Dell Threat Defense

Installation and Administrator Guide

Powered by Cylance

v20.05.06

© 2020 Dell Inc.

Registered trademarks and trademarks used in the Dell Threat Defense suite of documents: Dell™ and the Dell logo are trademarks of Dell Inc. Microsoft®, Windows®, Windows Server®, Active Directory®, Azure®, and Excel® are registered trademarks of Microsoft Corporation in the United States and/or other countries. OneLogin™ is a trademark of OneLogin, Inc. OKTA™ is a trademark of Okta, Inc. PINGONE™ is a trademark of Ping Identity Corporation. Mac OS® and OS X® are registered trademarks of Apple, Inc. in the United States and/or other countries.

2020-5-6

Information in this document is subject to change without notice.

Contents

OVERVIEW

Dell Threat Defense, powered by Cylance, 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. Threat Defense analyzes potential file executions for malware in the Operating System.

This guide explains using the Threat Defense Console, installing the Threat Defense Agent, and how to configure both.

How It Works

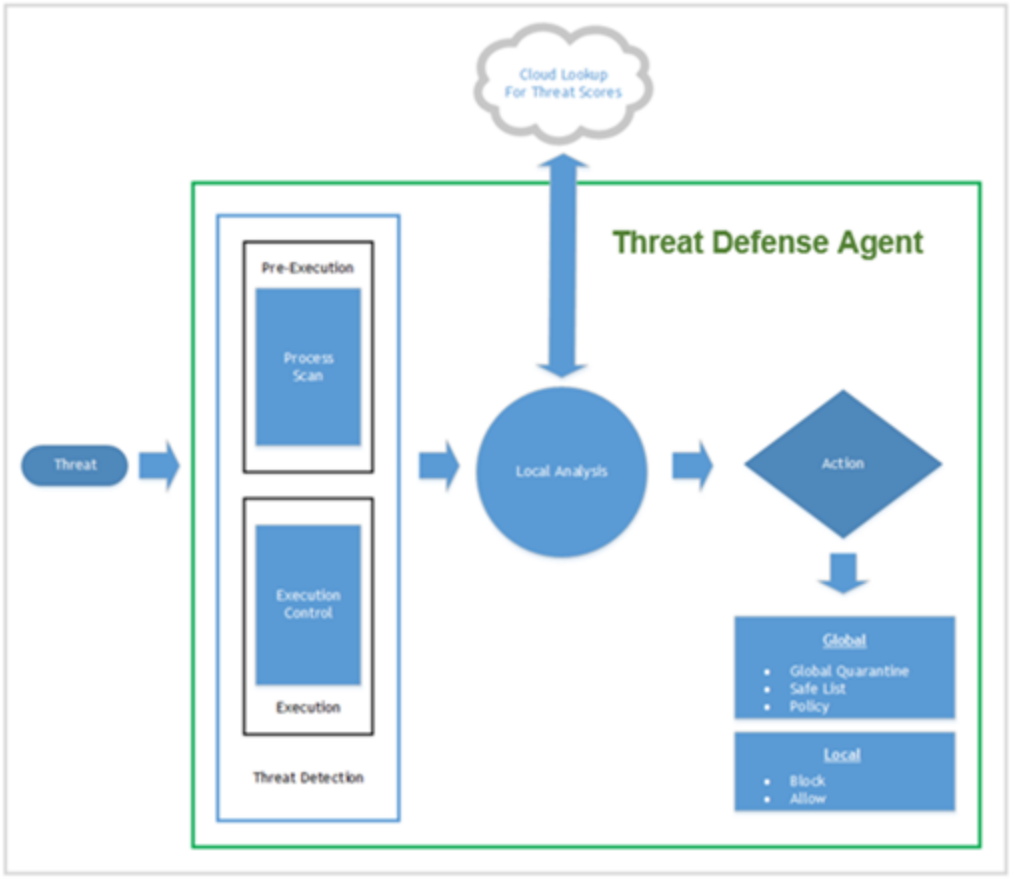


Figure 1: Threat Defense Flowchart

Threat Defense 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 Threat Defense. By constantly training on enormous, real-world data sets, Threat Defense stays one step ahead of the attackers.

- **Threat:** When a threat is downloaded to the device or there is an exploit attempt.
- **Threat Detection:** How the Threat Defense Agent identifies threats.
  - **Process Scan:** Scans processes running on the device.
  - **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.
- **Analysis:** How files are identified as malicious or safe.
  - **Cloud Lookup for Threat Scores**: 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.

Login

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

- North America: https://dellthreatdefense.cylance.com
- Asia-Pacific Northeast: https://dellthreatdefense-apne1.cylance.com

- Asia-Pacific Southeast: https://dellthreatdefense-au.cylance.com
- Europe: https://dellthreatdefense-euc1.cylance.com
- South America East: https://dellthreatdefense-sae1.cylance.com

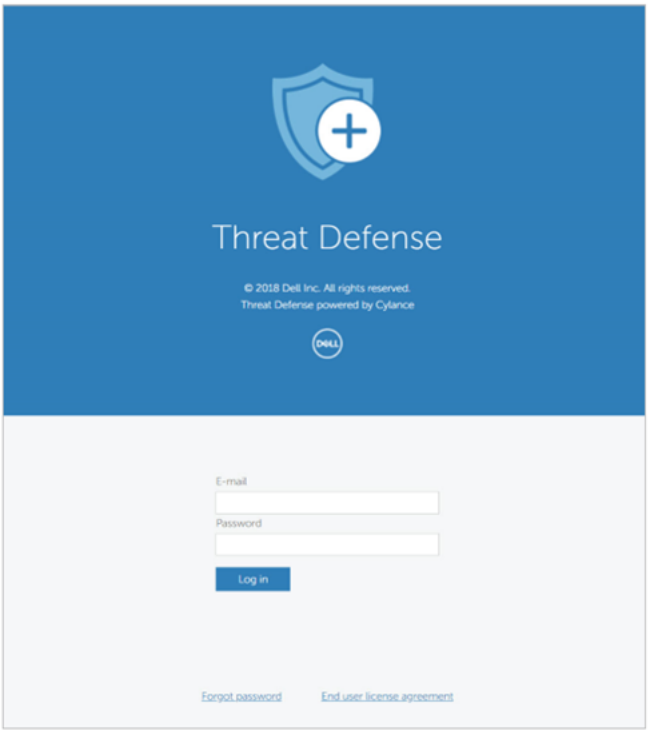


Figure 2: Console Login

CONSOLE CONFIGURATION

The Threat Defense 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).

The Threat Defense Console supports the following languages:

English	French	German	Italian
Japanese	Korean	Portuguese (Brazil)	Portuguese (Portugal)
Spanish			

Table 1: Supported Threat Defense Console Languages

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.

To Add a Policy

1. Select **Settings > Device Policy**.
2. Click **Add New Policy**.
3. Enter a Policy Name and select policy options.
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 Dell functions in your environment, you can create new policies with more features enabled.

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. With Auto-Upload enabled, suspicious files that have never been analyzed by Cylance are sent to Cylance for further analysis. This is only for files that are set to auto-run or are manually executed by the user.

       No personally identifiable information is shared with the Threat Defense Console or with other tenants (organizations).

       If the file is available for you to download (to perform your own threat research), the file name is replaced with the SHA256 hash and removes the file extension to prevent accidental detonation of the malicious file.

       WARNING: The contents of the downloaded file are not altered. If you change the file name to include the original file extension (like EXE), the file will work if launched.

    b. 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*.

    c. 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*).

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

    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 Dell'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**.

   - *Auto-Quarantine* moves any malicious files to the quarantine folder.

5. 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 Threat Defense as either *Unsafe* or *Abnormal*.

Tip: To learn more about the classification of *Unsafe* or *Abnormal* files, refer to "Threat Protection" on page 74.

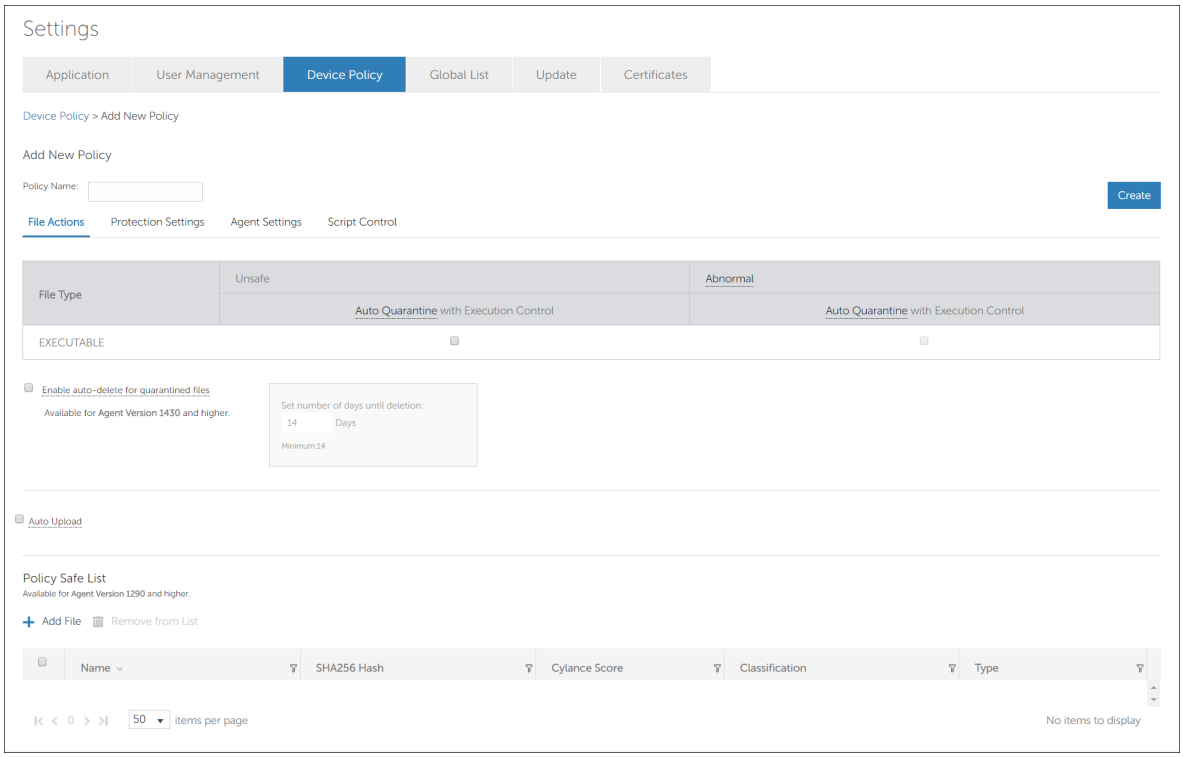


Figure 3: Policy Details > File Actions

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.

- `C:\ProgramData\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. Threat Defense 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 1432 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: This feature requires Agent 1432 or higher. For Agent 1422, or lower, upgraded to Agent 1432, 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.

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.

Threat Defense only uploads and analyzes unknown Portable Executable (PE) files. If the same unknown file is discovered on multiple devices in the organization, Threat Defense 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.

For more information about handling file exceptions (*Quarantine* or *Safe*) at the different levels (*Local*, *Policy*, or *Global*), see "Appendix B: Handling Exceptions" on page 131.

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**.

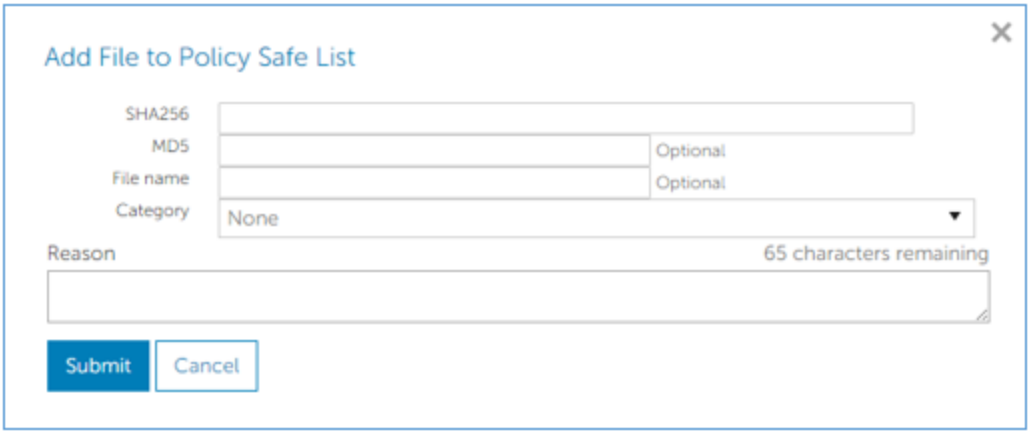


Figure 4: Add a File to the Policy Safe List

Protection Settings

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

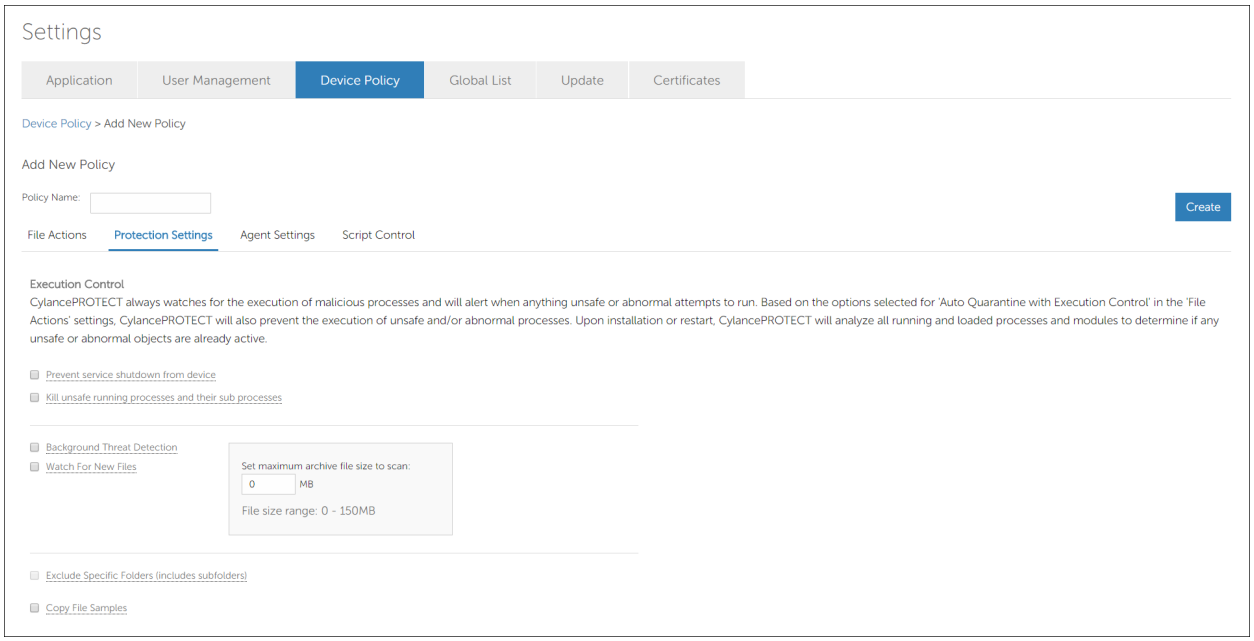


Figure 5: Policy > Protection Settings

Execution Control

Threat Defense 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 Threat Defense 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 Dell'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 63, 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, use an absolute path from the drive root (macOS doesn'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

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 Threat Defense considers *Unsafe* or *Abnormal*.

- Supports CIFS/SMB network shares.
- Specify one network share location. 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 not compressed.
- Files are not password protected.

WARNING: FILES ARE NOT PASSWORD PROTECTED. CARE MUST BE TAKEN SO THE MALICIOUS FILE IS NOT INADVERTENTLY EXECUTED.

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.

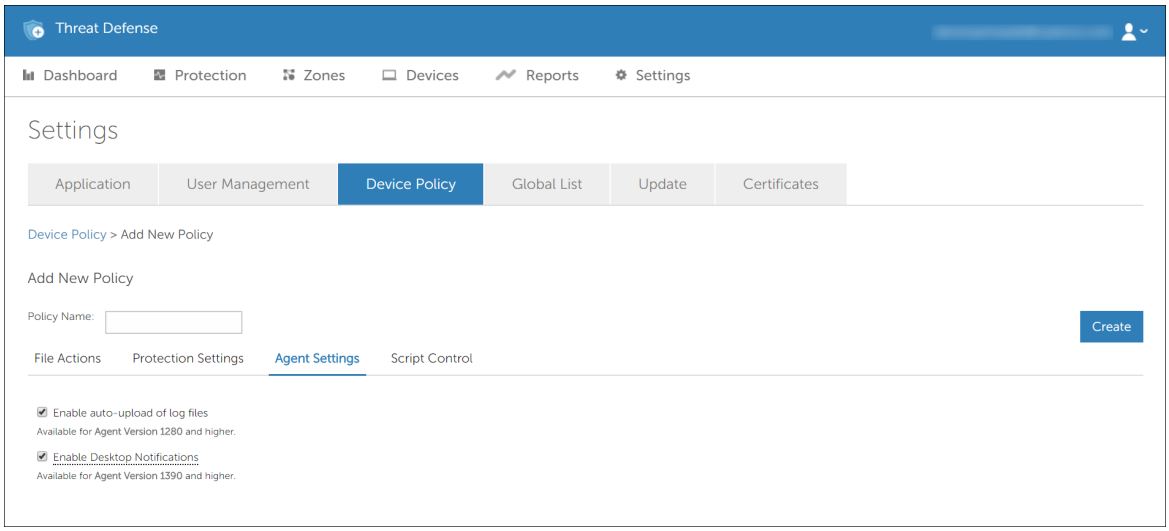


Figure 6: Device Policy > [select a device] > Agent Settings

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 1392 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.

3. Restart the Agent UI.

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 1382 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**.
    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.
    c. **Approve scripts in these folders (and subfolders):** Script folder exclusions must specify the relative path of the folder.
    d. **Block PowerShell Console usage:** Blocks the PowerShell console from launching. This provides additional security by protecting against the use of PowerShell one-liners. PowerShell must be set to Block for this option to

appear.

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.

4. Click **Save**.

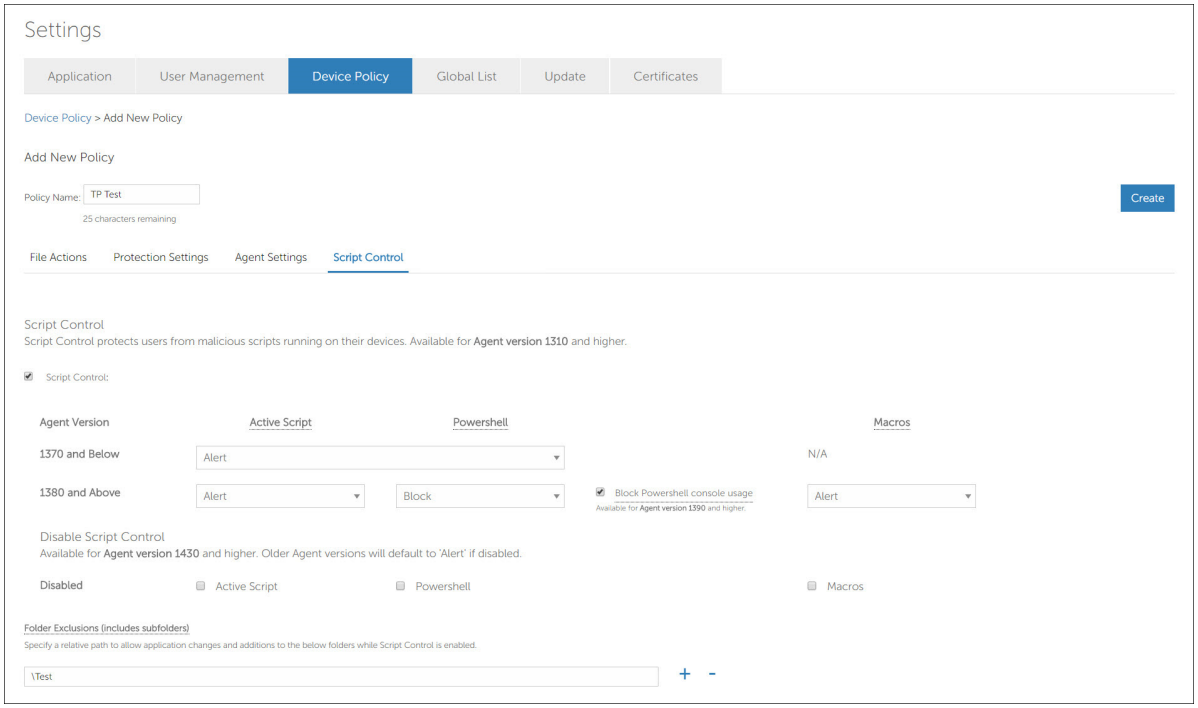


Figure 7: Policy Details > Script Control

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

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 Threat Defense, 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 will only select all entries on the displayed page. Entries on other pages in the list will not be selected.

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. Threat Defense 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 58.

Add a Test or Pilot Zone

1. Select **Settings > Agent 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**.

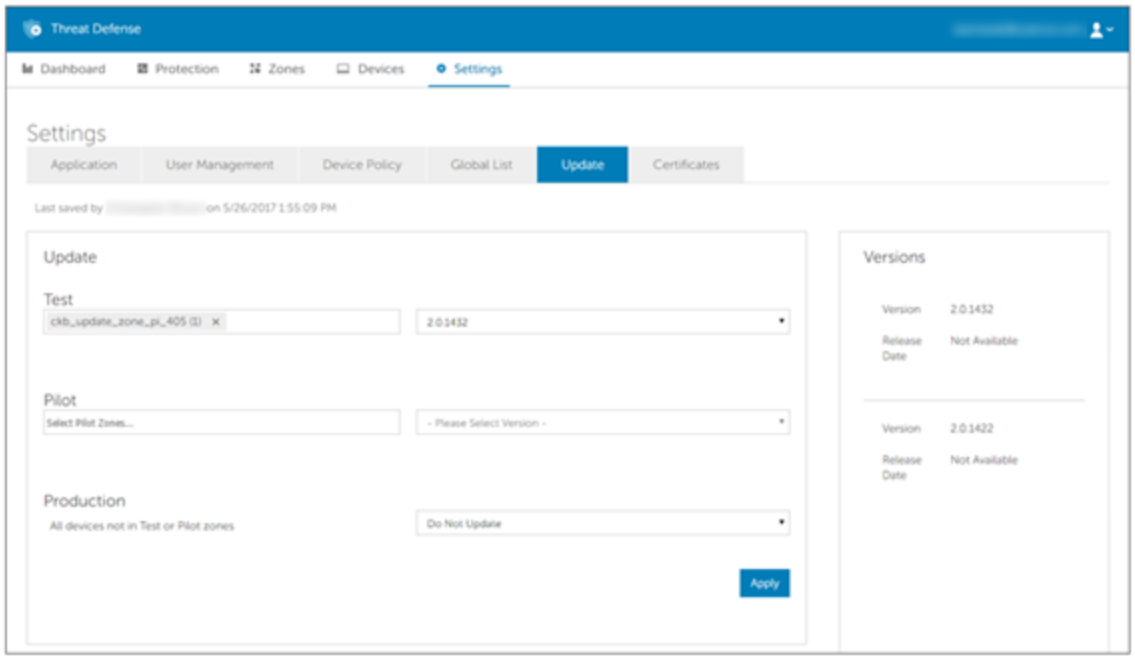


Figure 8: Zone-based Updating

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 — Workstations – Exclusions
- Policy Zone — Servers

- Policy Zone — Servers — Exclusions
- Policy Zone — Executives — High Protection

Dell 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.

