DARKTRACE

THREAT VISUALIZER ADMINISTRATION

Threat Visualizer Administration Training Manual
Manual v2.2.0 – Darktrace v5

Table of Contents

1. Learning Objectives

This course provides instructional workflows on how to configure the Darktrace Threat Visualizer. It is designed specifically for IT Administrators needing to oversee the set-up and maintain the administrative and system sides of Darktrace.

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

+ Understand Darktrace data capture
+ Understand how to configure subnets and optimize devices
+ Assign permissions and groups to users
+ Follow the Audit trail
+ Check the health of appliances through the System Status
+ Feel comfortable with deploying SaaS connectors
+ Configure different types of alerts
+ Understand how to integrate alerts with SIEMs and use the API
+ Set up the Darktrace Mobile App
+ Configure HTTPS Certificates
+ Create and restore from backups
+ Upgrade the Darktrace Appliance and Model Deck

2. Data Ingestion

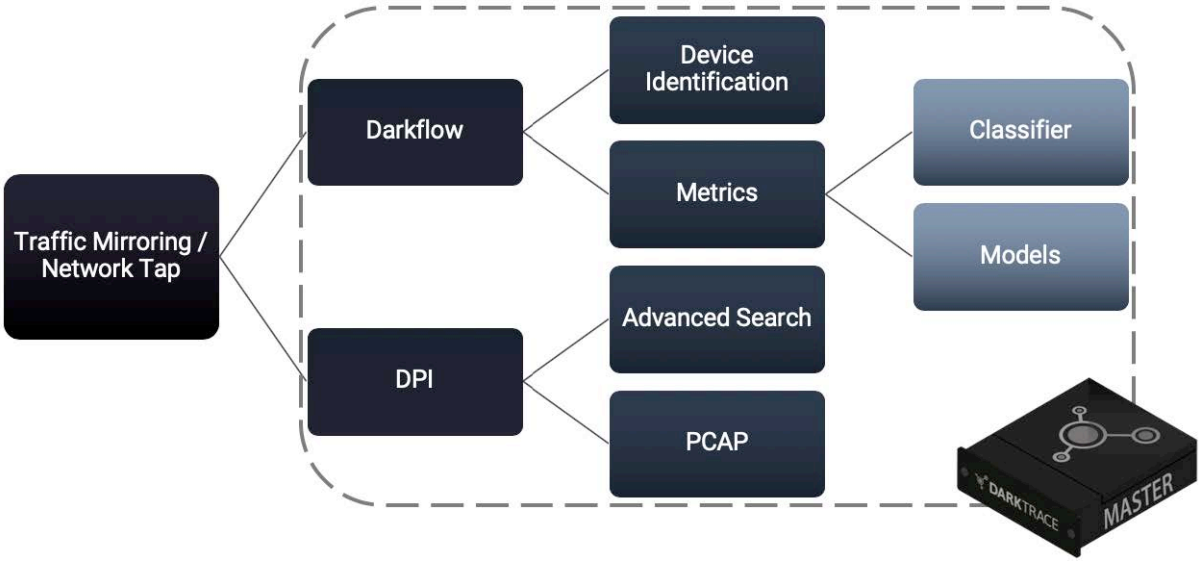
As network traffic is ingested into the Darktrace appliance from traffic mirroring techniques such as SPAN or Tap, it is divided into two areas: Darkflow and Deep Packet Inspection (DPI).

Darkflow is similar to Netflow as it extracts connection data such as ports, IP address and protocols. However, it is more advanced than Netflow as it more accurate and supports connections for longer periods of time. Darkflow automatically produces hundreds of Metrics which are saved to the appliance. The data is automatically classified and compared to a series of Models to map the network behavior and search for potential anomalies and threats.

The ingested network traffic is also saved for use in the Advanced Search application and for further packet inspection. Depending on the protocol employed, a part of every connection is stored for deep packet inspection on a rolling buffer.

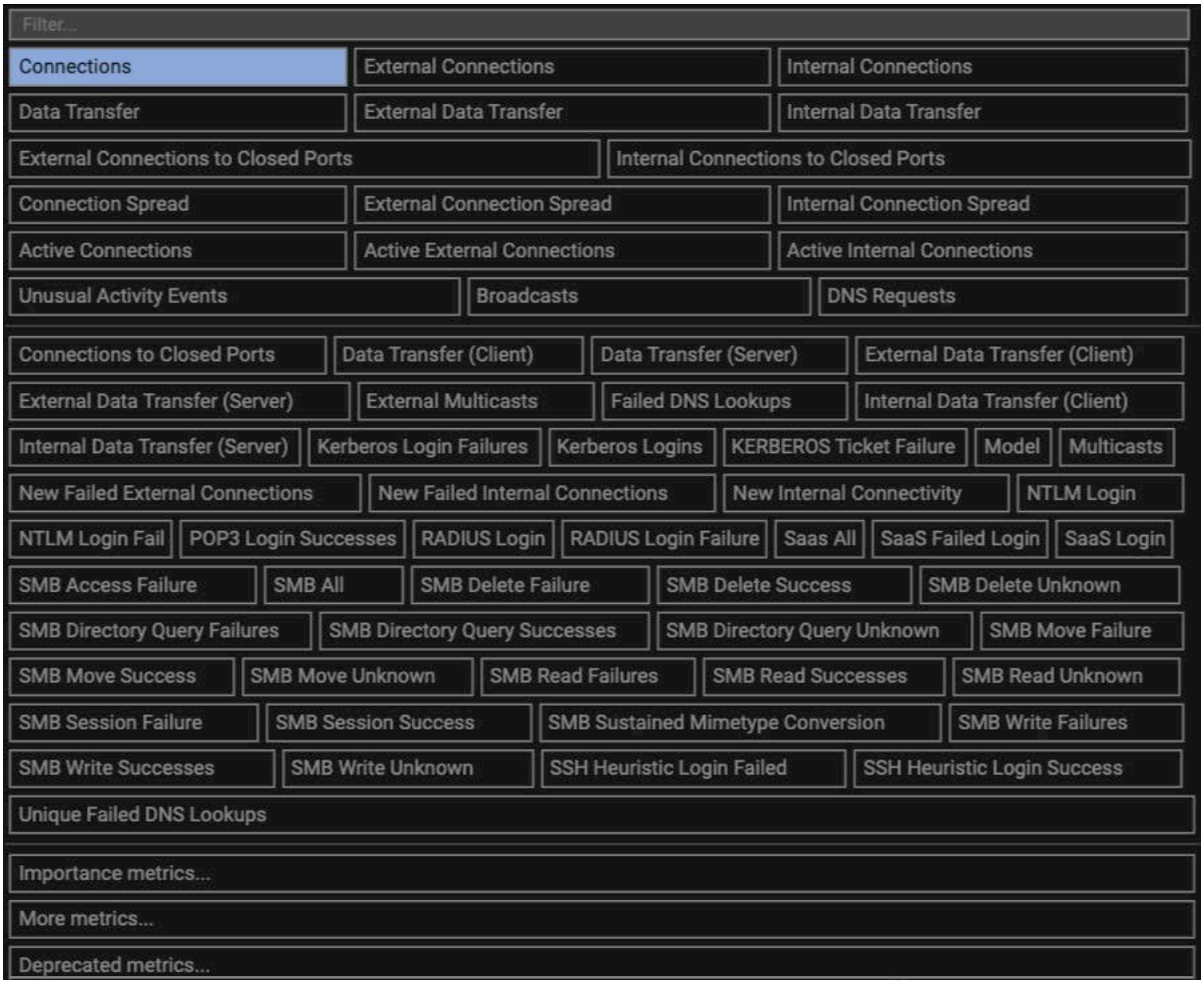
For encrypted TLS/SSL traffic, this may just contain the source, destination, time and size of the transfer. However, for HTTP, this can include a large portion of the webpage, which can facilitate investigation and forensic analysis. The Packet Capture (PCAP) data is typically opened in Darkshark or Wireshark applications to help navigate and understand the data quickly and easily.

The following diagram explains how network traffic is stored and processed through the Darktrace appliance.



Metrics

Darkflow produces a wide range of different Metrics, which are utilized to detect network anomalies and threats.

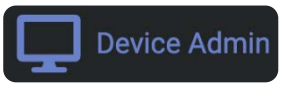


Mapping Data

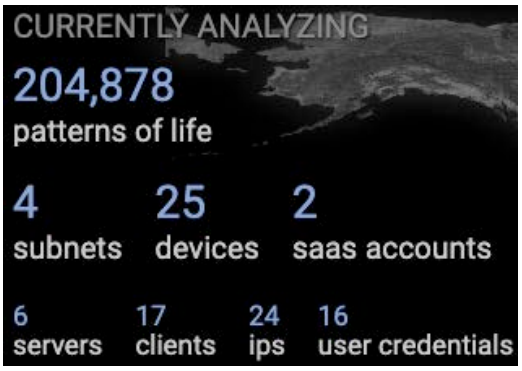
Mapping data is a subset of the data ingested by Darktrace and enables Darktrace to track devices as they move around a network. This is especially important in the analysis of user devices since these will typically have dynamically assigned IP addresses. Mapping data usually takes the form of DHCP events seen in transactional data provided by legitimate corporate DHCP servers. These are automatically ingested, and the tracking of devices is seamlessly handled by Darktrace. Other forms of mapping data may be used, depending on your specific environment.

3. Device Admin

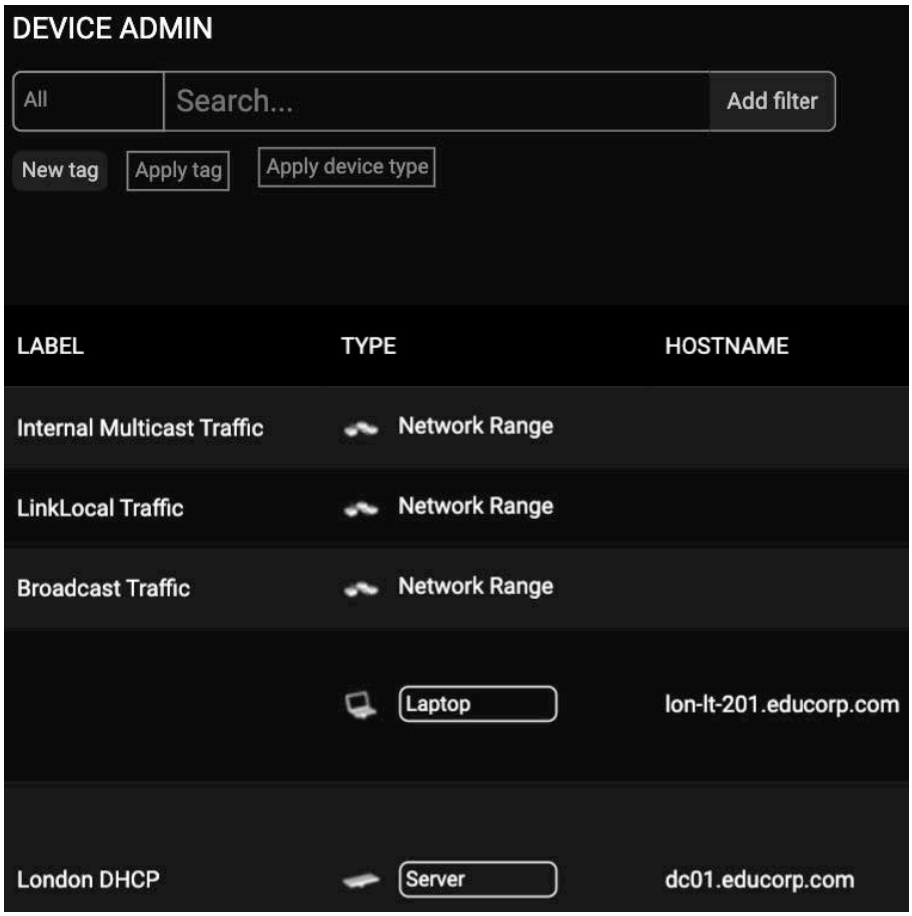
1. Under the main menu, hover over **Admin** and select **Device Admin.**



Alternatively, click the **number of devices** in the summary view to reach the same page.



2. This will open the **Device Admin** interface in a new tab. It lists all the devices which have ever been observed on the network since Darktrace was installed.



For each device on the network, the Device Admin page tabulates the: Label, Type, Hostname, Tags, MAC Address, Vendor, Operating System, IPs, Priority and the dates where the device was first and last seen on the network.

3. The columns displayed can be limited. Click **Edit columns** and deselect the columns as desired.

With columns deselected, the table will change. The workspace can be easily reset to show the default columns by clicking the **Show all** button.

4. **Labels** are nicknames for devices. Examples may include short descriptions to help understand a device's key function, such as DC1, Antivirus, or Darktrace. Labels are particularly useful if hostnames lack clearly defined naming conventions. It is not necessary to label every device, but it is recommended to name key servers or devices, especially those which often cause model breaches.

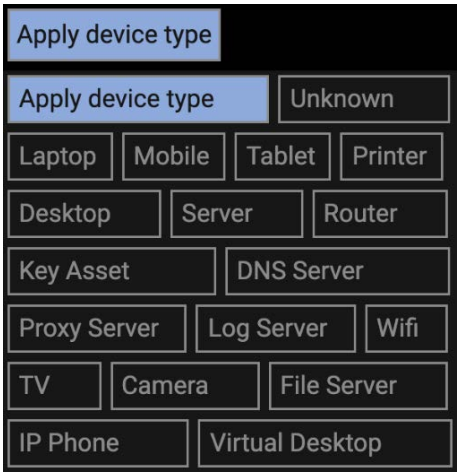
5. **Type** is like providing a category for a device. By analyzing the data flow, the Darktrace appliance will automatically predict the type of device, but it can also be manually set.

   For example, a device which receives connections on Port 53, is likely to be the Domain Name server. It is important to set the correct type so correct mathematical Models are employed to evaluate a device's behavior.

   The device type can be set manually in the Threat Visualizer with the device populated in the Omnisearch bar.

   However, to apply device types in bulk, utilize the drop-down menu by clicking **Apply device type**.

   Choose a device type and click the tick boxes to the left of the devices to assign the selected type.



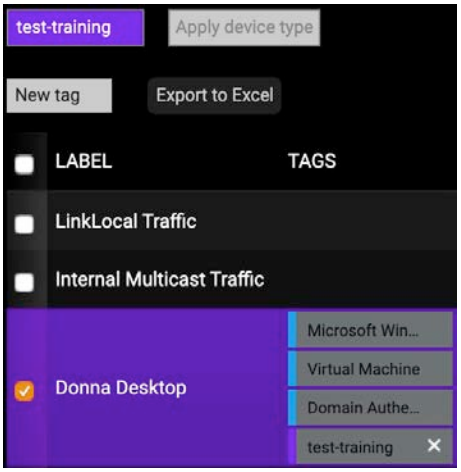
6. **Tags** are like roles for devices. They can be used to group similar devices together. Examples of Tags included DNS servers or Security devices. Tags are defined to facilitate searching for devices and tuning models to only fire if a tag has been set.

   a. To apply a Tag to devices, click **Apply tag** at the top of the screen. This will open a selection of available Tags.

   b. Once a Tag has been selected, click the **tick box** next to the devices to be tagged. This will highlight the row in the Tag color.

   c. Click the **New Tag** button to open a New Tag dialog. Upon creation, the Tag will be available in the menu of available Tags.



7. **Priority** is a method to boost the threat score of a device. By setting a high positive number, devices can be given a higher score. This denotes that a device has a greater priority for analysts when reviewing the model breaches. Priority values are discussed in more detail later in training.

8. At the end of every column, there is a **View device notes** button. This could be useful, for example, to input notes if a device requires more description than can be entered in the label. Click this and enter text in the dialog to add notes.

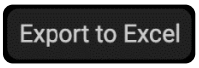
Devices which already have notes can be identified by a similar icon which contains an orange circle.

9. The final icon at the end of a row is a magnifying glass. Click this to **open the device in the Threat Visualizer**.

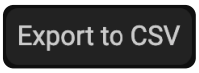
10. Device Admin is also useful to quickly find out how many devices are on the network, including legacy devices.

The **search bar** helpfully filters down the results displayed. Try searching for **DNS** and review the results.

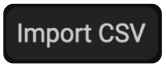
11. The results in this page can be exported in multiple formats. First, there is the option to **Export to Excel**, which will export a copy of the table into a spreadsheet.



12. Also, the contents of the table can be exported to CSV format. Click **Export to CSV** to obtain this file type.



13. The results can be updated by importing a **CSV file**:



a. Click **Import CSV**.

b. **Choose a file** of CSV format to upload.

Note: *Only the Label, Type and Priority columns can be modified in the Device Admin page by changing the values in the CSV file.*

Configure the Device Type

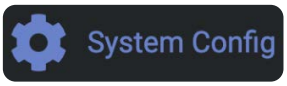
Darktrace will analyze the behavior of all devices and determine, based on each device's network behavior, whether it should be classified as one of two default device types: Client or Server.

Similar to the method used in the Device Admin page, a more granular type can be set for devices in the Threat Visualizer. For example, a device type can be changed from Desktop to Laptop, Router or Tablet. These distinctions help when investigating threats and analyzing network's activity.

