



ANTIGENA NETWORK

Training Manual



Darktrace Antigena Network

Training Manual
v2.0.2
Darktrace Version 5.1

Table of Contents

| | | | | |
|----|--|----|---------------------------------------|----|
| 1. | Learning Objectives..... | 1 | Model Definition | 22 |
| 2. | Prerequisites | 2 | Antigena Network Model Actions | 24 |
| 3. | Basic Antigena Network Concepts | 3 | Antigena Network Inhibitors | 25 |
| | Flow Structure..... | 5 | Antigena SaaS Inhibitors..... | 25 |
| | Antigena Network Actions | 6 | Antigena Network Model Logic..... | 26 |
| | Antigena Network Action Examples | 6 | 7. Tagging for Antigena Network | 27 |
| 4. | Configuring Antigena Network..... | 8 | 8. Recommended Deployment Schemes | 31 |
| | Console | 9 | General Recommendations..... | 32 |
| | Threat Visualizer System Config | 10 | Useful Deployment Schemes | 33 |
| | Antigena Network Enablement Modes | 12 | Early Stage Deployment..... | 33 |
| 5. | Antigena Network in Action | 14 | Tuning the Deployment | 34 |
| | Human Confirmation Mode | 15 | Optimized Deployment..... | 34 |
| | Active Mode and Testing Antigena Network | 19 | Exempting Users or Devices | 35 |
| 6. | Antigena Network Models..... | 21 | 9. Mobile App Antigena View..... | 36 |
| | | | 10. Learning Outcomes | 37 |

1. Learning Objectives

Course Agenda

This course provides a comprehensive understanding of Darktrace's autonomous response capability, Antigena Network.

It is designed for end users of Darktrace, primarily IT Administrators, who will be entrusted to oversee the Antigena actions.

The following document serves an educational guide for the key elements of Antigena Network.

By the end of this course, you will be able to complete the following objectives:

Configure Antigena Network options

Schedule Antigena Network modes

Understand Antigena Network Models

Tag devices for monitoring by Antigena Network

Handle Antigena Network actions raised by Darktrace

2. Prerequisites

Before embarking on the Antigena Network course, it is imperative that you have completed the appropriate prerequisites beforehand. A basic knowledge of the Threat Visualizer interface is necessary for understanding Antigena Network.

You should have already attended both Threat Visualizer Courses and therefore be familiar with the following topics:

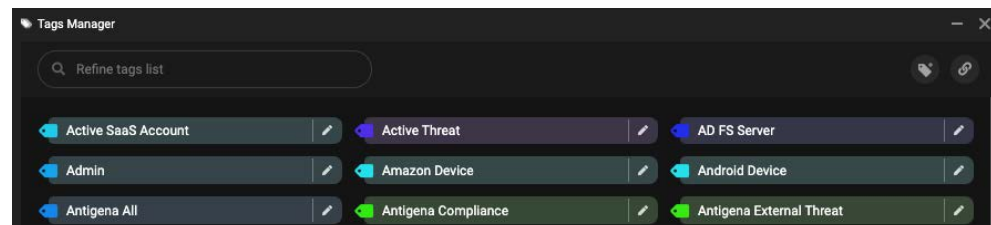
Threat Visualizer Part 1 - Familiarization

- Darktrace and its available solutions
- Navigating the Threat Visualizer Interface
- Investigating alerts
- Viewing device details
- Using the Dynamic Threat Dashboard

Threat Visualizer Part 2 - Investigation

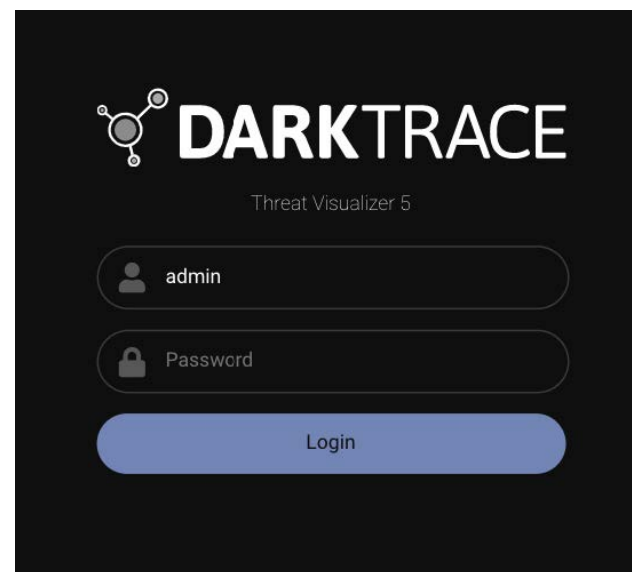
- AI Analyst
- Advanced Search fundamentals
- Creating Packet Captures
- Generating Executive Threat Reports
- General analytical workflows

It is also advisable that you are familiar with Tags and the Tags Manager as well as the Model Editor and how Models are structured.



This material is covered in the **Cyber Analyst Part 2 - Model Optimization** class, but eLearning concerning the Model Editor can be found on the [Customer Portal](#).

Furthermore, to carry out the workflows outlined in this training manual, it is recommended that you use the “**admin**” user account to access the Threat Visualizer and Console. Otherwise, you may not be able to access all the features and configuration options to enable and use Antigena Network.



3. Basic Antigena Network Concepts

Antigena is an autonomous response technology that can interact with network, SaaS, and email traffic. In this chapter, learn specifically about Antigena Network and what actions it can take on network traffic.

FLOW STRUCTURE

5

ANTIGENA NETWORK ACTIONS

6

Antigena Network Action Examples

6

3. Basic Antigena Network Concepts

Darktrace delivered the world's first proven Autonomous Response technology on the market with Darktrace Antigena. The innovative Antigena Network is a self-learning Cyber AI that autonomously responds in real-time to any potentially threatening behavior detected on the network by Darktrace's Immune System technology. Importantly, it does not rely on predefined signatures or prior knowledge. It takes targeted, surgical action to contain in-progress threats, neutralizing attacks in seconds without disrupting business processes, thereby buying human teams time to catch up.

Unmatched Speed



Responds within
2 seconds

Unrivaled Defense



7 Threats blocked
every minute

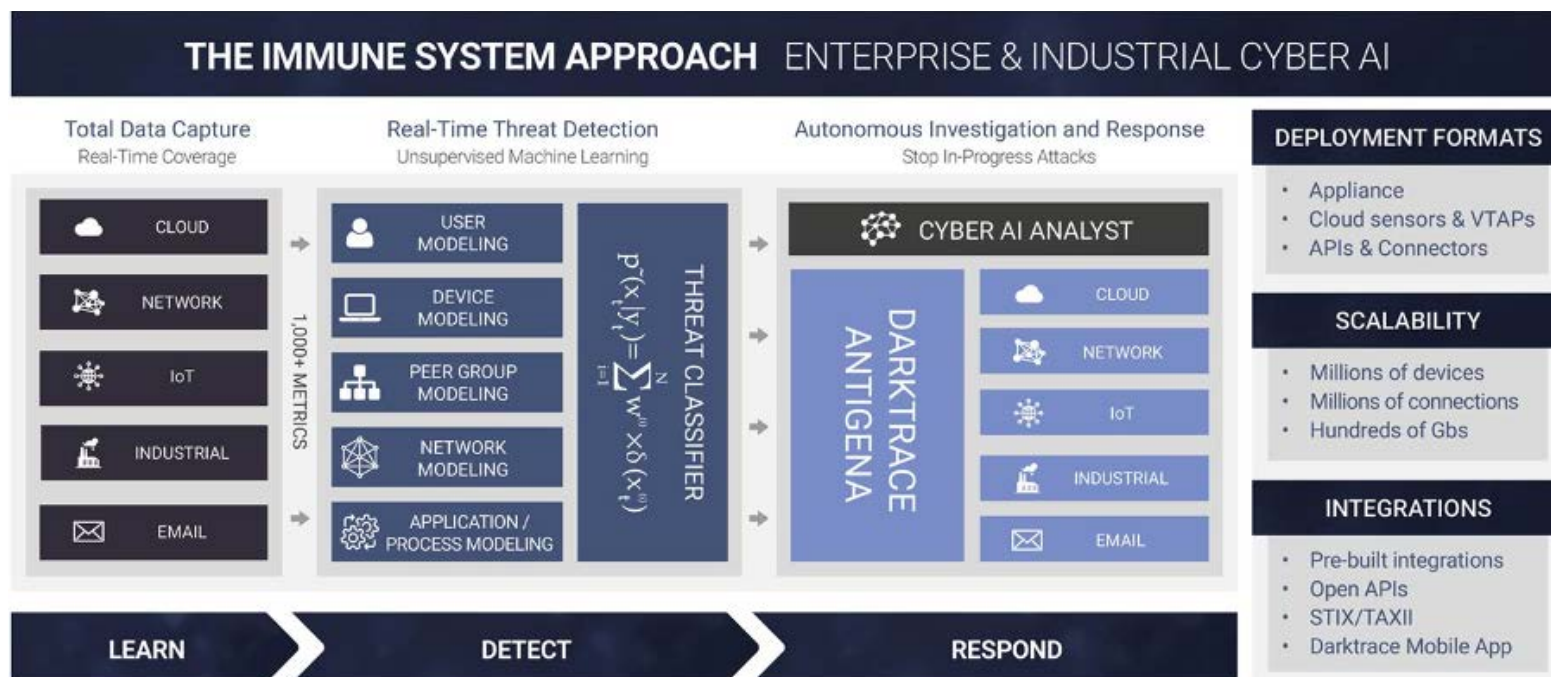
Boosts Productivity



10 hours a week saved
per security analyst

It achieves this by understanding the “patterns of life”, the usual behavior of users, devices, and networks so that Antigena Network can take action in a highly targeted manner, mitigating threats while avoiding over-reactions. Rather than generating broad quarantine measures, Antigena Network can surgically enforce the normal “pattern of life” of an infected device or user, neutralizing the threat within seconds while sustaining routine operations. The Antigena actions are not only granular, but can also dynamically adapt to the severity of a threat as it unfolds.

The Antigena Network module is customizable so can also be scheduled so it only runs out of office hours such as at the weekend, preventing malicious activity and enabling teams to investigate the incidents in work time. Furthermore, this technology can seamlessly integrate with your existing ecosystem, informing firewalls and network devices about attacks that have gotten through. Darktrace Antigena can act as the Cyber “AI brain” of the entire security stack, giving control back to the defenders and transforming the most complex and vulnerable organizations into resilient, self-defending businesses.



Flow Structure

Antigena Network responds to 'high-confidence threats' that strongly point to malicious activity, such as machine speed attacks or ransomware. Antigena interrupts connections by sending TCP Reset packets, or by integrating with your existing infrastructure and messaging directly to a firewall.

TCP Reset Packets are part of normal communications between two devices. When a device receives a reset packet, it will close the TCP Connection, be it an internal device or an external service such as a website. When Darktrace identifies suspicious activity, it will attempt to send Reset packets to both participating endpoints, the source and destination devices, both internally and externally. The Reset packet IP addresses are spoofed so that the devices believe the packets are not coming from Darktrace, but from each other.

When the Darktrace Appliance triggers an Antigena Network action, it informs all probes, including vSensors, to block the identified connections and ports. When they identify traffic to take action on, only the Darktrace appliance or probe that observed the packets of the connection will send TCP Reset packets to interrupt network activity.

By default, TCP reset packets are sent by the Administrative interface of Darktrace appliances. Additional interfaces can be set, however. Review the Darktrace Antigena Network Configuration Guide on our Customer Portal for more information.

Detect



- Firstly, Darktrace's **Immune System technology detects anomalous activity** live on the network.
- Example: A device uploading an unexpectedly large file to a rare external destination.



Respond



- Darktrace then applies **Antigena Network actions** to the offending device by intercepting the network's connection packets.
- It spoofs the IP address of the device and sends TCP Reset packets to the remote site instructing the endpoint that the connection has closed.
- Antigena sends the same Reset packets to the device, spoofing the external location's address.
- Through this approach, Antigena interferes with the network connection by preventing connections from transmitting and receiving information.



Protect



- After a specified interval, Antigena Network will cease closing packets and allow the device to continue transmitting data.

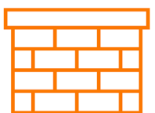
Antigena Network Actions

Antigena automatically acts within seconds to restrain or contain threats, allowing humans the time to catch up. It could only take 20 minutes for a major threat, such as a ransomware attack, to evolve into a crisis. Therefore, Antigena's automated actions can slow, or stop threats in a targeted fashion, to provide security teams with a vital time window in which to take mitigating action. This technology proactively allows networks to self-defend against specific threats, without disrupting your organization.

Once Darktrace has identified a potential threat, Antigena has the ability to take a variety of actions, depending on the severity of the anomalous activity. When Darktrace detects threats on a network, Antigena is programmed to proactively block threats.

