# Dell Threat Defense
# Installation and Administrator Guide
Powered by Cylance
v17.08.07

# 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.
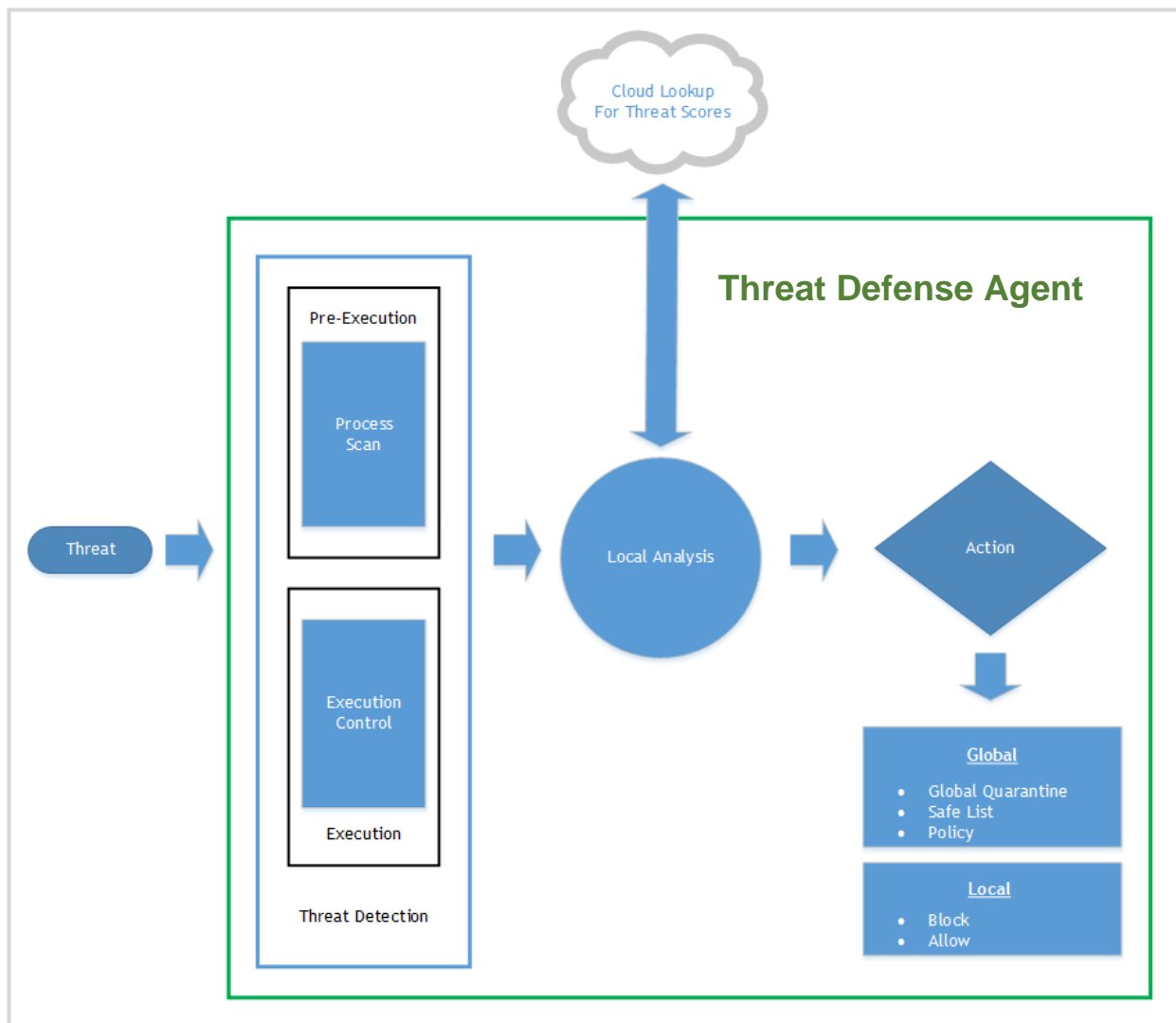
## How it Works

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.
- **Analysis**: How files are identified as malicious or safe.
  - **Cloud Lookup for Threat Scores**: The mathematical model in the cloud and 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

Dell recommends that users become familiar with the cloud-based Console before installing the Agent on endpoints. Understanding how endpoints are managed makes protecting and maintaining them easier. This workflow is a recommendation. Users can approach deploying in their environment in a way that makes sense for them.

**Example**: Zones help group devices in the organization. For example, configure a Zone with a Zone Rule that automatically adds new devices to a Zone based on selected criteria (such as Operating System, Device Name, or Domain Name).

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

# CONSOLE

The Threat Defense Console is a website that is logged in to, to 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.

| French | German | Italian | Japanese |
|---|---|---|---|
| Portuguese (Iberian) | Korean | Spanish | Portuguese (Brazilian) |

*Table 1: Supported Threat Defense Console Languages*

# 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 to go to the login page or go to:

- North America: http://dellthreatdefense.com
- Europe: http://dellthreatdefense-eu.cylance.com
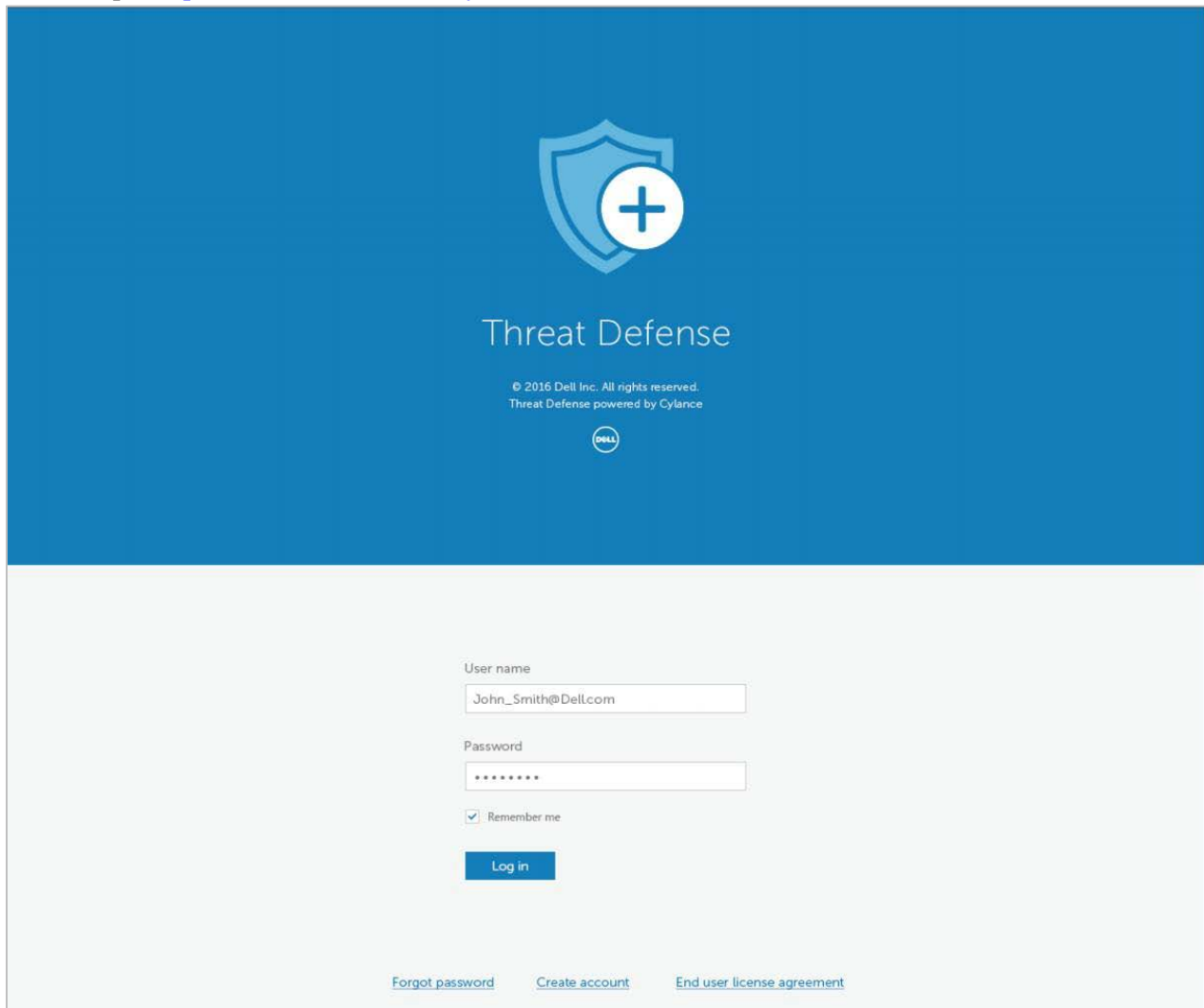


*Figure 2: Console Login*

# 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 can 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. Login to the Console (http://dellthreatdefense.com) as an Administrator. Only Administrators can create Policies.

2. Select **Settings > Device Policy**.

3. Click **Add New Policy**.

4. Enter a Policy Name and select policy options.

5. Click **Create**.

## 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 the Protection – Threats section.

*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**: Dell highly recommends that *Auto Quarantine* is tested on a small number of devices before applying it in the production environment. The test results should be observed to ensure that no business-critical applications are blocked at execution.

## Auto Upload

Dell recommends that users enable Auto Upload for both *Unsafe* and *Abnormal* files. Threat Defense automatically uploads any detected *Unsafe* or *Abnormal* file to the Cylance Infinity Cloud to perform a deeper analysis of the file and provides additional details.

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 for analysis, not one file per device.

## Policy Safe List

Add files that are considered safe, at the Policy level. The Agent will not apply any threat actions to files on this list.

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

1. Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) as an Administrator. Only Administrators can create Policies.

2. Select **Settings > Device Policy**.

3. Add a new policy or edit an existing policy.

4. Click **Add File** under *Policy Safe List*.

5. Enter the **SHA256** information. Optionally include the MD5 and File Name if known.

6. Select a **Category** to help identify what this file does.

7. Enter a reason for adding this file to the *Policy Safe List*.

8. 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.

### *Copy Malware Samples*

Allows specification of a network share in which to copy malware samples. 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: `c:\test`.

- All files meeting the criteria are 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.

## Script Control

Script control protects devices by blocking malicious Active Script and PowerShell scripts from running.

1. Log in to the Console (http://dellthreatdefense.com).

2. Select **Settings > Device Policy**.

3. Select a policy and click **Protection Settings**.

4. Select the check box to enable **Script Control**.

   a. **Alert**: Monitor scripts running in the 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.

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

5. Click **Save**.
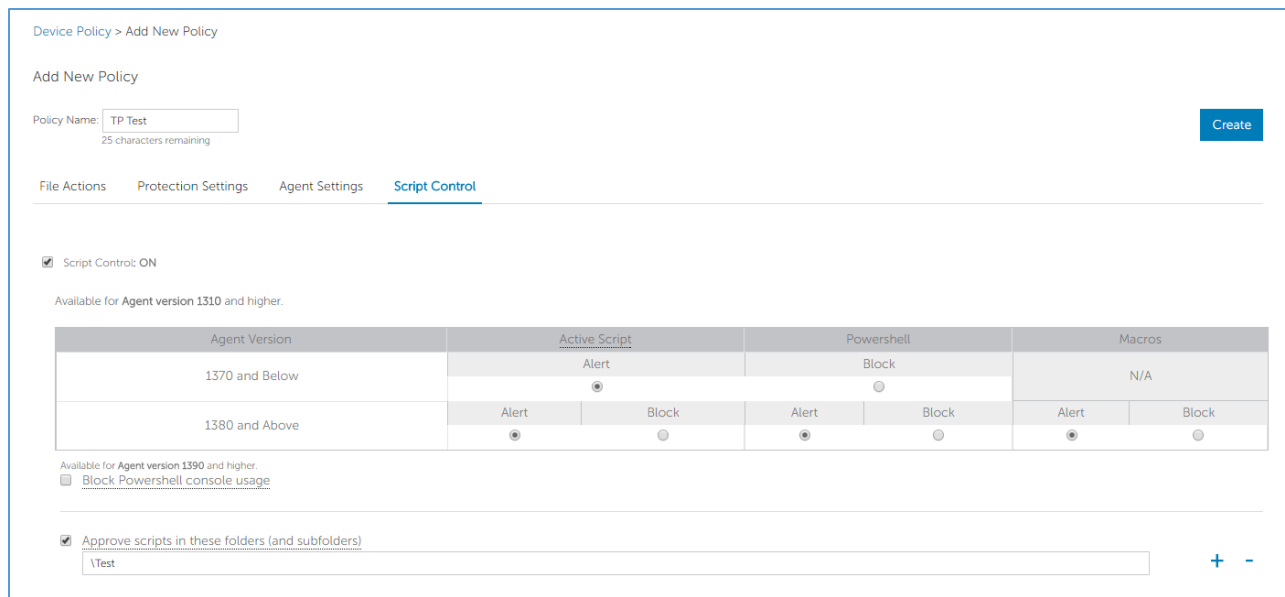
*Figure 6: Policy Details > Script Control*

## Agent Logs

*SETTINGS > Device Policy > [select a policy] > Agent Logs*

Enable Agent Logs in the Console to upload log files and allow viewing in the Console.

1. Log in to the Console (http://dellthreatdefense.com).

2. Select **Settings > Device Policy**.

3. Select a policy and click **Agent Logs**. Ensure the device selected for log files is assigned to this policy.

4. Select **Enable auto-upload of log files** and click **Save**.

5. Click the **Devices** tab and select a device.

6. Click **Agent Logs**. The log files display.

7. Click a log file. The log file name is the date of the log.
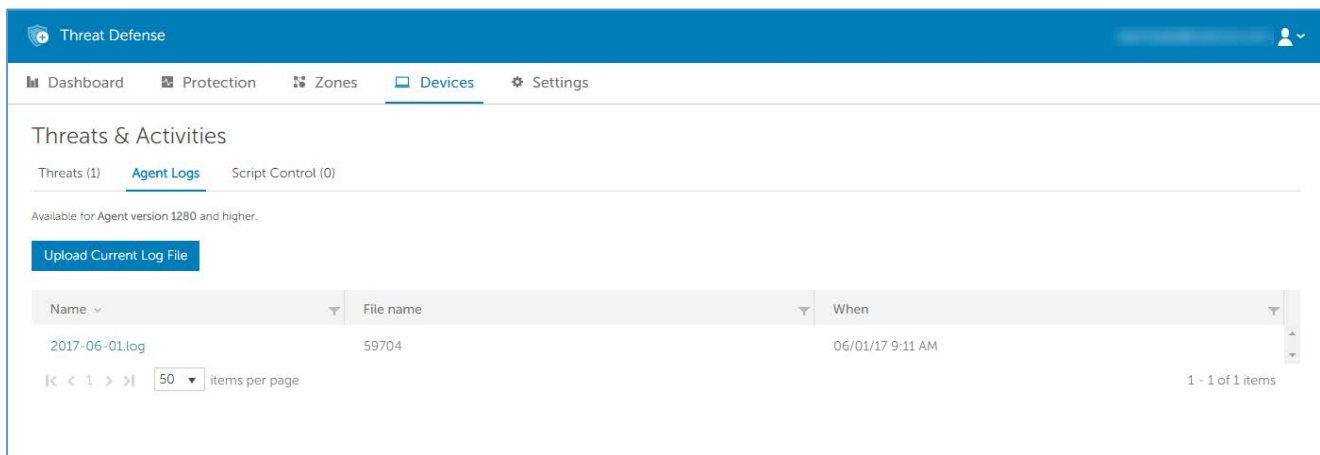


*Figure 7: Devices > [select a device] > Agent Logs*

Installation and Administrator Guide

# Policy Best Practices

When policies are first created, Dell recommends implementing policy features in a phased approach to ensure that performance and operations are not impacted. Create new policies with more features enabled as the understanding of how Threat Defense works in the environment.

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

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

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

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

    b.  Check the Console for any threat alerts.

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

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

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

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

2.  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).

3.  Under File Actions, turn on **Auto-Quarantine**.

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

4.  Under Protection Settings, turn on **Script Control**.

    Script Control protects users from malicious scripts running on their device.

    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`).

# Zones

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

An organization has a default Zone (Unzoned) that only Administrators 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 how that Zone is configured. This also allows Zone Managers and Users to access devices they are responsible for. 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 for the following reasons:

- 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, see [Zone Management Best Practices](#).

## *To Add a Zone*

1. Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) as an Administrator. Only Administrators can create Zones.

2. Click **Zones**.

3. Click **Add New Zone**.

4. 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.

5. Click **Save**.

## *To Add Devices to a Zone*

1. Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) 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 **Add Devices to Zone**. A list of devices displays.

5. 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 being used to organize devices, not manage the policy for those devices.

## *To Remove a Zone*

1. Log in to the Console (http://dellthreatdefense.com) as an Administrator. Only Administrators can remove Zones.

2. Click **Zones**.

3. Select the check boxes for the Zones to remove.

4. Click **Remove**.

5. Click **Yes** at the message asking for confirmation of the selected Zone removal.

## <u>Zone Properties</u>

Zone properties can be edited as needed.
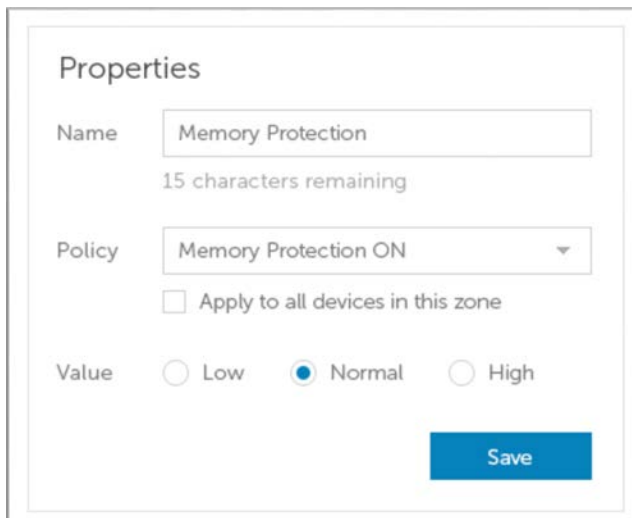
## *About Zone Priority*

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 to change the priority value.

