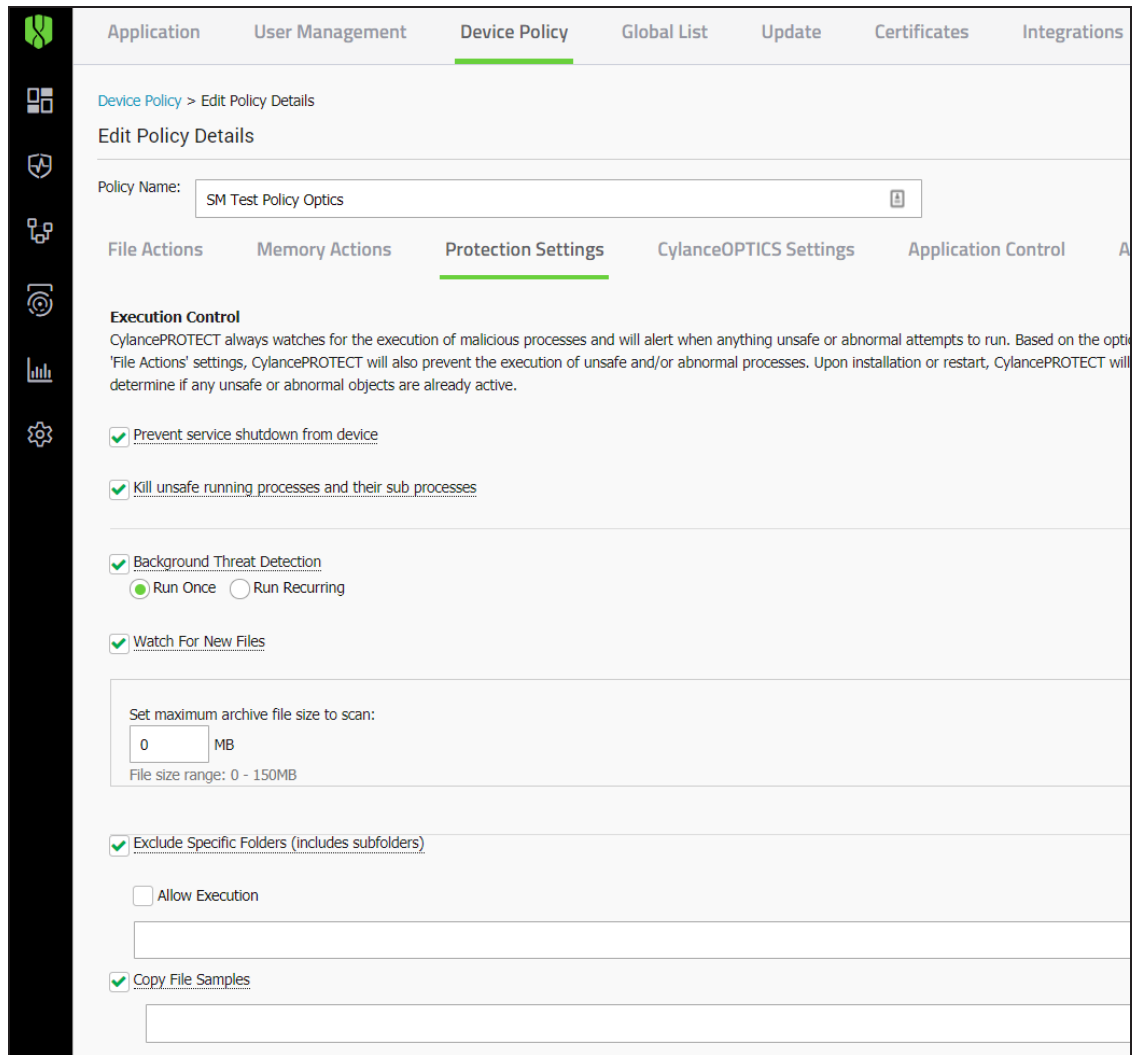


Figure 8: Policy > Protection Settings

Execution Control

CylancePROTECT always watches for the execution of malicious processes and alerts when anything *Unsafe* or *Abnormal* attempts to run.

Prevent Service Shutdown from Device

If selected, the Cylance service is protected from being shutdown either manually or by another process.

Kill Unsafe Running Processes and Their Sub Processes

Terminates processes, and child processes, regardless of state when a threat is detected (EXE or DLL). This offers a high level of control over malicious processes that might be running on a device. The file must be auto-quarantined, manually quarantined, or quarantined using the Global Quarantine list. This feature must be enabled before the file is quarantined.

Note: If this feature is enabled but the file is not quarantined or auto-quarantined, the processes will continue to run.

Example: A file is allowed to run, then you decide to quarantine the file. With this feature enabled, the file is quarantined and the process is terminated. Without this feature enabled, the file would be quarantined, but because the file was allowed to run, any processes started by the file could continue to run.

Background Threat Detection

Background Threat Detection will perform a full disk scan to detect and analyze any dormant threats on the disk. The full disk scan is designed to minimize impact to the end-user by using a low amount of system resources.

The user can choose to run the scan once (upon installation only) or run recurring (which performs a scan every 9 days). A significant upgrade to the detection model, like adding new operating systems, will also trigger a full disk scan. Each time a new scan is performed, all files will be rescanned.

It is recommended that users set Background Threat Detection to Run Once. Due to the predictive nature of the Cylance's technology, periodic scans of the entire disk are not necessary but can be implemented for compliance purposes.

To manually run a scan on an endpoint, see ["Enable Agent User Interface Advanced Options" on page 123](#), then run a detection.

Watch for New Files

The Agent will detect and analyze any new or modified files for dormant threats. It is recommended that users enable Watch for New Files. However, if Auto Quarantine is enabled for all *Unsafe* or *Abnormal* files, all malicious files will be blocked at execution. Hence, it is not necessary to enable Watch For New Files with Auto Quarantine mode unless the user prefers to quarantine a file as it is added to a disk (Watch For New Files) but before execution (Auto-Quarantine).

Set Maximum Archive File Size to Scan

Set the maximum archive file size the Agent will scan. This setting applies to Background Threat Detection and Watch for New Files. Setting the file size to 0MB means no archive files

will be scanned.

Exclude Specific Folders

Users are able to exclude specific folders, including subfolders, from Background Threat Detection and/or Watch For New Files (when these features are enabled) by specifying the path of the folder location. For Windows, use an absolute path (including the drive letter). For macOS or Linux, use an absolute path from the drive root (macOS and Linux don't use a drive letter) and remember to escape any spaces in the path.

Example — Windows: C:\Test

Example — macOS, exclusion without spaces: /Applications/SampleApplication.app

Example — macOS, exclusion with spaces: /Applications/ Sample\ Application.app

Example — Linux: /opt/application/

Copy File Samples (Malware)

Allows you to specify a network share to which file samples found by Background Threat Detection, Watch for Files, and Execution Control can be copied. This allows users to do their own analysis of files CylancePROTECT considers *Unsafe* or *Abnormal*.

- Supports CIFS/SMB network shares.
- Specify one network share location. You should use a fully qualified path. Example: \\server_name\shared_folder.
- All files meeting the criteria will be copied to the network share, including duplicates. No uniqueness test is performed.
- Files are compressed (requires Agent version 1390 and higher).
- Files are password protected (requires Agent version 1390 and higher). The password is "infected".

Application Control

Application Control is an optional setting and is enabled using a policy setting. This feature allows users to restrict any changes to executables on the device. Only applications that are on the device before Application Control is enabled are allowed to execute. Trying to add new applications or changing an existing application on the device will be denied.

IMPORTANT:

- Application is typically used for fixed function devices that are not changed after setup (example: point-of-sale machines).

- Application Control is available for Windows and Linux systems. Application Control is not supported by the macOS Agent.
- The Cylance Agent update is disabled when Application Control is enabled; this applies to CylancePROTECT and CylanceOPTICS.
- Trying to uninstall the Cylance Agent will fail when Application Control is enabled; this applies to CylancePROTECT and CylanceOPTICS.
- It is NOT recommended to run CylanceOPTICS on systems using Application Control. When Application Control is enabled, CylanceOPTICS will not function properly due to the restrictive nature of Application Control.

The main objectives of Application Control are:

- Deny execution of executable files from remote or external drives.
- Deny creation of new executables on the local drive. See [About Linux Agent and Application Control](#) below for differences in the Linux Agent.
- Deny changes to existing files on the local drive.

When you activate Application Control, the following recommended settings will take place (see image below). With Application Control enabled, you can edit these policy settings by going directly to their tasks.

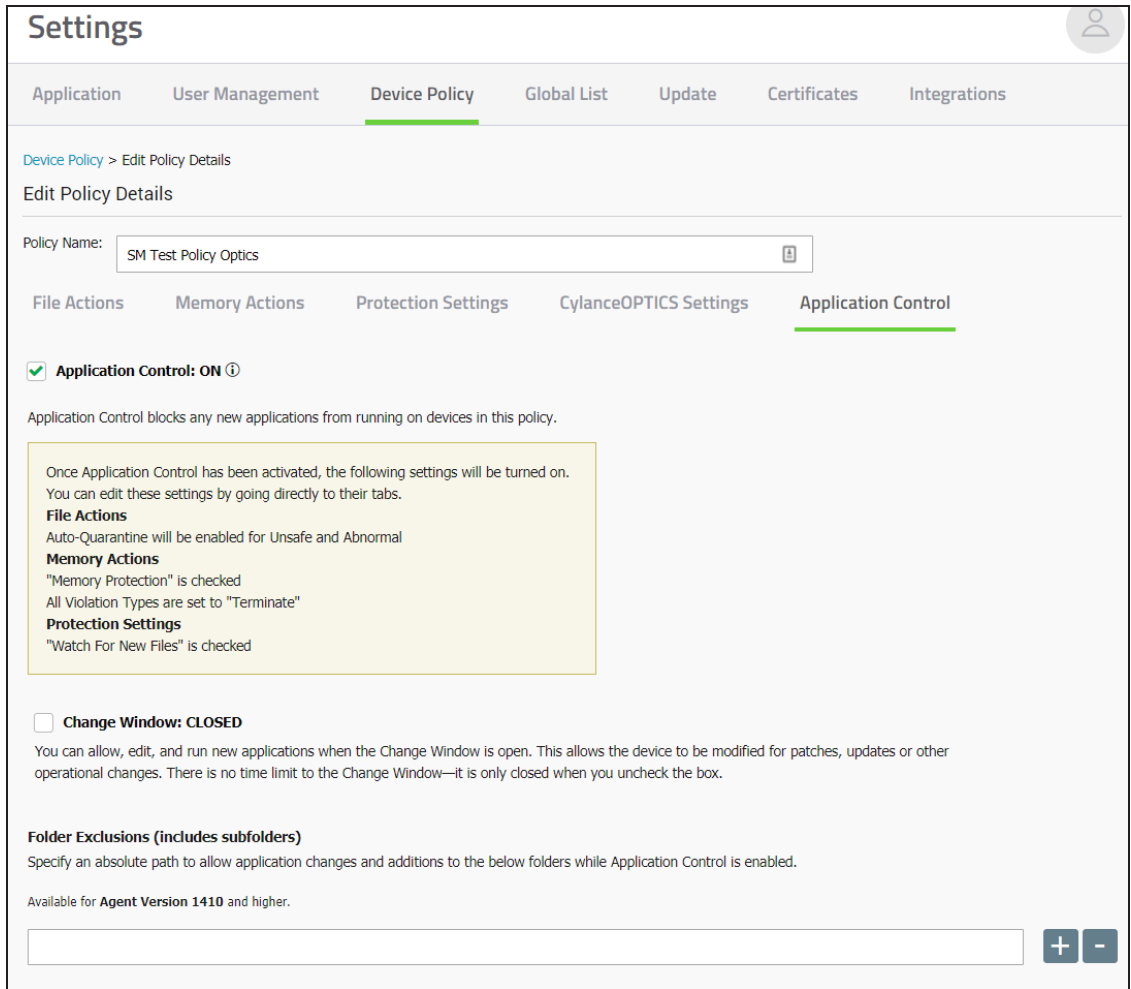


Figure 9: Policy Details > Application Control

To view Application Control activity, users can sign in to the Console and click any device that is in a device policy with Application Control enabled. The Device Details page lists all actions relevant to Application Control under the Threats & Activities section.

Notes:

- For Linux operating systems, Application Control uses the inventory system and only files in the inventory can execute. Application Control for Linux does not prevent a file from being created but does prevent inventoried files from being modified.
- If Application Control is enabled, functionality for CylanceOPTICS will fail.

Change Window

Use the Change Window option to temporarily disable Application Control to allow, edit, and run new applications or perform updates. This includes updating the Agent. After performing the necessary changes, turn Change Window off (Closed).

Note: Using the Change Window retains any changes made to the Application Control settings. Turning Application Control OFF and then back ON resets the Application Control settings back to default.

Folder Exclusions (Including Subfolders)

Specify an absolute path to allow application changes and additions to the specified folders while Application Control is enabled (requires Agent 1410 and higher).

About Linux Agent and Application Control

- Folder Exclusions are not supported by the Linux Agent.
- When Application Control is enabled, an inventory of all executable files on the local file system is generated. File execution is restricted to the files in the inventory.
- Even with Application Control enabled, you can add executable files to the device, but these will not run. Only applications in the inventory when Application Control is enabled are allowed to run.
- Allowing an update on a Linux device with Application Control enabled may cause issues.

Agent Settings

Settings > Device Policy > [select a policy] > Agent Settings

Enable Auto-upload of Log Files

Enable Agent Logs in the Console to upload log files and view them in the Console. Uploaded log files are stored for 30 days.

1. Select **Settings > Device Policy**.
2. Select a policy, and click **Agent Settings**. Ensure the device selected for log files is assigned to this policy.
3. Select **Enable auto-upload of log files** and click **Save**.
4. Click the **Devices** tab, and select a device.
5. Click **Agent Logs**. The log files display.
6. Click a log file. The log file name is the date of the log.

Settings

Application User Management **Device Policy** Global List Update Certificates Integrations

Device Policy > Edit Policy Details

Edit Policy Details

Policy Name:

File Actions Memory Actions Protection Settings CylanceOPTICS Settings Application Control **Agent Settings**

Enable auto-upload of log files
Available for **Agent Version 1280** and higher.

Enable Desktop Notifications
Available for **Agent Version 1390** and higher.

Figure 10: Device Policy > [select a device] > Agent Settings

THREATS & ACTIVITIES

Threats (1) Exploit Attempts (18) Application Control **Agent Logs** Script Control (0) External Devices (0)

Available for **Agent version 1280** and higher.

NAME	FILE SIZE	UPLOAD DATE
Optics-2018-10-23.csv	497.36 KB	10/24/18 12:01 AM
Optics-2018-10-22.csv	493.02 KB	10/23/18 6:26 PM
Optics-2018-10-21.csv	491.96 KB	10/23/18 6:26 PM
Optics-2018-10-20.csv	493.93 KB	10/23/18 6:26 PM
Optics-2018-10-19.csv	493.35 KB	10/23/18 6:26 PM
Optics-2018-10-18.csv	492.32 KB	10/23/18 6:26 PM
Optics-2018-10-17.csv	691.33 KB	10/23/18 6:26 PM
Optics-2018-10-16.csv	217.06 KB	10/23/18 6:26 PM
2018-10-23.log	1807.32 KB	10/24/18 12:00 AM
2018-10-22.log	1642.10 KB	10/23/18 12:00 AM
2018-10-21.log	1636.03 KB	10/22/18 12:00 AM
2018-10-20.log	1677.08 KB	10/21/18 12:00 AM
2018-10-19.log	1636.55 KB	10/20/18 12:00 AM
2018-10-18.log	1932.41 KB	10/19/18 12:00 AM
2018-10-17.log	2796.02 KB	10/18/18 12:00 AM
2018-10-16.log	1264.24 KB	10/17/18 12:00 AM
2018-10-15.log	951.97 KB	10/16/18 17:05 AM

50 Items per page

Figure 11: Devices > [select a device] > Agent Logs

Enable Desktop Notifications

Agent Notification popups can be configured on each device or set at the policy-level in the Console. Enabling or disabling the Agent Notification popups at the device-level takes precedence over the Console settings.

This feature requires Agent version 1390 or higher.

Note: In the Agent UI, the Events tab is cleared when the CylanceUI is restarted or when the device is rebooted.

To Enable Desktop Notifications from the Console

1. Select **Settings > Device Policy**.
2. Click on a policy, then click **Agent Settings**. Make sure the device you want log files for is assigned to this policy.
3. Select **Enable Desktop Notifications**, then click **Save**.

To Clear Agent Notifications on a Device

When Agent notifications are enabled or disabled on a device, that setting is saved to a file on the device. This setting overrides the setting in the policy. To allow the policy to control Agent notifications, this saved file must be deleted from the device (if this file exists).

1. On the device, right-click the Agent icon, then select **Exit**.
2. Delete the settings.
 - **Windows:** Delete the configuration file by going to `\Users\USERNAME\AppData\Local\Cylance\Desktop`, then delete `CylanceUI.cfg`
 - **macOS:** Run `defaults delete com.cylance.CylanceUI` from the Terminal.

Note: This command will return "Domain (com.cylance.CylanceUI) not found" if Enable Desktop Notifications was set the Console's policy instead of at the device-level.
 - **Linux:** Execute the following commands

```
gconftool-2 -u /apps/cylanceui/show_notifications
gconftool-2 -u /apps/cylanceui/user_changed_show_notifications
```
3. Restart the Agent UI.

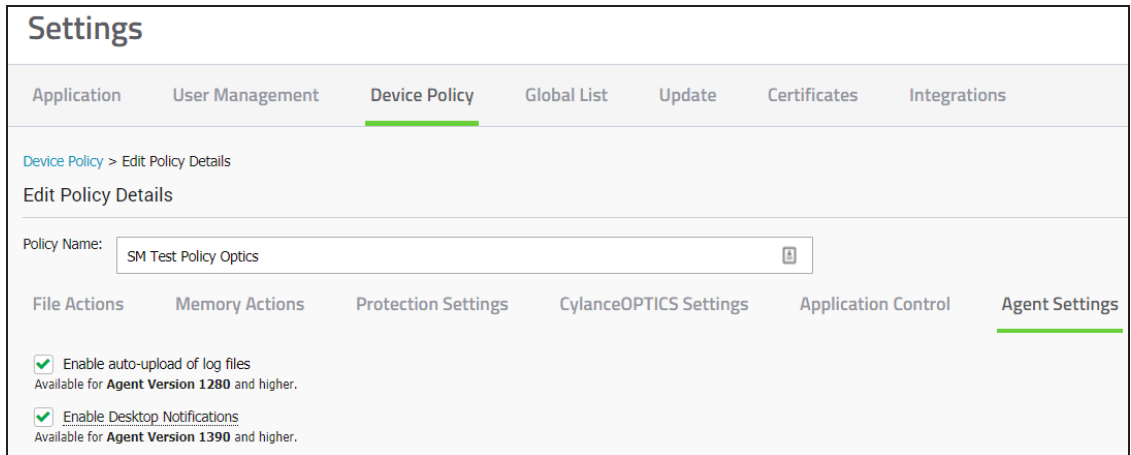


Figure 12: Policy Details > Agent Settings

Script Control

Settings > Device Policy > [select a policy] > Script Control

Script Control protects devices by blocking malicious Active Script and PowerShell scripts from running. With Agent versions 1380 and higher, you can alert or block malicious Microsoft Office macros.

Script Control monitors and protects against scripts running in your environment. The Agent is able to detect the script and script path before the script is executed. Depending on the policy set for Script Control (Alert or Block), the Agent will allow or block the execution of the script.

Microsoft Office macros use Visual Basic for Applications (VBA) that allows embedding code inside an Office document (typically Word, Excel, and PowerPoint). The main purpose for macros is to simplify routine actions, like manipulating data in a spreadsheet or formatting text in a document. However, malware creators can use macros to run commands and attack the system. It is assumed that a Microsoft Office macro trying to manipulate the system is a malicious action. The Agent looks for malicious actions originating from a macro that affects things outside the Microsoft Office products.

Tip: Starting with Microsoft Office 2013, macros are disabled by default. Most of the time, you do not need to enable macros to view the content of an Office document. You should only enable macros for documents you receive from users you trust, and you have a good reason to enable it. Otherwise, macros should always be disabled.

1. Select **Settings > Device Policy**.
2. Select a policy and click **Script Control**.
3. Select the check box to enable **Script Control**.

4. Set the Script Control action to **Alert** or **Block**. For Agent 1370 and lower, setting the action affects Active Script and PowerShell. For Agent 1380 and higher, the action can be set separately for Active Script, PowerShell, and Macros.

a. **Alert:** Monitors scripts running in your environment. Recommended for initial deployment.

b. **Block:** Only allow scripts to run from specific folders. Use after testing in Alert mode.

Note: If the script launches the PowerShell console, and Script Control is set to block the PowerShell console, the script will fail. It is recommended that users change their scripts to invoke the PowerShell scripts, not the PowerShell console.

5. For Agents 1430 and higher, enabling **Disable Script Control** means the script type will not be blocked or alerted on. For Agents 1420 and lower, the only settings are Alert or Block, meaning some action is always taken on the script type.

6. Add **Folder Exclusions (includes subfolders)**. Script folder exclusions must specify the relative path of the folder.

Notes:

- If you want to exclude a specific script, you must use a wildcard. See Use Wildcards in Script Control Exclusions below for more information.
- If the “everyone” group has write permissions (share or file) this makes the folder “world-writable” and CylancePROTECT will continue to alert/block on scripts. This is because if the everyone group has write permissions, anyone inside or outside of the organization can drop a script in a folder or subfolder and write to it. The world-writable restrictions applies not only to the direct parent folder, but all parent folders, all the way to the root.

7. Click **Save**.

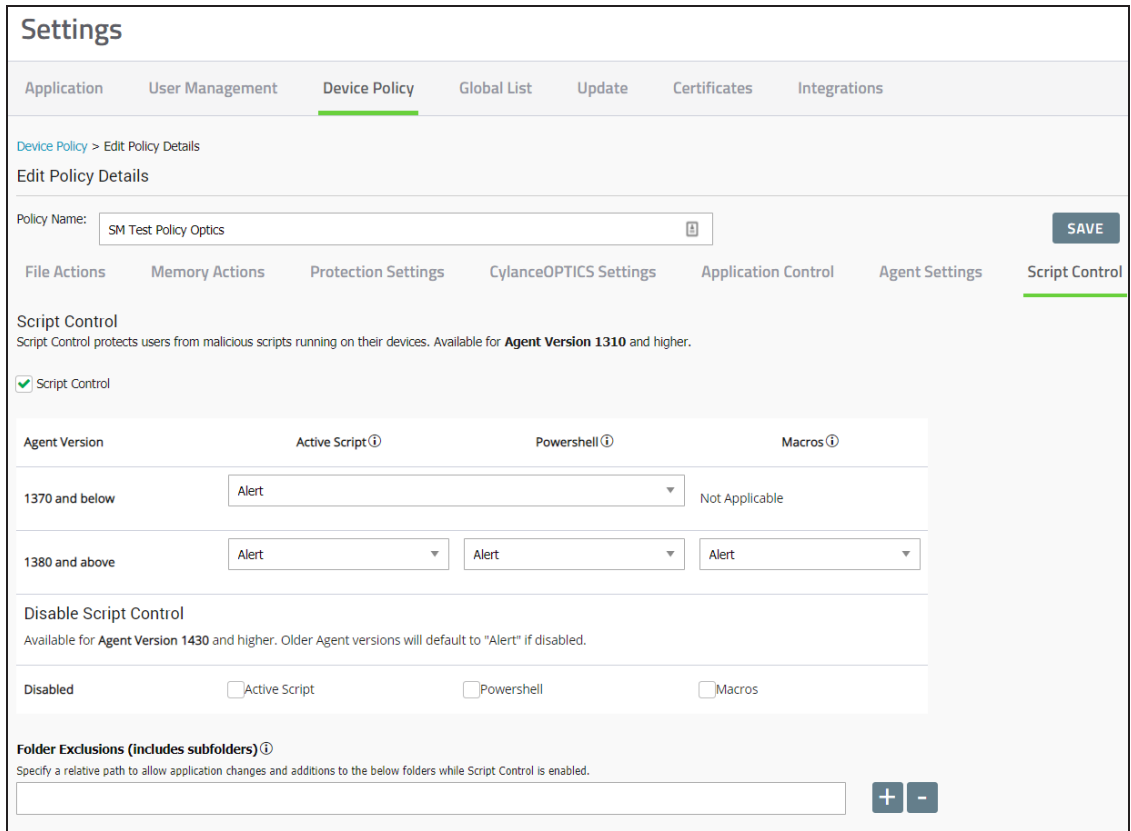


Figure 13: Policy Details > Script Control

Use Wildcards in Script Control Exclusions

With Agent 1490 and higher, you can use “*” as a wildcard in a script control exclusion. The wildcard can exclude a folder or a script.

Using script control exclusions with wildcards should reduce the number of alerts displayed in your Console. By allowing the exclusion of full or partial script names, you do not need to exclude an entire folder. By allowing the exclusion of partial script names, you can exclude a portion of the script name that is common for a group of scripts they want to exclude.

IMPORTANT: While using wildcards provides flexibility in allowing exclusions, it can also lower your security stance if the exclusion is too broad. For example, excluding the entire \Windows\Temp folder is not recommended. However, if a program or file you trust puts a script in the \Windows\Temp folder and CylancePROTECT blocks it, you can use a wildcard as part of the file name to exclude that script.

Things To Know About Wildcard Support

- Wildcard exclusions must use Unix-style slashes for Windows systems.
 - Example: /windows/system*/*.

- Wildcard exclusions use regular expressions (regex).
- The only token support for wildcards is `*`.
- Wildcard exclusions give you the flexibility to exclusively allow the script or macro file, as long as there is a `*` at any given path per examples below. Note that this does not apply to Access databases.
- Folder exclusions with a wildcard must have a wildcard at the end of the path to differentiate between a folder and a file.
 - Folder exclusion: `/windows/system32/*`
 - Folder exclusion: `/windows/*/test/*`
 - Folder exclusion: `/windows/system32/test*/*`
- File exclusions with a wildcard must have a file extension to differentiate between a file and a folder.
 - File exclusion: `/windows/system32/*.vbs`
 - File exclusion: `/windows/system32/script*.vbs`
 - File exclusion: `/windows/system32/*/script.vbs`
 - **One wildcard per level.**
 - So `/folder/*/script.vbs` matches `\folder\test\script.vbs` or `\folder\exclude\script.vbs` but does not work for `\folder\test\001\script.vbs`. This would require either `/folder*/001/script.vbs` or `/folder*/*/script.vbs`.
 - The wildcard would need to persist down per level to where the script resides.
 - Two or more wildcards per level are not allowed. For example, `*/folder/*file*.ext` is not allowed.
- Wildcards support full and partial exclusions.
 - Example - Full wildcard: `/folder/*/script.vbs`
 - Example - Partial wildcard: `/folder/test*/script.vbs`
- If you can identify a common relative path, you can exclude Universal Naming Convention (UNC) paths with a wildcard.
 - Example: For devices with names of DC01 – DC24, you could use `/dc*/path/to/script/`
- Network paths can also be excluded:

- //hostname/application/*
- //host*/application/*
- /*name*/application/*
- //hostname/*

Exclusion Examples

Adding exclusions for dynamic scripts that are run from a specific directory location or for a script that is run from multiple different user folders is possible by using wildcards in Script Control exclusions. As an example, you can use the token "*" in the exception path to ensure it covers your variants.

- **/users*/temp/* would cover:**

- \users\john\temp
- \users\jane\temp

- **/users*/temp/* would NOT cover:**

- \users\folder\john\temp
- \users\folder\jane\temp

Note: The above would require - /users*/*/temp/*.

- **/program files*/app/script*.vbs would cover:**

- \program files(x86)\app\script1.vbs
- \program files(x64)\app\script2.vbs
- \program files(x64)\app\script3.vbs

- **/program files*/app/script*.vbs would NOT cover:**

- \program files(x86)\app\script.vbs
- \program files\app\script1.vbs

Note: The first one would require /program files*/app/script.vbs or /program files*/app/*.vbs. The second would require /program files/app/script*.vbs or /program files*/script*.vbs.

- **//*example.local/sysvol/script*.vbs would cover:**

- \\ad.example.local\sysvol\script1.vbs

- **//*example.local/sysvol/script*.vbs would NOT cover:**

- \\ad.example.local\sysvol\script.vbs

- /users/*/*/*.vbs would cover:
 - /users/john/temp/script.vbs

Other Exclusion Options for Script Control

You can use the Global Safelist or add a Certificate as alternative methods to exclude scripts.

- Global Safelist a Script - Allows for Script Exclusion regardless of location.
 - Is inefficient if the script changes programmatically or is frequently updated (appends a new date/time, system request, etc. that automatically change the script and hash) and for Macros (these typically change for each execution because of the way the Macro pulls in the data).
 - May require more administrative work to maintain. As script hashes change, you will need to remove the old hash and add the new one to the safelist.
 - When attempting to add the the following SHA256 hash to the Global List, an error message displays. This message is due to Agent functionality. A SHA256 needs to be reported to the CylancePROTECT Console.
 - FE9B64DEFD8BF214C7490AA7F35B495A79A95E81F8943EE279DC99998D3D3440

This is a generic hash the CylancePROTECT Agent uses when a hash cannot be generated for a script. Examples of when a hash might not be generated include: if the script doesn't execute properly, the file doesn't exist, or there are permission issues.
 - FE9B64DEFD8BF214C7490BB7F35B495A79A95E81F8943EE279DC99998D3D3440

This is a generic hash the CylancePROTECT Agent uses when a Powershell one-liner is used and a hash cannot be generated for a script. Examples of when a hash might not be generated include: if the script doesn't execute properly, the file doesn't exist, or there are permission issues.
- Add a Certificate for a Script - Allows for Script Exclusion regardless of location.
 - Can be used for PowerShell and Active Scripts only (Does not work for Macros)
 - Should be a valid code signing certificate
 - Must be uploaded to the Console

Device Control

Device Control protects devices by controlling USB mass storage devices connecting to devices in the organization. With Agent version 1410 and higher, you can allow or block things identified as USB mass storage devices, including USB flash drives, external hard drives, and smartphones. Device Control is available for the Windows platform only.

Administrators can enable Device Control using a Device Policy, and can choose to allow or block access to USB mass storage devices. This only applies to USB devices that are classified as Mass Storage. USB peripherals, such as a keyboard, are not affected. For example, if an administrator creates a policy to block USB mass storage devices, an end-user can still use a USB mouse, but a USB flash drive would be blocked.

As part of a Device Control policy, administrators can also define exceptions to the policy. This is done by using the Vendor ID, Product ID, and Serial Number to specify the exception. Minimally, the Vendor ID must be entered, but the Product ID and Serial Number can also be used for a more specific exception.

When enabled, Device Control will log all USB mass storage devices that are inserted, along with the policy that was applied (Allow or Block). If Desktop Notifications are enabled, end-users will see a pop-up notification only if the policy is set to Block. Device Control events can be found on the Protection page, under the External Devices tab.

Note: SD Cards are not supported by Device Control at this time, however if they are used with a USB-based reader, the USB device may be detected by Device Control.

Enable Device Control

1. In the Console, select **Settings > Device Policy**.
2. Create a new policy or edit an existing policy.
3. Click the **Device Control** tab.
4. Select **Device Control** to enable it.

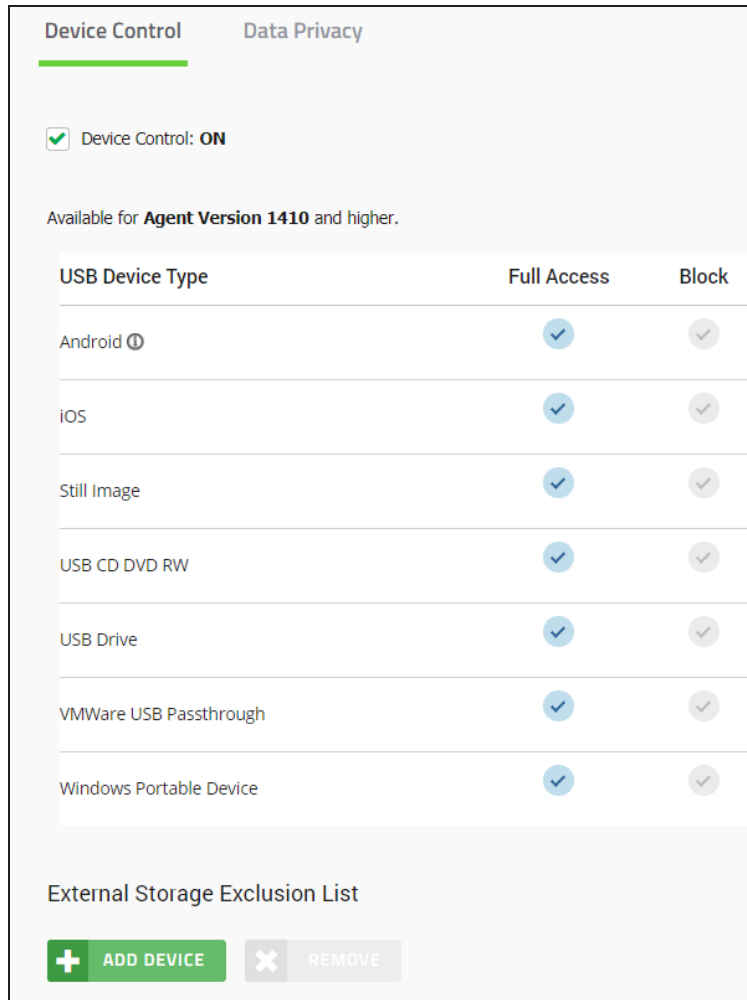


Figure 14: Device Policy > Device Control

- a. Block the USB Device Types you do not want connecting to devices. The following options are available:

Option	Description
Android	A portable device running Android OS, like a smartphone or a tablet. Note: An Android device could connect and be identified as Android, Still Image, or Windows Portable Device. If you want to block Android devices, consider blocking Still Image and Windows Portable Device as well.
iOS	An Apple portable device running iOS, like an iPhone or an iPad. Note: iOS devices will not charge when Device Control is enabled and set to Block unless the device is powered off. Apple includes

Option	Description
	their charging capability within functions of the device that are required for our iOS device blocking capability. Non-Apple devices do not bundle their charging capability in this manner and are not impacted.
Still Image	The device class containing scanners, digital cameras, multi-mode video cameras with frame capture, and frame grabbers. Note: The Agent sees Canon cameras as a Windows Portable Device, not as a Still Image device.
USB CD DVD RW	A USB optical drive.
USB Drive	A USB hard drive or USB flash drive.
VMware USB Passthrough	Allows a VMware virtual machine client to access USB devices connected to the host.
Windows Portable Device	Portable devices that use the Microsoft Windows Portable Device (WPD) driver technology, such as mobile phones, digital cameras, and portable media players.
Notes: <ul style="list-style-type: none"> • SD Cards are not supported by Device Control at this time, however if utilized with a USB based reader, the USB device may be detected by Device Control. • On Windows XP, the Windows Lumia 640 LTE phone is seen as a Still Image device. 	

5. Click **Save**.

Add External Storage Exclusion

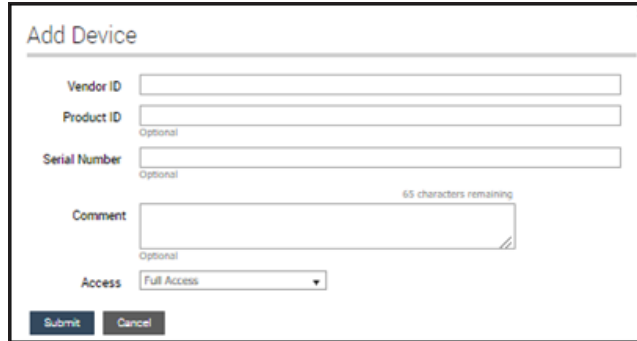
Before creating exclusions as part of the Device Control policy, you should first enable Device Control in a Policy, then insert a USB device and examine the logs to ensure the right Vendor ID, Product ID and Serial Number are used in the exception.

Notes:

- Not all manufacturers use a serial number with their products. Some manufacturers use the same serial number for multiple products.
- External Storage Exclusions are not editable. To update an exclusion, you must delete the existing (if no longer needed) and add a new exclusion.

To Add an Exclusion

1. In the Console, select **Settings > Device Policy**.
2. Create a new policy or edit an existing policy.
3. Click the **Device Control** tab and make sure Device Control is enabled.
4. Under External Storage Exclusion List, click **Add Device**.



The screenshot shows a modal window titled "Add Device". It contains the following fields and controls:

- Vendor ID**: A required text input field.
- Product ID**: An optional text input field.
- Serial Number**: An optional text input field.
- Comment**: An optional text area with a character count of "65 characters remaining".
- Access**: A dropdown menu currently set to "Full Access".
- Buttons**: "Submit" and "Cancel" buttons at the bottom.

Figure 15: Add device to External Storage Exception List

5. Enter the Vendor ID (required). Include the Product ID and Serial Number to refine the exclusion. You can also add a Comment to describe the exclusion.
6. For Access, select **Full Access** or **Block**.
7. Click **Submit**.

Bulk Import Device Control Exclusions

Administrators can create a CSV file that contains their Device Control exclusions, up to 500 exclusions per file. A sample template is provided in the Device Control article on the Support site.

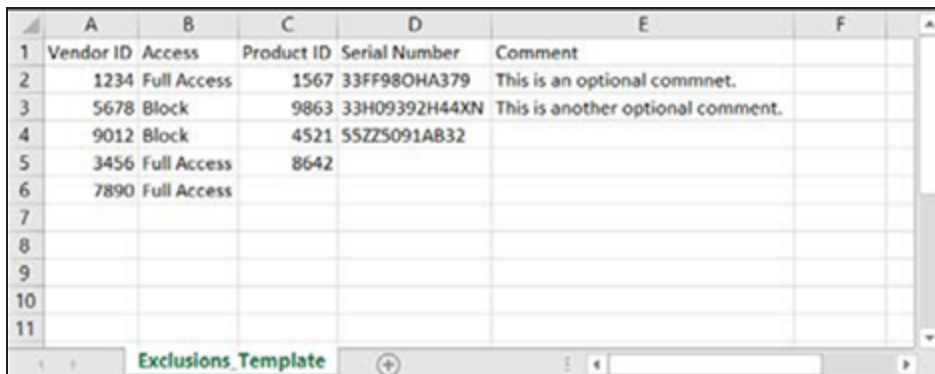
The maximum number of exclusions per policy is 5,000. On the Device Control tab in a policy, if the External Storage Exclusion List contains 5,000 entries, the Add Device button is disabled.

The CSV file format requirements are:

- Only CSV files are accepted.
- The header information is required in the CSV file. The import function will ignore the first line of the CSV file. If an exclusion is the first line in the import file, it will not be imported.
- Vendor ID and Access information are required for each exclusion.
- Optional information includes Product ID, Serial Number, and Comment.
- The Access column requires either Full Access or Block as the value, and only accepts

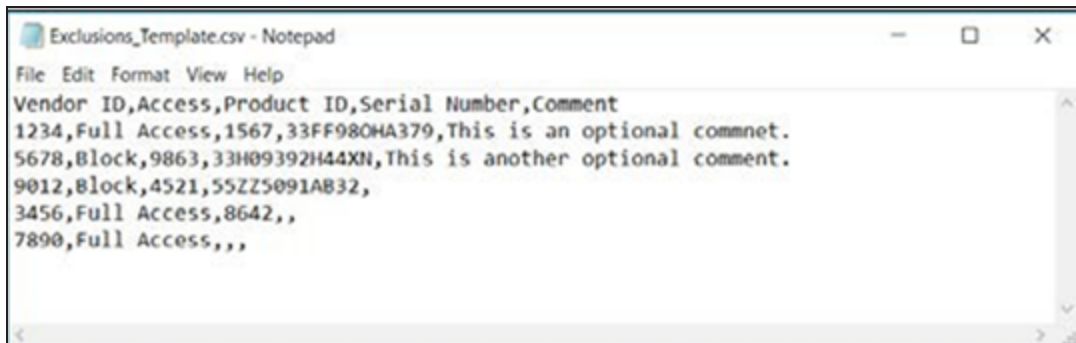
the values in English.

- The Comments column does not support commas (,).
- The maximum number of exclusions per CSV file is 500. If the import file contains more than 500 exclusions, an error message will display after you click the Upload button
- The maximum number of exceptions per policy is 5,000. A warning message should display if this number is exceeded.
- Non-English users who download the template and choose to edit it with Microsoft Excel may need to Import the file, setting options to UTF-8 and Comma Separated. Just opening the file may show unrecognizable characters.



	A	B	C	D	E	F
1	Vendor ID	Access	Product ID	Serial Number	Comment	
2	1234	Full Access	1567	33FF980HA379	This is an optional commnet.	
3	5678	Block	9863	33H09392H44XN	This is another optional comment.	
4	9012	Block	4521	55ZZ5091A832		
5	3456	Full Access	8642			
6	7890	Full Access				
7						
8						
9						
10						
11						

Figure 16: Bulk Import example using a spreadsheet



```
Exclusions_Template.csv - Notepad
File Edit Format View Help
Vendor ID,Access,Product ID,Serial Number,Comment
1234,Full Access,1567,33FF980HA379,This is an optional commnet.
5678,Block,9863,33H09392H44XN,This is another optional comment.
9012,Block,4521,55ZZ5091A832,
3456,Full Access,8642,,
7890,Full Access,,,
```

Figure 17: Bulk Import example using a text editor

Apply a Policy to a Device

Once a policy is created, it can be applied to a device. A policy contains the configuration settings the agent needs to protect the device the way you want to protect it. For example: You may want to enable Watch for New Files on your users workstations but not on your file servers. You control this by creating different policies for your workstations and files servers, and making sure you apply the right policy to the right device.

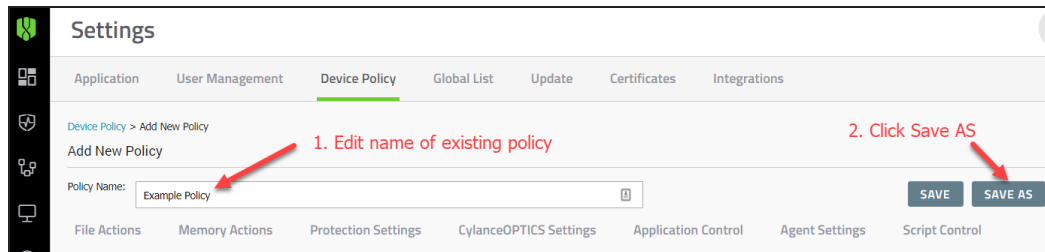
Applying a policy to a device takes effect as soon as the Agent receives the new or updated policy (the policy must be saved, and the policy must be assigned to the device). Policy changes do not require the endpoint to reboot for the update to take effect.