Antigena Network Action Examples

- Antigena can enforce the group's patterns of life of a device, allowing it to make any connections and data transfers that it or any of its peer group typically makes. Therefore, it can stop devices sending an unusually large volume of data to external devices which they do not normally communicate with.
- Antigena may enforce the pattern of life of a specific device, only allowing connections and data transfers which Darktrace considers normal for that device, such as Quarantining devices using administrative credentials for the first time.
- Antigena can block specific offending connections. In other words, it can block all connections on a specific port or inhibit connections to a specific device. For example, it might do this to interrupt the download of malicious files from rare external sources.
- Antigena can Quarantine a device so that all incoming and outgoing traffic to or from a device is blocked. This is useful to block ransomware encrypting internal network shares.
- Antigena can be employed to update your organization's existing firewall or network defenses. For example, this can block unusual SSH and RDP connections from non-administrative systems.

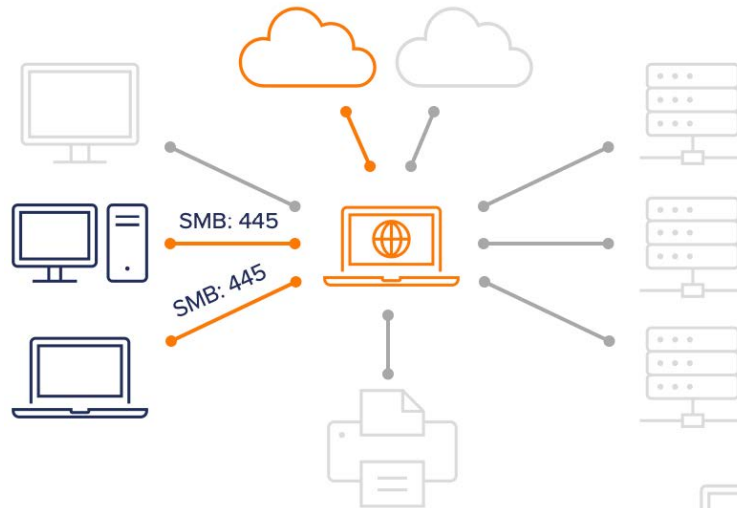


3. Basic Antigena Network Concepts

Antigena Network Actions

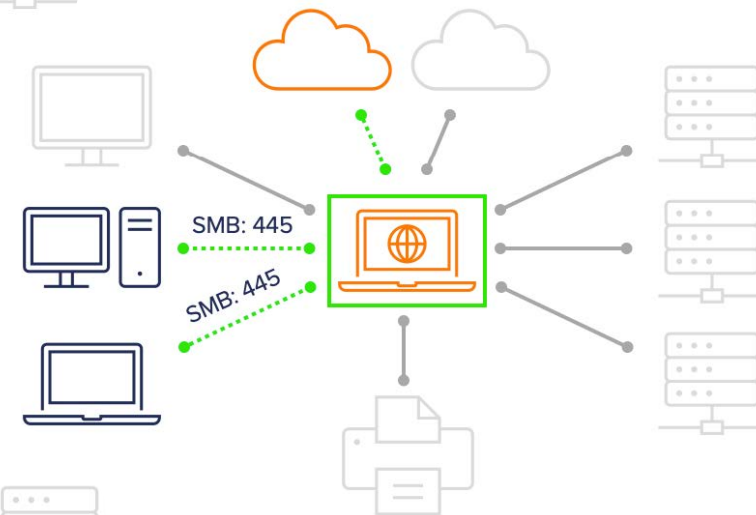
DETECT

A laptop device connects to a rare domain, where a download of an executable is observed. Following this activity, the device begins making anomalous connections to other internal connections. These connections take place over SMB port, 445, and are indicative of high confidence ransomware.



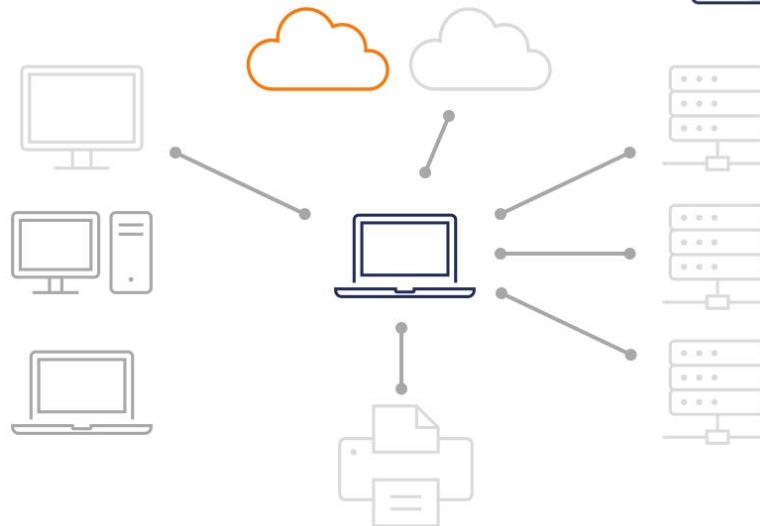
RESPOND

Antigena Network actions the offending device by intercepting the network's connection packets. It spoofs the IP address of the laptop and sends TCP Reset packets to the malicious site instructing the endpoint that the connection has closed. Antigena sends the same Reset packets to the device, spoofing the external location's address. Antigena interferes with the network connection by preventing connections from transmitting and receiving information.



PROTECT

Connections to the endpoint and internal vulnerable machines are blocked for a specified interval, averting the immediate threat. The security team is alerted to the incident. After the action time has elapsed, Antigena Network will cease closing packets and allow the device to resume transmitting data.



4. Configuring Antigena Network

Antigena Network requires a license and must be enabled in multiple locations: The Darktrace Console and the Threat Visualizer interface. In this chapter, learn how to configure Antigena Network and enable it using different modes.

CONSOLE

9

THREAT VISUALIZER SYSTEM CONFIG

10

ANTIGENA NETWORK ENABLEMENT MODES

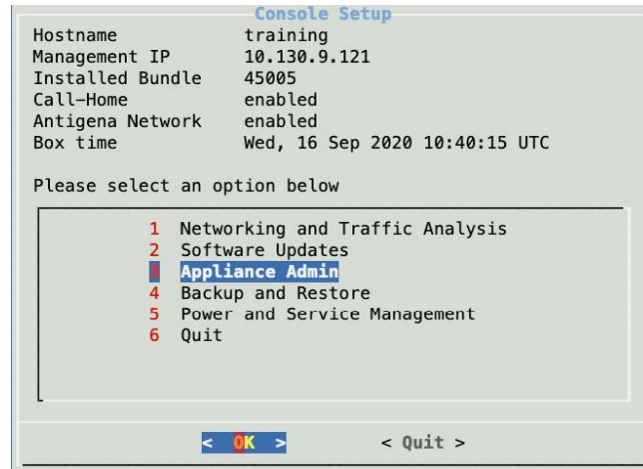
12

Console

Antigena Network must be enabled both in the console interface and the Threat Visualizer System Config before it can be used. If the following configuration is carried out on a Darktrace Unified View Server, it will propagate down to all connected master appliances.

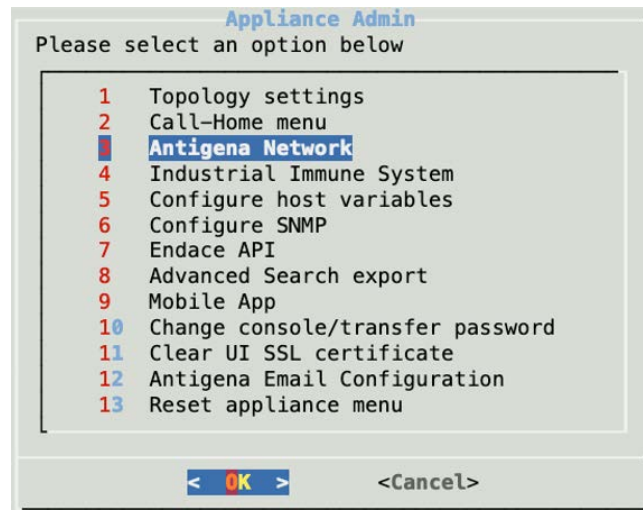
1. Firstly, within the Console, navigate down to option 3, **Appliance Admin**, and select it from the menu.

Select **OK** to proceed.



2. From the Appliance Admin page, select the **Antigena Network** option.

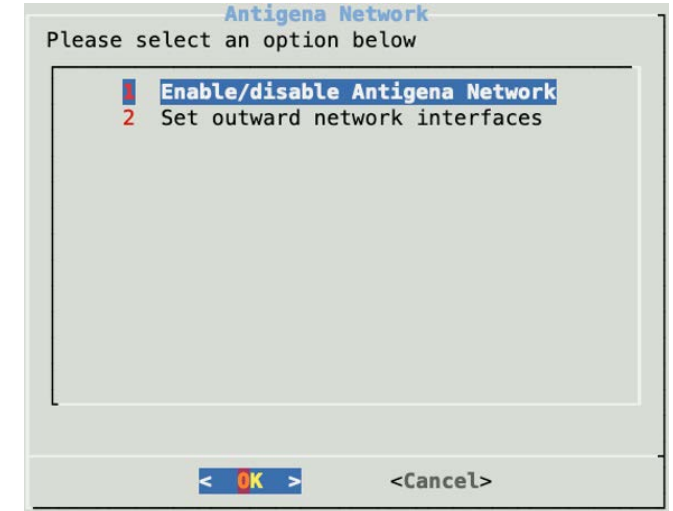
Select **OK** to continue.



3. From the Antigena Network options, select **Enable/disable Antigena Network**.

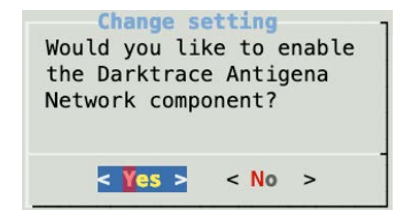
Again, select **OK** to proceed.

A prompt may appear describing Antigena Network. Click OK to continue to the next step.



4. When prompted to **enable the Darktrace Antigena Network component**, select **Yes**

Note: Configuration may take several minutes and can be tracked by a progress bar after selecting Yes. On completion of this step, it is possible the console will log out. Log back in to continue.



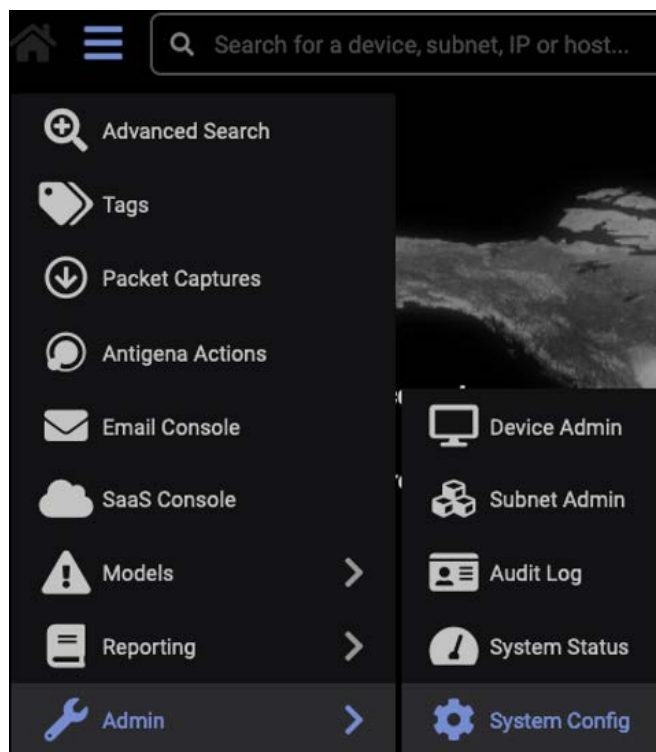
5. A window will appear indicating that the console setup process is now complete and this configuration has been **successfully applied**.



Threat Visualizer System Config

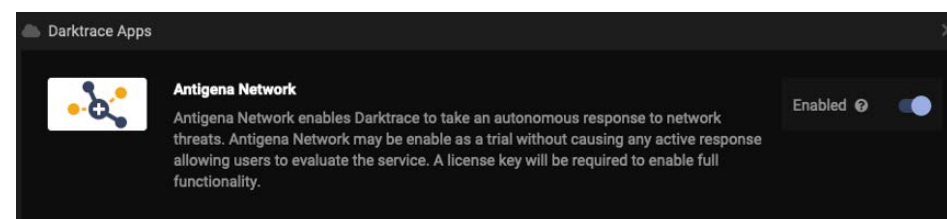
In order to enable Antigena Network, it is necessary to input the license key into the Darktrace System Configuration page.

1. Navigate to the **System Config** page, which is located under the Admin section of the Threat Visualizer main menu.
2. Once the System Config page has opened in a new tab, click on the **Modules** menu located on the left-hand side of the screen.
3. Within the Modules page, under Explore, click on **Darktrace Apps**.