### *To Edit Zone Properties*

1. Login to the Console (http://dellthreatdefense.com) as an Administrator or Zone Manager.

2. Click **Zones**.

3. Click a Zone from the *Zones List*.

4. Enter a new name in the **Name** field to change the Zone Name.

5. Select a different policy from the **Policy** dropdown menu to change the policy.

6. Select a **Low**, **Normal**, or **High** Value.

7. Click **Save**.



*Figure 8: Change Zone Properties*

# Zone Rule

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 pre-existing devices that match the rule are added to that Zone.
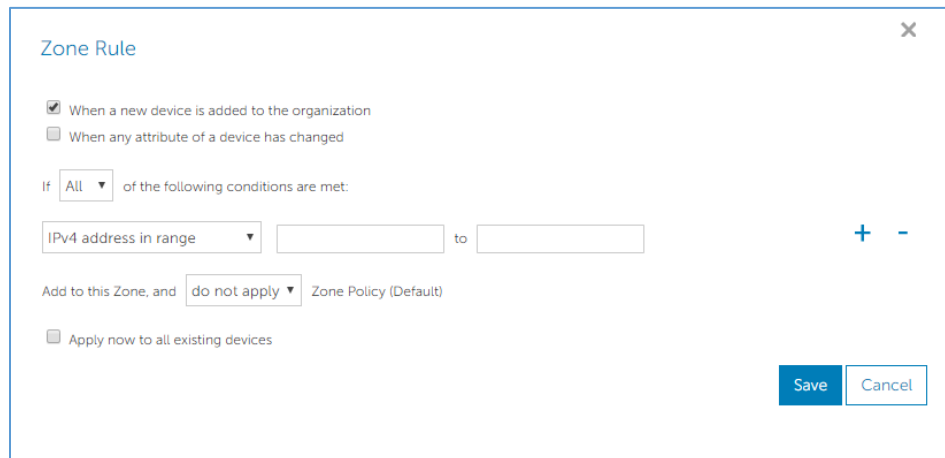
**Note**: Zone Rules automatically add devices to a Zone but cannot remove devices. Changing the device's IP address or hostname does not remove that device from a Zone. Devices must be removed manually from a Zone.

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 view which policy is applied to a device.

### To Add a Zone Rule

1. Login to the Console (http://dellthreatdefense.com) as an Administrator or Zone Manager.

2. Click **Zones** and select a Zone from the *Zones List*.

3. Click **Create Rule** under Zone Rule,

4. Specify the criteria for the selected Zone. Click the plus sign to add more conditions. Click the minus sign to remove a condition.

5. Click **Save**.



*Figure 9: 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.

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

- **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.

- **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.

- **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.

- **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: The Member Of (Group) must match this.
    - Contains: The Member Of (Group) must contain this.

- **Following Conditions Met**:
    - All: All conditions in the Zone Rule must match to add the device.
    - Any: At least one condition in the Zone Rule must match to add the device.

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

- 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, as follows.
    - o Example: CN=JDoe,OU=Sales,DC=dell,DC=COM
    - o Example: 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 *Zone Device List*.

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

## 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 that can be created, 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.

### *Add a Test or Pilot Zone*

1. Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) with an Administrator or Zone Manager account.

2. Select **Settings > Agent Update**.

3. 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.

4. Click **Please Select Version**.

5. Select an Agent version to apply to the Test or Pilot Zone.

6. Click **Apply**.
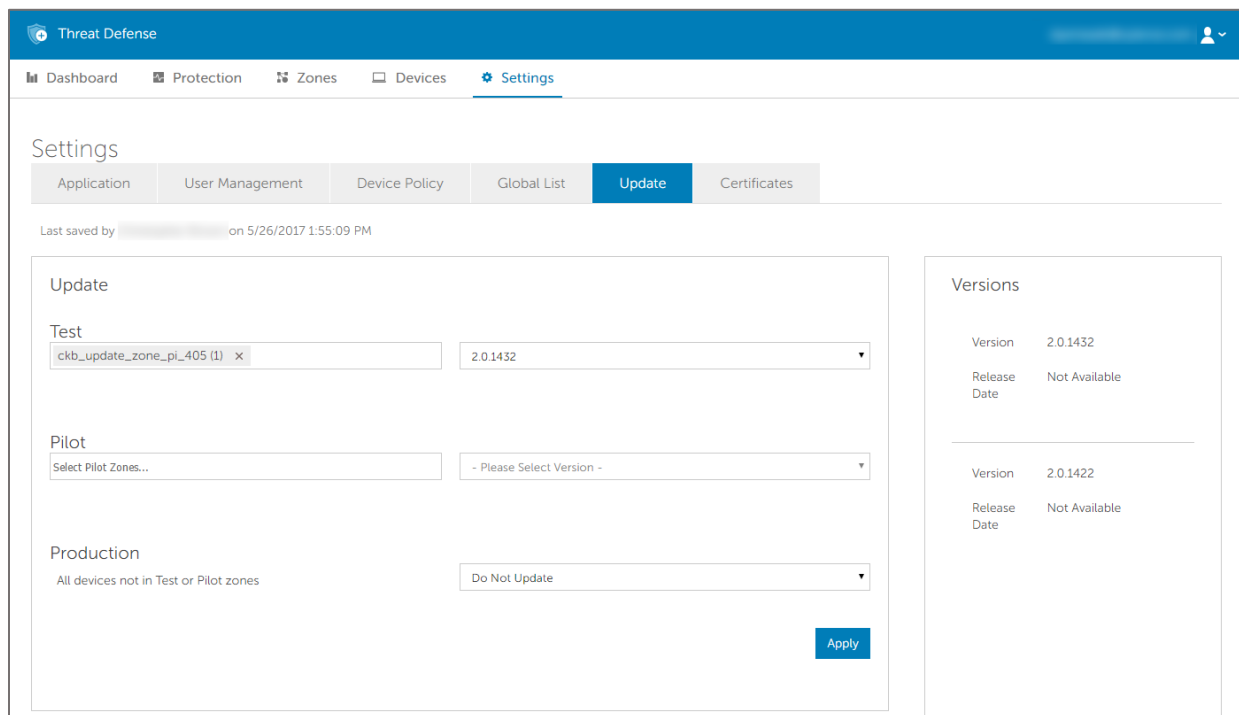


*Figure 10: Zone-based Updating*

## 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 –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)

Using the above Zone examples, a Zone Manager could be assigned to *RBAC Zone – Desktops – Europe*, and would only have access to devices within that Zone. If the Zone Manager user 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.

# User Management
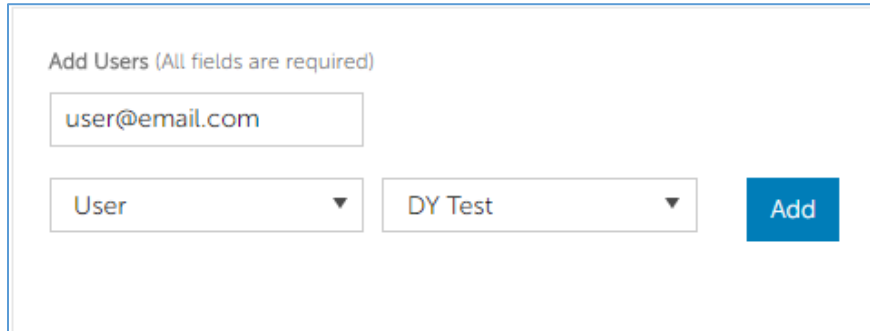
Administrators have global permissions and can add or remove users, assign users to Zones (either as a User or a Zone Manager), add or remove devices, create policies, and create Zones. Administrators can also delete users, devices, policies, and Zones permanently from the Console.

Users and Zone Managers only have access and privileges pertaining to the Zone to which they are assigned. This applies to devices assigned to the Zone, threats found on those devices, and information on the dashboard.

For a comprehensive list of user permissions allowed for each user, see Appendix C: User Permissions.

### To Add Users

1.  Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) as an Administrator. Only Administrators can create Users.

2.  Select **Settings > User Management**.

3.  Enter the user's email address.

4.  Select a Role in the Role dropdown menu.

5.  When adding a Zone Manager or User, select a Zone to assign them to.

6.  Click **Add**. An email is sent to the user with a link to create a password.



*Figure 11: Add Users*

### To Change User Roles

1.  Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) as an Administrator. Only Administrators can create Users.

2.  Select **Settings > User Management**.

3.  Click a user. The User Details page displays.

4.  Select a role and click **Save**.

### To Remove Users

1.  Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) as an Administrator. Only Administrators can create Users.

2.  Select **Settings > User Management**.

3.  Select the check box for the user or users to remove.

4.  Click **Remove**.

5.  Click **Yes** at the message asking for confirmation of the removal.

# 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-premises software is required to manage devices. Threat Defense 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:

| America Destinations | Europe Destinations | Asia Destinations | Protocol | Port |
| --- | --- | --- | --- | --- |
| login.cylance.com | login-euc1.cylance.com | login-au.cylance.com | HTTPS | TCP 443 |
| data.cylance.com | data-euc1.cylance.com | data-au.cylance.com | HTTPS | TCP 443 |
| protect.cylance.com | protect-euc1.cylance.com | protect-au.cylance.com | HTTPS | TCP 443 |
| update.cylance.com | update.cylance.com | update.cylance.com | HTTPS | TCP 443 |
| api.cylance.com | api-euc1.cylance.com | api-au.cylance.com | HTTPS | TCP 443 |
| download.cylance.com | download.cylance.com | download.cylance.com | HTTPS | TCP 443 |
| syslog.cylance.com | syslog.cylance.com | syslog.cylance.com | HTTPS | TCP 443 |

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 the 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):

   o Value Name = ProxyServer

   o 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.

# Devices

Once an Agent is installed on an endpoint, it becomes available as a device in the Console. Begin to manage devices by assigning policy (to handle identified *Threats*), group devices (using *Zones*), and manually take actions on each device (*Quarantine* and *Waive*).

## Device Management

Devices are computers with a Threat Defense Agent. Manage devices from the Console.

1. Login to the Console (http://dellthreatdefense.com) as an Administrator. Only Administrators can manage Devices.

2. Click **Devices**.

3. 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.

   - **Assign Policy**: Allows assignment of the selected devices to a policy.

   - **Add to Zones**: Allows adding the selected devices to a Zone or Zones.

4. Click a device to display the Device Details page.

   - **Device information**: Displays information such as Hostname, Agent Version, and 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.

5. Click **Add new device** to display a dialog with an Installation Token and links to download the Agent installer.

6. In the Zones column, click a Zone Name to display the Zone Details page.

## 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 information such as 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. 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 (*Global Quarantine*) when a file is *Quarantined*.

- **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 a file is *Waived*.

### *Exploit Attempts*

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

### *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**

1. 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 any log files are uploaded.

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, Dell recommends changing 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**

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

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

2. Enter the following command line and then press **Enter**.

```
Dell.ThreatDefense.exe –a
```

3. The Threat Defense icon displays in the system tray. Right-click, select **Logging**, then click **All** (same as Verbose in the Console).

**OR (For Mac OS X)**

1. Exit the currently running user interface.

2. Execute the following command from terminal.

```
sudo /Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -a
```
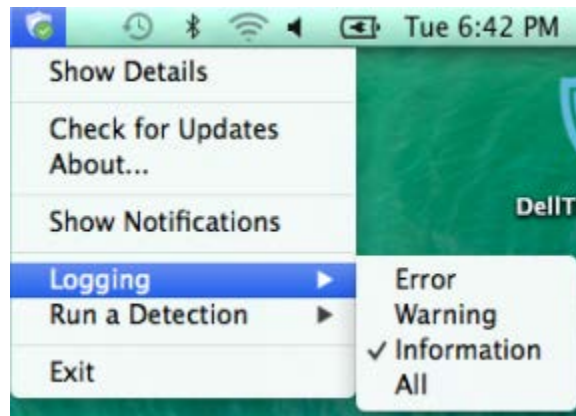
3. Right-click the new user interface once it opens. Select **Logging > All**.



*Figure 12: Mac OS X Verbose Logging*

## *Script Control*

Displays all activities relevant to Script Control, such as denied scripts.

## 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 does not issue an uninstall command to the Threat Defense Agent. The Agent needs to be uninstalled at the endpoint.

# Agent Update

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

The Agent checks in with the Console every 1-2 minutes. The Console reports the Agent's current state (*Online* or *Offline*, *Unsafe* or *Protected*), Version Information, Operating System, and Threat Status.

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. In order 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.

## *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.  Login to the Console ([http://dellthreatdefense.com](http://dellthreatdefense.com)) with an Administrator account.

2.  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.

3.  Select a specific Agent version in the Production dropdown list.

4.  For Production, also select Auto-Update or Do Not Update.

    a.  **Auto-Update** allows all Production devices to automatically update to the latest version in the *Supported Agent Versions List*.

    b.  **Do Not Update** prohibits all Production devices from updating the Agent.

5.  For the Test Zone, choose one or more Zones from the Zone dropdown list, then select a specific Agent version from the version dropdown list.

6.  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.
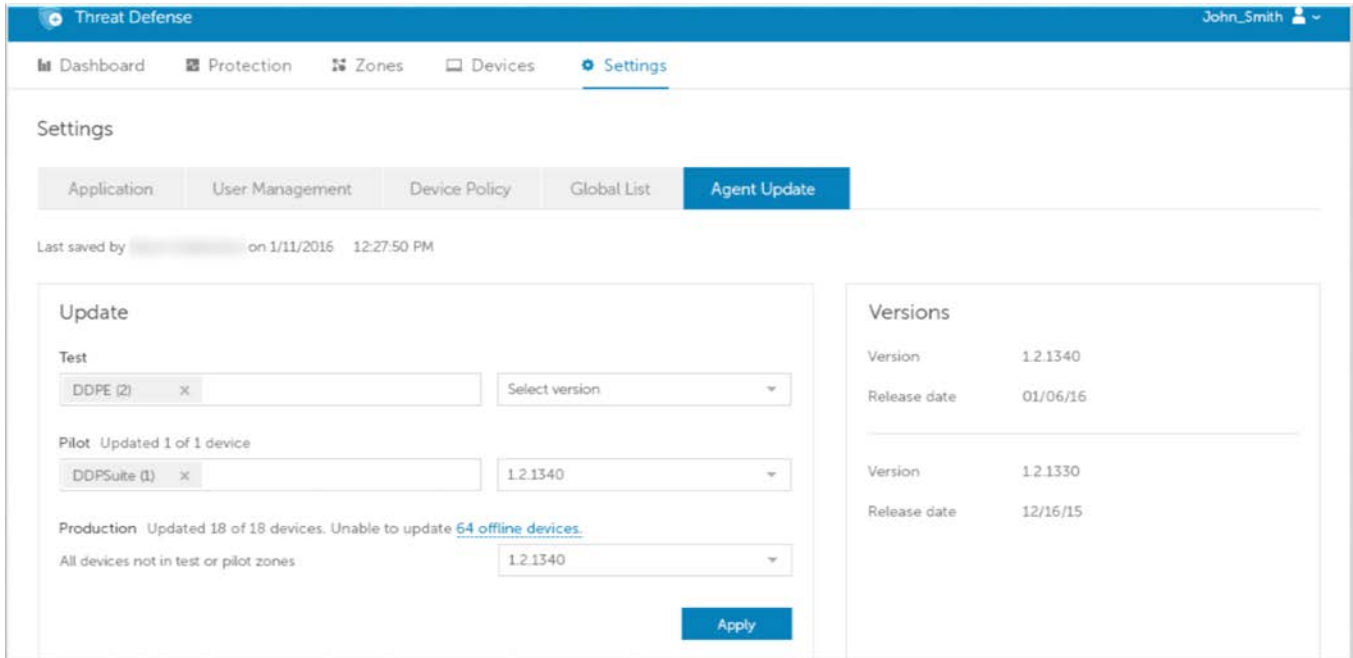