Clone a Device Policy

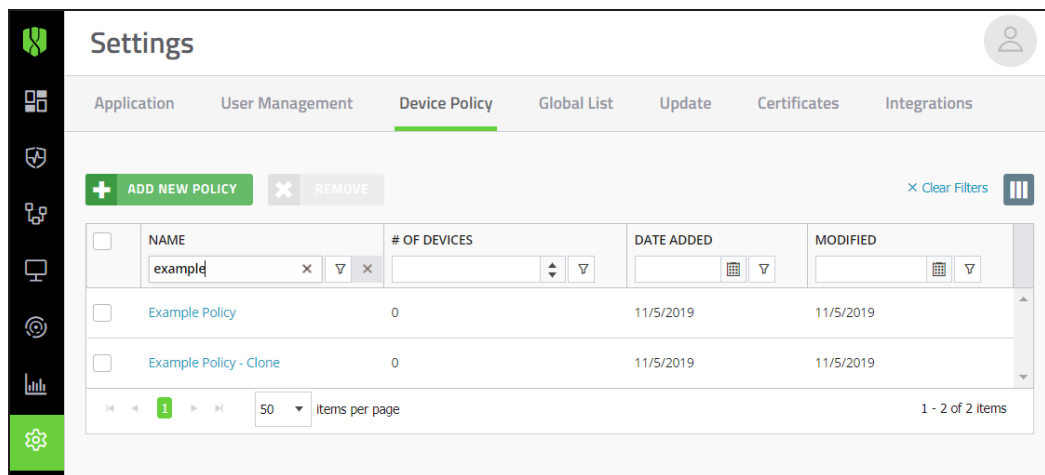
At times, you may want to clone an existing device policy to test a change to the policy on a small set of devices before rolling that change out to production.

To clone a device policy:

1. In the Console, select **Settings > Device Policy**.
2. Select the name of the device policy you want to clone. The Edit Policy Details page displays.
3. In the Policy Name field, enter the name for the clone, then click **Save As**. A message stating that the device policy was successfully created appears at the top of the page before returning you to the Device Policy page.



4. Verify that both device policies display in the list:



Now, you can edit the cloned policy to test changes.

Zones

A Zone is a way to organize and manage devices. For example, you may want to split your devices up based on geography or function. If there is a group of mission-critical devices, you can group those devices together and assign high priority to the Zone. Additionally, policies are applied at the Zone level, so you can group devices together in a Zone based on the policy that is applied to those devices.

An organization has a default zone (Unzoned) that only Administrators and users with permissions can access. New devices are assigned to Unzoned, unless there are Zone Rules that automatically assign devices to Zones.

Zone Managers and Users can be assigned to Zones, allowing them to view devices in those Zones. If a Zone Manager or User is responsible for a device with CylancePROTECT, make sure that device is in a zone to which they have access. At least one Zone must be created to allow anyone with a Zone Manager or User role to view it.

A device can belong to multiple Zones, but only one policy can be applied to a device. Allowing multiple Zones provides some flexibility in how devices are grouped. Restricting a device to a single policy eliminates conflicting features (for example, blocking a file when it should be *Allowed* for that device).

Devices existing in multiple zones could occur because:

- The device is manually added to multiple Zones
- The device complies with the rules of more than one Zone
- The device already resides in one Zone and then complies with rules of another Zone

For recommended ways to use Zones, refer to ["Zone Management Best Practices" on the next page](#).

Tip: Clicking the "select all" check box at the top of the list selects all entries on the displayed page. Entries on other pages in the list will not be selected.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

About Zone Priority

Zones can be assigned different priority levels (Low, Normal, or High) that classify the significance or criticality of the devices in that Zone. In several areas of the dashboard, devices are displayed by priority to help identify which devices need to be addressed immediately.

The priority can be set when a Zone is created or edit the Zone's to change the priority value.

Add a Zone

1. Click **Zones**
2. Click **Add New Zone**.
3. Enter a Zone Name, select a Policy, and select a Value. A Zone must have an associated Policy. The Value is the Priority for the zone.
4. Click **Save**.

Remove a Zone

1. Click **Zones**.
2. Select the check boxes for the Zones to remove.
3. Click **Remove**.
4. Click **Yes** at the message asking for confirmation of the selected Zone removal.

Zone Management Best Practices

Zones are best thought of as tags, where any device can belong to multiple Zones (or have multiple tags). While there are no restrictions on the number of Zones you can create, best practices identifies three different Zone memberships between testing, policy, and user-role granularity within the organization.

These three Zones consist of:

- Update Management
- Policy Management
- Role-Based Access Management

Zone Organization for Update Management

One common usage of Zones is to help manage Agent Updates. CylancePROTECT supports the latest Agent version and the previous version. This enables the enterprise to support change freeze windows, and do thorough testing of new Agent versions.

There are three suggested Zone types used to direct and specify the Agent testing and production phases:

- **Update Zone — Test Group:** These Zones should have test devices that properly represent devices (and software used on those devices) in the organization. This allows testing of the latest Agent and ensures deploying this Agent to the Production devices

does not interfere with business processes.

- **Update Zone — Pilot Group:** This Zone can be used as either a secondary Test Zone or as a secondary Production Zone. As a secondary Test Zone, this would allow testing new Agents on a larger group of devices before rollout to Production. As a secondary Production Zone, this would allow two different Agent versions – but then you must manage two different Production Zones.
- **Update Zone — Production:** Most devices should be in Zones assigned to Production.

Note: For updating the Agent to the Production Zone, see ["Agent Update" on page 112](#).

Add a Test or Pilot Zone

1. Select **Settings > Update**.
2. For Test or Pilot zones,
 - a. Click **Select Test Zones** or **Select Pilot Zones**.
 - b. Click a **Zone**.

If the Production Zone is set to **Auto-Update**, the Test and Pilot Zones are not available. Change Auto-Update in the Production Zone to something else to enable the Test and Pilot Zones.

3. Click **Please Select Version**.
4. Select an Agent version to apply to the Test or Pilot Zone.
5. Click **Apply**.

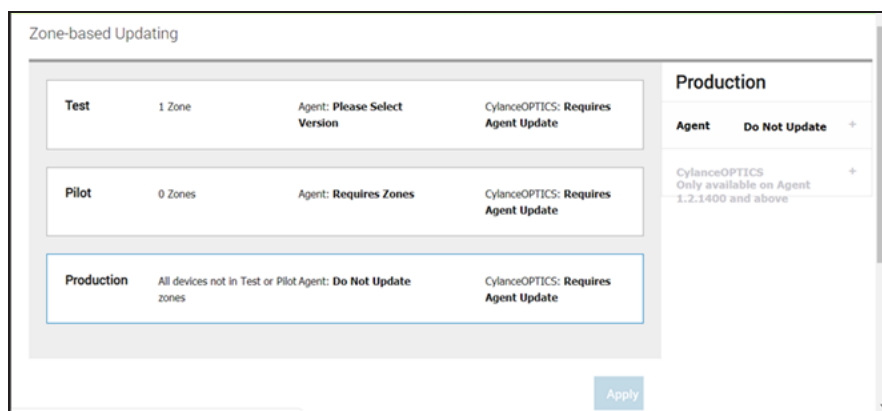


Figure 18: Zone-based Updating

Zone Organization for Policy Management

Another set of Zones to create helps apply different policies to different types of endpoints.

Consider the following examples:

- Policy Zone — Windows Workstations
- Policy Zone — macOS Workstations
- Policy Zone — Servers
- Policy Zone — Servers — Exclusions
- Policy Zone — Executives — High Protection

Cylance suggests applying a policy by default to all devices in this Policy Zone in each one of these Zones. Be careful not to put one device in multiple Policy Zones, as this can create a conflict over which policy is applied. Also remember that the Zone Rule engine can help automatically organize these hosts based on IP, Hostname, Operating System, and Domain.

Zone Organization for Role-Based Access Management

Role-based access is used to limit a console user's access to a subset of devices they are responsible for managing. This might include separation by IP range, host names, operating system, or domain. Consider groupings by geographical location, type, or both.

Administrators can view everything in the organization's console. Zone Managers and Users can only view data from the zones to which they are assigned. This allows access based on the role (Administrator, Zone Manager, or User) assigned to the user.

Example:

- RBAC Zone — Desktops — Europe
- RBAC Zone — Servers — Asia
- RBAC Zone — Red Carpet (Executives)

In the example above, you could assign a Zone Manager to *RBAC Zone— Desktops — Europe* to give access to devices within that Zone only. If the Zone Manager tried to view the other Zones, an error message stating they do not have permission to view it would be received. While a device could be in multiple Zones, and the Zone Manager would be able to view that device, if they tried to view the other Zones the device is associated with, they would not be allowed to, and would see the error message.

In other parts of the Console, such as the dashboard, the Zone Manager for *RBAC Zone — Desktops — Europe* would also be limited to threats and other information related to the Zone or devices assigned to that Zone.

The same restrictions apply to Users assigned to a Zone.

Zone Properties

Zone properties can be edited, as needed.

Edit Zone Properties

1. Click **Zones**.
2. Click a Zone from the *Zones List*.
3. Enter a new name in the **Name** field to change the Zone Name.
4. Select a different policy from the **Policy** drop-down list to change the policy.
5. Under Value, select a **Low**, **Normal** or **High** priority.
6. Click **Save**.

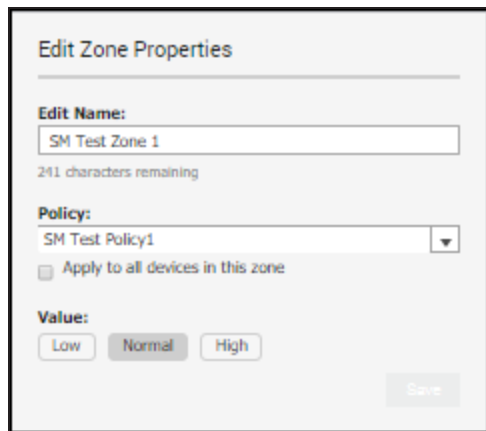


Figure 19: Change Zone Properties

Zone Rules

Devices can be automatically assigned to a Zone based on certain criteria. This automation is beneficial when adding numerous devices to Zones. When new devices are added that match a Zone Rule, those devices are automatically assigned to that zone. **If Apply now to all existing devices** is selected, all existing devices that match the rule are added to that Zone.

Note: Zone Rules automatically add devices to a Zone but cannot remove devices. Changing the device's IP address or hostname does not remove that device from a Zone. Devices must be removed manually from a Zone.

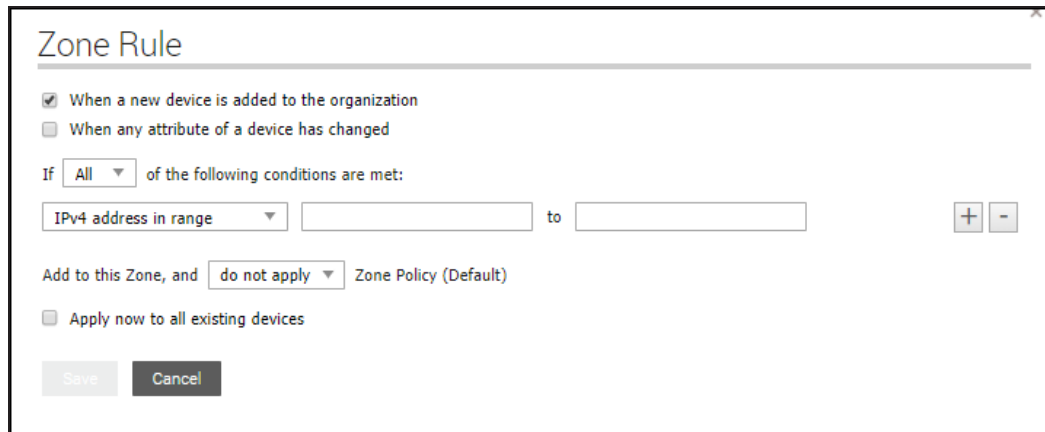
There is an option to apply the Zone Policy to devices that are added to the Zone as a result of matching the Zone Rule. This means the device's existing policy is replaced by the specified Zone Policy. Automatically applying a policy based on the Zone Rule should be used with care.

A device could be assigned to the wrong policy because the device matched a Zone Rule if not properly managed.

View the Device Details page in the Console to see which policy is applied to a device.

Add a Zone Rule

1. Click **Zones** and select a zone from the *Zones List*.
2. Click **Create Rule** under Zone Rule.
3. Specify the criteria for the selected zone. Click the plus sign to add more conditions. Click the minus sign to remove a condition.
4. Click **Save**.



The screenshot shows a 'Zone Rule' configuration window. It has a title bar with the text 'Zone Rule' and a close button. Below the title bar, there are two radio button options: 'When a new device is added to the organization' (which is selected) and 'When any attribute of a device has changed'. Below these is a label 'If' followed by a dropdown menu set to 'All' and the text 'of the following conditions are met:'. There is one condition listed: 'IPv4 address in range' with a dropdown arrow, followed by two empty text input boxes and the word 'to'. To the right of the input boxes are two buttons: a plus sign (+) and a minus sign (-). Below the condition is the text 'Add to this Zone, and' followed by a dropdown menu set to 'do not apply' and the text 'Zone Policy (Default)'. At the bottom left, there is a checkbox labeled 'Apply now to all existing devices'. At the bottom center, there are two buttons: 'Save' and 'Cancel'.

Figure 20: Zone Rule

Zone Rule Criteria

- **When a new device is added to the organization:** Any new device added to the organization that matches the Zone Rule is added to the Zone.
- **When any attribute of a device has changed:** When attributes on an existing device change and then match the Zone Rule, that existing device is added to the Zone.
- **Following Conditions Met:**
 - All: All conditions in the Zone Rule must match to add the device.
 - Any: At least one condition listed in the Zone Rule must match to add the device.
- **Device Name:**
 - Starts with: Device names must start with this.
 - Contains: Device names must contain this string, but it can be anywhere within

the name.

- Ends with: Device names must end with this.
- Does Not Start with: Device names must not start with this.
- Does Not Contain: Device names must not contain this anywhere within the name.
- Does Not End with: Device names must not end with this.

■ **Distinguished Name:**

- Starts with: Distinguished name must start with this.
- Contains: Distinguished name must contain this string, but it can be anywhere within the name.
- Ends with: Distinguished name must end with this.
- Does Not Start with: Distinguished name must not start with this.
- Does Not Contain: Distinguished name must not contain this anywhere in the name.
- Does Not End with: Distinguished name must not end with this.

■ **Member Of (LDAP):**

- Is: Member Of information must match this string.
- Contains: Member Of information must contain this string.
- Is Not: Member Of information must not match this string.
- Does Not Contain: Member Of information must not contain this string.

■ **Domain Name:**

- Starts with: Domain name must start with this.
- Contains: Domain name must contain this string, but it can be anywhere within the name.
- Ends with: Domain name must end with this.
- Does Not Start with: Domain name must not start with this.
- Does Not Contain: Domain name must not contain this anywhere within the name.
- Does Not End with: Domain name must not end with this.

■ **IPv4 Address in Range:** Enter an IPv4 address range.

- **Operating System:**

- Is: Operating system must be the selected system.
- Is Not: Operating system must not be the selected system. For example, if the only Zone Rule states that the operating system must not be Windows 8, then all operating systems, including non-Windows devices, are added to this Zone.

- **Zone Policy Apply:**

- Do Not Apply: Do not apply the Zone Policy as devices are added to the Zone.
- Apply: Apply the Zone Policy as devices are added to the Zone.

WARNING: Automatically applying a Zone Policy might negatively impact some of the devices on the network. Automatically apply the Zone Policy *only* if certain that the Zone Rule will *only* find devices that *must* have this particular Zone Policy.

- **Apply Now to All Existing Devices:** Applies the Zone Rule to all devices in the organization. This does not apply the Zone Policy.

About Distinguished Names (DN)

Some things to know about Distinguished Names (DN) when using them in Zone Rules:

- Wildcards are not allowed, but the "Contains" condition accomplishes similar results.
- DN errors and exceptions related to the Agent are captured in the log files.
 - For more information about log files, see ["Agent Settings" on page 34](#).
- If the Agent finds DN information on the device, that information is automatically sent to the Console.
- When adding DN information, it must be properly formatted.
 - CN=JDoe,OU=Sales,DC=Cylance,DC=COM
 - OU=Demo,OU=SEngineering,OU=Sales

Zones Device List

The *Zones Device List* displays all devices assigned to this Zone. Devices can belong to multiple Zones. Use **Export** to download a CSV file with information for all devices on the *Zones Device List*.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Zone Managers and Users can install the Agent on a device, but do not have access to the Default zone (Unzoned), and therefore cannot assign the new device to zones.

Add Devices to a Zone

1. Click **Zones**.
2. Click a zone from the *Zones List*. The current devices in that Zone display in the *Zones Device List*, at the bottom of the page.
3. Click **Add Devices to Zone**. A list of devices displays in the Add Device to Zone dialog box.
4. Select each device to add to the Zone and click **Save**. Optionally, select **Apply zone policy to selected devices**. Adding a device to a Zone does not automatically apply the Zone Policy because a Zone might be used to organize devices, not manage the policy for those devices.

Remove a Device from the Current Zone

Zone Managers and Users can install the Agent on a device, but do not have access to the Default zone (Unzoned), and therefore cannot remove a device from a zone.

1. Click **Zones**.
2. Click a zone from the *Zones List*. The current devices in that Zone display in the *Zones Device List*, at the bottom of the page.
3. Click **Remove Device from Zone**.
4. Click **Yes** to confirm the deletion. The device will be placed in Unzoned.

Copy Devices to another Zone

You can copy a device so it exists in an additional zone using this feature.

1. Login to the Console as an Administrator. Only Administrators can copy a device to a zone. Zone Managers and Users can install the Agent on a device, but do not have access to the Default zone (Unzoned), and therefore cannot copy devices to other zones.
2. Click **Zones**.
3. Click a zone from the *Zones List*. The current devices in that Zone display in the *Zones Device List*, at the bottom of the page.
4. Click **Copy Device**. A list of devices displays in the Copy Device to Zone dialog box.
5. Select each device to copy to the new Zone and click **Save**. Optionally, select **Apply zone policy to selected devices**. Adding a device to a Zone does not automatically

apply the Zone Policy because a Zone might be used to organize devices, not manage the policy for those devices.

AGENT INSTALLATION

Devices are added to the organization by installing the CylancePROTECT Agent on each endpoint. Once connected to the Cylance Console, apply policies (to manage identified threats) and organize devices based on organizational needs.

The CylancePROTECT Agent is designed to use a minimal amount of system resources. The Agent treats files or processes that execute as a priority because these events could be malicious. Files that are simply on disk (in storage but not executing) take a lower priority because while these could be malicious, these do not pose an immediate threat.

Per Zone Based Updates, the production group you set, controls which version of the installer you will be able to download.

- If you set your production to *Do Not Update* or *Auto Update*, you will receive the latest available installer version according to the phase you are assigned
- If you set your production to a specific version, you will receive that version of the installer under **Settings > Applications**.
- If a Zone Rule is set up, devices can be automatically assigned to a Zone if the device matches the Zone Rule criteria.

Download the Install File

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Install the Agent from the Application Page

1. Select **Settings > Application**.
2. Copy the **Installation Token**.
 - The Installation Token is a randomly generated string of characters that enables the Agent to report to its assigned account on the Console.
 - Use the Installation Token to install the Agent on endpoints in your environment. The Installation Token is required during installation, either in the installation wizard or as an installation parameter setting.
 - The Installation Token is not unique to each endpoint.

Note: Regenerating or deleting the Installation Token should only be used to prevent installation of new Agents with the existing token. All Agents installed using the token

prior to regenerating or deleting it will continue to communicate with the Console.

3. Beside CylancePROTECT, click the drop-down list beside the OS you want to install, then click the file type to download the installer.

- **For Windows**, it is recommended to use the MSI file to install the Agent. The MSI file size is smaller than the EXE file. The EXE contains both the x86 and x64 install files, while the MSI contains either the x86 or the x64 install file.

For information about the PROTECT + OPTICS install, see ["CylancePROTECT + CylanceOPTICS Windows Agent " on page 73](#) for download information and requirements.

- **For macOS**, it is recommended to use the PKG file for installation of the Agent. The DMG file is simply a disk image of the PKG file, and is available for scenarios where a disk image must be mounted for installation.

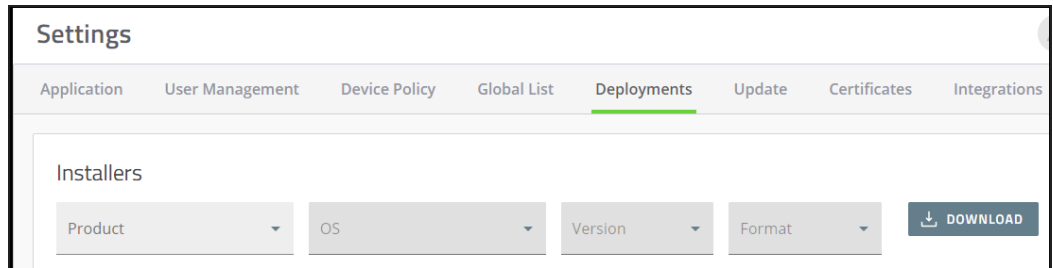
- **For Linux**, you can also download the agent UI, which is a separate file.

Note: The agent UI is not available for Amazon Linux.

Install the Agent from the Deployments Page

You do not need to update any custom roles for users to see the Deployments page. Any custom role that has the Installer Download checkbox selected under Application on the Edit Role dialog will have access to the download the installer from the Deployments page.

1. Select **Settings > Deployments**.



2. Under Installers, click the product you want to download under **Product**.
3. Click a supported operating system for the product under **OS**.
4. Click the version of the Agent to download under **Version**.
5. Click the file type to download under **Format**.
 - **For Windows**, it is recommended to use the MSI file to install the Agent. The MSI file size is smaller than the EXE file. The EXE contains both the x86 and x64 install files, while the MSI contains either the x86 or the x64 install file.

For information about the PROTECT + OPTICS install, see ["CylancePROTECT + CylanceOPTICS Windows Agent " on page 73](#) for download information and requirements.

- **For macOS**, it is recommended to use the PKG file for installation of the Agent. The DMG file is simply a disk image of the PKG file, and is available for scenarios where a disk image must be mounted for installation.
- **For Linux**, you can also download the agent UI, which is a separate file.
Note: The agent UI is not available for Amazon Linux.

6. Click **Download**. For installation information for each OS, review the following sections:

- ["Windows Agent" below](#)
- ["CylancePROTECT + CylanceOPTICS Windows Agent " on page 73](#)
- ["macOS Agent" on page 83](#)
- ["Linux Agent" on page 92](#)

7. Copy the **Installation Token** from the **Settings > Application** page.

- The Installation Token is a randomly generated string of characters that enables the Agent to report to its assigned account on the Console.
- Use the Installation Token to install the Agent on endpoints in your environment. The Installation Token is required during installation, either in the installation wizard or as an installation parameter setting.
- The Installation Token is not unique to each endpoint.

Note: Regenerating or deleting the Installation Token should only be used to prevent installation of new Agents with the existing token. All Agents installed using the token prior to regenerating or deleting it will continue to communicate with the Console.

Windows Agent

System Requirements

BlackBerry Cylance recommends that endpoint hardware (CPU, GPU, and so forth) meets or exceeds the recommended requirements of the target operating system. Exceptions are noted below (RAM, available hard drive space, and additional software requirements).

Supported Microsoft Windows Operating Systems

The device can be a physical or virtual machine.

OS	32-bit	64-bit	Notes
Windows XP SP3	X	X	KB 968730* and KB 2868626 hotfix must be installed.** *** The trusted root certificates listed in KB 293781 must be installed.
Windows Vista	X	X	The trusted root certificates listed in KB 293781 must be installed.
Windows 7	X	X	KB4054518 must be installed on Windows 7 (32-bit and 64-bit) and Windows 7 Embedded (32-bit and 64-bit) systems that use Agent 1494 or Agent 1550 and higher. For more information, read the KB article here . *** The trusted root certificates listed in KB 293781 must be installed. Support includes Windows Embedded Standard 7 and Embedded POSReady 7. Windows POSReady 7 requires Agent 1450 or higher.
Windows 8 and 8.1	X	X	Windows 8 Embedded requires Agent 1480 or higher. Windows RT is not supported.
Windows 10	X	X	Supports Enterprise, Pro, and Home editions Agent 1310 or higher. Windows 10 Anniversary Update (v1607) - Agent 1400 or higher. <ul style="list-style-type: none"> Microsoft Windows 10 Device Guard and Credential Guard are supported with Agent version 1410 or higher. Microsoft has also introduced a version of Windows Subsystem for Linux (WSL) in the Windows 10 Anniversary Update. WSL lets users run a bash shell on Ubuntu on Windows and has been received very positively by the developer community. WSL is disabled by default and Microsoft is likely to introduce more features before it becomes generally available. BlackBerry Cylance is following these updates and will introduce necessary controls for WSL when it becomes mainstream. Until then, BlackBerry Cylance recommends disabling this feature. Windows 10 Creators Update (v1703) - Agent 1440 or higher. <ul style="list-style-type: none"> Note: Windows 10 Creators Update has the same known issues as the Windows 10 Anniversary Update. Windows 10 Fall Creators Update (v1709 - Redstone 3) - Agent 1440 or higher.

OS	32-bit	64-bit	Notes
			<ul style="list-style-type: none"> ■ Agent 1480 added the detection of Microsoft OneDrive files. Note: There is one known issue with OneDrive files changing status from "Online-only file" to "Locally available file." ■ Enabling Windows Defender Device Guard Code Integrity will cause Modern Apps to fail with error 0xC000047E when Memory Protection or Script Control is enabled. This issue was resolved with the release of CylancePROTECT 1480. Please read: Memory Protection: Conflict with Modern Apps and Device Guard Code Integrity. ■ Note: Windows 10 Fall Creators Update has the same known issues as the Windows 10 Anniversary Update. <p>Windows 10 Enterprise 2016 LTSC (Long Term Servicing Branch) - Agent 1460 or higher.</p> <p>Windows 10 April 2018 Update (v1803) - Agent 1490 or higher.</p> <p>Windows 10 "Redstone 5" October 2018 Update (v1809) - Agent 1510 or higher.</p> <ul style="list-style-type: none"> ■ Case sensitive directories are not supported. ■ Note: Unified Write Filter (UWF) is not supported for Windows 10 at this time. The UWF is an optional feature within Windows OS. To ensure you do not experience a conflict, make sure that the UWF is disabled before installing the agent. <p>Windows 10 Enterprise 2019 LTSC - Agent 1510 or higher.</p> <p>Windows 10 "Redstone 6" May 2019 Update (v1903) - Agent 1530 or higher.</p> <ul style="list-style-type: none"> ■ Case sensitive file systems are not supported. <p>Windows 10 "19H2" November 2019 Update (v1909) - Agent 1540 or higher.</p> <ul style="list-style-type: none"> ■ Case sensitive file systems are not supported. <p>Windows 10 2004 "20H1" May 2020 update - Agent 1560 or higher.</p> <ul style="list-style-type: none"> ■ Case sensitive file systems are not supported.
Windows 10 IoT Enterprise	X	X	<p>Limited support is available in Agent 1510.</p> <ul style="list-style-type: none"> ■ Windows 10 IoT Core and Windows 10 IoT Core Services are not supported. ■ ARM is not supported. ■ The CylancePROTECT agent does not support the

OS	32-bit	64-bit	Notes
			Unified Write Filter (UWF) on Windows 10 IoT. The UWF is an optional feature within Windows OS. To ensure you do not experience a conflict, make sure that the UWF is disabled before installing the agent.
Windows Server 2003 SP2 and 2003 R2	X	X	KB 968730* and KB 2868626 hotfix must be installed.** *** The trusted root certificates listed in KB 293781 must be installed on Windows Server 2003 SP2.
Windows Server 2008 and 2008 R2	X (2008 only)	X	KB 3004394 hotfix must be installed.** *** The trusted root certificates listed in KB 293781 must be installed. KB4054518 must be installed on Windows Server 2008 R2 (64-bit) systems that use Agent 1494 or Agent 1550 and higher. For more information, read the KB article here . *** Windows Server 2008 and 2008 R2 Foundation editions require Agent 1540 or higher. Windows Server 2008 Server Core and 2008 R2 Server Core are not supported.
Windows Server 2012 and 2012 R2	–	X	Agent 1450 or higher. Supports Standard, Data Center, Essentials, Server Core, Embedded, and Foundation editions. <ul style="list-style-type: none"> Windows Server 2012 and 2012 R2 - Embedded edition requires Agent 1480 or higher. Windows Server 2012 and 2012 R2 Foundation editions require Agent 1540 or higher. Windows Server 2012 and 2012 R2 - Minimal Server Interface is not supported. Windows Storage Server 2012 is not supported.
Windows Server 2016	–	X	Agent 1410 or higher. Supports Standard, Data Center, Essentials, and Server Core editions. <ul style="list-style-type: none"> Windows Server Core 2016 requires Agent 1450 or higher Windows 2016 Nano Server is not supported. Windows Storage Server 2016 is not supported.
Windows Server 2019	–	X	Agent 1510 or higher. Supports Standard, Data Center, and Core editions. <ul style="list-style-type: none"> Windows Storage Server 2019 is not supported. Windows Server 2019 Data Center edition is

OS	32-bit	64-bit	Notes
			<p>supported on Agent 1530 or higher.</p> <ul style="list-style-type: none"> Windows Server 2019 Core edition is supported on Agent 1560 or higher. <p>Note: Windows Server 2019 Data Center does not support the following features:</p> <ul style="list-style-type: none"> Hyper-V Server Role is not supported with Shielded Virtual Machines Host Guardian Hyper-V Support Software-defined Networking Storage Spaces Direct
<p>* For Windows XP and Windows Server 2003, the hotfix in Microsoft's KB 968730 resolves a communication issue with the Console. These older operating systems can have issues obtaining a certificate if the certificate authority (CA) uses SHA256 encryption or higher. BlackBerry Cylance is required to use this level of encryption to meet Microsoft security requirements.</p> <p>** For additional information about errors when accessing secure Cylance hosts, click here.</p> <p>*** BlackBerry Cylance Support does not provide assistance in searching and implementation of any Microsoft related KB's or other 3rd party patches. For any issues with finding or implementing Microsoft related KB's, please reach out to Microsoft for assistance.</p> <p>Note: CylancePROTECT does not support scanning unhydrated files from Microsoft OneDrive.</p>			

Additional Windows Requirements

Type	Description
Processor	<ul style="list-style-type: none"> Requires at a minimum a two core processor. Supports the SSE2 Instruction set. Supports x86_64 instruction set. Does not support ARM instruction set.
RAM	<ul style="list-style-type: none"> 2 GB
Available Hard Drive Space	<ul style="list-style-type: none"> 600 MB <p>Note: Disk space usage can increase depending on features enabled, like setting the log level to Verbose.)</p>
Additional Software/ Requirement	<ul style="list-style-type: none"> NET Framework 3.5 (SP1) or higher (Note: .NET 4.0 must be the full version, not the .NET 4 Client Profile.) <p>Note: A fully functioning installation of .NET Framework that meets the above specifications is a requirement for the CylancePROTECT Agent to be installed and function as expected.</p> <ul style="list-style-type: none"> Internet Browser

Type	Description
	<ul style="list-style-type: none"> ■ Internet access to login, access the installer, and register the product ■ Local administrator rights to install the software ■ Root Certificates: <ul style="list-style-type: none"> • VeriSign Class 3 Public Primary Certification Authority - G5 • GeoTrust Global CA • thawte Primary Root CA • DigiCert Global Root C <p>Note: Devices missing any of the above root certificates may experience issues with the Cylance service not starting or the device being unable to communicate with the Console. Please see this article for more details about missing root certificates.</p>
Other	<ul style="list-style-type: none"> ■ TLS 1.2 is supported with Agent version 1420 or higher, and requires .NET Framework 4.5.2 or higher

Install the Agent — Windows

Ensure that all prerequisites are met prior to installing CylancePROTECT. See ["System Requirements" on page 61](#) for more information.

1. ["Download the Install File" on page 59](#).
2. Double-click CylancePROTECT.exe (or MSI).
3. Click **Install** at the CylancePROTECT setup window.
4. Enter the Installation Token and click **Next**
5. Optionally change the destination folder of CylancePROTECT.
6. Click **OK** to begin the installation.
7. Click **Finish** to complete the installation. Select the check box to launch CylancePROTECT.

The Agent does not require a reboot when it is installed.

Note: The Agent can run with Windows Defender installed on a device. This requires Agent version 1370 (and higher), a fresh installation of the Agent (not an upgrade), and Windows Defender must be running.

Windows Installation Parameters

The Agent can be installed interactively or non-interactively through GPO, Microsoft System Center Configuration Manager (commonly known as SCCM), MSIEXEC, etc. The MSIs can be customized with built-in parameters (shown below) or the parameters can be supplied from the command line.

Property	Value	Description
PIDKEY	<Installation Token>	Auto input the Installation Token
LAUNCHAPP	0 or 1	0: The system tray icon and the Start Menu folder is hidden at run-time. 1: The system tray icon and Start Menu folder is not hidden at run-time (default).
SELFPROTECTIONLEVEL	1 or 2	1: Only Local Administrators can make changes to the registry and services. 2: Only the System Administrator can make changes to the registry and services (default).
APPFOLDER	<Target Installation Folder>	Specifies the agent installation directory. The default location is: C:\Program Files\Cylance\Desktop
REGWSC	0 or 1	0: Indicates that CylancePROTECT is not registered with Windows as an anti-virus program. Allows CylancePROTECT and Windows Defender to run at the same time on the device. 1: Indicates that CylancePROTECT is registered with Windows as an antivirus program (default). Windows Defender: Windows Server 2016 and 2019 does not offer a Security Center function. The above commands will have no effect on Windows Server 2016 and 2019. If you wish to disable Windows Defender after installing CylancePROTECT on Windows Server 2016 and 2019, the following registry value can be set: <i>HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware</i> <i>REG_DWORD</i> <i>Value = 1</i> Note: The “Windows Defender” sub-key may not exist and may need to be created manually. For more information on how to manage Windows Defender via Group Policy, please read Use Group Policy settings to configure and manage Windows

Property	Value	Description
		Defender AV.
VENUEZONE	"Zone_Name"	<p>Requires Agent version 1380 or higher.</p> <ul style="list-style-type: none"> ■ Adds devices to a zone. ■ Replace Zone_Name with the name of an existing zone or a zone you want to create. ■ If the zone does not exist, the zone is created using the name provided. ■ If the device name or zone name contains a leading whitespace " Hello" or trailing whitespace "Hello ", Cylance removes the whitespace during device registration. <p>Note: Tabs, carriage returns, newlines, or other invisible characters are not permitted.</p> <ul style="list-style-type: none"> ■ Zone names cannot contain an equals sign, such as "Hello=World".
VDI	X	<p>Requires Agent version 1490 or higher.</p> <p>When installing CylancePROTECT on a Master Image, use the install parameter VDI=X where <X> is a "counter" for the total number of machines or images not connected to the domain (including the Master image) before creating a pool of workstations. The value for <X> determines when the Agent should start identifying the virtual machine utilizing VDI fingerprinting instead of the default Agent fingerprinting mechanism. For more information, see Appendix: VDI Best Practices.</p> <p>The VDI parameter utilizes a counter "X" and has a delayed effect, whereas the AD parameter is immediate upon installation.</p> <p>Note: The VDI fingerprinting for non-persistent virtual machines is designed for VMware products and works with Windows endpoints. For more information, see "Non-Persistent VDI Install Parameter" on page 218</p>
AD	1	<p>Requires Agent version 1520 or higher.</p> <p>Use the Active Directory (AD) parameter during initial installation on a master image that is domain connected. When installed on a domain connected master image, it will immediately utilize VDI fingerprinting on the master image and subsequently created pool of workstations.</p> <p>AD fingerprinting will take precedence over the VDI=<X> installation parameter. For more information, see Appendix: VDI Best Practices.</p>

Property	Value	Description
		Note: The VDI fingerprinting for non-persistent virtual machines is designed for VMware products and works with Windows endpoints. For more information, see "Non-Persistent VDI Install Parameter" on page 218
PROXY_SERVER	<ip_address>:<port_number>	Requires Agent version 1470 or higher. Specifies the IP address of the proxy server through which the Agent must communicate. Proxy server settings are added to the device's registry. Proxy server information will appear in the Agent log file. Example: PROXY_SERVER=123.45.67.89:1234
AWS	1	Requires Agent version 1500 or higher. Captures and includes the Amazon EC2 Instance ID to the Device Name field to help identify Amazon Cloud hosts. The Device Name is modified to include Hostname + Instance ID. Example: ABC-DE-123456789_i-0a1b2cd34efg56789 where the device name is ABC-DE-12345678 and the AWS EC2 ID is i-0a1b2cd34efg56789. Note: This feature is only for the Amazon EC2 Instance ID. This is not related to Amazon Linux.
PROTECTTEMPPATH	1	Change the location of the CylanceDesktopArchive and CylanceDesktopRemoteFile folder to the Cylance ProgramData folder. Requires Agent version 1480 or greater. For more information, please see our knowledge base article here .