Alternatively, begin typing "Antigena Network" into the search bar to dynamically filter the displayed modules.

4. From the available applications, choose **Antigena Network**.
5. A new window will open. Ensure that the Antigena Network **toggle is enabled**.

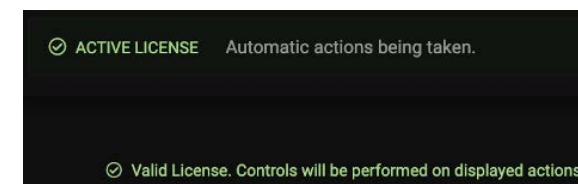
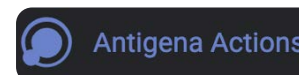


6. Further down this window, paste your **Network License key**, as supplied by Darktrace Support, into the relevant text field. At this point, save these changes.



7. Refreshing the page, the Antigena Network app should now read **Active License**.

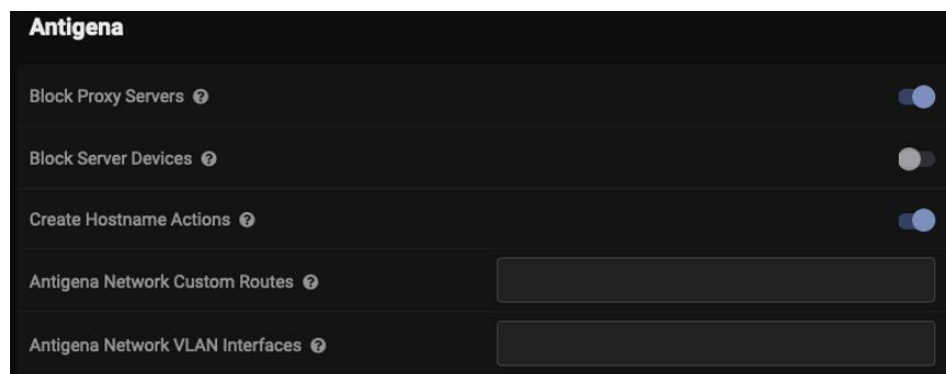
Success messages are displayed within the application window and access to Antigena Actions has been granted in the Threat Visualizer main menu.



4. Configuring Antigena Network

Threat Visualizer System Config

8. Next, navigate to the **Settings** tab on the left-hand side menu.
9. Type **Antigena** into the **search bar** and select the Antigena option to locate Antigena Network settings.
10. Under the Antigena heading, there are a handful of settings. The **defaults**, as configured in the image below, are Darktrace's recommendations.



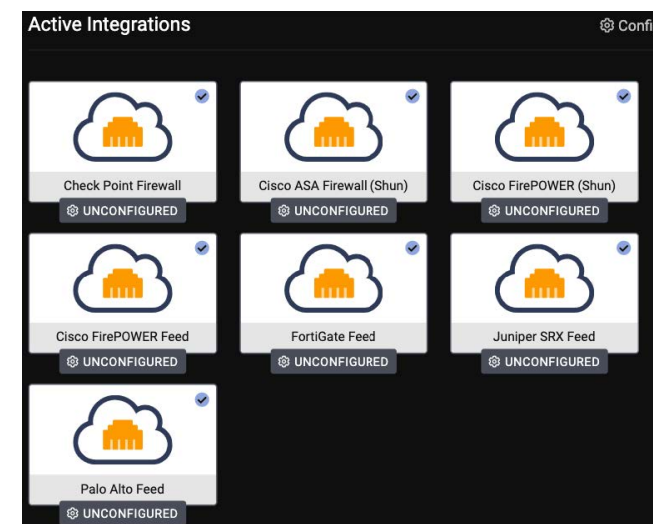
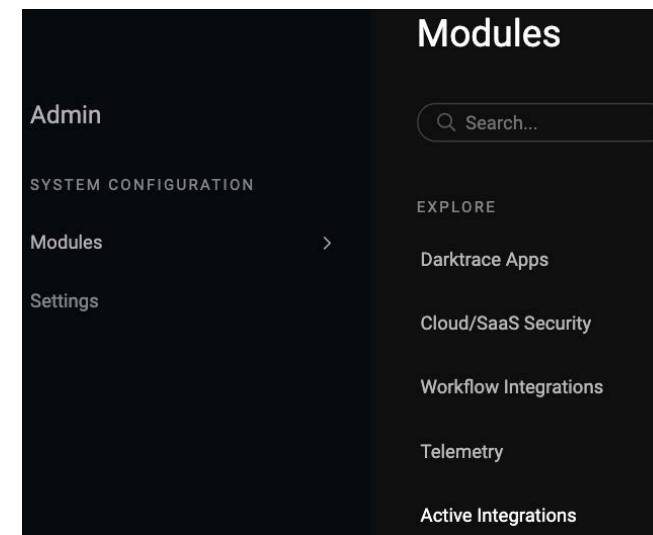
- a. The **Block Proxy Servers** setting allows Antigena to block all connections to proxy servers when individual hostnames or IP addresses cannot be blocked. It is recommended that this is set to true to provide an effective Antigena response for such situations.
- b. For most networks, particularly when turning on Antigena for the first time, **Block Server Devices** should be set to false. This will prevent Antigena quarantining any devices set as a server in Darktrace and reduce false positives. Over time, especially on smaller networks, it may be appropriate to enable Antigena on certain servers or for particular models.

- c. The third option, **Create Hostname Actions**, also defaults to true, allowing Antigena to create actions based on destination hostnames.
- d. The **Antigena Network Custom Routes** and **Antigena Network VLAN Interfaces** fields provide further options for changing the existing interface used by a Master appliance for sending TCP Reset packets.

11. Firewalls can also be configured to work with Antigena Network.

Locate the **Active Integrations** section from the **Modules** menu, previously accessed when activating Antigena Network.

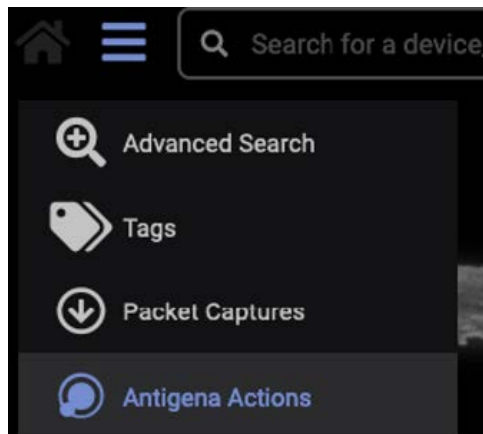
12. **Choose a firewall** to configure for your network and input the appropriate values, as prompted in the firewall window. Doing this allows Darktrace to provide an additional layer of protection by instructing your firewall to block IP addresses and ports for defined periods of time.



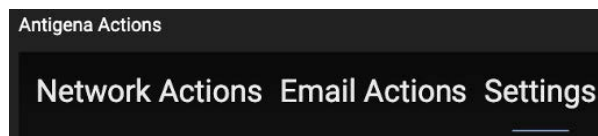
Antigena Network Enablement Modes

Antigena can be enabled in two modes: Human Confirmation Mode and Active Mode.

1. Navigate to the **Antigena Actions** page, which can be found in the main menu.



2. Select the **Settings** tab, located along the top of the Antigena Actions window.



3. A weekly **Antigena Network mode schedule** is presented. On this page, it is possible to see which mode Antigena is set to for each hour of every day throughout the week.

Action Schedule
Antigena will action your network according to your determined schedule.

Select a preset schedule | Clear Schedule

⚠ The time periods in which Antigena will use model settings
👤 The time periods in which Antigena actions will require human confirmation

| UTC | 00:00 | 01:00 | 02:00 | 03:00 | 04:00 | 05:00 | 06:00 | 07:00 | 08:00 | 09:00 | 10:00 | 11:00 | 12:00 | 13:00 | 14:00 | 15:00 | 16:00 | 17:00 | 18:00 | 19:00 | 20:00 | 21:00 | 22:00 | 23:00 |
|-----------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| Sunday | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |
| Monday | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |
| Tuesday | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |
| Wednesday | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |
| Thursday | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |
| Friday | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |
| Saturday | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |

The **purple icon** with a triangle represents **Active Mode**. In this mode, Antigena Network will proactively block threats for individual models that allow for **Automatic Antigena**, without needing permission from an administrator.



The **yellow icon** with a person represents **Human Confirmation Mode**. In this mode, Antigena Network will inform administrators that it wants to take action, but will wait for **approval** before doing so.



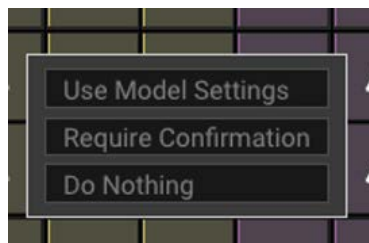
4. Configuring Antigena Network

Antigena Enablement Modes

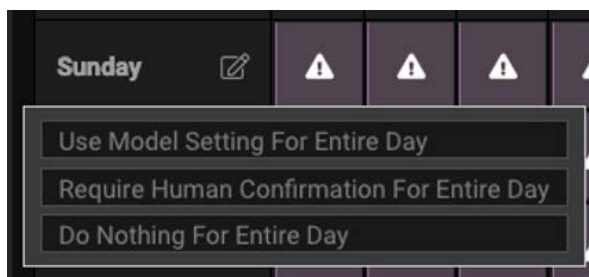
4. Clicking an **individual square** allows the mode to be changed for the selected hour.

There are multiple options available for each block: **Use Model Settings**, **Require Confirmation** and **Do Nothing**.

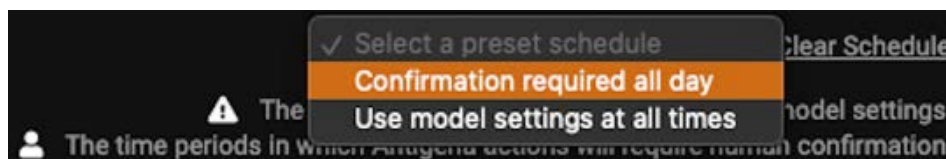
These represent Active Mode, Human Confirmation Mode and no Antigena actions respectively.



5. It is also possible to modify settings for a **full day** at once by clicking the edit icon next to the relevant day of the week.



6. Upon deploying Antigena Network, **Human Confirmation Mode** is recommended for a set period, often **1 to 2 months**.



Once Antigena breaches have been reviewed and optimized, enabling Active Mode is recommended, allowing Darktrace to deter threats at all times.

It is not uncommon to enable Active Mode for out of work hours, for example, during the weekend, evenings and early mornings. This means that if Antigena Network alerts occur during the day, an administrator can manually decide whether to block connections. However, outside of working hours, they will have the comfort of knowing Antigena will help protect their network and allow them to review incidents on their return.

5. Antigena Network in Action

There are multiple configurations Antigena Network can take, which can be deployed separately, or mixed together. In this chapter, learn about Human Confirmation Mode versus Active Mode and see them in action. This can help decide what configuration Antigena Network should be in for your organization.

HUMAN CONFIRMATION MODE

15

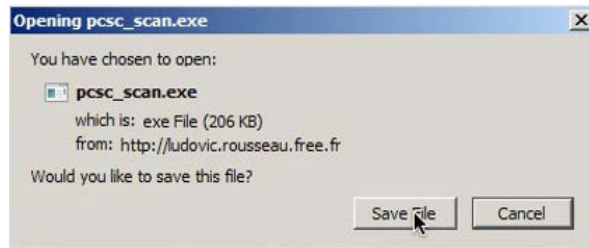
ACTIVE MODE AND TESTING ANTIGENA NETWORK

19

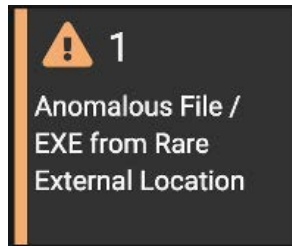
Human Confirmation Mode

In the following example, the deployment is set to Human Confirmation Mode for all days of the week. As a result, when an Antigena Network Model Breach occurs in the Threat Tray, there is no action taken until it has been approved. Let us walk through the workflow that is necessary in this situation.

1. This example demonstrates the effects of **downloading a Windows executable file** from an external destination not normally visited by the network using a device monitored by Darktrace.



2. Once the executable has downloaded, an **EXE from Rare External Location** Model Breach appears in the Threat Tray. However, there is no accompanying Antigena Network Model Breach. This is because Antigena Network needs to be informed of which devices are to be monitored through tagging.

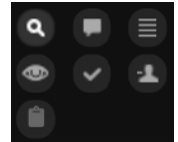


3. To start the tagging process for this device, make sure it is populated in the **Omnisearch bar**.



This can be achieved by typing identifiable device information, such as the device Label, user, hostname or IP address, into the Omnisearch bar.

Alternatively, click the **magnifying glass** in the Breach Log of the Model Breach of interest.



4. Use the **+ icon** under the Omnisearch bar to add an Antigena tag. In this case, select the Antigena All tag to apply it to the device.