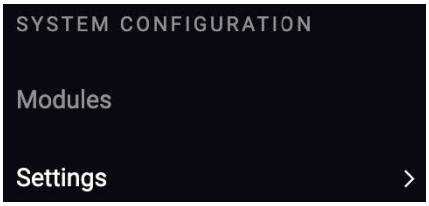
There are two additional methods of changing the Device Type:

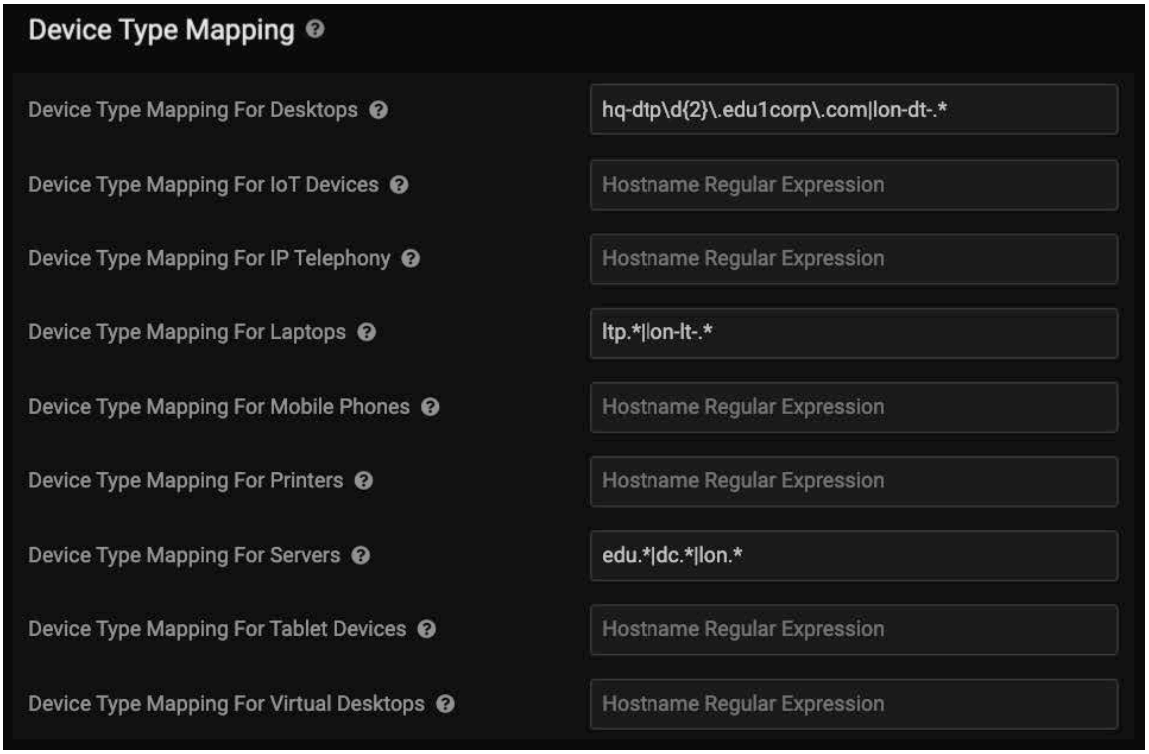
- **On the Configuration Page:** You can set the hostnames that Darktrace should expect to see for: Desktops, IP Phones, Laptops, Mobiles, Printers, Servers and Tablets.
- **In the Model Editor:** If you desire to be more granular, you can create a model where the Action of the model, if conditions are met, will be to change the device type.

1. If device hostnames follow a naming convention, it can be entered in the **System Config** page, found in the Threat Visualizer main menu.



2. Within the System Configuration page, navigate to **Settings**.
3. Locate the **Device Type Mapping** section to set the device types using text or regular expressions.





For example, the type, laptop, can be assigned with the following expression:

(lap|lp)[0-9]{5}.*

This checks for hostnames that begin with lap or lp followed by 5 numbers between 0 and 9. The .* acts as a wildcard to allow any additional characters.

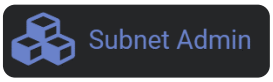
4. Further examples using regex are displayed in the table to the right.

   This takes effect **when the device is next seen** and will be applied to future devices as well.

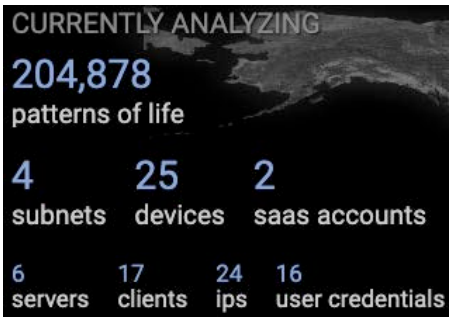
SET	Regex Value
Hostnames For Desktops	(mac|w7)-dsktp.+\.darktrace.corp
Hostnames For IP Phones	voice.+\.darktrace.corp
Hostnames For Laptops	(mac|w7)-.+\.darktrace.corp
Hostnames For Mobiles	iphone.+\.darktrace.corp
Hostnames For Printers	print.+\.darktrace.corp
Hostnames For Servers	srv\.dc(1|2).+\.darktrace.corp

4. Subnet Admin

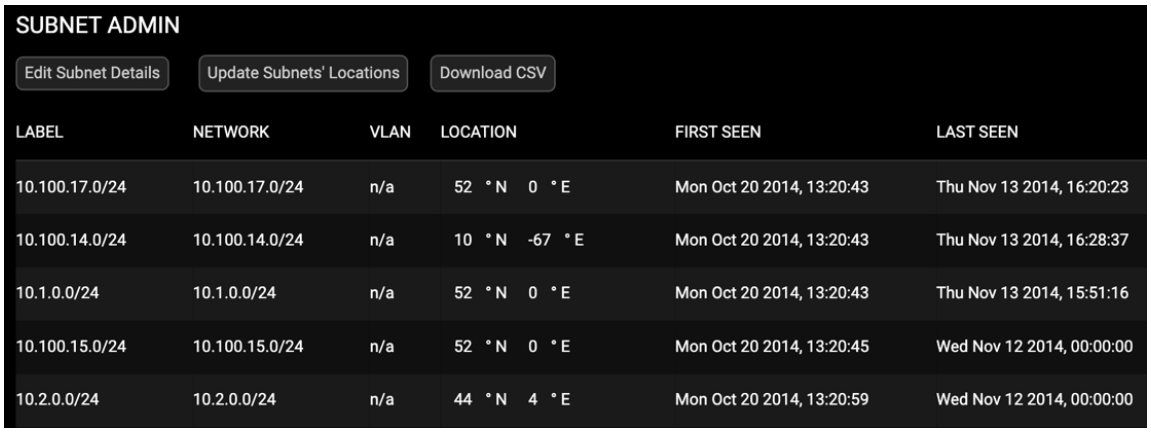
1. Review the **Subnet Admin** page, also found by navigating through the Admin menu.



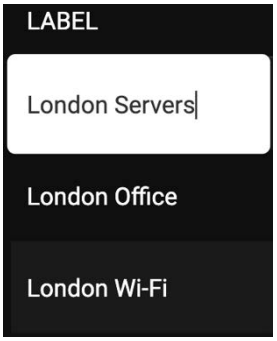
The alternative way to reach this page is to click the **number of subnets** in the summary view.



2. The Subnet Admin page has a **table** containing the **network ranges** and a plethora of useful information. By clicking the **headings**, the columns can be ordered in ascending or descending order.



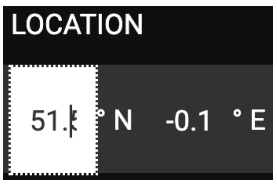
3. By labeling subnets on this page, it can make reading network diagrams much easier.



To add a **label**, click a network range and type in a nickname.

These values will then be searchable in the Omnisearch bar and will be presented in the Subnet View.

4. Setting the geographical coordinates will set the correct **location** for subnet cubes on the world map.

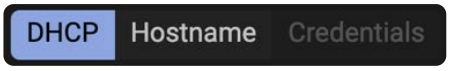


Click on a latitude or longitude number to edit the selected coordinate.

5. To update the latitude and longitude of multiple subnets, click the **Update Subnets' Location** at the top of the page.

A dialog will replace the button which allows the location for subnets matching an inputted range to be updated in bulk.

6. To enable Darktrace to best understand the network, **it is important to configure how the subnets should be tracked**.

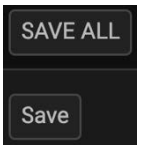


   Most regular dynamic subnets are fine using the DHCP option, but this option should be removed for static subnets.

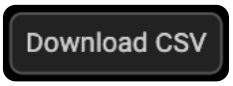
7. From this page, connections to or from devices within this subnet will be included as indicated by the **plus** button. For example, some SOC teams may not be interested in monitoring activities originating from their guest Wi-Fi subnets or others, such as Developer networks.

   To prevent Darktrace tracking and triggering model breaches in a Subnet, click the **tick** button.

8. It is possible to **Save** each row individually as manual changes are being made. However, if multiple rows have been changed, utilize the **Save All** button.



9. To download a copy of the current Subnet Admin table, click **Download CSV**. This will allow easy editing, or it could be useful to maintain a copy of the original table.



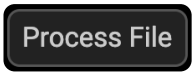
10. Rather than editing details from the Subnet Admin page, it is possible to upload an existing CSV file. Click Edit Subnet Details.

    a. A **Choose Files** option will become available.

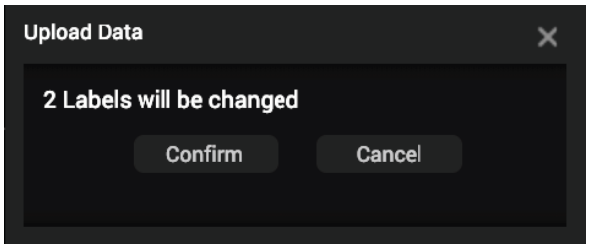
    Darktrace will accept CSV files in the same format as the CSV file that can be downloaded from the Subnet Admin page.

    Note: *It is possible to upload network ranges for subnets that are currently unseen in Darktrace in order to pre-define labels.*

    b. Once a file has been selected, a **Process File** button will appear.



    c. When the file has been processed, a prompt will appear **detailing the changes** that will be made. Click **Confirm** to proceed.



5. Device Tracking

Darktrace models every internal device that it observes on a network by analyzing every single packet to determine its source and destination. Each packet must be tied back to the same device every time.

The most reliable method to track IP addresses is by assigning devices with static IP addresses. This also means no configuration is required to instruct Darktrace how to model servers or devices that are static. However, in an increasing world of IoT, there may be thousands of IP addresses in use day in and day out that are having their IP address assigned dynamically, via DHCP. In the Threat Visualizer interface, there are multiple methods to track dynamic IP addresses. The most suitable method depends on the scenario and network traffic available.

Tracking by DHCP

Tracking by DHCP is the most reliable and preferred method to track IP address changes and is enabled by default.

To access a network, a device must begin by sending a DHCP ACK request. The DHCP ACK packet contains two necessary ingredients for Darktrace tracking: The device's assigned IP address and the device's MAC address. Darktrace will dissect this packet and extract the MAC address. As the MAC address will not change, it can be used as a unique identifier and is therefore the most trusted source for dynamic IP address tracking.

This method can mean a device such as a laptop can be displayed twice in Darktrace. One device for the connection via a physical Ethernet cable, and another for the Wi-Fi network card. Differentiating the two can assist Darktrace learn a pattern of life for a device. For example, typically a user's behavior can be very different on their Wi-Fi when compared to a wired connection. They may check their social media on public Wi-Fi, but never on the corporate LAN.

Tracking Devices by Log Input

When DHCP or Kerberos cannot be retrieved, DHCP or VPN logs can be sent to Darktrace to be parsed. Log Input allows custom log data to be read into Darktrace and map it to existing devices using the IP or MAC address. Assuming there is little delay retrieving uploaded information, it can be a very accurate method of tracking devices. This feature is most commonly used to provide device tracking information, but it can also enrich Darktrace data.

Users who log into the network remotely, via VPN, should be tracked via their credentials as their IP addresses will constantly change. Darktrace may never see the hostname for the device and entering credentials will always be the first thing that a VPN user needs to do before getting onto the network. For this, Darktrace can ingest VPN Logs that can be parsed to grab the user's internal IP address in use and the user associated with the traffic.

DHCP and username data is used to assign hostnames, IP addresses, or credentials to devices. Event data is used to add custom events into Darktrace. Note that this data will not be added to Advanced Search.

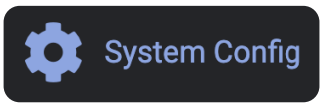
Logs should be sent in syslog format. Encrypted and unencrypted log ingestion is available along with multiple forwarding methods. Darktrace provides support for multiple log feeds into an appliance:

Port	Protocol	Receiver	Encryption	Propagation
1514	UDP or TCP	Master or Subordinate Master	Unencrypted	Will not propagate to other masters.
1514	UDP or TCP	vSensor (4.0.7+)/ Hardware Probe	Unencrypted	Forwarded to associated master appliance.
2514	UDP or TCP	Unified View	Unencrypted	Propagated to all subordinate masters.
6514	TCP	Master or Subordinate Master	TLS / SSL	Will not propagate to other masters.
6514	TCP	vSensor (4.0.7+)/ Hardware Probe	TLS / SSL	Forwarded to associated master appliance.
7514	TCP	Unified View	TLS / SSL	Propagated to all subordinate masters.

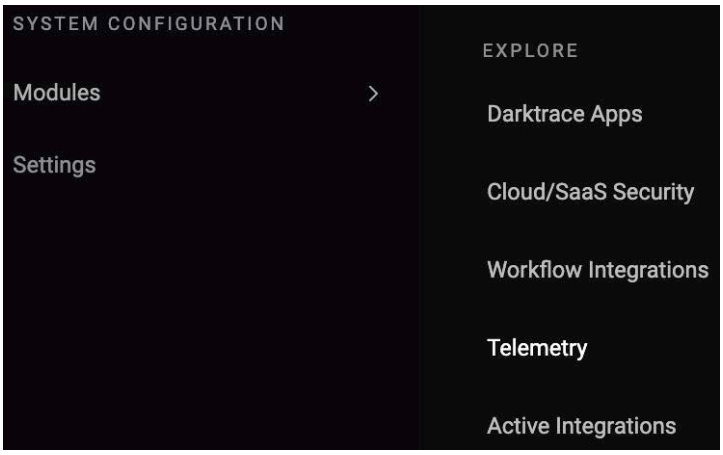
In addition to processing and transmitting network traffic, hardware probes and vSensors are able to ingest and forward syslog format logs to the Darktrace master. Pattern matching is configured on the master and propagated to the vSensor. Matching/Discarding is performed at the vSensor level where valid matches are then forwarded to the master.

1. Configure the **external device** to send syslog to a Darktrace master appliance or probe (vSensor or hardware) in the desired port/protocol combination, as outlined in the table above.

2. From the Darktrace master appliance intended to receive the logs, navigate to the **System Config** page from the Admin section of the Threat Visualizer Main Menu.

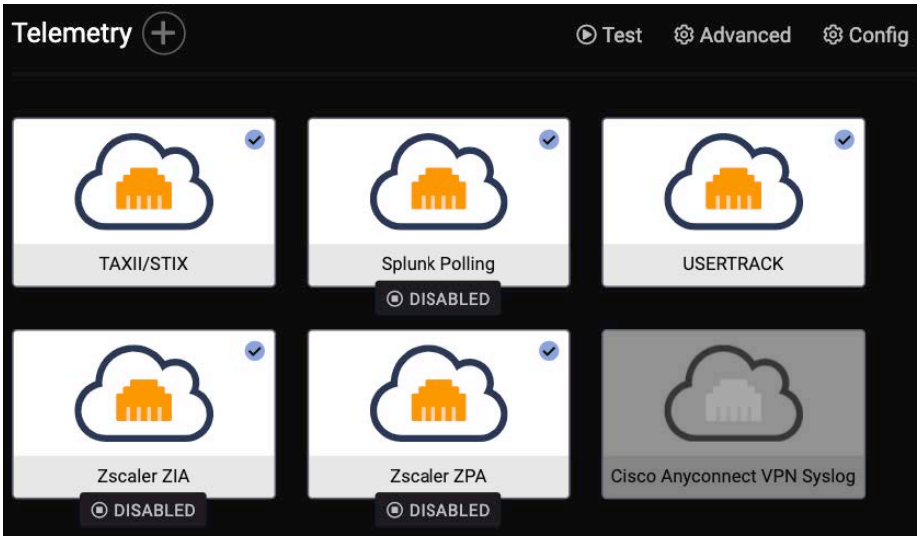


Select the **Modules** option from the left-hand menu.