*Figure 13: Agent Updates*

### 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
```

# 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.

## *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 anti-virus sources.
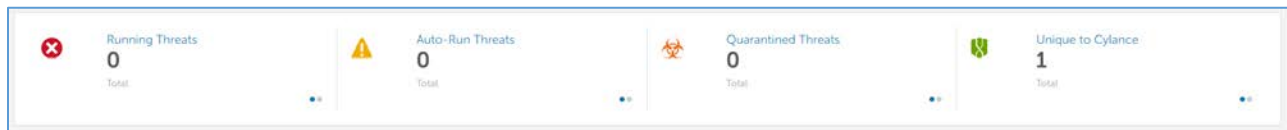


*Figure 14: Threat Statistics*

## *Protection Percentages*

Displays percentages for Threat Protection and Device Protection.

- **Threat Protection**: The percentage of threats which have had action taken (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*

Displays the total number of threats that require an action (*Quarantine*, *Global Quarantine*, *Waive*, and *Safe Lists*). 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.
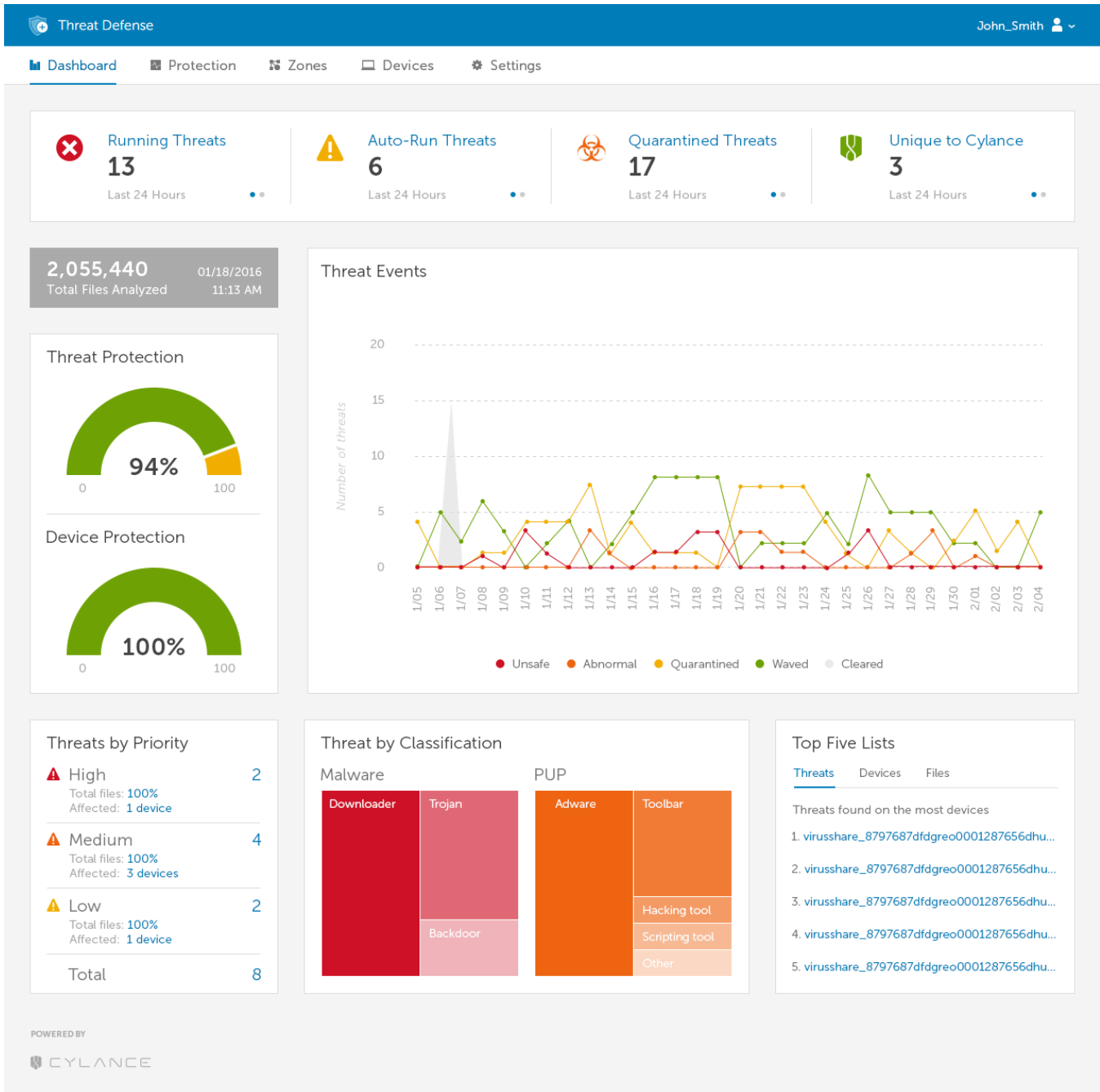


*Figure 15: Threat Defense Dashboard*

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.

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 been run previously.
- The file is set to auto run.
- The priority of the Zone where the threat was found.
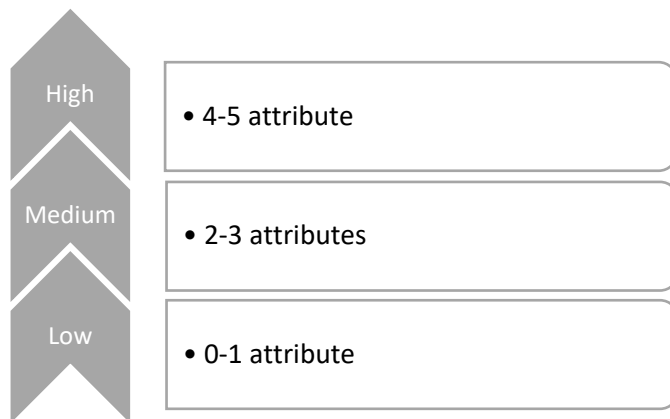


*Figure 16: Threat Classifications*

This classification helps Administrators determine which threats and devices to address first. Click either the threat or Device Number to view threat and Device details.

## 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.

# Protection – Threats

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 in order to further mitigate or respond to threats.

## File Type

**Unsafe**: A file with a score ranging from 60-100. An *Unsafe* file is one that the Threat Defense engine 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

A Cylance score is assigned to each file that is deemed *Abnormal* or *Unsafe*. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.

## Viewing Threat Information

The Protection tab on the Console displays detailed threat information, the Devices where the threats were found, and the actions taken on those Devices for those threats.

**Note**: The *Threat List* on the Protection tab 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.

### To View Threat Details
1. Login to the Console (http://dellthreatdefense.com).

2. Click the **Protection** tab to display a list of threats found in that organization.

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.
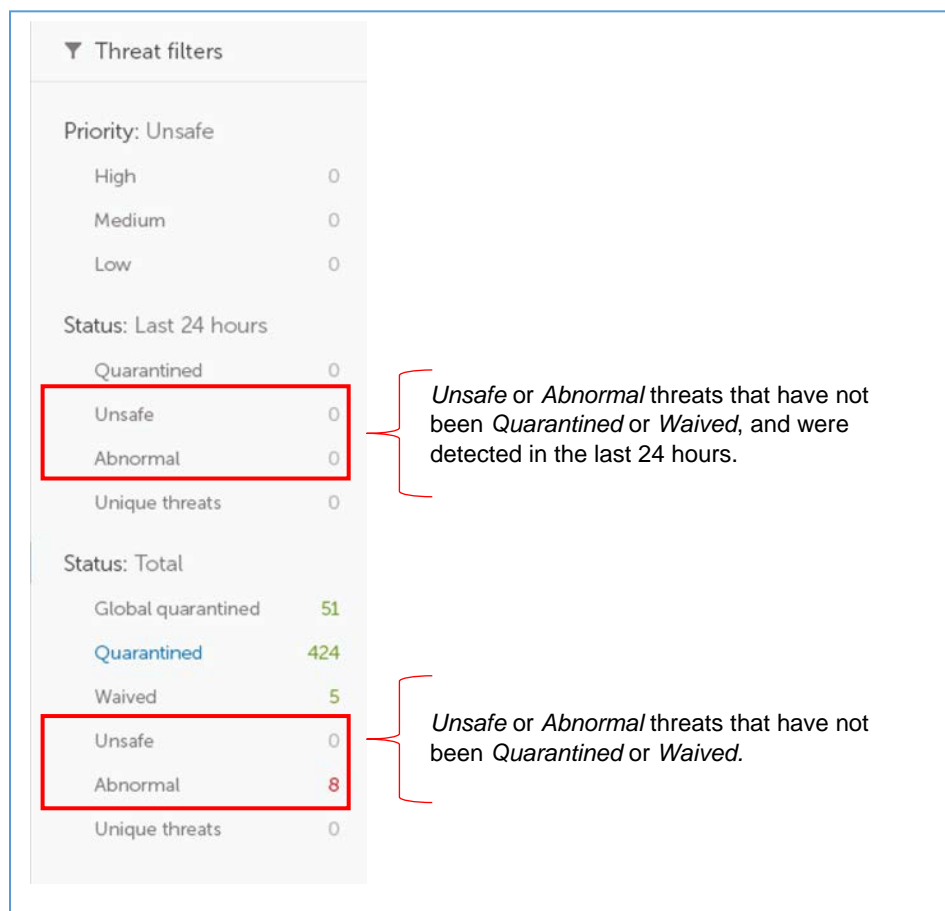


*Figure 17: Protection Page Threat Filters*

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 additional information on a specific threat, either click the threat name link (details display on a new page) or click anywhere in the threat's row (details display at the bottom of the page). Both views show the same content but have different presentation styles. The details include an overview of file metadata, a list of devices with the threat, and evidence reports.

    a. 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

b. 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.

c. Evidence Reports

- **Threat Indicators**: Observations about a file that the Cylance Infinity engine 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 that it attempted to communicate with.
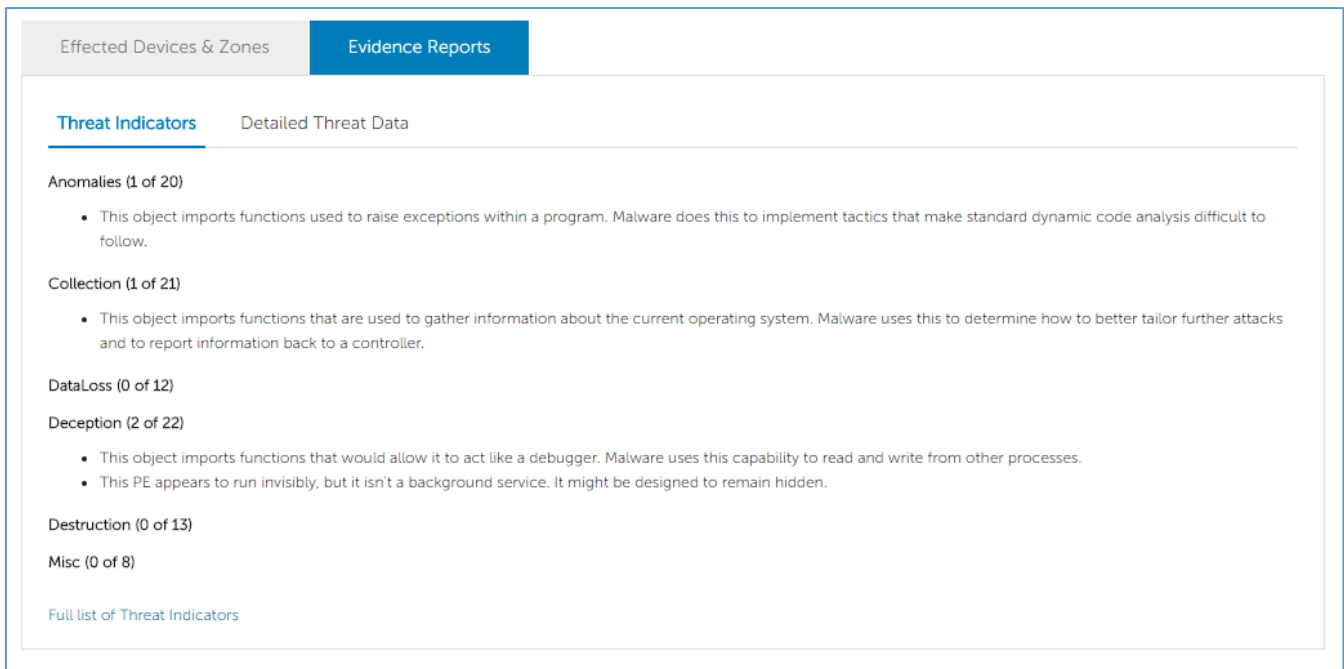


*Figure 18: Threat Indicators*

*Figure 19: Detailed Threat Data*

## To View Threat Indicators:

1. Login to the Console (http://dellthreatdefense.com).

2. Click **Protection** in the top menu to view a list of threats (or click **Devices**, then select a device).

3. Click the name of any threat. The Threat Details page displays.

4. Click **Evidence Reports**.

### *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*

The file has elements that are inconsistent or anomalous in some way. Frequently, they are inconsistencies in the structure of the file.

*Collection*

The file has evidence of data collection. This can include enumeration of device configuration or collection of sensitive information.

*Data Loss*

The file has evidence of data exfiltration. This can include outgoing network connections, evidence of acting as a browser, or other network communications.

*Deception*

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*

The file has evidence of destructive capabilities. Destruction includes the ability to delete device resources such as files and directories.

*Miscellaneous*

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.

## Addressing Threats

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

- *Quarantine*: *Quarantine* a specific file to prevent the file from being executed on that device.

  **Note**: You can quarantine a threat using the command-line on a device. This is available with the Windows Agent only. See Quarantine by Command-Line 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.

- *Global 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 to Cylance Infinity for analysis. If Auto-Upload is enabled, new files (ones that have not been analyzed by Cylance) are automatically uploaded to Cylance Infinity. If the file exists in Cylance Infinity, then the Upload File button is unavailable (greyed out).

- *Download File*: Download a file for your own testing purposes. This feature must be enabled for the organization. The user must be an Administrator. The threat must be detected using Agent version 1320 or higher.

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

## Address Threats on a Specific Device

1. Login to the Console (http://dellthreatdefense.com) as an Administrator or Zone Manager.

2. Click the **Devices** tab.

3. Search for and select the Device.

4. Alternately, a link to the device may be available from the Protection tab if it is listed with an associated threat.

5. All threats on that device are listed on the bottom of the page. Select the threat to either *Quarantine* or *Waive* the file on that device.



*Figure 20: Global Quarantine List*

## 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. Login to the Console (http://dellthreatdefense.com) as an Administrator.

2. Click **Settings > Global List**.

3. Click Global Quarantine or Safe.

4. Click **Add File**.

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

6. Click **Submit**.



*Figure 21: Global Quarantine List*



*Figure 22: Global Safe List*

# Protection – Script Control

Threat Defense provides details about Active and 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. Login to the Console (http://dellthreatdefense.com) as an Administrator.

2. Click Protection.

3. Click Script Control.

4. Select a script in the table. This updates the Details table with a list of affected devices.



*Figure 23: 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 the script was found on (example: Internal Hard Drive).

- **SHA256**: The SHA 256 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 script. Click device name to go to 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.

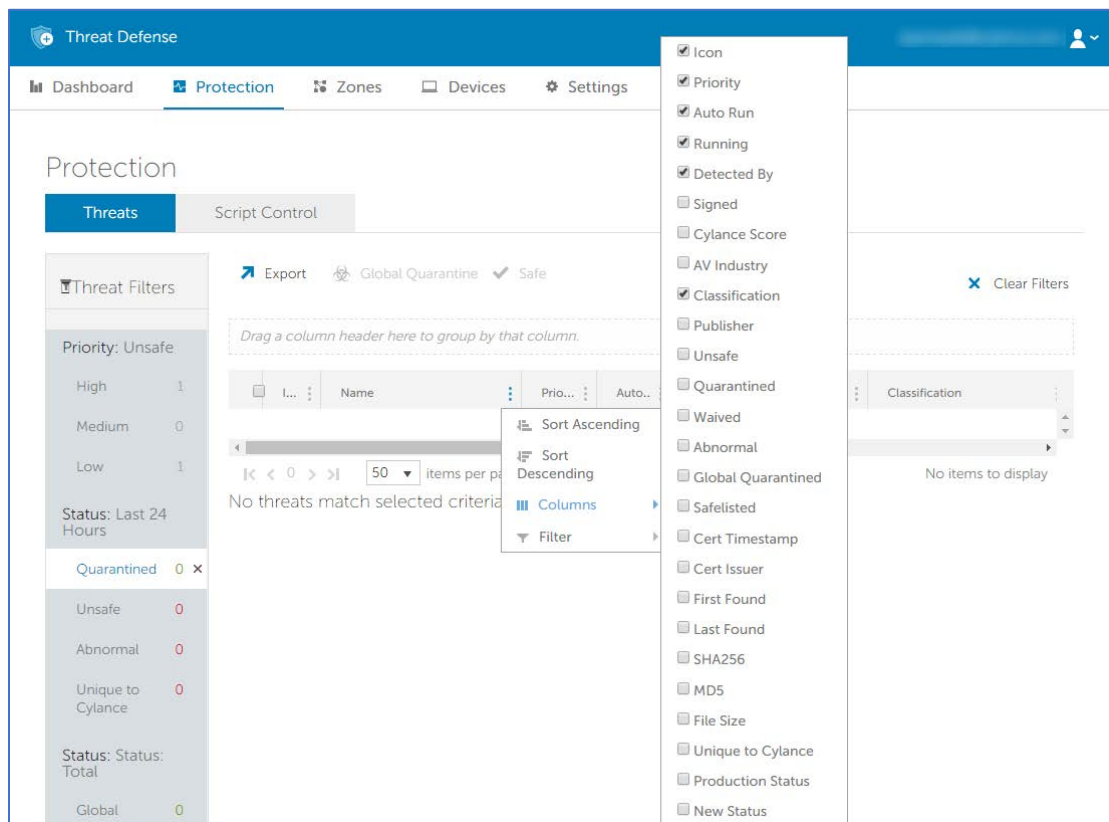- **Action**: The action take on the script (Alert or Block).



*Figure 24: Protection – Selecting Columns*

# Global List

*Global List* allows a file to be marked for *Quarantine* or to *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.

- **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. Login to the Console (http://dellthreatdefense.com) as an Administrator.

2. Select **Settings > Global List**.