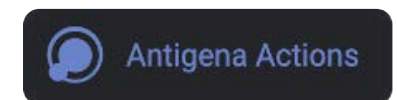
5. Using the device being monitored by Darktrace, try and **download a Windows executable** from a rare external site. This should trigger a different series of events.



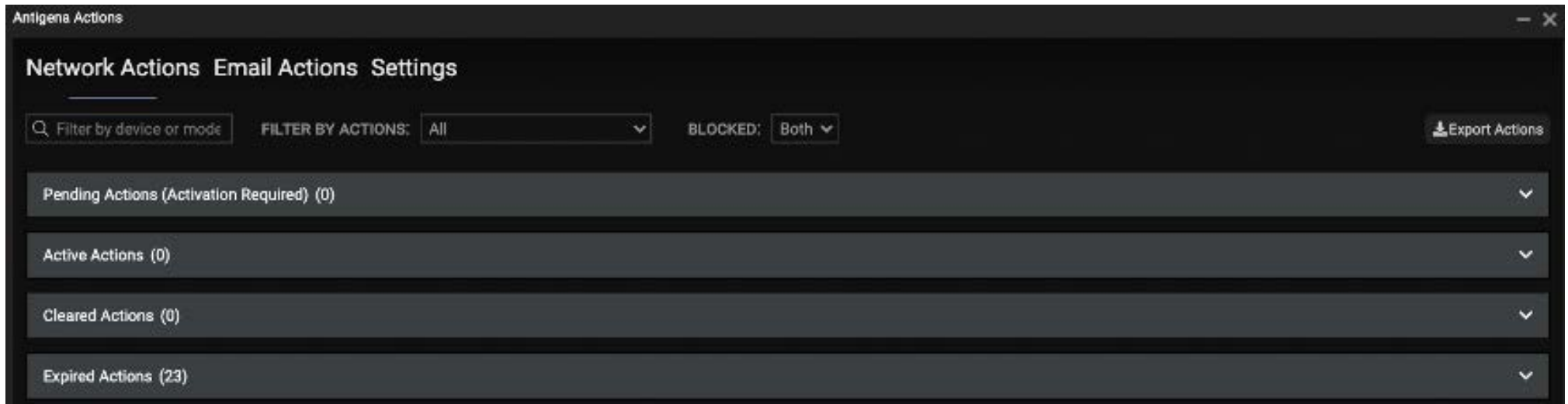
6. Returning to the Darktrace Threat Visualizer, a new **Antigena Network Model Breach** should be preset in the Threat Tray. As Human Confirmation Mode is currently configured, the presence of this breach does not indicate traffic has been actioned. Instead, this alert prompts that approval is necessary for action to be taken.



7. To review any actions requiring approval, navigate to the **Antigena Actions** page found in the main menu.



8. When this window opens, ensure **Network Actions** is selected so Pending, Active, Cleared and Expired Actions are visible. All of these panels are expandable/collapsible.



9. An action relating to the executable should be awaiting consent under the **Pending Actions** panel.

| Pending Actions (Activation Required) (1) | | | | |
|---|---|---|---------|--|
| DEVICE | ACTION | START / EXPIRATION (UTC) | BLOCKED | MODEL |
| Clara Desktop | Block connections to 212.27.63.159 port 80 and ludovic.rousseau.free.fr port 80 | <div>▶ Thu Aug 27 2020, 22:37:50 +01:00</div> <div>■ Thu Aug 27 2020, 22:42:50 +01:00</div> | No | Antigena / Network / External Threat / Antigena Suspicious File Block Activate |

| | |
|-------------------------|--|
| DEVICE | This is the device that is to be actioned. |
| ACTION | This is the action that Antigena Network would like to take. In this case, it will block the activity that matches the offending connection. |
| START/EXPIRATION | This is the time period of the action to be taken. |
| BLOCKED | This indicates whether an Antigena action has blocked any activity. |
| MODEL | This is the Antigena Model Breach that triggered the action. |

5. Antigena Network in Action

Human Confirmation Mode

10. At the end of the row, notice the **Activate** button. Clicking this will cause Antigena Network to start taking action on the device.

[Activate](#)

11. The activated action will now move to the **Active Actions** panel. All actions Antigena Network is currently taking on devices that are still within their expiry periods will appear here.

| Active Actions (1) | | | | |
|-------------------------------|---|--|---------|--|
| DEVICE | ACTION | START / EXPIRATION (UTC) | BLOCKED | MODEL |
| Clara Desktop | Block connections to 212.27.63.159 port 80 and ludovic.rousseau.free.fr port 80 | ▶ Thu Aug 27 2020, 22:37:50 +01:00 ■ Thu Aug 27 2020, 22:42:50 +01:00 | No | Antigena / Network / External Threat / Antigena Suspicious File Block Extend Clear |

12. Attempting the same activity again on the Antigena Network monitored device will result in the behavior being **blocked**.

13. Returning to the Antigena Actions panel and clicking the **Extend** button, allows the action duration to be extended from 5 minutes up to 48 hours in duration.

[Extend](#)

14. To the right of this, notice the **Clear** button. This allows the user to stop Antigena Network taking an action that is currently active, effectively deactivating it.

[Clear](#)

5 minutes

15 minutes

30 minutes

1 hour

2 hours


3 hours

6 hours

12 hours

24 hours

48 hours



The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

15. Any actions that are still within their set time period but have been cleared will appear in the **Cleared Actions** panel, below the Active Actions panel.

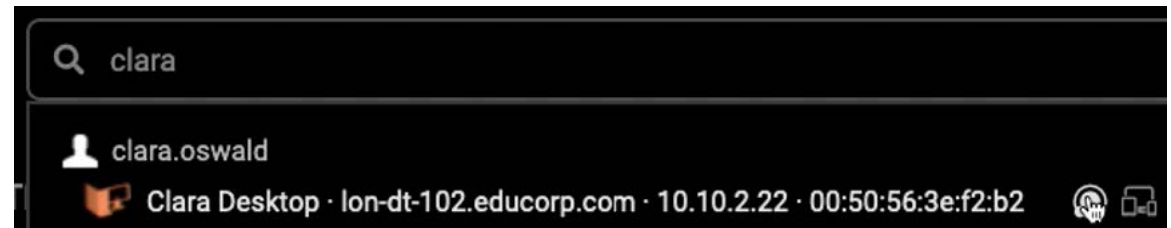
| Cleared Actions (1) | | | | |
|-------------------------------|---|--|---------|--|
| DEVICE | ACTION | START / EXPIRATION (UTC) | BLOCKED | MODEL |
| Clara Desktop | Block connections to 212.27.63.159 port 80 and ludovic.rousseau.free.fr port 80 | ▶ Thu Aug 27 2020, 22:37:50 +01:00 ■ Thu Aug 27 2020, 23:47:50 +01:00 | No | Antigena / Network / External Threat / Antigena Suspicious File Block Reactivate |

16. The **Reactivate** button, located at the end of a cleared action, can be used to prompt Antigena Network to start taking action again.
17. Any expired actions will move to the **Expired Actions** panel.

[Reactivate](#)

| Expired Actions (5) | | | | | |
|---------------------|--|------------------------------------|---------|---|----------------------------|
| DEVICE | ACTION | START / EXPIRATION (UTC) | BLOCKED | MODEL | |
| Clara Desktop | Block connections to 104.131.135.195 port 80 | ▶ Wed Sep 23 2020, 19:09:57 +01:00 | No | Antigena / Network / External Threat / Antigena Suspicious File Block | Reactivate |
| | | ■ Wed Sep 23 2020, 19:14:57 +01:00 | | | |
| Clara Desktop | Enforce group pattern of life | ▶ Tue Sep 15 2020, 18:04:51 +01:00 | No | Antigena / Network / External Threat / Antigena Suspicious File Pattern of Life Block | Reactivate |
| | | ■ Tue Sep 15 2020, 20:04:51 +01:00 | | | |

18. Note that the Antigena Actions page **for a specific device** can be found by populating the Omnisearch bar and by clicking the leftmost icon.



19. Also note that when an Antigena action requires approval, a **green pop-up notification** will be visible in the bottom right-hand side of the Threat Visualizer interface.

1 Antigena action requiring confirmation ✕

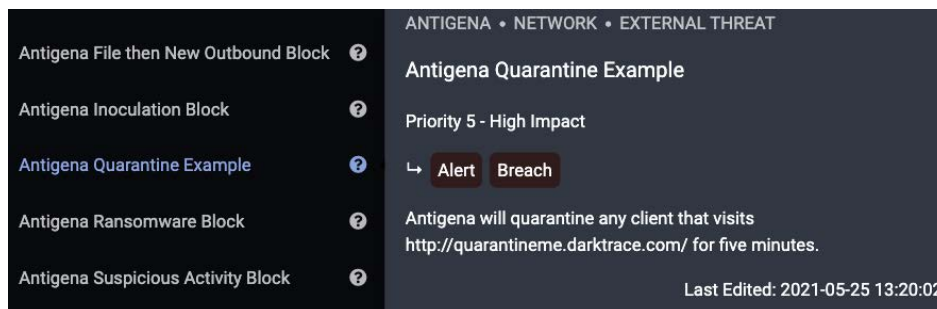
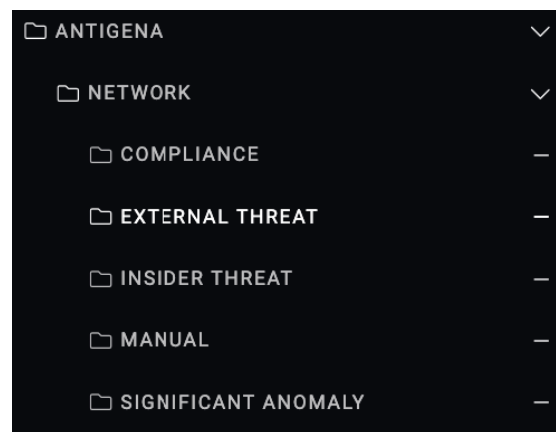
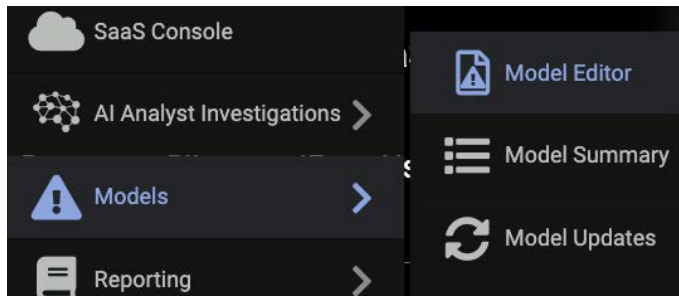
5. Antigena Network in Action

Active Mode and Testing Antigena Network

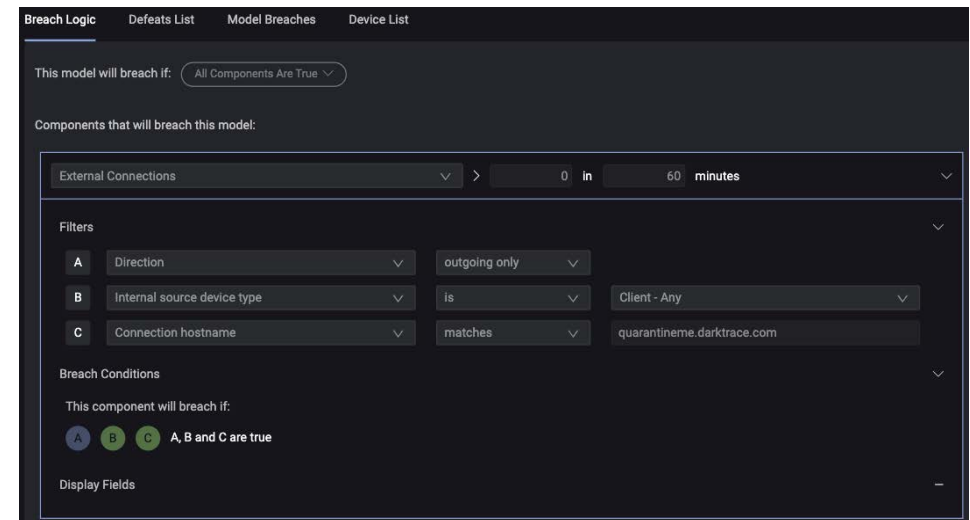
Active Mode and Testing Antigena Network

In this example, we are going to use Active Mode and will look at how you can use the Antigena Quarantine Example Model to quickly test whether your Antigena Network deployment is working as expected.