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**.

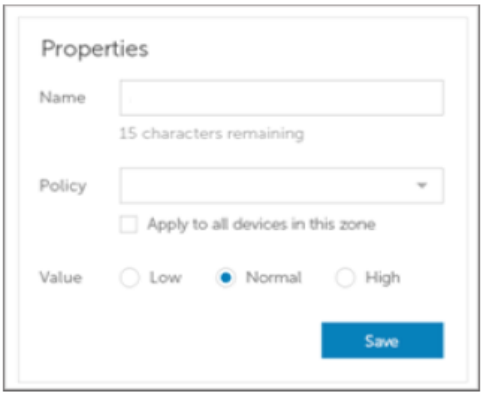


Figure 9: Change Zone Properties

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**.

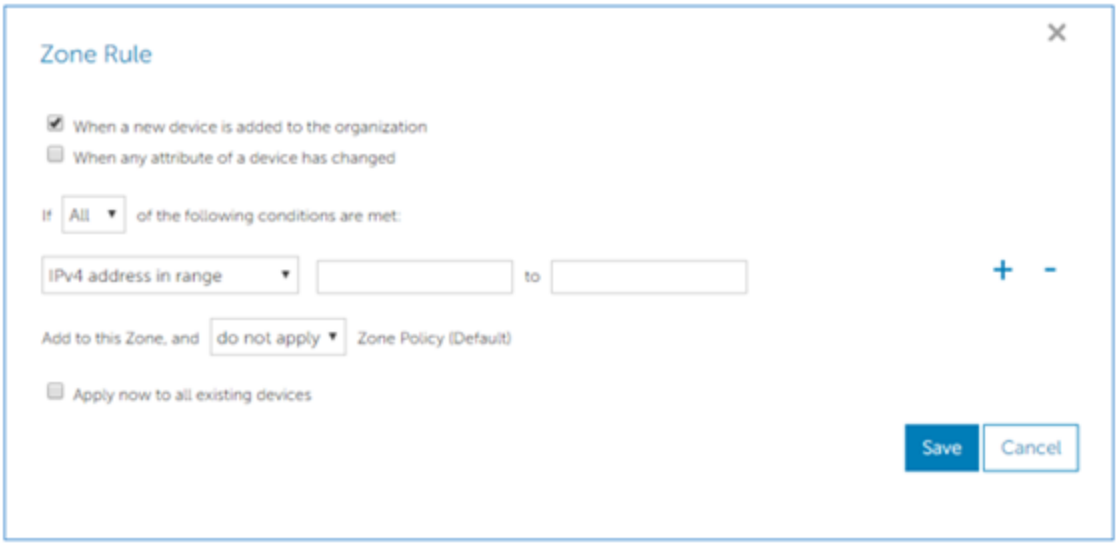


Figure 10: Zone Rule

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.
- **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.

- **Member Of (LDAP):**
  - Is: Member Of information must match this string.
  - Contains: Member Of information must 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.
- **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 17.
- 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=Dell,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*.

Note: If permission to view a Zone does not exist, and the Zone link in the Zones column is clicked anyway, a Resource Not Found page displays.

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

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 with an Administrator or Zone Manager account.
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 Threat Defense Agent on each endpoint. Once connected to the Dell Console, apply policies (to manage identified threats) and organize devices based on organizational needs.

The Threat Defense 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.

Download the Install File

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 Threat Defense, 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 Threat Defense + CylanceOPTICS Windows Agent Installer 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.

Tip: If a Zone Rule is set up, Devices can be automatically assigned to a Zone if the device matches the Zone Rule criteria.

Windows Agent

System Requirements

Dell 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 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 8 and 8.1	X	X	*
Windows 10	X	X	*
Windows 10 IoT Enterprise	X	X	*
Windows Server 2008 and 2008 R2	X (2008 only)	X	*
Windows Server 2012 and 2012 R2	–	X	*
Windows Server 2016	–	X	Supports Standard, Data Center, Essentials, and Server Core editions. *
Windows Server 2019	–	X	

* For specific requirements, read the System Requirements article.

Additional Windows Requirements

Type	Description
Processor	■ 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	■ 2 GB
Available Hard Drive Space	■ 300 MB **Note:** Disk space usage can increase depending on features enabled, like setting the log level to Verbose.)
Additional Software/ Requirement	■ .NET Framework 3.5 (SP1) or higher (**Note:** .NET 4.0 must be the full version, not the .NET 4 Client Profile.) **Note:** A fully functioning installation of .NET Framework that meets the above specifications is a requirement for the Threat Defense Agent to be installed and function as expected. ■ Internet Browser ■ Internet access to login, access the installer, and register the product ■ Local administrator rights to install the software ■ Root Certificates: • VeriSign Class 3 Public Primary Certification Authority - G5 • GeoTrust Global CA • thawte Primary Root CA • DigiCert Global Root C **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.
Other	■ TLS 1.2 is supported with Agent version 1422 or higher, and requires .NET Framework 4.5.2 or higher

Install the Agent — Windows

Ensure that all prerequisites are met prior to installing Threat Defense. See "System Requirements" on the previous page for more information.

1. "Download the Install File" on page 30.
2. Double-click DellThreatDefense.exe (or MSI).

3. Click **Install** at the Threat Defense setup window.

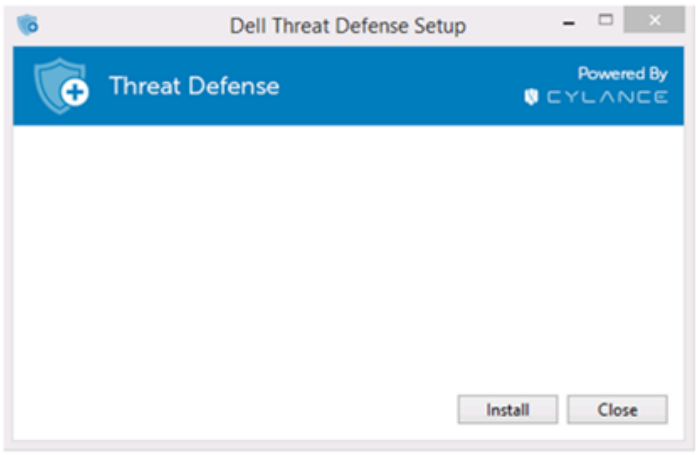


Figure 11: Setup Window

4. Enter the Installation Token provided by the Threat Defense Tenant and click **Next**

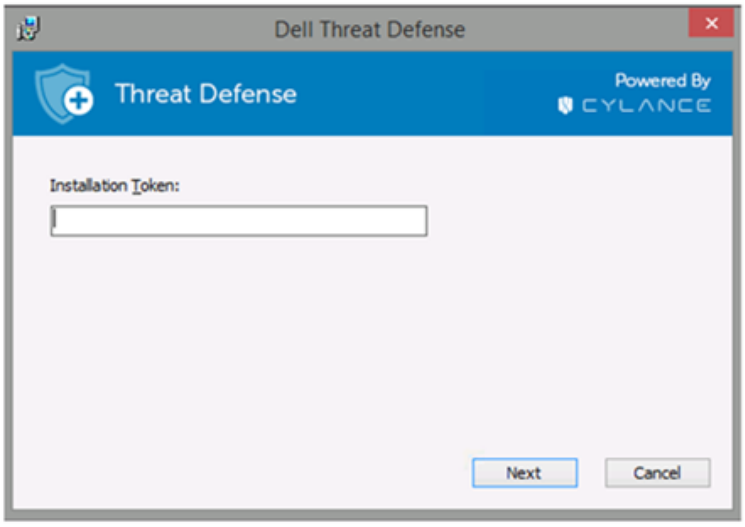


Figure 12: Installation Token Input Screen

Note: Contact your Threat Defense administrator or see KB article How To: Manage Threat Defense if access to the Installation Token is not available.

5. Optionally change the destination folder of Threat Defense.
6. Click **OK** to begin the installation.

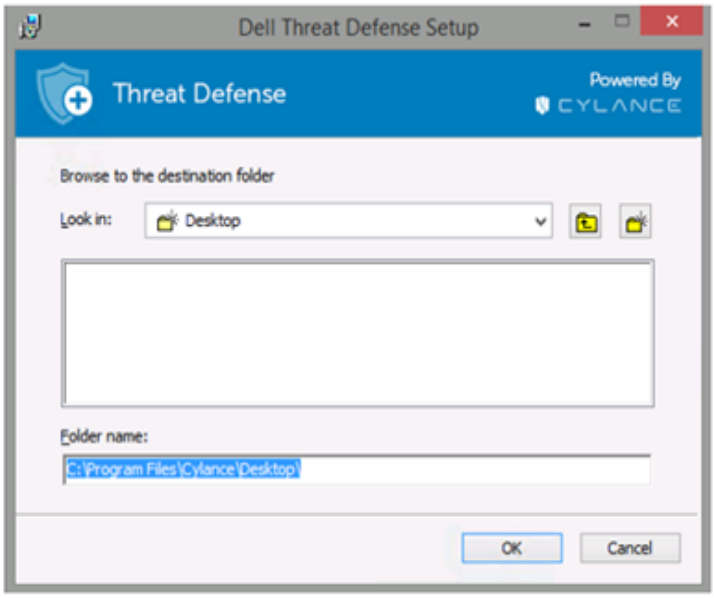


Figure 13: Installation Location

7. Click **Finish** to complete the installation. Select the check box to launch Threat Defense.

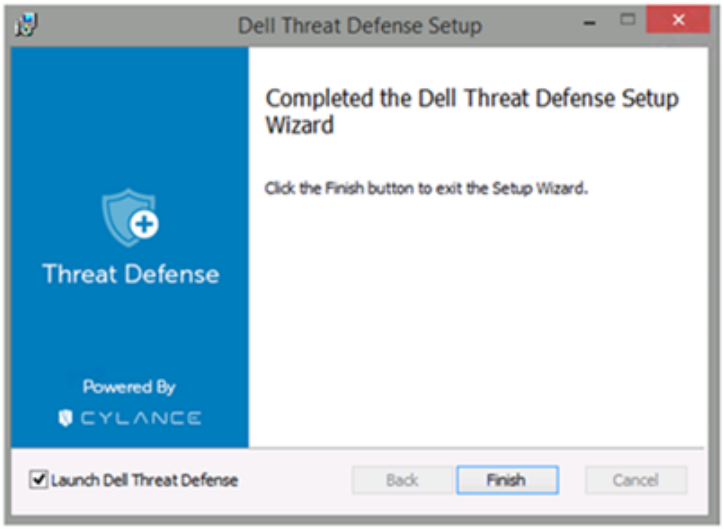


Figure 14: Installation Complete

Windows Installation Parameters

The Agent can be installed interactively or non-interactively through GPO, Microsoft System Center Configuration Manager (commonly known as SCCM), and MSIEXEC. 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
VENUEZONE	"Zone_Name"	Requires Agent version 1382 or higher. ■ 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 ", Dell removes the whitespace during device registration. **Note:** Tabs, carriage returns, newlines, or other invisible characters are not permitted. ■ Zone names cannot contain an equals sign, such as "Hello=World".
VDI	X	Requires Agent version 1492 or higher. When installing Threat Defense 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

Property	Value	Description
		fingerprinting mechanism. For more information, see Appendix: VDI Best Practices. The VDI parameter utilizes a counter "X" and has a delayed effect, whereas the AD parameter is immediate upon installation. **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 127
AD	1	Requires Agent version 1522 or higher. 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. AD fingerprinting will take precedence over the VDI=<X> installation parameter. For more information, see Appendix: VDI Best Practices. **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 127
PROXY_SERVER	<ip_ address>:<port_ number>	Requires Agent version 1472 or higher. 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 1502 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

Property	Value	Description
		and the AWS EC2 ID is i-0a1b2cd34efg56789.
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 2: Installation Parameters for Windows