Table 1: Installation Parameters for Windows

Example for PIDKEY, APPFOLDER, and LAUNCHAPP Parameters

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION
TOKEN> LAUNCHAPP=0 /L*v C:\temp\install.log
```

In the example above, the installation is silent and the installation log is saved to *C:\temp* (create the temp folder if it doesn't exist). When the Agent is running, both the system tray icon and the Start Menu Cylance folder are hidden. Additional information regarding different command line switches accepted by MSIEXEC can be found on [KB 227091](#).

Example for PIDKEY, VDI, and LAUNCHAPP Parameters

```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION
```

```
TOKEN> VDI=2 LAUNCHAPP=1
```

In the example above, the "2" for VDI is the total number of machines or images not connected to the domain (Master image + Additional/Parent image) before creating a pool of workstations.

Example for PIDKEY, AD, and LAUNCHAPP Parameters


```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION  
TOKEN> AD=1 LAUNCHAPP=1
```

In the example above, the AD parameter immediately utilizes VDI fingerprinting on the master image and subsequently created pool of workstations.

For examples on editing the MSI installation file for deployment through Group Policy, see the [Editing the MSI Installer using Orca](#) article.

Windows Installation Verification

Check the following files to verify successful Agent installation.

1. The program folder was created. Windows default: *C:\Program Files\Cylance\Desktop*
2. The CylancePROTECT icon is visible in the System Tray of the target device. 

This does not apply if parameter LAUNCHAPP=0 is used.

3. There is a CylancePROTECT folder under Start Menu\All Programs on the target device.
This does not apply if parameter LAUNCHAPP=0 is used.

4. The CylancePROTECT service was added and is running. There should be a CylancePROTECT service listed as running in the Windows Services panel of the target device.

5. The CylanceUI.exe process is running. There should be a CylanceUI.exe process listed under the Processes tab in the Windows Task Manager of the target device.

6. The device is reporting to the Console. Login to the console and click the Devices tab. The target device should show up and be listed in the online state.

Uninstall the Windows Agent

Before Uninstalling the Agent

Make sure all Agents have **Prevent Service Shutdown for Device** and **Application Control** disabled. This is done in a device policy. These features can prevent a successful Agent uninstall.

1. For the devices to uninstall the Agent from, assign these devices to a policy with no settings enabled.
 - a. Make sure the policy has no settings enabled, especially **Prevent Service Shutdown for Device** and **Application Control**.
 - b. Make sure these devices receive the new policy.

Another method is to delete the device from the Console and then restart the device (Application Control must be disabled). This should unregister the device and allow you to uninstall the Agent.

2. Follow the steps below to remove the Agent from the device.
3. After the Agent is removed from the device, the device can be removed from the Console.

Uninstalling the Agent on the device does not remove the device from the Console. You must manually remove the device from the Device tab in the Console after the Agent has been uninstalled.

To Uninstall the Windows Agent

To uninstall the Agent on a Windows system, use the Add/Remove Programs feature or use the Command Line. The Agent does not require a system reboot when it is uninstalled.

Note: The Agent uses msiexec to uninstall. There are some events, unrelated to the Agent, that require msiexec to reboot the system. If one of these events happens during a session when the Agent is uninstalled, then the system must be rebooted.

Note: If **Require Password to Uninstall Agent** (Settings > Application) is enabled, you will need to uninstall using the command line. For more information, see ["Password-Protected Uninstall" on page 114](#).

Uninstall Using Add / Remove Programs

1. Select **Start > Control Panel**.
2. Click **Uninstall a Program**. If you have Icons selected instead of Categories, click Programs and Features.
3. Select CylancePROTECT, then click **Uninstall**.

Uninstall Using the Command Line

1. Open the Command Prompt as an Administrator. Example: right-click **cmd.exe**, then select **Run As Administrator**.
2. Use the following commands, based on the installation package you used to install the Agent.

CylancePROTECT_x64.msi

- **Standard uninstall:** *msiexec /uninstall CylancePROTECT_x64.msi*
- **Windows Installer:** *msiexec /x CylancePROTECT_x64.msi*

CylancePROTECT_x86.msi

- **Standard uninstall:** *msiexec /uninstall CylancePROTECT_x86.msi*
- **Windows Installer:** *msiexec /x CylancePROTECT_x86.msi*

Product ID GUID:

- **Standard uninstall:** *msiexec /uninstall {2E64FC5C-9286-4A31-916B-0D8AE4B22954}*
- **Windows Installer:** *msiexec /x {2E64FC5C-9286-4A31-916B-0D8AE4B22954}*

The following commands are optional:

- **For quiet uninstall:** */quiet*
- **For quiet and hidden:** */qn*
- **For password protection uninstall:** *UNINSTALLKEY=<password>*
- **For auto quarantined files:** *QUARANTINEDISPOSETYPE=<0 or 1>*
 - 0: deletes all files and removes the q directory (default)
 - 1: restores all files
- **For uninstall log file:** */Lxv* <path>*
 - This creates a log file at the designated path (<path>), include the filename.
 - Example: *C:\Temp\Uninstall.log*

This creates a log file at the designated path (<path>). Include the filename. Example: *C:\Temp\Uninstall.log*

CylancePROTECTSetup.exe

- CylancePROTECT.Setup.exe /uninstall

The following commands are optional:

- **For quiet uninstall:** */quiet*
- **For Require Password to Uninstall Agent:**

UNINSTALLKEY="MyUninstallPassword"

- **For uninstall log file:** */! LOGFILEPATH*

This creates a log file at the designated path (<path>). Include the filename. Example: *C:\Temp\Uninstall.log*

- **For deletion of quarantine directory:**

QUARANTINEDISPOSETYPE=<value>

- 0: Deletes all files and removes the q directory (default)
- 1: Restores all files

Things to Know About Uninstall by Command Line

- If Device Control has been enabled at any time prior to uninstalling the Agent, Windows Installer will prompt for a reboot when uninstalling the Agent using Add/Remove Programs, or when using the command line with quiet, hidden, or passive commands. It is recommended to use the norestart command if the quiet, hidden, or passive commands are used.

CylancePROTECT + CylanceOPTICS Windows Agent

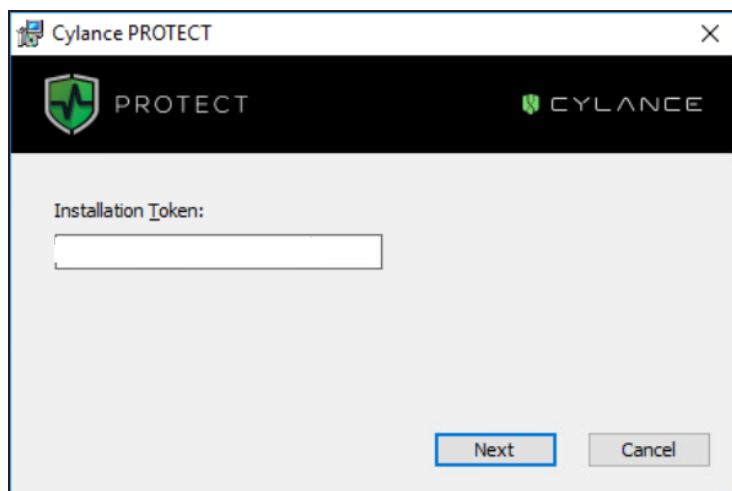
A Cylance unified setup installer is available to install CylancePROTECT and CylanceOPTICS agents on Microsoft Windows if both products have been purchased.

Note: The CylanceUnifiedSetup EXE and MSI installers are only available for new installs. For example, if you previously installed CylancePROTECT and now want to install CylanceOPTICS, you cannot use the exe or msi file to install CylanceOPTICS.

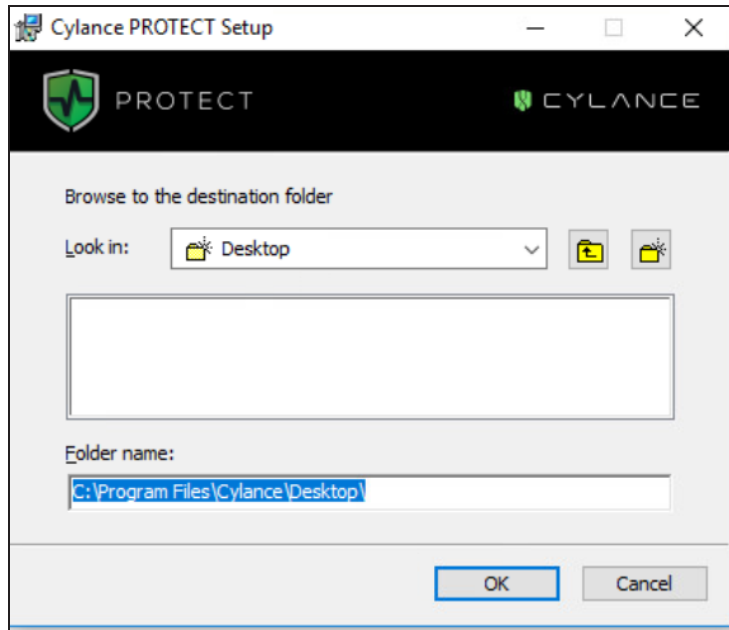
Install CylancePROTECT + CylanceOPTICS

Install CylancePROTECT + CylanceOPTICS from the EXE File

1. ["Download the Install File" on page 59.](#)
2. Double-click the CylanceUnifiedSetup.exe file from the download folder. The CylancePROTECT Setup dialog displays.
3. To install CylanceOPTICS with CylancePROTECT, click the **Install CylanceOPTICS** checkbox, then click **install**.
4. When prompted, paste the Installation Token into the dialog, then click **Next**.



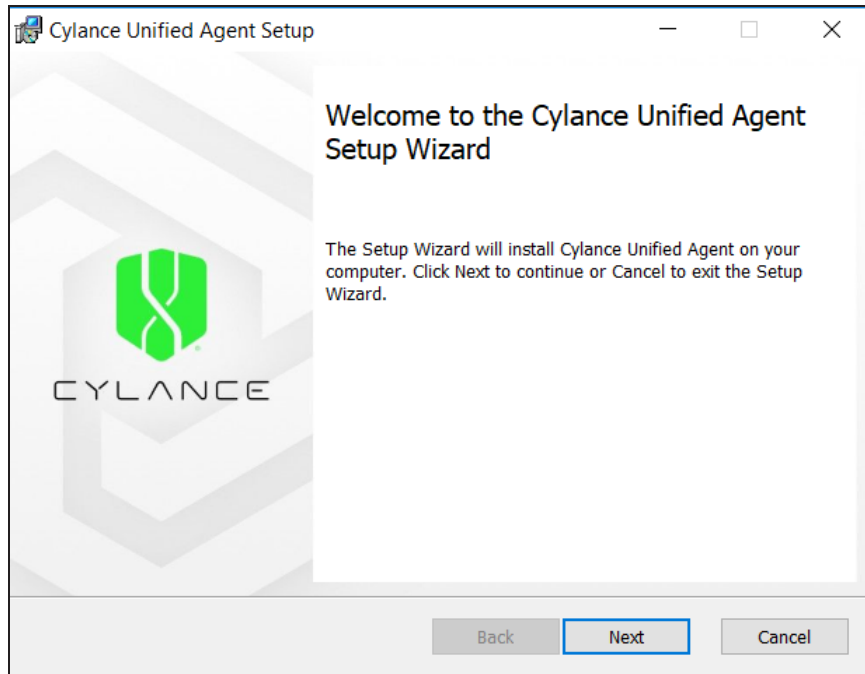
5. Select the folder where the agents will be installed, then click **OK**. By default:
 - CylancePROTECT is installed in C:\Program Files\Cylance\Desktop
 - CylanceOPTICS is installed in C:\Program Files\Cylance\Optics



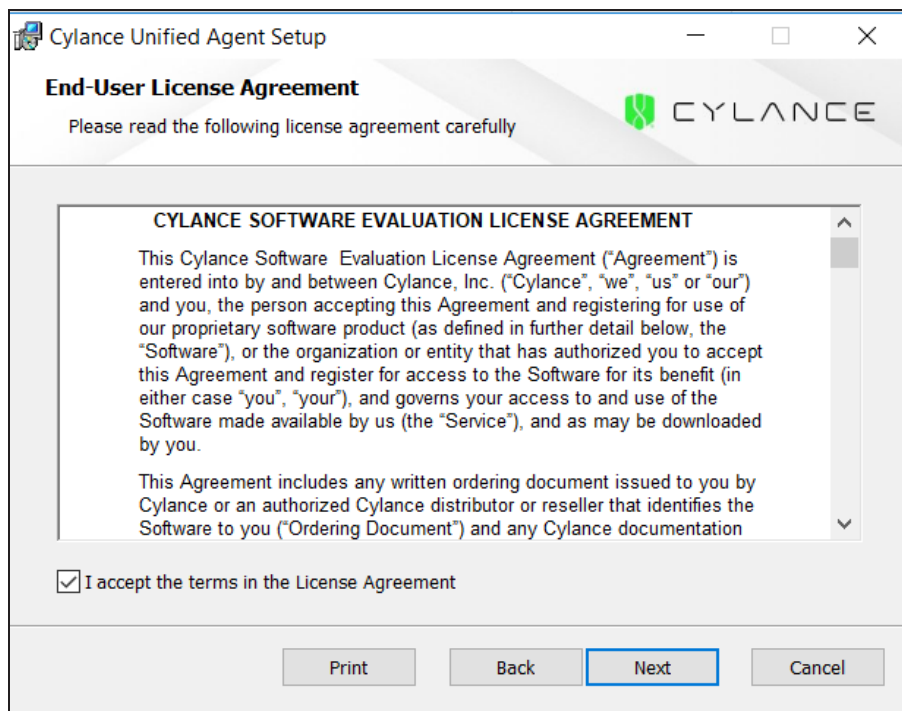
6. Click **Finish** on the Completed the CylancePROTECT Setup Wizard. A progress window indicates that CylanceOPTICS is being installed. When complete, a Successfully installed dialog displays.
7. Click **Close**.

Install CylancePROTECT + CylanceOPTICS from the MSI File

1. ["Download the Install File" on page 59.](#)
2. Double-click the CylanceUnifiedSetup.msi file from the download folder. The Cylance Unified Agent Setup dialog displays. Click **Next**.



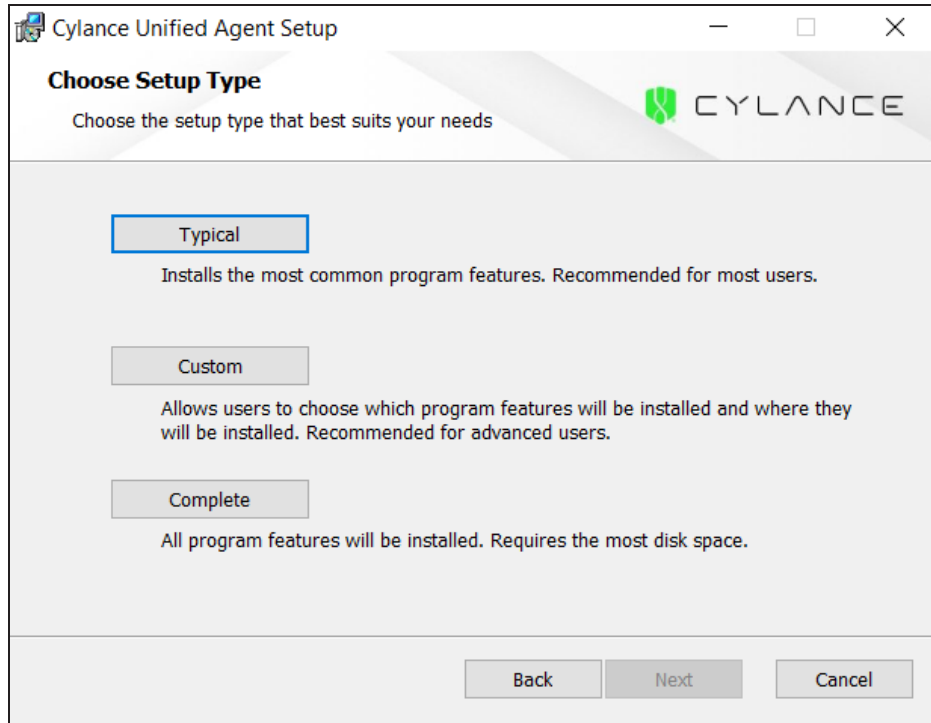
3. Click the checkbox to accept the terms in the License Agreement, then click **Next**.



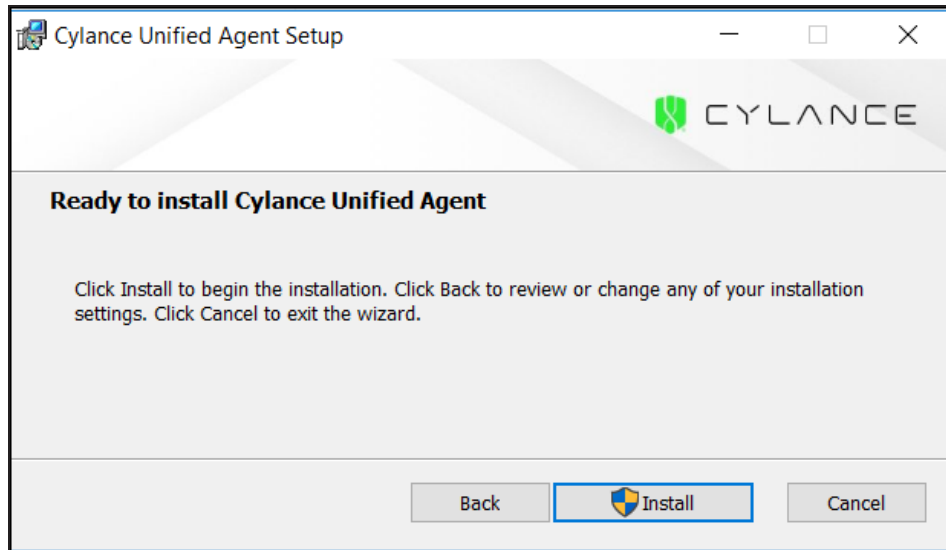
4. From the Choose Setup Type page, select one of the options:

- Typical
- Custom - **IMPORTANT:** If you click Custom, selecting “Feature will be installed when required” or “Entire feature will be unavailable” will cause the installation to return an error. Choosing any other option will install as expected.
- Complete

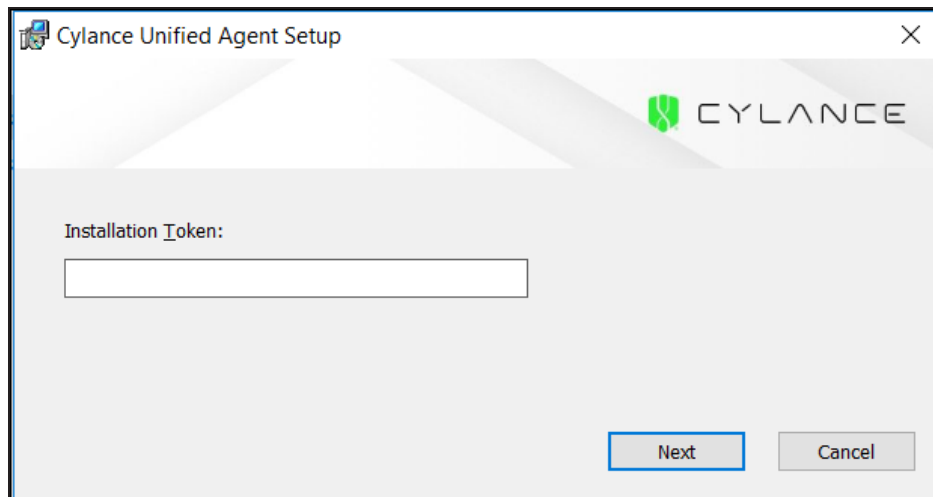
Note: At this time, Typical and Complete have the same functionality and will install CylancePROTECT + CylanceOPTICS.



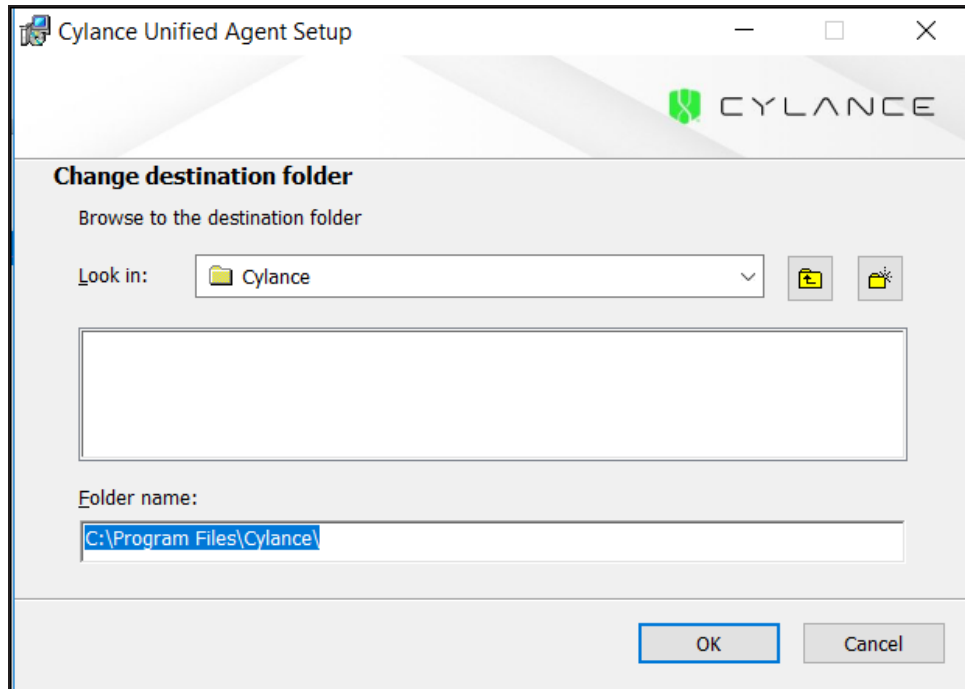
5. The Ready to Install page displays. Click **Install**.



6. When prompted, paste the Installation Token into the dialog, then click **Next**.



7. Select the folder where the agents will be installed then click **OK**. By default:
 - CylancePROTECT is installed in C:\Program Files\Cylance\Desktop
 - CylanceOPTICS is installed in C:\Program Files\Cylance\Optics



8. A progress window indicates that CylanceOPTICS is being installed. When complete, a Successfully installed dialog displays. Click **Finish**.

CylancePROTECT + CylanceOPTICS Installation Parameters

The CylancePROTECT Console contains a single package to install CylancePROTECT and CylanceOPTICS. With the Cylance unified setup installer, users can customize their installation and CylancePROTECT and CylanceOPTICS can be installed various ways such as through GPO or SCCM.

Note: Currently, the AD=1 and AWS parameters are not supported for the CylancePROTECT + CylanceOPTICS unified setup installer EXE file. If you wish to use these parameters, please use the unified setup installer MSI file.

Property	Value	Description
PIDKEY	<Installation Token>	Replace this value with the 24 character Installation Token from the Cylance Console's Settings > Application page to auto input the installation token during install. Example: PIDKEY=AB 1 cDe2fGHijkL3m4nOPQRSt
SELFPROTECTIONLEVEL	1 or 2	1: Only Local Administrators can make changes to the registry and services.

Property	Value	Description
		2: Only the System Administrator can make changes to the registry and services (default).
LAUNCHAPP	0 or 1	0: Hidden (The system tray icon and the Start Menu folder is hidden at run-time.) 1: Visible (The system tray icon and Start Menu folder is not hidden at run-time (default).)
INSTALLFOLDER	<Target Installation Folder>	Specifies the agent installation directory. Default location of CylancePROTECT Agent: C:\Program Files\Cylance\Desktop Default location of CylanceOPTICS Agent: C:\Program Files\Cylance\Optics
REGWSC	0 or 1	0: Indicates that CylancePROTECT is not registered with Windows as an anti-virus program. Allows CylancePROTECT and Windows Defender to run at the same time on the device. 1: Registers CylancePROTECT with Windows as an antivirus program (default). Windows Defender: Windows Server 2016 and 2019 does not offer a Security Center function. The above commands will have no effect on Windows Server 2016 and 2019. If you wish to disable Windows Defender after installing CylancePROTECT on Windows Server 2016 and 2019, the following registry value can be set: <i>HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware</i> <i>REG_DWORD</i> <i>Value = 1</i> Note: The “Windows Defender” sub-key may not exist and may need to be created manually. For more information on how to manage Windows Defender via Group Policy, please read Use Group Policy settings to configure and manage Windows Defender AV .
VENUEZONE	“Zone_Name”	Replace Zone_Name with the name of an existing zone or a zone you want to create. <ul style="list-style-type: none">■ If the zone does not exist, the zone is created using the name provided.■ The use of the number sign / hash character (#, U+0023) inside of a zone name will cause the install to fail due to a registry restriction, i.e. VENUEZONE="#zone_name".

Property	Value	Description
		<ul style="list-style-type: none"> ■ Tabs, Carriage Returns, Newlines, or any other invisible characters are not permitted, i.e., VENUZONE="My Cool Irltln Device"
INSTALLOPTICS	0 or 1	<p>0: Installs CylancePROTECT only on the endpoint (default).</p> <p>1: Installs both CylancePROTECT and CylanceOPTICS on the endpoint.</p>
PROXY_SERVER	<ip_address>:<port_number>	<p>Specifies the IP address of the proxy server through which the Agent must communicate. Proxy server settings are added to the device's registry. Proxy server information will appear in the Agent log file.</p> <p>Example: PROXY_SERVER=123.45.67.89:1234</p>
VDI	X	<p>When installing CylancePROTECT on a Master Image, use the install parameter VDI=X where <X> is a "counter" for the total number of machines or images not connected to the domain (including the Master image) before creating a pool of workstations. The value for <X> determines when the Agent should start identifying the virtual machine utilizing VDI fingerprinting instead of the default Agent fingerprinting mechanism. For more information, see Appendix: VDI Best Practices.</p> <p>Note: The VDI fingerprinting for non-persistent virtual machines is designed for VMware products and works with Windows endpoints. For more information, see "Non-Persistent VDI Install Parameter" on page 218</p>

Example Quiet Install of CylancePROTECT + CylanceOPTICS Executable

```
CylanceUnifiedSetup.exe /quiet PIDKEY=<YOURINSTALLTOKEN> LAUNCHAPP=1
INSTALLOPTICS=1
```

Example Quiet Install of CylancePROTECT + CylanceOPTICS MSI

```
CylanceUnifiedSetup_x64.msi /quiet PIDKEY=<YOURINSTALLTOKEN>
LAUNCHAPP=1 INSTALLOPTICS=1
```

Note: If the Cylance unified setup installer is used to install the application, and an uninstall password is setup in the console, you must use the uninstaller commands in ["Uninstall CylancePROTECT + CylanceOPTICS" on the next page](#).

Uninstall CylancePROTECT + CylanceOPTICS

Before attempting to uninstall the Agent:

- If **Require Password to Uninstall Agent** (Settings > Application) is enabled, you will need to uninstall using the command line. Make sure you have the password to uninstall and if the password contains an "&" character, the password must be the final parameter or errors may occur (for example: CylanceUnifiedSetup_x64.msi /uninstall /quiet UNINSTALLKEY=asdf&).
- If **Prevent Service Shutdown from Device** (Settings > Device Policy > Protection Settings) is enabled, either disable it in the policy or apply a different policy to the devices from which you want to uninstall the Agent. Another method is to delete the device from the Console and then restart the device (Application Control must be disabled). This should unregister the device and allow you to uninstall the Agent.

Uninstall Using Add / Remove Programs

1. Select **Start > Control Panel**.
2. Click **Uninstall a Program**. If you have Icons selected instead of Categories, click Programs and Features.
3. If you installed both CylancePROTECT and CylanceOPTICS, select **CylancePROTECT with CylanceOPTICS**, then click **Uninstall**. This uninstalls both products.

Uninstall Using the Command Line

You can use the command line for an unattended uninstall of the product(s) that were installed.

Examples

```
CylanceUnifiedSetup.exe /quiet /uninstall
```

or

```
CylanceUnifiedSetup_x64.msi /quiet /uninstall
```

Note: If you installed CylancePROTECT only using the CylanceUnifiedSetup .exe or .msi file, it will be uninstalled using the /quiet /uninstall command as shown in the examples above. If you installed CylancePROTECT + CylanceOPTICS using the CylanceUnifiedSetup .exe or .msi file, both agents will be uninstalled using the /quiet /uninstall command as shown in the examples above. If you did not use the CylanceUnifiedSetup .exe or .msi file to install the agent(s), you cannot use the .exe or .msi file to uninstall the agent(s).

Password Protected Uninstall

Examples

```
CylanceUnifiedSetup.exe /quiet UNINSTALLKEY="MyUninstallPassword"  
/uninstall
```

or

```
CylanceUnifiedSetup_x64.msi /quiet UNINSTALLKEY="MyUninstallPassword"  
/uninstall
```

Note: If utilizing an uninstall password that contains a special character or symbol, ensure that there are quotations around the uninstall password string to prevent any syntax issues.

Uninstall Parameters

- UNINSTALLKEY="MyUninstallPassword"
 - If an uninstall password has been defined in the Console (**Settings > Application** page), the password will need to be provided during uninstall of the agent.
- QUARANTINEDISPOSETYPE
 - 0: Deletes all files and removes the q directory (default).
 - 1: Restores all files.

macOS Agent

System Requirements

BlackBerry Cylance recommends that endpoint hardware (CPU, GPU, and so forth) meets or exceeds the recommended requirements of the target operating system. Exceptions are noted below (RAM, available hard drive space, and additional software requirements).

Supported macOS Operating Systems

The device can be a physical or virtual machine.

OS	Notes
Mac OS X 10.9	Agent 1300 or higher.
Mac OS X 10.10	Agent 1300 or higher.

OS	Notes
Mac OS X 10.11	Agent 1310 or higher.
macOS Sierra (10.12)	Agent 1410 or higher.
macOS High Sierra (10.13)	Agent 1450 or higher.* **
macOS Mojave (10.14)	Agent 1510 or higher.* ** ***
macOS Catalina (10.15)	Agent 1550 or higher.* ***

*macOS High Sierra 10.13 or higher includes a new security feature that requires users to approve new third-party kernel extensions. Read this [Agent Installation - macOS High Sierra - Secure Kernel Extension Loading](#) article for more information.

**Prior to CylancePROTECT Agent version 1510, the CylancePROTECT Agent was a 32-bit binary for macOS. With the release of 1510, the CylancePROTECT Agent for macOS is a 64-bit binary. With the advent of macOS High Sierra (10.13.4), Apple began to notify users that 32-bit based applications are not optimized to be used on a macOS based machine. This requires additional steps for Agent 1500 or earlier installations, and displays a notification for macOS High Sierra 10.13.4 once; or every 30 days for macOS Mojave 10.14. Read the [macOS and 32-bit compatibility](#) article for more information.

***macOS Mojave introduced a security feature that allows third-party applications to access protected user data.

- **macOS Mojave version 10.14.x (recommended)** - If you are running macOS Mojave and have installed CylancePROTECT, it is recommended that you enable Full Disk Access on your macOS system. If Full Disk Access is not enabled, CylancePROTECT will be unable to process files secured by user data protection.
- **macOS Catalina version 10.15.x or higher (required)** - If you are running macOS Catalina or higher and have installed CylancePROTECT, it is required that you enable Full Disk Access on your macOS system. If Full Disk Access is not enabled, Cylance products will be unable to process files secured by user data protection. Starting with macOS Catalina (10.15.x), this now includes the user's Desktop, Downloads, and Documents folders.

Read the [macOS - Full Disk Access Requirements](#) article for more information.

Notes:

- Case Sensitive volume formats are not supported on Mac OS X or macOS at this time.
- Support for macOS 64-bit is available in Agent 1510 or higher.

Additional macOS Requirements

Type	Description
Processor	<ul style="list-style-type: none"> ■ Requires at a minimum a two core processor ■ Supports the SSE2 instruction set ■ Supports x86_64 instruction set

Type	Description
RAM	<ul style="list-style-type: none"> ■ 2 GB
Available Hard Drive Space	<ul style="list-style-type: none"> ■ 600 MB <p>Note: Disk space usage can increase depending on features enabled, like setting the log level to Verbose.</p>
Additional Requirements	<ul style="list-style-type: none"> ■ Internet Browser ■ Internet access to login, access the installer, and register the product ■ Local administrator rights to install the software ■ Root Certificates: <ul style="list-style-type: none"> • VeriSign Class 3 Public Primary Certification Authority - G5 • GeoTrust Global CA • thawte Primary Root CA • DigiCert Global Root <p>Note: Devices missing any of the above root certificates may experience issues with the Cylance service not starting or the device being unable to communicate with the Console. Please see this article for more details about missing root certificates.</p>
Other	<ul style="list-style-type: none"> ■ TLS 1.2 is supported with Agent 1450 or higher

Install the Agent — macOS

1. ["Download the Install File" on page 59.](#)
2. Double-click the CylancePROTECT.dmg (or .pkg) to mount the installer.
3. Double-click the Protect icon from the PROTECT user interface to begin the installation.
4. Click Continue to verify that the Operating System and Hardware meet the requirements.
5. Click **Continue** at the Introduction screen.
6. Enter or copy/paste the Installation Token provided by the Tenant. Click **Continue**. The Destination Folder step displays.

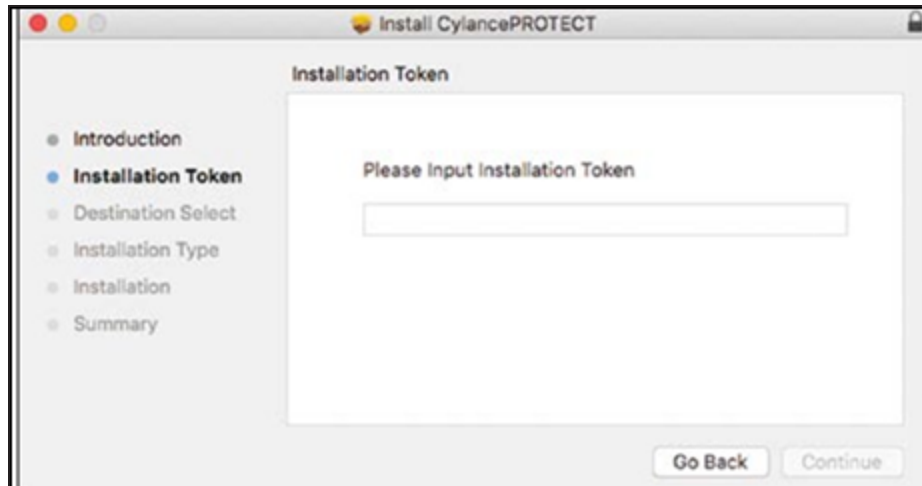
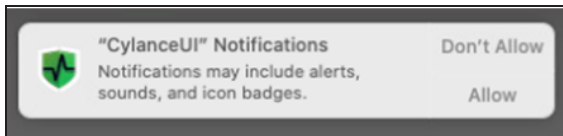


Figure 21: Installation Token Input Screen

7. Optionally change the installation location of CylancePROTECT.
Click **Install** to begin the installation.
8. Enter an administrator's Username and Password. Click **Install Software**.
9. Click **Close** at the Summary screen.
10. Click **OK**. When installation is done, the Completed step displays.
11. Click **Finish**.

Note: If you are installing CylancePROTECT on macOS Catalina, a notification prompts you to allow CylanceUI to display notifications. Click **Allow**.



Installation — System Management

The Agent can be installed directly on each system or through a system management software. Examples: GPO, SCCM, and MSIEXEC. When installing the Agent, Installation Parameters are provided to configure some installation settings.

Note: Ensure the target devices meet System Requirements and that you have the proper credentials for installing software.

Install the Agent from the Command Line

Install Without the Installation Token

```
sudo installer-pkg CylancePROTECT.pkg-target/
```

Install with the Installation Token

```
echo YOURINSTALLTOKEN >cyagent_install_token  
sudo installer -pkg CylancePROTECT.pkg-target/
```

Troubleshooting With the Install Token and Verbose Installer Logging

```
echo YOURINSTALLTOKEN >cyagent_install_token  
sudo installer -verboseR -dumplog -pkg CylancePROTECT.pkg -target /
```

Note: Review the following:

- Replace YOURINSTALLTOKEN in the echo line with the Installation Token on the Applications tab of the console.
- The echo command outputs a cyagent_install_token file, which is a text file with one installation option per line. This file must be in the same folder as the installation package, CylancePROTECT.pkg.
- For macOS Catalina - when installing the CylancePROTECT Agent using Terminal, a DYLD warning might display. This warning does not impact the installation. This warning is generated by the operating system, not by the CylancePROTECT installer.

Optional Installation Parameters

You can type the following in Terminal to create a file (cyagent_install_token) that the installer will use and apply the options you entered. Each parameter must be on its own line. This file must be in the same folder as the installation package.

The following is simply an example. You do not need to include all of the parameters in your file.

You can also create a file with a text editor that includes each parameter (on its own line). Just make sure the file is in the same folder as the installation package.

Example:

```

echo YOURINSTALLTOKEN > cyagent_install_token

echo SelfProtectionLevel=2 >> cyagent_install_token

echo VenueZone=zone_name >> cyagent_install_token

echo token LogLevel=2 >> cyagent_install_token

sudo installer -pkg CylancePROTECT.pkg-target /

```

macOS Installation Parameters

The CylancePROTECT Agent can be installed using command line options in the Terminal. The examples below use the PKG installer. For the DMG, simply change the file extension in the command.

Note: Ensure that the target endpoints meet system requirements and that the person installing the software has the proper credentials for installing software.

Property	Value	Description
InstallToken	Installation Token	Installation Token available in the Console (Settings > Application). This is required when installing the Agent.
NoCylanceUI		The Agent icon should not display on startup. The default is Visible.
SelfProtectionLevel	1 or 2	1: Only Local Administrators can make changes to the registry and services. 2: Only the System Administrator can make changes to the registry and services (default).
LogLevel	0, 1, 2, or 3	0: Error — Only error messages are logged. 1: Warning — Error and warning messages are logged. 2: Information (default) — Error, warning, and information messages are logged. This may provide some details during troubleshooting. 3: Verbose — All messages are logged. When troubleshooting, this is the recommended log level. However, verbose log file sizes can grow very large. BlackBerry Cylance recommends turning Verbose on during troubleshooting and then changing it back to Information when troubleshooting is complete.
VenueZone	“zone_name”	Introduced in Agent version 1380. <ul style="list-style-type: none"> ■ Adds devices to a zone. ■ If the zone does not exist, the zone is created using the name provided.

Property	Value	Description
		<ul style="list-style-type: none"> Replace zone_name with the name of an existing zone or a zone you want to create. If the device name or zone name contains a leading whitespace " Hello" or trailing whitespace "Hello ", Cylance removes the whitespace during device registration. <ul style="list-style-type: none"> Note: Tabs, carriage returns, newlines, or other invisible characters are not permitted. Zone names cannot contain an equals sign, such as "Hello=World".
ProxyServer	<IP_Address>:<Port_Number>	<p>Requires Agent version 1470 or higher.</p> <p>Proxy server settings are added to the device's registry. Proxy server information will appear in the Agent log file.</p> <p>Example: ProxyServer=123.45.67.89:1234</p>

Table 2: Installation Parameters for macOS

macOS High Sierra – Secure Kernel Extension Loading

macOS High Sierra (10.13) or higher includes a security feature that requires users to approve new third-party kernel extensions. This security feature only allows kernel extensions to load on a system that is already approved by the user. If an unapproved extension tries to load, the extension is blocked and displays a user alert.

If the Agent is installed without approving the extension, the Cylance icon displays a red dot. Clicking on the icon and selecting Show Details, displays the message “Driver Failed to Connect, Device Not Protected” at the bottom.

Note: This only affects new Agent installations on macOS High Sierra or higher. This will not affect Agents installed on macOS devices that were then upgraded to macOS High Sierra.

1. When installing the Agent on macOS High Sierra or higher for the first time, a user alert displays.



Figure 22: macOS User Alert

2. To approve the extension, click **Open Security Preferences**, or go to **System Preferences > Security & Privacy**.
3. Click **Allow**. Clicking the Allow button does not work over a Remote Desktop session. This is by design by Apple.

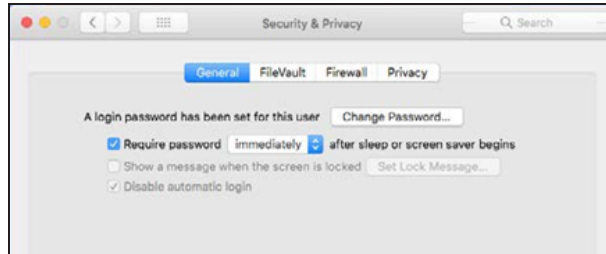


Figure 23: Allow the Agent to Install

Things To Know About Approving the Extension

- The Allow button will only be available for 30 minutes after installing the Agent. This is by design by Apple. To make it available again, do one of the following:
 - Uninstall and re-install the Agent.
 - Run the upgrade package to perform an in-place upgrade of the Agent. See the FAQ – Where can I download the latest upgrade package for CylancePROTECT article.
 - Open the Terminal and run: `sudo kextload /System/Library/Extensions/CyProtectDrvOSX.kext`

Note: Running this command results in an error message. This is expected behavior. Proceed to the next step.
- After performing one of the actions above:
 - Go to **System Preferences > Security & Privacy**.
 - Click **Allow**. If issues still persist after allowing the Agent extension, reboot the device.

Use Mobile Device Management

For environments that use Mobile Device Management (MDM), user interaction is not required to load properly signed kernel extensions if a valid MDM profile is installed on macOS 10.13.3 or lower. The CylancePROTECT macOS Agent installs a properly signed kernel extension.

Starting with macOS 10.13.4, User Approved Kernel Extension Loading is enabled on all devices, even those with an MDM profile. See Apple's configuration document. read the Kernel Extension Policy section to define **AllowedTeamIdentifiers**, and allow the Cylance TeamID **6ENJ69K633**.

For Deployments Without Mobile Device Management

User Approval Kernel Extension Loading without Mobile Device Management (MDM) can be done without requiring user approval.


- Use the `spctl kext-consent` command and the Cylance Team ID 6ENJ69K633 to perform a silent installation.

Example: `spctl kext-consent add 6ENJ69K633`

- The `spctl` command works in macOS Recover and NetBoot/NetInstall/NetRestore images. Reference the [Create a NetBoot NetInstall, or NetRestore image article by Apple](#).
- Reference these Apple articles for more information:
 - [TN2459](#)
 - [HT208019](#)
 - [HT201314](#)

macOS Installation Verification

Check the following files to verify successful Agent installation.

1. The program folder was created. macOS default: `/Applications/Cylance/`
2. The CylancePROTECT icon is visible in the System Tray of the target device. 
This does not apply if parameter NoCylanceUI is used.
3. The CylanceSvc is running in the Activity Monitor of the target device or use Terminal (eg. "ps -ax | grep -i cylance").
4. The Cylance logs are being generated and tracing out. The logs are located in the following location:
`/Library/Application Support/Cylance/Desktop/log`
5. The device is reporting to the Console. Login to the console and click the Devices tab. The target device should show up and be listed in the online state.

Uninstall the macOS Agent

Before you attempt to uninstall the Agent:

- If Require Password to Uninstall Agent (**Settings > Application**) is enabled, make sure you have the password to uninstall the product.
- If Prevent Service Shutdown from Device (**Settings > Device Policy > Protection Settings**) is enabled, either disable it in the policy or apply a different policy to the devices from which you want to uninstall the agent. Another method is to delete the device from the Console and then restart the device. This should unregister the device and allow you to uninstall the Agent.

Without Password

```
sudo /Applications/Cylance/Uninstall\ CylancePROTECT.app/Contents/MacOS/Uninstall\ CylancePROTECT
```

With Password