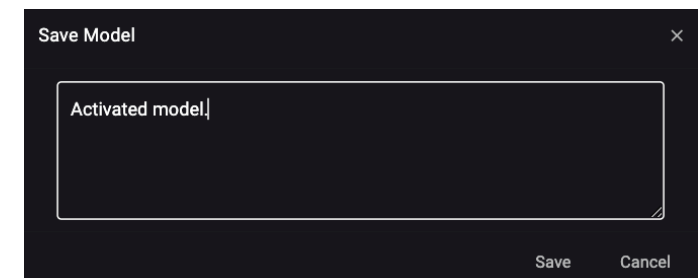
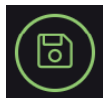
1. Navigate to the **Model Editor**, which is located in the Models submenu of the main menu.
2. Navigate through the following folders within the Model Editor: **Antigena > Network > External Threat**.
3. Open the **Antigena Quarantine Example** Model. This Model is used for testing Antigena Network. It will quarantine any device visiting **quarantine.darktrace.com**, as outlined in the Model preview/description.



4. Unlike other Antigena Models, this **testing Model** requires no tagging, which can be confirmed by reviewing the Model's component.



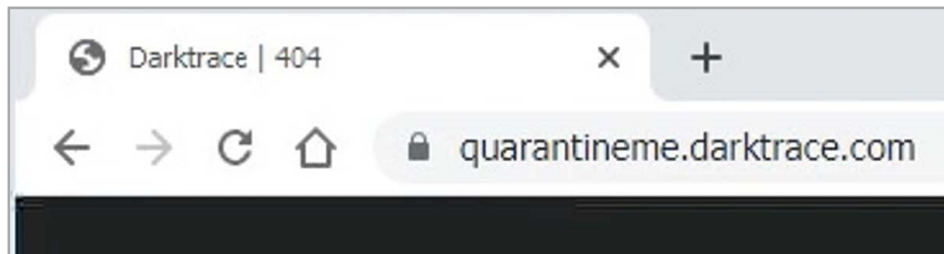
5. The Model is set to inactive by default:
 - a. The first step is to click **Edit Model** in the top right-hand corner of the page.
 - b. Enable the Model by switching the **Active toggle on**.
 - c. Click the Save Model icon in the top-right of the Model Definition.
 - d. Write a descriptive **commit message** which will be visible in the Model History.



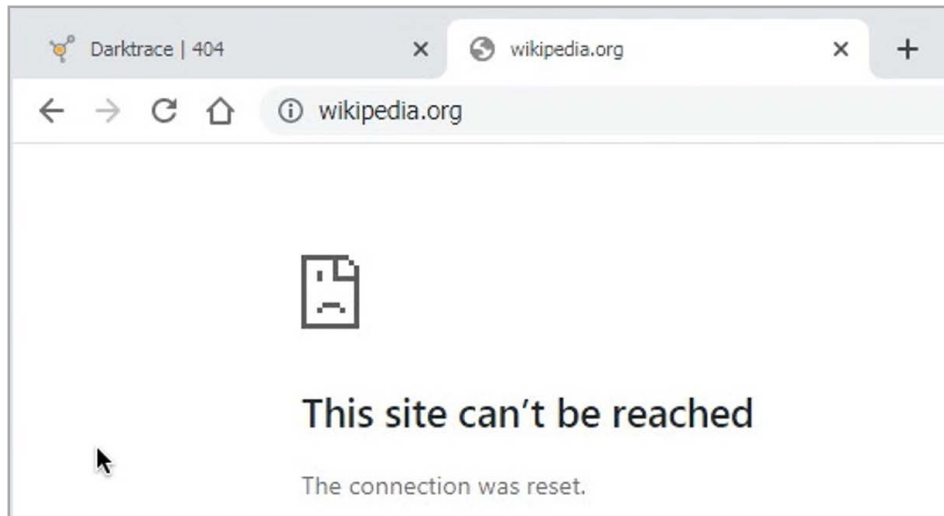
5. Antigena Network in Action

Active Mode and Testing Antigena Network

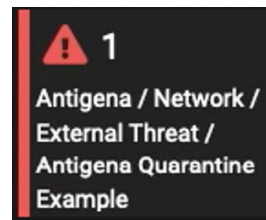
6. Navigating to an appliance being monitored on the network, visit **quarantineme.darktrace.com**.



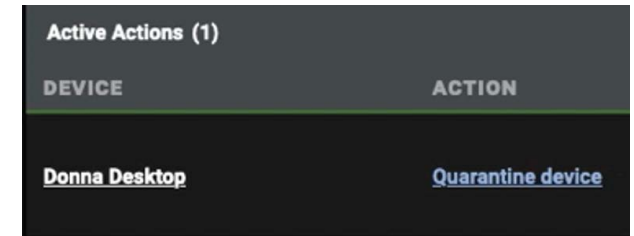
7. When in **Active Mode**, this should trigger the Antigena Network response. By navigating to another website, such as Wikipedia, it can be seen that Antigena Network has already started **blocking the device's network traffic**, meaning that the site cannot be reached.



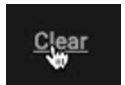
8. Navigating back to the Darktrace Threat Visualizer interface, the associated **Antigena Model Breach** which has been generated is visible within the Threat Tray.



9. Go to the Antigena Actions page. By viewing the **Active Actions** section, it is possible to confirm which actions are being taken on the device.



10. Click the **Clear** button to clear the in-progress action.



11. Try and **access Wikipedia again**. The cleared action means that network access has **returned to normal** on the device.



This example demonstrates how Active Mode differs from Human Confirmation Mode, as well as how the Antigena Quarantine Example model can be a convenient way to test whether an Antigena Network deployment is running as expected.

6. Antigena Network Models

In order to detect different threat types, Darktrace has a comprehensive Model deck which can cause Model Breaches to appear in the Threat Visualizer if triggered. Within the Model Editor, there are Antigena specific Models, which not only alert you to unusual activity, but can also apply autonomous actions. This chapter covers the Model Editor in the context of Antigena Network.

MODEL DEFINITION **22**

ANTIGENA NETWORK MODEL ACTIONS **24**

Antigena Network Inhibitors 25

Antigena SaaS Inhibitors 25

ANTIGENA NETWORK MODEL LOGIC **26**

Antigena actions are activated by Model Breaches within the Threat Visualizer. There is a collection of Antigena Network Models which are set to trigger on specific types of behaviour and are designed to perform different actions depending on the incident identified.

A large variety of actions are possible. For example, incoming and/or outgoing traffic can be blocked by Antigena Network or it can block incoming connections from the internet to a server on a specific port.

Model Definition

1. Within the **Model Editor**, navigate to **Antigena** folder and locate the **Network** subfolder.

2. For ease of administration, Antigena Network Models are **grouped into different categories**:

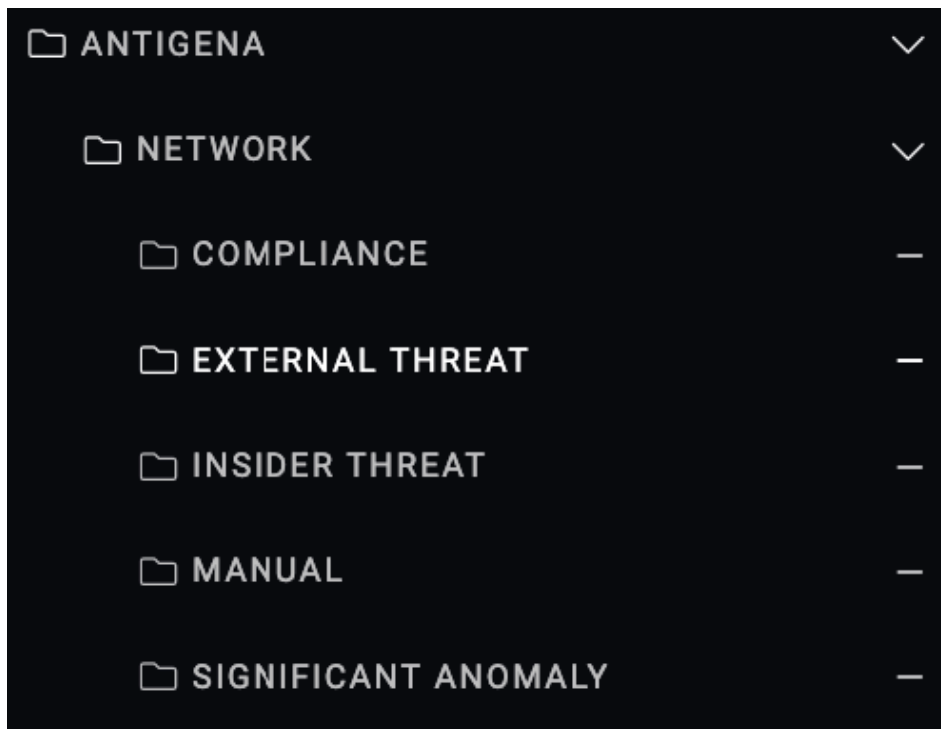
Compliance: These models fire when a device is breaking certain types of common compliance issues, such as the usage of Tor.

External Threat: These fire on external threats such as when ransomware is detected encrypting internal network shares. Antigena identifies such behaviour and can quarantine affected devices from the network.

Insider Threat: Insider threats are events within a network such Internal Data Transfer. This can breach, for example, if Darktrace identifies unexpectedly large downloads from internal servers to client devices particularly with devices they do not normally communicate with.

Manual: The models contained within this folder will enforce Antigena actions for any devices manually tagged with a “Manual” Antigena tag.

Significant Anomaly: This can include a large range of activity, usually when there is a large shift in network activity from what Darktrace has established as the norm.



6. Antigena Network Models

Model Definition

3. Move into the **External Threat** folder and select the **Antigena Suspicious File Block** Model. This is a Model that can react to any device that downloads a file from a rare external location.

The screenshot shows the 'Antigena Suspicious File Block' model definition. On the left is a sidebar with a list of models: 'Antigena Quarantine Example', 'Antigena Ransomware Block', 'Antigena Suspicious Activity Block', 'Antigena Suspicious File Block' (selected), 'Antigena Suspicious File Pattern of Life Block', and 'Antigena Watched Domain Block'. The main panel shows the model's details: 'ANTIGENA • NETWORK • EXTERNAL THREAT', 'Antigena Suspicious File Block', 'Priority 3 - Medium Impact', and two tags: 'Alert' and 'Breach'. The description states: 'A device downloaded a file from an uncommon external location. Action: Review the file that was downloaded by viewing the device's other model breaches. Clear any active blocks if the download was considered to be legitimate.' The 'Last Edited' timestamp is '2021-05-21 13:29:32'.

4. The Model Definition indicates that this Model will breach if a **target score is reached**.

The screenshot shows the 'Breach Logic' tab of the model definition. It features a tabbed interface with 'Breach Logic', 'Defeats List', 'Model Breaches', and 'Device List'. Under 'Breach Logic', it says 'This model will breach if:' followed by a dropdown menu showing 'A Target Score Is Reached'.

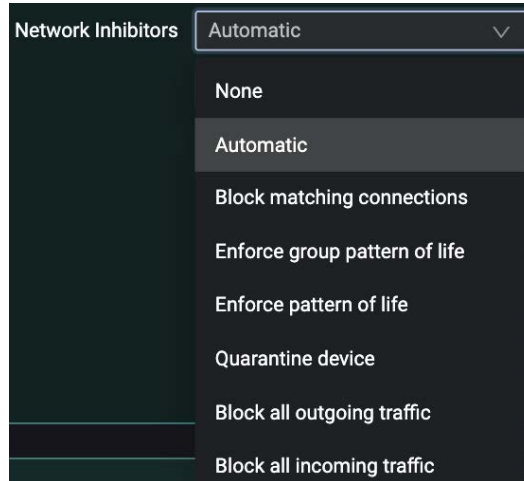
5. Scroll down to the **Model Actions** section of the Model Definition and notice the **Antigena subsection**. This option controls the Antigena Network functionality of the Model.

The screenshot shows the 'Model Actions' section. At the top are three buttons: '+ Priority Score', '+ Tag Device', and '+ Device Type'. Below is a section titled 'Alert External Systems' with the text: 'Models with alert turned on will be pushed out to external systems if conditions for such alerting are met.' Further down is the 'Antigena' subsection, titled 'Autonomous response capabilities'. It contains several settings: 'Network Inhibitors' set to 'Block matching connections', 'Antigena Email Inhibitors' set to 'None', 'Automatic Antigena' toggle switch turned on, 'Antigena Threshold' set to '10', and 'Antigena Duration' set to '7200'.

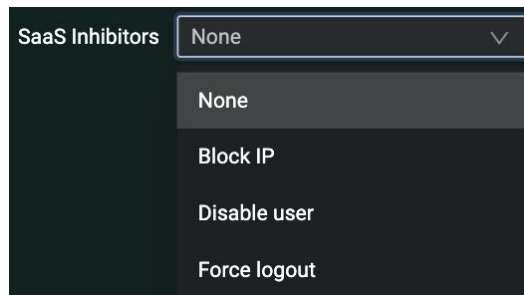
Antigena Network Model Actions

1. The Antigena Autonomous response capabilities is split up into different fields.

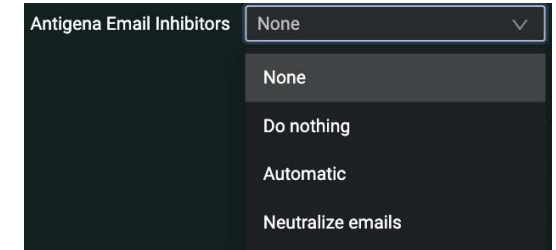
- a. First, review the **Network Inhibitors** section. This specifies what kind of action Antigena Network should take on any offending devices. Notice there may be further inhibitor options, depending on what modules are bundled with your deployment.