Example for PIDKEY, APPFOLDER, and LAUNCHAPP Parameters

```
msiexec /i DellThreatDefenseSetup_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`. When the Agent is running, both the system tray icon and the Start Menu Threat Defense 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 DellThreatDefenseSetup_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 DellThreatDefenseSetup_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.

Install the Windows Agent Using Wyse Device Manager (WDM)

This section explains how to create an install script, how to create an RSP package for WDM, and how to add the package to WDM to install on multiple thin clients simultaneously without user interaction.

Create a batch file script that will perform the command line install of Threat Defense. WDM executes this script during deployment.

1. Open Notepad. Using the command line parameters from above, enter the following command to execute the install, replacing `<INSTALLATION TOKEN>` with your provided token:

   ```
   msiexec /i C:\TDx86\DellThreatDefense_x86.msi
   PIDKEY=<INSTALLATION TOKEN> /q
   ```

   `C:\TDx86` is used for our directory, as this folder gets copied to this location on the thin client during installation.

2. Save the file with a .bat extension to the TDx86 folder. For example, `TDx86_Install.bat`.

   Create an RSP Package with which the Threat Defense Agent application can be installed onto multiple thin clients simultaneously without user interaction.

3. Open Scriptbuilder on a computer that has WDM installed.

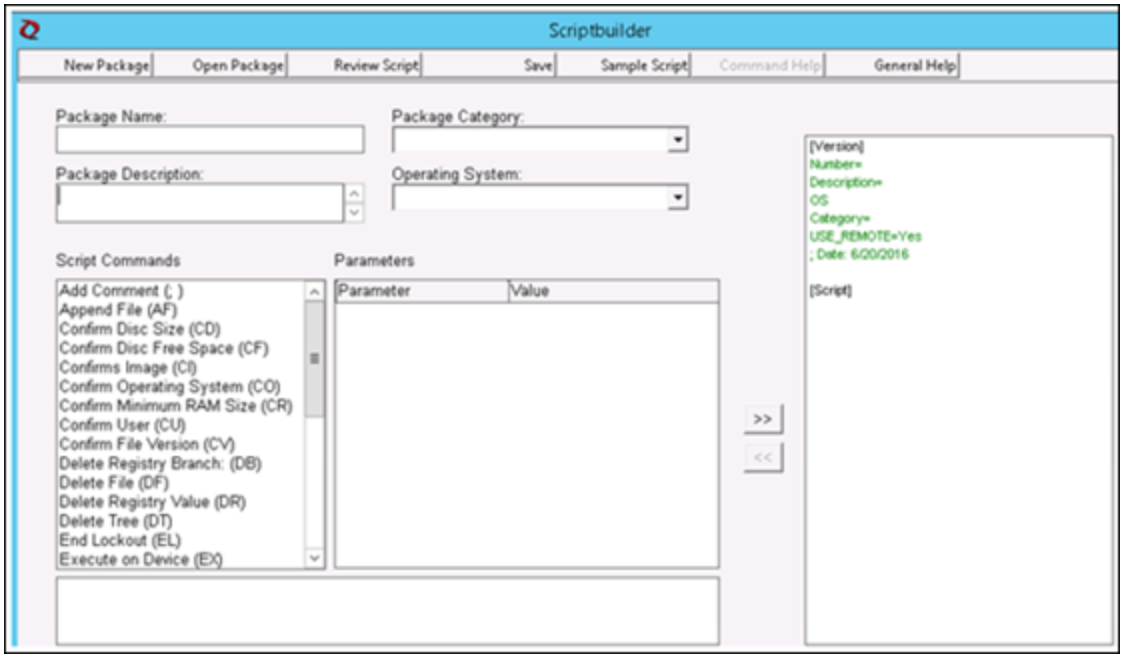


Figure 15: Scriptbuilder

4. Enter a Package Name and Package Description.
   - Select Other Packages under Package Category.
   - Select Windows Embedded Standard 7 under Operating System.

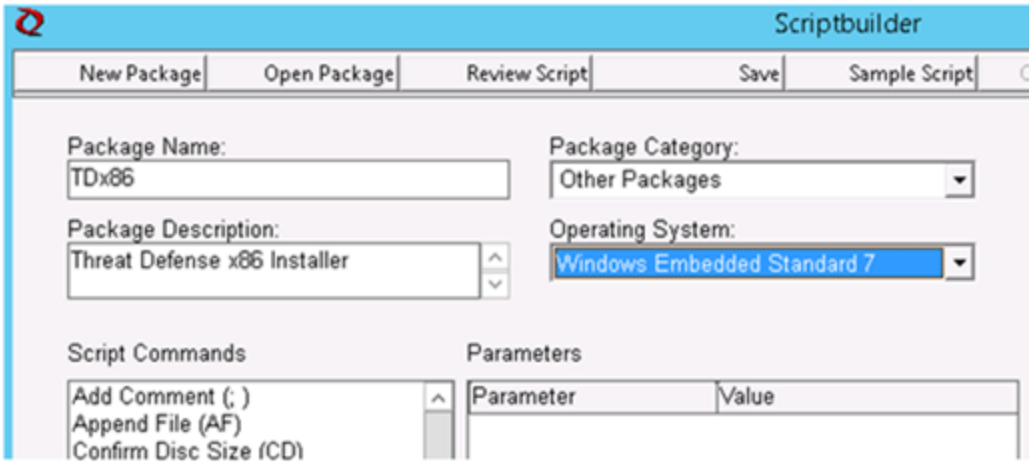


Figure 16: Scriptbuilder fields

5. Add Script Commands to verify target systems are WES7 or WES7p.
   - Select Confirm Operating System (CO) under Script Command
   - For the Device OS value, enter the appropriate operating system.

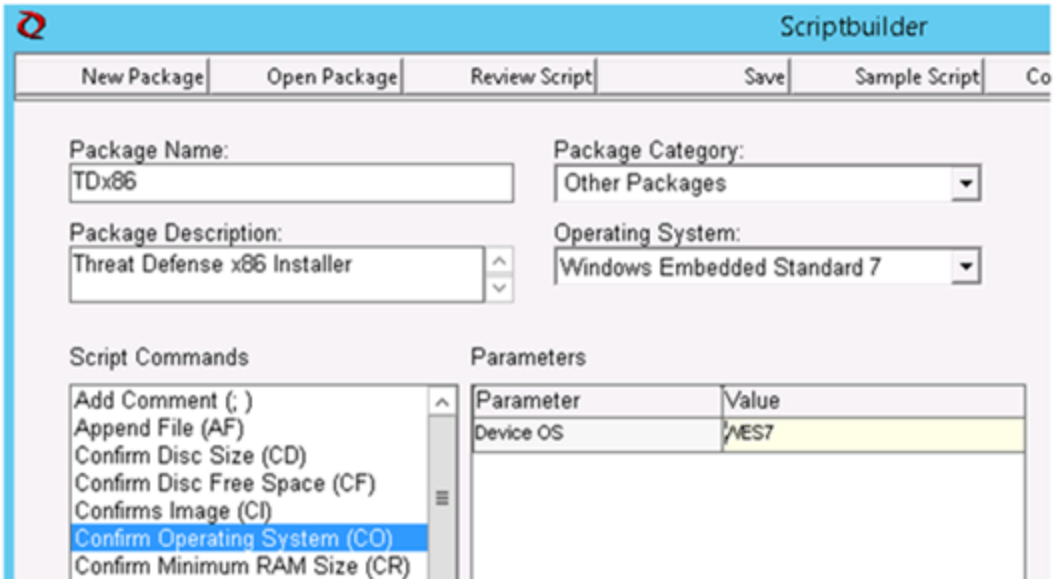


Figure 17: Scriptbuilder confirm OS

6. Use the double arrows to Add Item.

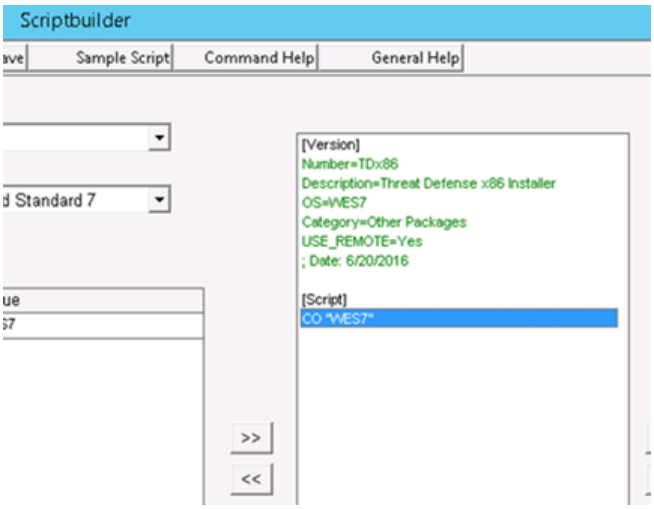


Figure 18: Scriptbuilder add item

7. Press **OK** at the prompt.

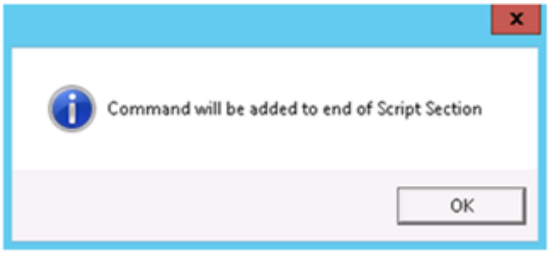


Figure 19: Command will be added to end of script

8. Add command to lock the thin client and to prevent user interaction.
    - Select **Script Command > Lockout User (LU)**. No value is necessary. However, in this example a Value of Yes is entered, so that the splash screen is removed if the installer fails or there is an error.

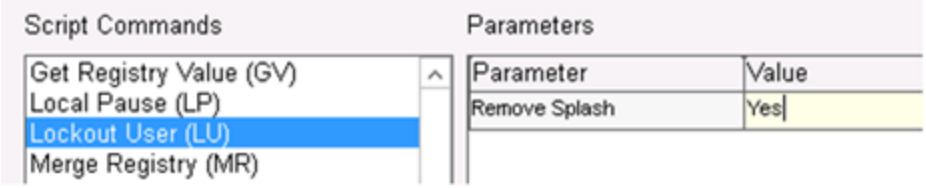


Figure 20: Script Commands

9. Add command to copy files to thin client.
    - Select Script Command X Copy (XC).
    - For the Repository Directory value, add * to the end of the existing <regroot>\.
    - For the Device Directory value, enter the path for the files to be copied to on the destination thin clients. In this example, the Package Name is used.

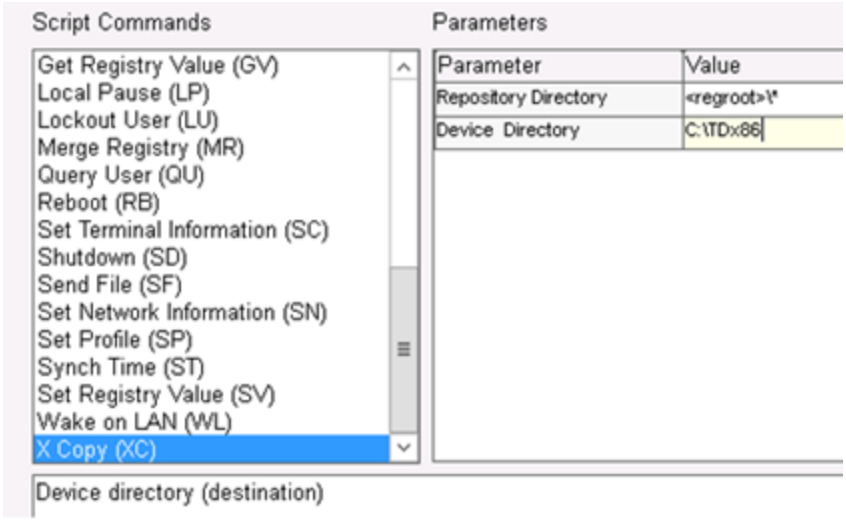


Figure 21: Script Parameters

10. Add command to execute the .bat install script.
    - Select **Script Command > Execute on Device (EX)**.
    - For the Device Filename value, enter the path `C:\TDx86\TDx86_install.bat`. The TDx86 folder gets copied from our previous command XC.
    - Add + as the Synchronous Execute value. This tells WDM to wait until the file being executed has completed to continue.

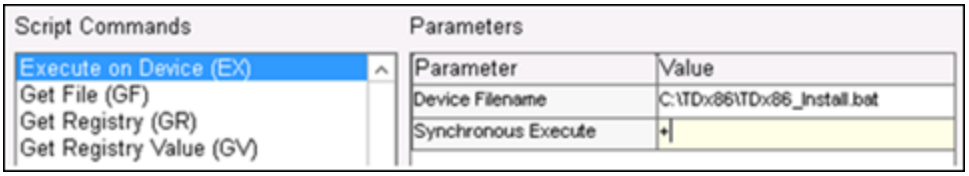


Figure 22: Script Parameters

11. Add command to delete files copied from thin client.
    a. Add Script Command **Delete Tree (DT)**.

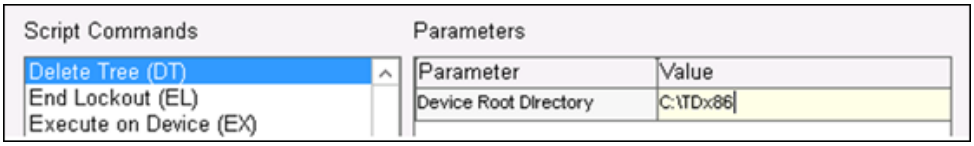


Figure 23: Script Parameters

12. Add commands to disable lock out.

a. Add Script Command **End Lockout (EL)**.

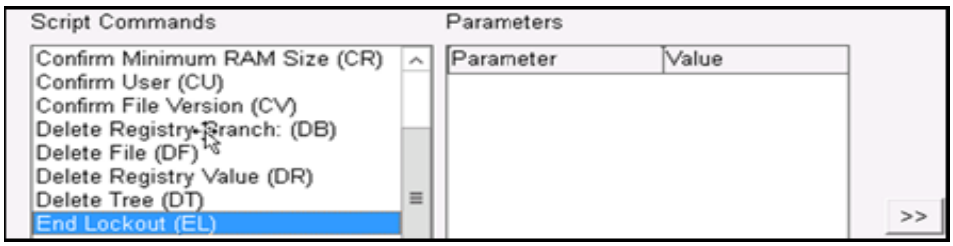


Figure 24: Script Parameters

13. To review, the script package should look similar to the following.

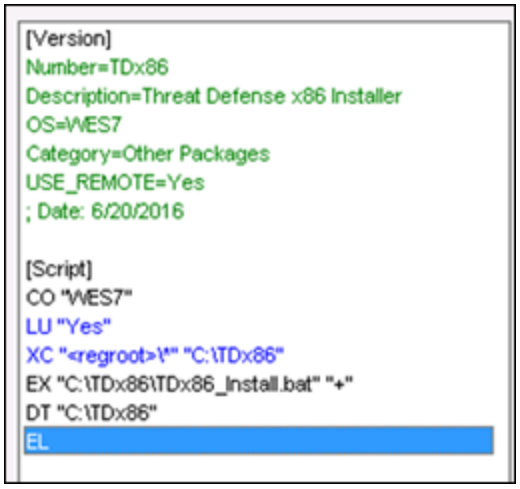


Figure 25: Script Review

a. If deploying Threat Defense to WES7P systems, update the operating system section to WES7P, Otherwise, the package fails to install.

Figure 26: Script Review

14. Save the package.

a. Click **Save** and browse to the location of the **TDx86** folder, if these instructions have been followed, the folder is on the Desktop.

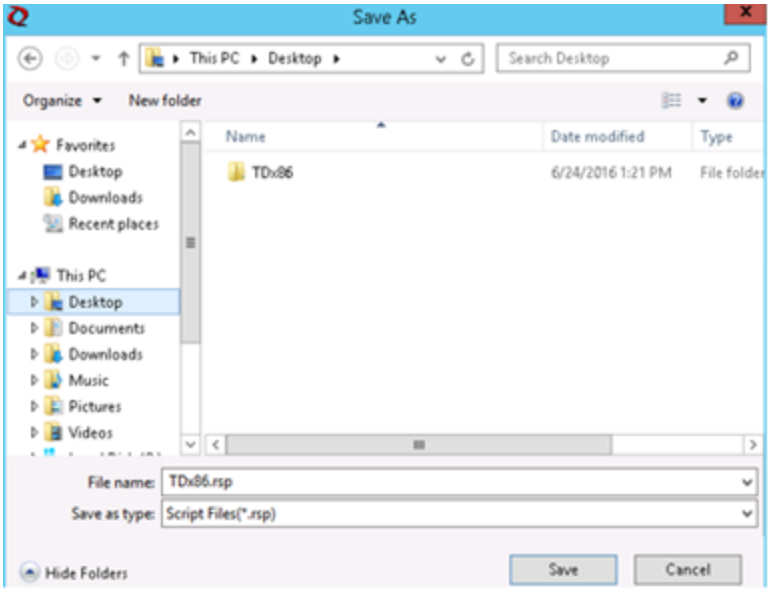


Figure 27: Save Location

15. Close Scriptbuilder.
16. Launch **WyseDeviceManager** to add the package to WDM.
17. Browse to **WyseDeviceManager > Package Manager > Other Packages**.

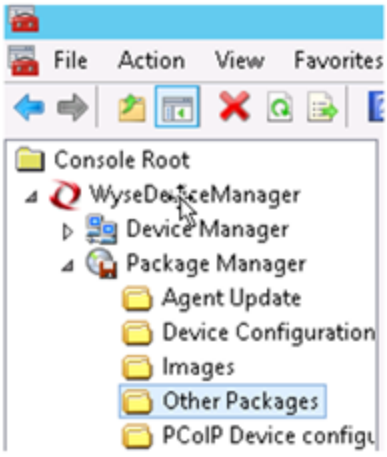


Figure 28: WyseDeviceManager

18. Select **Action > New > Package** from the menu bar.

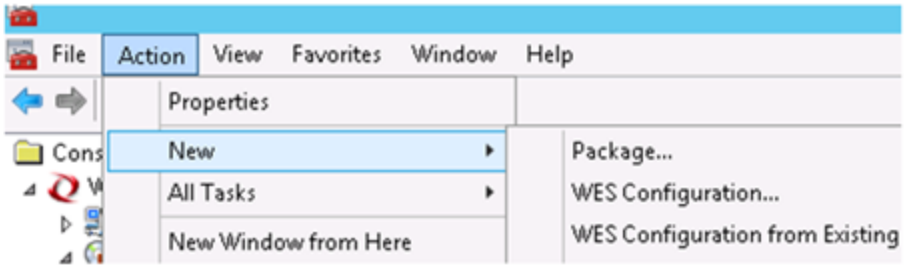


Figure 29: Menu bar

19. Select **Register a Package from a Script file (.RSP)** and click **Next**.

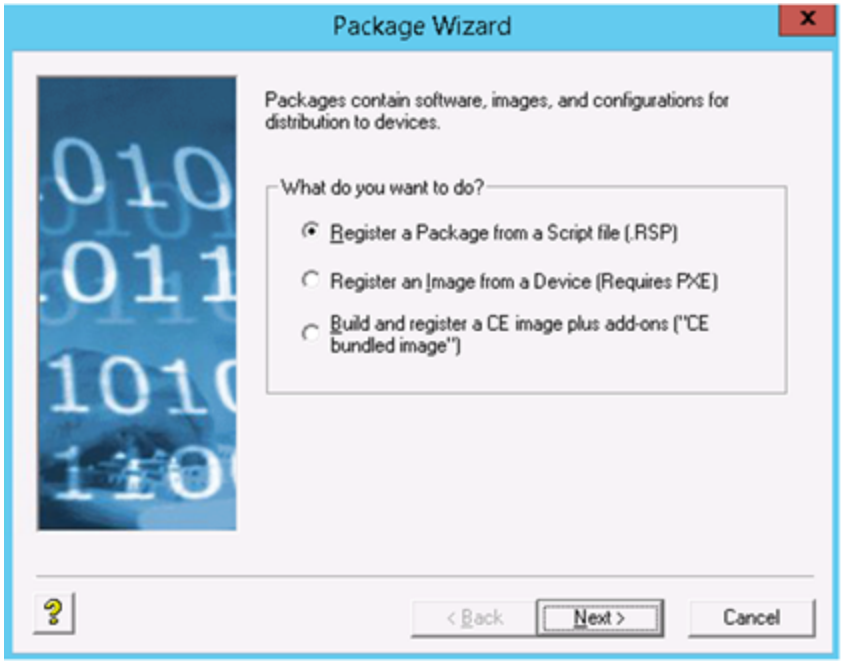


Figure 30: Package wizard

20. Browse to the location of the RSP file created in the previous step and click **Next**.

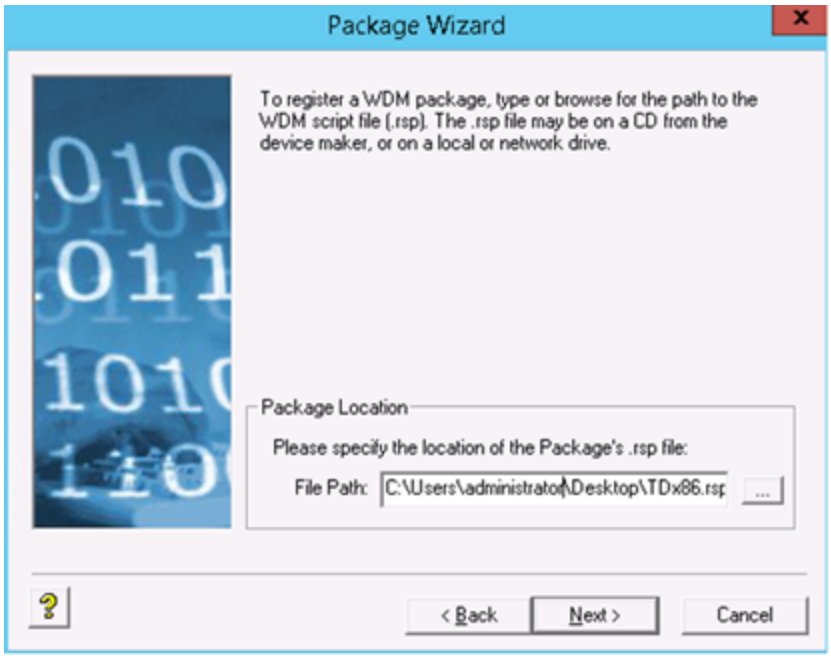


Figure 31: Location of .RSP file

21. Ensure that Active is selected and click **Next**.

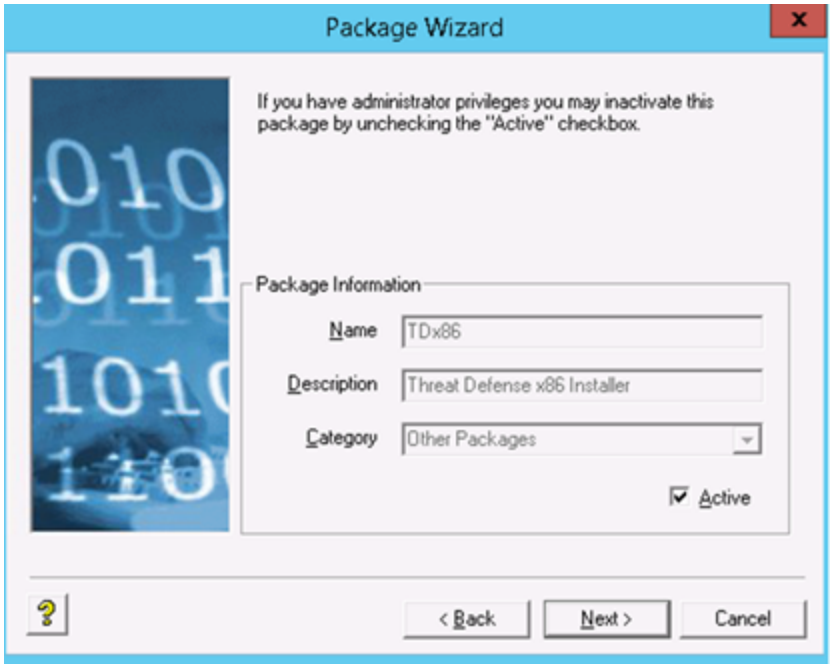


Figure 32: Package information

22. Click **Next** once WDM is ready to register the package.

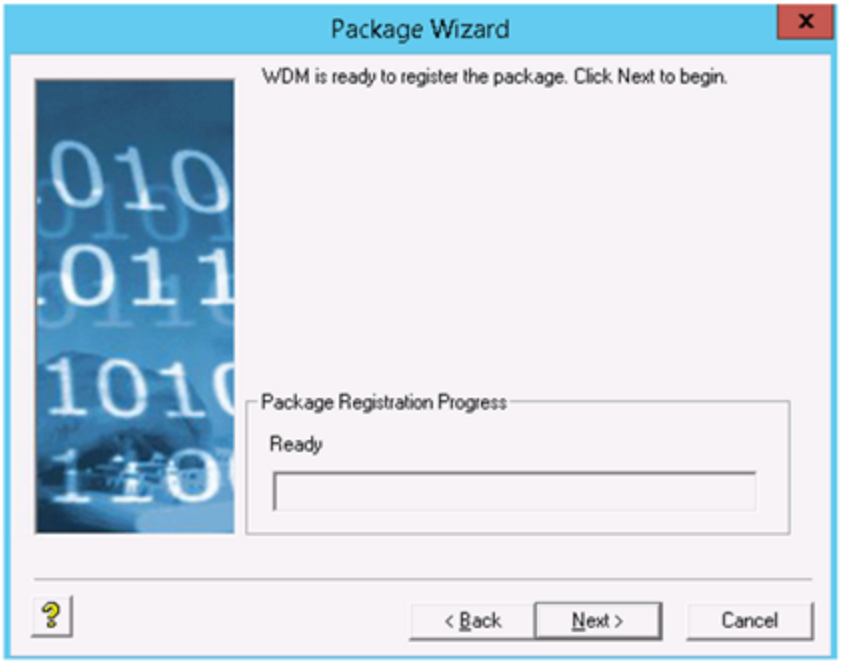


Figure 33: Ready to register the package

23. Click **Finish** when the package is successfully registered.

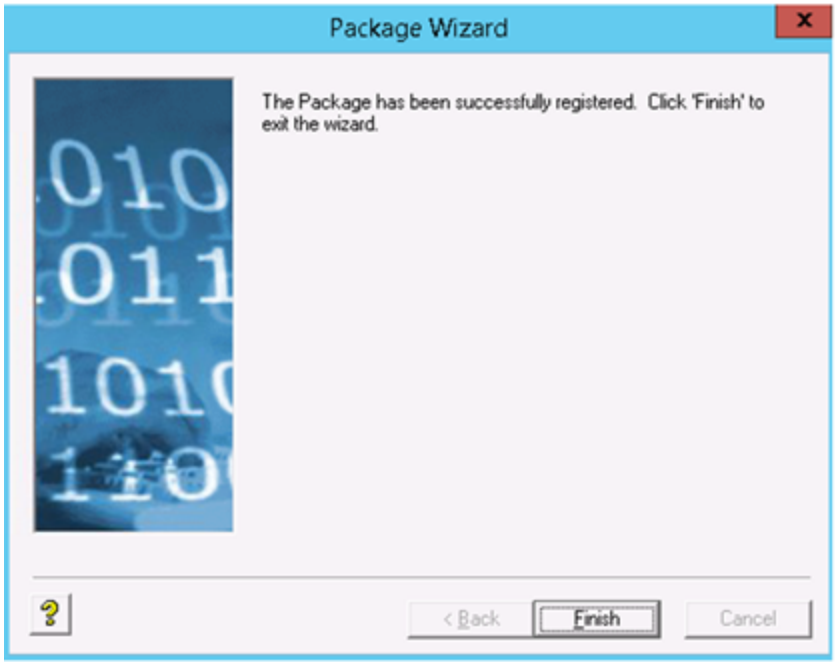


Figure 34: Finish wizard

24. The package will be visible in Other Packages.

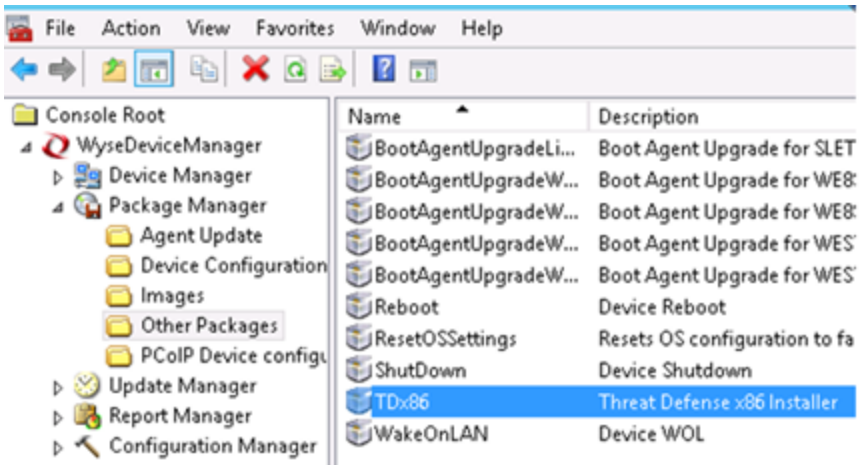


Figure 35: Location of package

25. Verify package contents:

    a. Open File Explorer and browse to **C:\inetpub\ftproot\Rapport** and locate the **TDx86** folder.

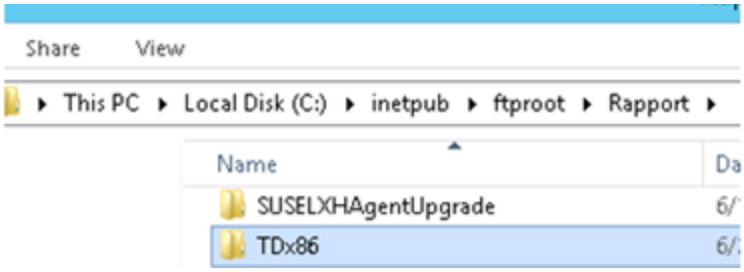


Figure 36: Inetpub location of package

    b. Open TDx86 folder and verify the folder include the installer and .bat file.

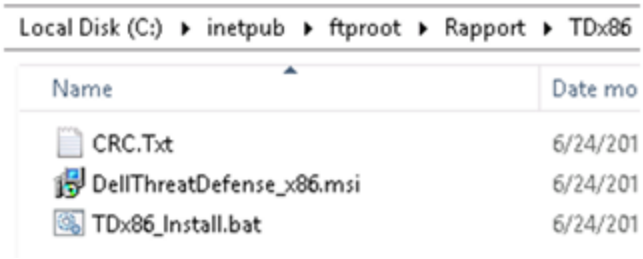


Figure 37: Inetpub location of installer

A package is now available in WDM that can deploy Threat Defense to multiple WES7 thin clients without user interaction.

Quarantine using the Command-Line

You can quarantine a file using the command-line on a device. This requires knowing the SHA256 hash for the threat.

Note: This feature is for Windows only and requires Agent 1432 or higher.

1. On the Windows device, open the command-line. Example: From the Start menu, search for cmd.exe.

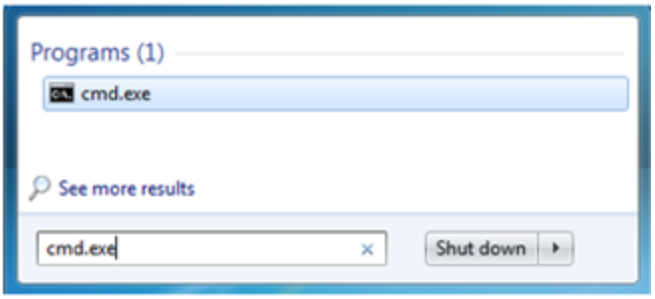


Figure 38: Search for cmd.exe

2. Invoke Dell.ThreatDefense.exe and include the argument **-q:<hash>**, where <hash> is the SHA256 hash for the file. This will prompt the Agent to send the file to the quarantine folder.

   Example Command-Line (Dell Threat Defense installed to the default location):

   ```
   "C:\Program Files\Cylance\Desktop\Dell.ThreatDefense.exe"
   -q:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2
   351f941
   ```

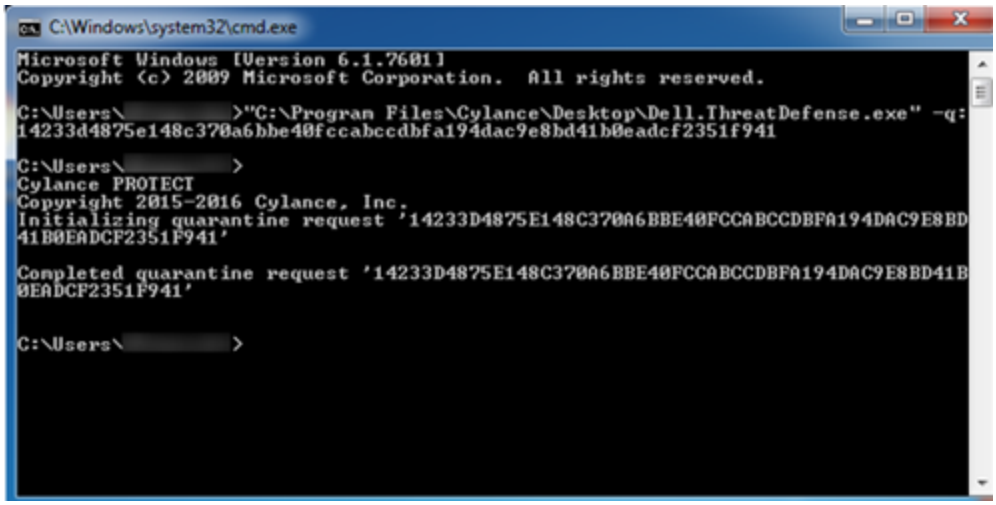


Figure 39: Quarantine a file by SHA256 hash

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 Threat Defense 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 Threat Defense folder under Start Menu\All Programs on the target device.

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

4. The Threat Defense service was added and is running. There should be a Threat Defense service listed as running in the Windows Services panel of the target device.
5. The Dell.ThreatDefense.exe process is running. There should be a Dell.ThreatDefense.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.

   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: If **Require Password to Uninstall Agent** is enabled, you will need to uninstall using the command line.

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 Dell Threat Defense, then click **Uninstall**.

Uninstall Using the Command Line

1. Open the Command Prompt as an Administrator.
2. Use the following commands, based on the installation package you used to install the Agent.

   DellThreatDefense_x64.msi

   - **Standard uninstall:** `msiexec /uninstall DellThreatDefense_x64.msi`
   - **Windows Installer:** `msiexec /x DellThreatDefense_x64.msi`

   DellThreatDefense_x86.msi

   - **Standard uninstall:** `msiexec /uninstall DellThreatDefense_x86.msi`
   - **Windows Installer:** `msiexec /x DellThreatDefense_x86.msi`

   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

   Example with Uninstall Key and Log Output:

   ```
   msiexec /x DellThreatDefense_xxx.msi /qn
   UNINSTALLKEY=<passwordhere> /l*v
   "C:\Path\ToOutput\output.log"
   ```

macOS Agent

System Requirements

Dell 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	
Mac OS X 10.10	
Mac OS X 10.11	
macOS Sierra (10.12)	*
macOS High Sierra (10.13)	*
macOS Mojave (10.14)	*
macOS Catalina (10.15)	*
* For specific requirements, read the System Requirements article.	

Additional macOS Requirements

Type	Description
Processor	■ Requires at a minimum a two core processor ■ Supports the SSE2 instruction set ■ Supports x86_64 instruction set
RAM	■ 2 GB
Available Hard Drive Space	■ 300 MB **Note:** Disk space usage can increase depending on features enabled, like setting the log level to Verbose.
Additional Requirements	■ Internet Browser ■ Internet access to login, access the installer, and register the product ■ Local administrator rights to install the software ■ Root Certificates: • VeriSign Class 3 Public Primary Certification Authority - G5 • GeoTrust Global CA

Type	Description
	• thawte Primary Root CA • DigiCert Global Root **Note:** Devices missing any of the above root certificates may experiences 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.

Install the Agent — macOS

Ensure that all prerequisites are met prior to installing Threat Defense. See "System Requirements" on the previous page.

Note: The macOS Agent will be Dell branded in a future release.

1. "Download the Install File" on page 30.
2. Double-click the Dell Threat Defense.dmg 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.

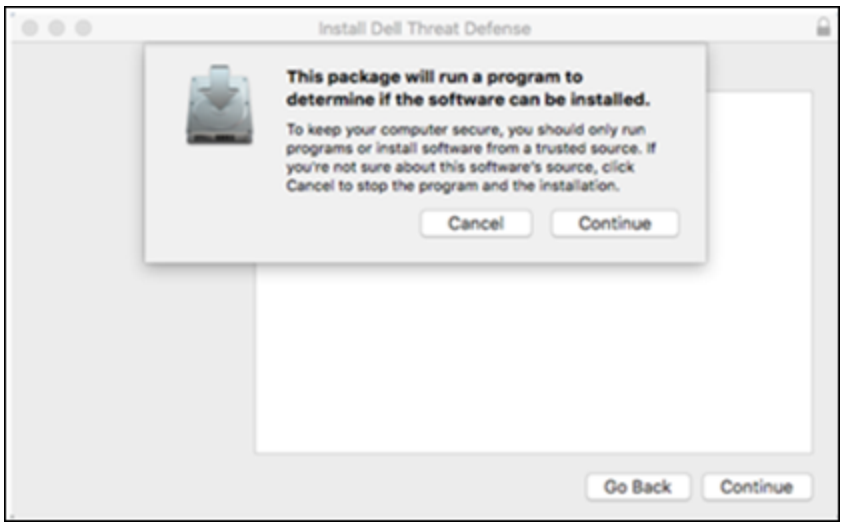


Figure 40: Operating System and Hardware Check

5. Click **Continue** at the Introduction screen.

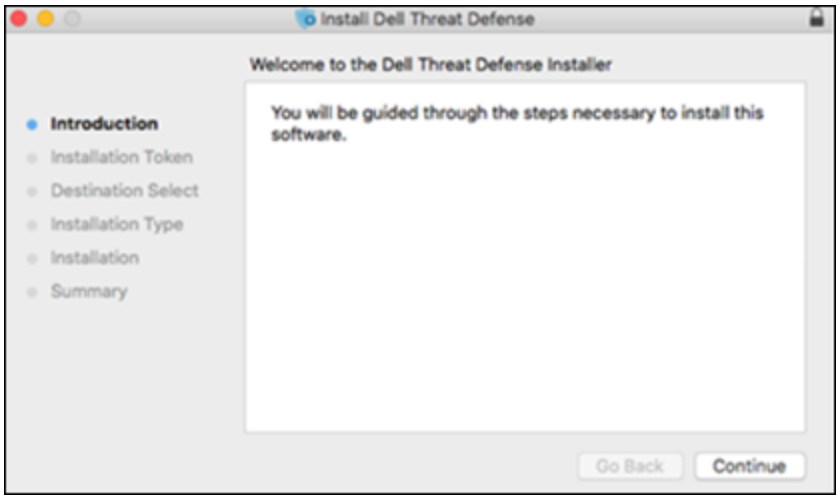


Figure 41: Introduction Screen

6. Enter the Installation Token provided by the Tenant. Click **Continue**. The Destination Folder step displays.

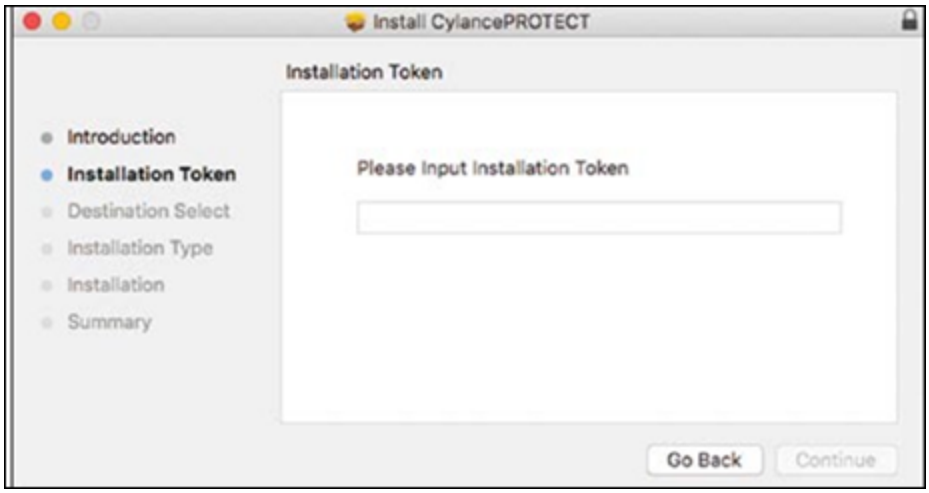


Figure 42: Installation Token Input Screen

Note: Contact your Threat Defense administrator or see KB article How To: Manage Threat Defense if access to the Installation Token is not available.

7. Optionally change the installation location of Threat Defense.

   Click **Install** to begin the installation.

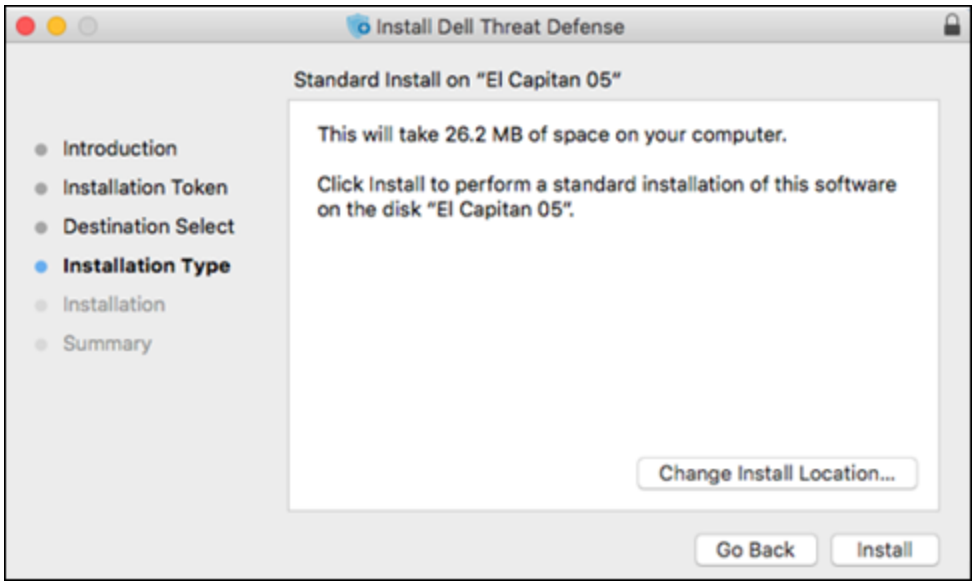


Figure 43: Installation Type Screen

8. Enter an administrator's Username and Password. Click **Install Software**.

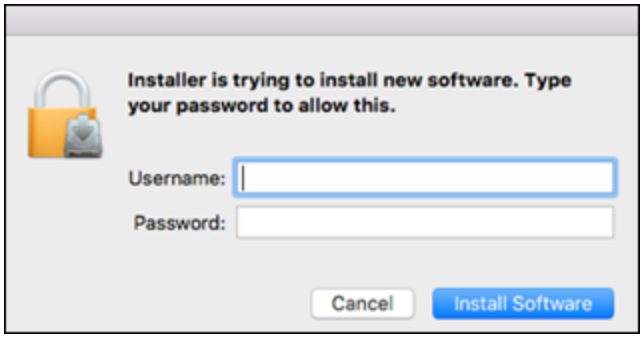


Figure 44: Input Credentials Screen

9. Click **Close** at the Summary screen.

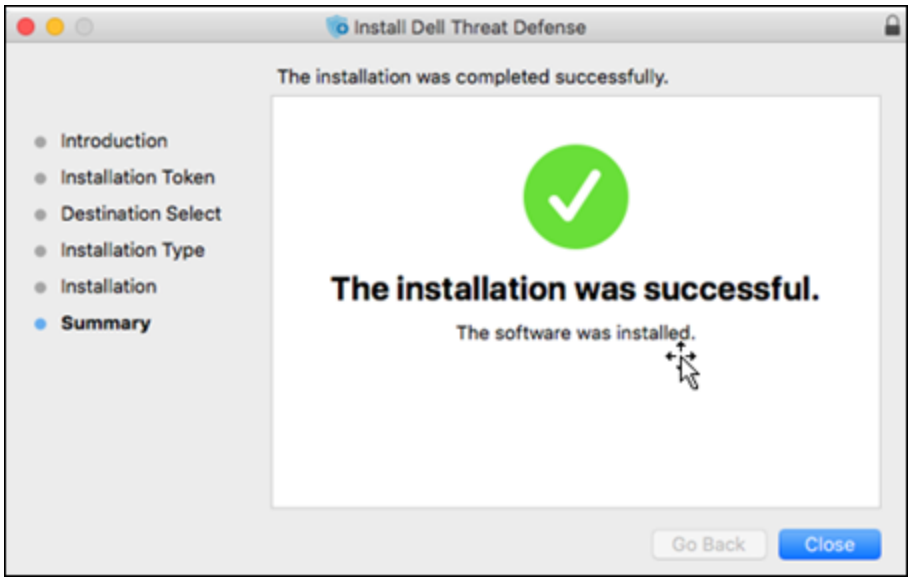
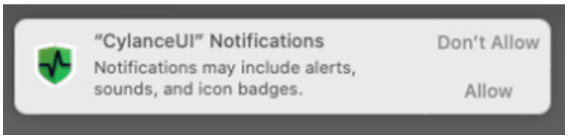


Figure 45: Installation Complete Screen

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



macOS Installation Parameters

The Threat Defense 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.
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).

Property	Value	Description
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. Dell recommends turning Verbose on during troubleshooting and then changing it back to Information when troubleshooting is complete.
VenueZone	“zone_name”	Introduced in Agent version 1382. ■ Adds devices to a zone. ■ If the zone does not exist, the zone is created using the name provided. ■ 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 ", Dell removes the whitespace during device registration. **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>	Requires Agent version 1472 or higher. Proxy server settings are added to the device’s registry. Proxy server information will appear in the Agent log file. **Example:** ProxyServer=123.45.67.89:1234

Table 3: Installation Parameters for macOS

Install the macOS Agent

Install without the Installation Token

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

Install with the Installation Token