3. Select the current list that the threat is assigned to. For example, click Unassigned to change an unassigned threat to either *Safe* or *Global Quarantine*.

4. Select the check boxes for the threats to change, and click a status button.

   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 to the *Unassigned List*.

### Add a File

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

1. Login to the Console (http://dellthreatdefense.com) as an Administrator.

2. Select **Settings > Global List**.

3. Select the list in which to add the file (*Global Quarantine* or *Safe*).

4. Click **Add File**.

5. Enter the SHA256 hash information. Optionally enter the MD5 and File Name information.

6. Enter a reason for adding this file.

7. Click **Submit**.

## Safe List by Certificate

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

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

- This functionality allows customers to establish a *White List*/*Safe List* by signed certificate which is represented by 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.

1. Add the certificate details to the Certificate Repository.

   a. Identify the certificate thumbprint for the signed Portable Executable (PE).

   b. Select **Settings > Certificates**.

   c. Click **Add Certificate**.

   d. Click either **Browse for certificates to add** or drag-and-drop the certificate to the message box.

   e. If browsing for the certificates, the Open window displays to allow selection of the certificates.

   f. Optionally add notes about this certificate.

   g. Click **Submit**. The Issuer, Subject, Thumbprint, and Notes (if entered) are added to the repository.

2. Add the Certificate to the *Safe List*.

   a. Select **Settings > Global List**.

   b. Select the **Safe** tab.

   c. Click **Certificates**.

   d. Click **Add Certificate**.

   e. Select a certificate from the *Safe List*. Optionally select a Category and add a reason for adding this certificate.
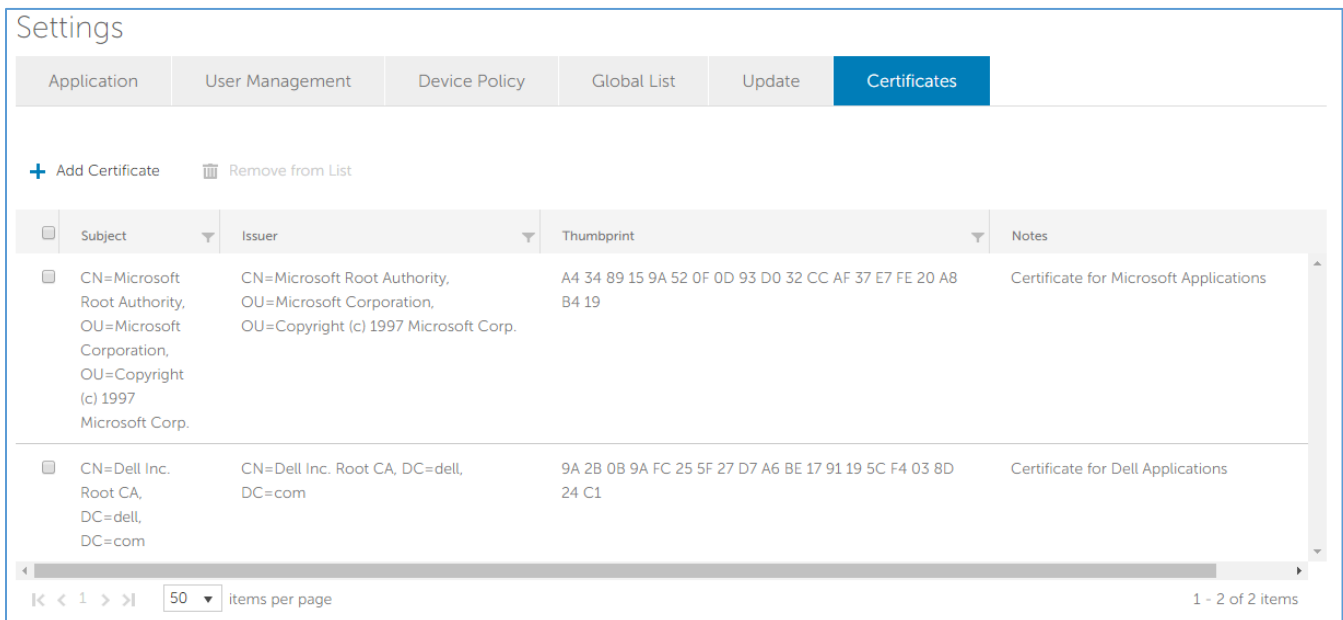
   f. Click **Submit**.



*Figure 25: 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**.

# Profile

The profile menu (upper-right corner) allows management of your account, Console audit logs to be viewed, and access to product help.

## My Account

Change your password and email notification setting on the My Account page.

1. Login to the Console (http://dellthreatdefense.com).

2. Click the profile menu in the upper-right corner, and select **My Account**.

3. To change your password:

    a. Click Change Password.

    b. Enter your old password.

    c. Enter your new password and 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.
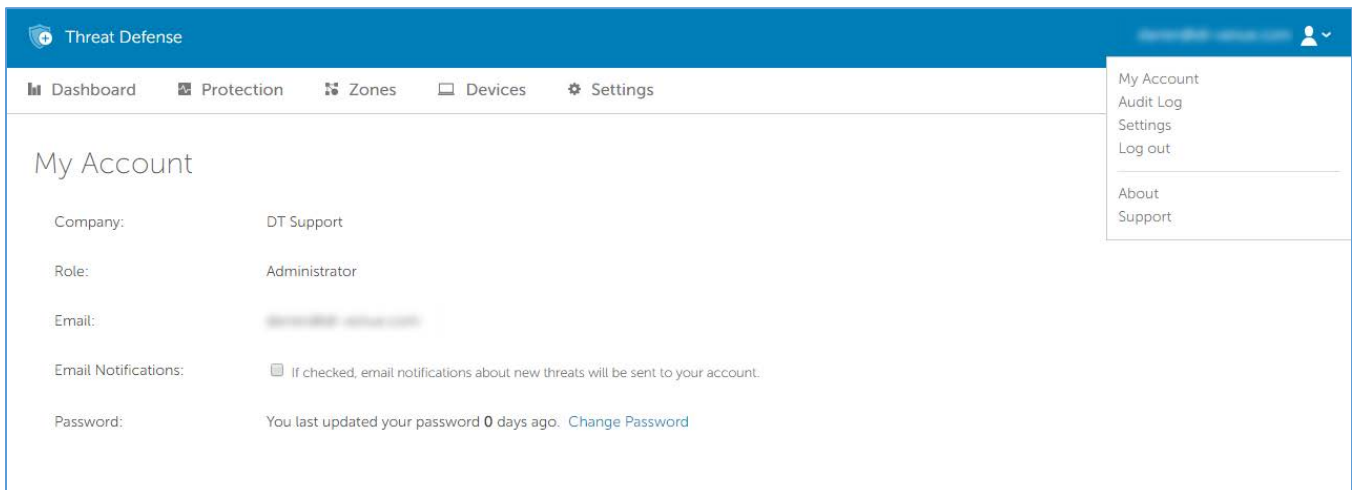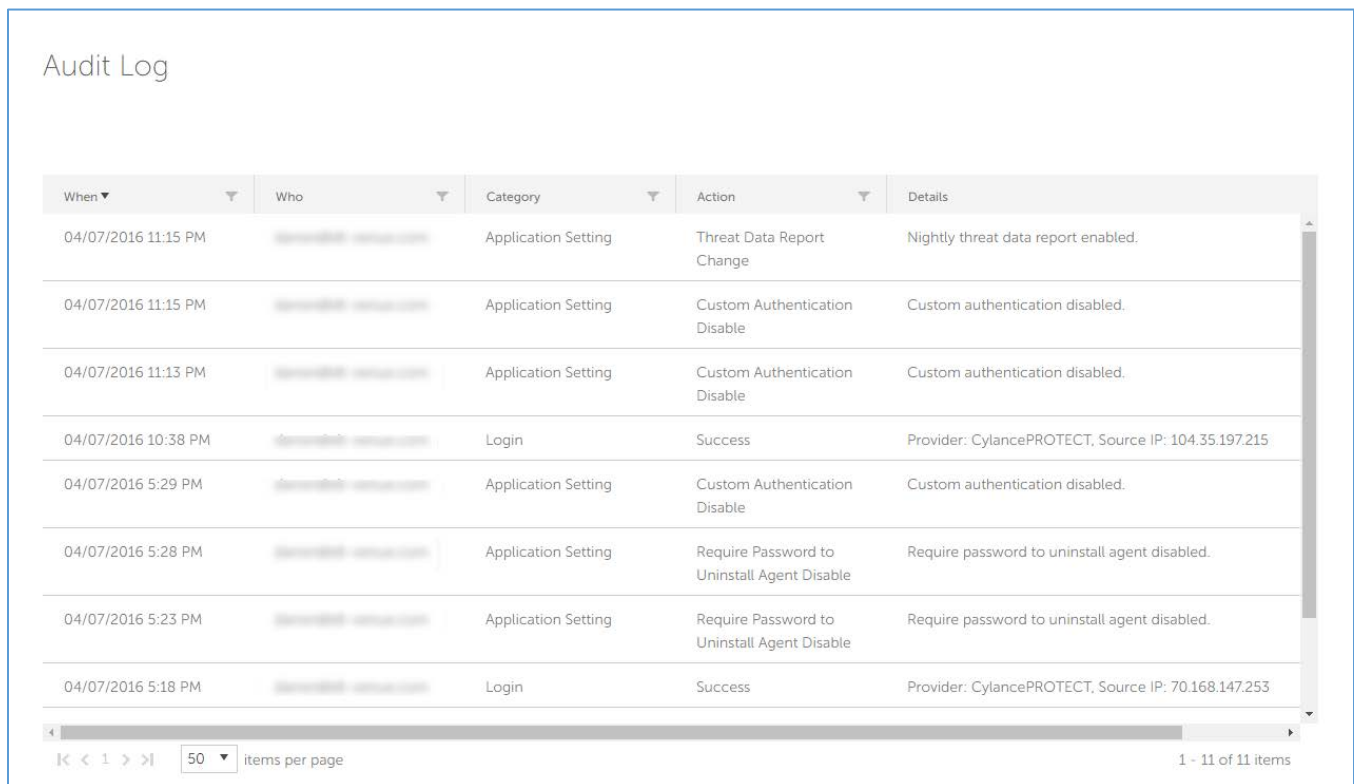


*Figure 26: My Account*

# Audit Logging

## *User Icon Dropdown list (upper right hand corner of Console)*

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 dropdown list on the upper right side of the Console, and selecting **Audit Log**. Audit logs are available for Administrators only.



*Figure 27: Audit Log*

# Settings

The Settings page displays the Application, User Management, Device Policy, Global List, and Agent Update tabs. The Settings menu item is available for Administrators only.

# APPLICATION

## Threat Defense Agent

Devices are added to the organization by installing the Threat Defense Agent on each endpoint. Once connected to the Console, apply policy (to manage identified threats) and organize the 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.

## 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).

| | |
|---|---|
| Operating Systems | • Windows 7 *(32-bit & 64-bit)*<br>• Windows Embedded Standard 7 *(32-bit)* and Windows Embedded Standard 7 Pro *(64-bit)*<br>• Windows 8 and 8.1 *(32-bit & 64-bit)**<br>• Windows 10 (*32-bit & 64-bit*)**<br>• Windows Server 2008 and 2008 R2 *(32-bit & 64-bit)***<br>• Windows Server 2012 and 2012 R2 *(64-bit)***<br>• Windows Server 2016 – Standard, Data Center and Essentials**** |
| RAM | • 2 GB |
| Available Hard Drive Space | • 300 MB |
| Additional Software/Requirements | • .NET Framework 3.5 (SP1) or higher (*Windows only*)<br>• Internet Browser<br>• Internet access to login, access the installer, and register the product<br>• Local administrator rights to install the software |
| Other Requirements | • TLS 1.2 is supported with Agent 1422 or higher, and requires .NET Framework 4.5 or higher |

*Table 2: System Requirements for Windows*

*Not Supported: Windows 8 RT
**Windows 10 Anniversary Update requires Agent 1402 or later.
***Not Supported: Server Core (2008 and 2012) and Minimal Server (2012).
****Requires Agent 1412 or later.

## *To Download the Install File*

1. Log in to the Console (http://dellthreatdefense.com).

2. Select **Settings > Application**.

3. 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. The Installation Token is required during installation, either in the installation wizard or as an installation parameter setting.

4. Download the Installer.

   a. Select the Operating System.

   b. Select the file type to download.

   For Windows, Dell recommends use of the MSI file for installation of the Agent.

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

## Install the Agent – Windows

Ensure that all prerequisites are met prior to installing Threat Defense. See System Requirements.

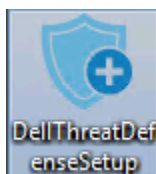1. Double-click DellThreatDefenseSetup.exe (or MSI) to begin the installation.



*Figure 28: Setup File for Windows*

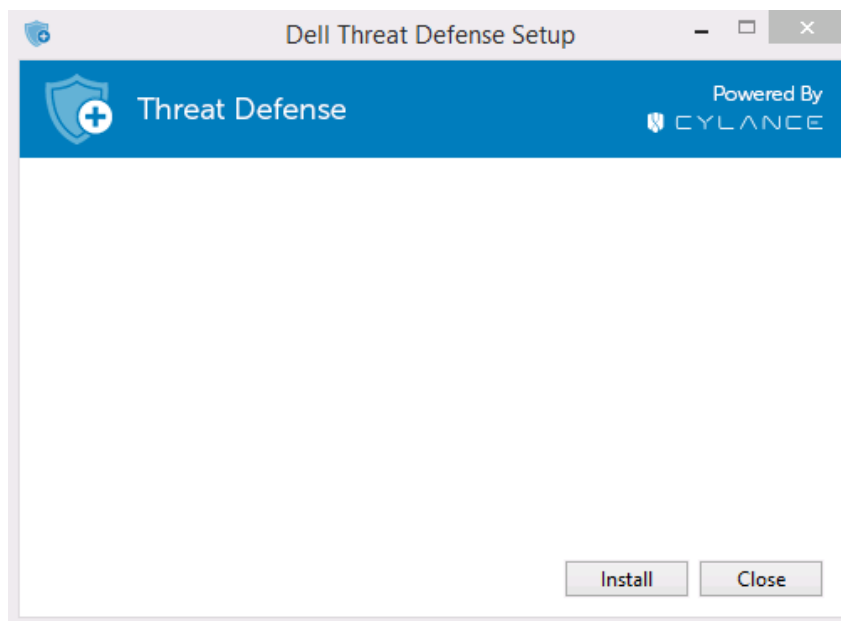2. Click **Install** at the Threat Defense setup window.



*Figure 29: Setup Window*

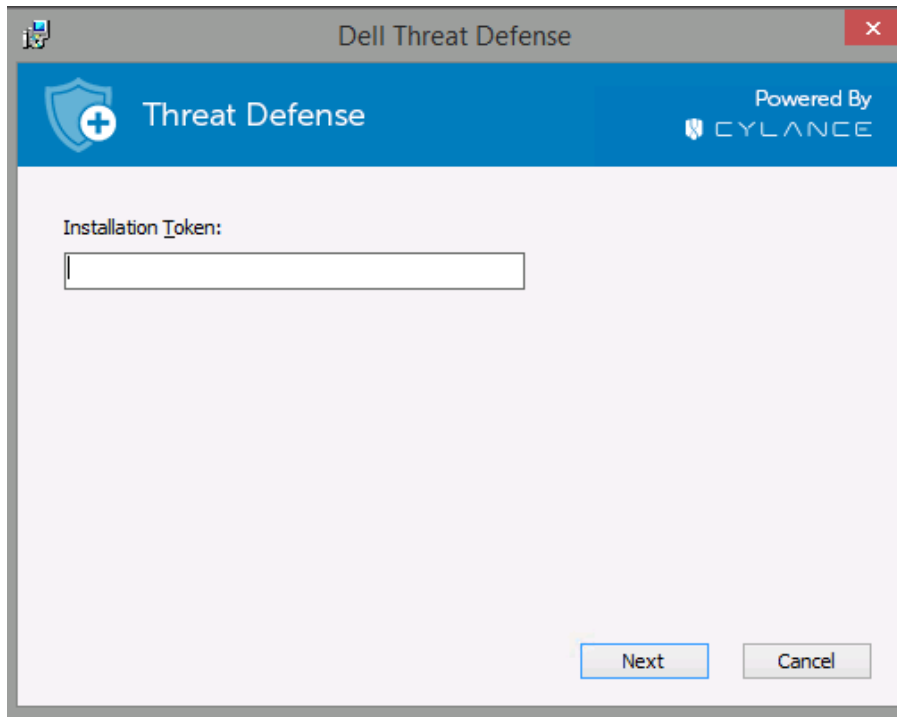3. Enter the Installation Token provided by the Threat Defense Tenant. Click **Next**.



*Figure 30: Installation Token Input Screen*

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

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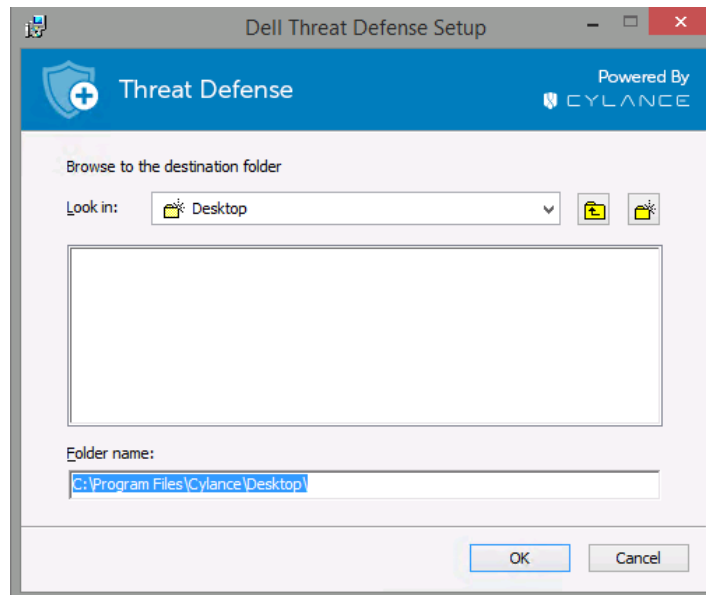
Click **OK** to begin the installation.



*Figure 31: Installation Location*

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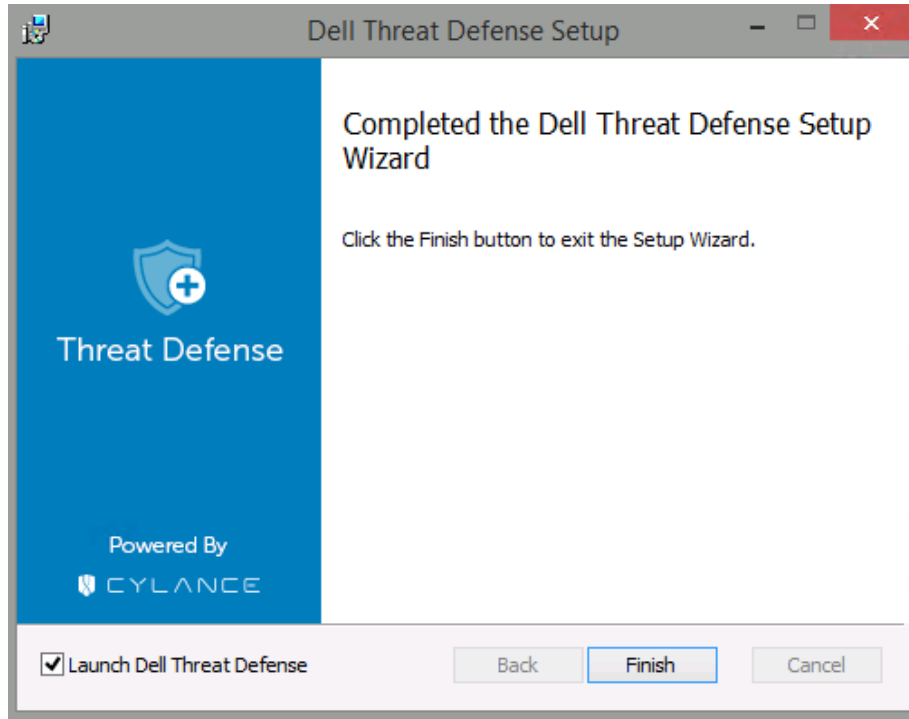


*Figure 32: Installation Complete*

## 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<br><br>1: The system tray icon and Start Menu folder are not hidden at run-time (default) |
| **SELFPROTECTIONLEVEL** | 1 or 2 | 1: Only Local Administrators can make changes to the registry and services<br><br>2: Only the System Administrator can make changes to the registry and services (default) |
| **APPFOLDER** | <Target Installation Folder> | Specifies the Agent installation directory<br><br>The default location is C:\Program Files\Cylance\Desktop |
| **VenueZone** | "Zone_Name" | Requires Agent version 1382 or higher<br><br>•Adds devices to a zone.<br><br>•If the zone does not exist, the zone is created using the name provided. |

| Property | Value | Description |
|---|---|---|
| | | •Replace zone_name with the name of an existing zone or a zone you want to create. |
| | | **Warning**: Adding spaces before or after the zone name will create a new zone. |

*Table 3: Installation Parameters for Windows*

The following command line example shows how to run the Microsoft Windows Installer Tool (MSIEXEC) passing it the PIDKEY, APPFOLDER, and LAUNCHAPP installation parameters:

```
msiexec /i DellThreatDefenseSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN>
LAUNCHAPP=0 /L*v C:\temp\install.log
```

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 in KB 227091.

## 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.

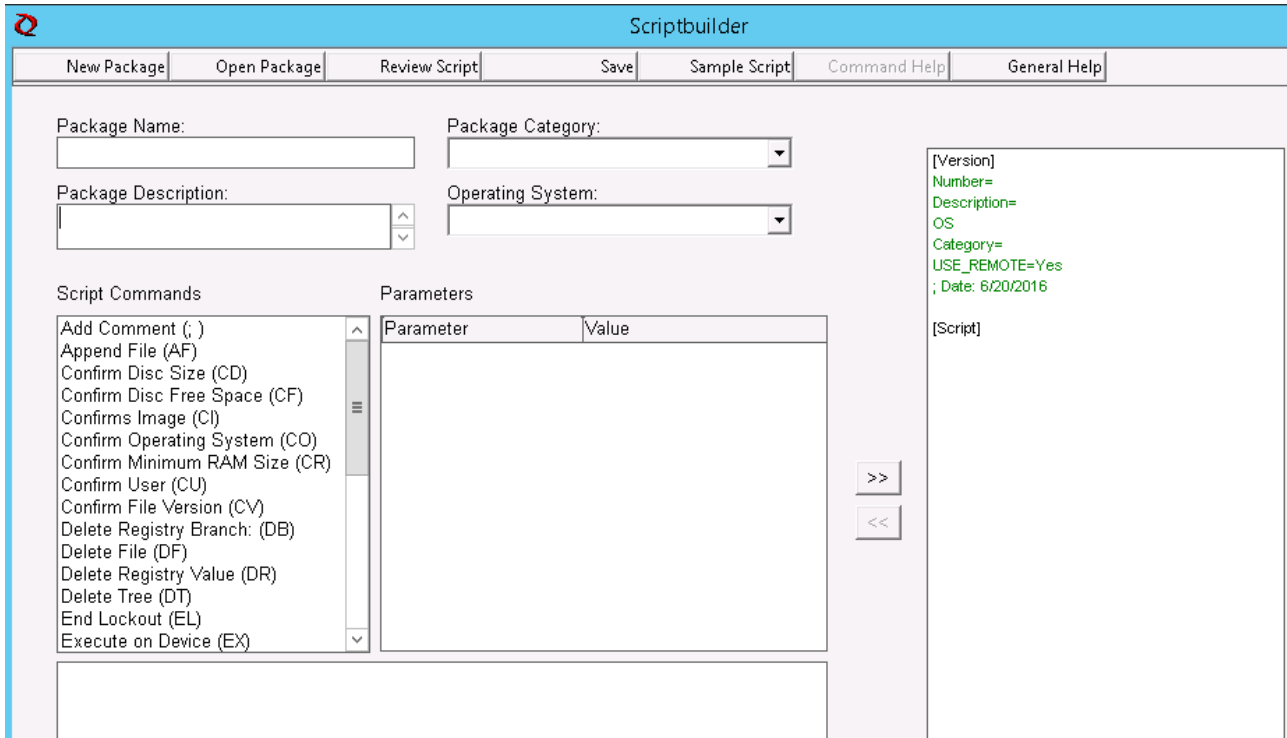3. Open Scriptbuilder on a computer that has WDM installed.



*Figure 33: Scriptbuilder*

4. Enter a Package Name and Package Description.

- Select Other Packages under Package Category.

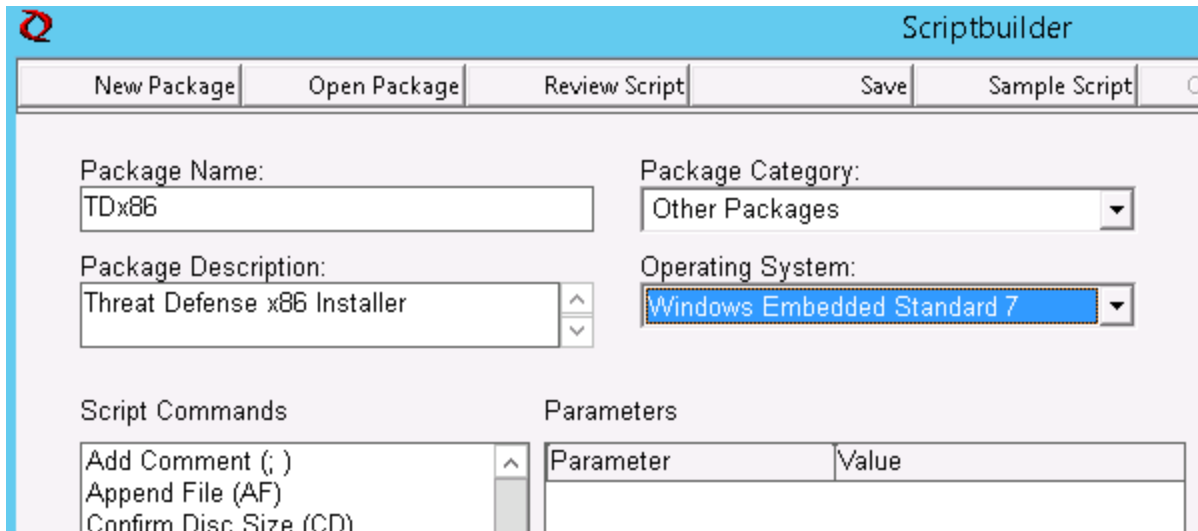- Select Windows Embedded Standard 7 under Operating System.



*Figure 34: Scriptbuilder fields*

5. Add Script Commands to verify target systems are WES7 or WES7p.

- Select Confirm Operating System (CO) under Script Command

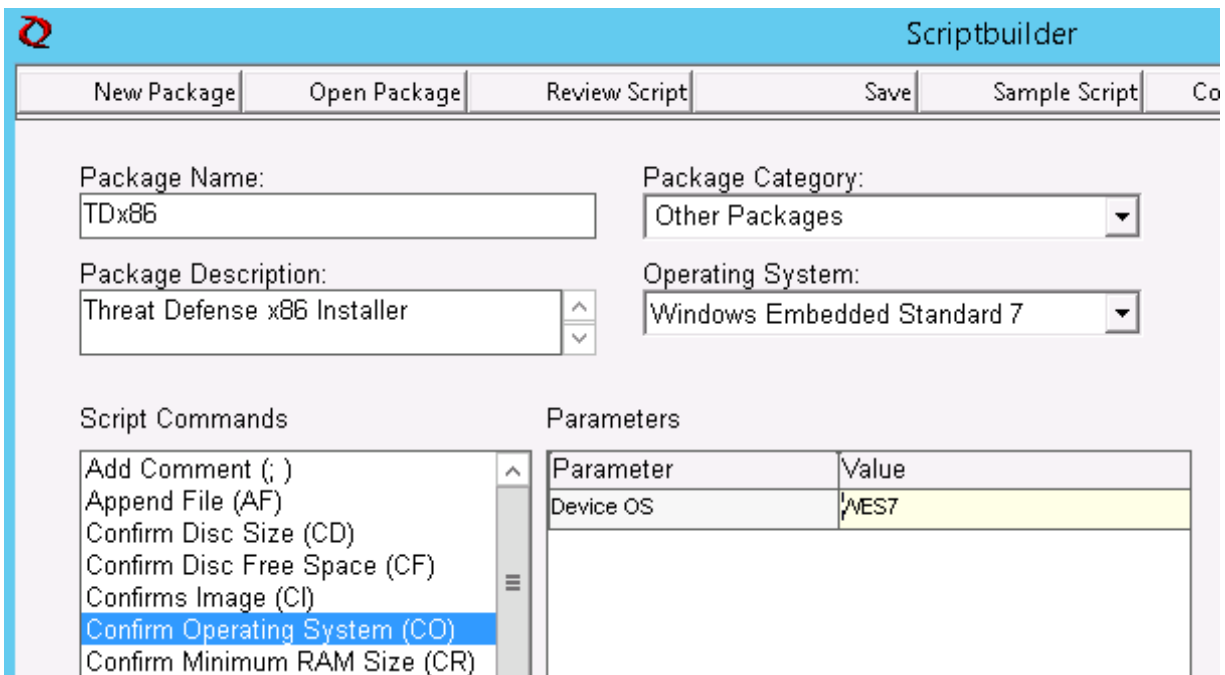- For the Device OS value, enter the appropriate operating system.



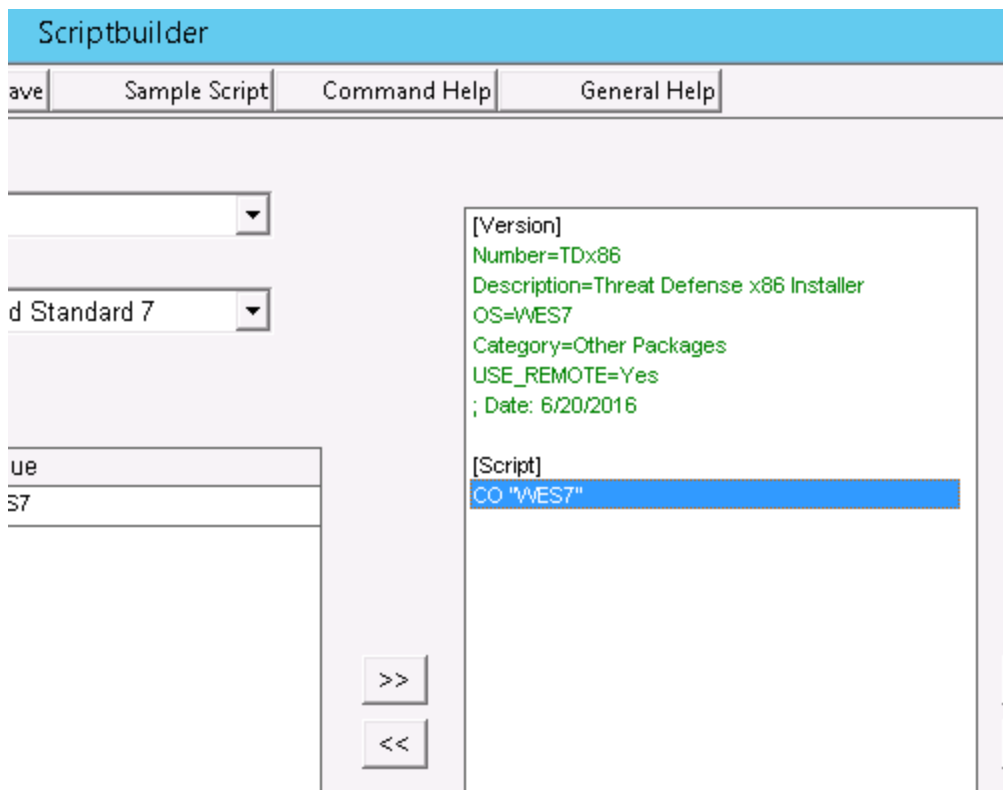*Figure 35: Scriptbuilder confirm OS*

6. Use the double arrows to Add Item.



*Figure 36: Scriptbuilder add item*
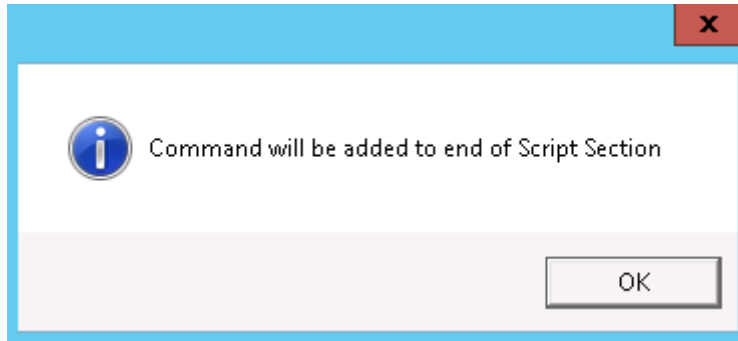
7. Press **OK** at the prompt.



*Figure 37: 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.



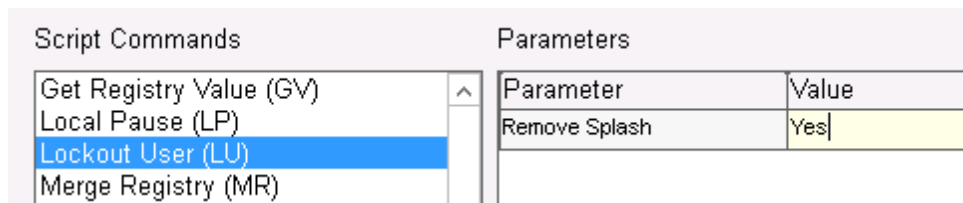*Figure 38: Script Commands*

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.
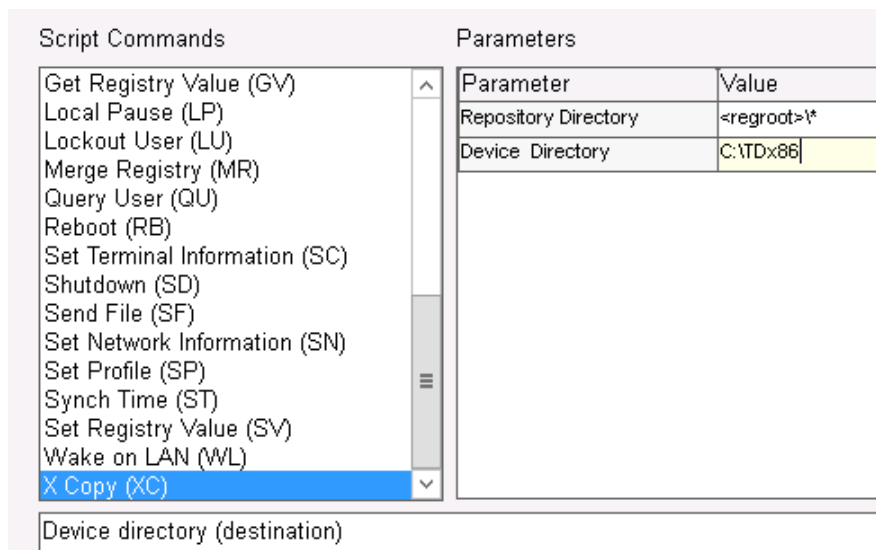


*Figure 39: Script Parameters*

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.
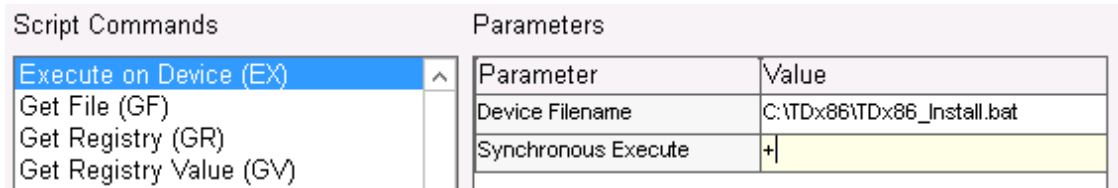


*Figure 40: Script Parameters*

11. Add command to delete files copied from thin client.

12. Add Script Command Delete **Tree (DT)**.
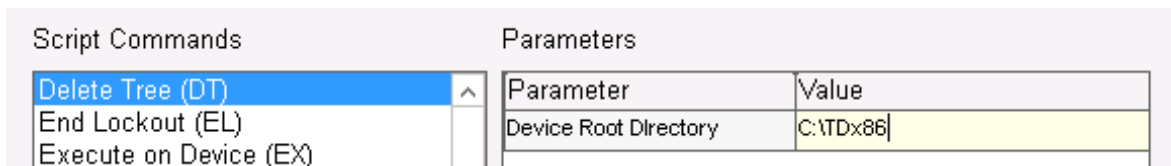


*Figure 41: Script Parameters*

12. Add commands to disable lock out.

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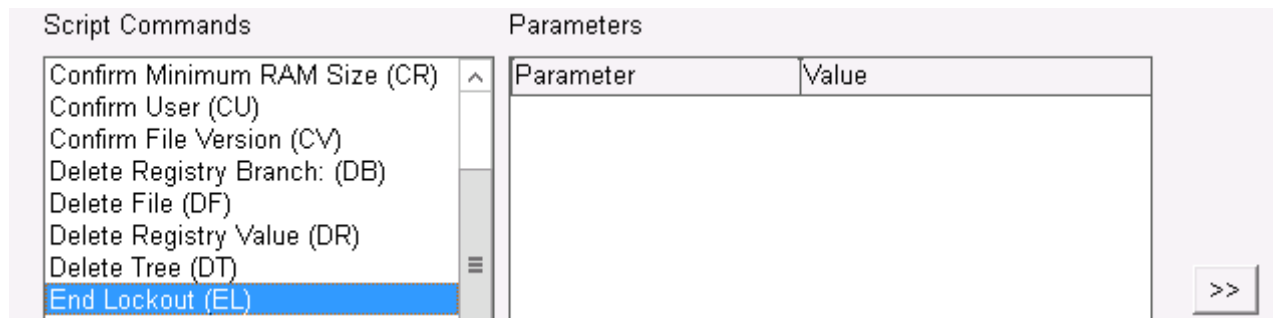


*Figure 42: Script Parameters*

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



*Figure 43: Script Review*

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



*Figure 44: Script Review*

14. Save the package.

> 14. Click **Save** and browse to the location of the **TDx86** folder, if these instructions have been followed, the folder is on the Desktop.
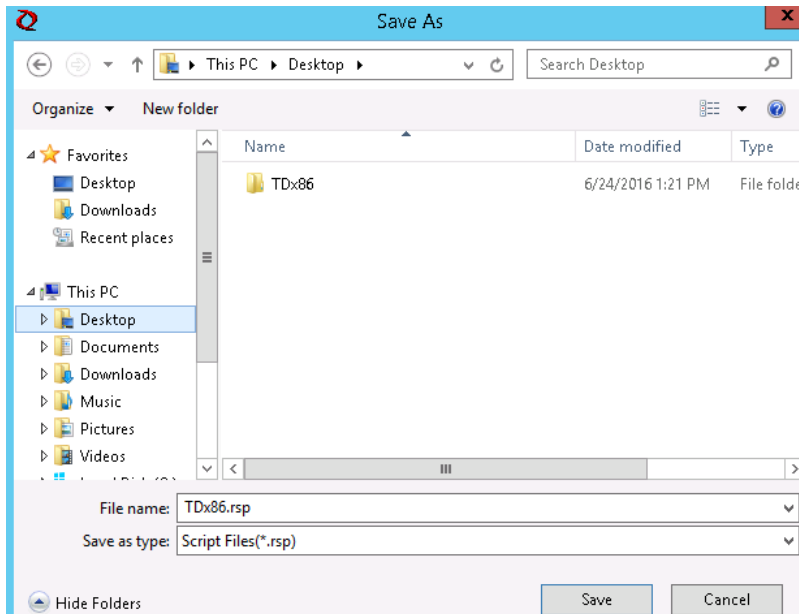


*Figure 45: Save Location*

15. Close Scriptbuilder.

16. Launch **WyseDeviceManager** to add the package to WDM.

17. Browse to **WyseDeviceManager > Package Manager > Other Packages**.
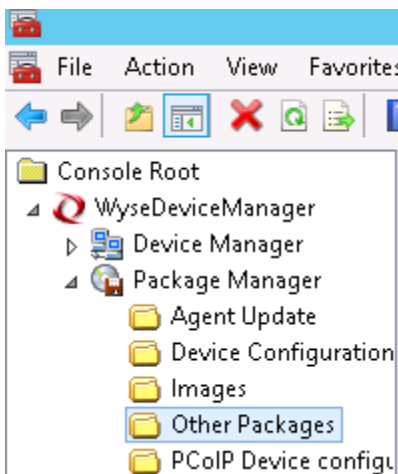


*Figure 46: WyseDeviceManager*

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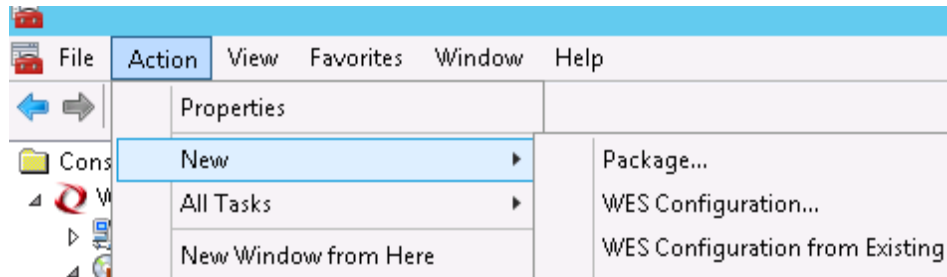


*Figure 47: Menu bar*

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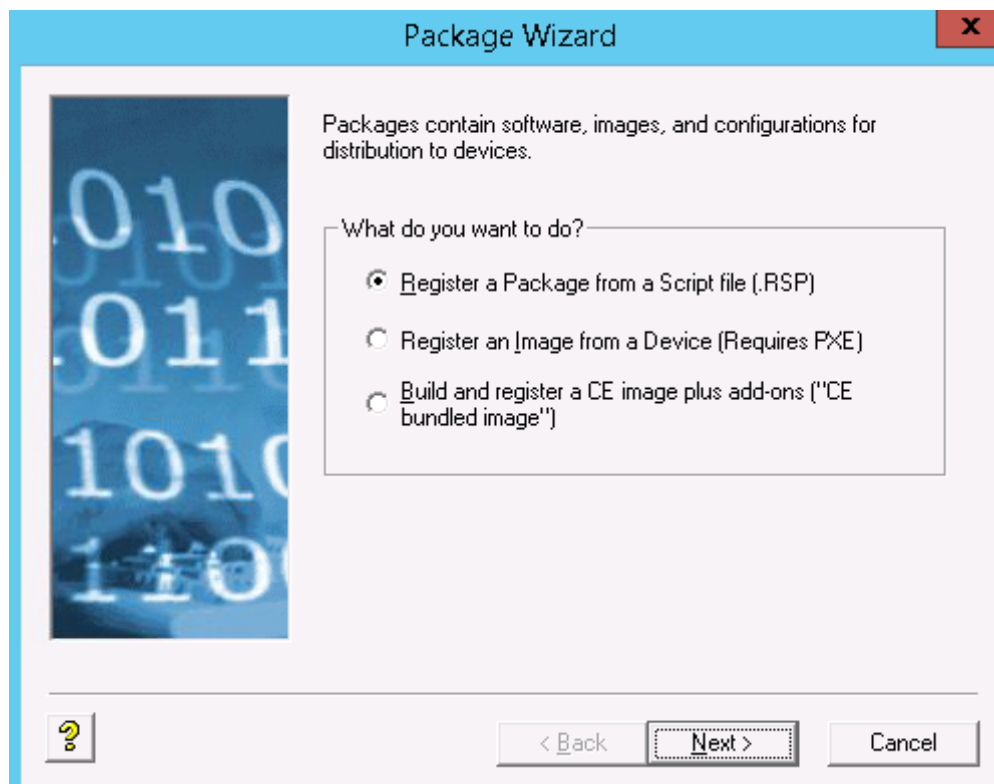


*Figure 48: Package wizard*

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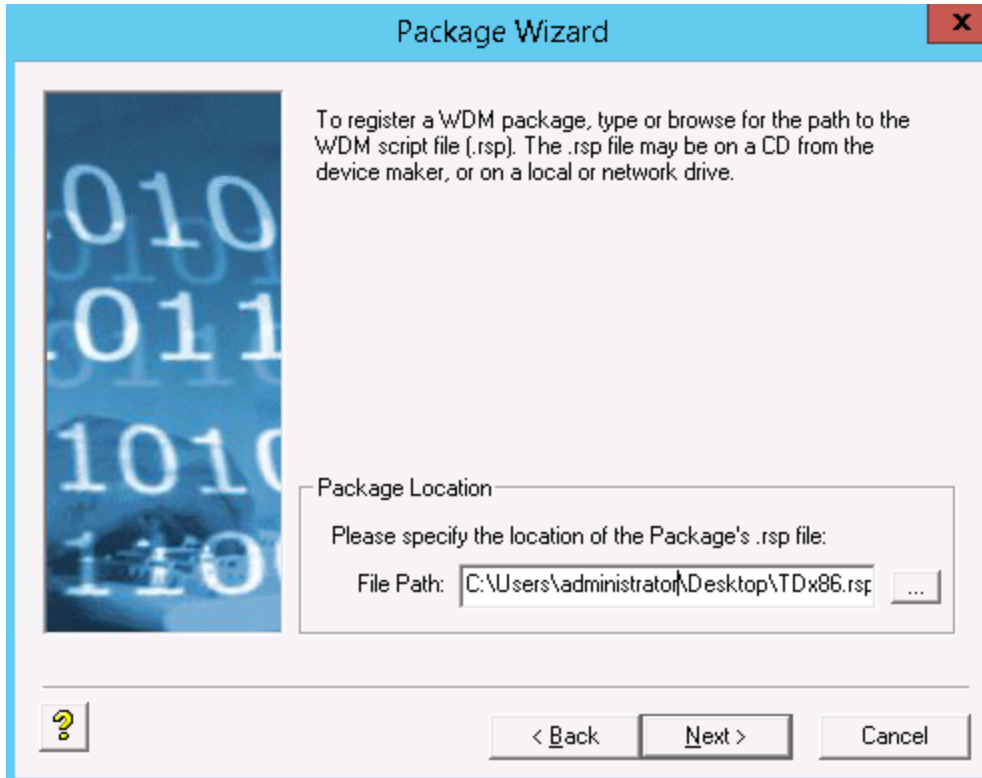


*Figure 49: Location of .RSP file*

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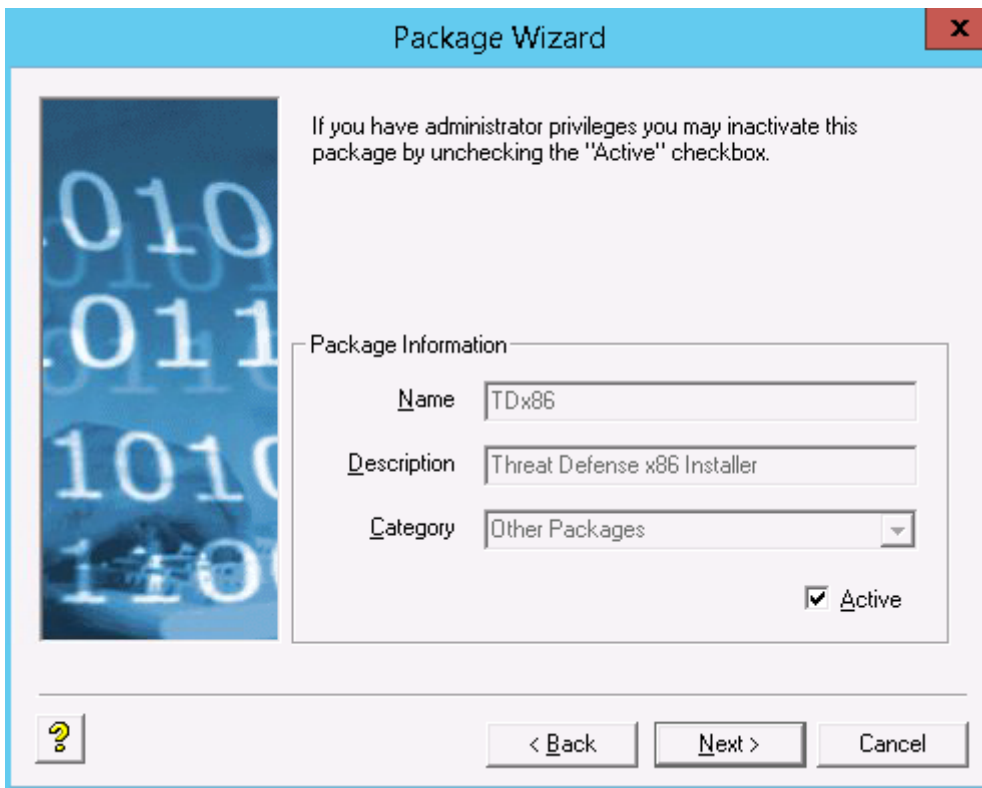


*Figure 50: Package information*

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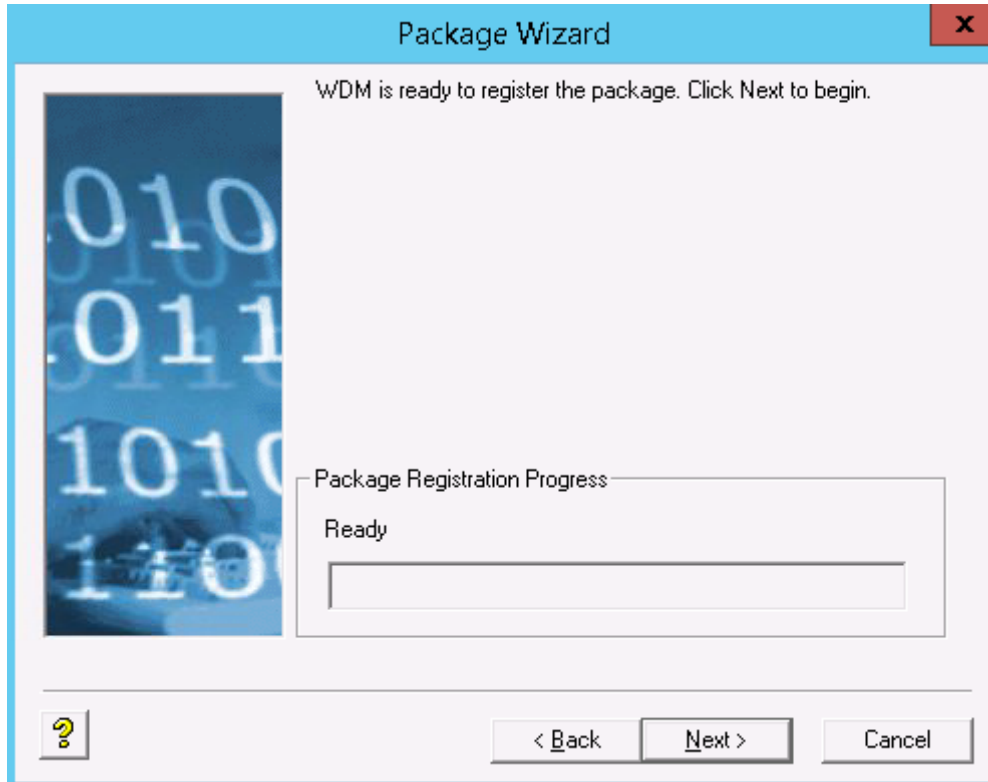


*Figure 51: Ready to register the package*

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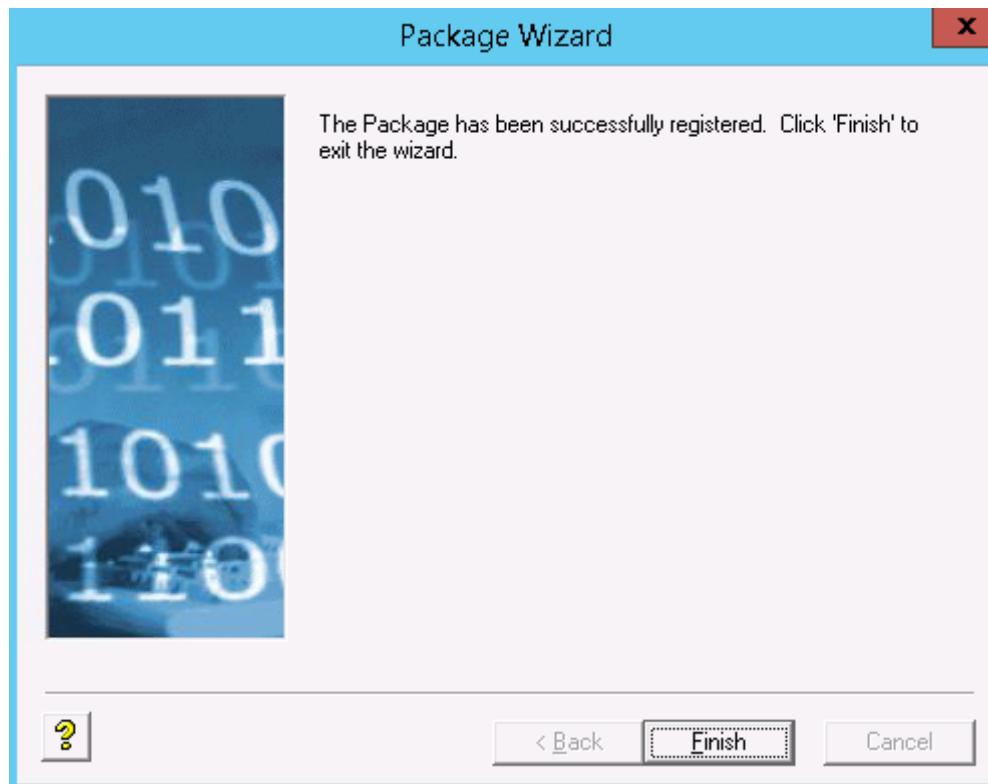


*Figure 52: Finish wizard*

24. The package will be visible in **Other Packages**.
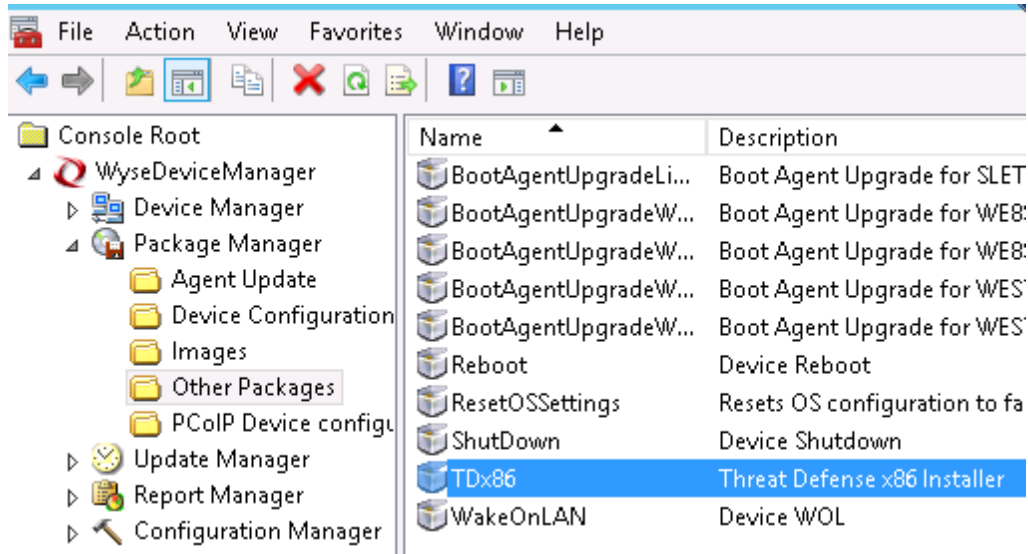


*Figure 53: Location of package*

25. Verify package contents:

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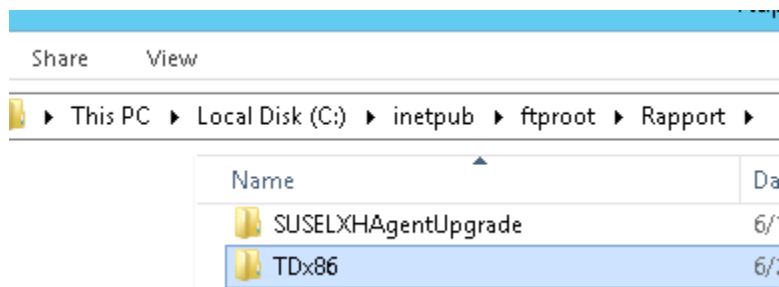


*Figure 54: Inetpub location of package*

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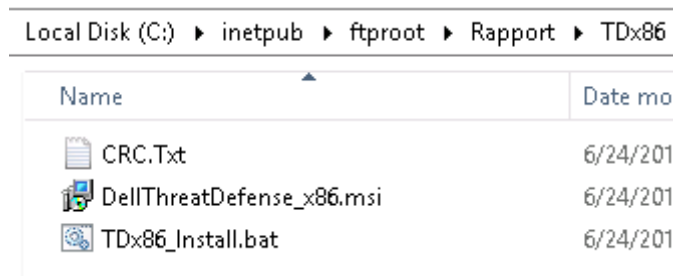


*Figure 55: Inetpub location of installer*