```
sudo /Applications/Cylance/Uninstall\ CylancePROTECT.app/Contents/MacOS/Uninstall\ CylancePROTECT --password=thisismypassword
```

Note: Replace *thisismypassword* with the uninstall password created in the Console.

Linux Agent

System Requirements

BlackBerry Cylance recommends that endpoint hardware (CPU, GPU, and so forth) meets or exceeds the recommended requirements of the target operating system. Exceptions are noted below (RAM, available hard drive space, and additional software requirements).

Supported Linux Operating Systems

The device can be a physical or virtual machine.

OS	32-bit	64-bit	Notes
RHEL/CentOS 6.6	X	X*	Agent 1430 or higher.**
RHEL/CentOS 6.7	X	X*	Agent 1430 or higher.**
RHEL/CentOS 6.8	X	X*	Agent 1430 or higher.**

OS	32-bit	64-bit	Notes
RHEL/CentOS 6.9	X	X	Agent 1470 or higher.**
RHEL/CentOS 6.10	X	X	Agent 1500 or higher.**
RHEL/CentOS 7.0	X	X*	Agent 1430 or higher.**
RHEL/CentOS 7.1	–	X	Agent 1430 or higher.**
RHEL/CentOS 7.2	–	X	Agent 1430 or higher.**
RHEL/CentOS 7.3	–	X	Agent 1430 or higher.**
RHEL/CentOS 7.4	–	X	Agent 1470 or higher.**
RHEL/CentOS 7.5	–	X	Agent 1490 or higher.**
RHEL/CentOS 7.6	–	X	Agent 1510 or higher.**
RHEL/CentOS 7.7	–	X	Agent 1550 or higher.**
RHEL/CentOS 7.8	–	X	Agent 1560 or higher.**
RHEL/CentOS 8.0	–	X	Agent 1560 or higher.**
SUSE (SLES) 11.4	–	X	Agent 1550 or higher.
SUSE (SLES) 12 SP1, SP2, SP3, SP4	–	X	Agent 1550 or higher for SP1, SP2, and SP3. Agent 1560 or higher for SP4.
Ubuntu LTS/Xubuntu 14.04***	X	X	Agent 1480 or higher.
Ubuntu LTS/Xubuntu 16.04***	X	X	Agent 1480 or higher.
Ubuntu LTS/Xubuntu 18.04***	–	X	Agent 1510 or higher.
Amazon Linux 1 (2017.09 and 2018.03)	–	X	Agent 1510 or higher.
Amazon Linux 2	–	X	Agent 1510 or higher.

* For RHEL/CentOS 64-bit systems, the Agent is a 32-bit binary and requires 32-bit libraries to run. Make sure all dependencies are installed before installing the Agent. Agent version 1470 and higher does not require the 32-bit libraries to run.

**FIPS support:

- For RHEL/CentOS 6.x and 7.x, FIPS support is available in Agent 1530 or higher. To enable FIPs, see [FEDERAL INFORMATION PROCESSING STANDARD \(FIPS\)](#) and [How can I make RHEL 6 or RHEL 7 FIPS 140-2 compliant](#) for more information.
- For RHEL/CentOS 8.0, FIPS support is available in Agent 1560 or higher. To enable

OS	32-bit	64-bit	Notes
<p>FIPS, see How RHEL 8 is designed for FIPS 140-2 requirements for more information.</p> <p>***Azure for Ubuntu is not supported at this time, only the Ubuntu distros mentioned above are supported.</p> <p>UEFI Secure Boot: The CylancePROTECT Agent for Linux kernel module is not signed at this time for UEFI Secure Boot. To utilize the Agent, perform one of the following options:</p> <ul style="list-style-type: none"> ■ Disable UEFI Secure Boot ■ Sign the kernel module. The kernel module can be found here: <code>/lib/modules/\$(uname -r)/extra</code> <p>Note: For a list of Linux kernel versions, per distro, see the Linux Distro Kernel List article.</p>			

Additional Linux Requirements

Type	Description
Processor	<ul style="list-style-type: none"> ■ Requires at a minimum a two core processor. ■ Supports the SSE2 instruction set ■ Supports x86_64 instruction set
RAM	<ul style="list-style-type: none"> ■ 2 GB
Available Hard Drive Space	<ul style="list-style-type: none"> ■ 600 MB <p>Note: Disk space usage can increase depending on features enabled, like setting the log level to Verbose.</p>
Additional Requirements	<ul style="list-style-type: none"> ■ Internet Browser ■ Internet access to login, access the installer, and register the product ■ Local administrator rights to install the software ■ Root Certificates: <ul style="list-style-type: none"> • VeriSign Class 3 Public Primary Certification Authority - G5 • GeoTrust Global CA • thawte Primary Root CA • DigiCert Global Root <p>Note: Devices missing any of the above root certificates may experience issues with the Cylance service not starting or the device being unable to communicate with the Console. Please see this article for more details about missing root certificates.</p>
Other	<ul style="list-style-type: none"> ■ TLS 1.2 is supported with Agent version 1450 or higher. ■ Required packages:

Type	Description
	<ul style="list-style-type: none"> • glibc • dbus-libs <ul style="list-style-type: none"> • RHEL/CentOS 7.x and 8.0 - dbus version 1.10.24 or higher • openssl-libs • libgcc • sqlite

Linux Installation

Note: Root permission is required to install the Linux Agent.

Create a Configuration File

Create the following file before installing the RPM or Deb:

/opt/cylance/config_defaults.txt

Add configuration settings to the file, such as:

InstallToken=YOURINSTALLTOKEN

SelfProtectionLevel=2

LogLevel=2

VenueZone=ZONE_NAME

UiMode=2

AWS=1

This file will be removed after the RPM has been installed.

Note:

- Creating the config_defaults.txt file on a DOS/Windows machine may cause device registration to fail on a Linux Agent. Text files created on DOS/Windows machines have a carriage return and line feed ("\r\n") as a line ending, but Linux/Unix machines have just a line feed ("\n") as a line ending. CylancePROTECT requires the config_defaults.txt file to contain only line feed ("\n") as a line ending. For instructions on how to convert the config_defaults.txt file to a proper format, see the knowledge base article [here](#).
- The configuration file will be removed after the RPM or Deb has been installed.

Property	Description
InstallToken	This is required. It is your Installation Token that you can find in the Console (Settings > Application).
SelfProtectionLevel	Can restrict access to the Cylance Service and folders. <ul style="list-style-type: none"> ■ 1 = Only Local Administrators can make changes to the registry and services. ■ 2 = Only the System Administrator can make changes to the registry and services. This should be the default setting.
LogLevel	Sets the level of information gathered in the debug logs. <ul style="list-style-type: none"> ■ 0 = Error ■ 1 = Warning ■ 2 = Information (this should be the default setting) ■ 3 = Verbose (log file size can grow quickly).
VenueZone	Use this to assign the Linux Agent to a zone in the organization. <ul style="list-style-type: none"> ■ Adds devices to a zone. ■ Replace zone_name with the name of an existing zone or a zone you want to create. ■ If the zone does not exist, the zone is created using the name provided. ■ If the device name or zone name contains a leading whitespace " Hello" or trailing whitespace "Hello ", Cylance removes the whitespace during device registration. <p>Note: Tabs, carriage returns, newlines, or other invisible characters are not permitted.</p> ■ Zone names cannot contain an equals sign, such as "Hello=World".
UiMode	Sets the mode for the Agent user-interface when the system starts. <ul style="list-style-type: none"> ■ 1 = Minimal user-interface ■ 2 = Full user-interface
AWS	Specifies the Agent is running on an AmazonCloud host. This will enable the Agent to capture the Instance ID and store it with the hostname to the Device Name field. <ul style="list-style-type: none"> ■ 1 = Capture ID <p>The Device Name is modified to include Hostname + Instance ID</p> <p>Example:</p> <p>ABC-DE-123456789_i- 0a1b2cd34efg56789 where the device name is ABCDE- 12345678 and the AWS EC2 ID is i-0a1b2cd34efg56789.</p>

Table 3: Installation parameters for Linux

Example script to create the configuration text file:

```
echo InstallToken=YOURINSTALLTOKEN > config_defaults.txt  
echo SelfProtectionLevel=# >> config_defaults.txt  
echo VenueZone=zone_name >> config_defaults.txt  
echo LogLevel=# >> config_defaults.txt
```

Note:

- The config_defaults.txt file must be in /opt/cylance/.
- In the example, replace YOURINSTALLTOKEN with your Installation Token from your Cylance Console.
- In the example, replace zone_name with the name of the Zone the device should be added to.

Installation Location

The following locations are created when you install the Linux Agent. Some locations are specific to the version of the operating system used.

- /opt/cylance/desktop
- /etc/init/cylancesvc.conf (RHEL/CentOS 6.x, Ubuntu 14.04, Amazon 2017.09 and 2018.03)
- /etc/init.d/cylancesvc (SLES 11.4)
- /usr/lib/systemd/system/cylancesvc.service (RHEL/CentOS 7.x and 8, Ubuntu 16.04 and 18.04, Amazon 2, SLES 12.x)
- /etc/modprobe.d/cylance.conf
- /etc/sysconfig/modules/cylance.modules (All OS's except SLES 11.4)
- /lib/modules/\$(uname -r)/extra
- /usr/src/CyProtectDrv-1.2
- /opt/cylance/lib64 (SLES 11.4 only; provides Open Source libraries described below)

Open Source Libraries (SLES 11.4)

The following Open Source libraries are packaged for SLES 11.4.

Library	License
glibc	LGPL
OpenSSL	OpenSSL, SSLeay

Table 4: SLES 11.4 Open Source Libraries

Install the RHEL/CentOS Agent Automatically

The Agent can be installed simply, along with the dependencies, using the yum command on RHEL/CentOS 7.x for CylancePROTECT Agent 1460 or higher or on RHEL/CentOS 8.0 for CylancePROTECT Agent 1560 or higher. This also installs the dependencies. For all Ubuntu operating systems, or RHEL/CentOS Agent 1450 and lower, you must install the dependencies first, then the product. See ["Install the RHEL/CentOS Agent Manually" below](#) or ["Install the Ubuntu Agent Manually" on page 100](#) for more information.

1. ["Download the Install File" on page 59.](#)
2. Create the following file before installing the RPM:

```
/opt/cylance/config_defaults.txt
```

For more information, see ["Create a Configuration File" on page 95](#)

3. For RHEL/CentOS 6, use the following command:

```
yum install bzip2 dbus dbus-libs
```

For all other versions you must install the dependencies independently first.

4. Use the following command to install the product:

```
yum install CylancePROTECT.version.rpm CylancePROTECTUI.version.rpm
```

Install the RHEL/CentOS Agent Manually

1. ["Download the Install File" on page 59.](#)
2. Create the following file before installing the RPM:

```
/opt/cylance/config_defaults.txt
```

For more information, see ["Linux Installation" on page 95.](#)

3. If the kernel version is not pre-built into the Agent, you will need to use the GNU Compiler Collection (GCC) to compile the kernel. For a list of kernels pre-built in the agent, see the [Linux Distro Kernel List Supported by Cylance.](#)

Run:

```
yum install gcc kernel-devel-$(uname -r)
```

4. For RHEL/CentOS 6, install the following using this command:

```
yum install bzip2 dbus
```

5. For 64-bit operating systems, you may need to install the 32-bit dependencies.

If using Agent version	With OS	Then
1560 or higher	RHEL8/CentOS8	You do not need to install the 32-bit dependencies.
1450 or higher	RHEL7/CentOS7	You do not need to install the 32-bit dependencies.
1460 or higher	RHEL6/CentOS6	You do not need to install the 32-bit dependencies.
1440 or lower	RHEL6.x/CentOS6.x RHEL7.x/CentOS7.x	You must install the 32-bit dependencies. The Agent is a 32-bit binary and requires 32-bit libraries to run.

Use the following command:

- RHEL/CentOS 6.x – *yum install glibc.i686 dbus-libs.i686 openssl.i686 libgcc.i686 sqlite.i686 openssl libgcc sqlite dbus*
- RHEL/CentOS 7.x – *yum install glibc.i686 dbus-libs.i686 openssl-libs.i686 libgcc.i686 sqlite.i686 openssl openssl-libs libgcc sqlite dbus dbus-libs*

6. Use the following command to install the Linux Agent:

```
rpm -ivh CylancePROTECT.version.rpm
```

7. Use the following command to install the Linux Agent UI (optional):

```
rpm -ivh CylancePROTECTUI.version.rpm
```

Note: Review the following:

- CentOS 7.x also requires that you replace the GNOME shell in order to view the CylancePROTECT UI. You can do this by pressing Alt+F2, then type r, then press **Enter**.
- There is a bug that can cause the GNOME extension to not be recognized. In case of failure, you will have to manually enable the GNOME extension. You can do this from the command line using gnome-tweak-tool. In the GNOME Tweak Tool, go to the Extensions tab and enable the CylanceUI. This bug has been fixed in CentOS 7.2 (GNOME 3.14).
- “Error:Multilib version problems found.” – If this error occurs when installing a package, then the corresponding 64-bit library must be installed or upgraded, along with the 32-bit library. This often means that the root cause is something else and multilib version checking is pointing out that there is a problem. For example:

- You have an upgrade for sqlite which is missing some dependency that another package requires. Yum is trying to solve this by installing an older version of sqlite of the different architecture. If you exclude the bad architecture, yum will tell you what the root cause is (which package requires what). You can try redoing the upgrade with `--exclude sqlite.otherarch`. This should display an error message showing the root cause of the problem.
- You have multiple architectures of sqlite installed, but yum can only see an upgrade for one of those architectures. If you don't need both architectures, you can remove the one with the missing update and everything will work.
- You have duplicate versions of sqlite installed already. You can use "yum check" to show these errors.
- To install or upgrade the matching SQLite library, use the following command:
`yum install sqlite.i686 sqlite`

This may also be a problem with dbus-libs, openssl, or libgcc. If so, replace sqlite with the correct library in the command above.

Install the Ubuntu Agent Manually

1. ["Download the Install File" on page 59.](#)

2. Create the following file before installing the Deb:

```
/opt/cylance/config_defaults.txt
```

For more information, see ["Create a Configuration File" on page 95.](#)

3. Install the dependencies:

```
sudo apt-get update -y && sudo apt-get install libxml2-utils make gcc bzip2 linux-headers-generic
```

Note: If the kernel version is not pre-built into the Agent, you will need to use the GNU Compiler Collection (GCC) to compile the kernel. For a list of kernels pre-built in the agent, see the [Linux Distro Kernel List Supported by Cylance.](#)

4. Use the following command to install the Linux Agent:

```
dpkg -i cylance-protect.deb
```

5. Use the following command to install the Linux Agent UI (optional):

```
dpkg -i cylance-protect-ui.deb
```

Install the Amazon Agent Automatically

For Amazon Linux 2, the Agent can be installed automatically, along with the dependencies:

1. ["Download the Install File" on page 59.](#)
2. Create the following file before installing the RPM:

```
/opt/cylance/config_defaults.txt
```

For more information, see ["Create a Configuration File" on page 95.](#)

3. Use the following command to install the product:

```
yum install CylancePROTECT.rpm
```

The Amazon Linux 2 Agent can also be installed manually by installing dependencies independently first via the steps below. For Amazon Linux 1, the agent must be installed using the manual steps below.

Install the Amazon Agent Manually

1. ["Download the Install File" on page 59.](#)
2. Run the following yum command to install dependencies:

```
yum install zlib glibc dbus-libs libgcc sqlite
```

Note: If the kernel version is not pre-built into the Agent, you will need to use the GNU Compiler Collection (GCC) to compile the kernel. For a list of kernels pre-built in the agent, see the [Linux Distro Kernel List Supported by Cylance.](#)

3. Create a configuration text file before installing the RPM.

For more information, see ["Create a Configuration File" on page 95](#)

4. Capture the Amazon EC2 Instance ID.

The CylancePROTECT agent can be configured to capture Amazon's Instance ID and concatenate it to the Device Name field. When creating the configuration file, add AWS=1 as a line item to the text file.

5. Install the RPM:

```
rpm -ivh CylancePROTECT.rpm
```

6. Install the script.

The install script 'install.sh' can be used to install the RPM. The script will prompt the user to enter the token and generate a config_defaults.txt file if one doesn't exist.

```
install.sh CylancePROTECT.rpm
```

Amazon Linux Commands

```
/opt/cylance/desktop/cylance -h
```

usage: cylance <options>

Option	Description
-r, --register=token	Register the agent with the Console using the provided token
-s, --status	Check for updates
-b, --start-bg-scan	Start background scan
-B, --stop-bg-scan	Stop background scan
-d, --scan-dir=dir	Scan directory
-l, --getloglevel	Get current log level.
-L, --setloglevel=level	Set log level
-P, --getpolicytime	Get the policy update time
-p, --checkpolicy	Check for policy updates
-t, --threats	List threats
-q, --quarantine=id	Quarantine a file by id (hash)
-w, --waive=id	Waive a file by id (hash)
-v, --version	Print this tool's version
-h, --help	Print this message

Table 5: Amazon Linux Command Line Options

Install the SUSE Agent Automatically

The Agent can be installed simply, along with the dependencies, using the zypper command on Agent 1540 or higher (SUSE 11.4 or SUSE 12 SP1, SP2, or SP3) or on Agent 1560 or higher (SUSE 12 SP4).

1. ["Download the Install File" on page 59.](#)
2. Create the following file before installing the RPM:

```
/opt/cylance/config_defaults.txt
```

For more information, see ["Create a Configuration File" on page 95](#)

3. Use the following command:

```
zypper install CylancePROTECT.rpm CylancePROTECTUI.rpm
```

Note: If zypper warns you that the packages are not signed, you will need to ignore the warning and continue.

Install the SUSE Agent Manually

1. ["Download the Install File" on page 59.](#)
2. Run the following zypper command to install dependencies:

For SUSE 11.4:

```
zypper install glibc, dbus-1, libgcc_s1, libsqlite3-0, zlib, bzip2, libxml2
```

For SUSE 12:

```
zypper install glibc, dbus-1, libopenssl1_0_0, libgcc_s1, libsqlite3-0, libz1, bzip2, libxml2-tools
```

3. Create a configuration text file before installing the RPM.

For more information, see ["Create a Configuration File" on page 95](#)

4. Use the following command to install the SUSE Agent:

```
rpm -ivh CylancePROTECT.rpm
```

5. Use the following command to install the SUSE Agent UI (optional):

```
rpm -ivh CylancePROTECTUI.rpm
```

Start the UI (Ubuntu and SUSE 12)

There is currently no reliable way to launch the UI on install, so the UI must be launched manually, or log out and then log back in.

Enable the UI in GNOME Shell

You will need to restart the GNOME Shell to load the UI on the top bar. Ubuntu 18.04 does not include the GNOME Tweak Tool by default. You will need to install it (if needed) before restarting the GNOME Shell.

1. For Ubuntu 18.04 only, run the following commands as root to install the GNOME Tweak Tool:

```
add-apt-repository universe
```

```
apt install gnome-tweak-tool
```

2. Restart the GNOME Shell Extension by pressing 'Alt+F2', then type 'r' in the dialog box, then 'ENTER'.

If the CylanceUI icon still does not show up, you will have to manually enable the GNOME Shell extension.

You can do this by launching the GNOME Tweak Tool either by typing 'gnome-tweaks' in a terminal.

In the GNOME Tweak Tool, go to the Extensions tab and enable the CylanceUI.

Installation — System Management

The Agent can be installed directly on each system or through a system management software. Examples: GPO, SCCM, and MSIEXEC. When installing the Agent, Installation Parameters are provided to configure some installation settings.

Note: Ensure the target devices meet System Requirements and that you have the proper credentials for installing software.

Set an Unauthenticated Proxy Server - Linux

These steps can be done before installation.

IMPORTANT: Unauthenticated proxies are supported with Agent 1430 or higher.

RHEL\CentOS 6.x

```
echo "env http_proxy=http://proxyaddress:port" > /etc/init/cylancesvc.override
initctl stop cylancesvc
initctl reload-configuration
initctl start cylancesvc
```

RHEL\CentOS 7.x and 8.0

```
mkdir /etc/systemd/system/cylancesvc.service.d
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf
echo "Environment=http_proxy=http://proxyaddress:port" >>
/etc/systemd/system/cylancesvc.service.d/proxy.conf
systemctl stop cylancesvc
systemctl daemon-reload
systemctl start cylancesvc
```

Ubuntu 14.04

```
env http_proxy="http://proxyaddress:port"
```



```
initctl stop cylancesvc
initctl reload-configuration
initctl start cylancesvc
```

Ubuntu 16.04 and 18.04

```
mkdir /etc/systemd/system/cylancesvc.service.d
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf
echo "Environment=http_proxy=http://proxyaddress:port" >>
/etc/systemd/system/cylancesvc.service.d/proxy.conf
systemctl stop cylancesvc
systemctl daemon-reload
systemctl start cylancesvc
```

Amazon Linux 1

```
echo "env http_proxy=http://proxyaddress:port" > /etc/init/cylancesvc.override
initctl stop cylancesvc
initctl reload-configuration
initctl start cylancesvc
```

Amazon Linux 2 and SUSE 12:

```
mkdir /etc/systemd/system/cylancesvc.service.d
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf
echo "Environment=http_proxy=http://proxyaddress:port" >>
/etc/systemd/system/cylancesvc.service.d/proxy.conf
systemctl stop cylancesvc
systemctl daemon-reload
systemctl start cylancesvc
```

Set an Authenticated Proxy Server - Linux

These steps can be done before installation.

IMPORTANT: Authenticated proxies are only available with HTTP on Agent 1530 or higher. If you downgrade to a version older than 1530, you will no longer be able to use authenticated proxies.

RHEL\CentOS 6.x

```
echo "env http_proxy=user:password@proxyaddress:port" >
/etc/init/cylancesvc.override

initctl stop cylancesvc

initctl reload-configuration

initctl start cylancesvc
```

RHEL\CentOS 7.x and 8.0

```
mkdir /etc/systemd/system/cylancesvc.service.d

echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf

echo "Environment=http_proxy=user:password@proxyaddress:port" >>
/etc/systemd/system/cylancesvc.service.d/proxy.conf

systemctl stop cylancesvc

systemctl daemon-reload

systemctl start cylancesvc
```

Ubuntu 14.04

```
echo "env http_proxy=user:password@proxyaddress:port" >
/etc/init/cylancesvc.override

initctl stop cylancesvc

initctl reload-configuration

initctl start cylancesvc
```

Ubuntu 16.04 and 18.04

```
mkdir /etc/systemd/system/cylancesvc.service.d

echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf

echo "Environment=http_proxy=user:password@proxyaddress:port" >>
/etc/systemd/system/cylancesvc.service.d/proxy.conf

systemctl stop cylancesvc

systemctl daemon-reload

systemctl start cylancesvc
```

Amazon Linux 1

```
echo "env http_proxy=user:password@proxyaddress:port" >
```

```
/etc/init/cylancesvc.override  
initctl stop cylancesvc  
initctl reload-configuration  
initctl start cylancesvc
```

Amazon Linux 2 and SUSE 12

```
mkdir /etc/systemd/system/cylancesvc.service.d  
echo "[Service]" > /etc/systemd/system/cylancesvc.service.d/proxy.conf  
echo "Environment=http_proxy=user:password@proxyaddress:port" >>  
/etc/systemd/system/cylancesvc.service.d/proxy.conf  
  
systemctl stop cylancesvc  
systemctl daemon-reload  
systemctl start cylancesvc
```

Kernel Driver

Load the Kernel Driver

Use the following command:

For all OS's except SUSE

```
modprobe cyprotect
```

SUSE

```
modprobe --allow-unsupported cyprotect
```

Note: If you don't want to keep using the `--allow-unsupported` flag, edit `/etc/modprobe.d/10-unsupported-modules.conf` and change `'allow_unsupported_modules'` to `'1'`.

Unload the Kernel Driver

Note: The Cylance Service must be stopped first.

Use the following command:

```
modprobe -r cyprotect
```

Check whether the Kernel Driver is Loaded

Use the following command:

```
lsmod | grep CyProtectDrv
```

If the kernel module is loaded, the command should output something like the following:

```
CyProtectDrv 210706 0
```

If the kernel module is not loaded, no output is returned.

Logging - Linux

Get the Log Level

Use the following command to view the current log level set for the Linux Agent:

```
/opt/cylance/desktop/cylance -l
```

Set the Log Level

Use the following command to set the log level for the Linux Agent. In the example below, “3” sets the log level to Verbose. Change the number to change the log level.

```
# Supported Levels: 0-3
```

```
# 0 - Error
```

```
# 1 - Warning
```

```
# 2 - Informational
```

```
# 3 - Verbose
```

```
/opt/cylance/desktop/cylance -L 3
```

How To Collect Logs

Use the following command to gather the log files from a Linux device. Log files are stored on the device for 30 days.

Note: You must do this as root.

For RHEL/CentOS:

```
ps aux > ~/ps.txt
```

```
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ' ' -f 1) > ~/maps.txt
```

```
cat /proc/cpuinfo > ~/cpu.txt
```

```
cat /proc/meminfo > ~/mem.txt
```

```
cat /proc/mounts > ~/mounts.txt
```

```
cat /proc/modules > ~/modules.txt
```

```
cat /proc/slabinfo > ~/slabinfo.txt
```

```
tar -cvzf cylancelogs-$(date --rfc-3339='date').tgz /var/log/messages*
/opt/cylance/desktop/log ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt ~/ps.txt
~/mem.txt ~/slabinfo.txt
```

For Ubuntu:

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ' ' -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339='date').tgz /var/log/syslog*
/opt/cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt
~/slabinfo.txt ~/mem.txt
```

For Amazon or SUSE:

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ' ' -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339='date').tgz /var/log/messages*
/opt/cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt
~/slabinfo.txt
```

Amazon Linux 1 Kernel Debug Messages

On Amazon Linux 1, the default setting is to NOT have kernel debug messages get directed to /var/log/messages.

To direct kernel debug messages to /var/log/messages, edit /etc/rsyslog.conf and add the following:

```
kern.* /var/log/messages
```

Then, restart rsyslogd or reboot.

Re-register a Linux Agent

If the Agent ever becomes unregistered from the Console, accidentally or otherwise, and the user needs to re-register with a token, use the following command:

For RHEL/CentOS and Ubuntu

```
/opt/cylance/desktop/cylance --register=token
```

For CentOS, you can also use the following command:

```
/opt/cylance/desktop/cylance --r=token
```

For Amazon Linux or SUSE

```
/opt/cylance/desktop/cylance -r token
```

Stop or Start the Linux Service

Use the following commands to start or stop the Cylance Service.

RHEL/CentOS 6.x, Ubuntu 14.04, and Amazon Linux 1

```
start cylancesvc
```

```
stop cylancesvc
```

RHEL/CentOS 7.x or 8.0, Ubuntu 16.04 or 18.04, Amazon Linux 2, SUSE 12

```
systemctl start cylancesvc
```

```
systemctl stop cylancesvc
```

SUSE 11.4

```
/etc/init.d/cylancesvc start
```

```
/etc/init.d/cylancesvc stop
```

Upgrade the Linux Agent

RHEL/CentOS 6.x, 7.x (on Agent 1460 or higher), and 8.0:

Use the zone-based updating mechanism on the Update page in the Console.

RHEL/CentOS 7.x (on Agent 1450 or lower), Ubuntu, Amazon, and SUSE:

The Agent must be upgraded manually.

1. Download the latest RPM or Deb package from the Console.
2. Use the following command to upgrade the Linux Agent:

RHEL/CentOS: `rpm -Uvh CylancePROTECT.version.rpm`

Ubuntu: `dpkg -i cylance-protect.deb`

Amazon or SUSE: `rpm -Uvh CylancePROTECT.rpm`

3. Use the following command to upgrade the Linux Agent UI.

RHEL/CentOS: `rpm -Uvh CylancePROTECTUI.version.rpm`

Ubuntu: `dpkg -i cylance-protect-ui.deb`

SUSE: `rpm -Uvh CylancePROTECTUI.rpm`

Uninstall the Linux Agent

Before Uninstalling the Agent

Make sure all Agents have **Prevent Service Shutdown for Device** and **Application Control** disabled. This is done in a device policy. These features can prevent a successful Agent uninstall.

1. For the devices to uninstall the Agent from, assign these devices to a policy with no settings enabled.
 - a. Make sure the policy has no settings enabled, especially **Prevent Service Shutdown for Device** and **Application Control**.
 - b. Make sure these devices receive the new policy.

Another method is to delete the device from the Console and then restart the device (Application Control must be disabled). This should unregister the device and allow you to uninstall the Agent.

2. Follow the steps below to remove the Agent from the device.
3. After the Agent is removed from the device, the device can be removed from the Console.

Uninstalling the Agent on the device does not remove the device from the Console. You must manually remove the device from the Device tab in the Console after the Agent has been uninstalled.

To Uninstall the Linux Agent

Use the following command to uninstall the Linux Agent.

For RHEL/CentOS:

```
rpm -e CylancePROTECT CylancePROTECTUI
```

Or

```
rpm -e $(rpm -qa | grep -i cylance)
```

For Ubuntu:

```
dpkg -P cylance-protect cylance-protect-ui
```

For Amazon or SUSE:

```
rpm -e $(rpm -qa | grep -i cylance)
```

Agent Update

Maintenance and management of CylancePROTECT Agents is hassle-free. Agents automatically download updates from the Console, and the Console is maintained by Cylance.

Note: The Agent checks in with the Console every 1-2 minutes to update the Console with the Agent's current state (*Online* or *Offline*, *Unsafe* or *Protected*), Version Information, Operating System, and Threat Status. The Agent Update is a separate check-in.

CylancePROTECT releases updates to the Agent on a monthly basis. These updates can include configuration revisions, new modules, and program changes. When an Agent update is available (as reported by the Console under **Settings > Agent Updates**), the Agent automatically downloads and applies the update. To control network traffic during Agent updates, all organizations are set to accommodate a maximum of 1000 device updates simultaneously. Users can also disable the Auto Update feature if they prefer.

Note: The maximum number of devices for simultaneous update can be modified by Cylance Support.

Zone-Based Updating

Zone-Based Updating allows an organization to evaluate a new agent on a subset of devices before deploying it to the entire environment (Production). One or more current Zones can be temporarily added to one of two Testing Zones (Test and Pilot) which can use a different Agent than Production.

Rollback Agent Version

If a device is using the latest Agent version, you can change it to the previous Agent version using Zone-Based Updating. A device will always update to the Agent version specified

(CylancePROTECT or CylanceOPTICS).

To Configure Zone-based Updates

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

1. Select **Settings > Update**. The three latest Agent versions are displayed.
If the Production Zone is set to **Auto-Update**, the Test and Pilot Zones are not available. Change Auto-Update in the Production Zone to something else to enable the Test and Pilot Zones.
2. Select a specific Agent version in the Production drop-down list.
3. For Production, also select Auto-Update or Do Not Update.
 - **Auto-Update** allows all Production devices to automatically update to the latest version in the *Supported Agent Versions List*.
 - **Do Not Update** prohibits all Production devices from updating the Agent.
4. For the Test Zone, choose one or more Zones from the Zone drop-down list, then select a specific Agent version from the version drop-down list
5. If desired, repeat step 5 for the Pilot Zone.

Note: When a device is added to a Zone that is part of the Test or Pilot Zone, that device starts using the Test or Pilot Zone's Agent version. If a device belongs to more than one Zone, and one of those Zones belongs to either the Test or Pilot Zone, the Test or Pilot Zone Agent version takes precedence. The priority is: Test, Pilot and then Production.

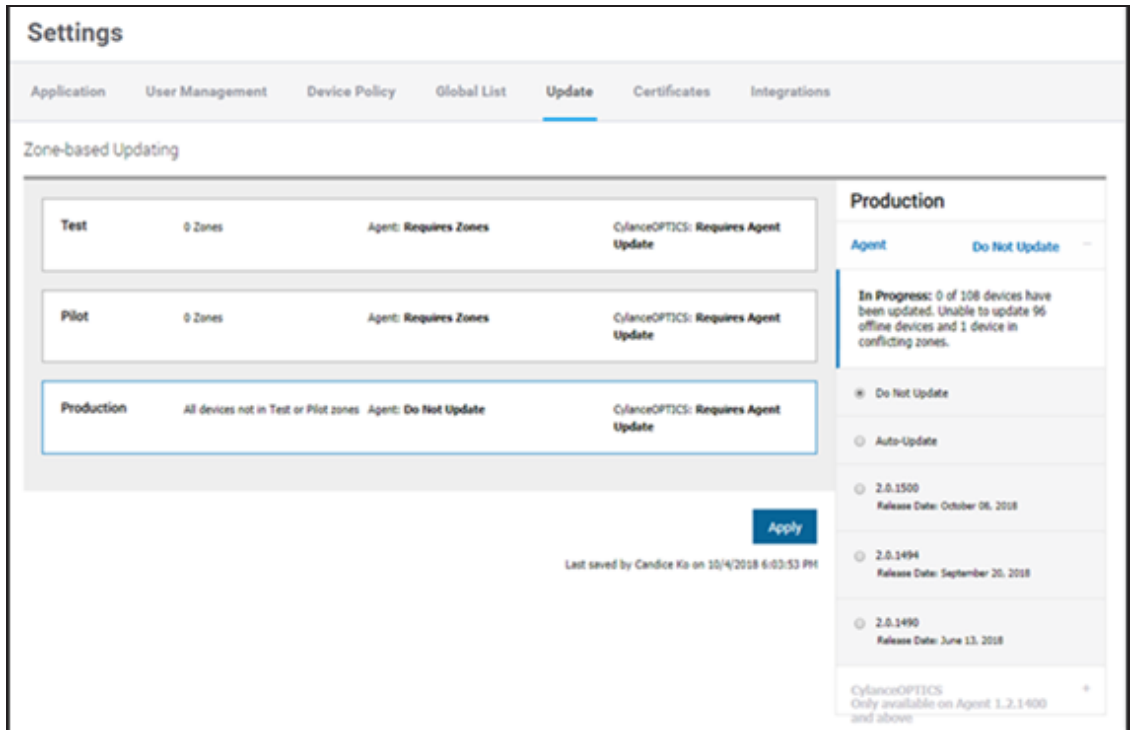


Figure 24: Agent Updates

To Trigger an Agent Update

To trigger an Agent update prior to the next hourly interval: (This requires accessing the device.)

1. Right-click the CylancePROTECT Agent icon in the system tray, and select **Check for Updates**.
2. Restart the CylancePROTECT service. This forces it to immediately check in with the Console.

OR

Updates can be initiated from the command line. Run the following command from the Cylance directory:

```
CylanceUI.exe-update
```

Password-Protected Uninstall

Administrators can require a password for uninstalling the Agent. When uninstalling the Agent with a password:

- If the MSI installer was used to install, you can uninstall using the MSI, Control Panel, or the command line.

- If uninstalling using the command line, add the uninstall string:
UNINSTALLKEY="MyUninstallPassword".

Example:

```
CylancePROTECTx64.msi UNINSTALLKEY="MyUninstallPassword"  
/uninstall
```

Note: If utilizing an uninstall password that contains a special character or symbol, ensure that there are quotations around the uninstall password string to prevent any syntax issues.

On Windows, if the password contains an "&" character, the password must be the final parameter or errors may occur (for example: CylancePROTECTSetup.exe /uninstall /quiet UNINSTALLKEY=asdf&).

- If the EXE installer was used to install and the uninstall is password protected, you must uninstall the EXE from the command line. You cannot uninstall by invoking the EXE directly or using Add/Remove Programs if a password is required to uninstall.

Example:

```
CylancePROTECTSetup.exe UNINSTALLKEY="MyUninstallPassword"  
/uninstall
```

To Create an Uninstall Password

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

1. Select **Settings > Application**.
2. Click the **Require Password to Uninstall Agent** check box.
3. Enter a password.
4. Click **Save**.

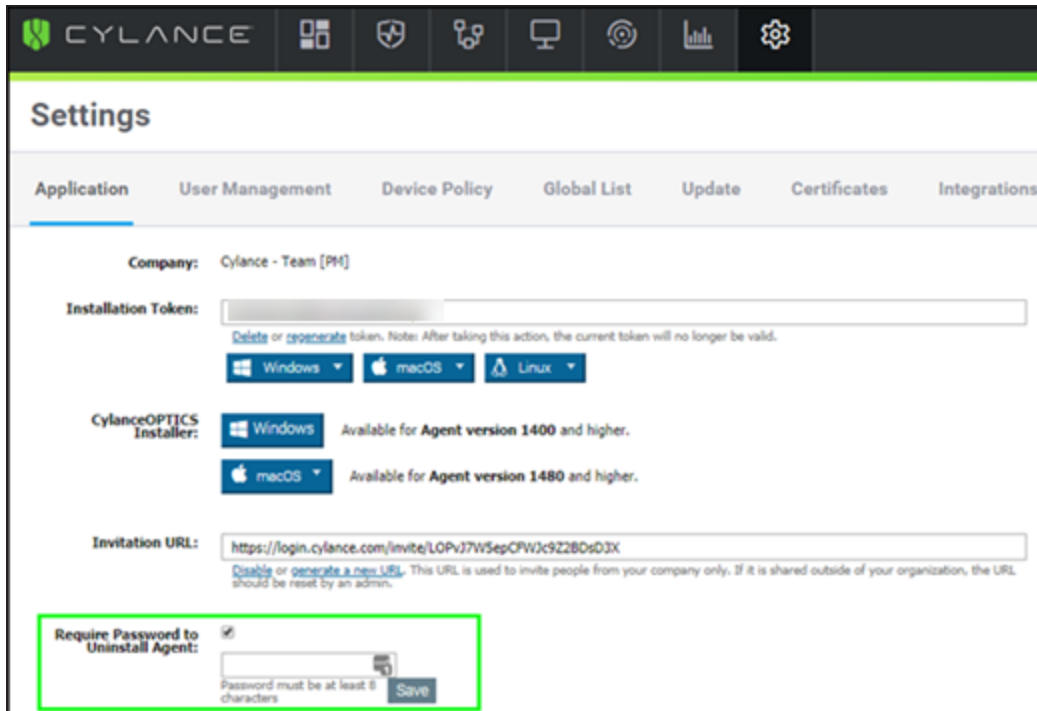


Figure 25: Configure Password-Protected Uninstall

Agent Service


Start Service

```
sudo launchctl load /Library/launchdaemons/com.cylance.agent_service.plist
```

Stop Service

```
sudo launchctl unload /Library/launchdaemons/com.cylance.agent_service.plist
```

Agent User Interface

The Agent user interface is enabled by default. Click  in the System Tray to view. Alternatively, the Agent can be installed to hide the Agent icon from the System Tray.

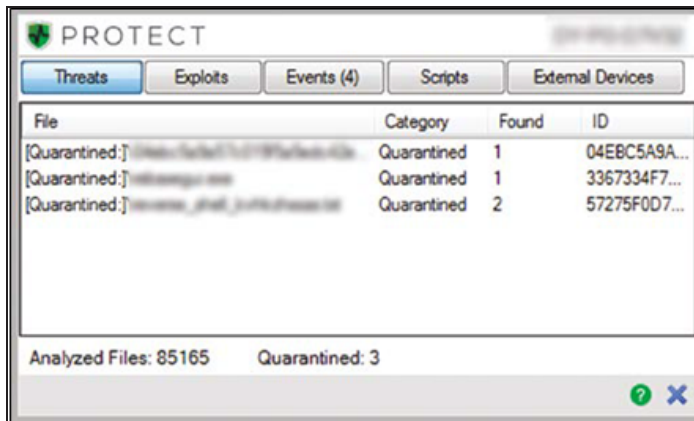


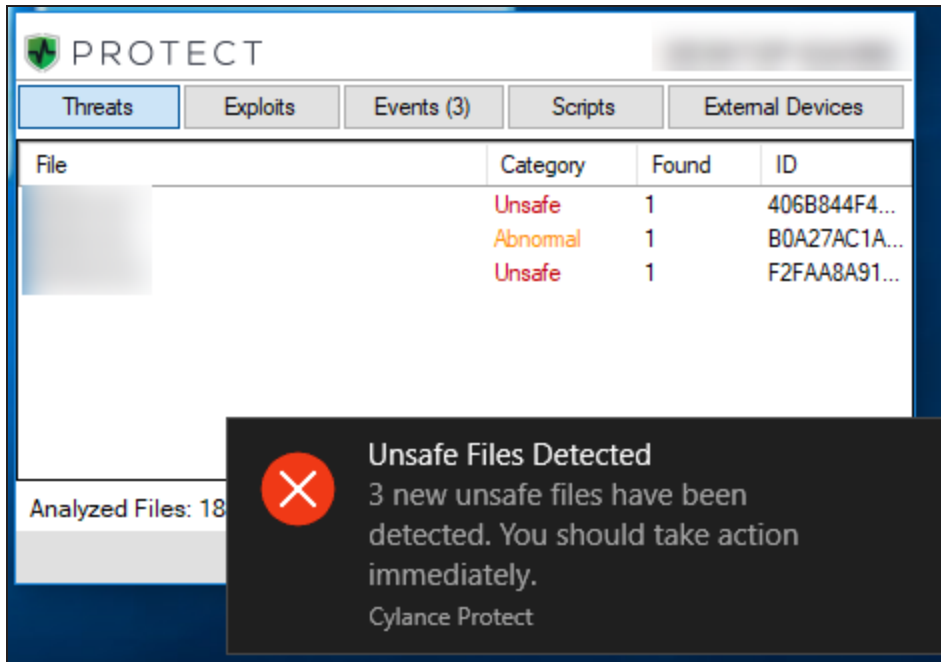
Figure 26: Agent User Interface

Agent UI Notifications

CylancePROTECT provides a number of notifications to alert users when a potential threat is identified on a device.

Desktop Notification

If **Enable Desktop Notifications** is set in the Device Policy, a notification displays when CylancePROTECT finds an unsafe or abnormal file. The notification is sent through the native Windows system notification. The following shows an example of the notification when two unsafe and one abnormal file is detected:



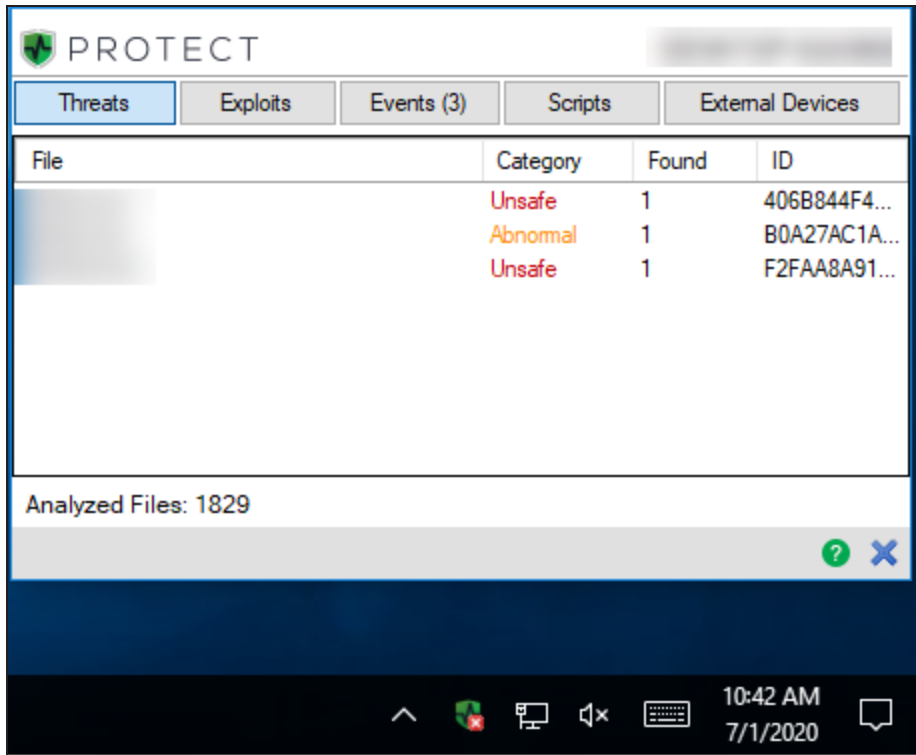
To enable this desktop notifications, see ["Agent Settings" on page 34](#).

System Tray Indicator and View of Unsafe/Abnormal Files

When CylancePROTECT finds an unsafe or abnormal file on a device, a red indicator displays


on the Cylance icon  in the System Tray.

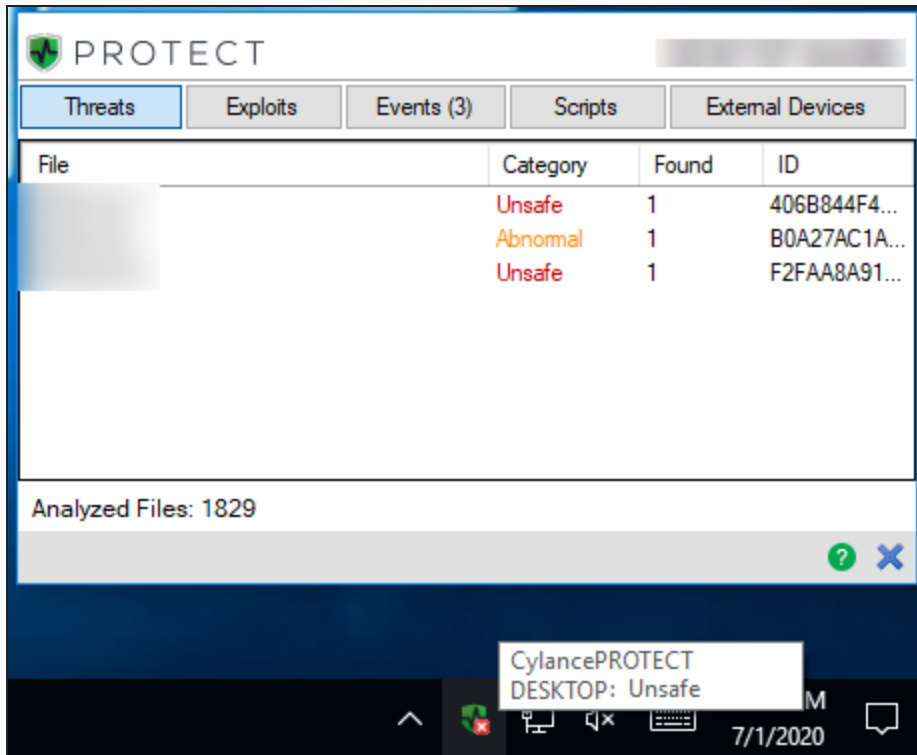
Clicking  shows the current state of the files, similar to the following:



Your device policy or administrator will quarantine or safelist the file; you do not need to take action on these files.

System Tray Indicator when Hovering

When unsafe or abnormal files are detected, if you hover over , an indicator displays informing you that there are unsafe files on the device.

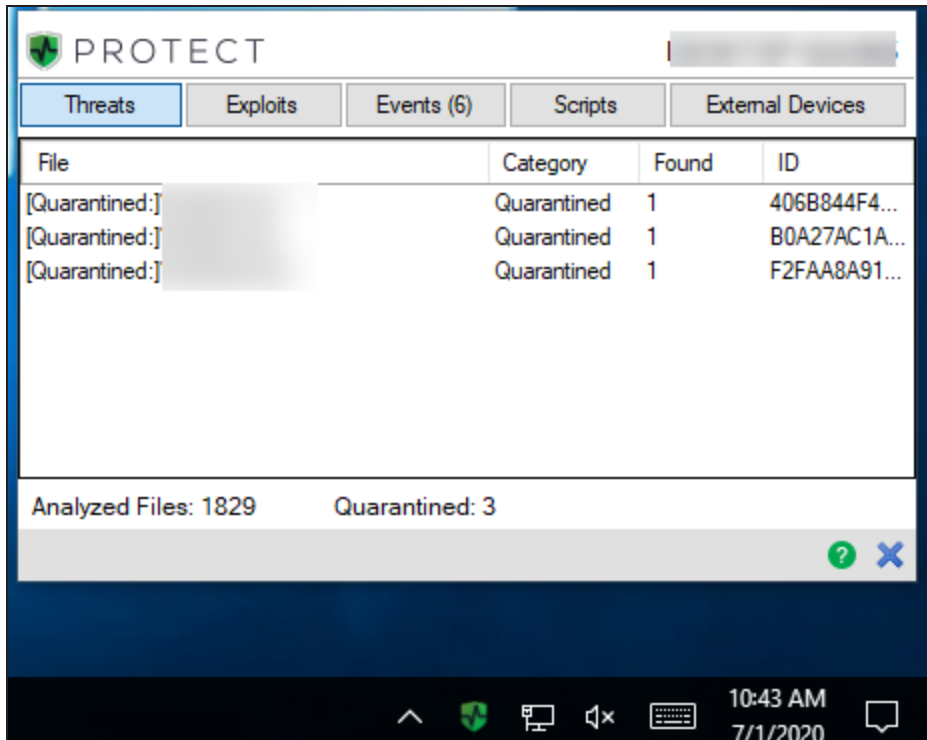


System Tray Indicator and Files when Quarantined

Once the files are quarantined or in a safe state, the Cylance icon returns to its original state -



The previously unsafe or abnormal files also show their updated status in the Agent UI:



Threats Tab

Displays all threats discovered on the device and the action taken. *Unsafe* means no action has been taken on the threat. *Quarantined* means the threat has been modified (to keep the file from executing) and has been moved to the *Quarantine* folder. *Waived* means a file is deemed safe by the administrator and *Allowed* to run on the device.


Events Tab

Displays any threat events that have occurred on the device.

Scripts Tab

Displays any malicious scripts that have run on the device and any action taken on the script.

Agent Menu Options

The Agent menu allows users to perform some actions on the device. Right-click  to see the menu.

Option	Description
Visit Cylance.com	Opens the BlackBerry Cylance website (cylance.com) in your default web browser.
Help / FAQ	Opens the BlackBerry Cylance Support website (support.cylance.com) in your default web browser.
Check for Updates	The Agent checks for and installs any updates available. Updates are restricted to the Agent version allowed for the zone to which the device belongs.
Check for Policy Update	The Agent checks if a policy update is available. This could be changes to the existing policy or a different policy being applied to the Agent.
About	Displays a dialog with the Agent version, name of the policy assigned to the device, the last time the Agent checked for an update, and the device's serial number.
System Check (Windows only)	Displays a list of Cylance services and drivers that are running on the device as well as their status (requires Agent 1510 or later). The following services and drivers display in the list: <ul style="list-style-type: none">■ CylanceSvc - This service allows the CylancePROTECT Agent to communicate with the Console.■ CyDevFlt - This driver is running when a Device Control Policy is applied.■ CyProtectDrv - This driver is running when CylancePROTECT is installed successfully.■ CyOptics - This service allows the CylanceOPTICS Agent to communicate with the Console.■ CyOpticsDrv - This driver is running when CylanceOPTICS is installed successfully.
Exit	Closes the Agent icon in the system tray. This does not turn off any of the Cylance services.
Options > Show Notifications	Select this option to display any new events as notifications.

Enable Agent User Interface Advanced Options

The CylancePROTECT Agent provides some advanced options via the user interface to provide features on devices without connectivity to the Console. The CylanceSVC.exe must be running when the Advanced Options are enabled.

Windows

1. If the Agent icon is visible in the system tray, right-click the icon and select **Exit**.
2. Launch the Command Prompt and enter the following command. Press Enter when complete.