```
echo [install_token] > cyagent_install_token
```

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

Replace `[install_token]` with the Installation Token. 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. Be cautious of file extensions, the example above shows the `cyagent_install_token` file has no file extension. Default settings within macOS have extensions hidden. Manually building this file with text edit or another text editor may automatically append a file extension that will need to be removed.

Optional Installation Parameters

Enter the following in Terminal to create a file (`cyagent_install_token`) that the installer uses to apply the options entered. Each parameter must be on its own line. This file must be in the same folder as the installation package.

The following is an example. All of the parameters are not needed in the file. Terminal includes everything contained within the single quotes in the file. Ensure that Enter/Return is pressed after each parameter to keep each parameter on its own line in the file.

A text editor may also be used to create the file that includes each parameter (on its own line). This file must be in the same folder as the installation package.

Example:

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token

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

macOS Installation Verification

Check the following files to verify successful Agent installation.

1. The program folder was created. macOS default: `/Applications/DellThreatDefense/`
2. The Threat Defense icon is visible in the System Tray of the target device.

   This does not apply if parameter NoCylanceUI is used.
3. There is a Threat Defense application in Applications (in Finder) on the target device.

   This does not apply if parameter NoCylanceUI is used.
4. 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

Without Password

```
sudo /Applications/DellThreatDefense/Uninstall\
DellThreatDefense.app/Contents/MacOS/Uninstall\
DellThreatDefense
```

With Password

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

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

Agent Update

Maintenance and management of Threat Defense Agents is hassle-free. Agents automatically download updates from the Console, and the Console is maintained by Cylance. Agents check for updates every 1 to 2 hours, with the check-in time being randomized to ensure that all devices do not perform an Agent Update simultaneously.

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.

Threat Defense 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 Dell Support. Read the Dell Data Security International Support Phone Numbers article for contact information.

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.

To Configure Zone-based Updates

1. Select **Settings > Agent 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.

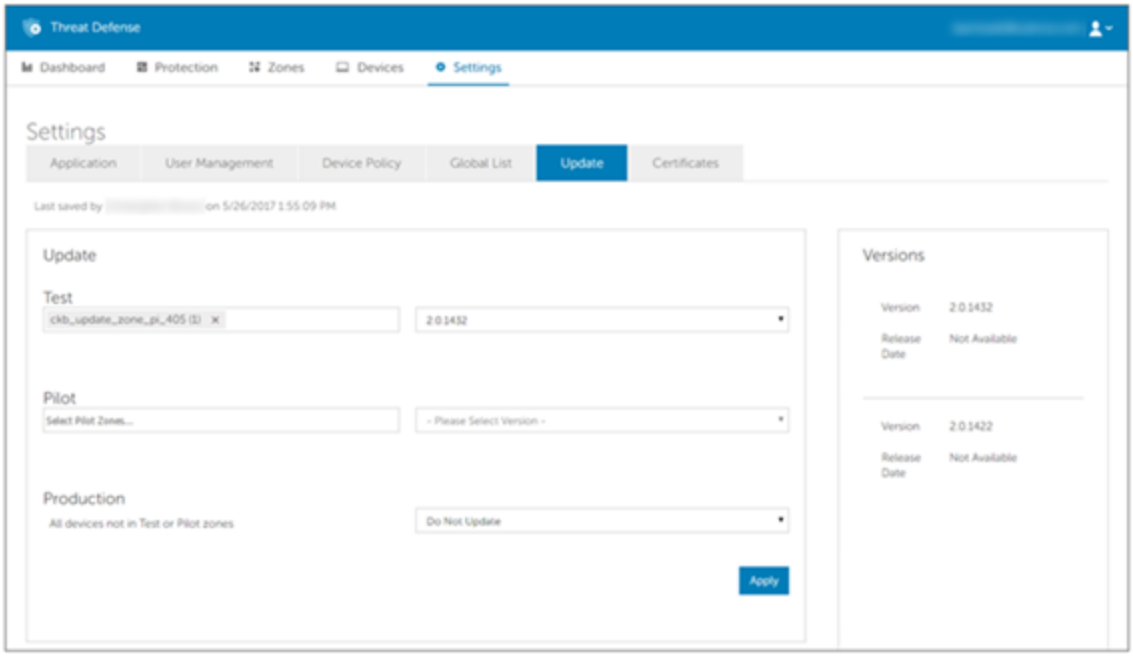


Figure 46: Agent Updates

To Trigger an Agent Update

To trigger an Agent update prior to the next hourly interval:

1. Right-click the Threat Defense Agent icon in the system tray, and select **Check for Updates**.
2. Restart the Threat Defense 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:

```
Dell.ThreatDefense.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:

  ```
  Dell Threat Defensex64.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: Dell Threat DefenseSetup.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:

  ```
  Dell Threat DefenseSetup.exe
  UNINSTALLKEY="MyUninstallPassword" /uninstall
  ```

To Create an Uninstall Password

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

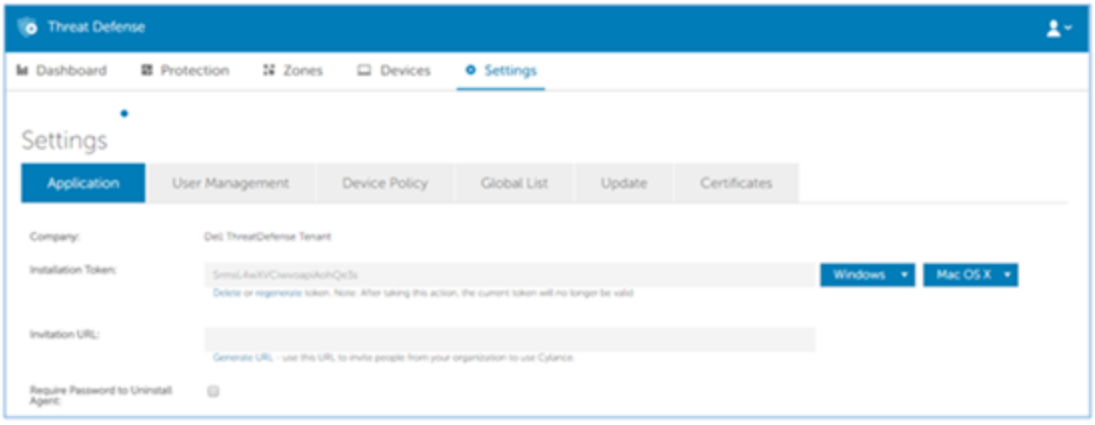


Figure 47: Configure Password-Protected Uninstall

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 the Agent icon in the system tray to view. Alternatively, the Agent can be installed to hide the Agent icon from the system tray.

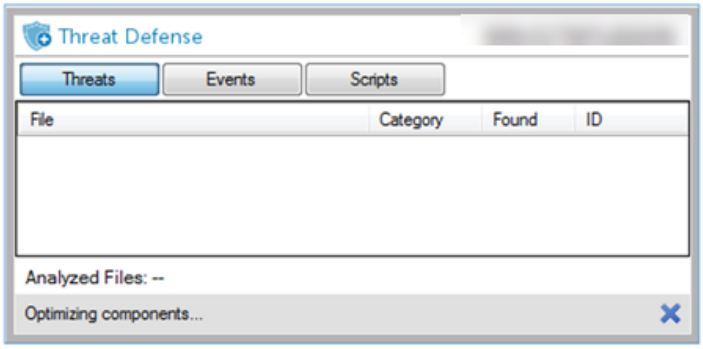


Figure 48: Agent User Interface

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

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

- **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.

  Note: Check for Policy Update is supported in version 1422 (or higher) for Windows and version 1432 (or higher) for macOS.
- **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.
- **Exit:** Closes the Agent icon in the system tray. This does not turn off any of the Threat Defense services.
- **Options > Show Notifications:** Select this option to display any new events as notifications.

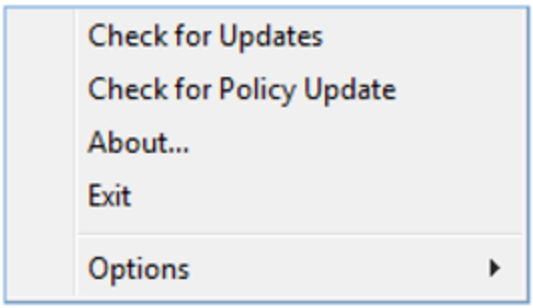


Figure 49: Agent Menu

Enable Agent User Interface Advanced Options

The Threat Defense 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.

   ```
   Dell.ThreatDefense.exe -a
   ```

   The Agent icon displays in the system tray.
4. Right-click the icon. *Logging*, *Run a Detection*, and *Threat Management* options display.

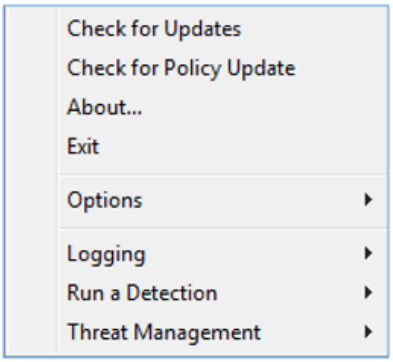


Figure 50: Agent Advanced UI Options

macOS

1. If the Agent icon is visible in the top menu, right-click the icon and select Exit.
2. Open terminal and run

   ```
   Sudo
   /Applications/DellThreatDefense/DellThreatDefense.app/Con
   tents/MacOS/DellThreatDefenseUI -a
   ```

   Note: This is the default install path for Dell Threat Defense. You may need to edit the path to match your environment accordingly.
3. The Agent UI will now appear with additional options.

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.

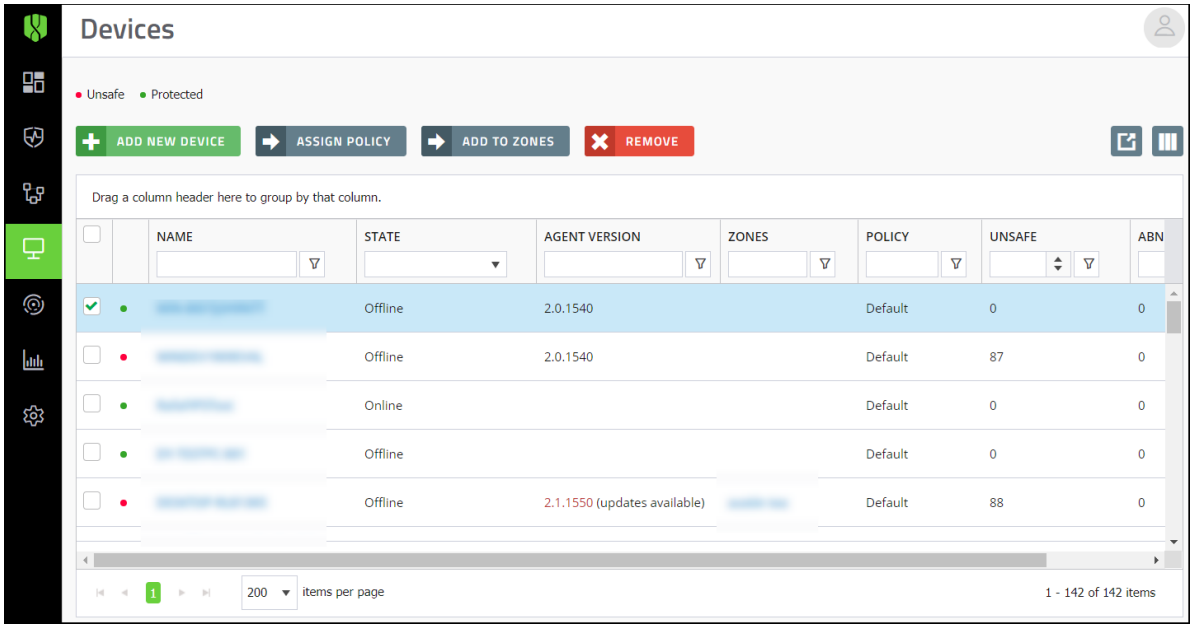
1. Select **Threat Management > Delete Quarantined**.
2. Click **OK** to confirm.

Virtual Machines

There are some recommendations when using the Threat Defense Agent on a virtual machine image. See "Appendix A: VDI Best Practices " on page 120 for more information

DEVICE MANAGEMENT

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



Tip: Clicking the "select all" check box at the top of the list will only select 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.
2. Select a device check box to allow the following actions:
    - **Export:** Creates and downloads a CSV file. The file contains device information (Name, State, and Policy) for all devices in the organization.
    - **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 the Deployments page where you can select a product to download. For more information, see "Download the Install File" on page 30.
5. In the Zones column, click a Zone Name to display the Zone Details page.

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.

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 Threat Defense user interface (right-click the Threat Defense 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 Threat Defense icon appears in the system tray. Right-click, select **Logging**, then click **All** (same as Verbose in the Console).

OR (For macOS)

1. Exit the currently running user interface.
2. Execute the following command from terminal.

    ```
    sudo
    /Applications/DellThreatDefense/DellThreatDefenseUI.app/C
    ontents/MacOS/DellThreatDefenseUI -a
    ```

3. Right-click the new user interface once it opens. Select **Logging > All**.

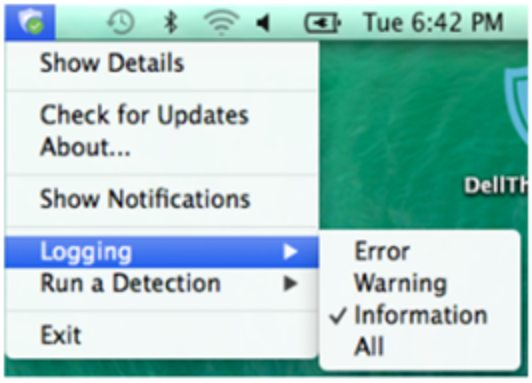


Figure 51: macOS Verbose Logging

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.

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 10.

Add an Exclusion

- 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 52: 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 Threat Defense 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 Threat Defense Agent. The Agent needs to be uninstalled at the endpoint.

THREAT MANAGEMENT

Dashboard

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

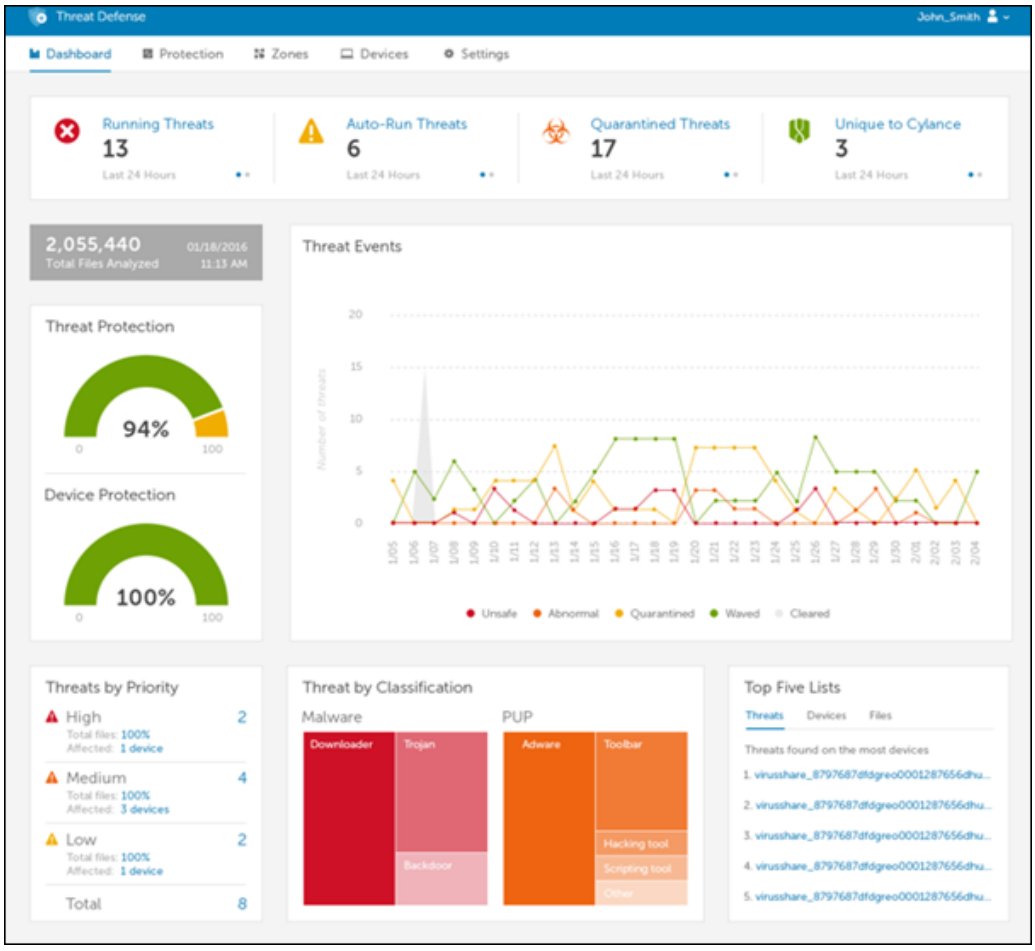


Figure 53: Threat Defense Dashboard

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 54: 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:** The percentage of devices associated with a policy that has Auto-Quarantine enabled.

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.

If all threats in a priority group have been acted upon (*Quarantine*, *Global Quarantine*, *Waive*, or *Safe List*), then the group will show 0 (zero).

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.

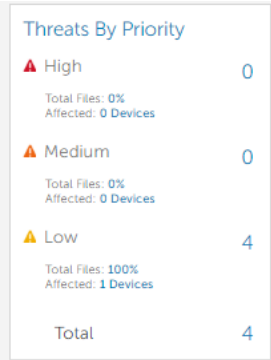


Figure 55: Dashboard Threats by Priority Section

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.

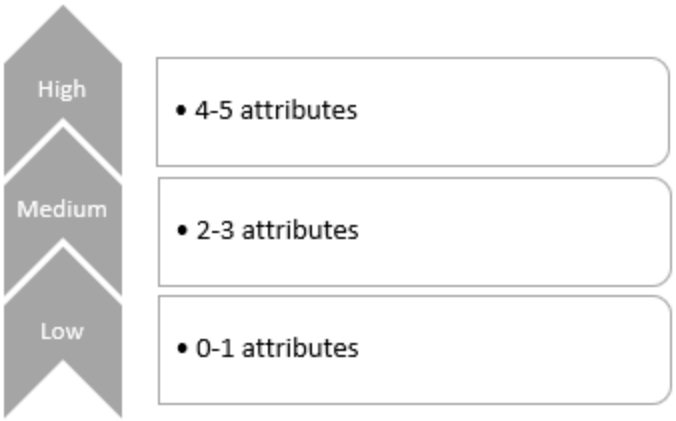


Figure 56: Threat Classifications

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

Attribute	Attribute Value	Score
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.

Top Five Lists

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

The Top Five 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 Five lists is to bring critical threats to your attention.

Threat Protection

Threat Defense 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.

For a list of Threat Indicators, read the What are Threat Indicators for Dell Endpoint Security Suite Enterprise and Dell Threat Defense? article.

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 Dell 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 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: ■ 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

Subclass	Definition	Examples
Downloader	Malware that downloads data to the host system.	Staged-Downloader
Dropper	Malware that installs other malware on a system.	
Exploit	Malware that attacks a specific vulnerability on the system.	
FakeAlert	Malware that masquerades as legitimate security software to trick the user into fixing fake security problems at a price.	Fake AV White Paper
Generic	Any malware that does not fit into an existing category.	
InfoStealer	Malware that records login credentials and/or other sensitive information.	Snifula
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.	Sality, 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.

Note: The Threat List on the Protection page has configurable columns. Click the down-arrow on any column to access the menu, then Show/Hide various threat details. The menu includes a filtering submenu.

Tip: Clicking the "select all" check box at the top of the list will only select 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.

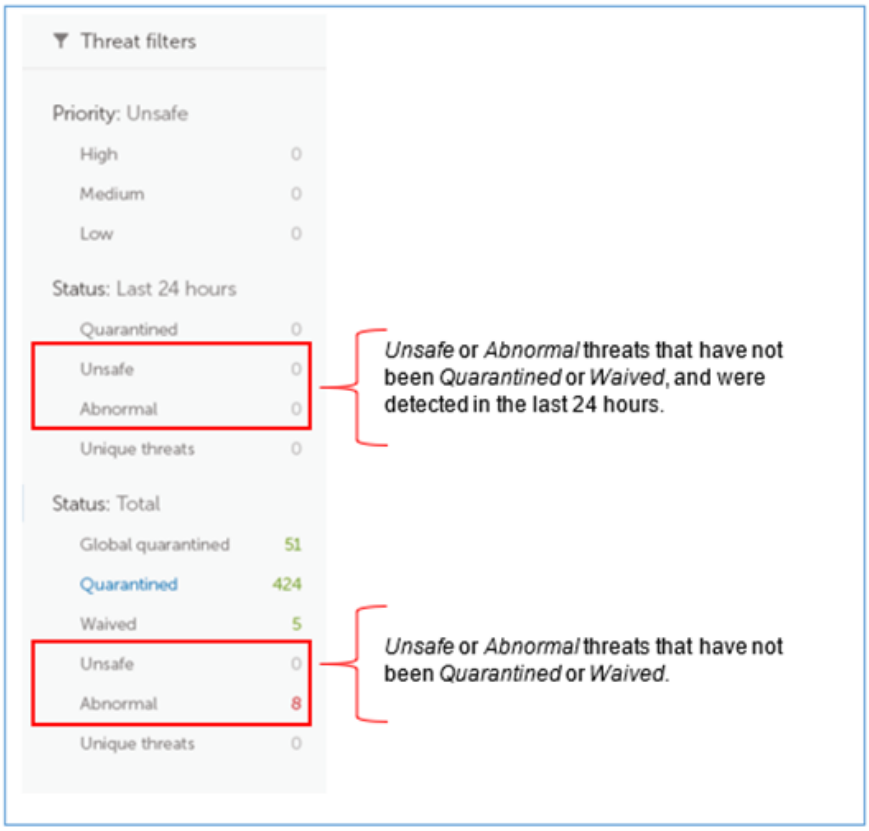