- i. For deployments including **SaaS**, Antigena can take one or more responses as a result of a model. Each SaaS platform is different, and depending on which SaaS platform is installed, the types of responses which can take place may vary.



- ii. If you have **Antigena Email**, there may be additional options to take automatic Antigena actions or neutralize emails.



- b. **Automatic Antigena** is employed when Use Model Settings (Active Mode) is set in the Antigena Actions submenu.



When Antigena actions fire and Automatic Antigena is turned off, actions are placed in the Inactive Network Actions section and require manual approval to activate regardless of what mode Antigena is currently set to. This is useful for turning off models that may be overfiring or are not concerns within your corporate environment.

- c. The **Antigena Threshold** sets the minimum model breach score that must be achieved in order to trigger the action. This defines how lenient Antigena Network should be in deciding whether to take action on the offending device.

The lower this is, the more likely Darktrace is to create an action in the Antigena Actions endpoint. This value is part of complex machine-learning based algorithms in the backend that include factors such as the regularity of such behavior for the device.

- d. Finally, the **Antigena Duration** setting specifies how long in seconds the action should last for. Many Antigena Models will have a default value of 3600 (1 hour), but this example has a 2 hour duration.

Antigena Network Inhibitors

| Action | Description |
|--------------------------------------|---|
| Automatic | This option lets Antigena automatically choose the best option using information gathered from the incident. For example, if it sees suspicious behaviour to an SMB share on port 445, it would choose to block just that port, but if it saw a range of suspicious connections to various places on the internet it would choose to block external connections instead. |
| Block Matching Connections | This option will block connections from the device to the destination endpoint seen in the incident on the destination port that was observed. This can be useful for when you need to take highly focused action that minimizes the impact on regular network behaviour. |
| Enforce Pattern of Life | Allows a device to make the connections that it usually makes based on Darktrace's established patterns of life for the device. In other words, it only allows connections and data transfers which Darktrace considers normal for that device. Anything else is blocked. |
| Enforce Group Pattern of Life | This option is more permissive than enforce pattern of life. It allows a device to make any connections and data transfers that it or any of its peer group typically make. This refers to the device's list of most similar devices. Therefore, if the offending device does not normally access a particular SMB share, but some devices in its peer group do, it will be allowed to access that share. |
| Quarantine Device | All network traffic coming into the device or originating from the device is blocked. This effectively completely shuts off the device from the rest of the network. |
| Block All Outgoing Traffic | Any network traffic originating from the offending device will be blocked. |
| Block All Incoming Traffic | Any network traffic coming into the offending device will be blocked. |

Antigena SaaS Inhibitors

| Action | Applicable Modules | Description |
|---------------------|-------------------------|---|
| Block IPs | Office 365 | Prevents access to the account from an IP or IP range for the duration set. |
| Disable User | Office 365, Zoom | Disables a user account for the duration set. |
| Force Logout | Office 365, Zoom | Forces the user to log out from the platform. This action is a one-off action, so will be repeated at the configured interval for the duration set. The default interval is 15 seconds and can be altered by a member of Darktrace support if required. |

Antigena Network Model Logic

1. Review the **Breach Logic** section for this Model. There are two components, both with a score weighting of 1. So, if either component's prerequisite conditions are met, the Model will fire.
2. Check the **first component**. Many Antigena Network Models base their detection off of standard Darktrace Model Breaches. This is denoted by the metric called **Model**. In this example, any Model that's file path contains "Anomalous File" will cause the Model to fire.

Model: [Model] > 0 in 60 minutes 1

Filters

| Filter ID | Field | Operator | Value |
|-----------|------------------------|------------------|---|
| A | Message | contains | Anomalous File / |
| B | Strength | > | 35 % |
| C | Tagged internal source | has tag | Antigena All |
| D | Tagged internal source | has tag | Antigena External Threat |
| E | Message | does not contain | Internal |
| F | Message | does not contain | Zip or Gzip from Rare External Location |

3. Importantly, notice that the Model contains filters checking for two tags: Antigena All or Antigena External Threat. The "OR" element in this can be confirmed by checking the Breach Conditions, located below the components.

Breach Logic Defeats List Model Breaches Device List

This model will breach if: A Target Score Is Reached

Components contributing to target score:

- Any Model (6 filters) 1
- Any File Transfer Start - Exe (9 filters) 1

Target Score: 1

Target Score must be reached within the following seconds: 60

Both components must share endpoints ☐

Breach Conditions

This component will breach if:

A B C D E F A, B, C, E and F are true

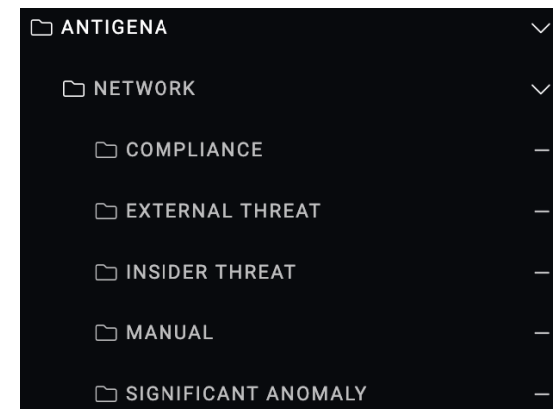
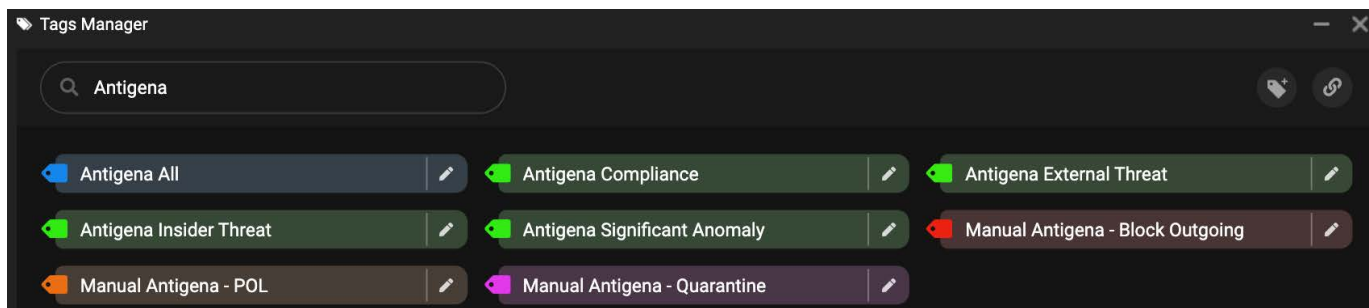
A B C D E F A, B, D, E and F are true

The Antigena Suspicious File Block example demonstrates how assigning different tags can enable or disable Antigena Network monitoring for different devices. Often, it is easy to tell which Model relates to which tags based on the subfolder of the Antigena folder they belong to. However, it is useful to check the Model Definition for tag filters, just to be sure, as some Models act on a wider range of tags. This will be discussed more in the next section.

7. Tagging for Antigena Network

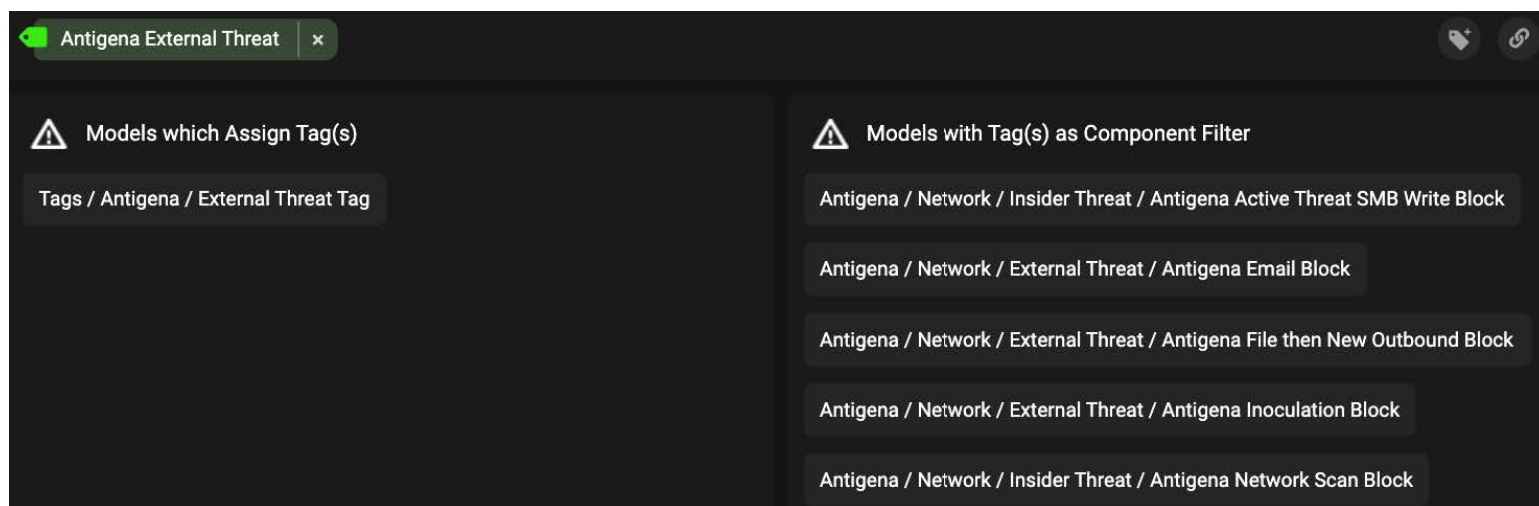
As shown in the previous chapter, Antigena Network Models require devices to be tagged with Antigena tags in order for them to be included in Antigena Network's monitoring. Covered in this section are multiple methods of tagging the devices on the network in order to begin the roll-out of Antigena Network.

1. Open the **Tags Manager** and search for Antigena in the search bar. A range of Antigena Tags are available.



2. The four green tags correspond to four of the folders located in the **Antigena > Network folder** in the Model Editor. Furthermore, the three Manual Antigena tags correspond to models defined in the Manual folder.
3. While the Models in these folders generally look for tags that match their folder name, some look for a wider range of tags.

By reviewing the tag in the Tags Manager, it is possible to verify which Models will act on it. For example, click the **Antigena External Threat tag** and we can see that it also allows monitoring by some models in the **Insider Threat folder**.

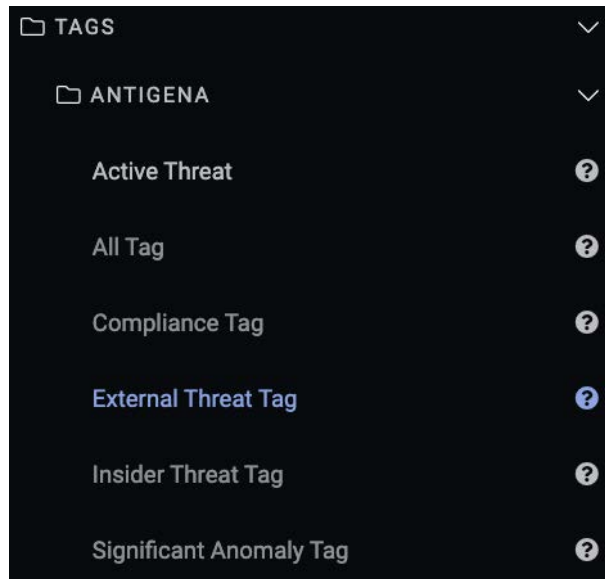


7. Tagging for Antigena Network

4. **Automatic tagging** is often the easiest method to implement Antigena Network. The simplest way to enable Antigena Network for a small network would be to apply the Antigena All tag to every device, which allows devices to breach Antigena Network Models.

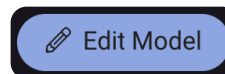
The recommended Antigena Network setup will vary depending on the deployment; some may initially focus on a specific type of breach and group of devices. This can assist in the process of tuning and removing false positives.

Begin by looking at the **Tags > Antigena > External Threat** tagging Model and use it to tag an internal subnets.