```
cd C:\Program Files\Cylance\desktop
```

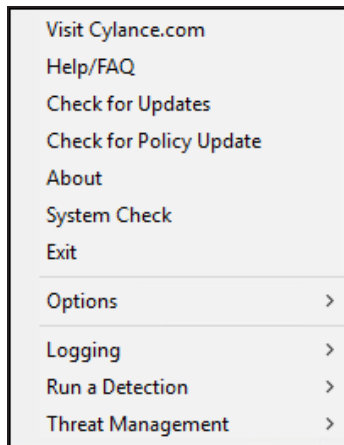
If the application was installed in a different location, you must navigate to that location in the command prompt.

3. Enter the following command and press Enter when complete.

```
CylanceUI.exe -a
```

The Agent icon displays in the system tray.

4. Right-click the icon. *Logging*, *Run a Detection*, and *Threat Management* options display.



Logging

Select the level of log information to collect from the Agent. The default is Information. Make sure you set the log level to All (Verbose) when troubleshooting. When troubleshooting is complete, change this back to Information (logging All information can generate very large log files).

Run a Detection

Allows users to specify a folder to scan for threats.

1. Select **Run a Detection > Specify Folder**.
2. Select a folder to scan, then click **OK**. Any threats found display in the Agent user interface.

Threat Management

Allows users to delete *Quarantined* files on the device.

1. Select **Threat Management > Delete Quarantined**.
2. Click **OK** to confirm.

Virtual Machines

Below are some recommendations for using the CylancePROTECT Agent on a virtual machine image. For best practices, see ["Appendix A: VDI Best Practices " on page 210](#).

- For non-persistent VDI environments, you can use Agent 1490 (or higher) and an installation parameter to instruct the Agent during installation that it will be running in a pool of cloned images. This will enable the Agent to recognize each clone as a unique device and persist their identification when they refresh. See ["Appendix A: VDI Best Practices " on page 210](#) for more information
- Some virtual machine software has security settings that conflict with CylancePROTECT's Memory Protection feature. This conflict may result in an unresponsive virtual machine. If this happens, it is recommended to either disable the Memory Protection feature or use different virtual machine software.

Enable Submitting Helpdesk Tickets

Add a menu item to the Agent UI to submit a ticket to your internal helpdesk for a threat. The ticket is sent using the default web browser.

Prerequisites

- Agent version 1300 and higher
- URL with an HTTP GET request (for submitting tickets)

Create a Custom Action

1. On the device, open the Registry Editor.
Note: Self Protection might need to be disabled to perform this step.
2. Navigate to the Cylance Desktop folder.
HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
3. Right-click inside the Registry Editor, then select **New > String Value**. A new string value is added to the registry.
4. Type CustomThreatActionDesc to name the value, then press **Enter**. This renames the value.
5. Double-click **CustomThreatActionDesc**, type a message to display and then click **OK**. This message displays when users right-click a threat in the Agent UI. Example: Submit Helpdesk Ticket.
6. Right-click inside the Registry Editor, select **New > String Value**, type CustomThreatActionURL, then press **Enter**.
7. Double-click **CustomThreatActionURL**, type the URL to which you wish to send the ticket information, then click **OK**.
8. Exit and restart the Agent UI.

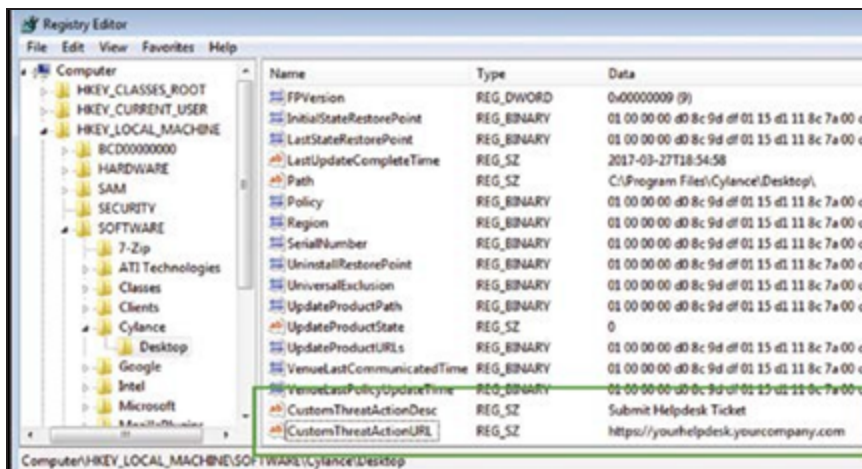


Figure 27: Add a Custom Action

URL Structure

The URL accepts four tokens which are substituted with the values associated with the threat.

- **CY_THREAT:** The SHA256 of the threat.
- **CY_PATH:** The path (location) where the file was found.

Example: C:\Temp\malware\thisisthemalware.exe.

- **CY_SCORE:** The Cylance Score assigned to the threat. A score from 60 to 100 is considered Unsafe. A score from 1 to 59 is considered Abnormal.
- **CY_STATE:** The state of the threat. Could be Unsafe, Abnormal, Waived, Safelisted, or Quarantined.
- **CY_MACHINENAME:** The name of the machine on which the threat was found.

Using the Action

1. On the device, click the Agent icon in the system tray.
2. Make sure the Threats tab is selected.
3. Right-click the threat for which you want to submit a ticket, then click the menu item to submit the ticket. The default web browser opens to the URL.

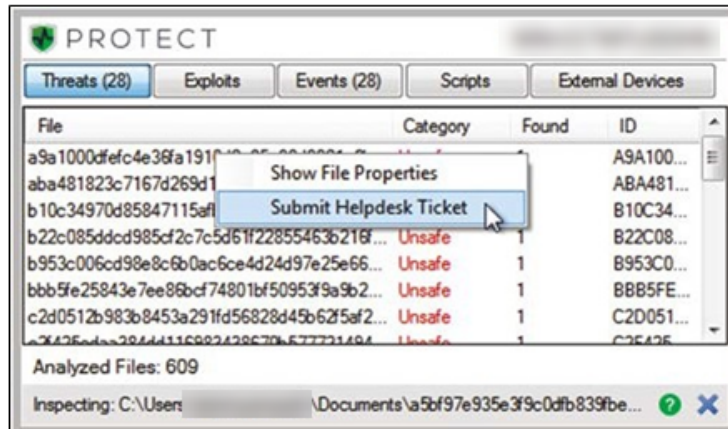


Figure 28: Submit a Ticket

Changing the Help / FAQ Link in the Agent UI

By default, the Help / FAQ link in the Agent user-interface takes you to the BlackBerry Cylance Support site. With Agent versions 1380 and higher, you can add a registry item to redirect this link to your own support site. This is helpful for organizations that want to use their own support or IT teams to field questions from their users before contacting BlackBerry Cylance Support.

1. On the device, right-click the Agent icon, then select **Exit**.
2. Stop the Cylance Service. While restarting the UI will load the new value, the service protects the registry from being changed, so the service must be stopped to set the new value. If **Prevent Service Shutdown** is enabled, you can't stop the service. You must

disable the **Prevent Service Shutdown** feature, create the help link, then re-enable the **Prevent Service Shutdown** feature.

3. Run the Registry Editor, then take ownership of the Cylance Desktop.
HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
4. Right-click inside the Registry Editor, then select **New > String Value**. A new string value is added to the registry.
5. Type CustomHelpFaqUrl to name the value, then press **Enter**. This renames the value
6. Double-click **CustomHelpFaqUrl**, type the URL for the help website, then click **OK**.
7. Exit, restart the Cylance Service, then restart the Agent UI.

DEVICE MANAGEMENT

Devices are computers with the CylancePROTECT Agent installed. Devices can be managed using the Console (web interface). This section outlines the options for managing Agents within the environment.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.


	NAME	STATE	AGENT VERSION	ZONES	POLICY	TARGET AGENT VERSION
<input type="checkbox"/>		Offline	2.1.1550 (updates available)	VEN-15751 - b	Default	2.1.1560
<input type="checkbox"/>		Offline	2.0.1460 (updates available)	VEN-15751 - b	DYLIB test	2.1.1560

Tip: Clicking the "select all" check box at the top of the list selects all entries on the displayed page. Entries on other pages in the list will not be selected.

1. Click **Devices** from the menu. A list of devices displays. You can search for a device name to filter the list in the Name field.
2. Select a device check box to enable the following actions:
 - **Remove:** Removes selected devices from the *Device List*. This does not uninstall the Agent from the device.

When a device is removed, it is unregistered and no longer communicates with the Console. On the device, the unregistered Agent displays a message that the installation token is required. Uninstall the Agent to remove it from the endpoint, or reapply the installation token to re-register the Agent with the Console.
 - **Assign Policy:** Allows assignment of the selected devices to a policy.
 - **Add to Zones:** Allows adding the selected devices to a Zone or Zones.
3. Click a device to display the Device Details page.
 - **Device information:** Displays information such as Hostname, Agent Version, Operating System Version.
 - **Device Properties:** Allows changing the Device Name, Policy, Zones, and Logging Level.

- **Threats & Activities:** Displays threat information and other activities related to the device. For more information, see "[Device Threats & Activities](#)" below.
4. Click **Add new device** to open a dialog or the Deployments page where you can select a product to download. For more information, see "[Download the Install File](#)" on [page 59](#).
 5. In the Zones column, click a Zone Name to display the Zone Details page.

Tip: Click  to download a CSV file of the list. The file contains device information (Name, State, and Policy) for all devices in the organization. Note that the Target Agent Version column is not included in the exported list.

Device Threats & Activities

Displays threat information and other activities related to the selected device.

Threats

Displays all threats found on the device. By default, the threats are grouped by status (*Unsafe*, *Abnormal*, *Quarantined*, and *Waived*).

- **Export:** Creates and downloads a CSV file that contains information for all threats found on the selected device. Threat information includes: Name, File Path, Cylance Score, and Status).
- **Quarantine:** *Quarantines* the selected threats. This is a *Local Quarantine*, meaning this threat is only *Quarantined* on this device. When quarantining a threat, a message displays and a reason is required when confirming the quarantine.

To *Quarantine* a threat for all devices in the organization, ensure that the **Also, quarantine this threat any time it is found on any device** check box is selected.

This option places the threat on the *Global Quarantine* list, which is applied to all devices in the organization, not just the affected device.

- **Waive:** Changes the status of the selected threats to *Waived*. A *Waived* file is allowed to run. This is a *Local Waive*, meaning this file is only allowed on this device.

To allow this file on all devices in the organization, select the **Also, mark as safe on all devices** check box (*Safe List*) when Waiving a file. This option places the file on the *Global Safelist*, which is applied to all devices in the organization, not just the selected device.

Exploit Attempts

Displays all exploit attempts on the device. This includes information about the Process Name, ID, Type, and Action taken.

Application Control

Displays all activities relevant to Application Control, like denied file changes. Application Control activities are also displayed in the Agent user interface, on the Events tab.

Agent Logs

Displays log files uploaded by the Agent on the device. The log file name is the date of the log.

To view Agent log files:

1. Upload the Current Log File for a single device.
 - a. Click **Devices > Agent Logs**.
 - b. Click **Upload Current Log File**. This could take a few minutes, depending on the size of the log file.

OR

Policy settings:

- a. Click **Settings > Device Policy > [select a policy] > Agent Logs**.
- b. Click **Enable auto-upload of log files**.
- c. Click **Save**.

To view verbose logs, change the Agent Logging Level before uploading any log files.

1. In the Console: **Devices > [click a device]**, select **Verbose** from the Agent Logging Level drop-down menu, and click **Save**. After the verbose log files are uploaded, make sure you change the Agent Logging Level back to *Information*.
2. On the device, close the CylancePROTECT user interface (right-click the CylancePROTECT icon in the system tray, then click **Exit**).

OR

Open the Command Line as an Administrator. Enter the following command and then press **Enter**.