Figure 57: Protection Page Threat Filters

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 wiave 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" below.

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.

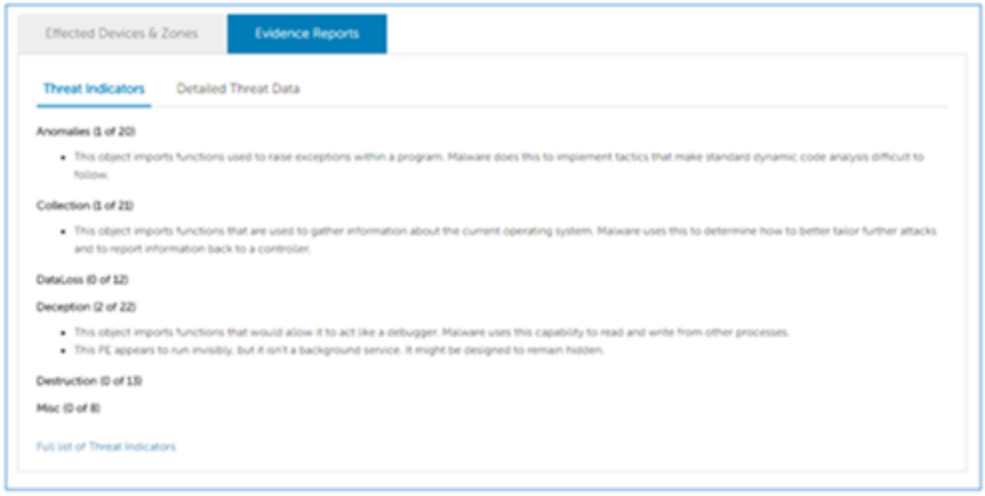


Figure 58: Threat Indicators

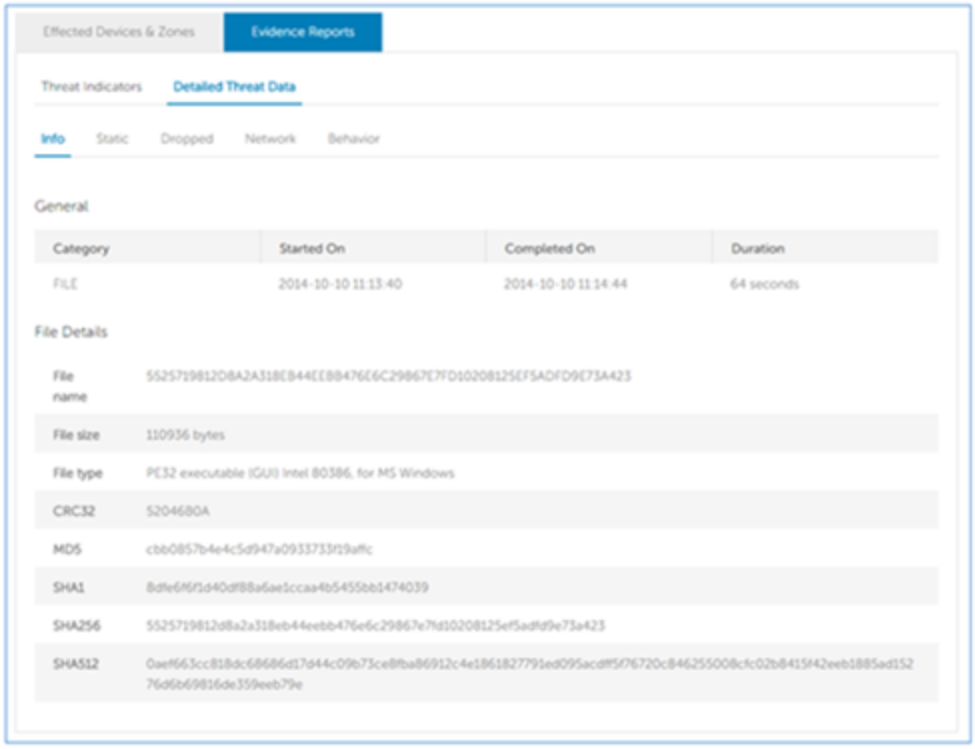


Figure 59: Detailed Threat Data

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

Category	Name	Description
		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.
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

Category	Name	Description
		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.
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

Category	Name	Description
		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 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

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.

  Note: You can quarantine a threat using the command-line on a device. This is available with the Windows Agent only. See "Quarantine using the Command-Line" on page 47 for more information.

- ***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, Threat Defense 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 1322 or higher.

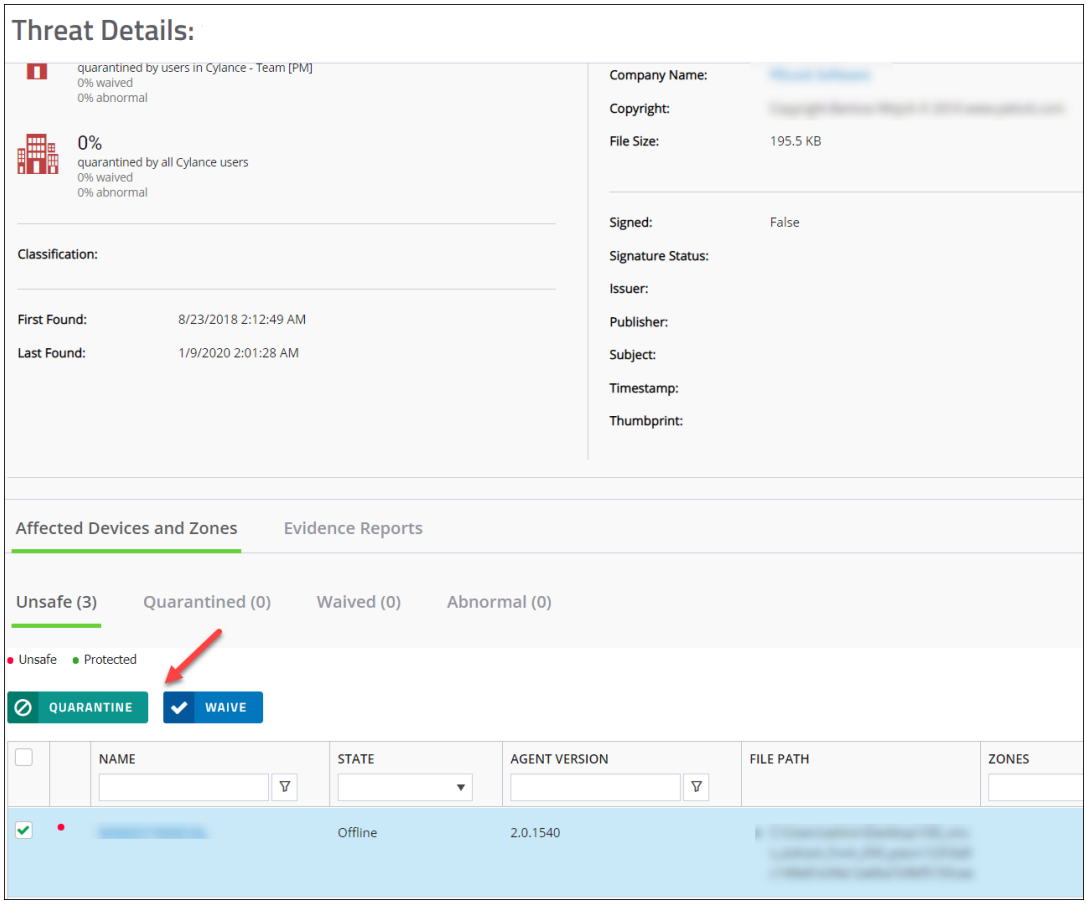
  Note: Applies to files that exist in the organization only (this could be as a threat, a quarantined file, or a safelisted file). The file must be available in the Cylance Cloud and all three hashes (SHA256, SHA1 and MD5) must match between the Cylance Cloud and the Agent. If not, then the Download File 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.

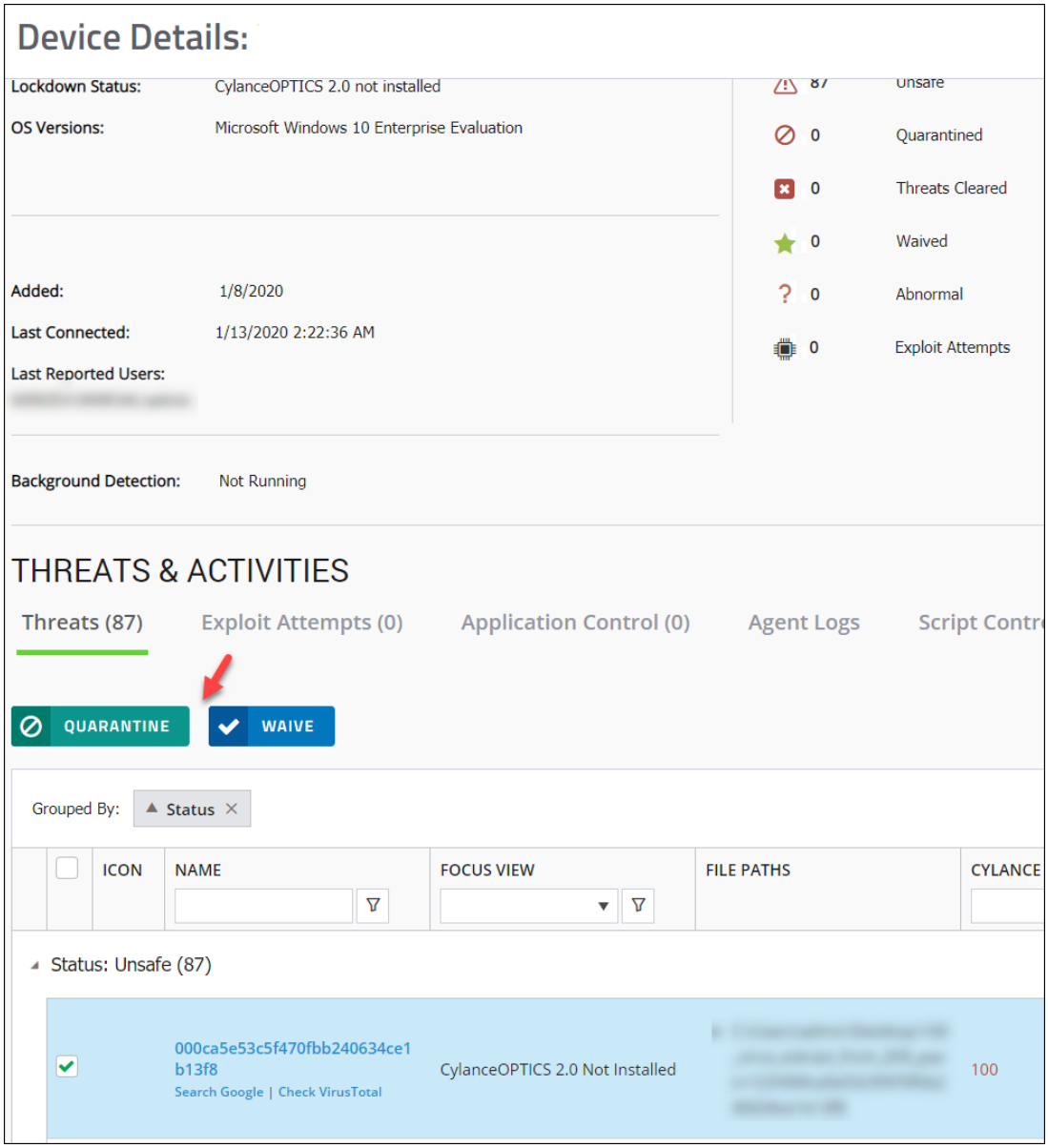
5. Click **Quarantine** or **Waive** (Safelist).



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**.

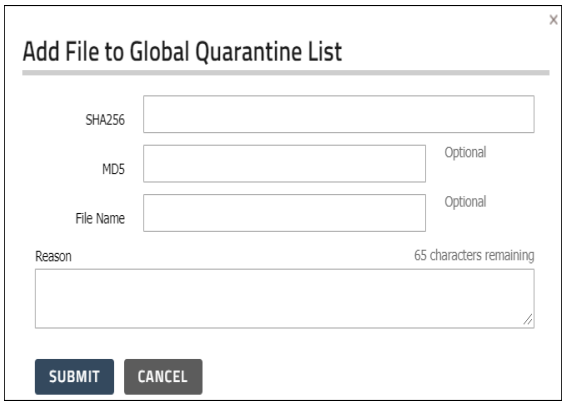


Address Threats Globally

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**.



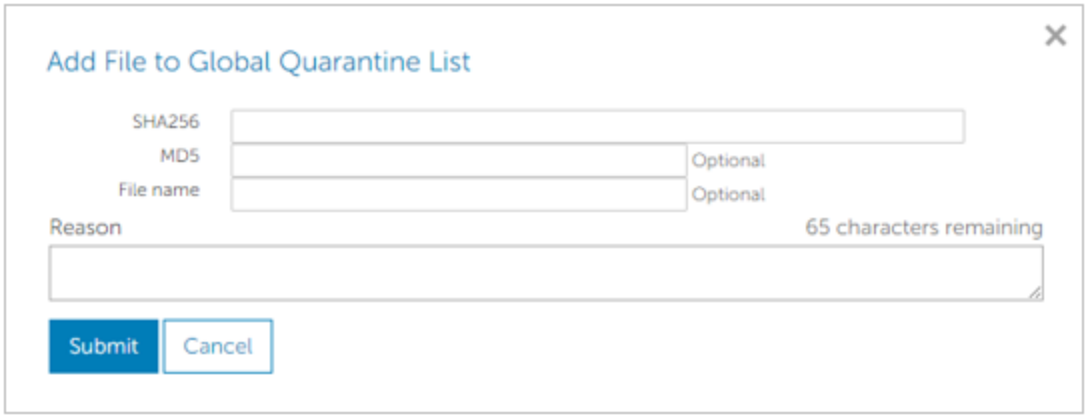


Figure 60: Global Quarantine List

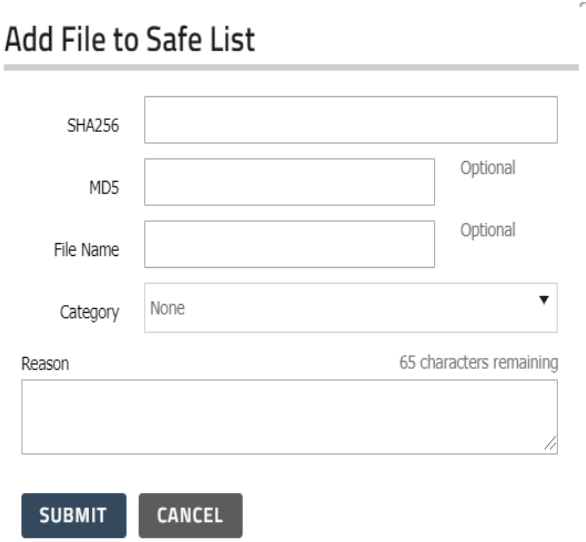


Figure 61: Global Safe List

Protection — Script Control

Threat Defense provides details about Active scripts, PowerShell scripts 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.

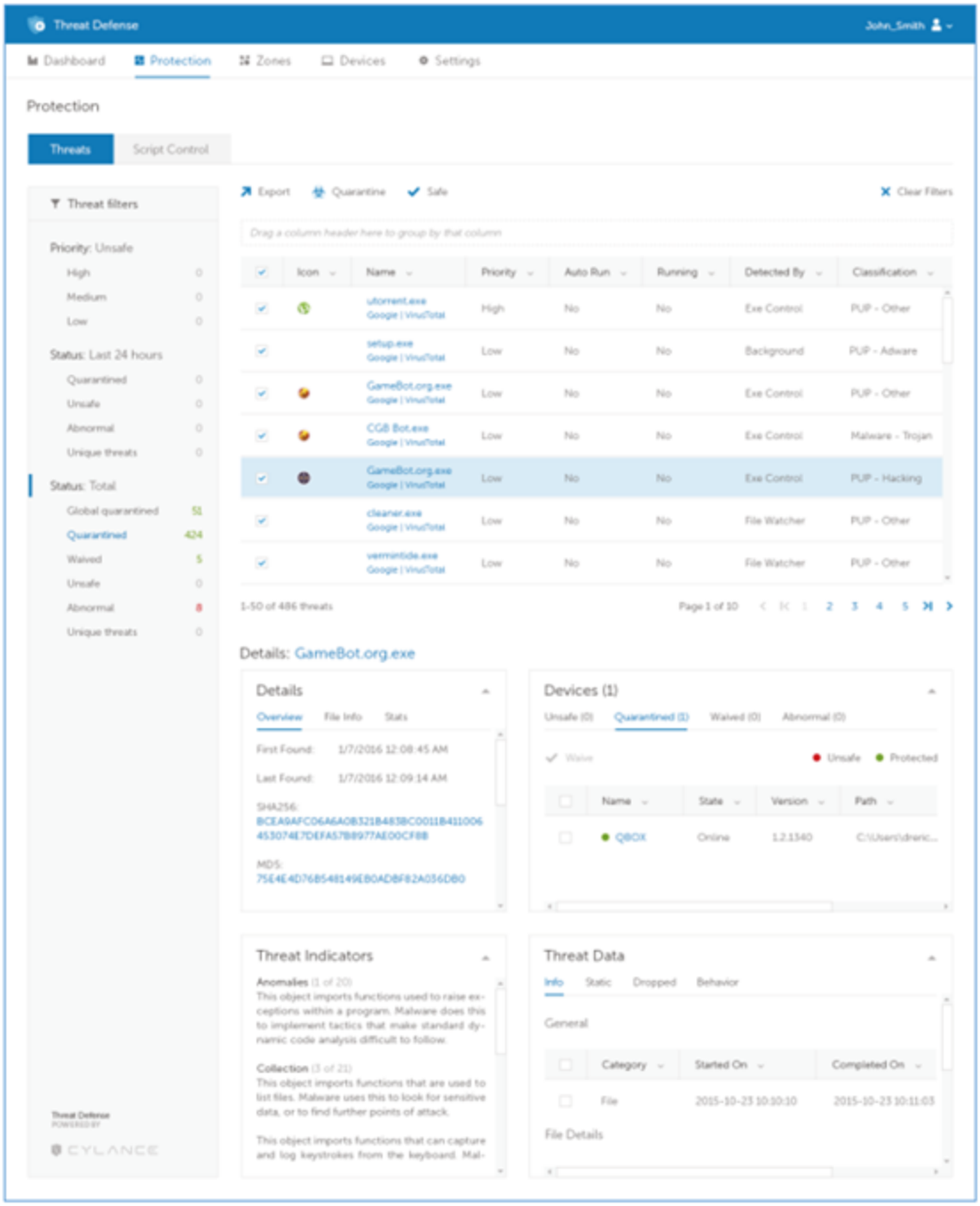


Figure 62: Script Tab — Protection Page

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).

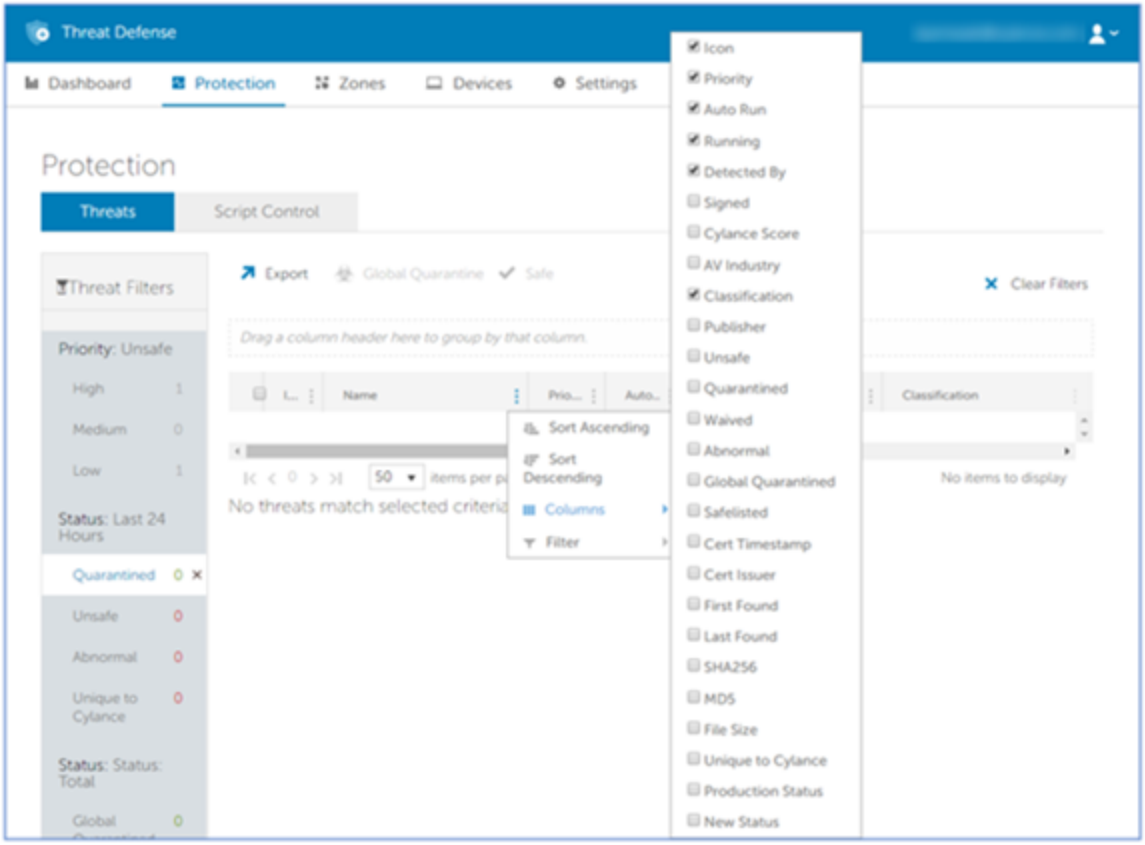


Figure 63: Protection – Selecting Columns

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 10.

- 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.

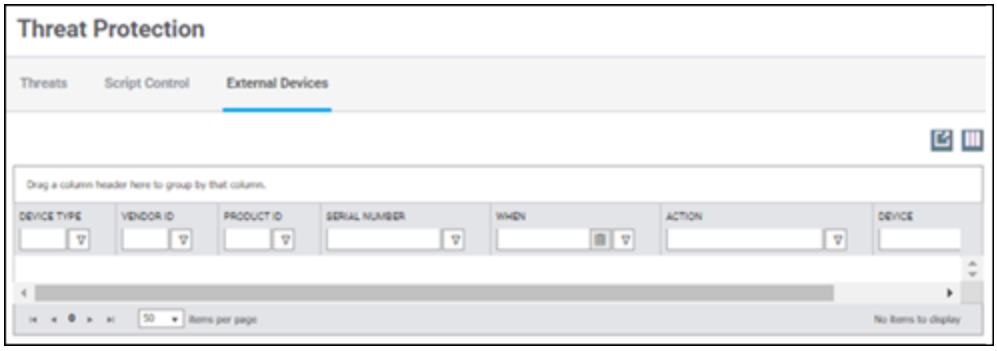


Figure 64: Protection > External Devices

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.

  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*.

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**.

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.

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.

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.

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.

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.

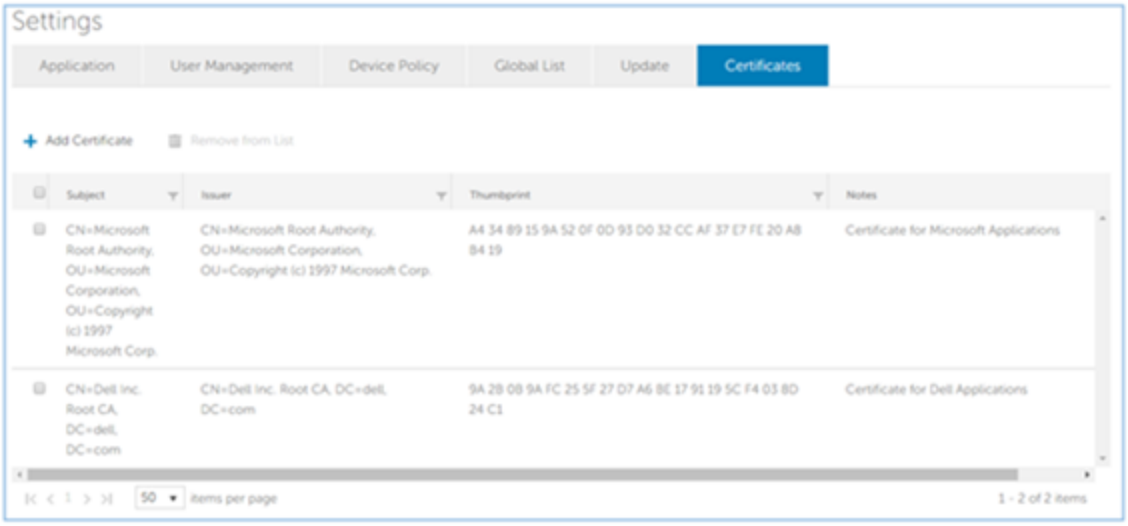


Figure 65: Certificate Repository

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 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.

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.

Threat Defense Overview Report

Provides an executive summary of your Threat Defense usage, from the number of zones and devices, to the percentage of your devices covered by Auto-Quarantine, Threat Events, Agent versions, and Offline Days for devices.

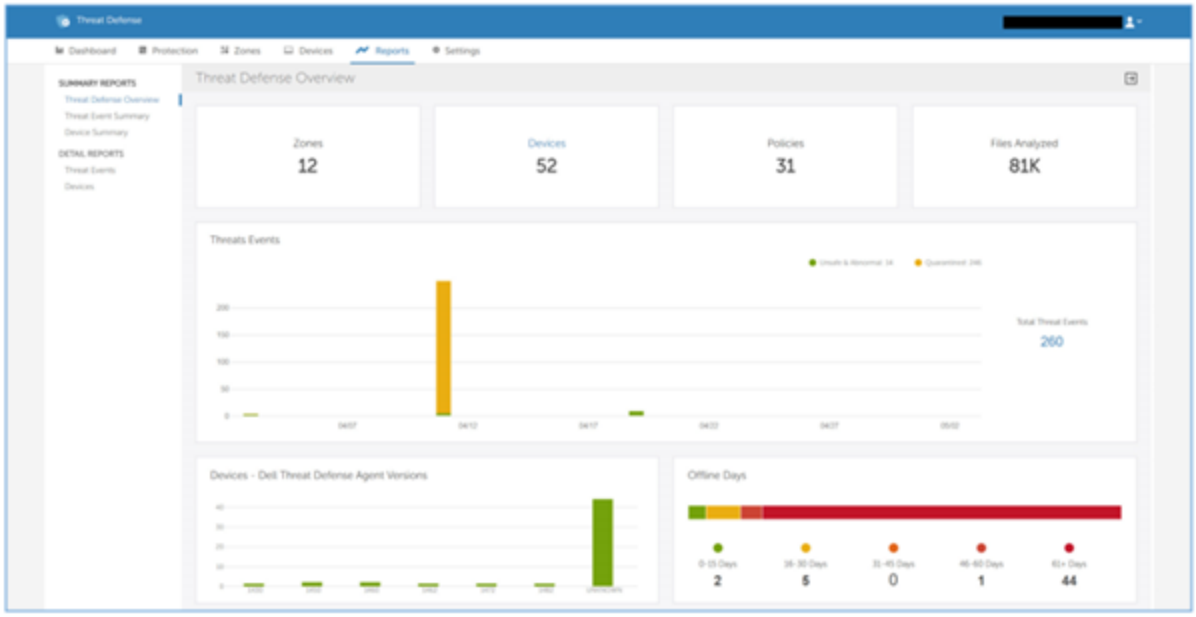


Figure 66: Summary Reports – Threat Defense Overview

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 Threat Defense 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.
- **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 – Dell Threat Defense Agent Version Stats:** Displays a bar chart representing the number of devices running a Threat Defense Agent version. Hovering over a bar in the chart displays the number of devices running that specific Threat Defense 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.

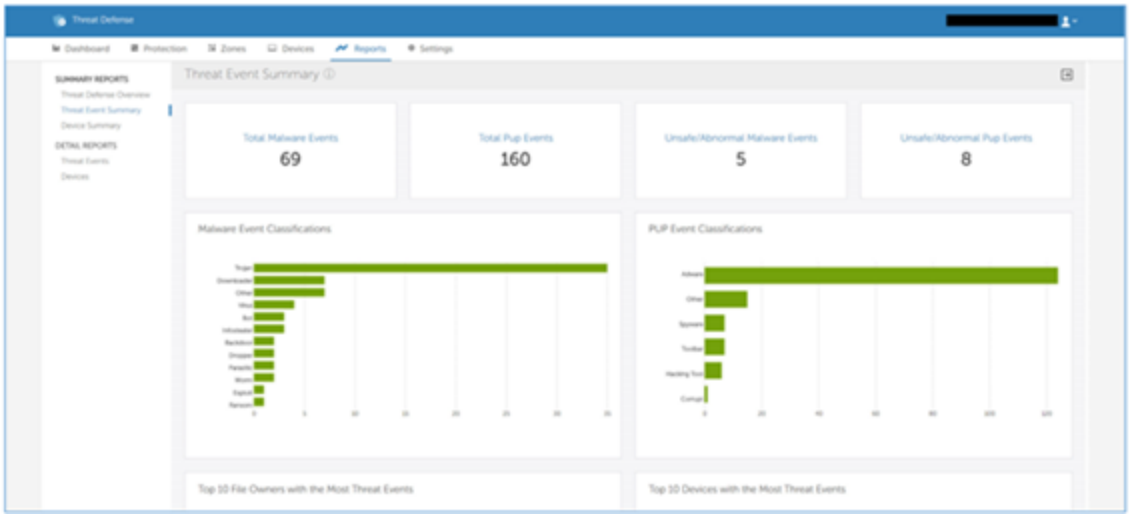


Figure 67: Summary Reports – Threat Event Summary

- **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 – Threat Defense Version Stats can identify older Threat Defense Agents. Offline Days may indicate devices that are no longer checking in to the Threat Defense Console and are candidates for removal.

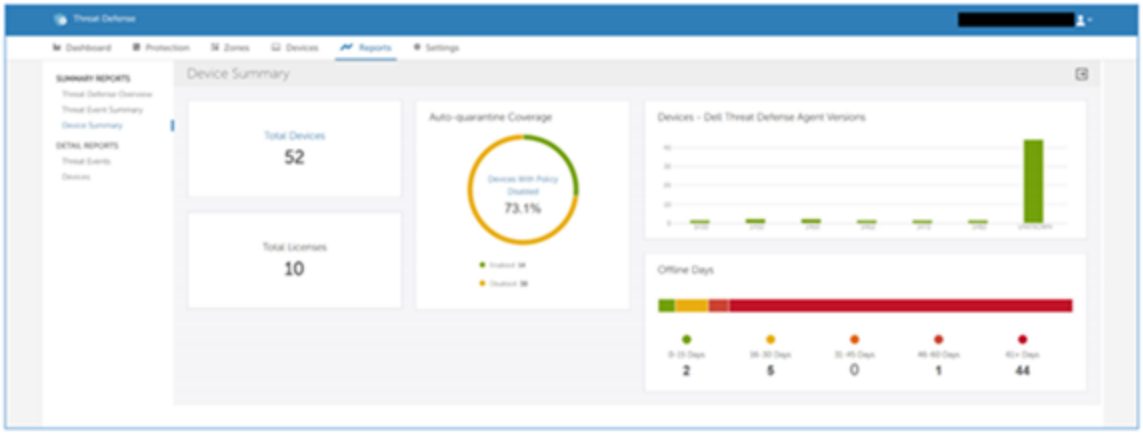


Figure 68: Summary Reports – Device Summary

- **Total Devices:** Displays a count of devices in the organization. A device is an endpoint with a registered Threat Defense 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 Threat Defense licenses the organization has purchased.

- **Devices – Dell Threat Defense Agent Version Stats:** Displays a bar chart representing the number of devices running a Threat Defense Agent version. Hovering over a bar in the chart displays the number of devices running that specific Threat

Defense 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.

- **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.

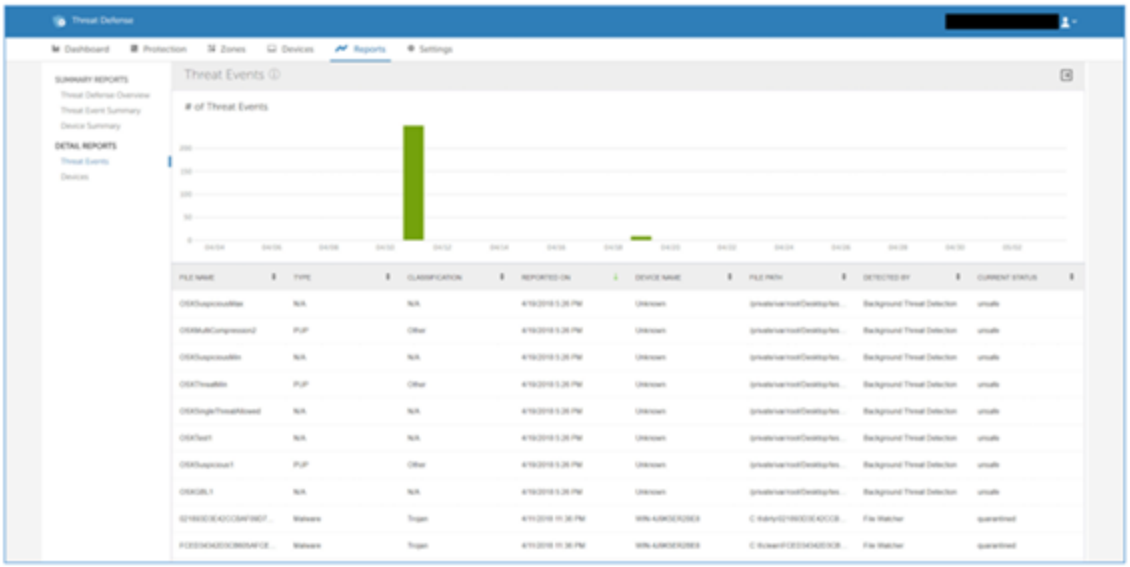


Figure 69: Detail Reports – Threat Events

- **# 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).

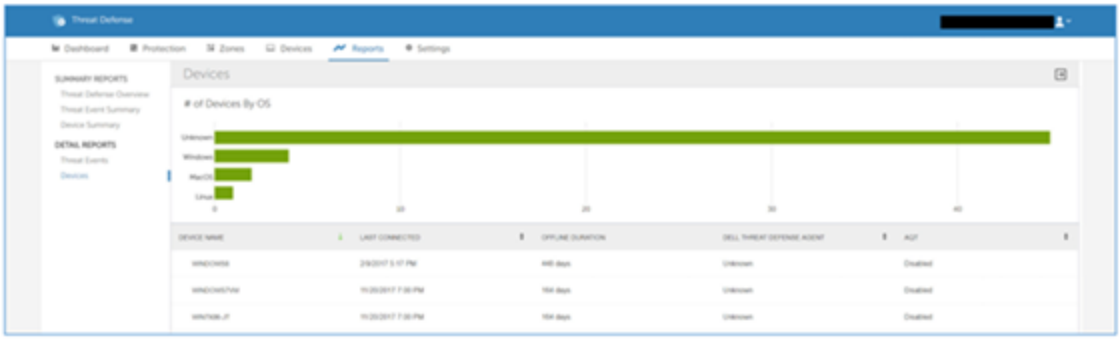


Figure 70: Detail Reports – Devices

- **# of Devices by OS:** Displays a bar chart with devices organized by major OS groups (Windows, 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 (Threat Defense 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.

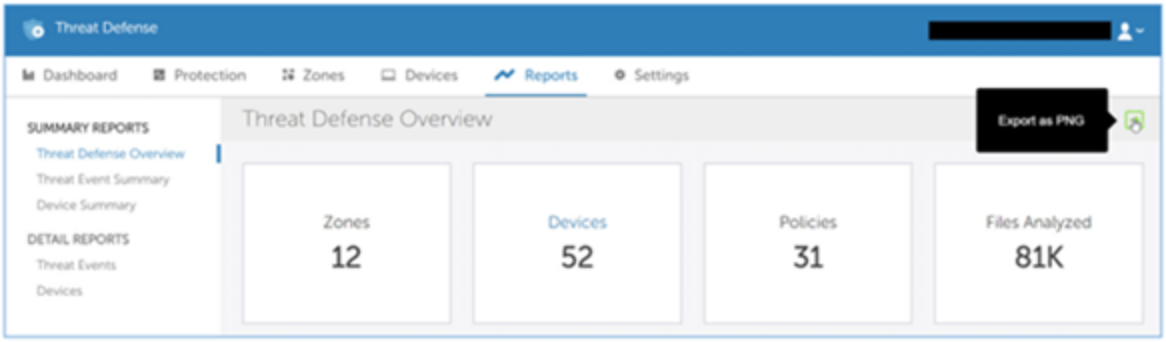


Figure 71: Export a Report

ADMINISTRATION

Application

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.

Syslog/SIEM Settings

Threat Defense 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 (Dell-specific payload) is limited to 2048 characters.

The following is a list of Syslog IP addresses for Dell Threat Defense.

Asia-Pacific North East (protect-apne1.cylance.com):

13.113.53.36

13.113.60.107

Asia-Pacific South East (including Australia; protect-au.cylance.com):

52.63.15.218

52.65.4.232

Europe – Central (protect-euc1.cylance.com):

52.28.219.170

52.29.102.181

52.29.213.11

North America (protect.cylance.com):

52.2.154.63

52.20.244.157

52.71.59.248

52.72.144.44

54.88.241.49

South America – East (protect-sae1.cylance.com):

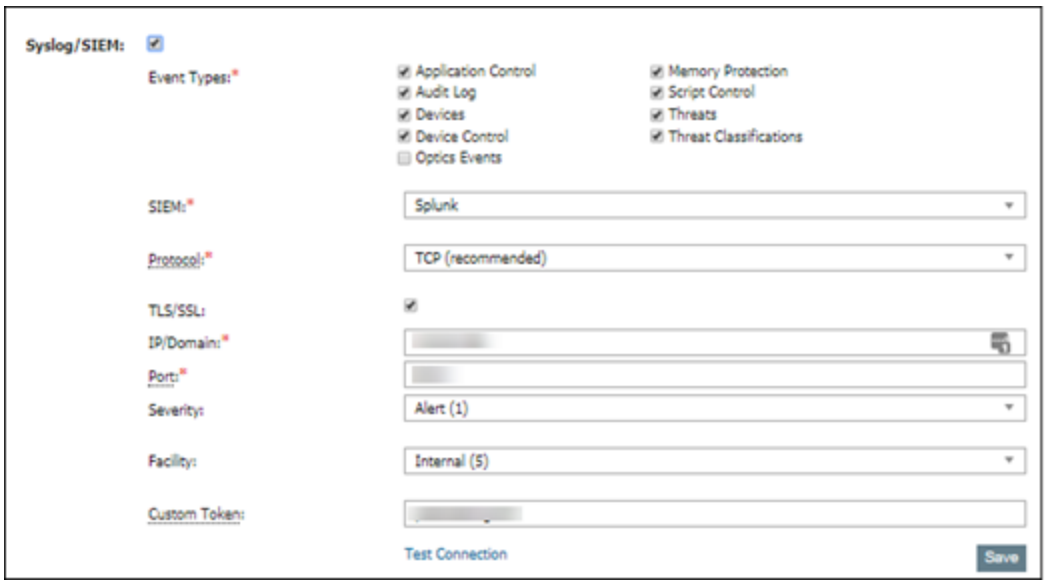
52.67.244.213

52.67.252.42

Figure 72: Configure Syslog/SIEM

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 Dell-specific payload (message). Examples provided in this section only contain the Dell-specific message.

Audit Log

Selecting this option will send the audit log of user actions performed in the Threat Defense 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