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.
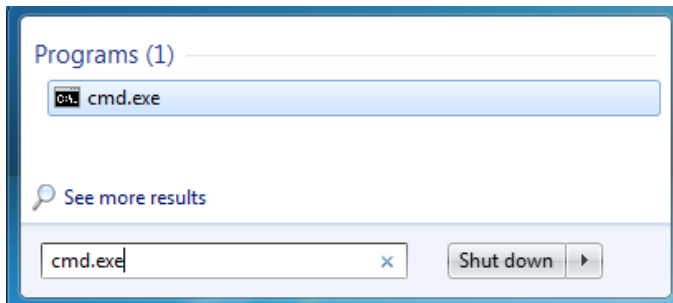


*Figure 56: Search for cmd.exe*

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:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```
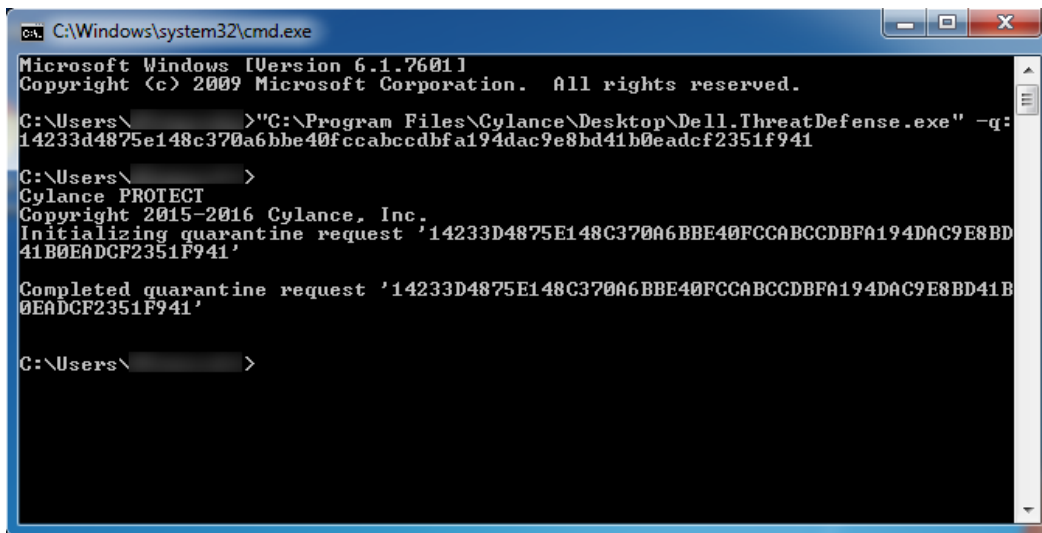


*Figure 57: Quarantine a file by SHA256 hash*

# Mac OS X 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).

| | |
|---|---|
| Operating Systems | • Mac OS X 10.9<br>• Mac OS X 10.10<br>• Mac OS X 10.11<br>• macOS 10.12* |
| RAM | • 2 GB |
| Available Hard Drive Space | • 300 MB |

*Table 4: System Requirements for Mac OS X*

*Requires Agent 1412 or later.

### *To Download the Install File*

1. Log in to the Console (http://dellthreatdefense.com).

2. Select **Settings > Application**.

3. 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. The Installation Token is required during installation, either in the installation wizard or as an installation parameter setting.

4. Download the Installer.

   a. Select the Operating System.

   b. Select the file type to download.

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

## Install the Agent – Mac OS X

Ensure that all prerequisites are met prior to installing Threat Defense. See System Requirements.

**Note:** The Mac OS X Agent will be Dell branded in a future release.

1. Double-click **DellThreatDefense.dmg** to mount the installer.

2. Double-click the *Protect* icon from the PROTECT user interface to begin the installation.

*Figure 58: Setup File for Mac OS X*

3. Click **Continue** to verify that the Operating System and Hardware meet the requirements.
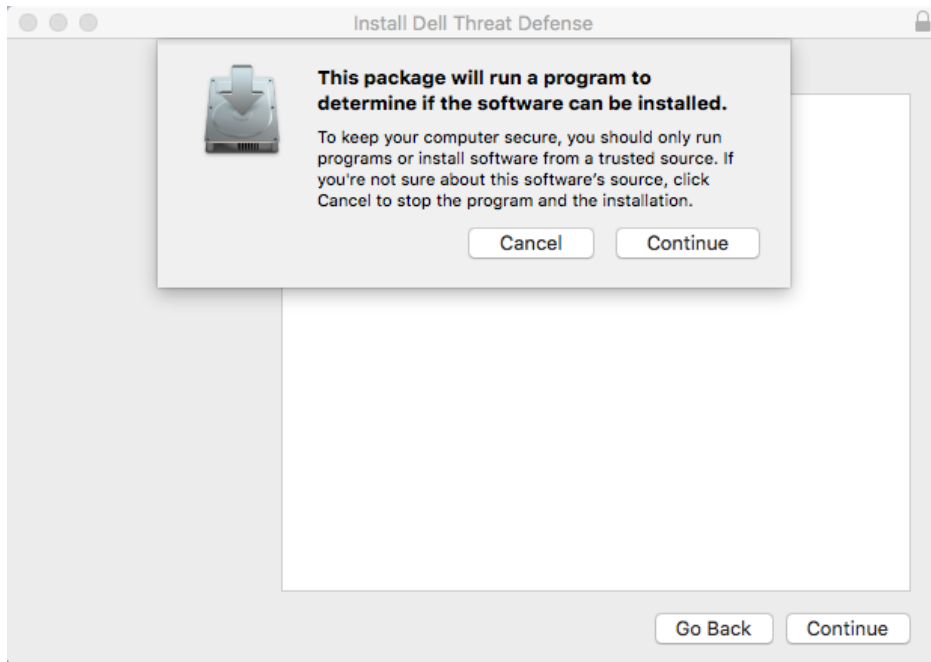


*Figure 59: Operating System and Hardware Check*

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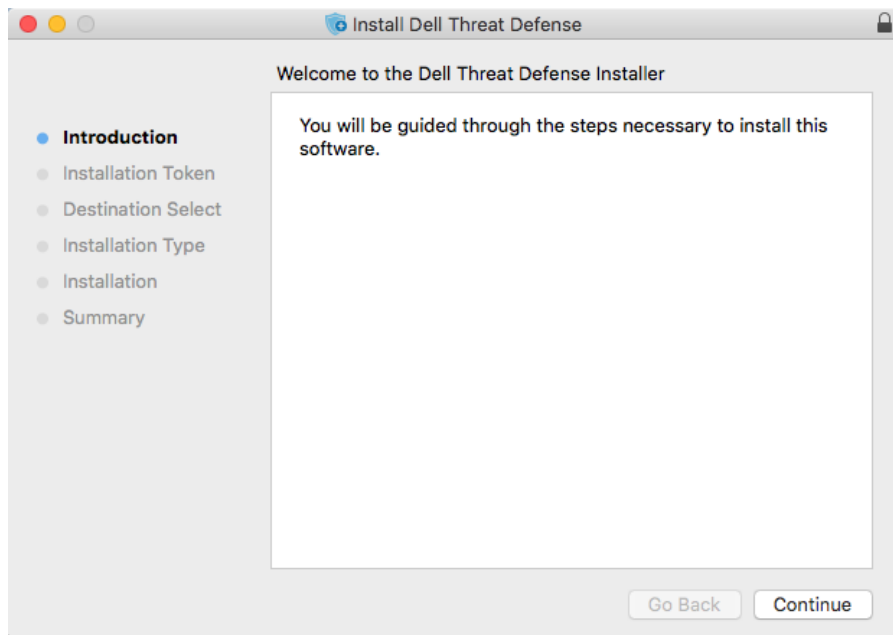


*Figure 60: Introduction Screen*

5.  Enter the Installation Token provided by the Threat Defense Tenant. Click **Continue**.
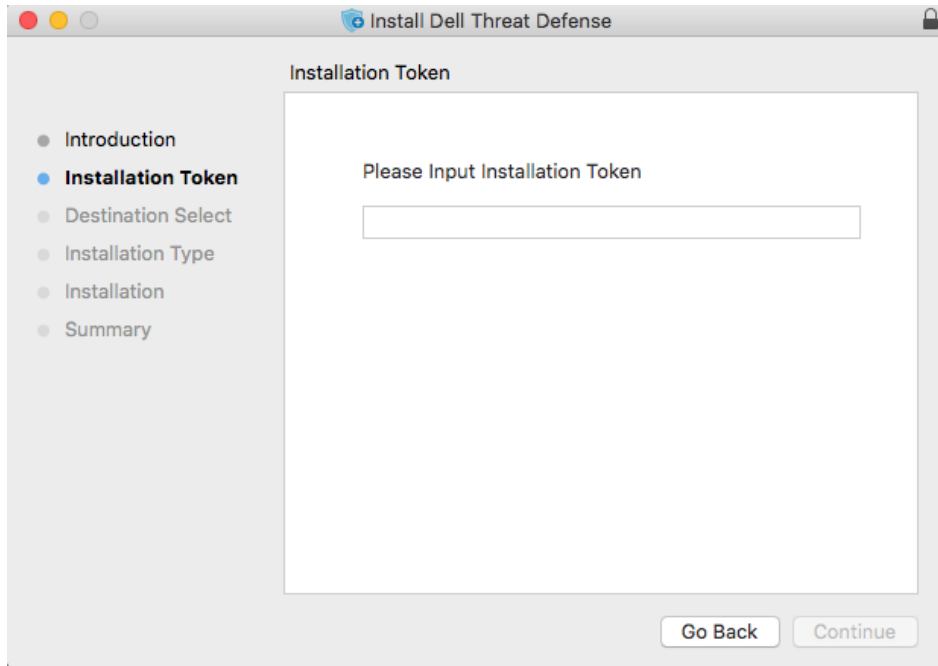


*Figure 61: Installation Token Input Screen*

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

6.  Optionally change the installation location of Threat Defense.

Click **Install** to begin the installation.
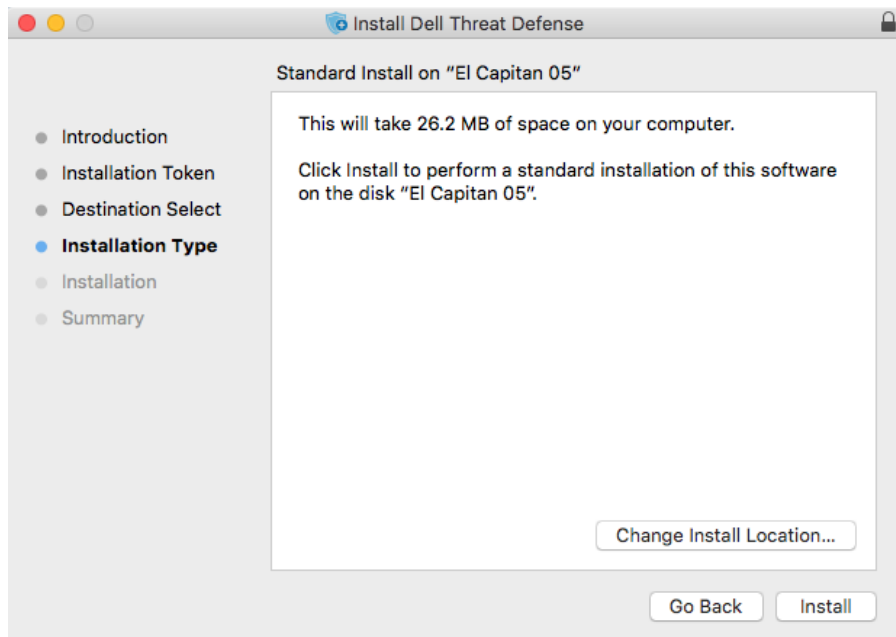


*Figure 62: Installation Type Screen*

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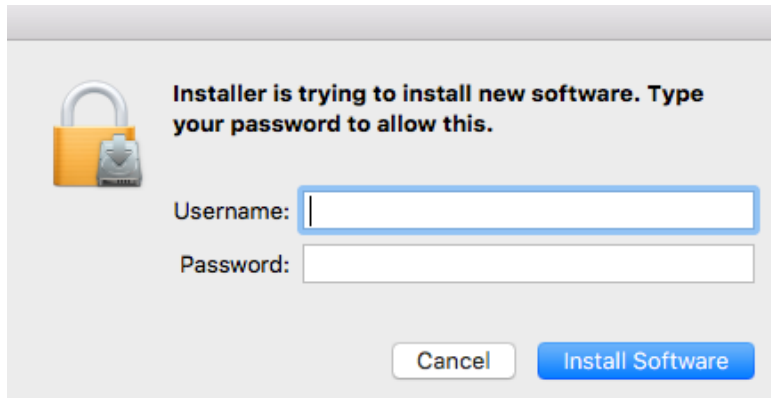


*Figure 63: Input Credentials Screen*

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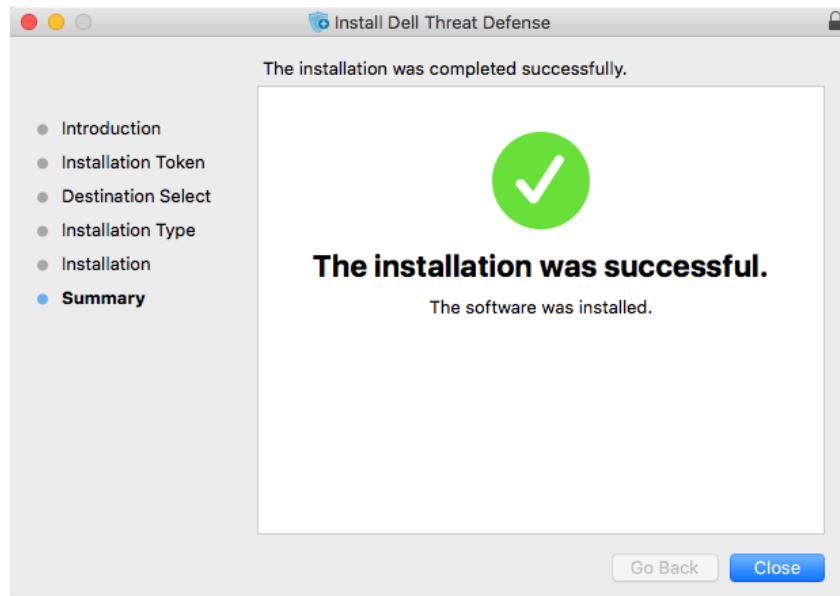


*Figure 64: Installation Complete Screen*

# Mac OSX Installation Parameters

The Threat Defense Agent can be installed using command line options in Terminal. The examples below use the PKG installer. For 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 available in the Console |
| **NoCylanceUI** | | The Agent icon should not display on startup. The default is Visible |
| **SelfProtectionLevel** | 0 or 1 | 1: Only Local Administrators can make changes to the registry and services. |

| Property | Value | Description |
|---|---|---|
| | | 2: Only the System Administrator can make changes to the registry and services (default). |
| 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 on Verbose during troubleshooting and then changing it back to Information when troubleshooting is complete. |
| VenueZone | "zone_name" | Requires Agent version 1382 or higher |
| | | •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. |
| | | **Warning**: Adding spaces before or after the zone name will create a new zone. |

*Table 5: Installation Parameters for Mac OS X*

## Install the 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/
```