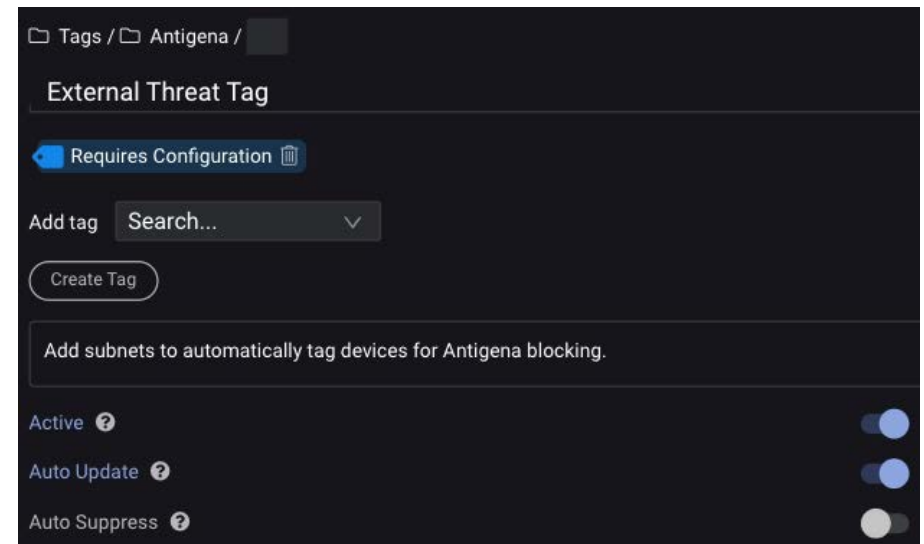


5. The Model is currently **inactive**.

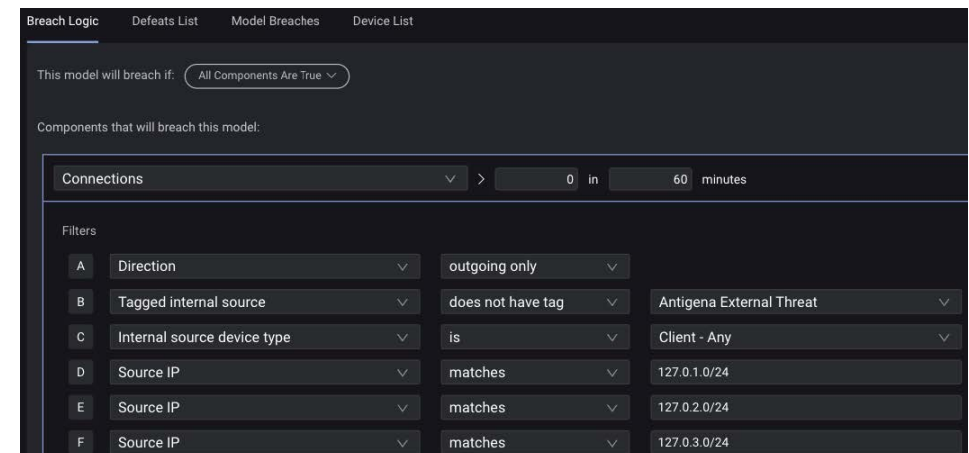
- a. To activate the Model, first click **Edit Model** in the top right before switching the **Active toggle to on**.



- b. **Turning it on and saving the changes** will make the Model automatically tag any devices it sees connections from in the IP address ranges specified in its component.



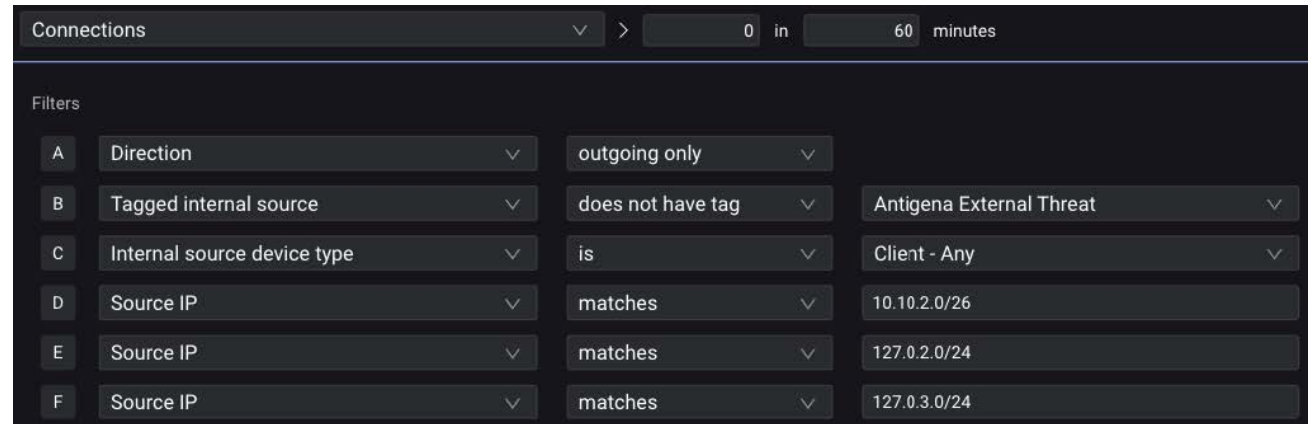
6. Confirm that the ranges in the **Breach Logic** component are **localhost ranges**. As localhost is reserved for internal loopback, this shouldn't affect tagging on the network until changed.



7. Tagging for Antigena Network

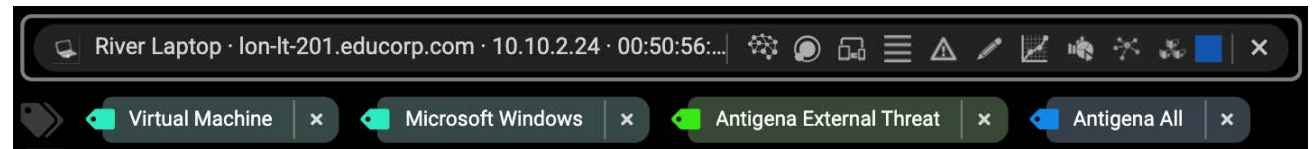
7. By changing one of the ranges in one of the **Source IP** filters to a **subnet on the network** and saving the changes, Darktrace will begin the Antigena Network External Threat tagging process.

For example, the example to the right shows that the first localhost range has been modified to the **10.10.2.0/26** range.

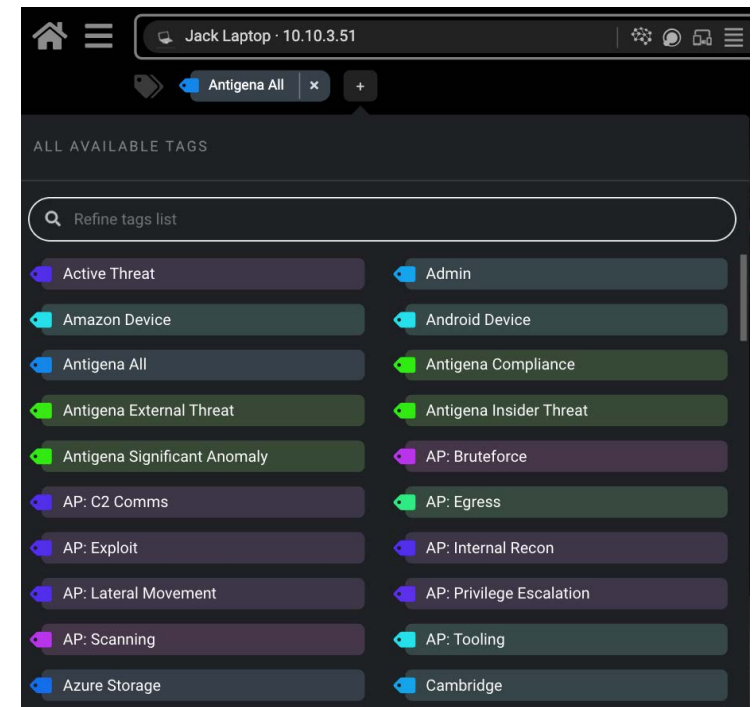
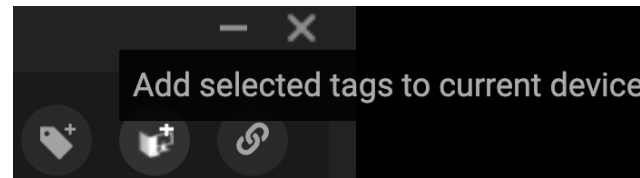


8. After a connection has been observed by a device on the established IP address range, the Antigena **External Threat** tag will be attached to that device.

This device will now be monitored and potentially acted on by Antigena Network Models looking for the Antigena External Threat tag, such as the ones in the External Threat folder.

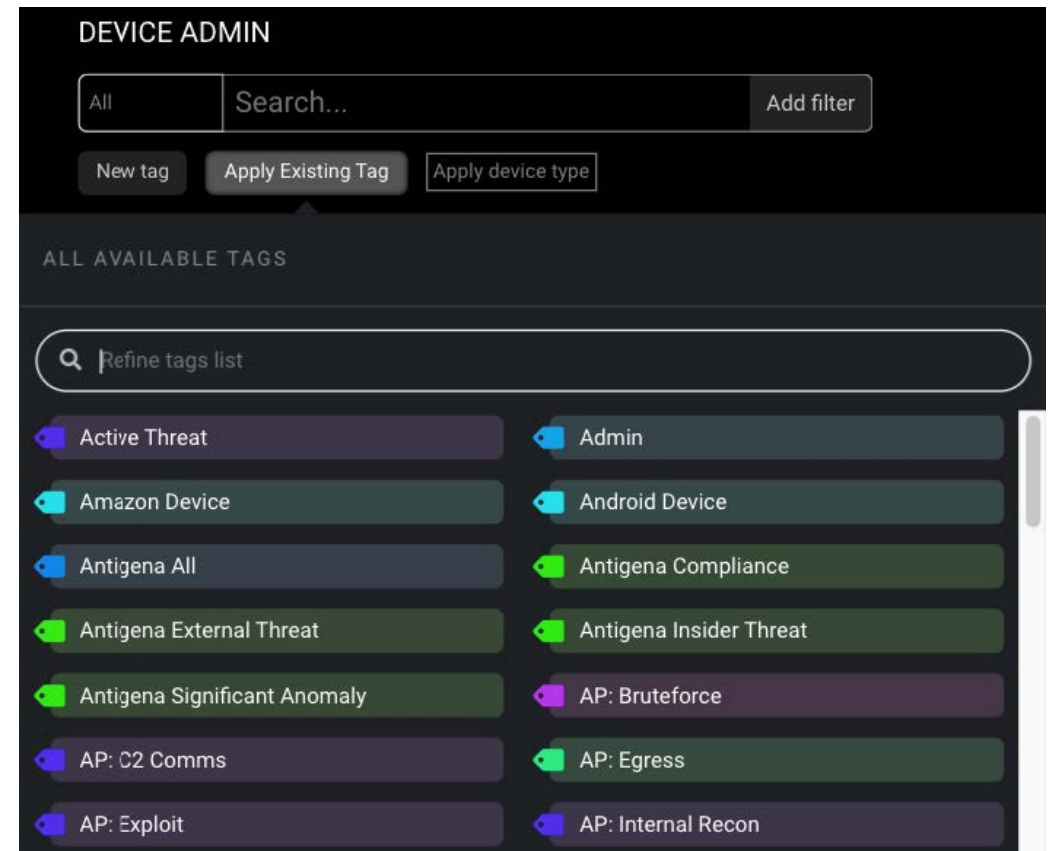
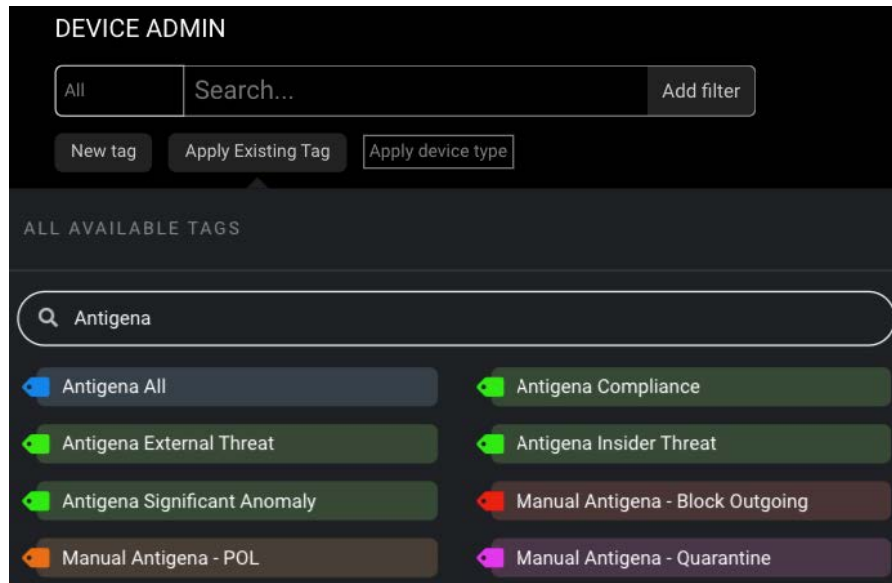


9. **Specific devices** outside of these subnet ranges can also be **monitored individually**.
 - a. With a device populated within the Omniseach bar, click the **plus (+) button** to apply a tag from a **drop-down menu** of all available tags.
 - b. Again, with the Omniseach bar populated with a specified device, open the **Tags Manager**. From here, **select a tag** and then click the **Add selected tags to current device** button.