```
Threat Defense: Event Type: AuditLog, Event Name: ThreatGlobalQuarantine, Message:
SHA256:A1E92E2E84A1321F499A5EC500E8B9A9C0CA28701668BF13EA56D3995A96153F,1CCC95B7B2F78
1D55D538CA01D6049762FDF6A75B32A06DF3CC2EDC1F1573BFA; Reason: Manually blacklisting
these 2 threats., User: (                    )
```

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

  ```
  Threat Defense: Event Type: Device, Event Name: Registration, Device Name:

  Threat Defense: Event Type: Device, Event Name: SystemSecurity, Device Name: WIN-
  55NATVQHBUU, Agent Version: 1.1.1270.58, IP Address: (), MAC Address:
  (7), Logged On Users: (), OS: Microsoft
  Windows Server 2008 R2 Standard Service Pack 1 x64 6.1.7601
  ```

- When a device is removed.

  Example Message for Device Removed Event

  ```
  Threat Defense: Event Type: Device, Event Name: Device Removed, Device Names: (
  ), User: ()
  ```

- When a device's policy, zone, name, or logging level has changed.

  Example Message for Device Updated Event

  ```
  Threat Defense: Event Type: Device, Event Name: Device Updated, Device Message:
  Renamed: ' to '; Policy Changed: 'Default' to
  'IRVPolicy1'; Zones Added: 'IRV1', User: John Smith ()
  ```

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

```
Threat Defense: Event Type: Threat, Event Name: threat_found, Device Name: [redacted]
1, IP Address: ([redacted]), File Name: virusshare_00fbc4cc4b42774b50a9f71074b79bd9,
Path: c:\ruby\host_automation\test\data\test_files\, SHA256:
1EBF3B8A61A7E0023AAB3B0CB24938536A1D87BCE1FCC6442E137FB2A7DD510B, 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, Dell 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

```
Threat Defense: Event Type: ThreatClassification, Event Name: ResearchSaved, Threat
Class: Malware, Threat Subclass: Worm, SHA256:
12184931373 21C1D1F897B0C25BEF17CDD0BE9C99B84B4DD8B51EAC8F9794F65
```

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 Threat Defense 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

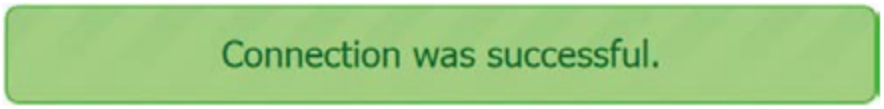
Specifies the severity of the messages that should appear in the Syslog server. This is a subjective field, and you may set it to whatever level you require. The value of severity does not change the messages that are forwarded to Syslog.

Facility

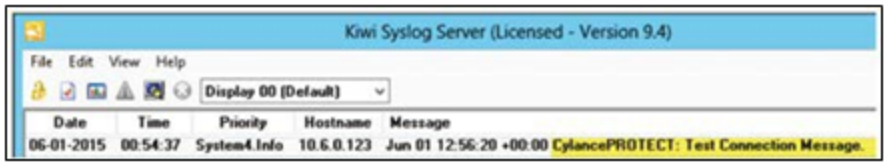
Specifies what type of application is logging the message. The default is Internal (or Syslog). This is used to categorize the messages when they are received by the Syslog server.

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 Threat Defense: 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.

An example can be found in the Custom Authentication Implementation article.

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

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 Threat Defense but was cleared when:
  - An administrator deleted the quarantined threats from the Threat Defense Console
  - A user deleted the threat that was on the disk. This includes if an application, other than Dell, 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

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.
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.

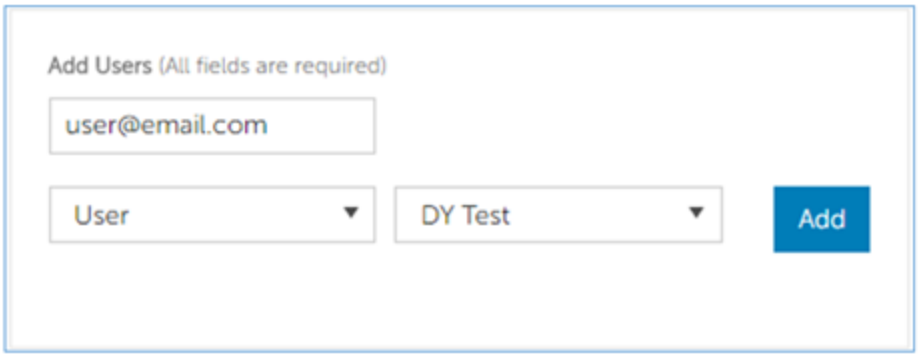


Figure 73: Add Users

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.

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.

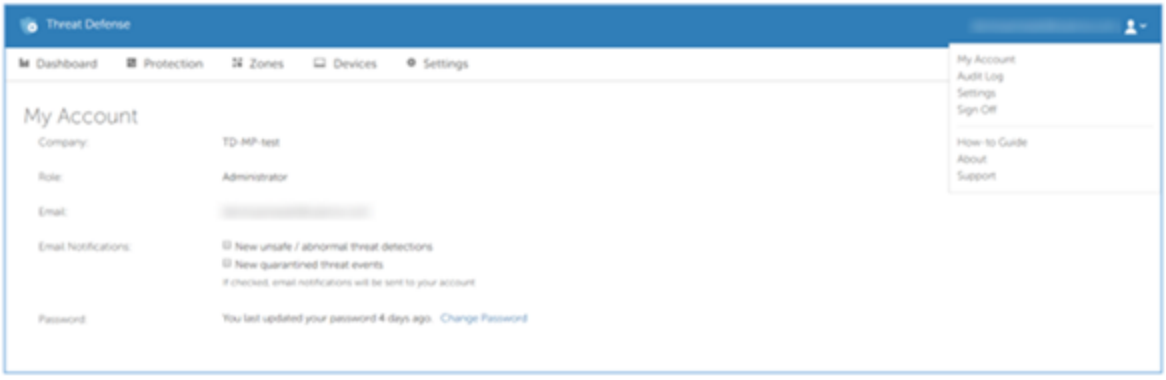


Figure 74: My Account

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)
- Agent Update (Edit)

The Audit Log can be viewed from the Console by navigating to the profile drop-down list list on the upper-right side of the Console, and selecting **Audit Log**.

The Audit Log can be exported as a CSV file for use in other applications. Click the **Export** button on the Audit Log page.

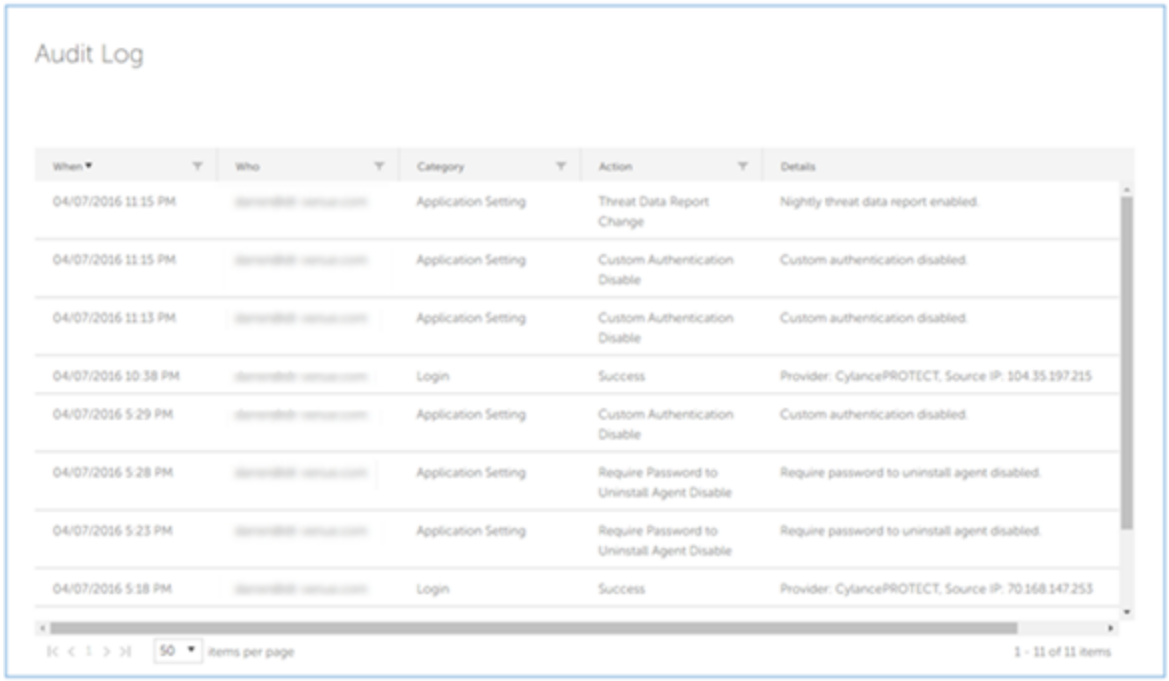


Figure 75: Audit Log

Network Related

Configure the network to allow the Threat Defense Agent to communicate with the Console over the Internet. This section covers firewall settings and proxy configurations.

Firewall

No on-premise software is required to manage devices. Agents are managed by and report to the Console (cloud-based user interface). 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.

Ensure that Agents can communicate with the following sites:

North America	Asia-Pacific Northeast	Asia-Pacific Southeast
login.cylance.com	login-apne1.cylance.com	login-au.cylance.com
data.cylance.com	data-apne1.cylance.com	data-au.cylance.com
protect.cyalnce.com	protect-apne1.cyalnce.com	protect-au.cylance.com
update.cylance.com	update-apne1.cylance.com	update-au.cylance.com
api.cylance.com	api.cylance.com	update-au.cylance.com
download.cylance.com	download.cylance.com	download.cylance.com

Europe	South America East
login-euc1.cylance.com	login-sae1.cylance.com
data-euc1.cylance.com	data- sae1.cylance.com
protect-euc1.cylance.com	protect- sae1.cylance.com
update-euc1.cylance.com	update- sae1.cylance.com
api.cylance.com	api.cylance.com
download.cylance.com	download.cylance.com

Alternatively, allow HTTPS traffic to *.cylance.com.

Proxy

Proxy support for Threat Defense 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.

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.

TROUBLESHOOTING

This section provides a list of questions to answer and files to collect when troubleshooting issues with Threat Defense. This information enables Dell Support to assist in resolving issues.

This section also contains some common issues and suggested solutions.

Note: Working on most issues will require verbose Agent log files that record the incident. It is recommended to enable verbose logging on the endpoint, record the incident, and send that log file to Dell Support. Read the Verbose Logging article 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).**
  - Read the Verbose Logging article for more information.

Performance Concerns

- Capture a screenshot of the Task Manager (Windows) or Activity Monitor (macOS) that shows the Threat Defense processes and memory consumption.
- Capture a dump of the Threat Defense process.
- Collect debug logs. See "Enable Debug Logging" on the next page.
- 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 114 for more information.
- Restart the Threat Defenseservice 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, Threat Defense maintains log files stored in `C:\Program Files\Cylance\Desktop\log`. For troubleshooting purposes, Threat Defense can be configured to produce more verbose logs. Read the Verbose Logging article for more information.

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 1372. Starting with Agent 1382 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}
```

Time Zone Variances

Depending on where you are in Threat Defense, the time zone used can vary.

Feature	Time Zone
Devices with an agent installed, including event notifications and agent logs.	Uses the time zone of the local machine.
Console, except for the Reports tab and exported data.	Uses the time zone for the user viewing the Console.
Reports tab in the Console.	Uses the UTC time zone.
Syslog events	Uses the UTC time zone.
Threat Data Report or any exported data in the console	Uses the UTC time zone.

APPENDIX A: VDI BEST PRACTICES

Dell customers can protect both physical and virtual machines with Threat Defense technology. This guide explains the best practices for deploying the Threat Defense Agent onto Windows-based virtual desktop infrastructure (VDI) workstations.

Note: Threat Defense resides at the guest OS level. Hypervisor level capability is not *yet* a Threat Defense capability.

Threat Defense 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

Threat Defense works well as a guest OS component and has the following advantages:

- Threat Defense 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, Threat Defense returns capacity to the IOPS budget.
- Threat Defense is not as memory intensive on a per guest basis. Therefore, Threat Defense returns capacity to the memory budget.

The preparation and deployment of Dell in virtual environments is similar to deployment on physical machines. However, the following recommendations for VDI deployments will ensure that Dell performs efficiently in a virtual environment with fewer allocated resources. The objective is to produce a clean image that Threat Defense has analyzed so that there are no outstanding malicious files (Unsafe or Abnormal) on the Gold image.

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 Threat Defense 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.

At a high level, the tasks are:

1. In the Threat Defense 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 Threat Defense.

   Note: For non-persistent virtual machines, see "Non-Persistent VDI Install Parameter" on page 127 for more information on preparing this Gold image.

b. Apply the **VDI_preparation** policy.

3. Use Threat Defense 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 Threat Defense **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 BTD scan.
   c. Use Threat Defense 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 Threat Defense malware prevention capabilities to production VDI images.

Gold Image Preparation

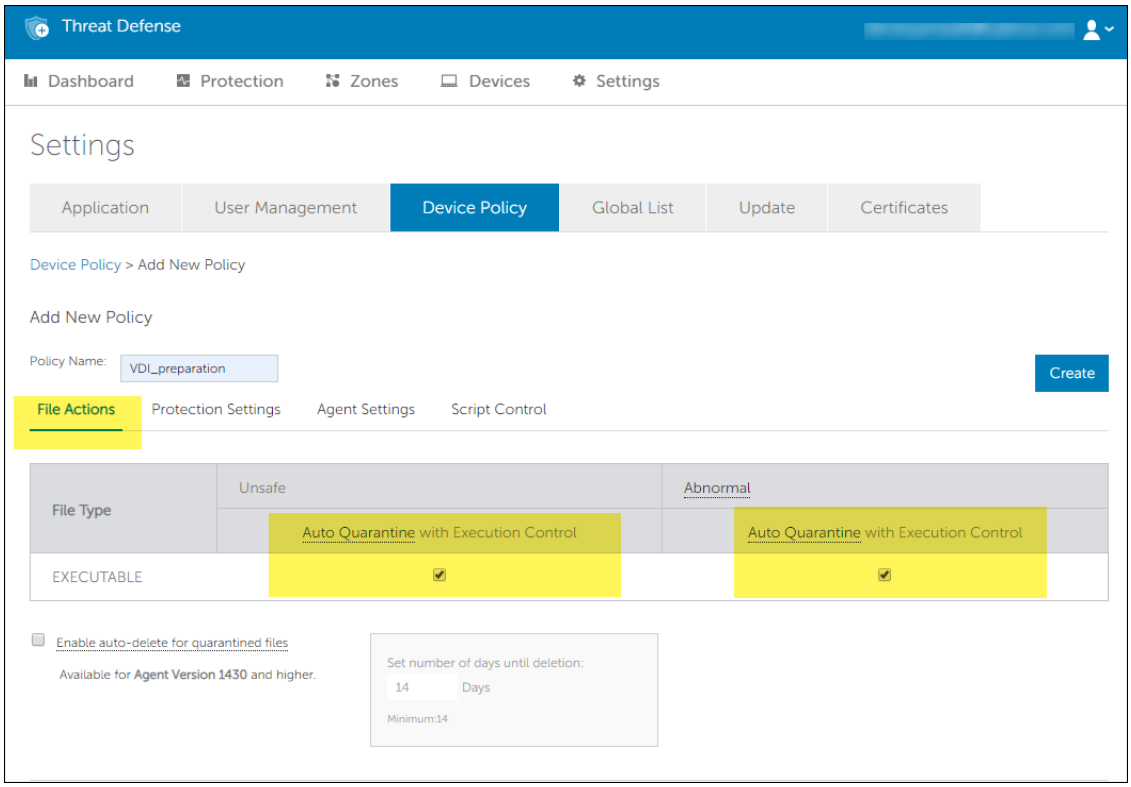
Create the Windows VDI Gold image. For a list of supported OSes, see "Windows Agent" on page 31.

Gold images should be fully scanned and prepared before deploying them as persistent or non-persistent production images. This is accomplished by installing the Threat Defense 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.

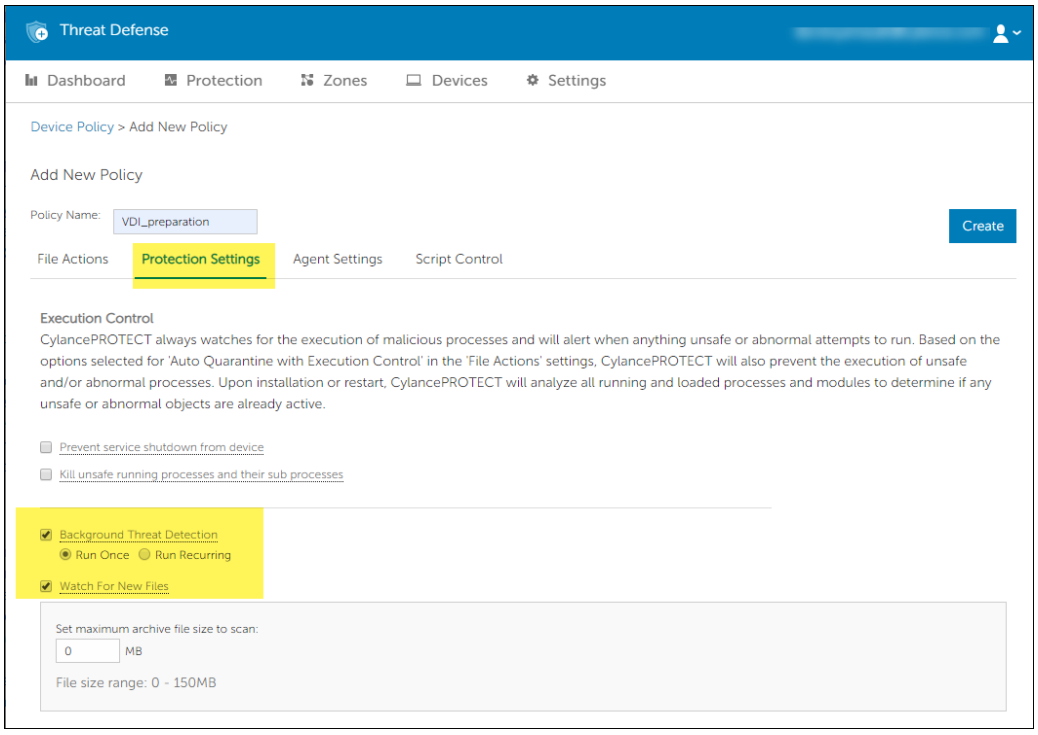
Policy Settings

From the Dell 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:

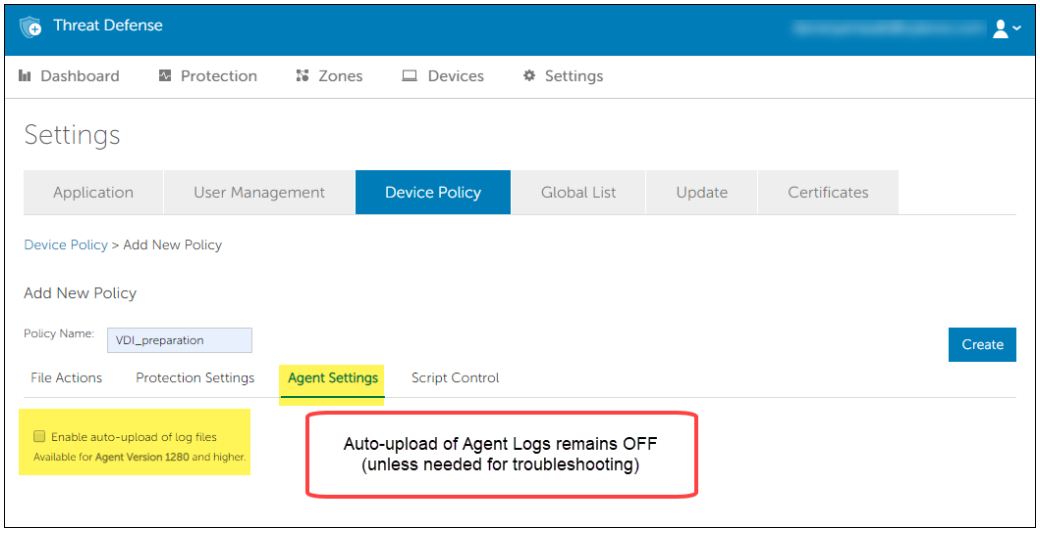
File Actions



Protection Settings



Agent Settings



Agent Installation

Agent Installation can be approached like a traditional installation on a physical machine. The Threat Defense Agent must first be downloaded from the Dell Console.

Example: MSI installation

- MSI Installer (using Standard Installer options)