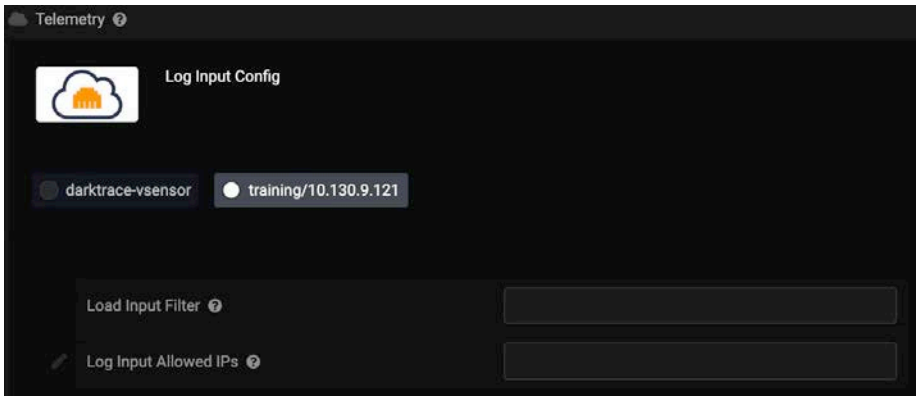


3. Locate the **Telemetry** section of the Modules layout.

4. From the top right-hand corner of this section, next to the Test option, select the **Config** button.

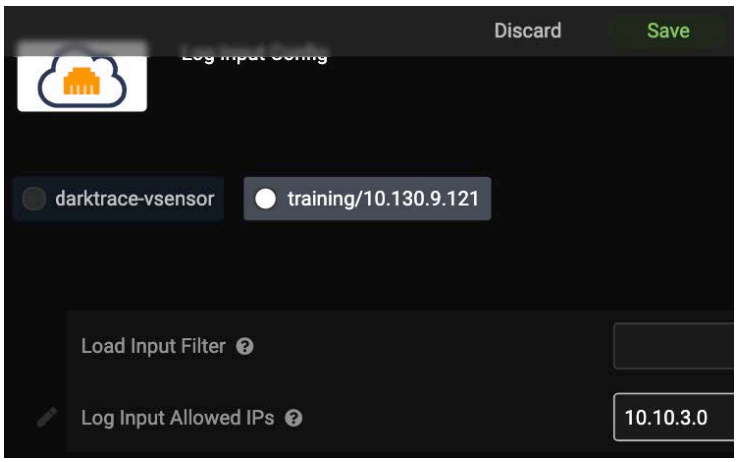


5. A new dialog will open. Within this dialog, select the **appliance or probe** which the logs are being sent to.



6. In the **Log Input Allowed IPs** field, enter the IP address of the device sending syslog.

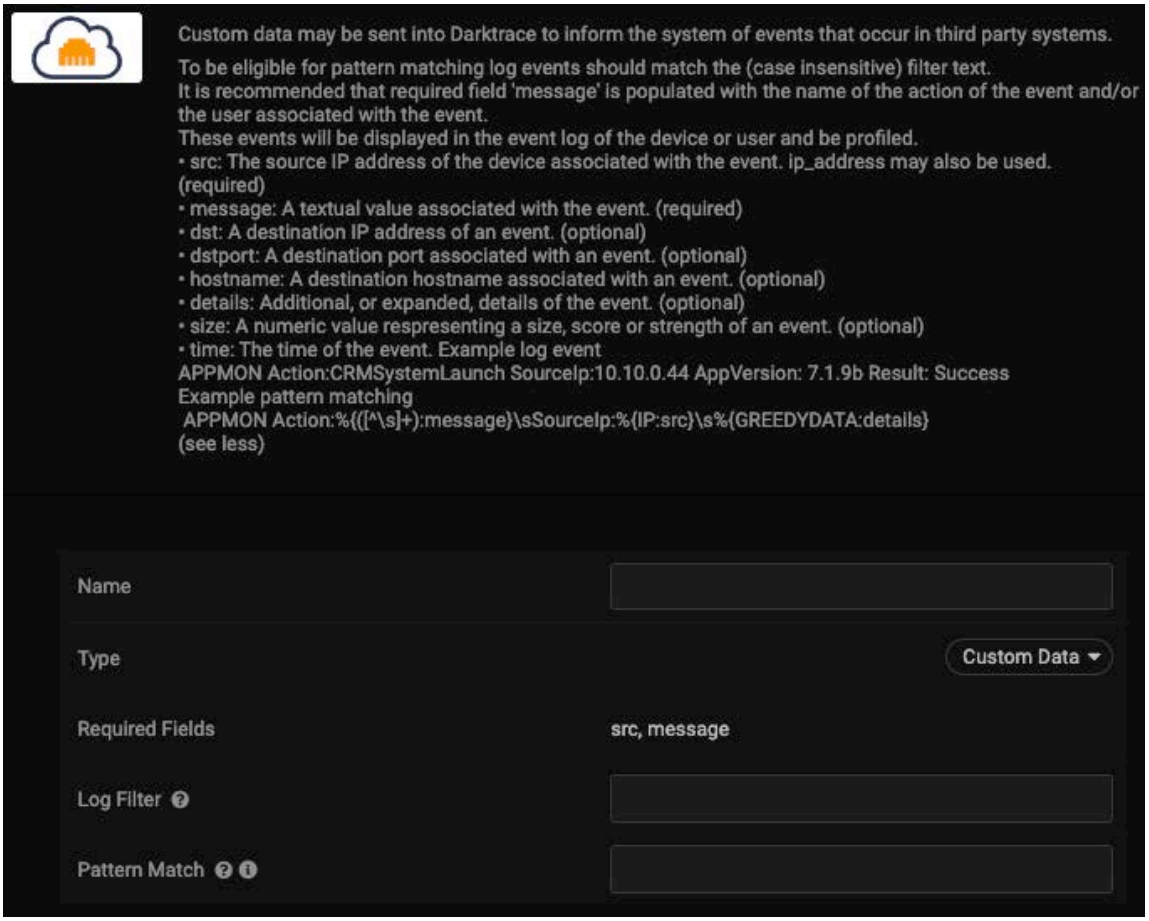
   Save any changes using the button at the top of the dialog.



7. In order for logs to be parsed, a **template must now be defined**. To begin this process, exit the Config dialog.

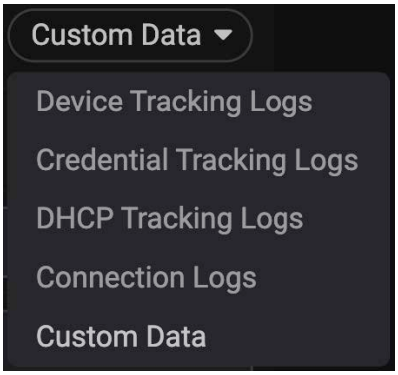
8. Next to the **Telemetry** heading, click the **plus** icon.

9. A new **dialog** will open, allowing a **template** to be defined. Matching patterns are used to extract relevant data from syslog format log entries or outputs from log polling integrations. Log entries are matched against each applicable configured pattern until a match is found. Once a match is found and data is extracted by the associated pattern, no further pattern matching will be attempted. Each template has a name, a type, a filter and an extraction pattern.



a. Begin by naming the event ingestion by entering a value into the **Name** field.

b. The **Type** drop-down menu has a range of data types available.



Selecting one of the pre-defined data types will change the description as presented at the top of the dialog window. It will also change the values stated in the **Required Fields** which must be mapped.

c. Each template requires a filter in the **Log Filter** field. This is usually a keyword which appears only in the entries intended for parsing by the template. Darktrace will only attempt to match the template to log entries that contain the filter. The filter does not affect the data that can be included in the pattern and can refer to data at any point in the log body.

d. The extraction pattern, as input into the **Pattern Match** field, will define how the log entry should be parsed. Patterns are constructed with Grok syntax. Click the tooltip icon next to the Pattern Match field to review built-in patterns.

   Grok patterns are used to extract values into a number of named fields using the syntax %{PATTERN:field} . PATTERN must be one of the built-in shortcut strings or a regular expression surrounded by parentheses. Multiple patterns can be configured, each one mapping to a named type. Patterns can use **perl** compatible regular expressions or one of a number of built-in shortcuts as shown in the examples below.

   > *Grok is a simple software that allows logs and other files to be easily parsed. With Grok, it is possible to turn unstructured log and event data into structured data. The Grok program is a tool for parsing log data and program output. It can match any number of complex patterns on any number of inputs (processes and files) and have custom reactions.*

Note: *Log input configured before v4.1, or configured on the legacy config page, must include the relevant 'type' pattern in the naming syntax. This is no longer required when configuring ingestion on the new System Config page.*

Worked Example

It is useful to have example entries of the format to be parsed to use when testing and refining the pattern.

The following log line is an example VPN server log and is intended for use in a subnet tracked by credentials.

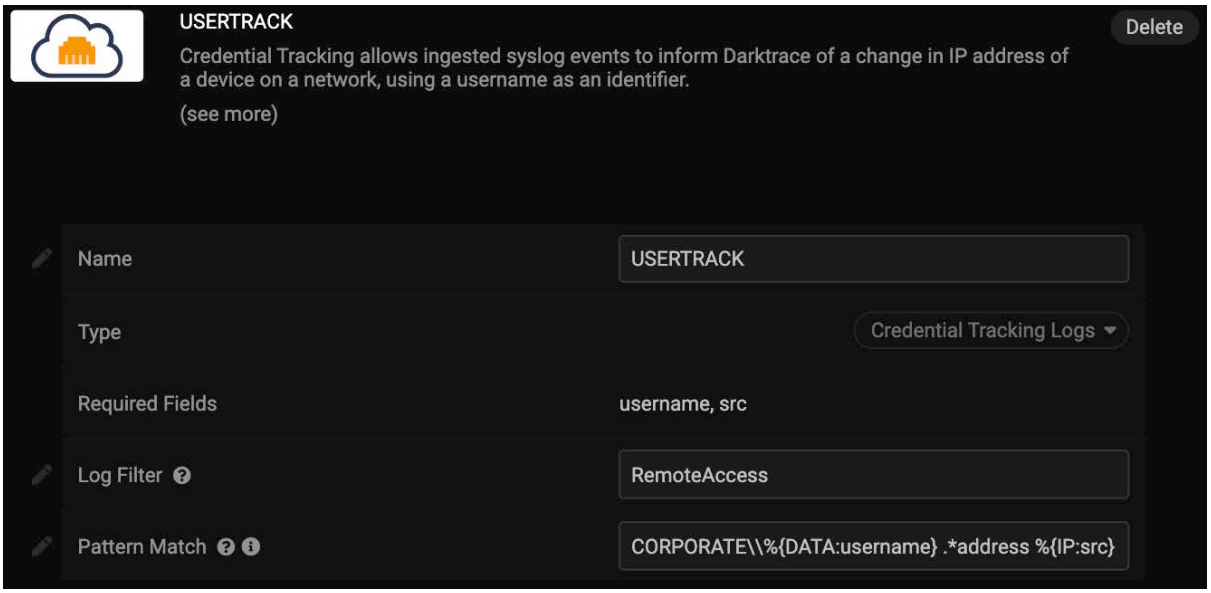
```
Information15/06/2020 09:41:16RemoteAccess2027 The user CORPORATE\Amy.Pond connected on port VPN1-440 has been assigned address 192.10.88.2
```

To parse this log, we need to create a template with the Credential Tracking Logs type. The information in this log can be gained when a user remotely accesses the network, so **RemoteAccess** can be used as a filter.

Credential tracking logs require a username and IP address, as indicated by the username and src required fields. It is also possible to obtain a timestamp, but this is optional. The following pattern should extract the username and IP address:

```
CORPORATE\\%{DATA:username} .*address %{IP:src}
```

The example above will take any log that contains RemoteAccess. In this case, it will look for a string of the form CORPORATE\username, where the username part of the string will be assigned to the username value. It will then look for the value for the source address and will return an IP address that matches the IP syntax.

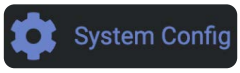


Once a template has been configured and saved, use the Test functionality to compare log lines with the configured pattern. Input can be loaded from lines seen or pasted into the field.

Encrypted Log Input TLS Certificates

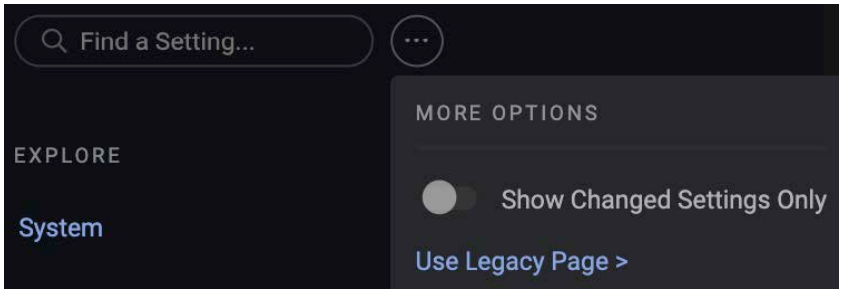
Encrypted log ingestion uses a default self-signed TLS/SSL certificate. If it is required by your syslog forwarder, the SHA1 and SHA265 fingers of the current certificate are available in the tooltip of the **Syslog TLS Certificate** field in the legacy System Config page. From this legacy view, it is also possible to add a custom certificate.

1. Navigate to the **System Config** Page.



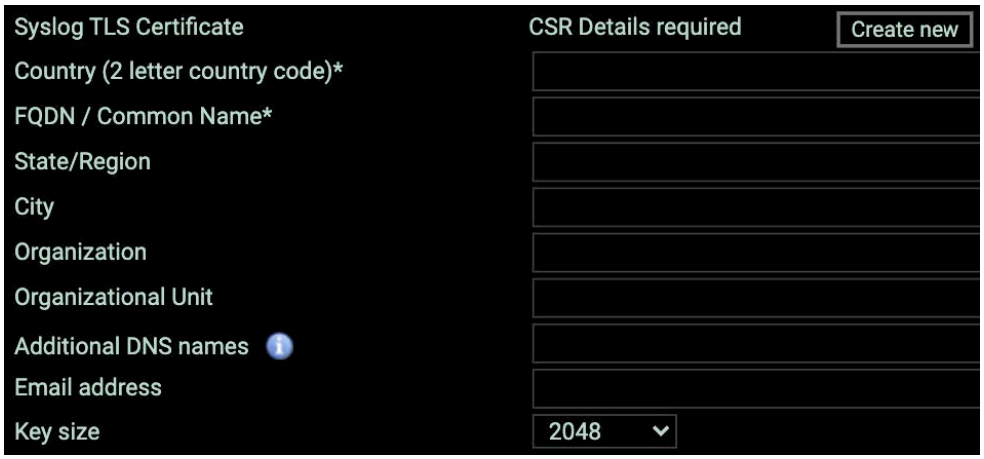
2. On the Settings page, click the **three dots** next to the **Find a Setting...** search bar for more options.

   Select the **Use Legacy Page** option.



   Once the legacy page has opened, locate the **Syslog TLS Certificate** field. If the certificate is to be changed for a master, probe or vSensor, be sure to select the correct field from the correct subsection.

3. Beside this field, click the **Create new** button and fill out the newly displayed fields.



   At a minimum, the Country Code and FQDN / Common Name must be completed. The FQDN field should contain the hostname of the master of probe to be contacted.

4. Save the fields to generate a CSR which can be exported and signed. Paste the signed certificate into the **Certificate** field below the CSR and save your changes.

Additional Device Tracking Notes

Darktrace provides support for multiple feeds into the appliance. If DHCP cannot be obtained from the current SPAN / TAP / port mirror session, Darktrace can create and support a new one, even if that means duplicate packets will be seen. Darktrace can also ingest syslog over UDP port 1514 from the DHCP server and can parse this traffic from the Log Input section of the Darktrace Configuration Page.

Tracking by Hostname

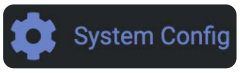
Darktrace passively reads hostnames for devices by observing devices making network requests such as DNS requests for IP addresses, Kerberos logins, and DHCP handshakes. This provides the Threat Visualizer with hostnames as enrichment data, allowing the easy identification of devices beyond an IP or MAC address.

If DHCP is unavailable, **Darktrace will default to tracking a device by its IP address**. This may mean it will lose track of devices where they have dynamic IP addresses. However, by configuring Darktrace options, hostnames can be appended to a device to better track them.