```
cd C:\Program Files\Cylance\Desktop
```

3. Enter the following command and then press **Enter**.

CylanceUI.exe -a

4. The CylancePROTECT icon appears in the system tray. Right-click, select **Logging**, then click **All** (same as Verbose in the Console).

Note: Agent Log files are retained for 30 days in the Console.

Script Control

Displays all activities relevant to Script Control, such as denied scripts. This list includes the date/time of the event, the file path, and the action taken.

Note: When filtering on the Drive Type values, RAM is the RAM disk (Virtual drive in memory), and Internal Hard Drive is an internal disk drive.

External Devices

Displays a log of all external devices if Device Control is enabled in the ["Device Policy" on page 17](#).

Add an Exclusion

Notes:

- Adding an exclusion that contains underscores in the serial number is currently not supported on the Device Details page. You must add the exclusion via the Device Policy instead.
- Adding an exclusion from the Device Details page affects the policy currently assigned to the device, not the policy that was assigned when the Device Control event occurred.

To Add an Exclusion

1. Click **Devices**.
2. Click a **device**.
3. Under Threats & Activities, click the **External Devices** tab.
4. From the list, click the Add as Policy Exclusion icon (plus symbol). The Add as Policy Exclusion window displays. The Policy name and Vendor ID display as part of the exclusion. The Product ID and Serial Number also display, if available.

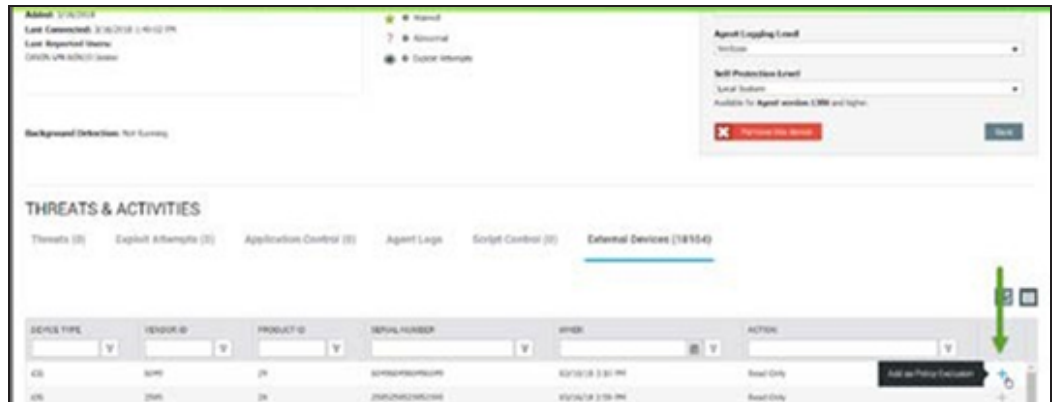


Figure 29: Device Details > Threats & Activities > External Devices

5. Select the Access for the exclusion. Full Access allows the USB mass storage device to connect to the endpoint. Block does not allow the storage device to connect to the endpoint.
6. Optionally, type a comment for this exclusion.
7. Click **Save Exclusion**. The Device Control exclusion is added to the assigned policy.

Duplicate Devices

When the CylancePROTECT Agent is first installed on a device, a unique identifier is created that is used by the Console to identify and reference that device. However, certain events, such as using a virtual machine image to create multiple systems, may cause a second identifier to be generated for the same device. Select the device and click **Remove** if a duplicate entry displays on the Devices page in the Console,

To aid in identifying such devices, use the column sorting feature on the Devices page to sort and compare the devices, typically by device name. Alternately, the *Devices List* can be exported as a .CSV file and then viewed in Microsoft Excel or something similar which has powerful sorting/ organizing features.

Example Using Microsoft Excel

1. Open the device CSV file in Microsoft Excel.
2. Select the device name column.
3. From the Home tab, select **Conditional Formatting > Highlight Cell Rules > Duplicate Values**.
4. Ensure that **Duplicate** is selected, then select a highlight option.
5. Click **OK**. Duplicate items are highlighted.

Note: The Remove command only removes the device from the Device page. This will not issue an uninstall command to the CylancePROTECT Agent. The Agent needs to be uninstalled at the endpoint.

THREAT MANAGEMENT

Dashboard

The Dashboard page displays once logged in to the CylancePROTECT Console. The Dashboard provides an overview of threats in the environment and provides access to different Console information from one page.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

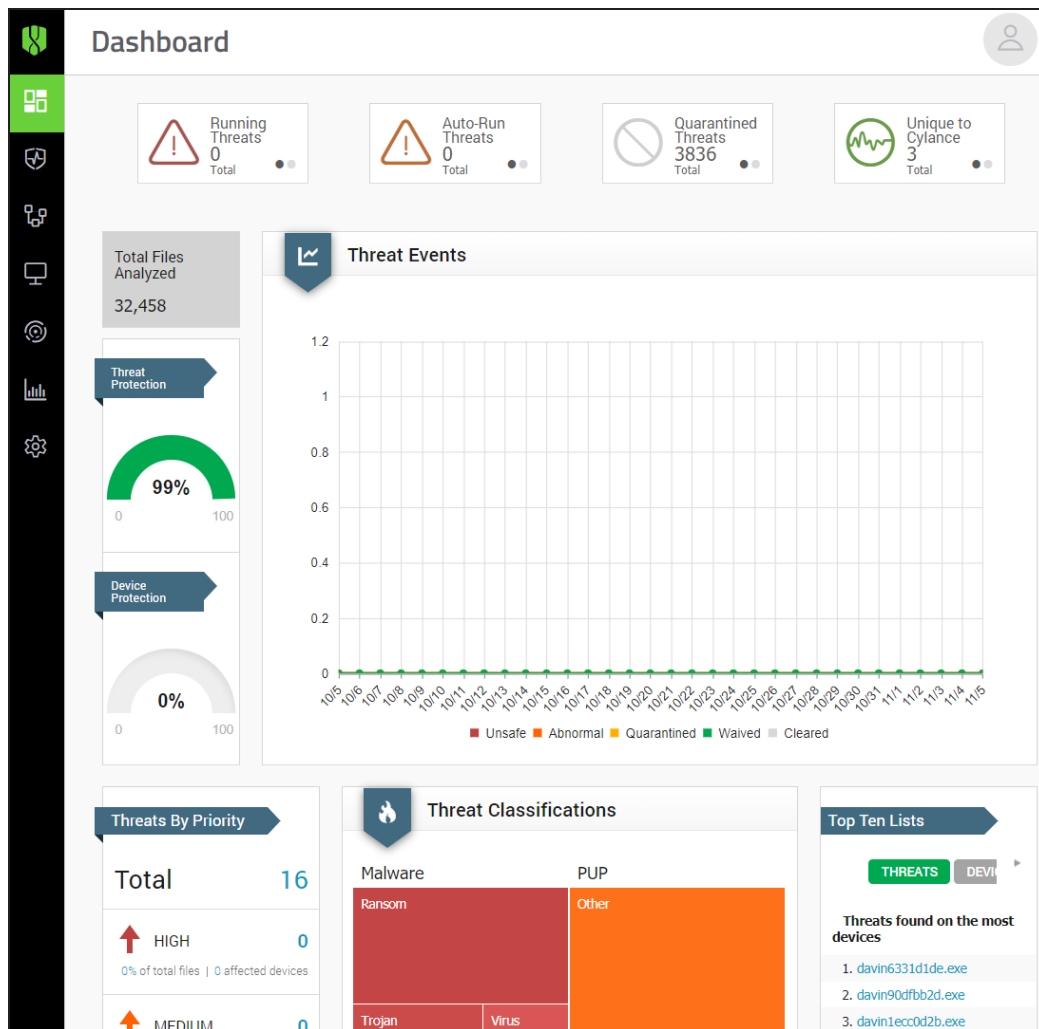


Figure 30: CylancePROTECT Dashboard

Threat Statistics

Threat Statistics provide the number of threats found within the *Last 24 Hours* and the *Total* for the organization. Click a *Threat Statistic* to go to the Protection page and display the list of threats related to that statistic.

- **Running Threats:** Files identified as threats that are currently running on devices in the organization.
- **Auto-Run Threats:** Threats set to run automatically.
- **Quarantined Threats:** Threats quarantined within the last 24 hours and the total.
- **Unique to Cylance:** Threats identified by Cylance but not by other antivirus sources.

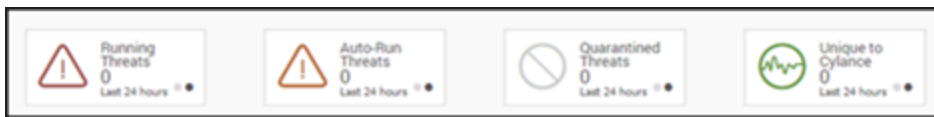


Figure 31: Threat Statistics

Protection Percentages

Displays percentages for Threat Protection and Device Protection.

- **Threat Protection:** The percentage of threats on which you have taken action (Quarantine, Global Quarantine, Waive, and Safe Lists).
- **Device Protection:** On the Dashboard, the Device Protection percentage meter displays how many devices are in a Policy with both Unsafe and Abnormal set to Auto-Quarantine (Policy > File Actions). If one or both of these settings are disabled, then the device is considered unprotected when calculating the Device Protection percentage. The Device Protection percentage meter displays a percentage for all devices in the organization.

Threats by Priority

This list displays the total number of threats that have not been acted upon and require more attention. Actions on threats include: *Quarantine*, *Global Quarantine*, *Waive*, and *Safe List*. The threats are grouped by priority (High, Medium and Low). This overview displays the total number of threats that require an action, separates that total by priority, provides a percentage total, and how many devices are affected.

Threats are listed by priority in the lower left corner of the Dashboard page. Specified are the total number of threats in an organization grouped by their priority classifications.

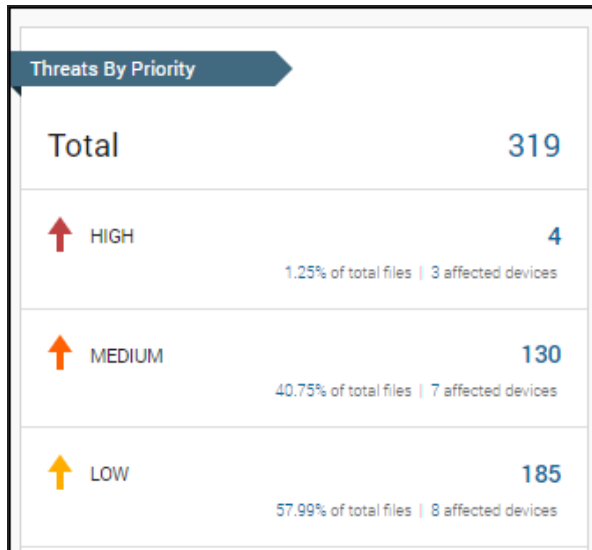


Figure 32: Dashboard Threats by Priority Section

A threat is classified as Low, Medium, or High based on the number of the following attributes it has:

- The file has a Cylance score greater than 80.
- The file is currently running.
- The file has previously been run.
- The file is set to auto run (attempts to maintain persistence or survive a reboot).
- The priority of the Zone where the threat was found.
- The file was detected by Execution Control.

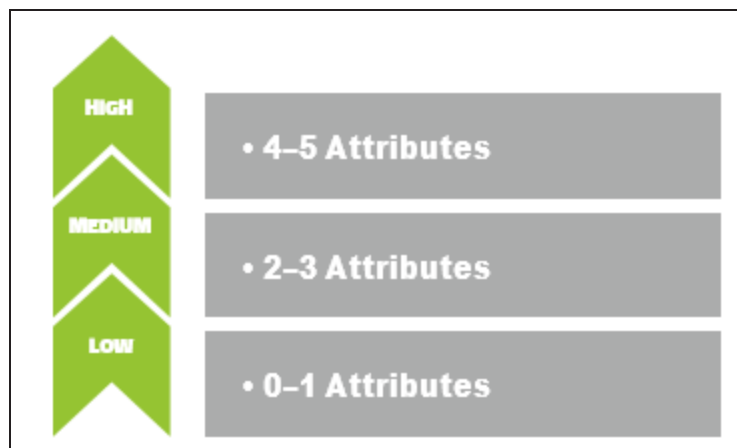


Figure 33: Threat Classifications

This classification helps Administrators determine which threats and devices to address first. Click either the threat information or affected devices to view threat and Device details. The following examples show how three threats are scored:

Example Threat 1

Attribute	Attribute Value	Score
Score	90	+1
Currently running on any device	True	+1
Ever run on any device	True	+1
Set to Auto run on any device	True	+1
Is found in any "high" criticality Zone	True	+1
Detected by Execution Control	False	+0
Total Score:		5: High Priority

Example Threat 2

Attribute	Attribute Value	Score
Score	65	+0
Currently running on any device	True	+1
Ever run on any device	False	+0
Set to Auto run on any device	True	+1
Is found in any "high" criticality Zone	False	+0
Detected by Execution Control	False	+0
Total Score:		2: Medium Priority

Example Threat 3

Attribute	Attribute Value	Score
Score	20	+0
Currently running on any device	False	+0
Ever run on any device	False	+0
Set to Auto run on any device	False	+0
Is found in any "high" criticality Zone	False	+0
Detected by Execution Control	True	+5
Total Score:		5: High Priority

Although Example Threat 3 has a total attribute score of "5", it would not be displayed under the Threats by Priority in any priority. This is because the Cylance score is "20" or abnormal. Only unsafe files are displayed under the Threats by Priority.

Threats can be detected by one of the following:

- Background Threat Detection - This is the File System Scanner. It runs in the background at low priority scanning the file system for files that contain threats. Threats "resting" on the file system represent the lowest priority, since they would be blocked if attempted to be executed.
- File Watcher - The File Watcher detects changes in the host's file system (file copy, move, etc.), and initiates a check of the new/modified files. Threats discovered here would represent a higher priority since they could be a payload arriving through some other normal activity, such as clicking on a link in a document or web page, running a malware delivery application that in and of itself is safe, etc.
- Execution Control - Threats discovered by Execution Control would represent the most significant threat to a system, as they were detected when attempting to actually be run. They could be malicious applications masquerading as legitimate applications that trick a user into running, processes being launched by another "safe" process, etc. They represent threats that are actively attempting to be exploited. Threats detected by Execution Control are automatically classified as a "High" priority threat.

Threat Events

Displays a line graph with the number of threats discovered over the last 30 days. Lines are color-coded for *Unsafe*, *Abnormal*, *Quarantined*, *Waived*, and *Cleared* files.

- Hover over a point on the graph to view the details.
- Click one of the colors in the legend to show or hide that line.

Threat Classifications

Displays a heat map of the types of threats found in the organization, such as viruses or malware. Click an item in the heat map to go to the Protection page and display a list of threats of that type.

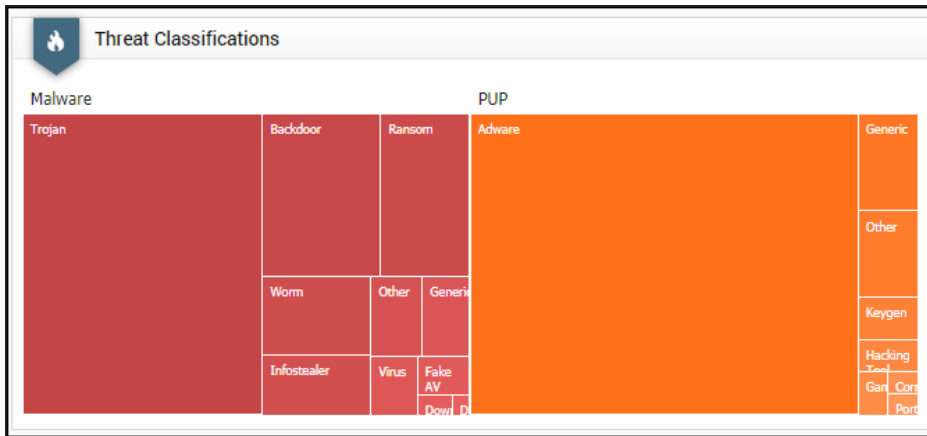


Figure 34: Dashboard Threat Classifications Section

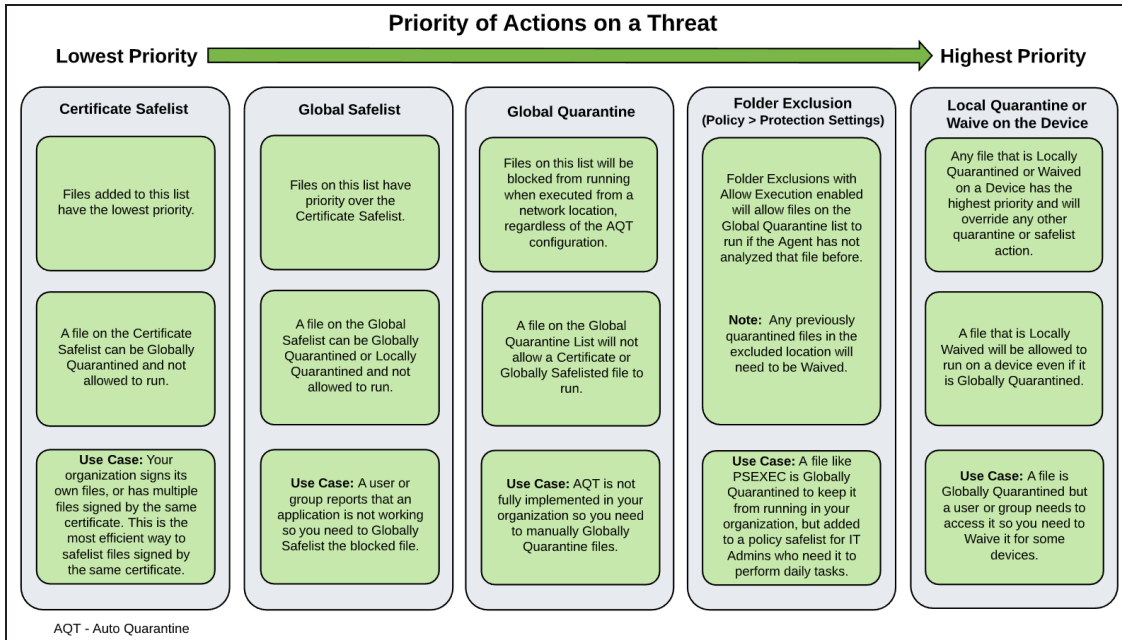
Top Ten Lists

Displays lists for the Top Ten Threats found on the most devices, the Top Ten Devices with the most threats, and the Top Ten Zones with the most threats in the organization. Click a list item for more details.

The Top Ten lists on the dashboard highlight *Unsafe* Threats in the organization that have not been acted upon, such as *Quarantined* or *Waived*. Most of the time these lists should be empty. While *Abnormal* Threats should also be acted upon, the focus of the Top Ten lists is to bring critical threats to your attention.

Priority of Threat Actions

The following image shows the priority of actions when quarantining or safelisting a file.



Threat Protection

CylancePROTECT can do more than simply classify files as *Unsafe* or *Abnormal*. It can provide details on the static and dynamic characteristics of files. This allows administrators to not only block threats, but to understand threat behavior to further mitigate or respond to threats.

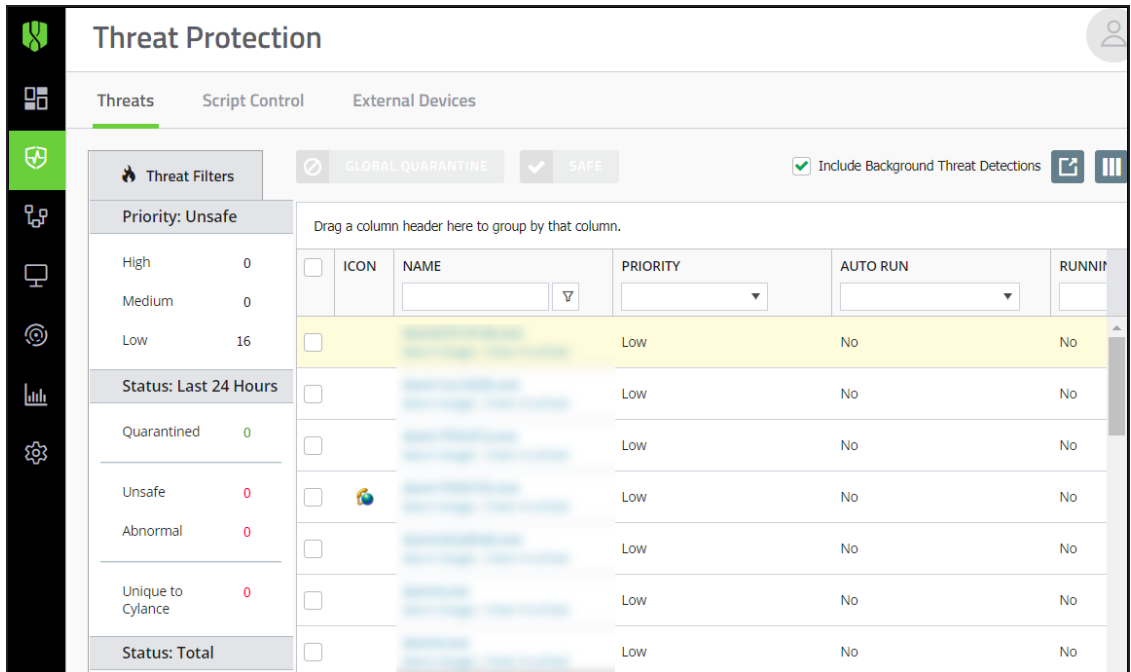


Figure 35: Threat Protection Page

Unsafe and Abnormal Files

Unsafe: A file with a score ranging from 60-100. An *Unsafe* file is one that the Cylance Cloud finds attributes that greatly resemble malware.

Abnormal: A file with a score ranging from 1-59. An Abnormal file has a few malware attributes but less than an *Unsafe* file, thus is less likely to be malware.

Note: Occasionally, a file may be classified as *Unsafe* or *Abnormal* even though the score displayed does not match the range for the classification. This could result from updated findings or additional file analysis after the initial detection. For the most up-to-date analysis, enable Auto Upload in the Device Policy.

Cylance Score

Represents the confidence level that the file poses a real danger to your environment. The higher the score, the greater the confidence level that the file can be used for malicious purposes. Based on the score, threats are considered either unsafe or abnormal.

Files with a score that are identified as a potential threat will have a **red** score (unsafe or abnormal). Files with a score that are identified as safe will have a **green** score. Under normal circumstances you will not see safe (green) files displayed in the console. Safe files that are shown in the Console are typically displayed when the file has been added to your global quarantine list and quarantined on a device.

Files that would be considered unsafe/abnormal (red score) are treated as safe if you add the files to your global safe list and will not be displayed in the Console.

Note: Review the following:

- Occasionally, a file may be classified as either unsafe or abnormal even if the score displayed doesn't match the range for the score. This may be due to update findings or additional file analysis that may have been performed after the initial detection. For the most up-to-date threat analysis, enable Auto Upload in the policy.
- The Cylance Score is independent of Threat Classification. Most Threat Classifications are a manual process that is undertaken by a human threat researcher and assigned on a file by file basis. It is possible for a file to have a Cylance Score but not have a classification until a later date.

File Classification

Below is a list of possible file status entries that may appear under classification for each threat along with a brief description of each entry:

File Unavailable

Due to an upload constraint (example: file is too large to upload) the file is unavailable for analysis. If classification is necessary, please contact Cylance support for an alternate method to transfer the file for analysis.

UNKNOWN (Blank Entry)

The file has not been analyzed by Cylance's analysis team yet. Once the file is analyzed, the classification will be updated with a new status.

Trusted - Local

The file has been analyzed by the Cylance research team and has been deemed safe (not malicious, not a PUP). A file identified as Trusted - Local can be globally safelisted so that the file will be allowed to execute and not generate any additional alerts if found on other devices within your organization. The reason for the 'Local' designation is due to the fact that the file did not come from a trusted source (such as Microsoft or other trusted installer) and therefore cannot be added to our trusted cloud repository.

PUP

The file has been identified as a Potentially Unwanted Program. This indicates that the program may be unwanted, despite the possibility that users consented to download it. Some PUPs may be permitted to run on a limited set of systems in your organization (EX. A VNC application allowed to run on Domain Admin devices). A Console Admin can choose to waive or block PUPs on a per device basis or globally quarantine or safelist based on company policies. Depending

on how much analysis can be performed against a PUP, further subclassification may be possible. Those subclasses are shown below and will aid an Admin in determining whether a particular PUP should be blocked or allowed to run:

Subclass	Definition	Examples
Adware	Technologies that provide annoying advertisements (example: pop-ups) 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
Corrupt	Any executable that is malformed and unable to run.	
Game	Technologies that create an interactive environment with which a player can play.	Steam, Games, League of Legends
Generic	Any PUP that does not fit into an existing category.	
Hacking Tool	Technologies that are designed to assist hacking attempts.	Cobalt, Strike, MetaSp0it
Portable Application	Program designed to run on a computer independently, without needing installation.	Turbo
Scripting Tool	Any script that is able to run as if it were an executable.	AutoIT, py2exe
Toolbar	Technologies that place additional buttons or input boxes on-screen within a UI.	Nasdaq Toolbar, Bring Me Sports
Other	Is a category for things that don't fit anything else, but are still PUPs. There a lot of different PUPs, most of which aren't malicious but several that 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 indicates the file can be used for malicious and non-malicious purposes. Caution should be used when allowing the use of these files in your organization. For example, while PsExec can be a useful tool for executing processes on another system, that same benefit can be used to execute malicious files on another system.

Subclass	Definition	Examples
Crack	Technologies that can alter (or crack) another application to	

Subclass	Definition	Examples
	bypass licensing limitations or Digital Rights Management protection (DRM).	
Generic	Any Dual Use tool that does not fit into an existing category.	
KeyGen	Technologies which can generate or recover/reveal product keys that can be used to bypass Digital Rights Management (DRM) or licensing protection of software and other digital media.	
Monitoring Tool	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"> ■ user keystrokes ■ email messages ■ chat and instant messaging ■ web browsing activity ■ screenshot captures ■ application usage 	Veriato 360, Refog Keylogger
Pass Crack	Technologies that can reveal a password or other sensitive user credentials either by cryptographically reversing passwords or by revealing stored passwords.	l0phtcrack, Cain & Abel
RemoteAccess	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
Tool	Programs that offer administrative features but can be used to facilitate attacks or intrusions.	Nmap, Nessus, P0f

Malware

The Cylance research team has definitively identified the file as a piece of malware, the file should be removed or quarantined as soon as possible. Verified malware can be further subclassified as one of the following:

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.	

Subclass	Definition	Examples
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
Parasitic	Parasitic viruses, also known as file viruses, spread by attaching themselves to programs. Typically when you start a program infected with a parasitic virus, the virus code is run. To hide itself, the virus then passes control back to the original program.	
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.	Salinity, Virut
Worm	Malware that propagates by copying itself to another device.	Code Red, Stuxnet

View Threat Information

The Protection page on the Console displays high-level threat information that you can drill-down to learn more about a threat.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Tip: Clicking the "select all" check box at the top of the list selects all entries on the displayed page. Entries on other pages in the list will not be selected.

To View Threats

1. Click **Protection** from the menu to display a list of threats found in the organization.
2. To hide Background Threat Detections from the list, uncheck the **Include Background**

Threat Detections check box. By hiding Background Threat Detection events, you can quickly review events that were detected due to execution control, running module scans, or watch for new files versus a background scan.

Note: If you hide Background Threat Detection events, the filter option will also be removed from the Detected By column's drop-down list. The option is added to the drop-down list when Include Background Threat Detections are enabled (check box is selected).

3. Use the filter on the left menu bar to filter by Priority (high, medium, or low) and Status (*Quarantined*, *Waived*, *Unsafe*, or *Abnormal*).

Note: Numbers that are displayed in red on the left pane indicate outstanding threats that have not been *Quarantined* or *Waived*. Filter on those items to view a list of files that need to be examined.

🔥 Threat Filters	
Priority: Unsafe	
High	0
Medium	0
Low	16
Status: Last 24 Hours	
Quarantined	0
Unsafe	0
Abnormal	0
Unique to Cylance	0
Status: Total	
Global Quarantined	2
Quarantined	3837
Waived	0
Unsafe	16
Abnormal	0
Unique to Cylance	9

Unsafe or abnormal threats that have not been quarantined or waived, and were detected in the last 24 hours.

Unsafe or Abnormal threats that have not been quarantined or waived.

Figure 36: Protection Page Threat Filters

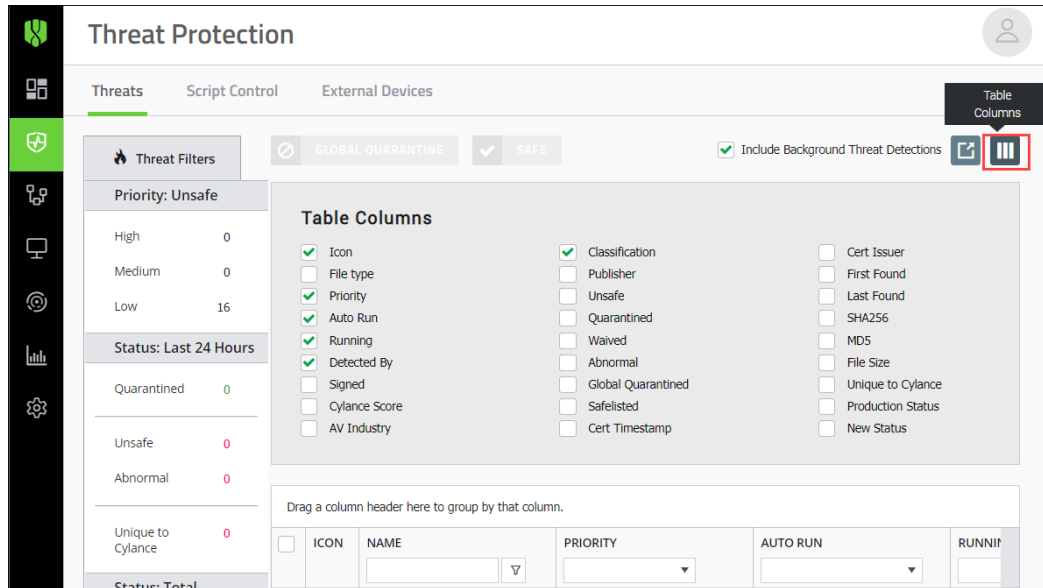


Figure 37: Protection Page Threat Information

4. To add columns so additional threat information can be viewed, click the down arrow next to one of the column names, then select a column name.
5. To view details for a threat, click the threat link to open details on a page where you can quarantine or waive the threat.

OR

To view details at the bottom of the page without access to quarantine or waive the file, click anywhere in the threat's row.

Both views show the same content but have different presentation styles. For more information, see ["Threat Details" on the next page.](#)

Save a Filter

After you have filtered for the threats you want to view, you can save these filters by bookmarking the page. The table columns selected and the filters applied creates a unique URL in the Console. Bookmarking the results page and then opening that bookmark later will apply the same columns and filters to the latest threat data.

You can share your saved filters by sharing the bookmark with other Console users in the organization. The results from using a filter might vary depending on the user role assigned to the user: Administrators can see everything in the Console, while Zone Managers and Users can only see the zones to which they are assigned (this includes devices and threats).

Threat Details

The Threat Details page provides details on the static and dynamic characteristics of files. This allows administrators to not only block threats, but to understand threat behavior to further mitigate or respond to threats.

Threat details are aggregated by the SHA256 hash and include the following information:

- File Metadata
 - Classification (assigned by the Cylance Advanced Threat and Alert Management (ATAM) Team)
 - Cylance score (confidence level)
 - AV Industry conviction (links to VirusTotal.com for comparison to other vendors)
 - Date first found, Date last found
 - SHA256
 - MD5
 - File Information (author, description, version, and so forth)
 - Signature Details
- Devices - The *Device/Zone* List for a threat can be filtered by the threat's state (*Unsafe*, *Quarantined*, *Waived*, and *Abnormal*). Click the state filter links to show the devices with the threat in that state.
 - **Unsafe:** The file is classified as *Unsafe*, but no action has been taken.
 - **Quarantined:** The file was already *Quarantined* due to a policy setting.
 - **Waived:** The file was *Waived* or *White Listed* by the Administrator.
 - **Abnormal:** The file is classified as *Abnormal*, but no action has been taken.
- Evidence Reports
 - **Threat Indicators:** Observations about a file that the Cylance Cloud has analyzed. These indicators help understand the reason for a file's classification and provide insight into a file's attributes and behavior. Threat Indicators are grouped into categories to aid in context.
 - **Detailed Threat Data:** Detailed Threat Data provides a comprehensive summary of the static and dynamic characteristics of a file, including additional file metadata, file structure details, and dynamic behaviors such as files dropped, registry keys created or modified, and URLs with that it attempted to communicate with.

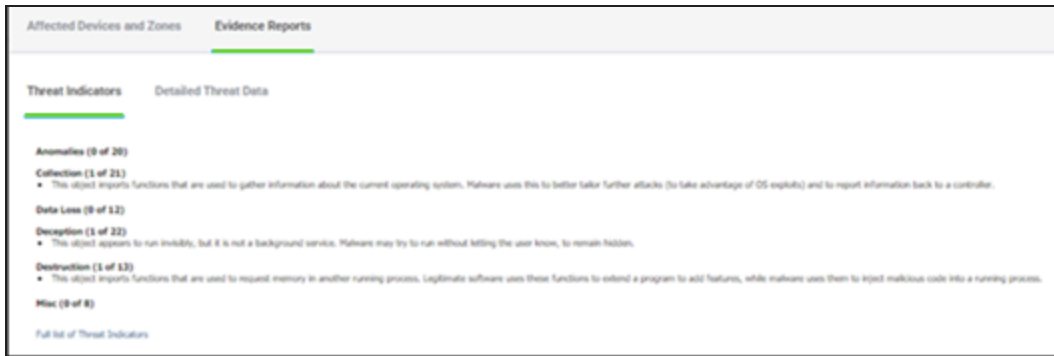


Figure 38: Threat Indicators

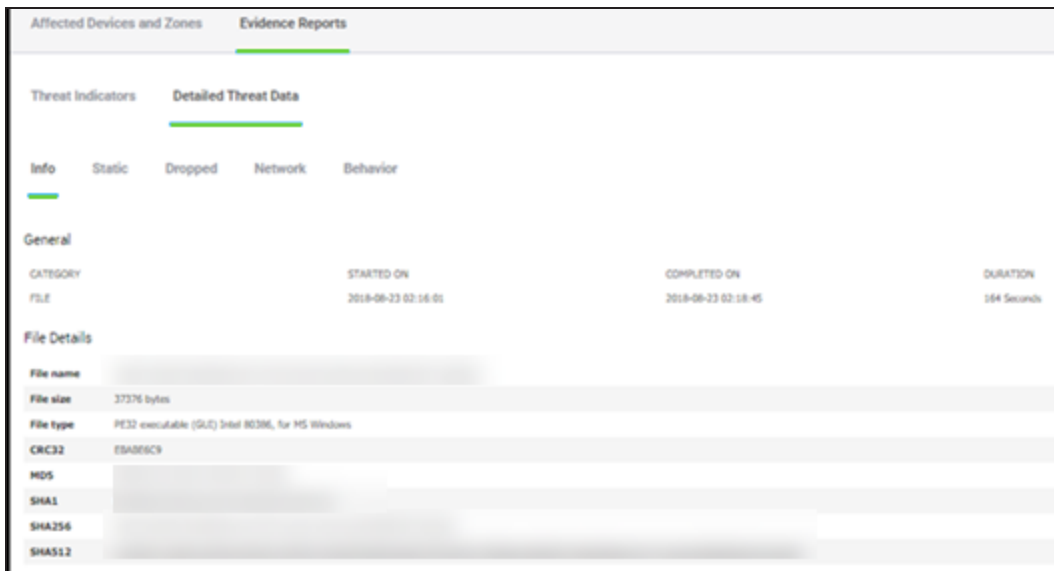


Figure 39: Detailed Threat Data

View Threat Indicators

1. Click **Protection** in the menu. The Threat Protection page opens to the Threats tab.
2. In the Threats table, click a threat to open the Threat Details page.
3. In the bottom section of the page, click the **Evidence Reports** tab.
4. Review the Threat Indicators (see category descriptions below) and Detailed Threat Data tabs.

Threat Indicator Categories

Each category represents an area that has been frequently seen in malicious software and is based on deep analysis of over 100 million binaries. The Threat Indicators report indicates how many of those categories were present in the file.

- Anomalies (20 indicators) – The file has elements that are inconsistent or anomalous in some way. Frequently, they are inconsistencies in the structure of the file.
- Collection (21 indicators) – The file has evidence of data collection. This can include enumeration of device configuration or collection of sensitive information.
- Data Loss (12 indicators) – The file has evidence of data exfiltration. This can include outgoing network connections, evidence of acting as a browser, or other network communications.
- Deception (22 indicators) – The file has evidence of attempts to deceive. Deception can be in the form of hidden sections, inclusion of code to avoid detection, or indications of improper labeling in metadata or other sections.
- Destruction (13 indicators) – The file has evidence of destructive capabilities. Destruction includes the ability to delete device resources such as files and directories.
- Miscellaneous (8 indicators) – All other indicators that do not fit into other categories.

Note: Occasionally, the Threat Indicators and Detailed Threat Data sections have no results or are not available. This happens when the file has not been uploaded. Debug logging may provide insight as to why the file was not uploaded.

Indicators

Category	Name	Description
Anomalies	16bitSubsystem	This object utilizes the Windows 16-bit subsystem, a less secure and less monitored part of the operating system. This subsystem is intended for running older software (MS-DOS) on newer operating systems; modern software rarely requires it. Malware typically takes advantage of the 16-bit subsystem to exploit security flaws in the subsystem and gain additional privileges.
Anomalies	Anachronism	Compiled executables typically include a 4-byte value which represents the time and date the executable was compiled on. Professionally written software has little reason to modify this timestamp value; however, an attacker could modify this value so an executable would appear to be compiled in the future or past. Note: Borland Delphi uses a static value for all compiled executables.

Category	Name	Description
Anomalies	AppendData	This portable executable (PE) file has some extra content appended to it, beyond the normal areas of the file. With legitimate files, appending (or adding) data to an executable file allows a software company to include data with their program instead of needing separate data files. But appended data can frequently be used to embed malicious code or data and is often overlooked by protection systems.
Anomalies	Base64Alphabet	This object contains evidence of using Base64 encoding. Base64 is an encoding scheme used to represent data as ASCII text typically consisting of A-Z, a-z, 0-9, +, and /. Malware often uses Base64 to avoid detection. For example, the suspicious data "thisisabot" can be concealed by encoding it as "dGhpc2lzYWJvdA==" using Base64.
Anomalies	CommandlineArgsImport	This object imports functions that can be used to read arguments from a command line and malware can use this to collect information. Command line arguments are parameters passed to the program, like opening a specific file or using values. Some organizations may even pass usernames and passwords with a command like net use.
Anomalies	ManifestMismatch	This object appears to have inconsistencies in its manifest, a file containing metadata about the object. This metadata includes any relationship and dependencies with other components, version information, and security permissions required by the assembly. Malware creators might manipulate this metadata to avoid detection or directly copy the manifest of a legitimate file into their executable.
Anomalies	NontrivialDLLEP	This object is a DLL with a nontrivial (critical) entry point. Entry points are common among DLLs, but a malicious DLL may use its entry point to place itself inside a process. An entry point is where control goes from the operating system to the program, at which point the program is executed.
Anomalies	PossibleBAT	This object contains evidence of having a standard Windows batch file included. Legitimate programs rarely have a reason to include a batch script alongside of the program. Malware creators will often do this to avoid common antivirus scanning techniques. Some malware will commonly use a batch file to hide specific actions within the file, like containing commands to execute another command, execute another malicious program, or delete itself after execution.

Category	Name	Description
Anomalies	PossibleDinkumware	This object shows evidence of including some components from Dinkumware. Dinkumware is frequently used in various malware components; however, it also has legitimate uses and provides C++ libraries that ship with Microsoft Visual C++.
Anomalies	RaiseExceptionImports	This object imports functions used to raise exceptions within a program. Malware does this to make standard dynamic code analysis difficult to follow. Example: Malware might be designed to set up a custom exception handler, raise an exception, and then check if the custom exception handler catches it. If no exception is caught, the malware knows a debugger probably caught the exception and that a debugger is being used.
Anomalies	ResourceAnomaly	This object contains malformed content or other unusual data in the resource section. The resource section of a PE or DLL typically contains icons, images, menus, and strings. Malware creators may embed malicious executables, malicious DLLs, obfuscated data, and/or other configuration data in the resource section.
Anomalies	RWXSection	This object may contain modifiable code and implies that the object was built using a non-standard compiler or was modified after it was originally built. While some organizations may create and use software built using these techniques, this is not the industry standard.
Anomalies	StringInvalid	The object contains an invalid string, which could be an attempt to conceal a suspicious string or craft the object to interfere with analysis. Example: The invalid string could be trying to hide a suspicious file by changing the file name slightly. "OKtoUse.dll" and "0KtoUse.dll" look similar, but the second DLL name uses a zero instead of the upper-case O.
Anomalies	StringTableNotTerminated	This object contains a malformed string table. This might indicate the file is corrupt or was crafted to interfere with identifying the object as malware. Example: Malware creators might store strings in an encrypted format to hide malicious functionality.
Anomalies	StringTruncated	The object appears to be missing some string information or contain partial strings. This might indicate the file is corrupt or was crafted to interfere with identifying the object as malware. Malware creators might encode the malicious strings to avoid detection and then decode those strings at run time.
Anomalies	SuspiciousPDataSection	This object is hiding something in the PDATA area and

Category	Name	Description
		it cannot be identified. The PDATA section is typically used to process runtime structures, but this particular object contains something else.
Anomalies	SuspiciousRelocSection	This object is hiding something in the RELOCATIONS area and it cannot be identified. The RELOCATIONS area is typically used for relocating particular symbols, but this particular object contains something else.
Anomalies	SymbolInvalid	This object contains an invalid symbol string. In programming, a symbol is a data type used to name variables and functions. Malware does this to conceal a suspicious string or craft the object to interfere with identifying it as malware.
Anomalies	SymbolTruncated	This object appears to be missing some symbol information. This might indicate the file is corrupt or was crafted to interfere with identifying the object as malware. In programming, a symbol is a data type used to name variables and functions. Malware might use symbol information to hide the actual address of a malicious function and instead just specify the function name.
Anomalies	VersionAnomaly	This object has issues with how it presents its version information. Malware typically strips, removes, or directly copies version information of another executable to avoid detection.
Collection	BrowserInfoTheft	This object might try to read passwords stored in a web browser's cache. Malware does this to collect username and password information to send back to the malware's creator(s).

Addressing Threats

Determining the type of action to take on some threats may depend on a device's assigned user. Actions applied to threats can be applied at the Device level or at a Global level. Below are the different actions that can be taken against detected threats or files:

- **Quarantine:** *Quarantine* a specific file to prevent the file from being executed on that device.
- **Global Quarantine:** *Global Quarantine* a file to prevent the file from being executed on any device across the entire organization.

Note: *Quarantine* a file to move the file from its original location to the *Quarantine* directory
(C:\ProgramData\Cylance\Desktop\q).

- **Waive:** Waive a specific file to allow that file to run on the device specified.
- **Safe:** Global Safe List a file to allow that file to run on any device across the entire organization.

Note: Occasionally, CylancePROTECT may *Quarantine* or report a “good” file (this could happen if the features of that file strongly resemble those of malicious files). *Waiving* or *Globally Safe Listing* the file can be useful in these instances.

- **Upload File:** Manually upload a file or analysis. If Auto-Upload is enabled, new files (ones that have not been analyzed by Cylance are automatically uploaded. If the file exists, then the Upload File button is unavailable (grayed out).
- **Download File:** Download a file for your own testing purposes. The user must be an Administrator. The threat must be detected using Agent version 1320 or higher.

Note: The file must be available in the Cylance Cloud and all three hashes (SHA256, SHA1 and MD5) must match between the Cylance Cloud and the Agent. If not, then the Download File button is not available.

Address Threats on a Specific Device

From the Protection Page:

1. Click **Protection** from the menu.
2. Click a threat in the list top open the Threat Details page.
3. At the bottom of the page, under Affected Devices and Zones, select one of the tabs.
4. Click the checkbox beside the device.

5. Click **Quarantine** or **Waive** (Safelist).

Threat Details:

quarantined by users in Cylance - Team [PM]
0% waived
0% abnormal

0% quarantined by all Cylance users
0% waived
0% abnormal

Classification:

First Found: 8/23/2018 2:12:49 AM
Last Found: 1/9/2020 2:01:28 AM

Company Name:
Copyright:
File Size: 195.5 KB

Signed: False
Signature Status:
Issuer:
Publisher:
Subject:
Timestamp:
Thumbprint:

Affected Devices and Zones Evidence Reports

Unsafe (3) Quarantined (0) Waived (0) Abnormal (0)

Unsafe Protected

QUARANTINE **WAIVE**

<input type="checkbox"/>	NAME	STATE	AGENT VERSION	FILE PATH	ZONES
<input checked="" type="checkbox"/>		Offline	2.0.1540		

From the Devices Page:

1. Click **Devices** from the menu.
2. Click a device in the list to open the Device Details page.
3. At the bottom of the page, under Threats & Activities, select the Threats tab.
4. Click the checkbox beside the threat.

5. Click **Quarantine** or **Waive**.

Device Details:

Lockdown Status: CylanceOPTICS 2.0 not installed

OS Versions: Microsoft Windows 10 Enterprise Evaluation

Added: 1/8/2020

Last Connected: 1/13/2020 2:22:36 AM

Last Reported Users:

Background Detection: Not Running

THREATS & ACTIVITIES

Threats (87) | Exploit Attempts (0) | Application Control (0) | Agent Logs | Script Contr

QUARANTINE **WAIVE**

Grouped By: Status

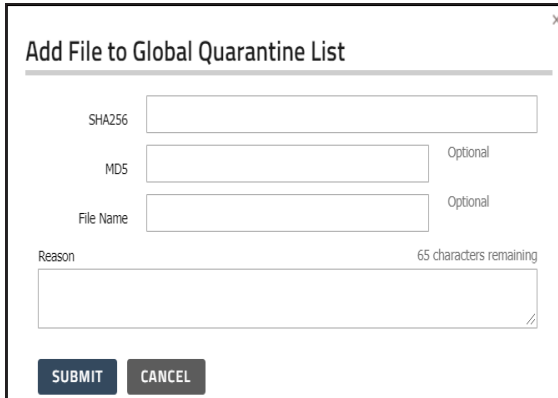
ICON	NAME	FOCUS VIEW	FILE PATHS	CYLANCE
✓	000ca5e53c5f470fbb240634ce1b13f8 Search Google Check VirusTotal	CylanceOPTICS 2.0 Not Installed		100

Address Threats Globally

Files added to the *Global Quarantine List* or *Global Safe List* are either *Quarantined* or the file is *Allowed* on all Devices across all Zones.

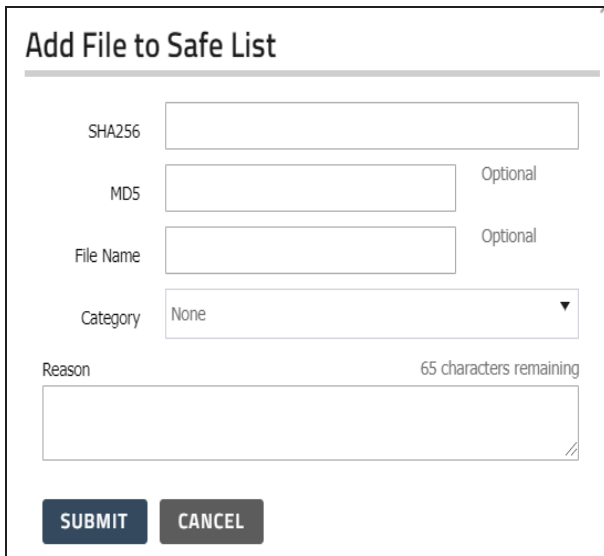
1. Click **Settings > Global List**.
2. Click **Global Quarantine** or **Safe**.
3. Click **Add File**.

4. Add the file's SHA256 (required), MD5, name, and the reason it's being placed on the *Global List*.
5. Click **Submit**.



The screenshot shows a web form titled "Add File to Global Quarantine List". It contains the following fields: a required text input for "SHA256"; an optional text input for "MD5"; an optional text input for "File Name"; and a text area for "Reason" with a "65 characters remaining" indicator. At the bottom, there are two buttons: "SUBMIT" and "CANCEL".

Figure 40: Global Quarantine List



The screenshot shows a web form titled "Add File to Safe List". It contains the following fields: a required text input for "SHA256"; an optional text input for "MD5"; an optional text input for "File Name"; a dropdown menu for "Category" currently set to "None"; and a text area for "Reason" with a "65 characters remaining" indicator. At the bottom, there are two buttons: "SUBMIT" and "CANCEL".

Figure 41: Global Safe List

Protection — Script Control

CylancePROTECT provides details about Active scripts, PowerShell scripts, and Microsoft Office macros that have been blocked or alerted upon. With Script Control enabled, the results display on the Script Control tab on the Protection page. This provides details about the script and the Devices affected.

To View Script Control Results

1. Click **Protection**.
2. Click **Script Control**.
3. Select a script in the table. This updates the Details table with a list of affected devices.

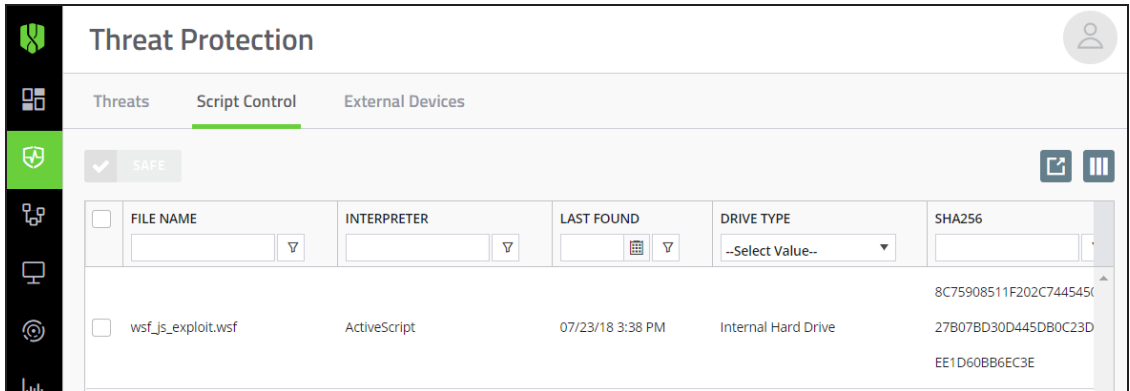


Figure 42: Script Tab — Protection Page

Script Control Column Descriptions

- **File Name:** The name of the script.
- **Interpreter:** The script control feature that identified the script.
- **Last Found:** The date and time the script was last run.
- **Drive Type:** The type of drive on which the script was found (example: Internal Hard Drive).
- **SHA256:** The SHA256 hash of the script.
- **# of Devices:** The number of devices affected by this script.
- **Alert:** The number of times the script has been alerted upon. This could be multiple times for the same device.
- **Block:** The number of times the script was blocked. This could be multiple times for the same device.

Details Column Descriptions

- **Device Name:** The name of the device affected by the script. Click the device name to go to the Device Details page.
- **State:** The state of the device (online or offline).
- **Agent Version:** The Agent version number currently installed on the device.

- **File Path:** The file path from which the script was executed.
- **When:** The date and time when the script was run.
- **Username:** The name of the logged in user when the script was run.
- **Action:** The action taken on the script (Alert or Block).

Protection — External Devices

You can view External Device logs on the Protection page.

Add an External Device Exclusion

To use this feature, Device Control must be enabled in the ["Device Policy" on page 17](#).

Notes:

- Adding an exclusion that contains underscores in the serial number is currently not supported on the Threat Protection page. You must add the exclusion via the Device Policy instead.
- Adding an exclusion from the Protection page affects the policy currently assigned to the device, not the policy that was assigned when the Device Control event occurred.

To Add an Exclusion

1. Click **Protection**.
2. Click **External Devices**.
3. Click the **Add as Policy Exclusion** icon (plus symbol).

The Add as Policy Exclusion window displays. The Policy name and Vendor ID display as part of the exclusion. The Product ID and Serial Number also display, if available.

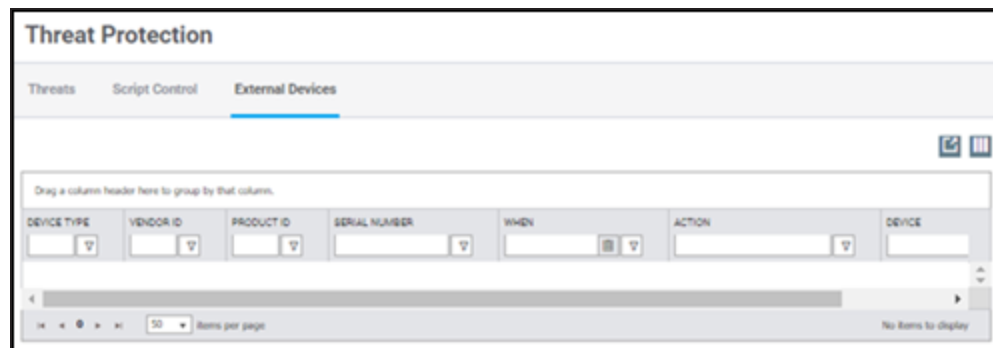


Figure 43: Protection > External Devices

4. Select the Access for the exclusion. **Full Access** allows the USB mass storage device to connect to the endpoint. **Block** does not allow the storage device to connect to the endpoint.
5. Optionally, type a comment for this exclusion.
6. Click **Save Exclusion**. The Device Control exclusion is added to the assigned policy

Global List

Global List allows a file to be marked for *Quarantine* or *Allow* those files on all devices in the organization.

- **Global Quarantine:** All Agents in the organization *Quarantine* any file on the *Global Quarantine List* that is discovered on the device.
IMPORTANT: Before quarantining a file, make sure it will not take down your servers or negatively impact your business.
- **Safe:** All Agents in the organization *Allow* any file on the *Safe List* that is discovered on the device.
- **Unassigned:** Any threat identified in the organization that is not assigned to either the *Global Quarantine* or *Safe List*.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Change Threat Status

To change a threat status (*Global Quarantine*, *Safe*, or *Unassigned*):

1. Select **Settings > Global List**.
2. Select the list to which the threat is assigned. For example, click *Unassigned* to change an unassigned threat to either *Safe* or *Global Quarantine*.
3. Select the check boxes for the threats to change, and click one of the following buttons.
 - a. **Safe:** Moves the files to the *Safe List*.
 - b. **Global Quarantine:** Moves the files to the *Global Quarantine List*.
 - c. **Remove from List:** Moves the files from the *Global Quarantine List* or *Safe list* to the *Unassigned List*. This button is not available for the *Unassigned list*.
Note: Removing all occurrences of the threat from your environment (removed from all devices and removed from all locations on a device) will remove it from the *Unassigned List*.

Add an Executable File

Manually add an executable file to the *Global Quarantine* or the *Safe List*. The SHA256 hash information for the file being added is required.

1. Select **Settings > Global List**.
2. Select the list to which to add the file (*Global Quarantine* or *Safe*).
3. Click **Add File**.
4. Enter the SHA256 hash information. Optionally, enter the MD5 and File Name information.
5. Enter a reason for adding this file.
6. Click **Submit**.

Add a Script File

Manually add a script file to the *Global Safe List*. The SHA256 hash information for the file being added is required.

Note: Adding a script to the Safe List will remove it from the Threat Protection page. If multiple scripts have the same SHA256 hash, all of those filenames will be removed from the list.

1. Select **Settings > Global List**.
2. Select **Safe**, then select **Scripts**.
3. Click **Add Script**.
4. Enter the SHA256 hash information. Optionally, enter the File Name.
5. Enter a reason for adding this file.
6. Click **Submit**.

Export a List

You can export a Global List to a CSV file.

1. Select **Settings > Global List**.
2. Select a list you want to export. You can filter the data before you export.
3. Click the **Export** icon.
4. Select **Everything** or **Current Filters**, then click **Export**.

Safe List Scripts by Hash

Administrators can add a script hash (SHA256), to the Global Safe List to allow these scripts to run in the organization. Safe Listing a script hash can be done on the Protection page or on the Global List page. This feature was introduced in Agent version 1470.

Note: Adding a script to the Safe List will *not* remove it from the Threat Protection page. To see if a script has been added to the Safe List, select Settings > Global List, then locate the script in the list.

Safelist Scripts from the Threat Protection Page

1. Select **Protection** from the menu, then click **Script Control**.
2. Select one or more scripts from the list.
3. Click **Safe**. The selected scripts are added to the Global Safe List.

Safelist Scripts from the Global List Page

1. Select **Settings > Global List**, click **Safe**, then click **Scripts**.
2. Click **Add Script**.
3. Enter the SHA256 hash, File Name (optional), and Reason for safelisting this hash.
4. Click **Submit**.

Safe List by Certificate

Customers have the ability to safe list files by signed certificate, which allows any custom software that is properly signed to run without interruption.

- This functionality allows customers to establish a *White List/Safe List* by signed certificate which is represented by the SHA1 thumbprint of the certificate.
- Certificate information is extracted by the Console (Timestamp, Subject, Issuer, and Thumbprint). The certificate is not uploaded or saved to the Console.
- The certificate timestamp represents when the certificate was created.
- The Console does not check if the certificate is current or expired.
- If the certificate changes (for example: renewed or new), it should be added to the Safe List in the Console.
- Safe List by Certificate for Script Control works with PowerShell, ActiveScript, and Office Macros.

Note: This feature currently works with Windows and macOS Operating Systems only.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Add the Certificate Details to the Certificate Repository

1. Identify the certificate thumbprint for the signed Portable Executable (PE).
2. Select **Settings > Certificates**.
3. Click **Add Certificate**.
4. Click either **Browse for certificates to add** or drag-and-drop the certificate to the message box. If browsing for the certificates, the Open window displays to allow selection of the certificates.
5. Optionally, you can select the file type the certificate **Applies to**, Executable, or Script. This allows you to safelist an executable or script by a certificate, instead of a folder location.
6. Optionally, add notes about this certificate.
7. Click **Submit**. The Issuer, Subject, Thumbprint, and Notes (if entered) are added to the repository.

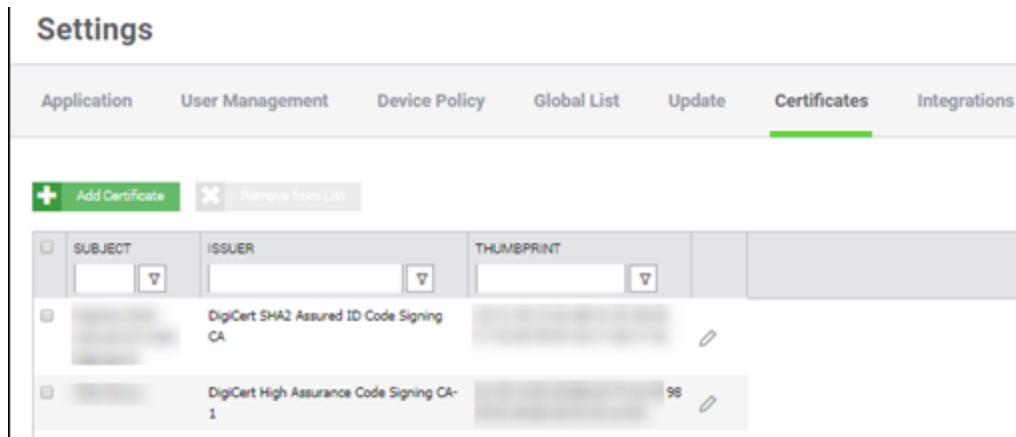


Figure 44: Certificate Repository

Viewing Thumbprints for a Threat

On the Protection tab, Threat Details now display the certificate thumbprint. From the screen, select **Add to Certificate** to add the certificate to the Repository.

Privileges

Add to Certificate is a function available to Administrators or custom roles with permissions only. If the certificate is already added to the Certificate Repository, the Console displays **Go to**

Certificate. Certificates are view-only by Zone Managers, who see the option **Go to Certificate**.

REPORTS

The Reports page in the Console offers Summary and Detail reports to provide overviews and details related to your devices and threats in the organization.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Reports display threats in an event-based manner. An event represents an individual instance of a threat. For example, if a particular file (specific hash) is located in three different folder locations on the same device, the threat event count will equal three. Other areas of the Console, such as the Threat Protection page, may display threat counts for a particular file based on the number of devices on which the file is found, regardless of how many instances of the file are present on any given device. For example, if a particular file (specific hash) is located in three different folder locations on the same device, the threat count will equal one.

Reporting data is refreshed every three minutes (approximate) and uses a UTC time zone.

CylancePROTECT Overview Report

Provides an executive summary of your CylancePROTECT usage, from the number of zones and devices, to the percentage of your devices covered by Auto-Quarantine and Memory Protection, Threat Events, Memory Violations, Agent versions, and Offline Days for devices.

Overview Report Descriptions

- **Zones:** Displays the number of zones in the organization.
- **Devices:** Displays the number of devices in the organization. A device is an endpoint with a registered CylancePROTECT Agent.

Click any link on this widget to see the Devices Detail Report with a detailed list of devices.

- **Policies:** Displays the number of policies created in the organization.
- **Files Analyzed:** Displays the number of files analyzed (across all devices in the organization).
- **Auto-Quarantine Coverage:** Displays the number of devices with a policy that has both Unsafe and Abnormal selected for Auto-Quarantine; these devices are considered Enabled. Disabled devices are assigned to a policy that has one or both of these options disabled. The pie chart displays the percentage of devices assigned to a policy with Auto-

Quarantine disabled for either Unsafe, Abnormal, or both.

Click this widget to see a detailed list of devices with the selected Auto-Quarantine status.

- **Memory Protection Coverage:** Displays the number of devices with a policy that has Memory Protection set to Block or Terminate for 11 or more of the 16 memory violation types listed in a policy; these devices are considered Enabled. Disabled devices are assigned to a policy that has Memory Protection set to Block or Terminate for 10 or less of the memory violation types. The pie chart displays the percentage of devices assigned to a policy with 10 or less memory violation types set to Block or Terminate.

Click this widget to see a detailed list of devices with the selected Memory Protection status.

- **Memory Violations:** Displays a bar chart with memory violations that were either Alerted/Ignored (Alert/ Ignore) or Blocked/Terminated (Block/Term) over the last seven days. Hovering over a bar in the chart displays a breakdown of each data type.
- **Threat Events:** Displays a bar chart with Unsafe, Abnormal, and Quarantined threat events, grouped by day, for the last 30 days. Hovering over a bar in the chart displays the total number of threat events reported on that day.

Threats are grouped by the Reported On date, which is when the Console received information from the device about a threat. The Reported On date may differ from the actual event date if the device was not online at the time of the event.

Click this widget to see a detailed threats list.

- **Devices – CylancePROTECTVersion Stats:** Displays a bar chart representing the number of devices running a CylancePROTECT Agent version. Hovering over a bar in the chart displays the number of devices running that specific CylancePROTECT Agent version.

Click this widget to see a list of devices grouped by OS for the selected agent version.

- **Offline Days:** Displays the number of devices that have been Offline for a range of days (from 0-15 days, up to 61+ days). Also displays a bar chart color-coded with each range of days.

Click this widget to see a list of devices grouped by OS for the selected range of offline days.

Threat Event Summary Report

The Threat Event Summary Report shows the quantity of files identified in two of Cylance's threat classifications: malware and potentially unwanted programs (PUPs), and includes a

breakdown of specific sub-category classifications for each family. In addition, the Top 10 lists for File Owners and Devices with Threats display threat event counts for the Malware, PUPs, and Dual Use threat families.

- **Total Malware Events:** Displays the total number of malware events identified in the organization.
Click this widget to see a detailed list of all malware events.
- **Total PUP Events:** Displays the total number of PUP events identified in the organization.
Click this widget to see a detailed list of all PUP events.
- **Unsafe/Abnormal Malware Events:** Displays the total number of Unsafe and Abnormal malware events found in the organization.
Click this widget to see a detailed list of Malware that is in an Unsafe/Abnormal state.
- **Unsafe/Abnormal PUP Events:** Displays the total number of Unsafe and Abnormal PUP events found in the organization.
Click this widget to see a detailed list of PUPs that are in an Unsafe/Abnormal state.
- **Malware Event Classifications:** Displays a bar chart with each type of malware classification for threat events found on devices in the organization. Hovering over a bar in the chart displays the total number of malware events found for that classification.
Click an event classification in this widget to see a detailed list of the selected malware events.
- **PUP Event Classifications:** Displays a bar chart with each type of potentially unwanted program (PUP) classification for threat events found on devices in the organization. Hovering over a bar in the chart displays the total number of PUP events found for that classification.
Click an event classification in this widget to see a detailed list of the selected PUP events.
- **Top 10 File Owners with the Most Threat Events:** Displays a list of the top 10 file owners who have the most threat events.
This widget displays events from all Cylance file-based threat families, not just Malware or PUP events.
Click this widget to see a detailed list of threats for the selected File Owner.
- **Top 10 Devices with the Most Threat Events:** Displays a list of the top 10 devices that have the most threat events.

This widget displays events from all Cylance file-based threat families, not just Malware or PUP events.

Click this widget to see a detailed list of threats for the selected Device Name.

Device Summary Report

The Device Summary Report shows multiple device-centric measures of importance. Auto-Quarantine Coverage reveals threat prevention coverage and can be used to show progress. Devices – CylancePROTECT Version Stats can identify older CylancePROTECT Agents. Offline Days may indicate devices that are no longer checking in to the CylancePROTECT Console and are candidates for removal.

- **Total Devices:** Displays a count of devices in the organization. A device is an endpoint with a registered CylancePROTECT Agent.

Note: The number of licenses displayed is an approximate count and may not reflect an accurate license count.

Click this widget to see a detailed list of all devices.

- **Total Licenses:** Displays the total number of CylancePROTECT licenses the organization has purchased.
- **Devices – CylancePROTECT Version Stats:** Displays a bar chart representing the number of devices running a CylancePROTECT Agent version. Hovering over a bar in the chart displays the number of devices running that specific CylancePROTECT Agent version.

Click this widget to see a detailed list of devices that have the selected agent version installed.

- **Auto-Quarantine Coverage:** Displays the number of devices with a policy that has both Unsafe and Abnormal selected for Auto-Quarantine; these devices are considered Enabled. Disabled devices are assigned to a policy that has one or both of these options disabled. The pie chart displays the percentage of devices assigned to a policy with Auto-Quarantine disabled for Unsafe, Abnormal, or both.

Click this widget to see a detailed list of devices with the selected Auto-Quarantine status.

- **Memory Protection Coverage:** Displays the number of devices with a policy that has Memory Protection set to Block or Terminate for 11 or more of the 16 memory violation types listed in a policy; these devices are considered Enabled. Disabled devices are assigned to a policy that has Memory Protection set to Block or Terminate for 10 or less

of the memory violation types. The pie chart displays the percentage of devices assigned to a policy with 10 or less memory violation types set to Block or Terminate.

Click this widget to see a detailed list of devices with the selected Memory Protection status.

- **Offline Days:** Displays the number of devices that have been Offline for a range of days (from 0-15 days, up to 61+ days). Also displays a bar chart color-coded with each range of days.

Click this widget to see a list of devices grouped by OS for the selected range of offline days.

Threat Events Detail Report

The Threat Events Detail Report provides data for threat events found in the organization. Threats are grouped by the Reported On date, which is when the Console received information from the device about a threat. The Reported On date may differ from the actual event date if the device was not online at the time of the event.

- **# of Threat Events:** Displays a bar chart displaying threat events reported in the organization. Hovering over a bar in the chart displays the total number of threat events reported on that day. The bar chart displays the last 30 days.
- **Threat Events Table:** Displays threat event information.
Click a device name to see details for the selected device.
- **Reported On:** Allows selecting a date or date range to filter the threat events table. Click the Last Connected field, select a start date from the calendar, then either click the same date again (to view only that day) or click an end date to select a date range. To clear the date filter applied to the threat events table, refresh the page.

Devices Detail Report

The Devices Detail Report shows you how many devices you have for an OS family (Windows, macOS, and Linux).

- **# of Devices by OS:** Displays a bar chart with devices organized by major OS groups (Windows, Linux, and macOS). Hovering over a bar in the chart displays the total number of devices in that OS group.

Click this widget to see a detailed list of devices for the selected OS.

- **Devices Table:** Displays a list of device names, and device information, for devices in

the organization.

Click a device name to see details for the selected device.

- **Last Connected:** Allows selecting a date or date range to filter the devices table. Click the Last Connected field, select a start date from the calendar, and either click the same date again (to view only that day) or click an end date to select a date range. To clear the date filter applied to the devices table, refresh the page.

Export Reports

The Summary Reports (CylancePROTECT Overview, Threat Event Summary, and Device Summary) can be exported as a PNG image file.

The Detail Reports (Threat Events and Devices) can be exported as a comma-separated values (CSV) file.

To export a report, click the Export button in the upper-right hand corner of the Reports page.

- **For Threat Events, the CSV file contains:** FileName, Type, Classification, Reported On, DeviceName, FilePath, DetectedBy, and CurrentStatus.
- **For Devices, the CSV file contains:** Memory Protection, Device Name, Last Connected, Offline Duration, Agent Version, AQT (Auto-Quarantine), and Device OS.

ADMINISTRATION

Application

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Invitation URL

Use this feature to generate a URL for users that you have added to the Console to invite users to create an account in the Console.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Syslog/SIEM Settings

CylancePROTECT can be configured to forward events to a Syslog server. The content of each event is Unicode plain text consisting of key-value pairs, separated by commas. Due to the size limitation of most Syslog servers, the details of each message (Cylance-specific payload) is limited to 2048 characters.

See ["SIEM / Syslog URLs" on page 203](#) for a list of IP addresses.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Change Syslog Settings

1. Select **Settings > Application**.
2. Select the **Syslog/SIEM** checkbox. Configuration options expand.

3. Select the options you want and type in any server information needed.
4. Click **Save**.

Event Types

Syslog events have standard fields like timestamp, severity level, facility, and a Cylance-specific payload (message). Examples provided in this section only contain the Cylance-specific message.

Application Control

This option is only visible to users who have the Application Control feature enabled. Application Control events represent actions occurring when the device is in Application Control mode. Selecting this option will send a message to the Syslog server whenever an attempt is made to modify or copy an executable file, or when an attempt is made to execute a file from an external device or network location.

Example Message for Deny PE File Change