**Note**: 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 Mac OSX and 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/
```

## Uninstall the Agent

**Without Password**

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

**With Password**

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

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

# 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
```

## *Installation Verification*

Check the following files to verify successful Agent installation.

1. The program folder was created.

   - Windows default: **C:\Program Files\Cylance\Desktop**

   - Mac OS X default: **/Applications/DellThreatDefense/**

2. The Threat Defense icon is visible in the system tray of the target device.

   This does not apply if parameter LAUNCHAPP=0 (Windows) or NoCylanceUI (Mac OS X) 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 (Windows) or NoCylanceUI (Mac OS X) 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.

## 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.
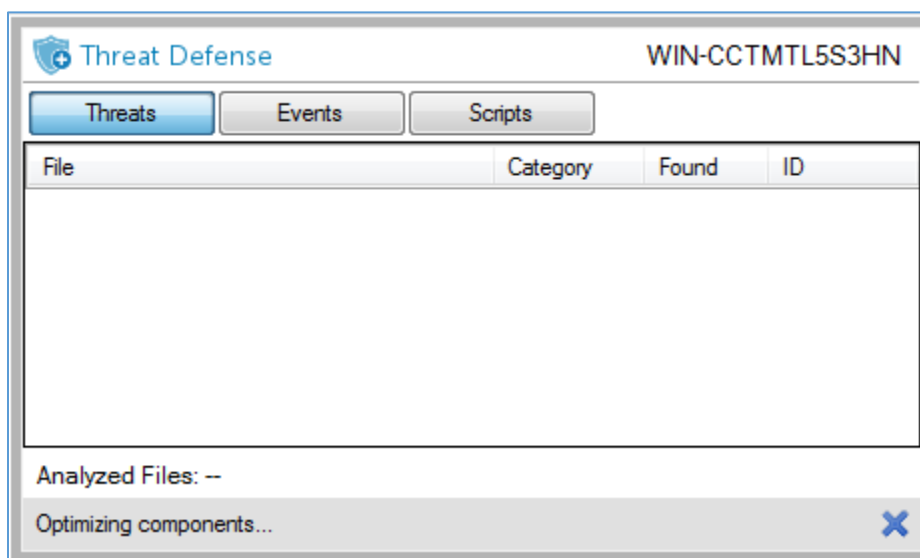


*Figure 65: Agent User Interface*

## 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 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 provides access to help and updates for Threat Defense. Access is also provided to the Advanced User Interface that provides more menu options.