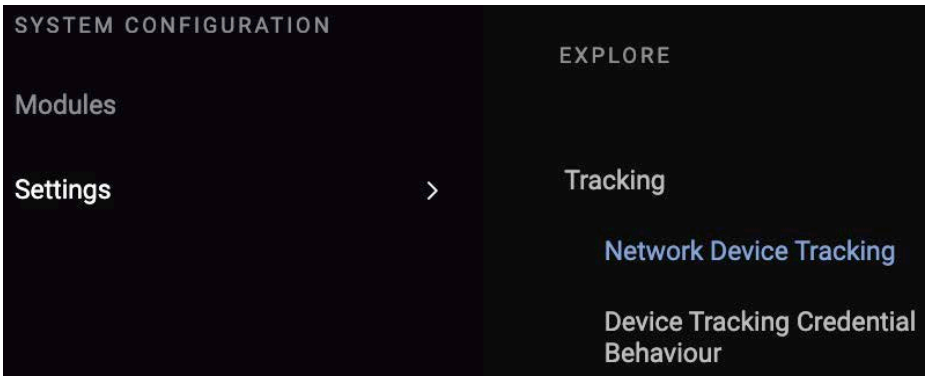
To aid in this process, there are three ways to configure Darktrace to look for hostnames:

Passively look for hostnames in Kerberos traffic

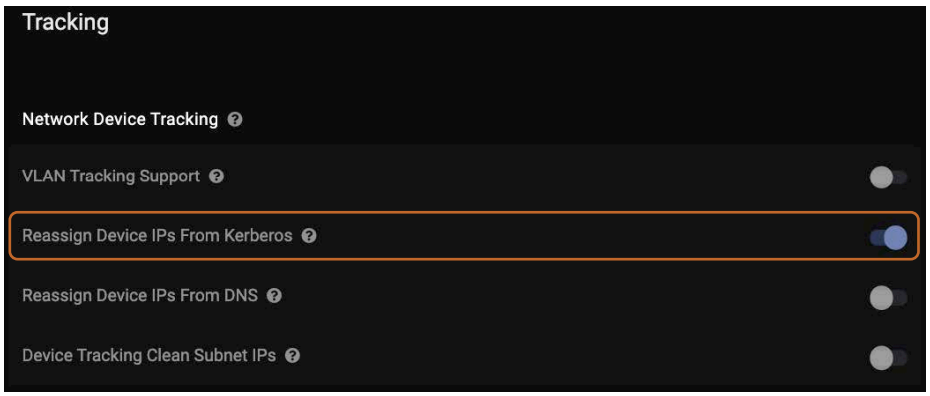
1. Navigate to the **System Config** page.



2. From the System Configuration Settings, locate the **Network Device Tracking** subsection of the Tracking section.



3. Of the options presented on the right, locate the **Reassign Device IPs From Kerberos** parameter and confirm it is enabled.



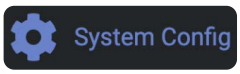
When DHCP is not available, setting this to true will enable Darktrace to append hostnames when performing Kerberos authentication.

If suitable Kerberos packets are available in Darktrace, it will look for hostnames and reassign IP addresses to them. This is particularly useful if you are unable to poll DNS servers as described below. **It is recommended to always set this to true**, so if it has been disabled, use to toggle to enable it.

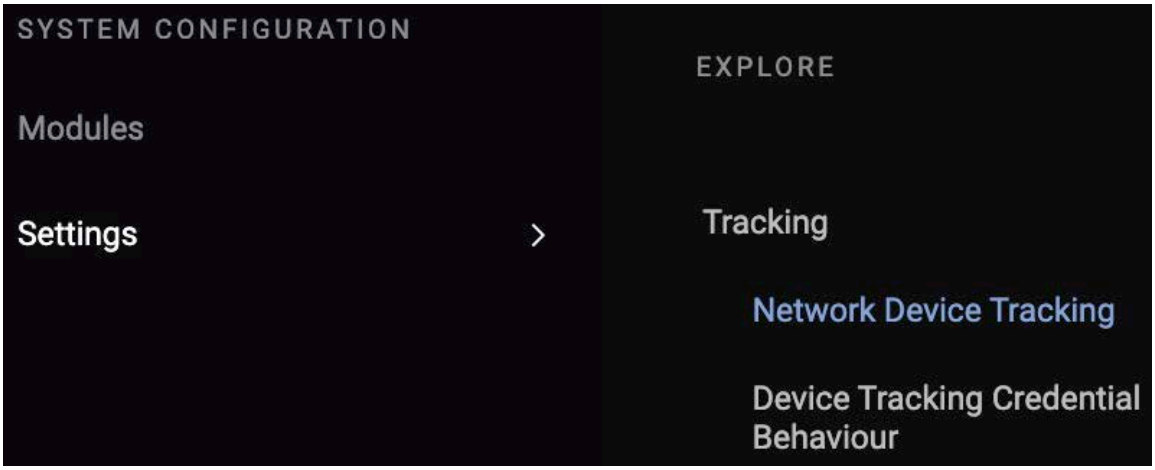
Passively look for hostnames in DNS traffic

It is also possible reassign IPs for client devices based on hostnames observed in DNS traffic and assign them to a network device.

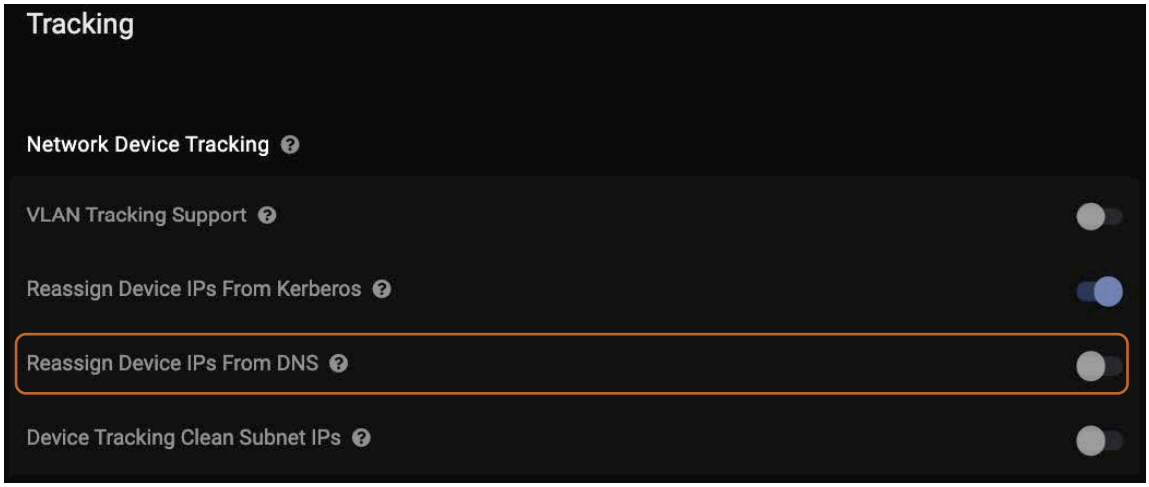
1. Open of the **System Config** page from the main menu.



2. From the System Configuration Settings, locate the **Network Device Tracking** subsection of the Tracking section.



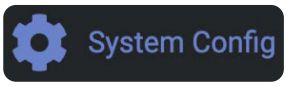
3. Review the **Reassign Device IPs From DNS** setting. By default, this option is disabled. Typically enabling this setting is **not recommended**, so only enable this setting if all other options have been exhausted.



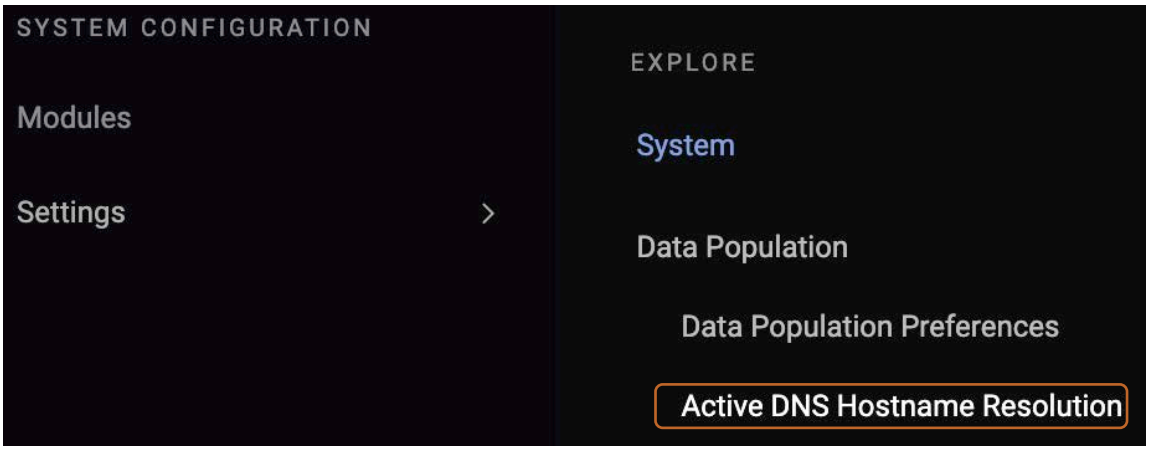
Polling DNS Servers to append hostnames

When set to poll, Darktrace uses network administration command-line tools to poll DNS servers (DIG commands) for the hostname associated with an IP address when it becomes active on the network. The hostname resolution will be cached for a time that is set. As IP addresses change frequently, these are both critical components.

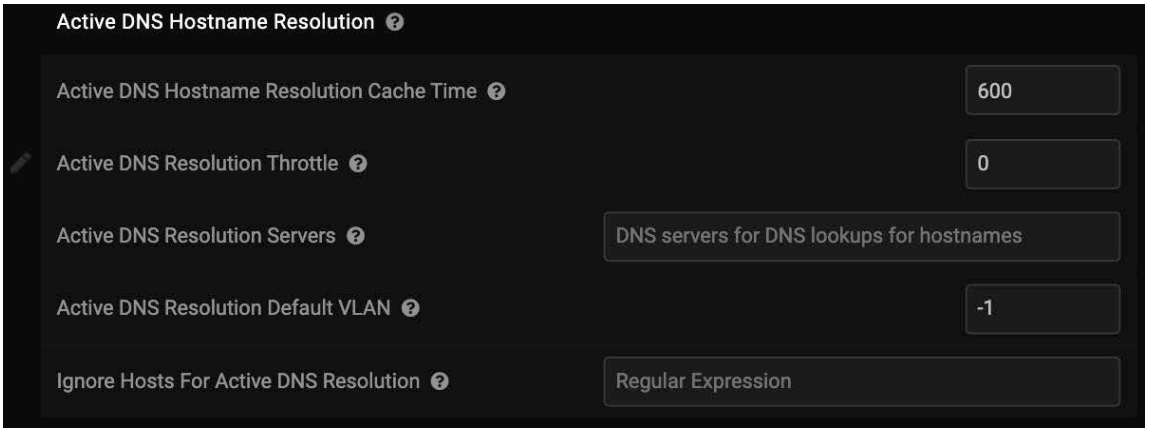
1. Within the **Settings** section of the **System Config** page, review the Poll Network settings.



2. Locate the **Data Population** section and navigate to the **Active DNS Hostname** Resolution subsection.



3. Within the Active DNS Hostname Resolution section, there are a range of fields.



   a. The **Active DNS Hostname Resolution Cache Time** controls how long IP/hostname pairs found via DNS resolution are cached for. Entering a value of greater than 0 will provide access to the required fields needed for configuring active hostname resolution.

      A value of 7200 seconds (2 hours) is typical, but a minimum of 600 seconds (10 minutes) is required to continue inputting options.

   b. When performing DNS resolution, the **Active DNS Resolution Throttle** value limits the maximum frequency of requests per second. The default value is 10 but can be altered if desired.

Note: *When a value is modified from the default, you will see a pencil icon to the left of the field.*

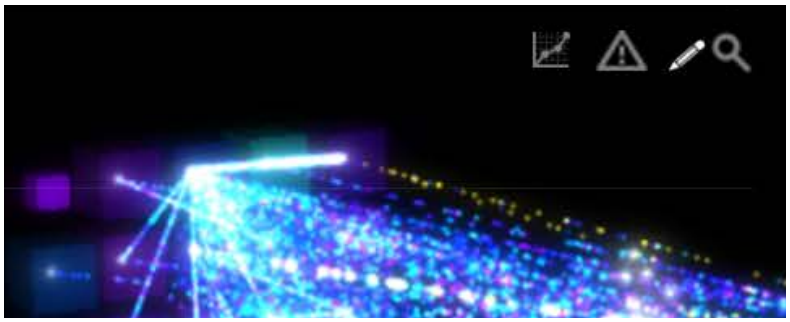
c. The **Active DNS Resolution Servers** field controls the servers polled for DNS resolution. A maximum of 5 servers can be entered as comma-separated values, where the entry order defines the query order. If the field is left empty, polling will be completed using the DNS servers configured via the console.

4. **Save Changes** by clicking the button which will be displayed at the top of the screen when values are entered.

Tracking by Credentials

Darktrace automatically detects logins via Kerberos and other credentials. By extracting the source IP address and the credential, the system can identify which device is being used at the time. If Darktrace is unable to obtain DHCP or DIG, credentials can be employed to track devices instead. This is most commonly used when Darktrace has no other means of identifying the device besides the individuals/users logging into them (e.g. VPN users).

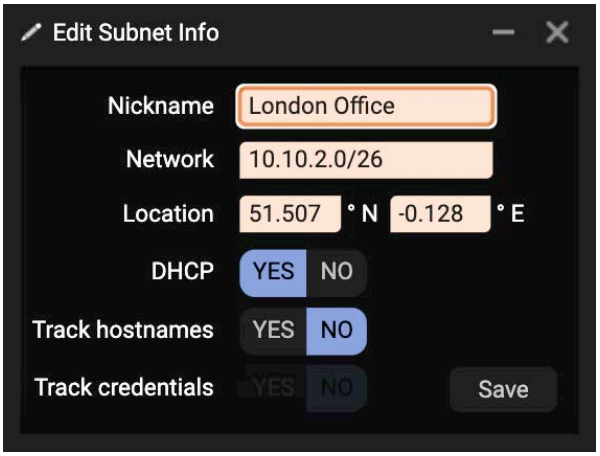
1. In the **Subnet View**, i.e. with a subnet populated in the **Omnisearch** bar, click the **Edit Subnet** Info symbol, indicated by the pencil icon.



2. The **DHCP** subnet setting controls if Darktrace should track devices by DHCP.

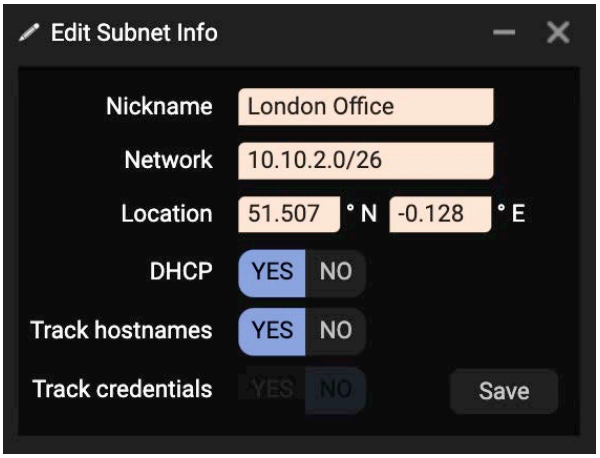
   When disabled, Darktrace will track all devices in a subnet by their IP addresses.

   When enabled, devices are tracked through their MAC addresses. However, if there is no DHCP data for the entire subnet, it will failover, meaning devices will be tracked based on hostname using sources such as Kerberos or DNS data.



3. It is possible to have multiple tracking methods employed for a subnet. Toggling the **DHCP** and Track hostnames to YES will track devices based on the hostnames seen in DHCP data.

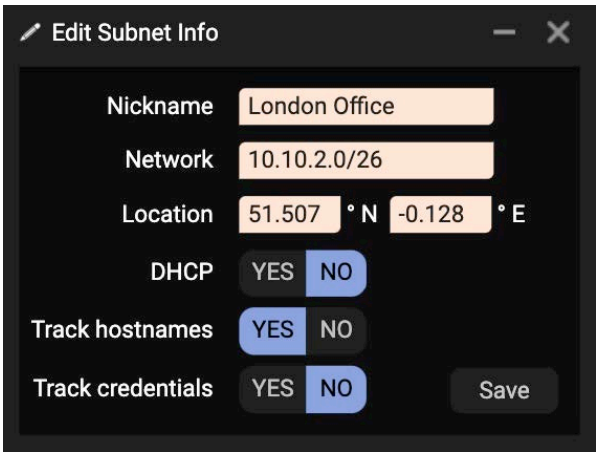
   If there is no DHCP data for the entire subnet, the devices will be tracked based on data such as Kerberos or DNS.



4. Setting **Track hostnames** to **Yes** will force Darktrace to only track devices by hostnames, not MAC addresses. This hostname information will be pulled from data sources such as Kerberos or DNS.

   Tracking devices by hostname will assist Darktrace in distinguishing between the various devices which may share the same IP.

   The Track hostnames function is also useful for tracking credentials for users accessing a network over a VPN.

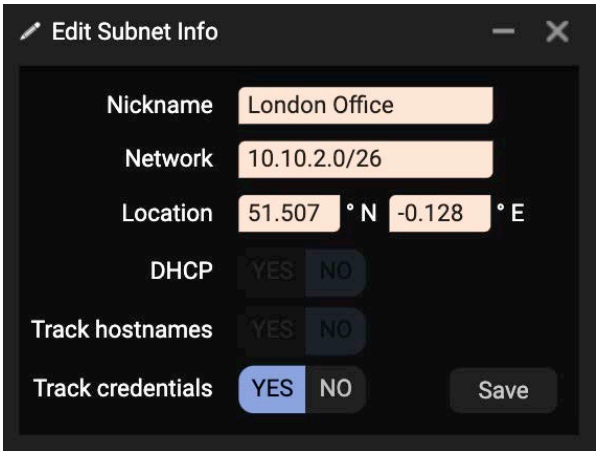


   Example: Tracking laptops connecting to a network through a docking station. The IP address seen by Darktrace will remain the same, but multiple laptops could use the docking station during the lifetime of the IP address.

5. In order to select **Track Credentials**, the DHCP setting must be toggled to **NO**.

   Enabling this value will automatically create a separate device in Darktrace for each user. The hostname is a combination of the Subnet and user credentials.