```
CylancePROTECT: Event Type:  
AppControl, Event Name: pechange,  
Device Name: WIN- 7entSh64, IP  
Address: (192.168.119.128),  
Action: PEFileChange, Action Type:  
Deny, File Path: C:\Users\admin\  
AppData\Local\Temp\MyInstaller.  
exe, SHA256:04D4DC02D96673EC  
A9050FE7201044FDB380E3CFE0D727E  
93DB35A709B45EDAA
```

Example Message for Deny Execution from External Drive

```
CylancePROTECT: Event Type:  
AppControl, Event Name:  
executionfromexternaldrives, Device  
Name: WIN-7entSh64, IP Address:  
(192.168.119.128), Action:  
  
PEFileChange, Action Type: Allow, File  
Path: \\shared1\psexec.exe, SHA256:  
F8DBABDFA03068130C277CE49C60E35C02  
9FF29D9E3C74C362521F3FB02670D5
```

Audit Log

Selecting this option will send the audit log of user actions performed in the CylancePROTECT Console (website) to the Syslog server. Audit log events will always appear in the Audit Log screen, even when this option is unchecked.

Example Message for Audit Log Being Forwarded to Syslog

```
CylancePROTECT: Event Type: AuditLog,
Event
Name: ThreatGlobalQuarantine, Message:
SHA2
56:A1E92E2E84A1321F499A5EC500E8B
9A9C0CA28701668BF13EA56D3995A96153F,
1CCC95B7B2F78

1D55D538CA01D6049762FDF6A75B32A06DF
3CC2EDC1F1573BFA; Reason: Manually
blacklisting these 2 threats., User:
(johnsmith@contoso.com)
```

Devices

Selecting this option sends device events to the Syslog server.

- When a new device is registered, you will receive two messages for this event: Registration and SystemSecurity.

Example Message for Device Registered Event

```
CylancePROTECT: Event Type: Device,
Event Name: Registration, Device Name:
WIN- 55NATVQHBUU

CylancePROTECT: Event Type: Device,
Event Name: SystemSecurity, Device
Name: WIN- 55NATVQHBUU, Agent Version:
1.1.1270.58, IP Address: (10.3.0.154),
MAC Address: (005056881877),
Logged On Users: (WIN-55NATVQHBUU\
Administrator), OS: Microsoft Windows
Server 2008 R2 Standard Service Pack 1
x64 6.1.7601
```

- When a device is removed.
- When a device's policy, zone, name, or logging level has changed.

Example Message for Device Updated Event

```
Cyl CylancePROTECT: Event Type:  
ExploitAttempt, Event Name: blocked,  
Device Name: WIN-7entSh64, IP Address:  
(192.168.119.128), Action: Blocked,  
Process ID: 3804, Process Name: C:\  
AttackTest64.exe, User Name: admin,  
Violation Type: LSASS Read
```

Memory Protection

Selecting this option will log any Memory Exploit Attempts that might be considered an attack from any of the Tenant's devices to the Syslog server.

There are four types of Memory Exploit actions:

- **None:** Allowed because no policy has been defined for this violation.
- **Allowed:** Allowed by policy.
- **Blocked:** Blocked from running by policy.
- **Terminated:** Process has been terminated.

Example Message of Memory Protection Event

```
Cyl CylancePROTECT: Event Type:  
ExploitAttempt, Event Name: blocked,  
Device Name: WIN-7entSh64, IP Address:  
(192.168.119.128), Action: Blocked,  
Process ID: 3804, Process Name: C:\  
AttackTest64.exe, User Name: admin,  
Violation Type: LSASS Read
```


Threats

Selecting this option will log any newly found threats, or changes observed for any existing threat, to the Syslog server. Changes include a threat being removed, quarantined, waived, or executed.

There are five types of Threat Events:

- **threat_found:** A new threat has been found in an *Unsafe* status.
- **threat_removed:** An existing threat has been removed.
- **threat_quarantined:** A new threat has been found in the *Quarantine* status.
- **threat_waived:** A new threat has been found in the *Waived* status.
- **threat_changed:** The behavior of an existing threat has changed (examples: score, quarantine status, running status).
- **threat_cleared:** A threat that has been Waived, added to the Safe List or deleted from quarantine on a device.

Example Message of Threat Event

```
CylancePROTECT: Event Type:
Threat, Event Name: threat found,
Device Name: SH-Win81- 1, IP
Address: (10.3.0.132), File Name:
virusshare_00fbc4cc4b42774b50a9f71074b
79bd9, Path: c:\ruby\host_automation\
test\data\test_files\, SHA256:
1EBF3B8A61A7E0023AAB3B0CB24938536A1
D87BCE1FCC6442E137FB2A7DD510B, Status:
Unsafe,

Cylance Score: 100, Found Date:
6/1/2015 10:57:42 PM, File Type:
Executable, Is Running: False, Auto
Run: False, Detected By: FileWatcher
```

Threat Classifications

Each day, Cylance will classify hundreds of threats as either Malware or potentially unwanted programs (PUPs). By selecting this option, you are subscribing to be notified when these events occur.

Example Message of Threat Classification

```
CylancePROTECT: Event Type:  
ThreatClassification, Event Name:  
ResearchSaved, Threat Class: Malware,  
Threat Subclass: Worm, SHA256:  
1218493137321C1D1F897B0C25BEF17C  
DD0BE9C99B84B4DD8B51EAC8F979 4F65
```

Security Information and Event Management (SIEM)

Specifies the type of Syslog server or SIEM to which events are being sent.

Protocol

This must match what you have configured on your Syslog server. The choices are UDP or TCP. UDP is generally not recommended as it does not guarantee message delivery. TCP is the default, and we encourage customers to use it.

TLS / SSL

Only available if the Protocol specified is TCP, TLS/SSL ensures the Syslog message is encrypted in transit from CylancePROTECT to the Syslog server. We encourage customers to checkmark this option. Be sure your Syslog server is configured to listen for TLS/SSL messages.

IP / Domain

Specifies the IP address or fully-qualified domain name of the Syslog server that you have setup. Consult with your internal network experts to ensure firewall and domain settings are properly configured.

Port

Specifies the port number on the machines that the Syslog server will listen to for messages. It must be a number between 1 and 65535. Typical values are: 512 for UDP, 1235 or 1468 for TCP, and 6514 for Secured TCP (example: TCP with TLS/SSL enabled).

Severity

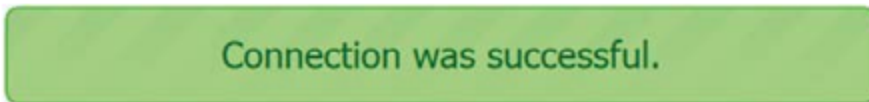
Specifies the severity of the messages that should appear in the Syslog server. This is a subjective field, and you may set it to whatever level you require. The value of severity does not change the messages that are forwarded to Syslog.

Facility

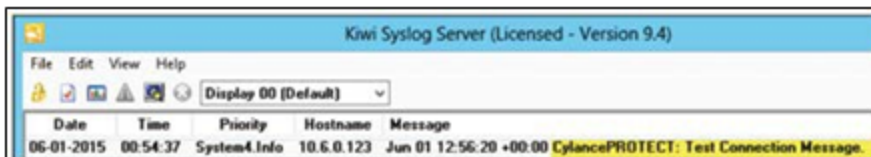
Specifies what type of application is logging the message. The default is Internal (or Syslog). This is used to categorize the messages when they are received by the Syslog server.

Testing the Connection

Click Test Connection to test the IP/Domain, Port, and Protocol settings. If you entered valid values, after a couple of moments, you should see a success confirmation pop-up.



On the Syslog server console, you should see the CylancePROTECT: Test Connection Message like this:



Custom Authentication

Use external Identity Providers (IdP) to login to the Console. This requires configuring settings with your IdP to obtain an X.509 certificate and a URL for verifying your IdP login. Custom Authentication works with Microsoft SAML 2.0. This feature has been confirmed to work with OneLogin, Okta, [Microsoft Azure](#), and PingOne. This feature also provides a Custom setting and should work with other Identity Providers who follow Microsoft SAML 2.0.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Note: Custom Authentication does not support Active Directory Federation Services (ADFS).

- **Strong Authentication:** Provides multi-factor authentication access.
- **Single Sign-On:** Provides single sign-on (SSO) access.

Note: Selecting Strong Authentication or Single Sign-On does not affect the Custom Authentication settings, because all configuration settings are handled by the Identity Provider (IdP).

- **Allow Password Login:** Selecting this option allows you to login to the Console directly and using SSO. This allows you to test your SSO settings without being locked out of the Console. Once you have successfully logged into the Console using SSO, it is recommended that you disable this feature.
- **Provider:** Select the service provider for the custom authentication.
- **X.509 Certificate:** Enter the X.509 certification information.
- **Login URL:** Enter the URL for the custom authentication.

Threat Data Report

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

Comma-separated value files (CSV) that contain the following information about the organization:

- **Threats:** Lists all threats discovered in the organization. This information includes File Name and File Status (Unsafe, Abnormal, Waived, and Quarantined).
- **Devices:** Lists all devices in the organization that have an Agent installed. This information includes Device Name, OS Version, Agent Version, and Policy applied.
- **Events:** Lists all events related to the Threat Events Graph on the Dashboard, for the last 30 days. This information includes File Hash, Device Name, File Path, and the Date the event occurred.
- **Indicators:** Lists each threat and the associated threat characteristics.
- **Cleared:** A threat that was found by CylancePROTECT but was cleared when:
 - An administrator deleted the quarantined threats from the CylancePROTECT Console

- A user deleted the threat that was on the disk. This includes if an application, other than Cylance, deleted the threat

When this feature is enabled, the report is automatically updated at 1:00 AM Pacific Standard Time (PST).

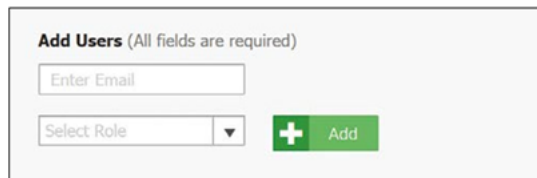
The Threat Data Report provides URLs and a token that can be used to download each report without requiring a login to the Console. You can also delete or regenerate the token, as needed, allowing you to control who has access to the report.

User Management

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on the next page](#) for more information.

Add Users

1. Select **Settings > User Management**.
2. Enter the user's email address.
3. Select a Role from the Role drop-down list. For more information about roles, see ["Role Management" on the next page](#).
4. Select the role to assign for existing zones from the table.
5. Click **Add**. An email is sent to the user, with a link to create a password.



The screenshot shows a form titled "Add Users (All fields are required)". It has two input fields: "Enter Email" and "Select Role" (a dropdown menu). To the right of the "Select Role" dropdown is a green button with a white plus sign and the text "Add".

Figure 45: Add Users

Change User Roles

1. Select **Settings > User Management**.
2. Click a user from the list. The User Details page displays.
3. Select a new role for this user.
4. If you selected a Zone Manager or User role, set the following:
 - a. Default Zone Role (for future zones): Select whether this user will be a zone manager, user, or not have permissions anytime a new zone is created

- b. Zone role (for existing zones): Select the role(s) for this user for existing zones.
5. Click **Save**. Users will see any changes the next time they log in.

Remove Users

1. Select **Settings > User Management**.
2. Select the check box for the user or users to remove.
3. Click **Remove**.
4. Click **Yes** at the message asking for confirmation of the removal.

Role Management

You can create custom roles (Role Based Access Control or RBAC) or use a predefined role to manage user access to features. Predefined roles have the following permissions and cannot be modified:

- Administrators have global permissions and can add or remove users, assign users to zones (either as a User or a Zone Manager), add or remove devices, create policies, and create zones. Administrators can also delete users, devices, policies, and zones permanently from the Console.
- Users and Zone Managers only have access and privileges pertaining to the Zone to which they are assigned. This applies to devices assigned to the Zone, threats found on those devices, and information on the dashboard. Zone Managers have the following additional privileges:
 - Remove devices from zone
 - Edit device name
 - Edit assigned zone name
 - Apply policy to zone
 - Remove policy from zone
 - Assign zone managers or users to zones they manage
 - Remove users from zone
- Read-only users have permission to view data for all zones and settings in the Cylance Console, including the Audit Log, but they cannot take any actions or change any settings. The role is useful for someone conducting an audit or compliance review.

Note: The CylanceOPTICS feature does not display for Read-only users.

Some menu options, pages, and features may not be available based on your role's permissions.

Additional Notes:

- The Dashboard displays for all predefined and custom roles regardless of permissions.
- Regardless of their permissions, users assigned to a custom role cannot enable Email Notifications on the My Account page (Profile menu in top right of the Console).
- In order for a menu icon to display, a user must have access to that feature. For example, if a user does not have access to Zones, the Zones icon does not display on the menu.

Add a Role

At this time, custom roles are globally scoped and provide full operational access to the related pages and actions for a defined area.

Example: If a custom role has *Allow* checked for Zones, any user assigned to the role can add/remove zones, create/edit/delete rules, add/remove devices from a zone, and any other functionality available on the Zones or Zone Details pages.

If access is not selected for a role, users will not see that page in the side navigation menu and will not be able to navigate to the page from other locations in the Console.

Example: If a custom role has *Allow* checked for Threats, but unchecked for Devices, the Threat Protection page displays in the side navigation menu, but the Devices page does not display. If the user opens the Threat Protection page and selects a threat, on the Threat Details page, the Affected Devices and Zones list populates with a list of devices that contain the threat, but if the user clicks the link for a device, a Resource Not Found error page displays since they do not have permissions for Devices.

1. Select **Settings > User Management**.
2. Click on **Roles**.
3. Click on **Add New Role**.

Add New Role

Role Name

255 characters remaining

Page Access	Allow	Settings Access	Allow
Threat Protection	<input type="checkbox"/>	Application	<input checked="" type="checkbox"/>
Zones	<input type="checkbox"/>	Installation Token Management	<input checked="" type="checkbox"/>
Devices	<input type="checkbox"/>	Installer Download	<input checked="" type="checkbox"/>
CylanceOPTICS	<input type="checkbox"/>	Invitation URL	<input checked="" type="checkbox"/>
Reports	<input type="checkbox"/>	Uninstall Password Management	<input checked="" type="checkbox"/>
Audit Log	<input type="checkbox"/>	Support Login	<input checked="" type="checkbox"/>
		Syslog/SIEM	<input checked="" type="checkbox"/>
		Custom Authentication	<input checked="" type="checkbox"/>
		User Management	<input type="checkbox"/>
		Device Policy	<input type="checkbox"/>
		Global List	<input type="checkbox"/>
		Update	<input type="checkbox"/>
		Certificates	<input type="checkbox"/>
		Integrations	<input type="checkbox"/>

Figure 46: Add New Role

4. Enter a name for the role, then click on the **Allow** checkbox beside any feature you want to allow this role to access.

Access	Description
Threat Protection	<p>Provides access to the Threats, Script Control, and External Devices pages.</p> <p>If this permission is unchecked:</p> <ul style="list-style-type: none"> • The Threat Protection icon does not display in the main menu. • The Dashboard page displays but attempting to drill-down to a threat from the Dashboard page results in a Resource Not Found page. • Attempting to drill-down to a threat from pages the user has access to (e.g. if the user has access to the Device Details page and clicks a threat under Threats & Activities) results in a Resource Not Found page. <p>Note: If you want to Global Quarantine or Safelist a threat from these pages, you will also need Global List permissions.</p>
Zones	<p>Provides access to the Zones and Zone Details pages.</p> <p>If this permission is unchecked:</p> <ul style="list-style-type: none"> • The Zones icon does not display in the main menu. • Attempting to drill-down to a zone from pages the user has access to (e.g. if the user has access to the Devices page and clicks a zone in the table) results in a Resource Not Found page. • You cannot add/edit/remove a zone on Device Details > Edit Device Properties.

Access	Description
Devices	<p>Provides access to the Devices and Device Details pages.</p> <p>If this permission is unchecked:</p> <ul style="list-style-type: none"> • The Devices icon does not display in the main menu. • Attempting to drill-down to a device from pages the user has access to (e.g. if the user has access to the Threat Details page and clicks a device under Affected Devices and Zones in the table) results in a Resource Not Found page. <p>Note: If you want to Global Quarantine or Safelist a threat from these pages, you will also need Global List permissions.</p>
CylanceOPTICS	<p>Provides access to the CylanceOPTICS page and features.</p> <p>If this permission is unchecked, the CylanceOPTICS icon does not display in the main menu.</p> <p>Note: If you do not have a license for CylanceOPTICS, this checkbox does not display.</p>
Reports	<p>Provides access to the Device and Threat summary and detailed reports.</p> <p>If this permission is unchecked, the Reports icon does not display in the main menu.</p>
Audit Log	<p>Provides access to the Audit Log page from the Profile menu (top-right).</p> <p>If this permission is unchecked, the Audit Log option does not display in the Profile menu.</p>
Application	<p>Provides access to the Application page under Settings. You can specify whether the role can:</p> <ul style="list-style-type: none"> • Copy, delete, or regenerate the Installation Token. • Download agent installers for devices from the Application page, Deployments page, or Add New Device dialog. • Copy, disable, or generate a URL to provide access to the Console. • Require a password to uninstall an agent and configure the password to use. • Select whether Cylance Customer Support can log into the tenant to troubleshoot issues. • Select whether Syslog/SIEM applications can be configured to work with CylancePROTECT. • Enable Custom Authentication for the Console. <p>Note the following:</p> <ul style="list-style-type: none"> • If all sub-options are unchecked, the Applications menu option does not display under Settings in the main menu. • If a sub-option is unchecked, it does not display on the

Access	Description
	<p>Applications page.</p> <ul style="list-style-type: none"> In order for a user to download and install an agent, they must have permissions for the Installation Token and Installer (unless the token is provided separately).
User Management	<p>Provides access to the User Management and Roles pages under Settings.</p> <p>If this permission is unchecked, the User Management menu option does not display under Settings in the main menu.</p> <p>Note: User Management Permissions and Role Management Permissions are associated, so if a user is assigned a role with User Management permissions selected, that user will also have access to Role Management functionality.</p>
Device Policy	<p>Provides access to the Device Policy page under Settings. Policies set on this page determine how the Agent handles malware it encounters.</p> <p>If this permission is unchecked:</p> <ul style="list-style-type: none"> The Device Policy menu option does not display under Settings in the main menu. At this time, users who have Device permissions but not Device Policy permissions can assign a different policy to a device on the Device Details page > Edit Device Properties due to overlapping permissions.
Global List	<p>Provides access to the Global Quarantine, Safelist, and Unassigned pages under Settings. It also displays the Global Quarantine and Safelist buttons on the Protection (Threats, Script Control) and Device Details (Threats & Activities) pages.</p> <p>If this permission is unchecked:</p> <ul style="list-style-type: none"> The Global List menu option does not display under Settings in the main menu. The Global Quarantine and Safelist buttons will not display on any related pages.
Update	<p>Provides access to the Zone-based Updating page under Settings. This page determines which Agent version is installed for all devices in a zone.</p> <p>If this permission is unchecked, the Update menu option does not display under Settings in the main menu.</p>
Certificates	<p>Provides access to the Certificates page under Settings. This page is used to Safelist executable files or scripts using a signed certificate.</p> <p>If this permission is unchecked, the Certificates menu option does not display under Settings in the main menu.</p>
Integrations	<p>Provides access to the Integrations page under Settings. This page is</p>

Access	Description
	<p>used to provide integration with third party programs.</p> <p>If this permission is unchecked, the Integrations menu option does not display under Settings in the main menu.</p>

5. Click **Submit**.

Edit a Role

1. Select **Settings > User Management**.
2. Click on **Roles**.
3. Click on an existing role in the list. The Edit Role dialog displays.
4. Modify the name or permissions, then click **Submit**.

The updated name or permissions will be applied to any users assigned to the existing role.

View Users Assigned to a Role

From the Roles page, if a predefined or custom role has users assigned, you can click the **Assigned Users** link in the table to view the email for any users assigned to that role.

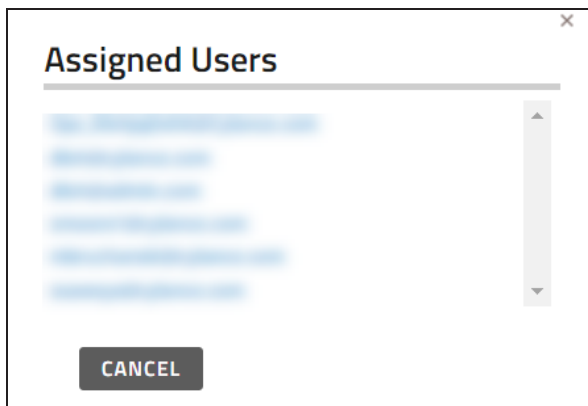


Figure 47: Assigned Users

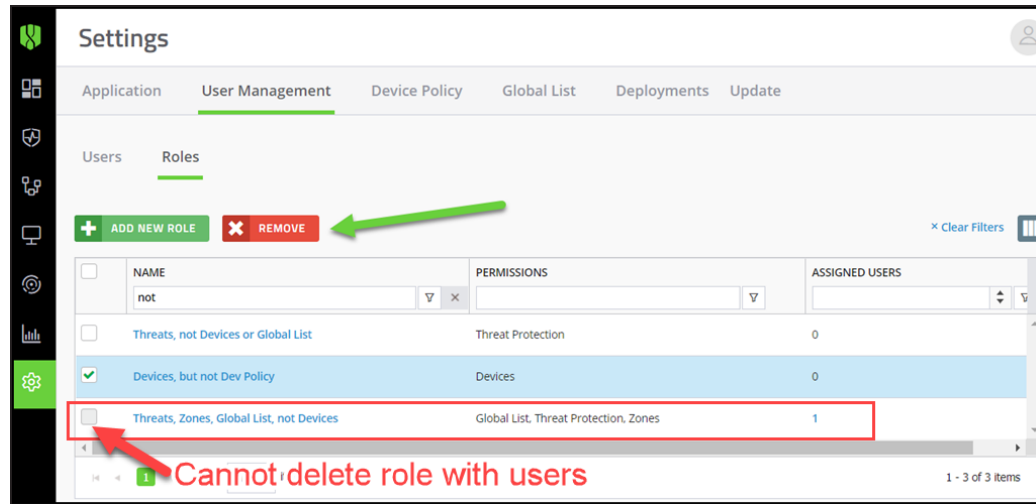
Clicking on a user's email link to view the User Details page for that user.

Delete a Role

If a role does not have any users assigned to it, you can delete the role.

1. Select **Settings > User Management**.
2. Click **Roles**.

3. Click a checkbox beside a role that does not have any users assigned to it. If a role has users assigned to it, you cannot select the checkbox.
4. Click **Remove**, then confirm the role's removal.



My Account

Change your password and email notification setting on the My Account page.

1. Login to the Console.
2. Click the profile menu in the upper-right corner, and select **My Account**.
3. To change your password:
 - a. Click **Change Password**. Password fields display.
 - b. Enter your old password.
 - c. Enter your new password, then re-enter it to confirm it.
 - d. Click **Update**.
4. Select or de-select the check box to enable or disable Email Notifications. Enabling and disabling the check box is automatically saved. Email Notifications are available for Administrators only. This email is sent on an hourly basis and one email notification contains all of the data, whether one email notification option or both options are selected.
 - New unsafe / abnormal threat detections: Receive an email when a new Unsafe or Abnormal threat is detected on any device in your organization.

- New quarantined threat events: Receive an email when a new threat is quarantined on any device in your organization.

Note: Review the following:

- Email notifications are not available if you have been assigned a custom role.
- The email will come from `td-no-reply@cylance.com`.

Audit Logs

The Audit Log contains information about the following actions performed from the Console:

- Login (Success, Failure)
- Policy (Add, Edit, Remove)
- Device (Edit, Remove)
- Threat (Quarantine, Waive, Global Quarantine, Safe List)
- User (Add, Edit, Remove)
- Custom Role (Add, Edit, Remove)
- Agent Update (Edit)
- Device API (Update Device, Update Device Threat, Delete Devices)
- Global List API (Add to Global List, Delete from Global List)
- Policy API (Create Policy, Delete Policy or Delete Policies, Update Policy)
- Tenant User API (Create User, Delete User, Update User)
- Zone API (Create Zone, Delete Zone, Update Zone)

The Audit Log can be viewed from the Console by navigating to the profile drop-down list on the upper-right side of the Console, and selecting **Audit Log**.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

The Audit Log can be exported as a CSV file for use in other applications. Click the **Export** button on the Audit Log page.

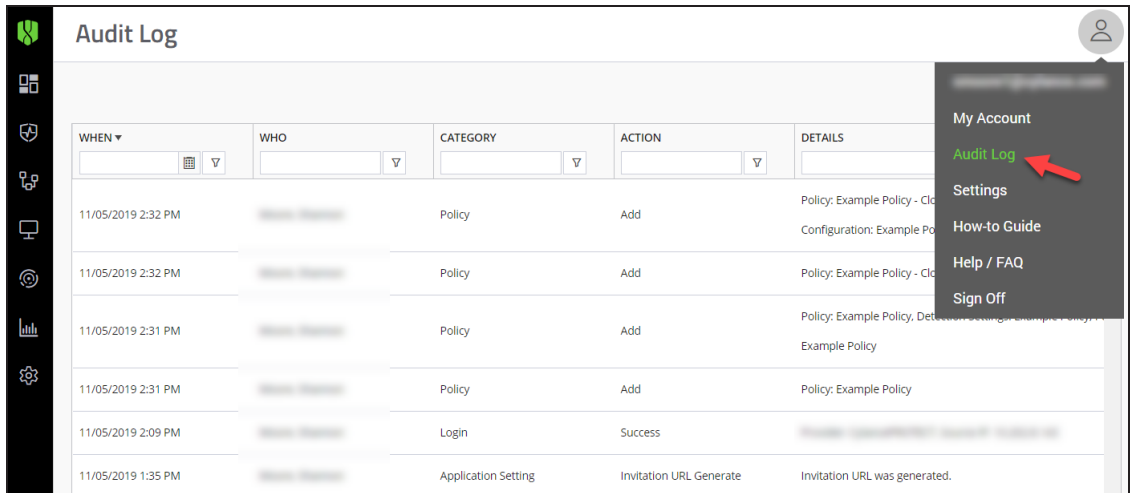


Figure 48: Audit Log

How-To Guide

Online guide with a description of features in the Console.

Help and FAQ

Help and Frequently Asked Questions (FAQ) are hosted on the Support website. Clicking the Help/FAQ link in the profile menu (upper-right corner of the Console) takes you to the BlackBerry Cylance Support homepage.

Language Preferences

The Console supports the following languages:

English	French	German
Italian	Japanese	Korean
Portuguese (Brazil)	Portuguese (Portugal)	Spanish

Table 6: Supported CylancePROTECT Languages

The Console will use the language preferences or settings in your web browser to determine which localized content to display.

In Google Chrome

1. Click **Customize and Control Google Chrome** (upper-right), then click Settings.
2. Scroll down and click **Advanced**.

3. Click **Language**.
4. Click **Add languages**, select the language you want to add, then click Add. You can change the order of the languages by dragging a language to the preferred location.
5. Close the Settings page.

In Mozilla Firefox

1. Click **Open Menu** (upper-right), then click Options.
2. In the left-pane, click **Content**.
3. Under Languages, click **Choose**.
4. Select the language you want to display from the **Select a language to add** list, then click **Add**.
5. Click **OK**.

Network Related

Configure the network to allow the CylancePROTECT Agent to communicate with the Console over the Internet. This section covers firewall settings and proxy configurations.

Tip: CylancePROTECT supports a Disconnected Mode for Agents disconnected from the network and cannot access the Console.

Firewall

No on-premise software is required to manage devices. Agents are managed by and report to the Console. Port 443 (HTTPS) is used for communication and must be open on the firewall in order for the Agents to communicate with the Console. The Console is hosted by Amazon Web Services (AWS) and does not have any fixed IP addresses.

For a list of Cylance hosts to allow, based on the region to which the organization belongs, see ["Cylance Host URLs" on page 200](#). Alternatively, you can allow HTTPS traffic to *.cylance.com.

Proxy

Proxy support for CylancePROTECT is configured through a registry entry. When a proxy is configured, the Agent uses the IP address and port in the registry entry for all outbound communications to Console servers.

Note: SSL inspection is not supported and must be bypassed for all **CylancePROTECT** traffic (*.cylance.com).

1. Access the registry.
Note: Elevated privileges or taking ownership of the registry may be required depending on how the Agent was installed (Protected Mode enabled or not).
2. In Registry Editor, navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop**.
3. Create a new String Value (REG_SZ):
 - Value Name = ProxyServer
 - Value Data = proxy settings (For example, http://123.45.67.89:8080)

The Agent attempts to use the credentials of the currently logged in user to communicate out to the Internet in authenticated environments. If an authenticated proxy server is configured and a user is not logged onto the device, the Agent cannot authenticate to the proxy and cannot communicate with the Console. In this instance, either:

- Configure the proxy and add a rule to allow all traffic to *.cylance.com.
- Use a different proxy policy, allowing for unauthorized proxy access to Cylance hosts (*.cylance.com).

By doing this, if no user is logged onto the device, the Agent does not need to authenticate and should be able to connect to the cloud and communicate with the Console.

Integrations

The CylancePROTECT Console provides integration with some third party programs.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

CylanceOPTICS API

The CylanceOPTICS API is part of the Cylance API version 2.0 and is available to users who have both CylanceOPTICS and Cylance API v2.0 enabled. The Cylance API is a set of RESTful APIs that allow users to programmatically access and manage CylanceOPTICS settings. The API Application Management interface provides self-service credential management and allows for the creation and management of multiple applications with different levels of API access. For more information, see the [Cylance User API Guide](#).

TROUBLESHOOTING

This section provides a list of questions to answer and files to collect when troubleshooting issues with CylancePROTECT. This information enables BlackBerry Cylance Support to assist in resolving issues.

For up-to-date information about CylancePROTECT, visit the BlackBerry Cylance Support Knowledge Base at <https://support.cylance.com>.

Note: In the Console, there is a How-To Guide that explains product features. Access this guide from the Account drop-down list (upper-right corner of the Console menu).

Missing Menu Options, Pages, and Functionality

Starting in November 2019, Cylance introduced custom roles (Role Based Access Control or RBAC) in the Console to manage access to features and functionality. If your role's permissions do not include access to a feature or option, one or more of the following may occur:

- A menu icon may not display.
- A page may not display.
- Clicking a link on a page may return a "Resource Not Found. Sorry, but the resource you are looking for cannot be found or you do not have permission to view it."
- Buttons on a page may be disabled or removed.
- Functionality or features on a page may be disabled or removed.

See ["Role Management" on page 182](#) for more information.

Installation Parameters

- **What Is the Installation Method? Provide Any Parameters Used.**
 - **Example** — Windows: Use LAUCHAPP=0 when installing from the command line to hide the Agent icon and Start Menu folder at run time.
 - **Example** — macOS: Use SelfProtectionLevel=1 when installing from the command line to disable Self Protection on the Agent.
- **Which Steps of the Installation Could Be Verified?**

- **Example** — Windows: Was the MSI or EXE installer used?
- **Example** — Any OS: Were any command line options used, such as Quiet Mode or No Agent UI?
- **Enable Verbose Logging for the Installation (Windows only).**
 - In the Registry Editor, go to HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
 - Create a new String with Logging for the value name and voicewarmupx for the value data.
 - Reproduce the issue by attempting the installation or uninstallation.
 - Collect the log files from the temp folder. C:\user_profile\AppData\Local\Temp.

Note: The Temp folder location may vary depending on the user who logged on and the Environment variable settings in Windows.

Performance Concerns

- Capture a screenshot of the Task Manager (Windows) or Activity Monitor (macOS) that shows the Cylance processes and memory consumption.
- Capture a dump of the Cylance process.
- Collect debug logs.
- Collect output of System Information during the issue.
 - For Windows: msinfo32 or winmsd
 - For macOS: System Information
- Collect any relevant Event Logs (Windows) or Console information (macOS).

Update, Status, and Connectivity Issues

- Ensure that port 443 is open on the firewall and the device can resolve and connect to Cylance.com sites.
- Is the device listed in the Devices page of the Console? Is it Online or Offline? What is its Last Connected time?
- Is a proxy being used by the device to connect to the Internet? Are the credentials properly configured on the proxy? See ["Proxy" on page 191](#) for more information.
- Restart the CylancePROTECTservice so that it attempts to connect to the Console.

- Collect debug logs. See ["Enable Debug Logging" below](#) for more information.
- Collect the output of System Information during the issue.
 - For Windows: msinfo32 or winmsd
 - For macOS: System Information

Enable Debug Logging

By default, CylancePROTECT maintains log files stored in *C:\Program Files\Cylance\Desktop\log*. For troubleshooting purposes, CylancePROTECT can be configured to produce more verbose logs via KB Debug Logging.

Script Control Incompatibilities

Issue

When Script Control is enabled on some devices, it can cause conflicts with other software running on those devices. This conflict is typically due to the Agent injecting into certain processes that are being called by other software.

Solution

Depending on the software, this issue can be resolved by adding specific process exclusions to the Device Policy in the Console. Another option is to enable Compatibility Mode (registry key) on each affected device. However, if exclusions are not effective, You should disable Script Control in the Device Policy affecting the devices to restore normal system functionality.

Note: This Compatibility Mode solution is for Agent 1360. Starting with Agent 1380 and higher, the injection process has been updated for compatibility with other products.

Compatibility Mode

Add the following registry key to enable Compatibility Mode:

1. In the Console, Memory Protection must be disabled in the Policy before adding the Compatibility Mode setting.
2. Using the Registry Editor, go to *HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop*.
3. Right-click **Desktop**, click **Permissions**, take ownership and grant **Full Control**. Click **OK**.

4. Right-click **Desktop** and select **New > Binary Value**.
5. Name the file **CompatibilityMode**.
6. Open the registry setting and change the value to 01.
7. Click **OK**, then close Registry Editor.
8. A restart of the system may be required.

Command Line Options

Using Psexec

```
psexec -s reg add HKEY_LOCAL_
MACHINE\SOFTWARE\Cylance\Desktop /v CompatibilityMode /t
REG_BINARY /d 01
```

To perform a command on multiple machines, you can use the Invoke-Command cmdlet:

```
$servers = "testComp1","testComp2","textComp3"