## *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 the device belongs to.

- **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 installation token used during installation.

- **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.
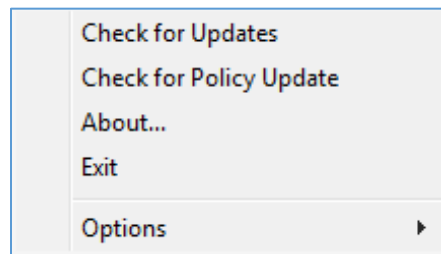


*Figure 66: Agent Menu*

## 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, 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.
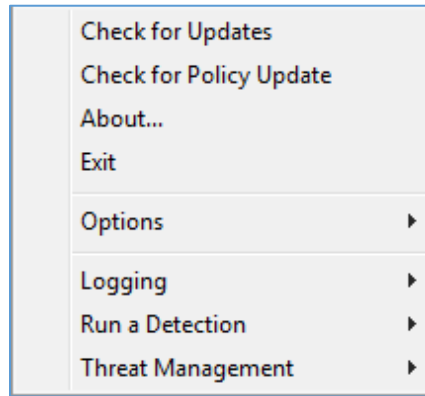
*Figure 67: Agent Advanced User Interface Options*

### Mac OSX/macOS

1. If the Agent icon is visible in the top menu, right-click the icon and select **Exit**.

2. Open terminal and run

    a. Sudo
       /Applications/DellThreatDefense/DellThreatDefense.app/Contents/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. Dell recommends setting 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 and 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.

When creating a virtual machine image to be used as a template, disconnect the virtual machine network settings before installing the Agent. This prevents the Agent from communicating with the Console and configuring the Device Details. This prevents duplicate devices in the Console.

# Password-Protected Uninstall

*SETTINGS > Application*

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

- If the MSI installer was used to install, either uninstall using the MSI or use the Control Panel.

- If the EXE installer was used to install, use the EXE to uninstall. Using the Control Panel does not work if the EXE installer was used and a password is required to uninstall.

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

## To Create an Uninstall Password

1. Login to the Console (http://dellthreatdefense.com) with an Administrator account.
2. Select **Settings > Application**.
3. Select the check box to **Require Password to Uninstall Agent**.
4. Enter a password.
5. Click **Save**.
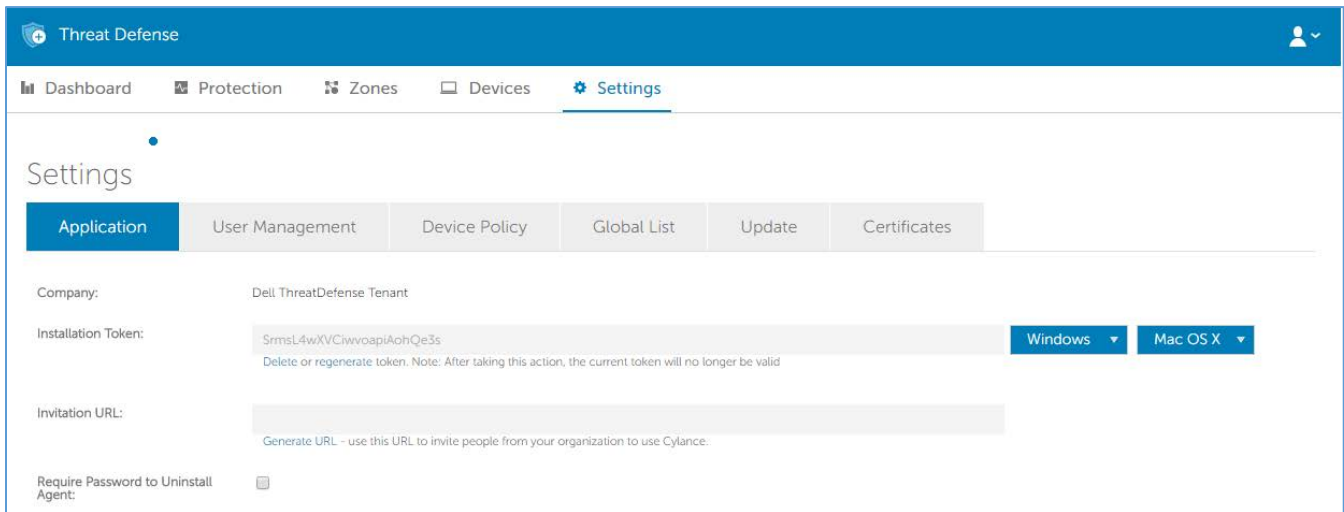


*Figure 68: Configure Password-Protected Uninstall*

# Integrations

The Threat Defense Console provides integration with some third party programs.

## Syslog/SIEM

Threat Defense can integrate with Security Information Event Management (SIEM) software using the Syslog feature. Syslog events are persisted at the same time the Agent events are persisted to the Console.

For the latest IP addresses for Syslog messages, contact Dell Support.



*Figure 69: Configure Syslog/SIEM*

## *Event Types*

### *Audit Log*
Select this option to send the audit log of user actions performed in the Console (website) to the Syslog server. Audit log events always display in the Audit Log screen, even when this option is de-selected.

*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: (johnsmith@contoso.com)
```

### Devices

Select this option to send device events to the Syslog server.

- When a new device is registered, two messages for this event are received: Registration and SystemSecurity.

  *Example Message for Device Registered Event*

  ```
  Threat Defense: Event Type: Device, Event Name: Registration, Device Name: WIN-
  55NATVQHBUU

  Threat Defense: Event Type: Device, Event Name: SystemSecurity, Device Name: WIN-
  55NATVQHBUU, Agent Version: 1.1.1270.58, IP Address: (10.3.0.154), MAC Address:
  (005056881877), Logged On Users: (WIN-55NATVQHBUU\Administrator), OS: Microsoft
  Windows Server 2008 R2 Standard Service Pack 1 x64 6.1.7601
  ```

- When a device is removed.

  *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: 'WIN-55NATVQHBUU' to 'WIN-2008R2-IRV1'; Policy Changed: 'Default' to
  'IRVPolicy1'; Zones Added: 'IRV1', User: John Smith (johnsmith@contoso.com)
  ```

### Threats

Select this option to 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: ▓▓▓▓▓▓-
1, IP Address: (▓▓.▓.▓.▓▓▓), 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

Hundreds of threats are classified each day as either Malware or Potentially Unwanted Programs (PUPs). If this option is selected, you subscribe 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:
1218493137321C1D1F897B0C25BEF17CDD0BE9C99B84B4DD8B51EAC8F9794F65
```

### SIEM (Security Information and Event Management)

Specifies the type of Syslog server or SIEM that events are to be sent to.

### Protocol

This must match what is configured on your Syslog server. The choices are UDP or TCP. UDP is generally not recommended as it does not guarantee message delivery. Dell recommends TCP (default).

### 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. Dell encourages customers to select this option. Ensure that the 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 the customer has setup. Consult with your internal network experts to ensure firewall and domain settings are properly configured.

### Port

Specifies the port number on the devices that the Syslog server listens 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 display in the Syslog server. This is a subjective field, and it may set to whatever level preferred. 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 valid values are entered, after a couple of moments, a *success* confirmation displays.

# Custom Authentication
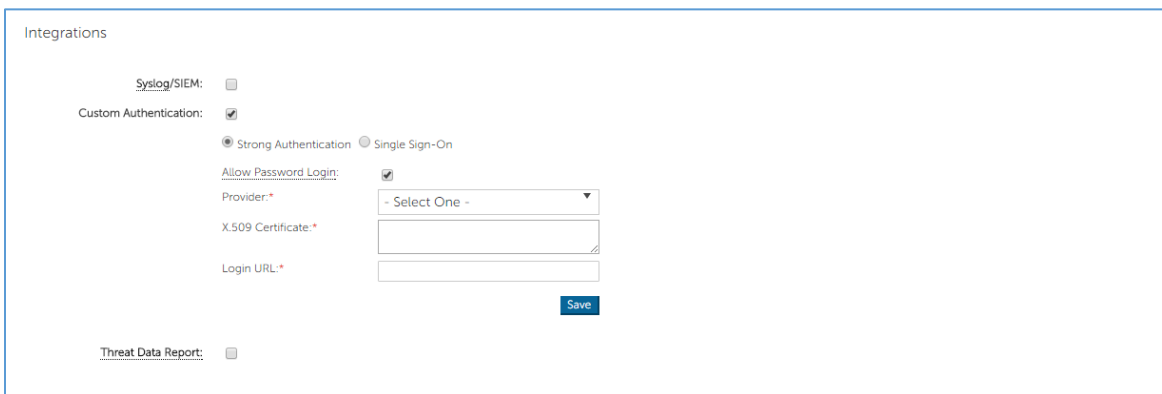
Use external Identity Providers (IdP) to log in to the Console. This requires configuring settings with your IdP to obtain an X.509 certificate and a URL for verifying your IdP login. Custom Authentication works with Microsoft SAML 2.0. This feature has been confirmed to work with OneLogin, OKTA, Microsoft Azure, and PingOne. This feature also provides a Custom setting and should work with other Identity Providers who follow Microsoft SAML 2.0.

**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**: A selection of 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**: Select this option to allow login to the Console directly, using SSO. This allows SSO setting tests without being locked out of the Console. Once successfully logged into the Console using SSO, Dell recommends that this feature is disabled.

- **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.



*Figure 70: Configure Custom Authentication*

# Threat Data Report

A spreadsheet that contains 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 a Threat Defense Agent installed. This information includes Device Name, Operating System Version, Agent Version, and Policy applied.

- **Threat Indicators**: Lists each threat and the associated threat characteristics.

- **Cleared**: Lists all files that have been *Cleared* in the organization. This information includes files that were *Waived*, added to the *Safe List*, or *Deleted* from the *Quarantine* folder on a device.

- **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.

When this feature is enabled, the report is automatically updated at 1:00AM Pacific Standard Time (PST). Click **Regenerate Report** to manually generate an update.

The Threat Data Report provides a URL and token that can be used to download the report without requiring a login to the Console. A token can also be deleted or regenerated, as needed, which allows control over who has access to the report.
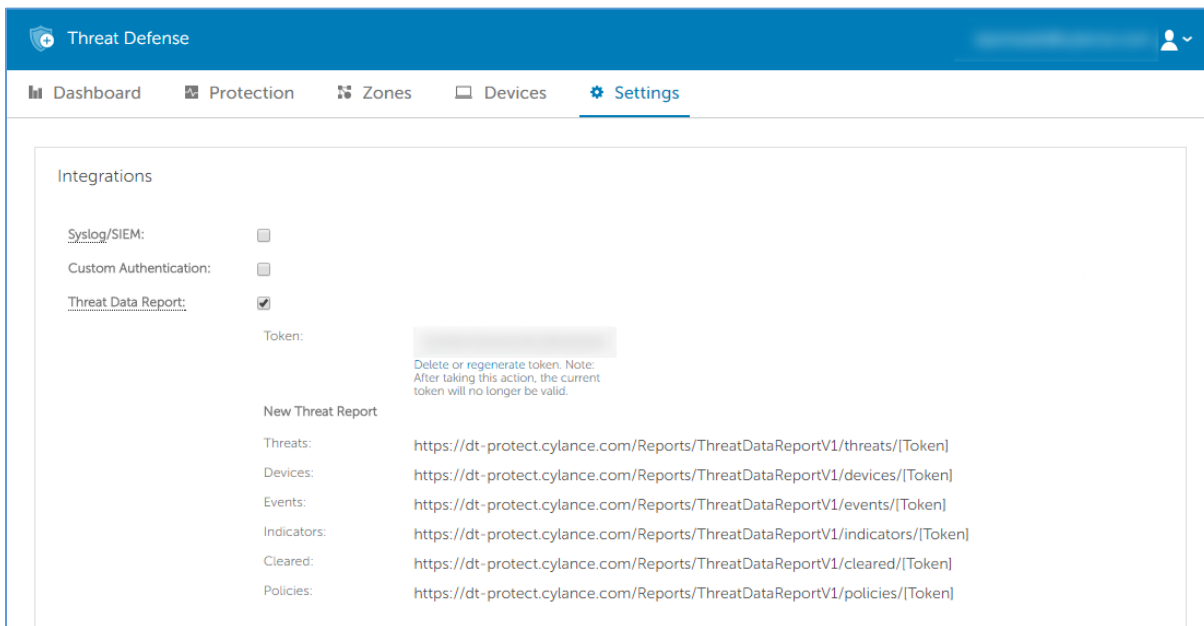


*Figure 71: Generate Threat Data Report*

# 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.

## Support

### 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 – Mac OS X: 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 user interface.
- Enable verbose logging for the installation.

### Performance Concerns

- Capture a screenshot of the Task Manager (Windows) or Activity Monitor (Mac OS X) that shows the Threat Defense processes and memory consumption.
- Capture a dump of the Threat Defense process.
- Collect debug logs.
- Collect output of System Information during the issue.
    - For Windows: msinfo32 or winmsd
    - For Mac OS X: System Information
- Collect any relevant Event Logs (Windows) or Console information (Mac OS X).

### 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?
- Restart the Threat Defense service so that it attempts to connect to the Console.
- Collect debug logs.
- Collect the output of System Information during the issue.
    - For Windows: msinfo32 or winmsd
    - For Mac OS X: System Information

## Enabling 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.

# 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, Dell recommends disabling Script Control in the Device Policy affecting the devices, to restore normal device functionality.

**Note**: This Compatibility Mode solution is for Agent version 1370. 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. Using the Registry Editor, go to **HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop**.

2. Right-click **Desktop**, click **Permissions**, take ownership and grant **Full Control**. Click **OK**.

3. Right-click **Desktop**, select **New > Binary Value**.

4. Name the file **CompatibilityMode**.

5. Open the registry setting and change the value to **01**.

6. Click **OK**, then close Registry Editor.

7. A restart of the device 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 devices, 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}
```

# APPENDIX A: 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) files, detected as *Unsafe* or *Abnormal*, to the Cylance Infinity Cloud for analysis. |
| Console | Threat Defense Management User Interface |
| Device Policy | Threat Defense policy that can be configured by 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) |
| Infinity | The Mathematical Model used to score files |
| 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) |
| 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. |

# 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.



| Agent Version | Active Script | | Powershell | | Macros | |
|---|---|---|---|---|---|---|
| | Alert | | Block | | | |
| 1370 and Below | ○ | | ● | | N/A | |
| | Alert | Block | Alert | Block | Alert | Block |
| 1380 and Above | ○ | ● | ○ | ● | ○ | ● |
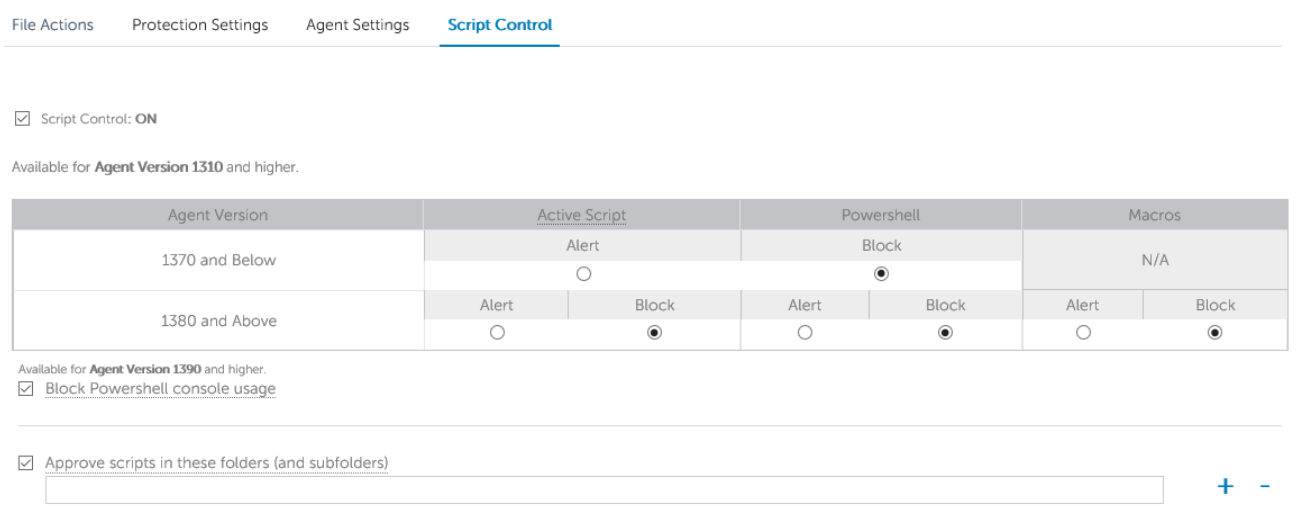
*Figure 72: Script Control*

## Certificates

**Global**: Add certificates to the Console, then add them to the *Global Safe List*. This allows applications 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.

| | USER | ZONE MANAGER | ADMIN |
|---|---|---|---|
| **Agent Update** | | | |
| View/Edit | | | X |
| **Audit Logging** | | | |
| View | | | X |
| **Devices** | | | |
| 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 |
| **Zones** | | | |
| Create Zone | | | X |
| Delete Zone | | | X |
| Edit Zone Name – Any | | | X |
| Edit Assigned Zone Name | | X | X |
| **Policy** | | | |
| 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 |
| **Threats** | | | |
| 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 |
| **Settings** | | | |
| Generate or delete install token | | | X |
| Generate or delete invite URL | | | X |
| Copy install token | X | X | X |
| Copy invite URL | | | X |
| **User Management** | | | |
| Assign users to any Zone | | | X |
| Assign users to managed Zone | | X | X |
| 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 |

# 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).