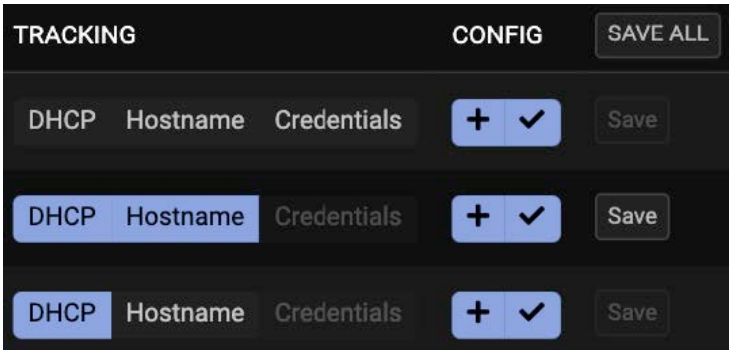
   Devices are tracked based on their username using data from sources such as Kerberos, NTLM or Radius.



   Example: Shift workers could share the same desktop device during the day. The device will keep the same DHCP information, but the credentials will change.

   ***Note:** Combinations of these three tracking settings, DHCP, Hostname and Credential, can also be changed via the Subnet Admin page.*

   If none of them are selected, tracking will be disabled, and device objects will be modelled on all data to/from their IP.



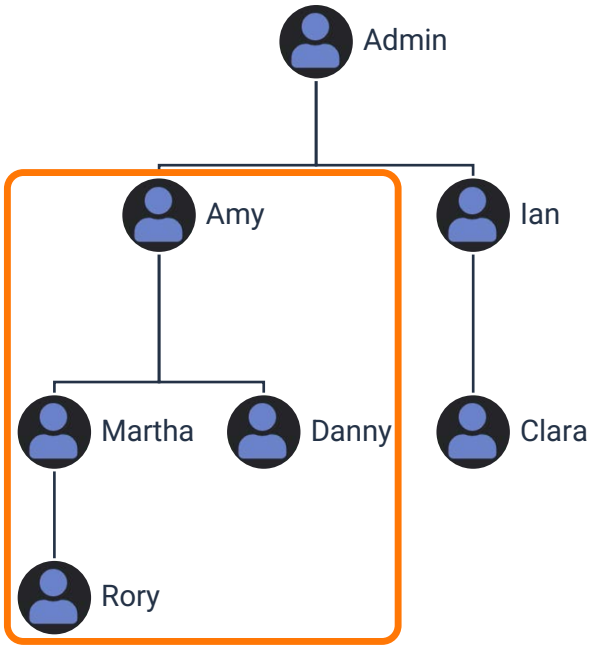
6. User and Group Permissions

To have access to the Threat Visualizer, users should be granted the relevant permissions for their respective roles. Permissions can be assigned on a user basis, but if a team of users have similar roles, permissions can be assigned to groups and applied in this way.

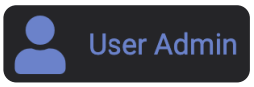
User Admin

User Admin is a page where permissions can be set on a per-user basis. However, permissions can only be assigned to users which are visible. The users which are displayed on the page are dependent on a hierarchy of who created the users.

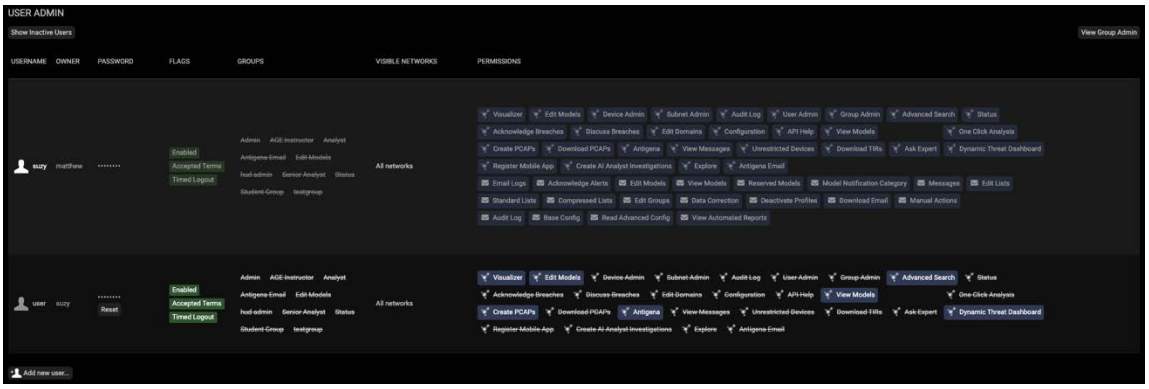
In the hierarchy to the right, the Admin, or "parent", user would be able to see all the other "child" and "concurrent child" users in the User Admin page. Therefore, Admin can assign permissions to all the users on the right. However, if Amy logs in, she will only be able to see and assign permissions to the users highlighted in orange. This is because Amy created Martha and Danny's users and Martha created Rory's.



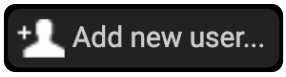
1. Within the menu, navigate to **Admin** to open up the **User Admin** page.



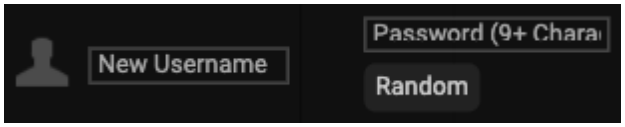
2. Upon opening in a new tab, notice a table of **username**, **owners**, **passwords**, **flags**, **groups**, **visible networks** and **permissions**.



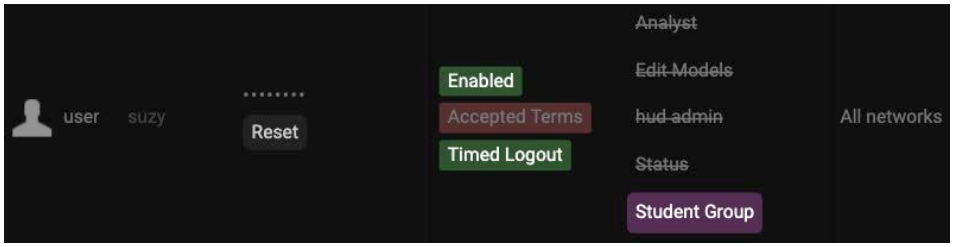
3. As an administrator, it may be desirable to create new users. To do so, click the **Add new user** button at the bottom of the page.



4. Input the new **username**. Then, create a **password** by typing into the box or clicking random. Click **Save** to create the user.

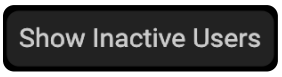


5. The administrator which created the user will be the owner.

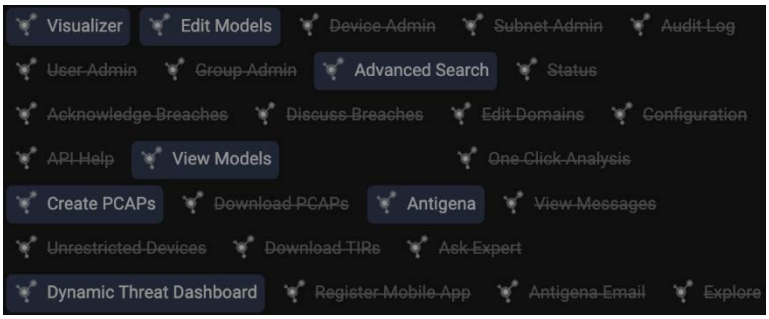


The owner can then **edit** user details. This includes the functionality to change the username, password and permissions. Also, in this row, there is the option to **deactivate** the user, enforce a **timed logout** or apply the user to **groups** created in the Group Admin page.

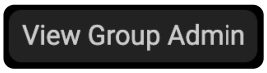
6. **Disabling** a user, by clicking the green **Enabled** so it turns red, will hide the user from the User Admin page. Click **Show Inactive Users** to view all users that are under ownership.



7. On the right of the screen, select the **permissions** for the user. Blue highlighted permissions are assigned to the user. Crossed out permissions indicate the user does not have these privileges.

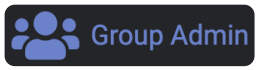


8. To assign permissions to groups rather than individuals, click **View Group Admin** in the top right-hand corner of the screen.



Group Admin

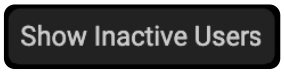
1. To open the **Group Admin** page from the Threat Visualizer, navigate to Group Admin from the Admin section of the main menu.



2. The Group Admin page opens in a new tab. Existing Groups will be each given a row with **assigned permissions**.

   a. Users who have been assigned to certain groups within the User Admin page will be listed in the **Users** column. If a user belongs to a group, their name will be highlighted. If they do not belong to a group, their name will be crossed out.

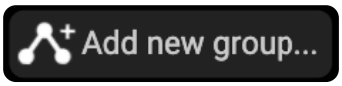
   b. If the user is inactive, they may not be visible in the Users column. To rectify this, click **Show Inactive Users** at the top of the page.



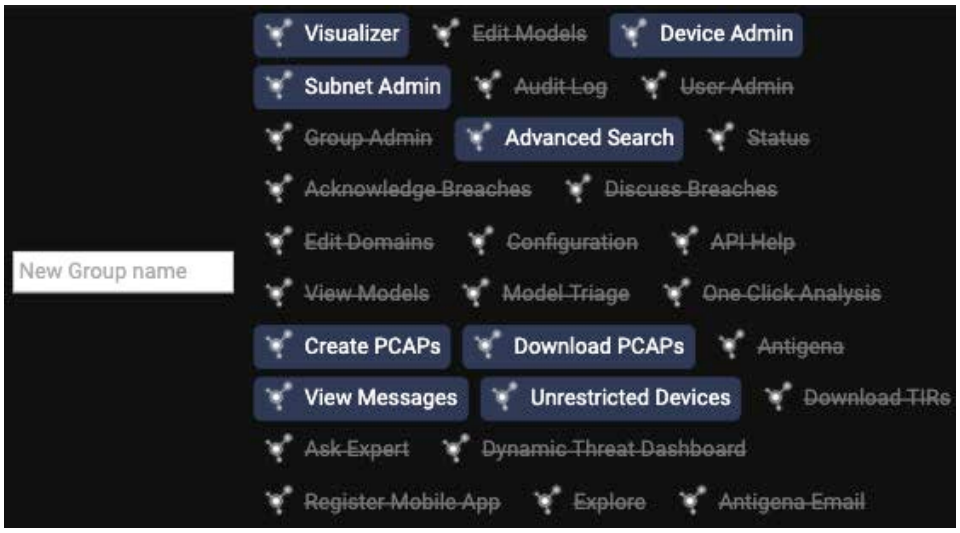
   c. Groups can be applied to users on certain **Networks**. Multiple network range values can be input, separated by new lines. Invalid inputs will highlight the box in red.

   Note: *If Network Ranges are input to limit visibility for certain groups, it is necessary to fill out all other groups with a value of 0.0.0.0/0.*

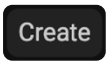
3. To create a new Group, click Add new group at the bottom of the page.



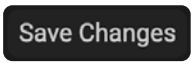
An empty group will be created with some pre-highlighted permissions.



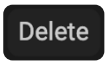
a. Once a Group name has been input and the desired permissions selected, click **Create**.



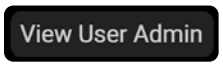
b. If any changes are made, make sure to click **Save Changes**.



c. Finally, click Delete to remove a group.

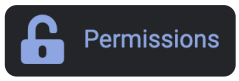


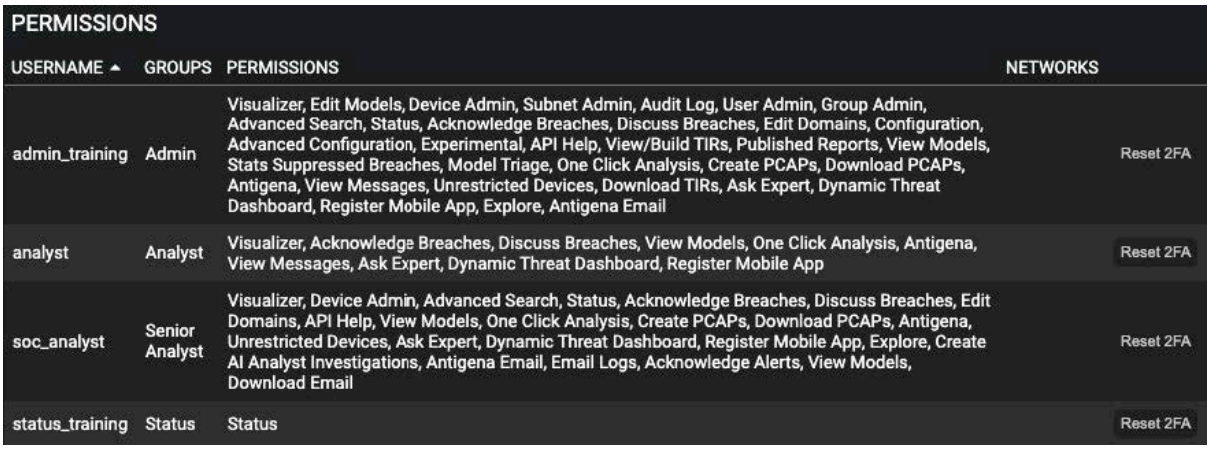
4. To pivot to the User Admin page, click **View User Admin** in the top right-hand corner of the page.



Permission Breakdown

By accessing the Permissions page from the Admin section of the Threat Visualizer main menu, permissions can be viewed on a username and Group basis.





The table below gives a short breakdown for each permission available as well as a recommendation for which level of access the user is expected to have.

Permission	Description	Recommended User
Visualizer	Grants access to the Threat Visualizer interface.	End User, Super User
Edit Models	Make changes to Models. ***Note:*** *Edit Models controls whether to display the Ignore any future breaches button in the Breach Log. Using tags can also be a good way of tuning models without requiring access to edit a model.*	Admin, Super User
Device Admin	Lists all devices observed by Darktrace. Useful for searching, bulk tagging, or changing device types.	Admin
Subnet Admin	Lists all subnets, labels, and whether DHCP is enabled.	Admin
Audit Log	Lists captured user behavior such as logging into Darktrace.	Admin

User Admin	Controls access to user privileges.	Admin
Group Admin	Controls access to group privileges.	Admin
Advanced Search	Provides a deep insight into network traffic making every connection searchable. Excellent for investigating suspicious activity.	Admin, End User, Super User
Status	Check the system health of the Darktrace appliance, probes, and network traffic.	Admin, Super User
Acknowledge Breaches	Enables users to acknowledge Model Breaches.	Admin, End User, Super User
Discuss Breaches	Makes comments on model breaches to control and highlight which users are working on a Model Breach.	Admin, End User, Super User
Edit Domains	Make changes to domain information. ***Note:*** *Provides access to the Trusted Domains page under Intel.*	Admin, Super User
Configuration	Make changes to the System Config page.	Admin
API Help	Provides information on the Threat Visualizer API.	Admin, Developers
View Models	View a Model to help with understanding how a breach occurred.	Admin, End User, Super User
One Click Analysis	Provides a quick view of the Model Breach to assist in identifying and investigating alerts.	Super User
Create PCAPs	Enables users to create Packet Captures in the Threat Visualizer application.	Admin, Super User

Download PCAPs	Allows user to download created Packet Captures for investigation in Wireshark or Darkshark.	Admin, Super User
Antigena	Enables Antigena functionality. The Darktrace appliance must be configured to enable Antigena.	Admin, Super User
View Messages	View comments on Model Breaches. Useful to view which users are working on a breach.	Admin, End User, Super User
Unrestricted Devices	View all user credentials that have accessed a device. Disabling this option restricts users to an obfuscated view.	Admin, End User, Super User
Download TIRs	Enables users to download Threat Intelligence Reports.	Admin, Super User
Ask Expert	With Ask the Expert enabled, ask Analysts questions about particular Model Breaches. This will open a window to drag and drop Breach Log details and post questions.	Admin, End User, Super User
Dynamic Threat Dashboard	Provides access to the Dynamic Threat Dashboard	Admin, End User, Super User
Register Mobile App	Provides users with access to link their account to the App from the Account Settings. ***Note:*** *The Mobile App settings under Alerting within the System Config page must be set before this feature can be employed.*	End User, Super User
Create AI Analyst Investigations	Allows the user to prompt AI Analyst to investigate a device for a chosen timeframe on demand.	Admin, End User, Super User
Antigena Email	Allows access to Antigena Email console.	Admin, End User, Super User
Explore	Gives the Explore option in the main menu.	Admin, End User, Super User

Useful Configurations

Basic threat analysis with obfuscation privileges

Users can analyze devices, make comments, and acknowledge breaches but cannot identify users associated with the device.

Visualizer	~~Edit Models~~	~~Device Admin~~	~~Subnet Admin~~	~~Audit Log~~
~~User Admin~~	~~Group Admin~~	~~Advanced Search~~	~~Status~~	Acknowledge Breaches
Discuss Breaches	~~Edit Domains~~	~~Configuration~~	~~API Help~~	View Models
One Click Analysis	~~Create PCAPs~~	~~Download PCAPs~~	Antigena	View Messages
~~Unrestricted Devices~~	~~Download TIRs~~	Ask Expert	Dynamic Threat Dashboard	
Register Mobile App	Create AI Analyst Investigations		~~Antigena Email~~	~~Explore~~

Full threat analysis privileges

Users can provide full threat analysis across the whole Cyber AI Platform, including the use of Advanced Search, and have the capability to identify users.