  ```
  msiexec /package Dell Threat Defense_x64.msi /quiet
  PIDKEY=<INSTALLATION TOKEN> LAUNCHAPP=1
  ```

- MSI Installer (using Windows Installer options)

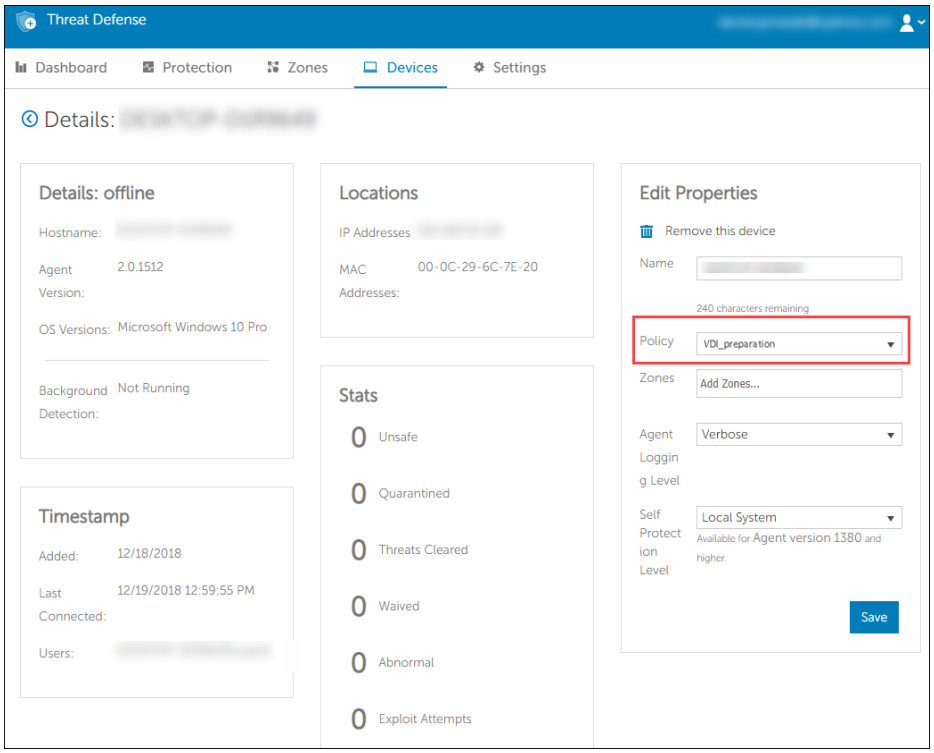
  ```
  msiexec /i Dell Threat Defense_x64.msi /qn
  PIDKEY=<INSTALLATION TOKEN> LAUNCHAPP=1
  ```

For further installation parameters and instructions, see "Windows Installation Parameters" on page 34.

For non-persistent virtual machines, see "Non-Persistent VDI Install Parameter" on page 127 for more information on preparing this Gold image.

Apply the Policy and Review Findings

1. Open the Dell 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).

5. 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 Dell 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.

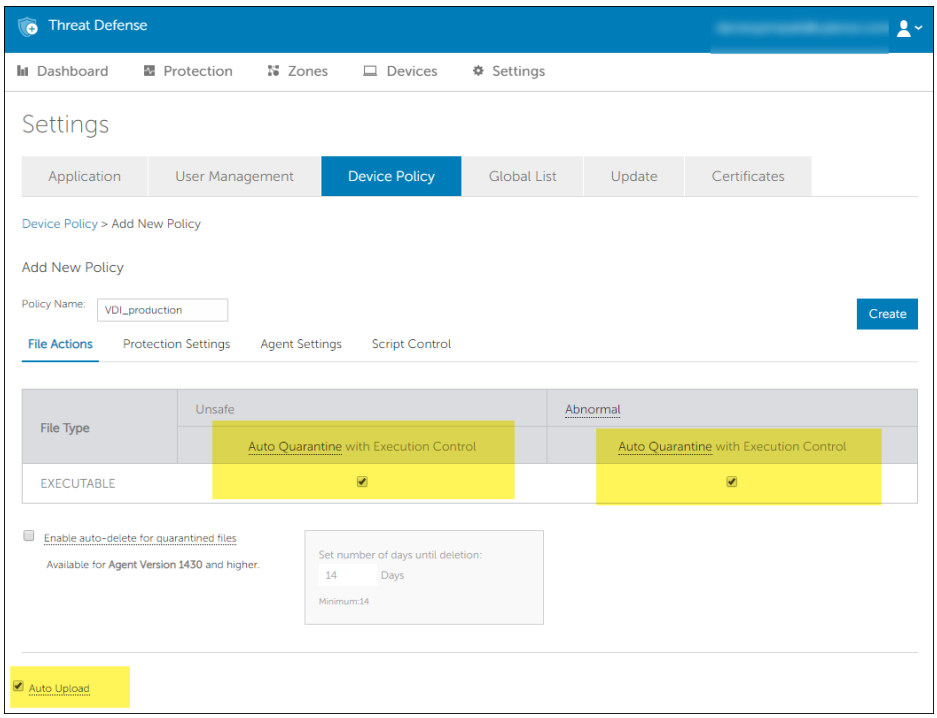
Conversely, non-persistent desktops are typically one-time use systems. The user starts the VDI desktop session, performs work and then upon shutdown, the system is destroyed. While being used, these non-persistent systems check-in to the Dell Console and are registered as a device. If the UUID already 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 127 for more information on preparing this Gold image.

1. When the Gold image has been prepared and is ready for production, apply the Threat Defense **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:

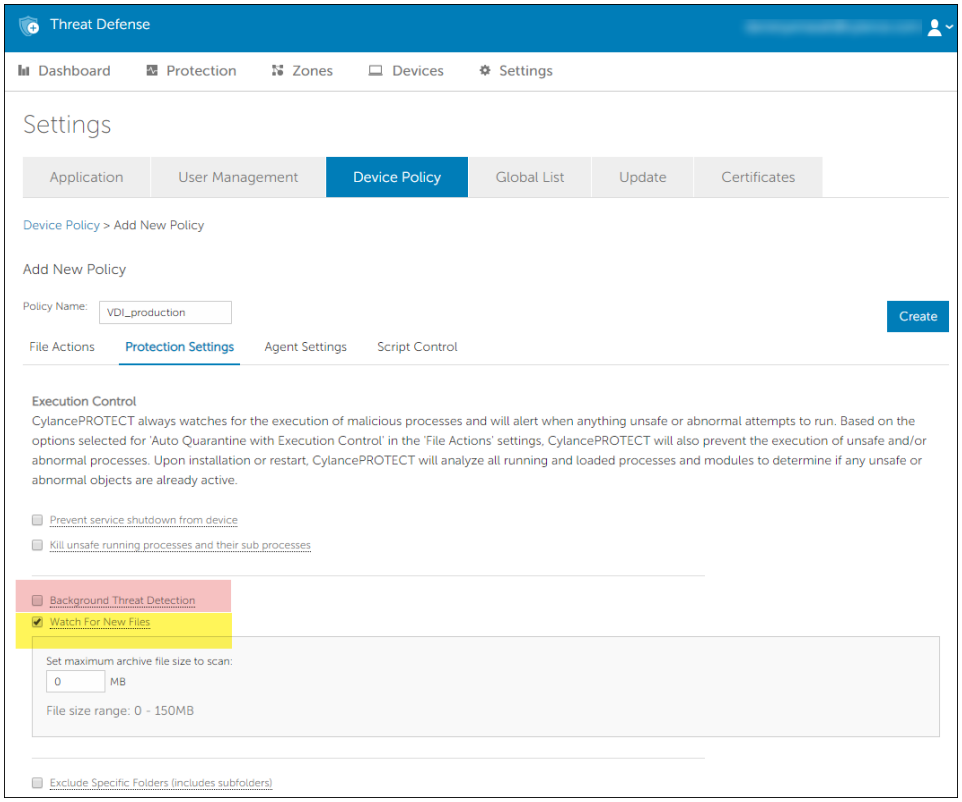
   File Actions

   This policy adds Auto Quarantine with Execution Control.



Protection Settings

Background Threat Detection is toggled OFF in this policy. It is not necessary to re-run BTD for clone images since this was completed during the Gold image preparation phase.



2. 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, Threat Defense 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 Script Control

Threat Defense also offers Script Control as optional protective policy components. Running the Threat Defense 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. Script Control may require special consideration in VDI environments.

This function uses 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 Threat Defense's ability to properly monitor memory. Hence, it is recommended to always test Script Control on test machines before deploying to production.

Non-Persistent VDI Install Parameter

Dell uses a unique fingerprint to identify endpoints with a Threat Defense Agent.

There are two different, but similar installation parameters that can be utilized:

- VDI=<X>

  This feature is available in Threat Defense Agent version 1492 and higher.

- AD=1

  This feature is available in Threat Defense Agent version 1522 and higher.

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 DellThreatDefenseSetup_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.

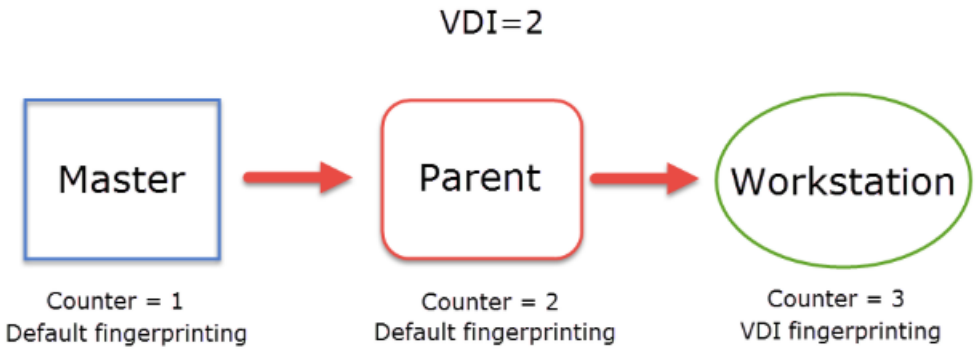


Figure 76: VDI=X Example

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 utilize 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 DellThreatDefenseSetup_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 utilize 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 utilized on a master image that is domain connected, will immediately utilize VDI fingerprinting on the master image and subsequently created pool of workstations.

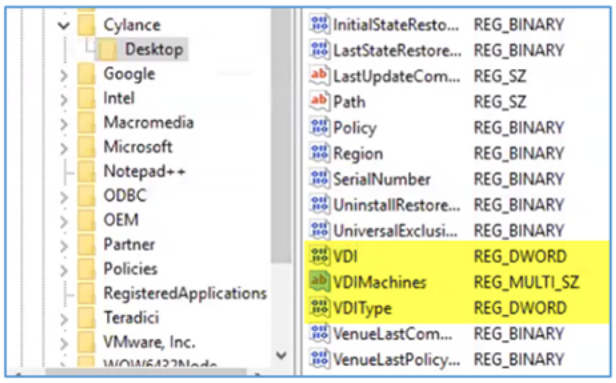
VDI=<X> utilizes a counter "X" and has a delayed effect, where as "AD=1" is immediate upon installation.

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 Threat Defense Console under **Settings > Update**.

If the entire environment is virtual, simply set "Production" to "Do Not Update".

If the environment is mixed, and there are a specific subsection of virtual machines, users can utilize 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 24.

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 BTD scan and can skip to step 5.
3. Use Threat Defense 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: HANDLING EXCEPTIONS

There are times when users need to either manually *Quarantine* or *Allow* (*Waive*) a file. Threat Defense provides ways to handle exceptions for each device (*Local*), for a group of devices (*Policy*), or for the entire organization (*Global*).

Files

Local: *Quarantine* or *Waive* (*Safe List*) a file on the device. Useful to temporarily *Block* or *Allow* a file until there is time to analyze it. *Waiving* a file on a device is also useful if that device is the only device on which the file should be allowed to *Execute*. Dell recommends use of *Policy* or *Global* if this action needs to be performed on multiple devices.

Policy: *Safe List* a file on all devices assigned to a policy. Useful to allow a file for a group of devices (for example, allowing IT devices to run tools that could be used for malicious purposes, such as PsExec). *Quarantine* a file at the Policy level is not available.

Global: *Quarantine* or *Safe List* a file for the organization. *Quarantine* a known malicious file in the organization. *Safe List* a file that is known to be good and is used in the organization, but the Agent is flagging as malicious.

Scripts

Policy: Script Control allows approving scripts to run from a designated folder. Allowing scripts to run for a folder also allows scripts in sub-folders.

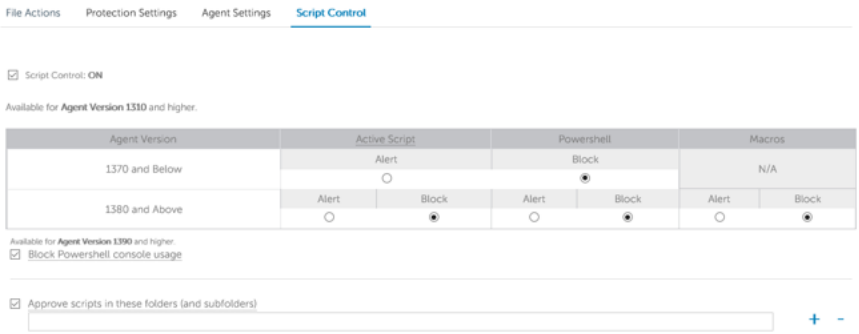


Figure 77: Script Control

Certificates

Global: Add certificates to the Console, then add them to the *Global Safe List*. This allows applications and scripts signed by this certificate to run in the organization.

To add a certificate, select **Settings > Certificates**, then click **Add Certificate**.

To add the certificate to the *Global Safe List*, select **Settings > Global List**, select the **Safe** tab, select the **Certificates** tab, then click **Add Certificate**.

APPENDIX C: USER PERMISSIONS

Actions users can perform depends upon the user permission (role) assigned to them. In general, Administrators can perform actions anywhere in the organization. Zone Managers and Users are restricted to the Zones they are assigned to. This restriction includes only being able to access devices within a Zone, and only seeing threat data related to those devices. If a Zone Manager or User cannot see a device or threat, chances are the device does not belong to any Zones assigned to them. Read-Only users can view most of the content in the Console, but they cannot take any actions or change any settings.

Audit Logging	USER	ZONE MANAGER	READ ONLY	ADMIN
View			X	X
Devices				
View Devices		X	X	X
Add Devices – Global				X
Add Devices to a Zone				X
Remove Devices – Global				X
Remove Devices from a Zone		X		X
Edit Device Name		X		X
Policy				
View Policies		X	X	X
Create Policy – Global				X
Create Policy for a Zone				X
Add Policy – Global				X
Add Policy to a Zone		X		X
Remove Policy – Global				X
Remove Policy from a Zone		X		X
Reports				
View Reports				X
Export Reports				X
Sript Control				
View Script Control events	X	X	X	X
Quarantine Scripts – Global	X	X		X
Quarantine Scripts in a Zone	X	X		X
Waive Scripts – Global				X

Audit Logging	USER	ZONE MANAGER	READ ONLY	ADMIN
Waive Scripts in a Zone	X	X		X
Global Quarantine/Safe				X
Settings – Application				
View Application settings	X	X	X	X
Generate or delete install token				X
Generate or delete invite URL				X
Copy install token	X	X		X
Copy invite URL				X
Settings – Certificate				
View Certificates		X	X	X
Add Certificate				X
Remove Certificate				X
Settings – Device Policy				
View Policies		X	X	X
Create Policies				X
Edit Policies				X
Remove Policies				X
Settings – Global List				
View Global List		X	X	X
Add File or Script				X
Add to Safe List				X
Add to Global Quarantine List				X
Remove From List				X
Settings – Update				
View Update			X	X
Select Zones				X
Select Agent Version				X
Settings – User Management				
View Users		X	X	X
Assign Users to any Zone			X	X
Assign Users to managed Zone		X		X

Audit Logging	USER	ZONE MANAGER	READ ONLY	ADMIN
Assign Zone Manager – Global				X
Assign Zone Manager to managed Zones		X		X
Delete users from Console				X
Remove Users from Zone – Global				X
Remove Users from managed Zone		X		X
Threats				
View Threats	X	X	X	X
Quarantine Files – Global				X
Quarantine Files in a Zone	X	X		X
Waive Files – Global				X
Waive Files in a Zone	X	X		X
Global Quarantine/Safe				X
Zones				
View Zones		X	X	X
Create Zone				X
Delete Zone				X
Edit Zone Name – Any				X
Edit Assigned Zone Name		X		X

APPENDIX D: FILE-BASED WRITE FILTER

The Dell Threat Defense Agent can be installed on a system running Windows Embedded Standard 7 (Thin Client). On embedded devices, writing to the system's storage might not be allowed. In this case, the system might use a File-Based Write Filter (FBWF) to redirect any writes to the system's storage to the cache in the system's memory. This can cause issues with the Agent losing changes whenever the system restarts.

When using the Agent on an embedded system, use the following procedure:

1. Before you install the Agent, disable FBWF using the command: `fbwfmgr /disable`.
2. Restart the system. This allows disabling FBWF to take effect.
3. Install the Dell Threat Defense Agent.
4. After installing the Agent, re-enable FBWF using the command: `fbwfmgr /enable`.
5. Restart the system. This allows enabling FBWF to take effect.
6. In FBWF, exclude the following folders:
    a. C:\Program Files\Cylance\Desktop – Excluding this folder allows Agent updates to persist after a system restart.
7. Use the following command to exclude the Desktop folder:
   `fbwfmgr /addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. This assumes you are installing to the default directory. Change the exclusion to the folder you installed the Agent to.
8. If you plan to store threats on the machine for testing against the Agent, be sure to exclude the storage location from FBWF as well (`C:\Samples` for example).

APPENDIX E: GLOSSARY

Abnormal — A suspicious file with a lower score (1 – 59); less likely to be malware.

Administrator — Tenant manager for **Threat Defense**.

Agent —Threat Defense Endpoint Host that communicates with the Console.

Audit Log — Log that records actions performed from the **Threat Defense** 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 — Threat Defense Management User Interface.

Cylance Cloud — The Mathematical Model used to score files.

Device Policy —Threat Defense policy that can be configured by an organization administrator that defines how threats are handled on all devices.\

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).

Organization — A tenant account using the **Threat Defense** service.

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

Threats — Potentially malicious files detected by **Threat Defense**, 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).

Watch for New Files — Feature that will detect and analyze any new files on disk.

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.