$credential = Get-Credential -Credential
{UserName}\administrator

Invoke-Command -ComputerName $servers -Credential
$credential -ScriptBlock {New-Item -Path
HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type
REG_BINARY -Value 01}
```

Enable Support Login

Allows Support to help users troubleshoot Console issues by providing Support access to the user's tenant and act on behalf of the user. This allows Support to see what the user sees, with the same level of permission as the user. All actions taken by Support are tracked in the Audit Log.

Some menu options, pages, and features may not be available based on your role's permissions. See ["Role Management" on page 182](#) for more information.

1. Select **Settings > Application**.
2. Select **Enable Support Login**.

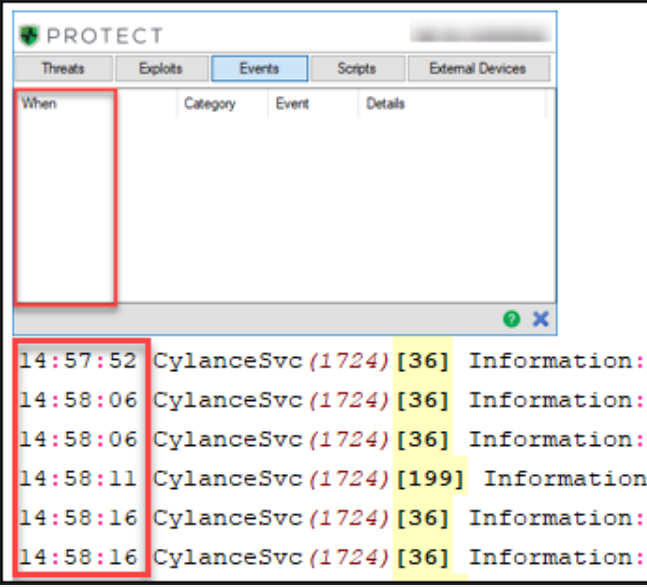
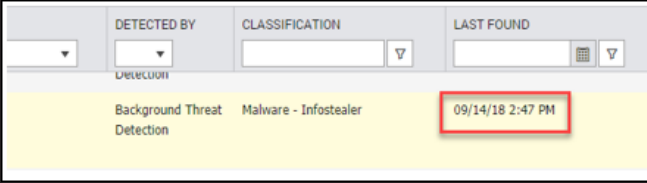
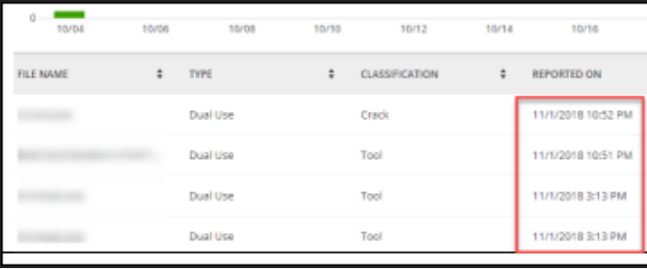
Virtual Machines

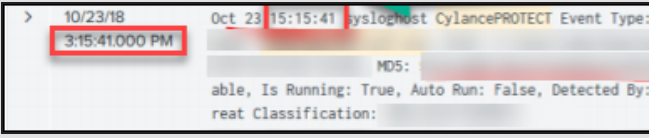
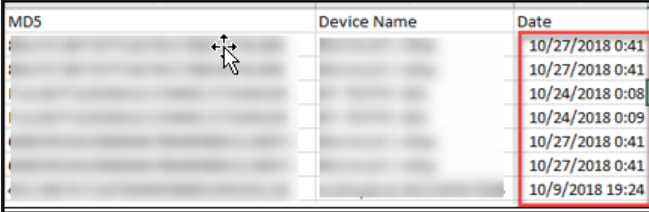
Below are some recommendations for using the CylancePROTECT Agent on a virtual machine image. For best practices, see ["Appendix A: VDI Best Practices " on page 210.](#)

- For non-persistent VDI environments, you can use Agent 1490 (or higher) and an installation parameter to instruct the Agent during installation that it will be running in a pool of cloned images. This will enable the Agent to recognize each clone as a unique device and persist their identification when they refresh. See ["Appendix A: VDI Best Practices " on page 210](#) for more information
- Some virtual machine software has security settings that conflict with CylancePROTECT's Memory Protection feature. This conflict may result in an unresponsive virtual machine. If this happens, it is recommended to either disable the Memory Protection feature or use different virtual machine software.

Time Zone Variances

Depending on where you are in CylancePROTECT, the time zone used can vary.

Feature	Time Zone
<p>Devices with an agent installed, including event notifications and agent logs.</p> 	<p>Uses the time zone of the local machine.</p>
<p>Console, except for the Reports tab and exported data.</p> 	<p>Uses the time zone for the user viewing the Console.</p>
<p>Reports tab in the Console.</p> 	<p>Uses the UTC time zone.</p>
<p>Syslog events</p>	<p>Uses the UTC time zone.</p>

Feature	Time Zone
	
<p>Threat Data Report or any exported data in the console</p> 	<p>Uses the UTC time zone.</p>

CYLANCE HOST URLS

The Agents report to, and are managed by the Console. For environments that must allow domains through a firewall, use the list of domains below, based on the region to which the organization belongs.

To verify the domain to which you belong, login to the Console and check the URL, then match that information to the correct list below.

Note: When logging in to the Console, you must use the correct login URL, which is based on the region to which the organization belongs. If you are using the correct login credentials but cannot login, check the URL.

North America

Required for Agent Communication and Console Navigation

The below domains are required to allow the Agent to communicate correctly to the Console, as well as to access and navigate the Console successfully.

- login.cylance.com
- data.cylance.com
- protect.cylance.com
- update.cylance.com
- api.cylance.com
- download.cylance.com

Additional Domains Required for Console Navigation

The below domains are also required to navigate the Console successfully. They are not required for the CylancePROTECT Agent to communicate to the Console successfully.

- cdn.cylance.com
- venueapi.cylance.com

Asia-Pacific North East

Required for Agent Communication and Console Navigation

The below domains are required to allow the Agent to communicate correctly to the Console, as well as to access and navigate the Console successfully.

- login-apne1.cylance.com
- data-apne1.cylance.com
- protect-apne1.cylance.com
- update-apne1.cylance.com
- api.cylance.com
- download.cylance.com

Additional Domains Required for Console Navigation

The below domains are also required to navigate the Console successfully. They are not required for the CylancePROTECT Agent to communicate to the Console successfully.

- cdn.cylance.com
- venueapi-apne1.cylance.com

Asia-Pacific South East (including Australia)

Required for Agent Communication and Console Navigation

The below domains are required to allow the Agent to communicate correctly to the Console, as well as to access and navigate the Console successfully.

- login-au.cylance.com
- data-au.cylance.com
- protect-au.cylance.com
- update-au.cylance.com
- api.cylance.com
- download.cylance.com

Additional Domains Required for Console Navigation

The below domains are also required to navigate the Console successfully. They are not required for the CylancePROTECT Agent to communicate to the Console successfully.

- cdn.cylance.com
- venueapi-au.cylance.com

Europe Central

Required for Agent Communication and Console Navigation

The below domains are required to allow the Agent to communicate correctly to the Console, as well as to access and navigate the Console successfully.

- login-euc1.cylance.com
- data-euc1.cylance.com
- protect-euc1.cylance.com
- update-euc1.cylance.com
- api.cylance.com
- download.cylance.com

Additional Domains Required for Console Navigation

The below domains are also required to navigate the Console successfully. They are not required for the CylancePROTECT Agent to communicate to the Console successfully.

- cdn.cylance.com
- venueapi-euc1.cylance.com

South America East

Required for Agent Communication and Console Navigation

The below domains are required to allow the Agent to communicate correctly to the Console, as well as to access and navigate the Console successfully.

- login-sae1.cylance.com
- data-sae1.cylance.com
- protect-sae1.cylance.com
- update-sae1.cylance.com
- api.cylance.com
- download.cylance.com

Additional Domains Required for Console Navigation

The below domains are also required to navigate the Console successfully. They are not required for the CylancePROTECT Agent to communicate to the Console successfully.

- cdn.cylance.com
- venueapi-sae1.cylance.com

Note: api2.cylance.com is a deprecated IP address, and was removed from the required list of IP addresses above.

SIEM / Syslog URLs

CylancePROTECT can integrate with your Security Information Event Management (SIEM) software using Syslog. Syslog events will be persisted at the same time the Agent events persist to the Console. Syslog events display using the UTC time zone while Agent events display using the device's time zone.

The Syslog server IP addresses are static to ensure communication with your Syslog servers. Allow all IP addresses for the region to which the organization belongs. There are multiple IP addresses for fail-over solutions and future expansion.

If you do not use a Syslog server, then you do not need to allow this IP address through your firewall.

To configure Syslog/SIEM, see ["Syslog/SIEM Settings" on page 172](#)

Asia-Pacific North East (login-apne1.cylance.com)

- 13.113.53.36
- 13.113.60.107

Asia-Pacific South East (login-au.cylance.com):

- 52.63.15.218
- 52.65.4.232

Europe Central (login-euc1.cylance.com):

- 52.28.219.170
- 52.29.102.181
- 52.29.213.11

North America (login.cylance.com):

- 52.2.154.63
- 52.20.244.157
- 52.71.59.248
- 52.72.144.44
- 54.88.241.49

South America (login-sae1.cylance.com):

- 52.67.244.213
- 52.67.252.42

Undeliverable Messages

If the CylancePROTECT Syslog integration cannot successfully deliver syslog messages to your server, an email notification will be sent to any Administrators in the organization with a confirmed email address. The email notification is to alert any Administrators about the Syslog issue. If no action is taken, Syslog messaging is disabled after 20 minutes.

If the issue is resolved before the 20 minute time period has ended, then syslog messages will continue to be delivered. If the issue is resolved after the 20 minute time period, an Administrator in the organization must re-enable Syslog messaging in the Console (**Settings > Application > Syslog/SIEM**).

AGENT STATUS INFORMATION FILE

The Agent provides a way for users to get Agent Status information from a device. This file provides information about the Agent that users would see in the Agent user interface, except for Events information. This allows users to get Agent information without needing to go directly to the Agent UI.

Enabling this feature requires adding a few registry keys. This functionality was introduced in Agent version 1370. The file is available in XML and JSON file formats.

Note: The Status file contains the latest information only. It does not contain any historical status information. The file is over-written at a set interval.

1. On the device, open the Registry Editor and navigate to:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop
 - You might need to change the registry permissions to add these keys.
2. Create the following keys in the Desktop folder. Use DWORD (32-bit) and Hexadecimal.
 - **StatusFileEnabled:** File is written if the registry value is greater than zero. Default value is 1, so the file is written by default.
 - **StatusFileType:** The file format written. If the value is zero (0), then a JSON file is written. If the value is 1, then an XML file is written. The default value is 1.
 - **StatusFilePath:** Location of the Status file. The default path is:
CommonAppData\Cylance\Status\Status.json Status.json (or Status.xml)
Example: C:\ProgramData\Cylance\Status
 - **StatusPeriod:** How often the file is written. The default value is 60, so the file is over-written every 60 seconds. The minimum value is 15 for a 15-second interval.

Status Information Type	Description
snapstop_time	The date and time the Status information was collected. The date and time are local to the device.
ProductInfo	<ul style="list-style-type: none">■ version: CylancePROTECT Agent version on the device.■ last_communicated_timestamp: Date and time of the last check for an Agent Update.■ serial_number: Installation Token used to register the Agent.■ device_name: Name of the device on which the Agent is installed.
Policy	<ul style="list-style-type: none">■ type: Status of the Agent, whether it is Online or Offline.

Status Information Type	Description
	<ul style="list-style-type: none"> ■ id: Unique identifier for the policy. ■ name: Policy name.
ScanState	<ul style="list-style-type: none"> ■ last_background_scan_timestamp: Date and time of the last Background Threat Detection scan. ■ drives_scanned: List of drive letters scanned.
Threats	<ul style="list-style-type: none"> ■ count: The number of threats found. ■ max: The maximum number of threats included in the Status file. ■ Threat: <ul style="list-style-type: none"> • file_hash_id: Displays the SHA256 hash information for the threat. • file_md5: The MD5 hash information. • file_path: The path where the threat was found. Includes the file name. • is_running: Is the threat currently running on the device? True or False. • auto_run: Is the threat file set to run automatically? True or False. • file_status: Displays the current state of the threat, like Allowed, Running, or Quarantined. See the Threat: FileStatus table below. • o file_type: Displays the type of file, like Portable Executable (PE), Archive, or PDF. See the Threat: FileType table below. • o score: Displays the Cylance Score. The score displayed in the Status file ranges from 1000 to -1000. In the Console, the range is 100 to -100. • o file_size: Displays the file size, in bytes.
Exploits	<ul style="list-style-type: none"> ■ count: The number of exploits found. ■ max: The maximum number of exploits included in the Status file. ■ Exploit <ul style="list-style-type: none"> • ProcessId: Displays the process ID of the application identified by Memory Protection. • ImagePath: The path from which the exploit originates. Includes the file name. • ImageHash: Displays the SHA256 hash information for the exploit. • FileVersion: Displays the version number of the exploit file. • Username: Displays the name of the user who was logged in to the device when the exploit occurred. • Groups: Displays the group with which the logged in user is associated.

Status Information Type	Description
	<ul style="list-style-type: none"> • Sid: The Security Identifier (SID) for the logged in user. • ItemType: Displays the exploit type, which relates to the Violation Types (KB 204295888). See the Exploit: ItemType table below. • State: Displays the current state of the exploit, like Allowed, Blocked, or Terminated. See the Exploit: State table below. • MemDefVersion: The version of Memory Protection used to identify the exploit. This is typically the Agent version number. • Count: The number of times the exploit attempted to run.
Scripts	<ul style="list-style-type: none"> ■ count: The number of scripts run on the device. ■ max: The maximum number of scripts included in the Status file. ■ Script <ul style="list-style-type: none"> • script_path: The path from which the script originates. Includes the file name. • file_hash_id: Displays the SHA256 hash information for the script. • file_md5: Displays the MD5 hash information for the script, if available. • file_sha1: Displays the SHA1 hash information for the script, if available. • drive_type: Identifies the type of drive from which the script originated, like Fixed. • last_modified: The date and time the script was last modified. • interpreter: <ul style="list-style-type: none"> • name: The name of the script control feature that identified the malicious script. • version: The version number of the script control feature. • username: Displays the name of the user who was logged in to the device when the script was launched. • groups: Displays the group with which the logged in user is associated. • sid: The Security Identifier (SID) for the logged in user. • action: Displays the action taken on the script, like Allowed, Blocked, or Terminated . See the Script: Action table below.

Threat: FileStatus	Value
None	0x00

Threat: FileStatus	Value
Threat	0x01
Suspicious	0x02
Allowed	0x04
Quarantined	0x08
Running	0x10
Corrupt	0x20

Threat: FileType	Value
Unsupported	0
PE	1
Archive	2
PDF	3
OLE	4

Exploit: ItemType	Value	Related Violation Type
None	0	n/a
StackPivot	1	Stack Pivot
StackProtect	2	Stack Protect
OverwriteCode	3	Overwrite Code
OopAllocate	4	Remote Allocation of Memory
OopMap	5	Remote Mapping of Memory
OopWrite	6	Remote Write to Memory
OopWritePe	7	Remote Write PE to Memory
OopOverwriteCode	8	Remote Overwrite Code
OopUnmap	9	Remote Unmap of Memory
OopThreadCreate	10	Remote Thread Creation
OopThreadApc	11	Remote APC Scheduled

Exploit: ItemType	Value	Related Violation Type
LsassRead	12	LSASS Read
TrackDataRead	13	RAM Scraping
CpAllocate	14	Remote Allocation of Memory
CpMap	15	Remote Mapping of Memory
CpWrite	16	Remote Write to Memory
CpWritePe	17	Remote Write PE to Memory
CpOverwriteCode	18	Remote Overwrite Code
CpUnmap	19	Remote Unmap of Memory
CpThreadCreate	20	Remote Thread Creation
CpThreadApc	21	Remote APC Scheduled
ZeroAllocate	22	Zero Allocate
DyldInjection	23	DYLD Injection
MaliciousPayload	24	Malicious Payload

Oop = Out of Process; Cp = Child Process

Exploit: State	Value
None	0
Allowed	1
Blocked	2
Terminated	3

Script: Action	Value
None	0
Allowed	1
Blocked	2
Terminated	3

APPENDIX A: VDI BEST PRACTICES

Cylance customers can protect both physical and virtual machines with CylancePROTECT technology. This guide explains the best practices for deploying the CylancePROTECT Agent onto Windows-based virtual desktop infrastructure (VDI) workstations.

Note: CylancePROTECT resides at the guest OS level. Hypervisor level capability is not *yet* a CylancePROTECT capability.

Note: CylanceOPTICS is not supported in VDI environments.

CylancePROTECT is proven to work on the following enterprise virtualization technologies:

- Microsoft RDS/Terminal Services
- Microsoft Hyper-V
- Citrix XenDesktop
- VMware Horizon/View
- VMware Workstation
- VMware Fusion

CylancePROTECT works well as a guest OS component and has the following advantages:

- CylancePROTECT is not as IOPS (Input/Output Operations Per Second) intensive on a per guest basis because the technology does not require daily disk scans. Therefore, CylancePROTECT returns capacity to the IOPS budget.
- CylancePROTECT is not as memory intensive on a per guest basis. Therefore, CylancePROTECT returns capacity to the memory budget.

The preparation and deployment of Cylance in virtual environments is similar to deployment on physical machines. However, the following recommendations for VDI deployments will ensure that Cylance performs efficiently in a virtual environment with fewer allocated resources. The objective is to produce a clean image that CylancePROTECT has analyzed so that there are no outstanding malicious files (Unsafe or Abnormal) on the Gold image. For information about Unsafe and Abnormal files, read the [FAQ – What is a Cylance Score?](#) article on the Cylance Support site.

Once the Gold image is thoroughly vetted, production VDI images can be cloned from it. Production machines derived from the master image should run a CylancePROTECT policy that does not perform the Background Threat Detection scan (BTD) since this was already performed on the Gold image. By avoiding unnecessary recurring scans, each production image attaches minimal IOPS load on the bare metal infrastructure.

For information about VDI related issues, read the [VDI Trending Issues](#) article on the Cylance Support site.

At a high level, the tasks are:

1. In the CylancePROTECT Console, create **VDI_preparation** and **VDI_production** policies. These policies, explained in more detail below, will vary in their features.

Example: VDI_preparation includes Background Threat Detection, **VDI_production** does not.

2. Prepare the VDI Gold image:

- a. Install CylancePROTECT.

Note: For non-persistent virtual machines, see "[Non-Persistent VDI Install Parameter](#)" on page 218 for more information on preparing this Gold image.

- b. Apply the **VDI_preparation** policy.

3. Use CylancePROTECT to Safelist or Global Quarantine binaries on the Gold image as necessary.

4. When the Gold image has been prepared and is ready for production, apply the CylancePROTECT **VDI_production** policy.

5. Begin deploying the Gold image onto production machines.

Note: You must set Zone-based updating to **Do Not Update** for the cloned devices.

6. When you are ready to apply an agent update:

- a. Update the Gold image with the new agent.

- b. If any files other than the agent are updated or added to the Gold image, reapply the **VDI_preparation** policy and allow the Background Threat Detection scan to run. If you are only updating the agent, you do not need to run the BTM scan.

- c. Use CylancePROTECT to Safelist or Global Quarantine binaries on the Gold image as necessary.

- d. Apply the **VDI_production** policy.

- e. Reseal the Gold image.

- f. Verify that the agent update was propagated to the clone devices.

Malware Prevention

The following section expands on the overview presented above and details how to add CylancePROTECT malware prevention capabilities to production VDI images.

Gold Image Preparation

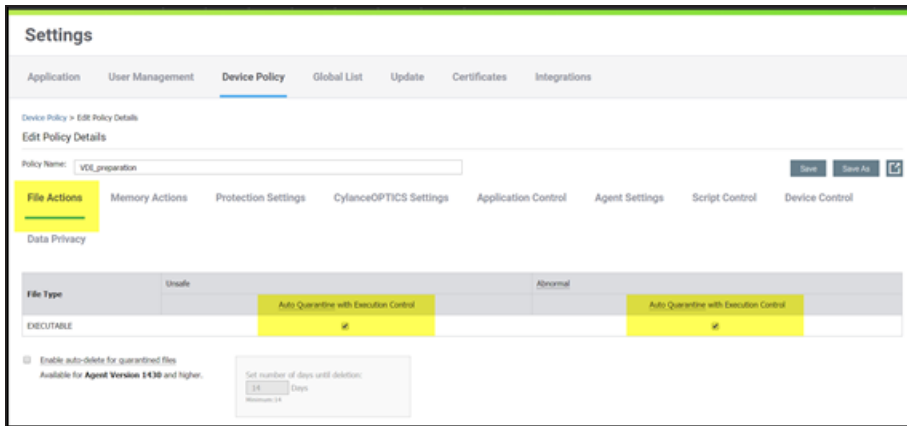
Create the Windows VDI Gold image. For a list of supported OSes, see ["Windows Agent" on page 61](#).

Gold images should be fully scanned and prepared before deploying them as persistent or non-persistent production images. This is accomplished by installing the CylancePROTECT Agent and running a full disk scan, also known as Background Threat Detection (BTD). BTD ensures the image is clean of any resident malware and provides the opportunity to resolve any findings with other installed software applications if they are in a known good state.

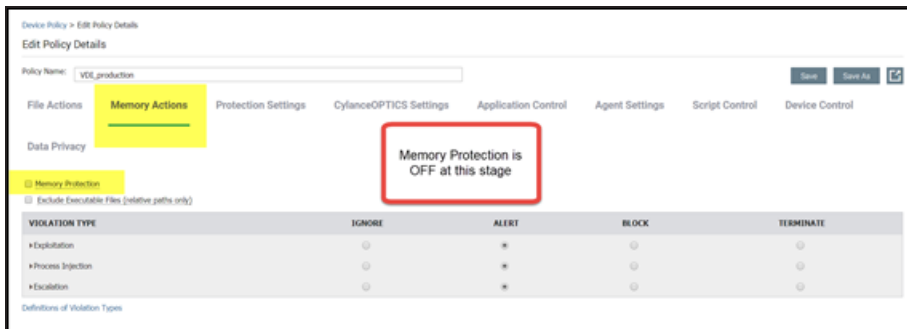
Policy Settings

From the Cylance Console, create a **VDI_preparation** policy, then apply that policy to the Gold image. Typical basic settings from within the device policy screen are as follows:

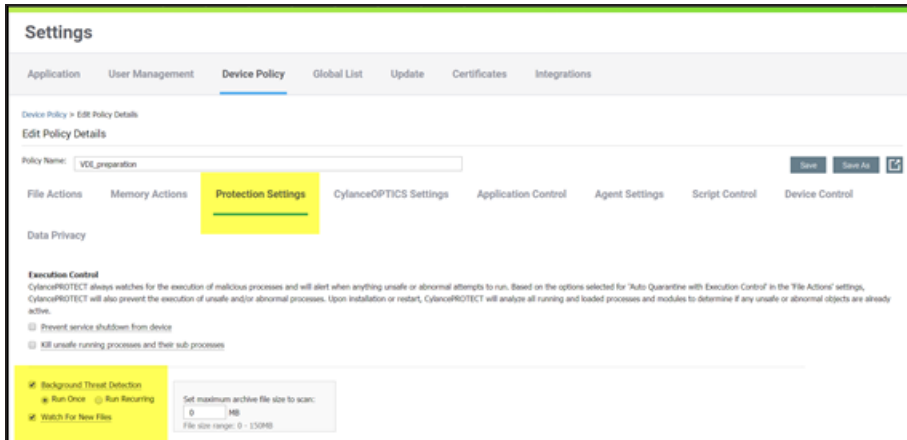
File Actions



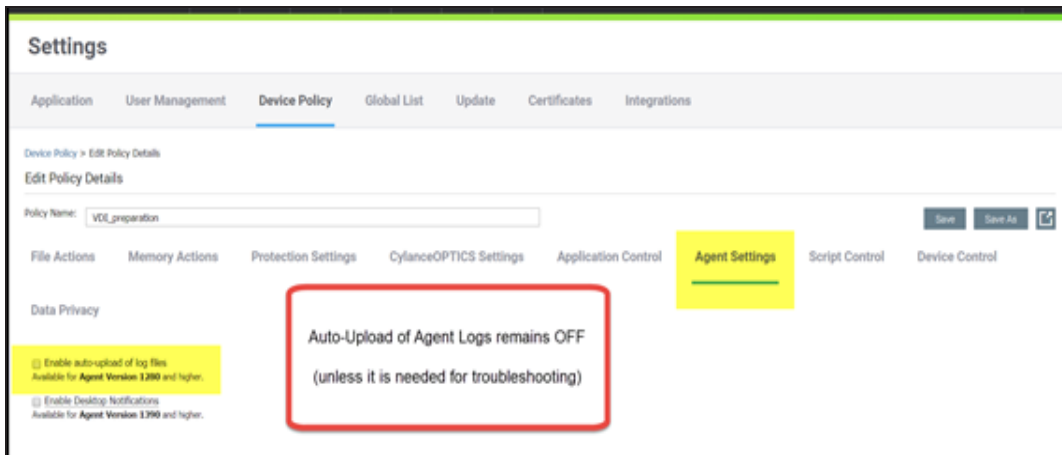
Memory Actions



Protection Settings



Agent Settings



Agent Installation

Agent Installation can be approached like a traditional installation on a physical machine. The CylancePROTECT Agent must first be downloaded from the Cylance Console.

Example: MSI installation

- MSI Installer (using Standard Installer options)

```
msiexec /package CylancePROTECT_x64.msi /quiet  
PIDKEY=<INSTALLATION TOKEN> LAUNCHAPP=1
```

- MSI Installer (using Windows Installer options)

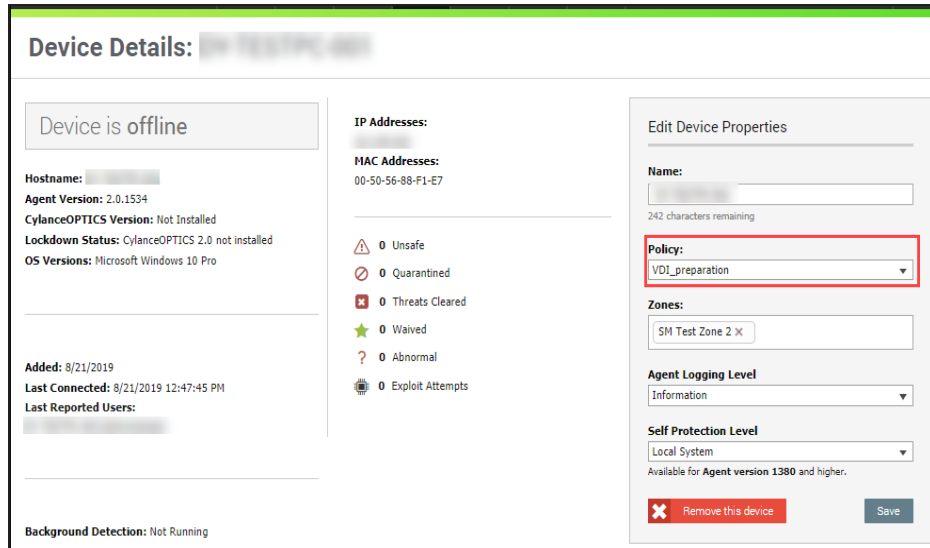
```
msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN>  
LAUNCHAPP=1
```

For further installation parameters and instructions, see ["Windows Installation Parameters" on page 67](#).

For non-persistent virtual machines, see ["Non-Persistent VDI Install Parameter" on page 218](#) for more information on preparing this Gold image.

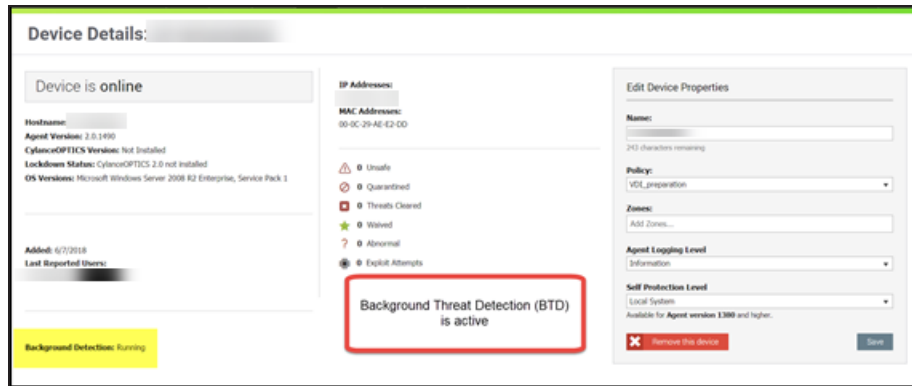
Apply the Policy and Review Findings

1. Open the Cylance Console to the Devices page.
2. Select the Gold image from the device list. The Device Details page for the Gold image displays.
3. Under Edit Device Properties, select the **VDI_preparation** policy from the Policy drop-down list:

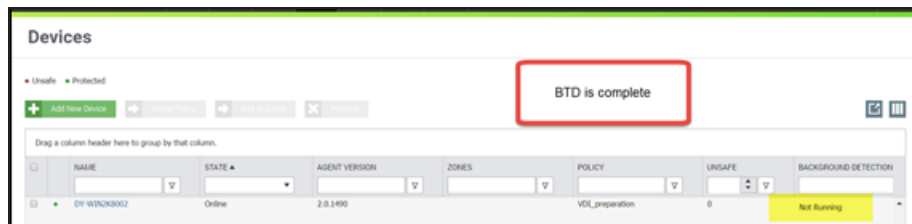


4. Click **Save**.

Once the agent is using the policy, typically within a few minutes, the BTD scan will begin. Allow the BTD scan to fully complete prior to using it as the Gold image. By design, BTD requires several hours to complete depending upon the size of the disk and activity on the image as it is being scanned. The device details will indicate whether the BTD is "Running" or "Not Running" (i.e. completed).



- Once BTD is complete, you will want to review findings in the console and take action on any findings by Safelisting or excluding any false positive convictions. Once this is complete and the machine is in a safe (or green state in the Devices tab), the image is now ready to be used as the master for production images.



Secure Production Images

Make sure your virtual solution (Citrix, VMware, etc.) deploys each cloned image with a unique UUID or ID that differs from the Gold image. Image uniqueness is typically part of each vendor's deployment process and is outside the scope of this document. Virtual UUID's are used to calculate each device's "Device Fingerprint" ID that is used for registration to the Cylance Console. If the UUID for each image is identical, this will cause each VDI desktop instance to overwrite the others (with that same UUID / ID) causing console confusion, thus this is to be avoided.

Next, let's explore persistent versus non-persistent desktops. Persistent desktops are spawned from the Gold image and typically are not destroyed after use. They "persist" even when the user goes home for the evening, resuming the next day with the same VDI desktop. For persistent machines that do not refresh regularly, there are no special considerations that need to be taken into account, as these machines register to the console and are managed like any other physical or persistent virtual device.

Conversely, non-persistent desktops are typically one-time use systems. The user starts the VDI desktop session, performs work and then upon shutdown, the system is destroyed. While being used, these non-persistent systems check-in to the Cylance Console and are registered as a

device. If the UUID already exists, then this new device is registered as a duplicate. When these devices are destroyed, they will appear as offline duplicate device records that never come back online because they no longer exist. Unless Zone Rules are configured to automatically assign a policy to devices, the newly registered device received the Default policy instead of the previously assigned policy. Depending on the Default policy configuration, this could impact the level of protection for the device. To avoid this, it is recommended to configure Zone Rules so all newly registered devices automatically receive the appropriate policy.

To avoid duplicate devices in the Console, see ["Non-Persistent VDI Install Parameter" on page 218](#) for more information on preparing this Gold image.

1. When the Gold image has been prepared and is ready for production, apply the CylancePROTECT **VDI_production** policy. It is from this Gold image that clones will be created, so deploying with the correct policy assigned is critical. Typical settings from within the device policy screen are as follows:

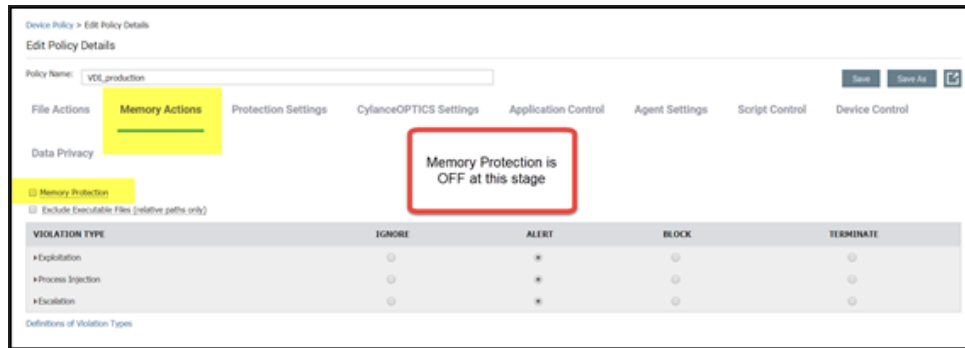
File Actions

This policy adds Auto Quarantine with Execution Control.



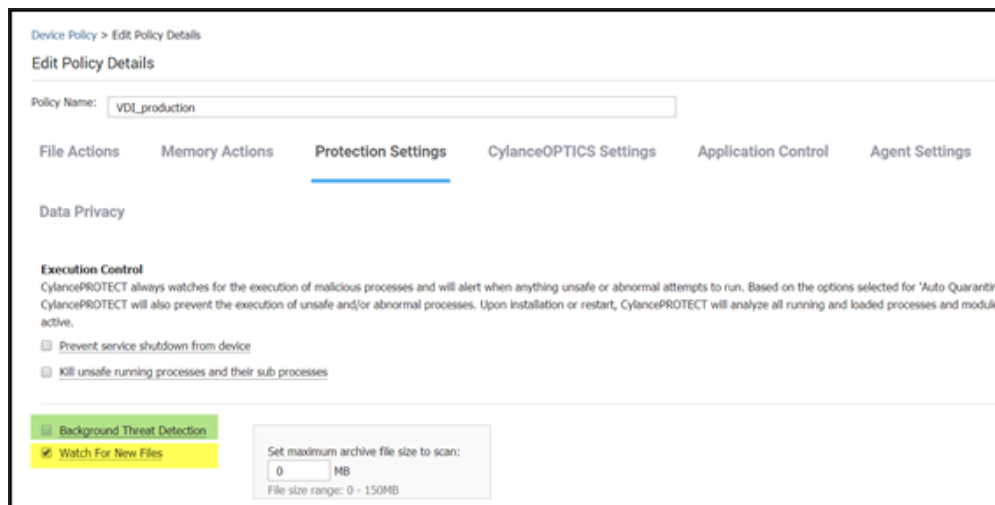
Memory Actions

The use of Memory Protection for VDI is described in ["Layering in Memory Protection & Script Control" on page 218](#).



Protection Settings

Background Threat Detection is toggled OFF in this policy. It is not necessary to re-run BTM for clone images since this was completed during the Gold image preparation phase.



- Save the Policy and deploy it to the Gold image that will be used as the source for production clones. Background Threat Detection is not recommended, nor necessary for production virtual images since the image is in a known clean state after completion of the initial Background Threat Detection within the Gold image policy. By selecting **Watch for New Files** (aka, file watcher) in the policy, CylancePROTECT will inspect and prevent execution of any new threats that are introduced to the clones' file system.

Note: If you are experiencing high IOPS, try disabling Watch For New Files to see if that resolves the issue.

Additionally, it is recommended to disable the Agent UI in certain virtual environments (such as Citrix XenApp) to conserve overall system resources. To install the agent without

the UI enabled, you can specify an installation parameter (LAUNCHAPP = 0). See [Microsoft Windows Command Line Options](#) for more details.

3. Create a template from the Gold image.
4. Create the clone images based on the Gold image template with the VDI_production policy applied to them.

Layering in Memory Protection & Script Control

CylancePROTECT also offers Memory Protection and Script Control as optional protective policy components. Running the CylancePROTECT Agent at the guest OS level on each virtual machine provides the added benefit of being able to protect against malicious scripts and malicious processes running in memory. Both Memory Protection and Script Control may require special consideration in VDI environments.

Both of these functions use a process injection method whereby the Agent code injects itself into running processes to identify and block unwanted or unauthorized code from running. Any product that injects itself into running processes such as plugins, tools, or DLLs – especially those used in virtualized management – may cause adverse effects, therefore testing is warranted. This can, at times, conflict with CylancePROTECT's ability to properly monitor memory. Hence, it is recommended to always test Memory Protection and Script Control on test machines before deploying to production. Please see the following Support Knowledgebase Article for known issues with Memory Protection: [Known Memory Protection and Script Control Incompatibilities](#).

Cylance Support constantly monitors these types of operational issues. This article will be updated as new information becomes available.

If any system conflicts or instabilities persist, Compatibility Mode for Memory Protection can be enabled as a fail-safe option. See [CylancePROTECT Compatibility Mode for Memory Protection](#) for more information.

In summary, we recommend that you test with Memory Protection in Alert Only mode and make more stringent policy changes from there. If the system becomes unstable, you can always turn Memory Protection off. Upon the next agent check-in the policy will be updated and stability typically returns.

Non-Persistent VDI Install Parameter

Cylance uses a unique fingerprint to identify endpoints with a CylancePROTECT Agent.

There are two different, but similar installation parameters that can be utilized:

- VDI=<X>

This feature is available in CylancePROTECT Agent version 1490 and higher.

- AD=1

This feature is available in CylancePROTECT Agent version 1520 and higher.

Note: Currently, the AD parameter is not supported for the CylancePROTECT + CylanceOPTICS Unified EXE Installer. If you wish to use the AD parameter, please use the CylancePROTECT + CylanceOPTICS unified MSI installer.

Details for VDI=<X>

Use the below installation parameter during initial installation of the Agent on a Master image to use this feature.

Installation Parameter:

VDI=<X>

Example: `msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> VDI=2 LAUNCHAPP=1`

Where <X> is a "counter" for the total number of machines or images not connected to the domain (including the Master image) before creating a pool of workstations. The value for <X> determines when the Agent should start identifying the virtual machine utilizing VDI fingerprinting instead of the default Agent fingerprinting mechanism.

Example: VDI=2, where "2" is the total number of machines or images not connected to the domain (Master image + Additional/Parent image) before creating a pool of workstations.

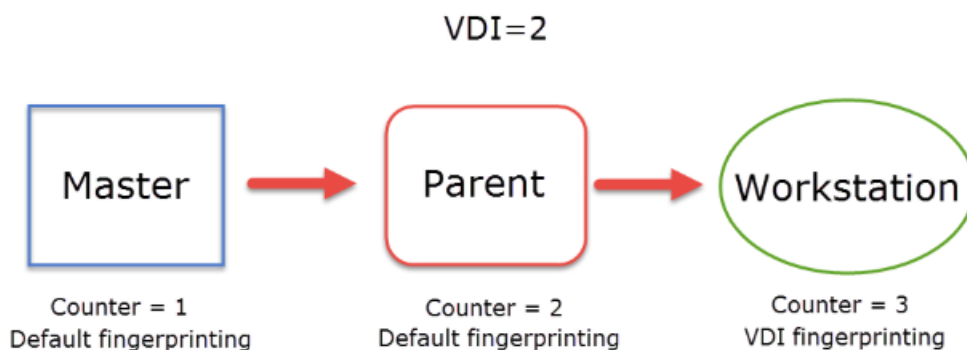


Figure 49: VDI=X Example

1. The Agent is installed on the Master image using the above installation parameter. The Agent generates a fingerprint utilizing the default method. This creates registry entries for the fingerprinting as well as a registry containing a "counter".

2. A Parent image is provisioned from the Master image. The Agent generates a unique fingerprint, separate from the Master image. The "counter" registry entry is now set to "2", identifying that the Parent image is the second machine. The default fingerprinting method is utilized for the Parent image because the "counter" has not exceeded a value of "2".
3. Machines are provisioned from the Parent image. At this point, when the Agent generates a unique fingerprint, the Agent will see that the "counter" now has a value of "3". The Agent now knows to use the VDI fingerprinting method instead of the default fingerprinting method, preventing duplicate machines from appearing on the Console.

Details for AD=1

Use the below installation parameter during initial installation of the Agent on a Master image to use this feature.

Installation Parameter:

AD=1

Example: `msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> AD=1 LAUNCHAPP=1`

The installation parameter "AD=1" is similar to "VDI=<X>" in that both are designed to use VDI fingerprinting when installed on a master image that is domain connected.

The difference between AD=1 and VDI=<X> is that AD=1 when used on a master image that is domain connected, will immediately use VDI fingerprinting on the master image and subsequently created pool of workstations.

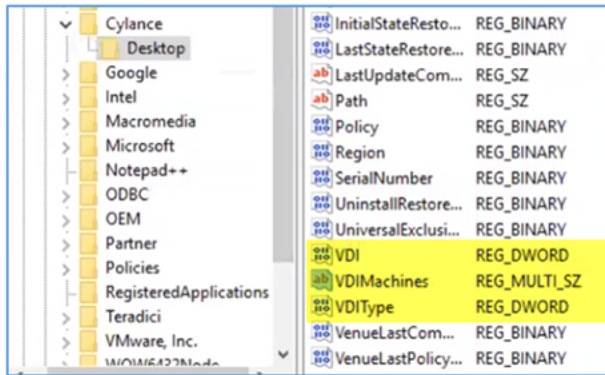
VDI=<X> utilizes a counter "X" and has a delayed effect, where as "AD=1" is immediate upon installation.

AD=1 will take priority over the VDI=<X> installation parameter.

Verification

After the Agent is installed using the VDI install parameter, you can check the registry to verify. The following registry entries appear in HKLM\SOFTWARE\Cylance\Desktop:

- VDI
- VDIMachines
- VDIType



VDI Agent Update Process

It is recommended to set any virtual machines to "Do Not Update" or set the virtual machines to a specific Agent version on the CylancePROTECT Console under **Settings > Update**.

If the entire environment is virtual, simply set "Production" to "Do Not Update".

If the environment is mixed, and there is a specific subsection of virtual machines, you can use Zone-based Updating to assign specific virtual machines to a specific Agent version. Doing so prevents the machine from updating to a different Agent version.

If an Agent update is required, it is recommended to only update the Gold Image. The updated Gold Image would then be used to create children/clone virtual machines which will then contain the updated Agent.

For information on Zone-based updating, see ["Zone Organization for Policy Management" on page 52](#).

1. Install the agent update on the Gold image.
2. If any files other than the agent are updated or added to the Gold image, reapply the **VDI_preparation** policy and allow the Background Threat Detection scan to run. If you are only updating the agent, you do not need to run the BTM scan and can skip to step 5.
3. Use CylancePROTECT to Safelist or Global Quarantine binaries on the Gold image as necessary.
4. Re-apply the **VDI_production** policy.
5. Reseal the Gold image.
6. Verify that the agent update was propagated to the clone devices.

APPENDIX B: CYLANCE EXCLUSIONS

AND WHEN TO USE THEM

The following is general guidance on what each Cylance exclusion does and when the exclusion could be used. Instructions on how to enable or disable exclusions are provided in the appropriate links to other articles.

Policy Safe List (File Actions)

The Policy Safe List is similar to the Global Safe List, except this is at the Policy level. The Policy Safe List takes precedence over the Global Quarantine List. So a file added to the Policy Safe List will run on any device assigned to the policy, even if that file is also added to the Global Quarantine List.

Example Scenario:

As an IT Administrator, I frequently use privilege escalation tools like PSEXEC to perform my daily tasks. I do not want my users to have the same ability, and I want to prevent them from using such tools without impacting my daily duties. To do this, I can add PSEXEC to the Global Quarantine List, and add the same file hash to my Policy Safe List. I then make sure only myself and other authorized users are assigned to that particular Device Policy where I safelisted PSEXEC.

Result: All users that are not assigned to the Device Policy will have PSEXEC quarantined, but users assigned to the Device Policy will be able to use it.

Exclude Executable Files (Memory Protection)

Memory Protection functions by hooking into processes and monitoring for specific actions that those processes are performing. If a process performs a particular action that the Agent is monitoring, such as an LSASS dump, the Agent will react to that action depending on the Device Policy. There is no "analysis" that occurs with Memory Protection, it is a straight forward "if the process is doing something the Agent is monitoring for, the Agent will respond with the instructed action." Because of this, it is possible for false positives to occur where an application is being alerted on, blocked, or terminated by Memory Protection. This is not a deficiency with Memory Protection, but how the application (being monitored) was designed to function.

Excluding executable files allows you to tell Memory Protection to ignore a certain executable.

Example Scenario:

I am using an application called "Text.exe". Memory Protection is assigned to *Block* in my Device Policy. I know that Test.exe is a known good application, but every time I run the application in a certain manner, Memory Protection blocks the process and thus prevents me from performing my job duties.

To allow Test.exe to run, I add a Memory Protection exclusion like:

- \Application\SubFolder\Test.exe

Memory Protection exclusions are relative paths. This means that a drive letter is not required, and it is possible to exclude all the way down to the executable level.

Further Examples:

- \SubFolder\Test.exe
- \Test.exe

Note: It is not recommended to exclude at the executable level as this would allow any executable with that name to run (not be monitored by Memory Protection). Meaning, if a malicious file were named Test.exe, it would be allowed to run on any device with the Memory Protection exclusion in the Device Policy.

Exclude Specific Folders (Protection Settings)

Excluding Specific Folders can also be referred to as Directory Whitelisting or Directory Safelisting. When a specific directory is excluded, the Agent will ignore files in that particular directory, including sub-folders.

If Allow Execution is enabled, the Agent will completely ignore any executables that are launched in those directories.

Example Scenario:

I am a developer building an application. During my compilation, numerous temporary files will drop in a specific directory (C:\DevFiles\Temp). These files are seen as Unsafe by the Agent due to the various characteristics of the file, and are subsequently quarantined.

To prevent further files from being quarantined, I request that the directory these files are dropping in be whitelisted. My Cylance Console administrator then adds the following exclusion to my assigned Device Policy:

- C:\DevFiles\Temp

Folder Exclusions (Script Control)

Script Control exclusions are similar to Directory Whitelisting in that excluding a directory will allow the scripts in that particular directory to run.

Exclusions for Script Control are relative paths. Exclusions will also include sub-folders in that directory.

Example Scenario:

I am an IT administrator attempting to run a script located in C:\Scripts\Subfolder\Test. The script is blocked by Script Control every time I attempt to run the script.

To resolve this I add the following exclusion to my Device Policy:

- \Scripts\Subfolder\Test

Further Exclusion Examples:

- \Scripts\
■ \Subfolder\
■ \Test
■ \Subfolder\Test

APPENDIX C: GLOSSARY

- Abnormal** — A suspicious file with a lower score (1 – 59); less likely to be malware.
- Administrator** — Tenant manager for **CylancePROTECT**.
- Agent** —**CylancePROTECT** Endpoint Host that communicates with the Console.
- Application Control** — Device Policy setting that enables administrator to implement system lockdown for organization's devices.
- Audit Log** — Log that records actions performed from the **CylancePROTECT** Console.
- Auto-Quarantine** — Automatically prevent execution of all *Unsafe* and/or *Abnormal* files.
- Auto Upload** — Automatically upload any unknown Portable Executable (PE), detected as Unsafe or Abnormal,
- Background Threat Detection** — Full Disk Scan that is lightweight and is used to detect dormant threats.
- Console** — **CylancePROTECT** Management User Interface.
- Cylance Cloud** — The Mathematical Model used to score files.
- Device Policy** —**CylancePROTECT** policy that can be configured by an organization administrator that defines how threats are handled on all devices.\
- File Watcher** — Feature that detects and analyzes any new files on disk.
- Global Quarantine** — Prevent execution of a file globally (across all devices in an organization).
- Global Safe List** — Allow execution of a file globally (across all devices in an organization).
- Memory Protection** — Device Policy setting that monitors and blocks exploit attempts.
- Organization** — A tenant account using the **CylancePROTECT** service.
- Quarantine** — Prevent execution of a file locally (on a specific device).
- Threats** — Potentially malicious files detected by **CylancePROTECT**, classified either as *Unsafe* or *Abnormal*.
- Unsafe** — A suspicious file with a high score (60 – 100) likely to be malware.
- Waive** — Allow execution of a file locally (on a specific device).
- Zone** — A way to organize and group devices within an organization according to priority, functionality, and so forth.
- Zone Rule** — Feature that enables automation of assigning devices to specific zones based on IP addresses, Operating System, and device names.

 **BlackBerry** | **CYLANCE.**

www.cylance.com