Visualizer	~~Edit Models~~	Device Admin	~~Subnet Admin~~	~~Audit Log~~
~~User Admin~~	~~Group Admin~~	Advanced Search	Status	Acknowledge Breaches
Discuss Breaches	Edit Domains	~~Configuration~~	API Help	View Models
One Click Analysis	Create PCAPs	Download PCAPs	Antigena	View Messages
Unrestricted Devices	~~Download TIRs~~	Ask Expert	Dynamic Threat Dashboard	
Register Mobile App	Create AI Analyst Investigations		Antigena Email	Explore

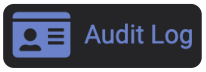
Full administration privileges

Users can perform detailed threat analysis and administer changes to the system configuration settings.

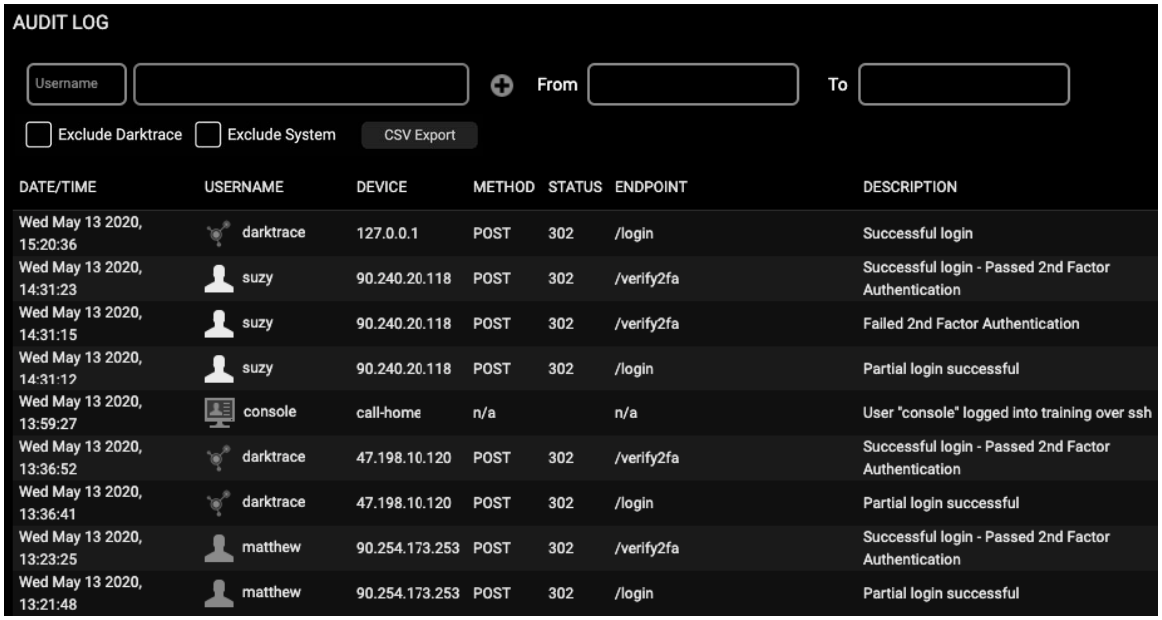
Visualizer	Edit Models	Device Admin	Subnet Admin	Audit Log
User Admin	Group Admin	Advanced Search	Status	Acknowledge Breaches
Discuss Breaches	Edit Domains	Configuration	API Help	View Models
One Click Analysis	Create PCAPs	Download PCAPs	Antigena	View Messages
Unrestricted Devices	Download TIRs	Ask Expert	Dynamic Threat Dashboard	
Register Mobile App	Create AI Analyst Investigations		Antigena Email	Explore

7. Understanding the Audit Trail

1. Click **Admin** and then **Audit Log** from the main menu.



2. The **Audit Log** provides information about user actions within the Darktrace Threat Visualizer.



A table containing the date and time of an action, which user performed it, from which device and to which endpoint is presented.

a. Notice the username icon for each event.

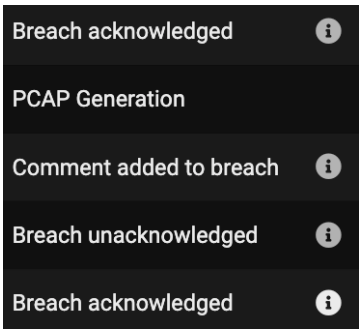
   i. The **monitor** icon is related to command line or SSH access, e.g. when a user uses the console app

   ii. The **Darktrace logo** icon appears when a user is utilizing the Darktrace account to login to an appliance

   iii. The **silhouette/person** icon is indicative of events from a user generated account

b. Every event has a short **description**, but some events may have a tooltip icon.

   Click a **tooltip icon** to obtain more information about an entry which can help gain more of an understanding of what occurred.



3. The search bar at the top of the page can **restrict results** to **individual users**, **methods** or **endpoints**.

__Note:__ The user interacts with the UI via HTTP via four available __Methods__: __PUT__, __GET__, __POST__ or __DELETE__. These actions occur with respect to the results displayed in the __Endpoint__ column.

a. Select a mechanism to restrict results, type in the search bar and press enter on the keyboard to filter the Audit Log.

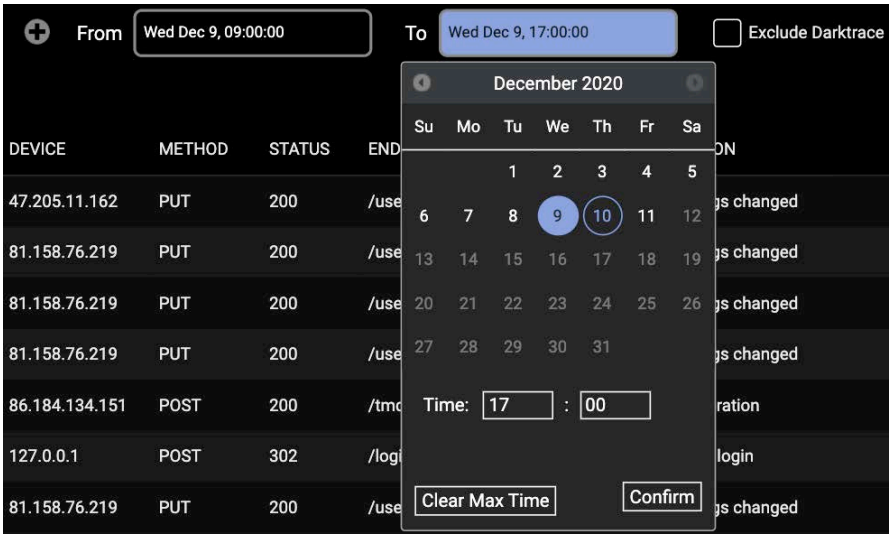
b. Applied filters will appear under the search bar in blue. To **remove** a filter, click it.

4. To exclude Darktrace events from the results in the Audit Log, check the tick box named **Exclude Darktrace**.

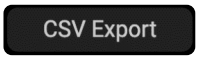
5. Similarly, to exclude System events from the results, check the tick box named Exclude System.

6. Checking accesses to the Threat Visualizer can be done by time frame.

   Click the **From** and **To** time selectors, remembering to click on the Confirm buttons when selecting the date / time ranges.

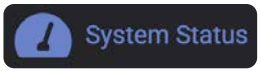


7. It is also possible to export the selected elements in a CSV file format by clicking on the **CSV Export** in the top right of the page.

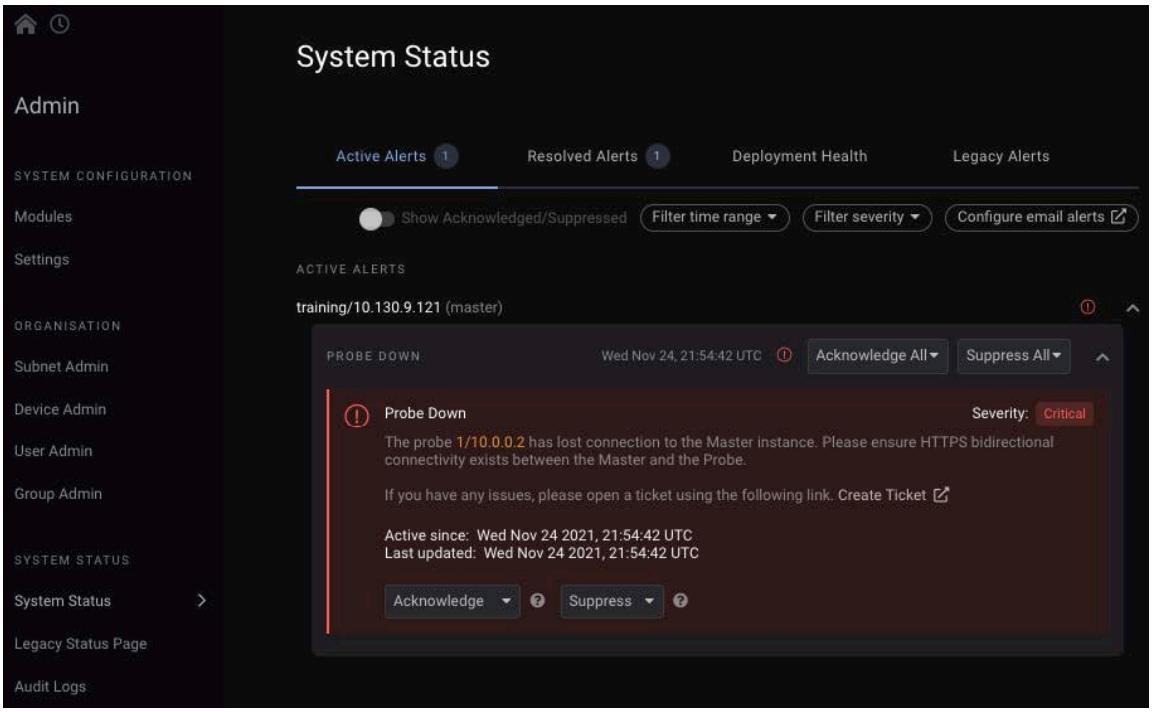


8. System Status

1. In **Menu**, select **Admin** > **System Status**. This provides useful statistics about the version and health of your appliance.

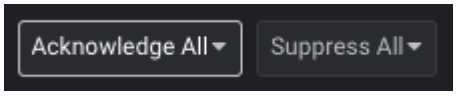


2. Upon opening, the System Status page will present a menu down the left-hand side which provides shortcuts to various **administrative pages** within the Threat Visualizer.

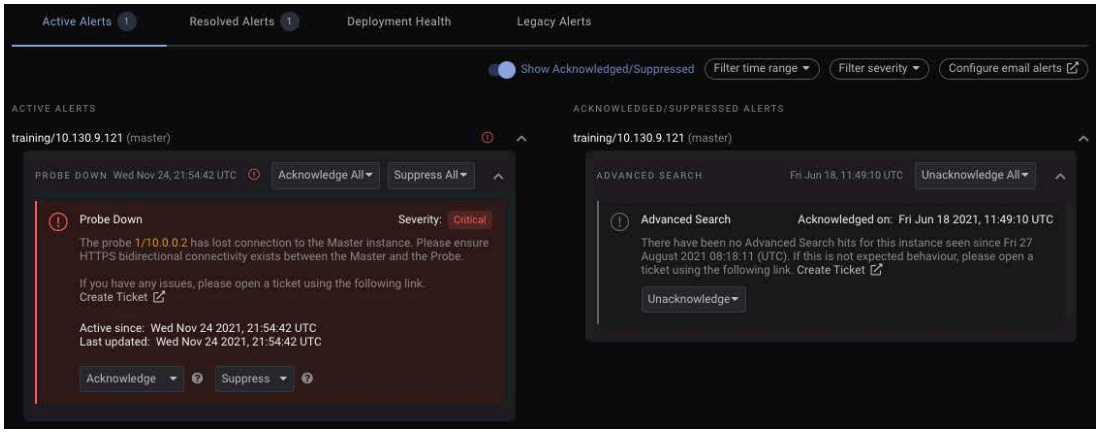


3. On the right-hand portion of the page, any existing **System Alerts** (Active Alerts and Resolved Alerts) will be displayed in their respective tabs. Review the alerts presented here.

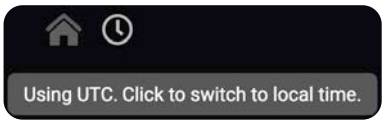
   a. **New Alerts** can be acknowledged in bulk for the current user or all users and can be suppressed for a chosen time period.



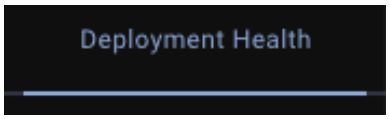
   b. To view **Acknowledged/Suppressed** alerts, use the toggle at the top of the page to display the alerts in two columns.



4. This page will be automatically presented in UTC. Click the clock icon in the top left of the page to switch to the local timezone.



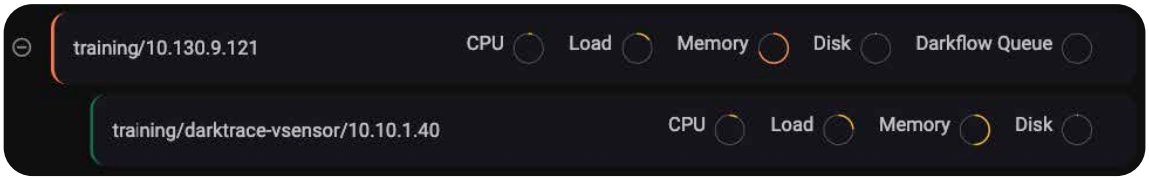
5. At the top of the page, notice the **Deployment Health** tab. Click on this to view the appliances which are being analyzed by Darktrace.



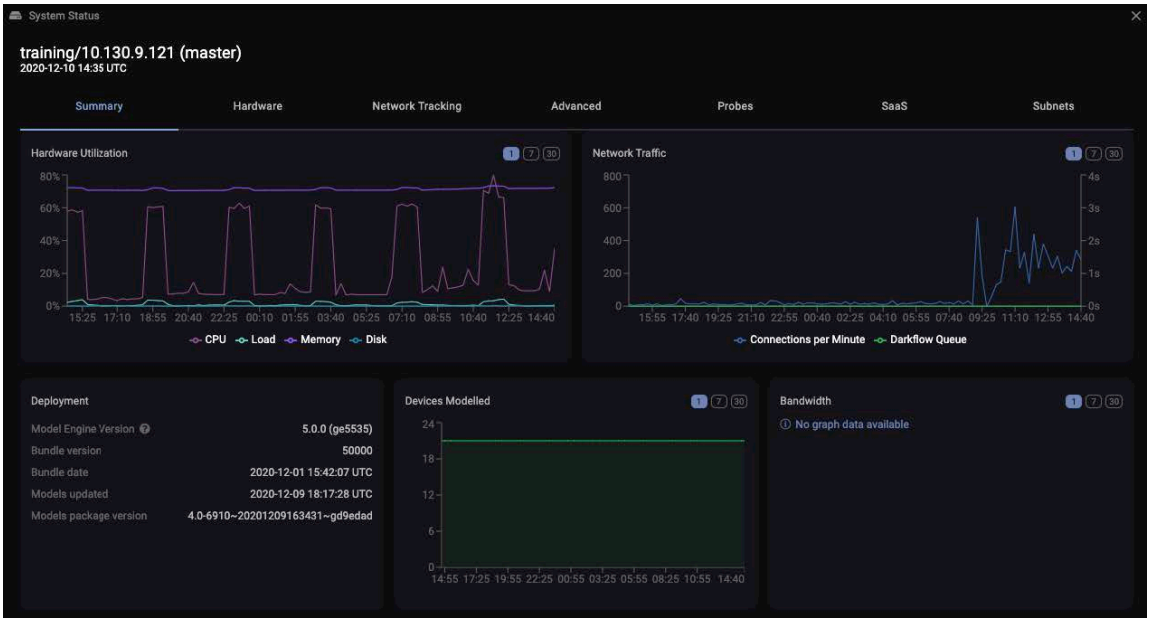
6. This will open a tree of appliances, displaying a hierarchy of the deployed Darktrace architecture in **Branch View**.

Note: *The color of the appliance is the first indicator of its health. This can be useful for determining which appliance may need looking into.*

7. To switch from Branch View to **List View**, select the right most icon in the Deployment Health display. The List View will present visual statistics for CPU, Load, Memory and Disk utilisation.