7. Tagging for Antigena Network

10. It is also possible to attach tags individually or in bulk using the **Device Admin** page.
- a. Simply use the **search bar** to filter the devices displayed in the table, select the **Apply Tag** button and then **choose the tag** to be affixed to the devices.



- b. It is possible to select **individual devices** by clicking the **tick boxes** in the appropriate row, or the tag can be applied in bulk to **all devices** displayed on the page by clicking the tick box at the top of the **tick box column**.

The rows of devices which are tagged in this way temporarily inherit the colour of the tag.

| | LABEL | TYPE | HOSTNAME | TAGS |
|-------------------------------------|----------------------|------------|------------------------|---|
| <input type="checkbox"/> | | | | <input type="checkbox"/> Antigena All |
| <input type="checkbox"/> | Domain Controller 01 | DNS Server | | <input checked="" type="checkbox"/> DNS Server <input type="checkbox"/> |
| | | | | <input checked="" type="checkbox"/> Microsoft Windows <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | Clara Desktop | Desktop | lon-dt-102.educorp.com | <input type="checkbox"/> Antigena All |
| | | | | <input checked="" type="checkbox"/> Microsoft Windows <input type="checkbox"/> |
| | | | | <input checked="" type="checkbox"/> Domain Authenticated |
| | | | | <input checked="" type="checkbox"/> Virtual Machine |
| | | | | <input checked="" type="checkbox"/> Antigena External Threat <input type="checkbox"/> |

8. Recommended Deployment Schemes

GENERAL RECOMMENDATIONS **32**

USEFUL DEPLOYMENT SCHEMES **33**

Early Stage Deployment 33

Tuning the Deployment 34

Optimized Deployment 34

EXEMPTING USERS OR DEVICES **35**

General Recommendations

There are many ways to configure Antigena Network. The following are general recommendations to minimize misfires:

- We recommend that the deployment process is started in Human Confirmation Mode for the first month or two, with the end goal being an eventual switch to Active Mode.

This being said, some customers like to keep Active Mode for outside of work hours, such as evenings and weekends, with the added control of Human Confirmation Mode being there during work hours. This is another balanced approach that you can take.

- During this initial tuning and optimization phase, make sure you are happy with the Antigena Network breaches and that they are breaching in manageable numbers.

If there are too many, then it can be worth continuing this phase. Of course, the definition of a manageable number will change based on the size of your network.

- As mentioned in the tagging chapter, for particularly small networks, the Antigena All tag attached to all devices might be a viable approach, but for most networks a gradual step-by-step approach to tagging the network is usually preferred.

For larger networks, Antigena External Threat is an alternative starting point, which can be built on as time goes by.

- In the Antigena section of the System Config page, keep Block Server Devices to false so Antigena Network only runs on client devices. Once Antigena Network Model Breaches have been reviewed during the initial tuning and optimization phase, then it may be a good time to gradually introduce servers as necessary.





Useful Deployment Schemes

The following schemata are useful starting points when tuning Antigena Network and are based on different factors. Finding the best balance of simplicity and noise (the number of low-level potentially false-positive alerts) is an important consideration, especially as network size grows. Review the following options and evaluate which one provides the best balance for your deployment roll-out.



Early Stage Deployment

For a balanced approach when introducing Antigena Network into the corporate environment, it may be prudent to monitor the most severe activity on client devices. As such, the general recommendation is to apply the Antigena External Threat tag to all client devices for the first couple of months. This results in a manageable breach load for initial surveillance and scrutiny before tuning outwards. In early stages, Human Confirmation Mode is commonly used.

| | Antigena All | Antigena External Threat | Antigena Significant Anomaly | Antigena Insider Threat | Antigena Compliance |
|---|--|---|------------------------------|-------------------------|---------------------|
| Any Client device |  Networks < 1000 devices |  Networks > 1000 devices | | | |
| Specific Servers which do not interact with the whole network | | | | | |
| Client devices tagged by specific role (e.g. Sales, Finance) | | | | | |

Small Networks

For small networks, where the device count is below 1000, the simplest scheme is to apply the Antigena All tag to all client devices. For larger deployments this may cause noise, but for small networks where the breaches can be reviewed, Antigena Network can be entirely manageable when using Human Confirmation Mode.

Tuning the Deployment



After the External Threat tag has been applied, other Antigena specific tags may also be appended to devices to give a more comprehensive coverage of client devices, focusing on areas which may be of interest. For example, the Compliance tags may not be relevant for some deployments, but depending on your internal policies, may be appropriate and could provide enhanced visibility and enforcement. Overall, utilizing device tags to tune the deployment often provides a smooth transition from Human Confirmation Mode into Active Mode.

Eventually, once client devices have full coverage, following some configuration, specific servers may also have Antigena tags. This will apply a proportionate action if the server is observed triggered high severity breaches.

Optimized Deployment

This final scheme may take time to set up and should depict Antigena Network at its optimum level of performance. It is recommended to continually monitor Antigena Network and tune it over time to suit the network environment.

In this scheme, the tagging of client devices has been customized based on the role which a device takes within the company, or the subnet that it belongs to. For example, the finance team might perform duties that exempt it from certain compliance policies, and therefore the tagging might reflect this. Individual Antigena Network Models could be updated to exempt devices with particular tags that mark their corporate department.

| | Antigena All | Antigena External Threat | Antigena Significant Anomaly | Antigena Insider Threat | Antigena Compliance |
|---|----------------|---|---|-------------------------|---------------------|
| Any Client device | | | | | As appropriate |
| Specific Servers which do not interact with the whole network | |  |  | | |
| Client devices tagged by specific role (e.g. Sales, Finance) | As appropriate | As appropriate | As appropriate | As appropriate | As appropriate |

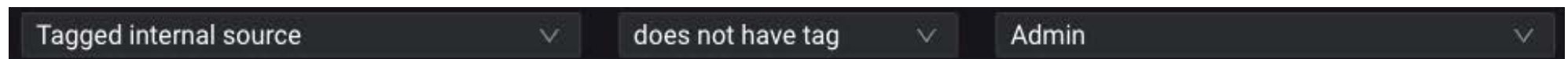
Exempting Users or Devices

When initially configuring Antigena Network, or after reviewing the resulting breaches and actions, you may wish to remove key devices from Antigena Network monitoring.

A common example is that members of the IT Security team often perform different sets of activity from regular network users and are therefore more likely breach Darktrace models. For instance, they could carry out port scans as part of network health and compliance checking. Exempting their devices can have a significant impact on reducing model breaches and actions.

Here are some ways you can accomplish this:

- By making sure the devices do not have any Antigena tags on them. You may have to edit the automatic tagging Models to exempt devices with the **Admin tag** on them by applying an additional filter in the Breach Logic Components.



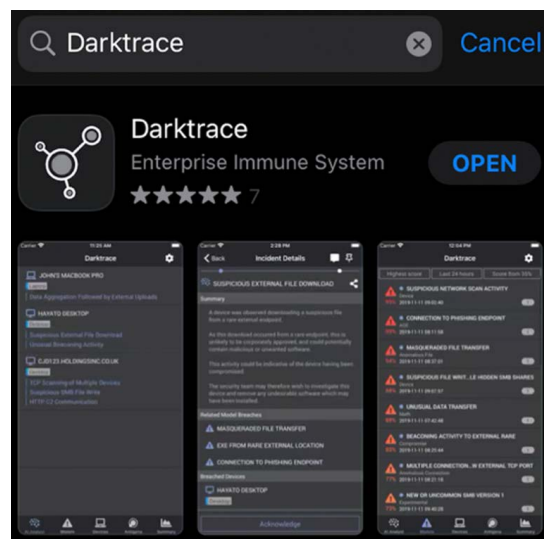
- Making sure such administrator devices are tagged with the correct Threat Visualizer tags can help in the first place, since this will exempt them from more standard Enterprise Immunes System Model Breaches which make up the basis for detection in many Antigena Network Models.
- Furthering on from the second point, tuning and optimizing the Darktrace Enterprise Immune System in general, especially for IT team devices, will have a positive knock on effect on the accuracy of your Antigena Network deployment.

9. Mobile App Antigena View

The Darktrace Mobile App can be used to manage Antigena Actions on the go. Any decisions made in the Mobile App will be mirrored in the Threat Visualizer.

For the purposes of this manual, it is assumed that the Mobile App has already been configured within the System Config page and has been downloaded and registered in the Account Settings.

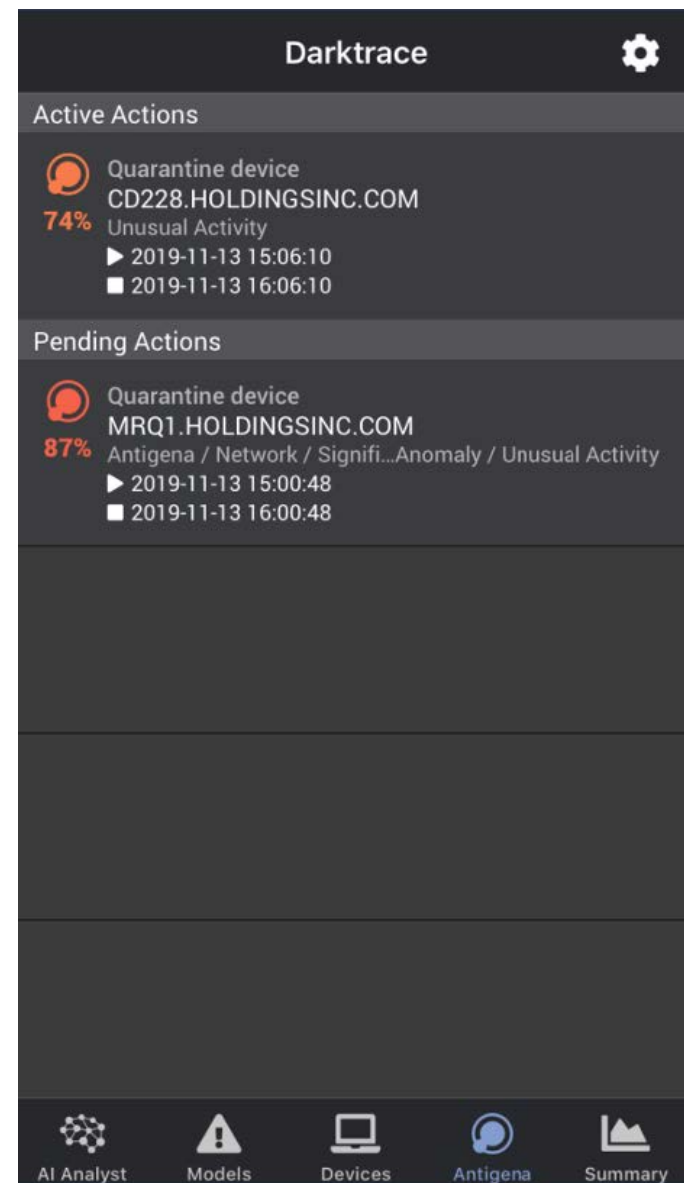
For more information about setting up this app, refer to the Customer Portal Product Guides.



1. The **Antigena** screen of the Mobile App displays recent Antigena actions listed by category; **Active**, **Pending**, **Cleared** and **Expired**.

Note that **Active** devices are currently being controlled by Antigena whereas **Inactive** devices are not being controlled by Antigena.

2. Tap on an **individual Antigena action** to review details of the device, the Model that prompted the action and the timing of the Antigena action.
3. **Swipe left** on an Antigena Action to open up more options, allowing for changes.
 - a. **Extend** will lengthen the Antigena action on the device for the specified time.
 - b. **Activate** will inform Antigena to start controlling the device with the specified action.
 - c. **Clear** will inform Antigena to stop controlling the device.
4. Tap the desired action to provide **time options** for how long the Antigena Action should be Extended, Activated or Cleared for.
5. **Swipe left** again to activate the right-hand option.



10. Learning Outcomes

Course Agenda Checklist

Thank you for completing this course on Antigena Network.

We hope this have given you the confidence to tackle a variety of aspects within your deployment.

Contact Us

For all further education inquiries, contact:

EMEA: training-emea@darktrace.com

APAC: training-apac@darktrace.com

US/LATAM: training-amer@darktrace.com

For technical support with your installation, go to <https://customerportal.darktrace.com>

When contacting support, please make sure you provide as much detail as possible.

Complete the learning outcomes checklist below:

+ I can configure Antigena Network options

+ I know how to schedule Antigena Network modes

+ I have an understanding of Antigena Network Models

+ I am able to tag devices for monitoring by Antigena Network

+ I can handle Antigena Network actions raised by Darktrace