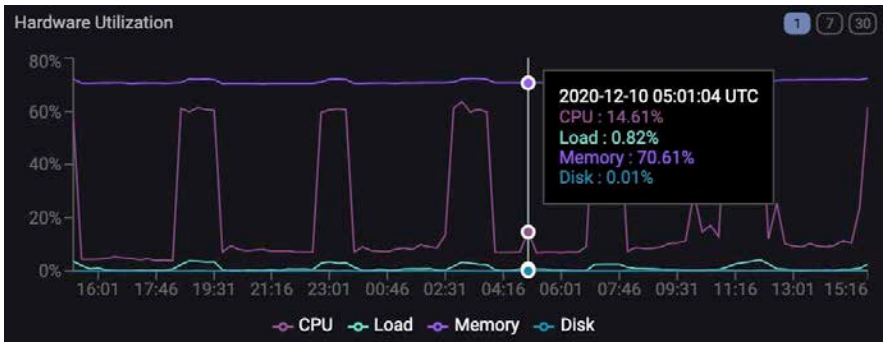
8. From either view, click a Master **appliance name** to open the appropriate System Status page. Each Master appliance has statistics that can be broken up into a variety of tabs, as presented across the top of the window. The default tab, **Summary**, will display key information about the appliance.



Displayed in the Summary above is the Hardware utilization (CPU, Load, Memory and Disk), Network traffic (Connections per minute and Darkflow Queue), Deployment information, the number of Devices Modelled and Bandwidth. Many of these statistics can be viewed in different pages.

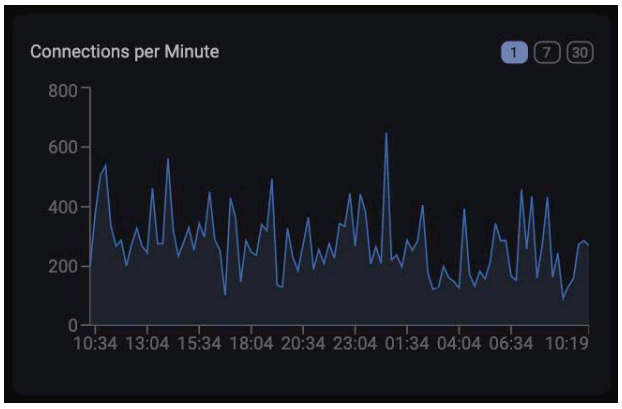
9. Each graph can plot data for the last day, the last 7 days or the last 30 days by changing the number in the top right-hand corner of the graph.

10. By **hovering** anywhere on the graph, the **data points** at that point in time will be highlighted. Furthermore, a small dialog will display the data for any graphed values.



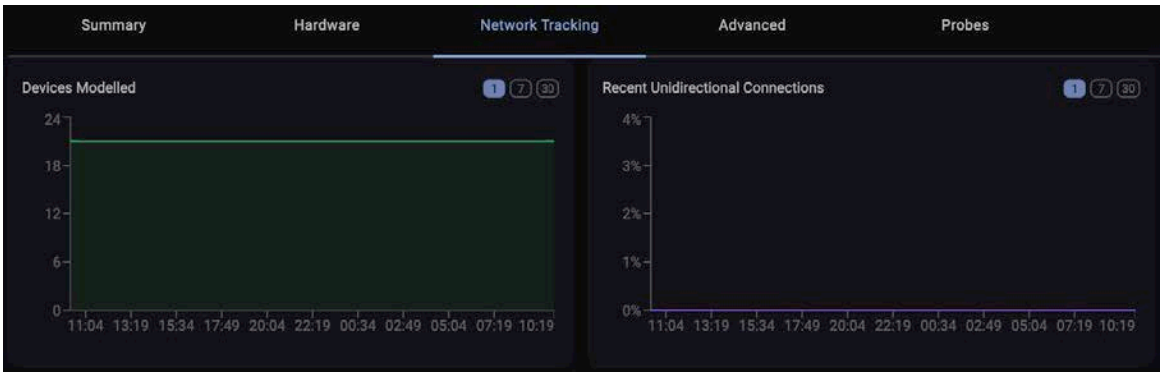
11. Click the **Hardware** tab along the top of the window. This tab displays similar information to the summary, such as the Hardware Utilization. However, notice the **Darkflow Queue** and **Connections per Minute** graph have been separated.

The **Darkflow Queue** states how long real time data takes to be displayed in the Threat Visualizer. Up to 5 minutes is an acceptable threshold but empty is the optimum value.

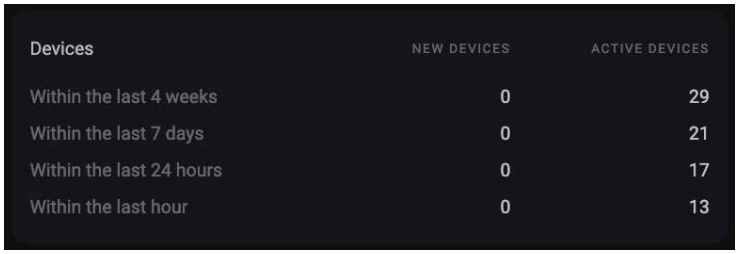


The **Connections per Minute** can show any unusual peaks or troughs over the last day, week or month.

12. The next tab, **Network Tracking**, presents a mixture of graphs, lists and tables. Notice the **Devices Modelled** and **Recent Unidirectional Connections** graphs

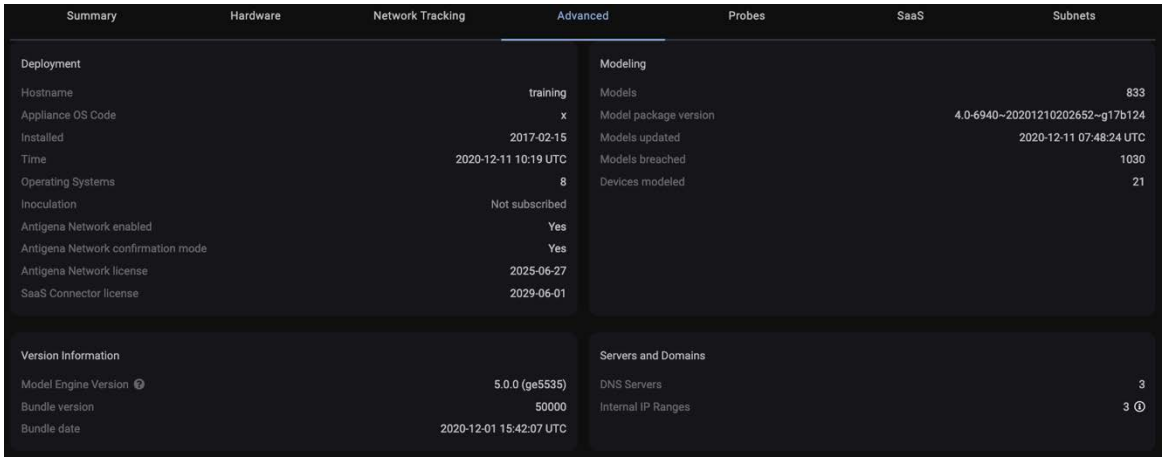


The **number of Devices Modelled** may vary over time. Statistics about new and active devices are tabulated underneath the graph and the way in which they are tracked is also presented on the page.

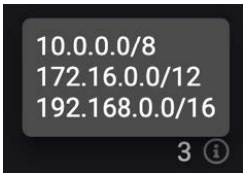


Recent Unidirectional Connections is typically between 0% and 10%. Too much unidirectional traffic may mean significant amounts of traffic is missing from the network.

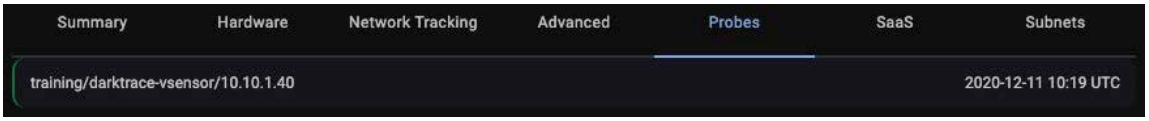
13. Moving along the tabs, click on **Advanced**. This presents a range of deployment information, including when the appliance was **installed** and **updated**, the appliance **version**, **licenses**, and details of the **modelled servers and domains**.



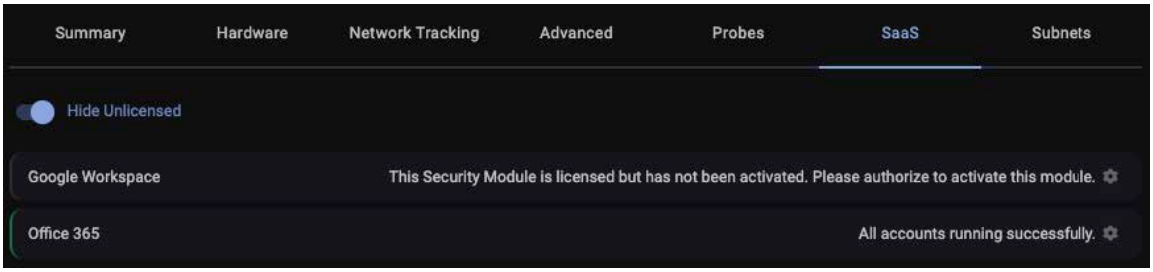
__Note:__ Clicking on a tooltip icon will open up extra information in a small dialog window.



14. The **Probes** tab will list any probes which are linked to the master appliance which is currently being viewed.

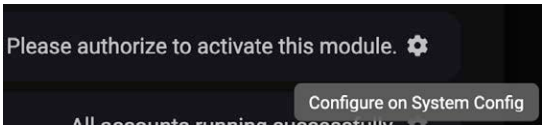


15. Similarly, the **SaaS** tab will list any SaaS modules which are licensed for the deployment and provide additional information if action is required. Accounts which are running successfully will be colored in **green**.

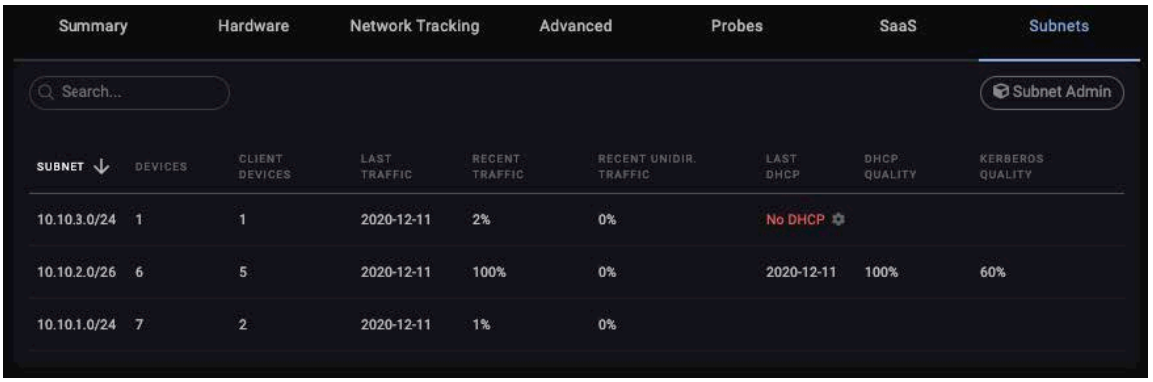


a. To view available, unlicensed SaaS modules, use the **Hide Unlicensed toggle**.

b. Clicking on a **cog icon** will open the **System Config** page for the appropriate module, allowing the user to complete set up or check the settings.

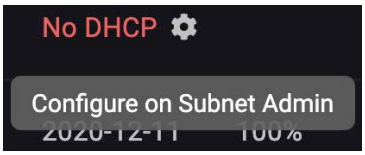


16. Finally, there is a **Subnets** tab available. This presents a limited set of information in comparison to the Subnet Admin page but will show a breakdown of the number of devices on each subnet and the tracking quality.

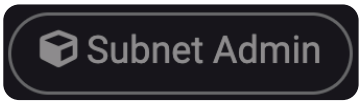


a. For deployments with a large number of subnets, there is a **search bar** which can be used to dynamically filter what is displayed on the page.

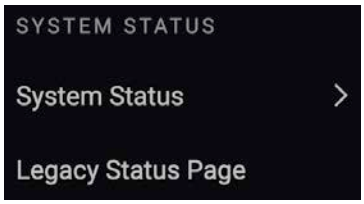
b. Where appropriate, the tracking will be **highlighted**, indicating configuration is required in **Subnet Admin**. Click the **cog icon** to be taken to the relevant page.



c. Also, there is a shortcut to the Subnet Admin page by simply clicking the **Subnet Admin** button presented in the top right-hand corner of the Subnets tab.

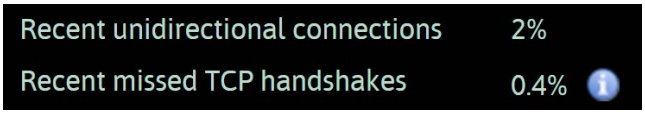


17. To return to the Status page from previous Darktrace versions, click **Legacy Status Page** from the menu on the left-hand side of the page.



a. The **version number** is presented under the Darktrace logo in the top left-hand corner of the interface.

b. Within the **Traffic Analysis** section, underneath Recent unidirectional connections, is the value for **Recent missed TCP handshakes**.

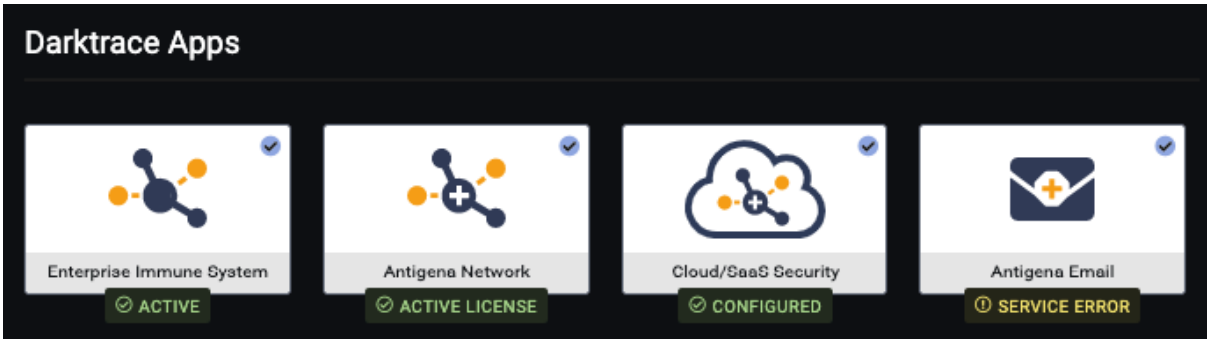


This tracks the percentage of connections in a recent timeframe where the start of a TCP three-way handshake was missing.

Similar to the percentage of recent unidirectional connections, 20% or over may indicate misconfiguration when capturing network traffic. A system alert will fire for capture loss greater than 30%. Such activity should be investigated.

9. Configuring Darktrace Modules

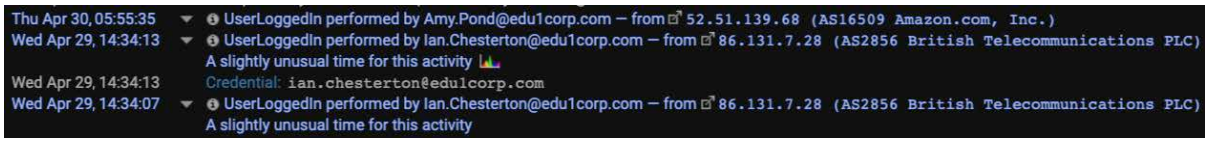
Within the System Configuration page, there is a Modules section, which provides a visual way of understanding what is and what is not enabled on your Darktrace deployment. It instantly outlines which products make up your Darktrace suite but can also highlight additional telemetry and workflow and integration modules that you may wish to enable and configure.



SaaS Connectors

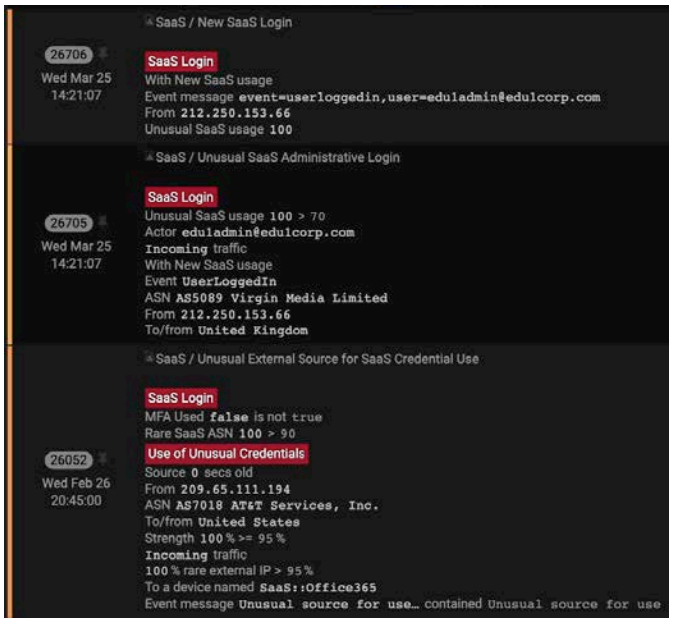
Whether in the cloud or physical, the Darktrace Master will interrogate the security APIs of the relevant SaaS solutions. Darktrace offers a variety of Cloud and SaaS connectors, which can all be authorized within the Darktrace System Config, including Office 365, G Suite, Box, Dropbox, Salesforce, Egnyte and JumpCloud. To enable any of these connectors, a license is required.

Without a SaaS connector, Darktrace will see traffic to these solutions, but it will be encrypted. For example, the Event Logs will show encrypted communications on port 443, but the credential used, and which files are uploaded, downloaded or deleted will not be identifiable.



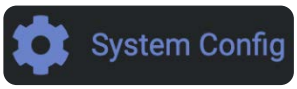
Connectors, such as the Office 365 Connector, can monitor a range of categories:

- Login
- Failed login
- Resource viewed
- Resource modified
- File uploaded
- File downloaded
- Resource created
- Resource deleted
- Sharing
- Admin
- Miscellaneous



An easy way to deploy SaaS connectors within Darktrace are outlined below. Note that different Module settings may vary slightly.

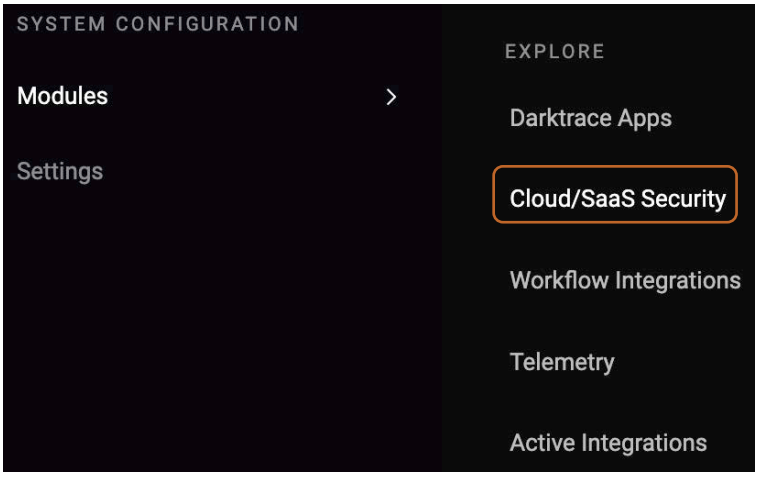
1. Navigate to the **System Config** page.

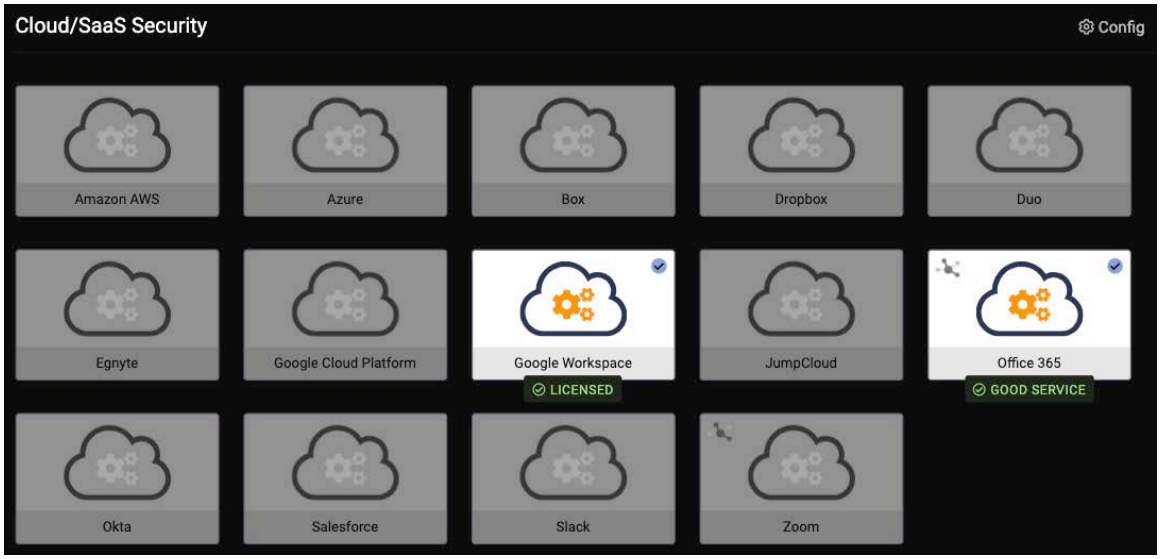


2. Within the **Modules** menu, navigate to the **Cloud/SaaS Security** subsection.

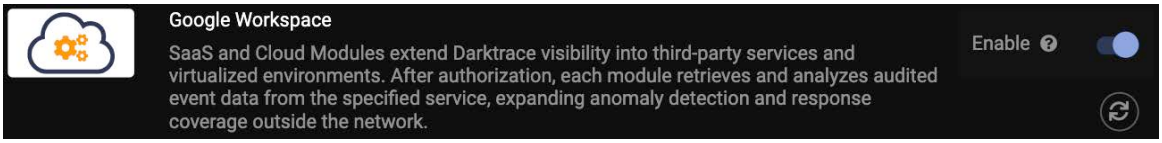
3. Highlighted modules in the **Cloud/SaaS Security** section are licensed, or in use.

   Click the appropriate module from the available options to open a window allowing for further configuration.





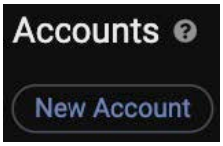
4. Upon opening the appropriate window, ensure the connector is **enabled**.



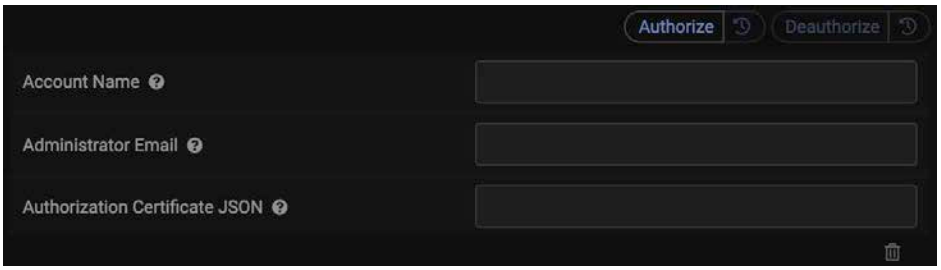
5. Under the **Information** heading, next to the field labelled **Authorization Instructions**, click the link for further instructions.

6. Follow the module specific steps on the page and **log in to the SaaS provider**.

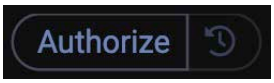
7. Within the Darktrace module window, click the **New Account** button to add a new account.



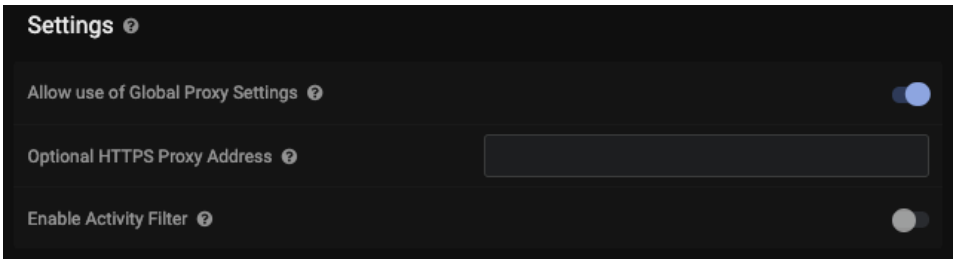
8. Clicking on the New Account button will open up more **fields**. Fill these out using the tooltips for assistance.



9. Click the **Authorize** button above these fields to begin monitoring your Cloud/SaaS environment. After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful or if any errors occurred.



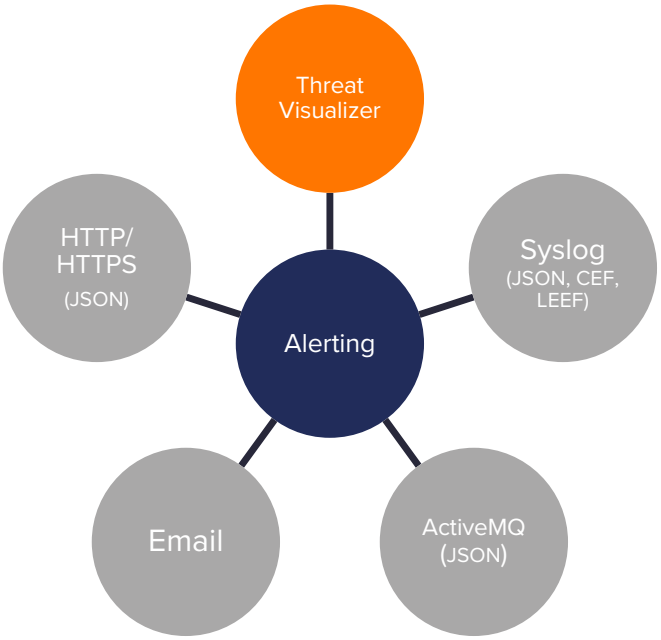
10. Optionally, scroll down the window and configure the **proxy server** details.



Note: *These can be found under the Settings heading of the configuration window after a module has been activated.*

11. Once the module has been **successfully configured**, a message will appear within the **Status** section of the window.

Configuring Alerts

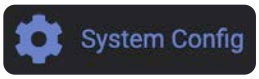


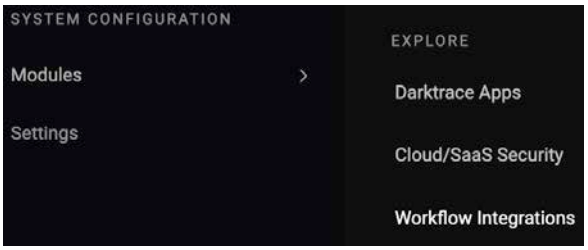
1. Darktrace can interact with an organization's existing alerting or security information system.

   - **ActiveMQ**: Apache ActiveMQ is an open-source message broker written in Java together with a full Java Message Service (JMS) client.
   - **Syslog**: Syslog is a widely used standard for message logging.
   - **HTTP/HTTPS**: HTTP POST
   - **Email**: Standard Email Server Settings

   Note: *For alerts to contain links back to the Threat Visualizer, the Fully Qualified Domain Name (FQDN) value must be set in the Settings section. This field should contain the resolvable hostname or IP address of the Darktrace Threat Visualizer.*

2. From the main menu, navigate to **Admin** and review **System Config**.

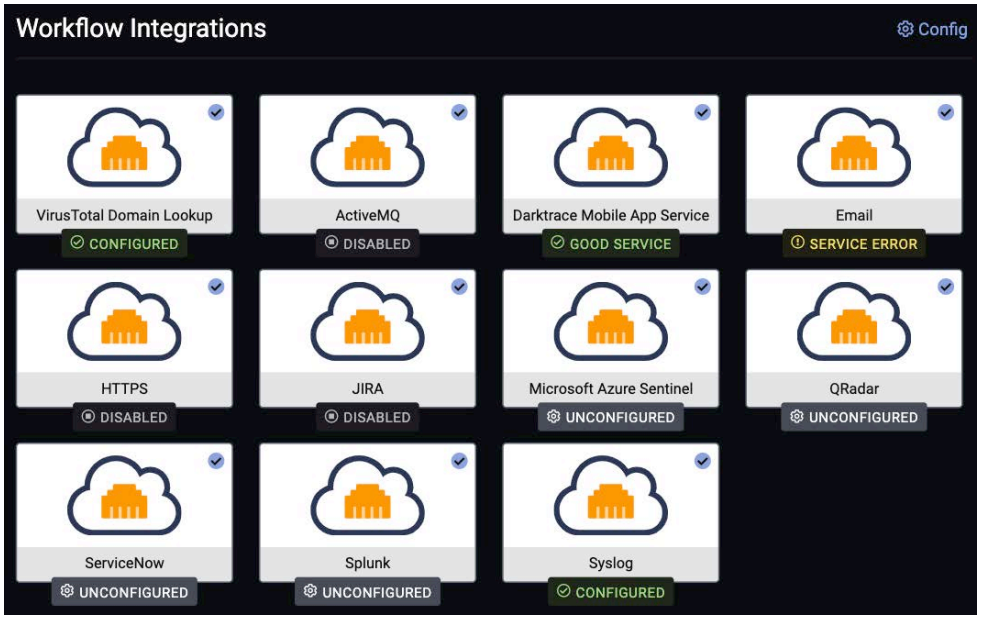




   Navigate from the **Modules** menu on the left to the **Workflow Integration** section.

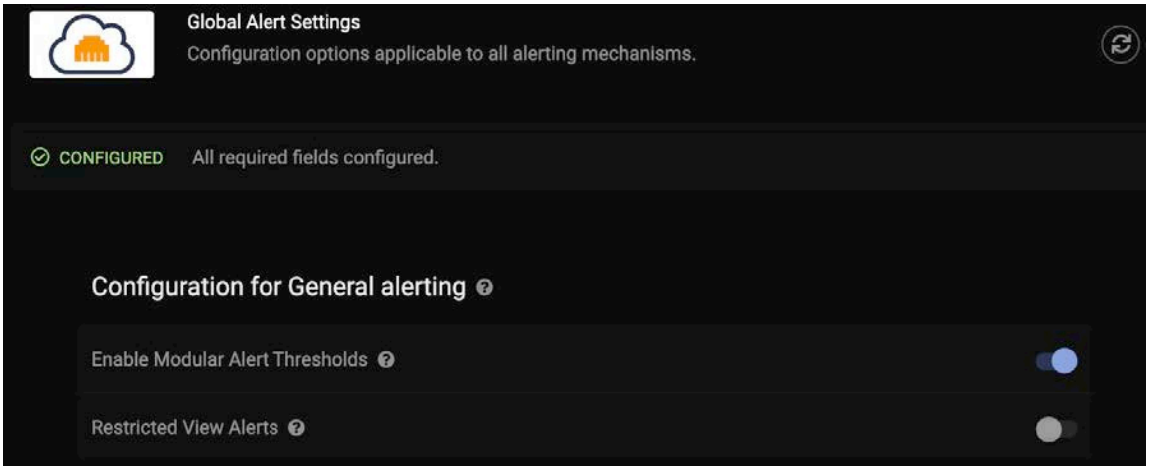
   Presented under the Workflow Integrations are a range of available alerting modules. Clicking on any of these will open up the associated configuration.

Note: *Alerts are only sent for Models where the Action is set to Alert.*

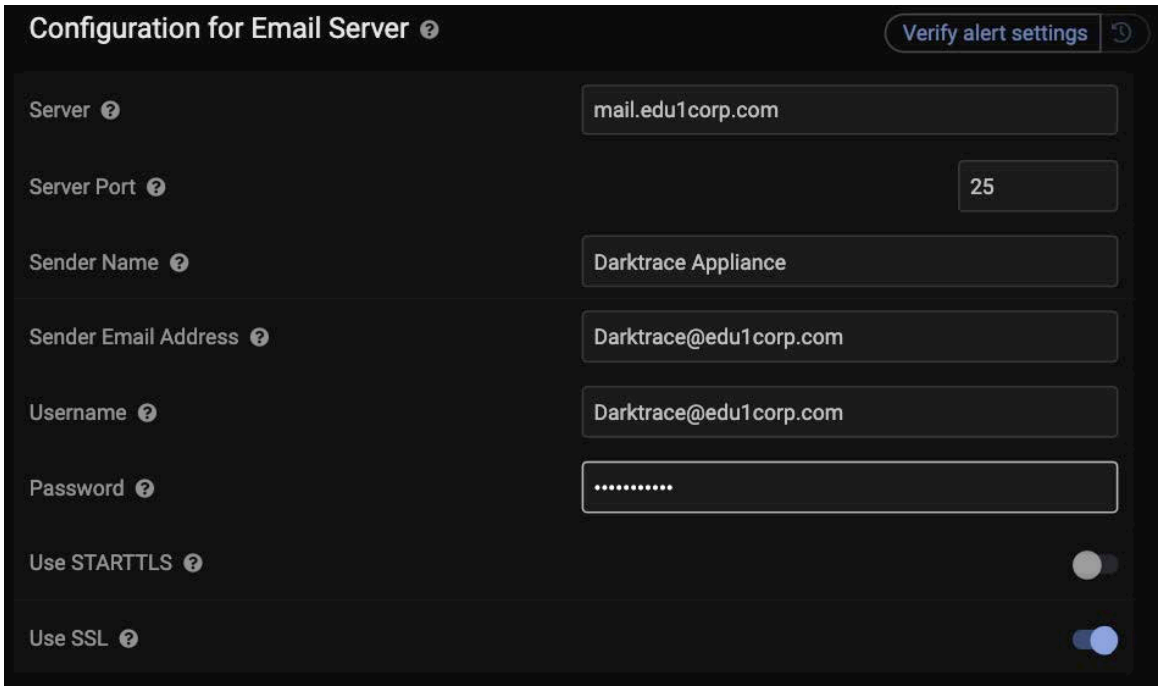


3. In the top right-hand corner of the Workflow Integrations section, click the **Config** button to open a Global Alert Settings option.

4. As there are multiple alerting options available, this Config page allows global thresholds to be enabled or disabled. If different alert types require different thresholds, use the toggle next to **Enable Modular Alert Thresholds**. Close this window once global alert configuration has been decided.



5. Select an **alerting type** from the Workflow Integrations, for example, **Email**.



a. First of all, complete the **Server** and **Server Port** fields to configure which server will be used to send email alerts.

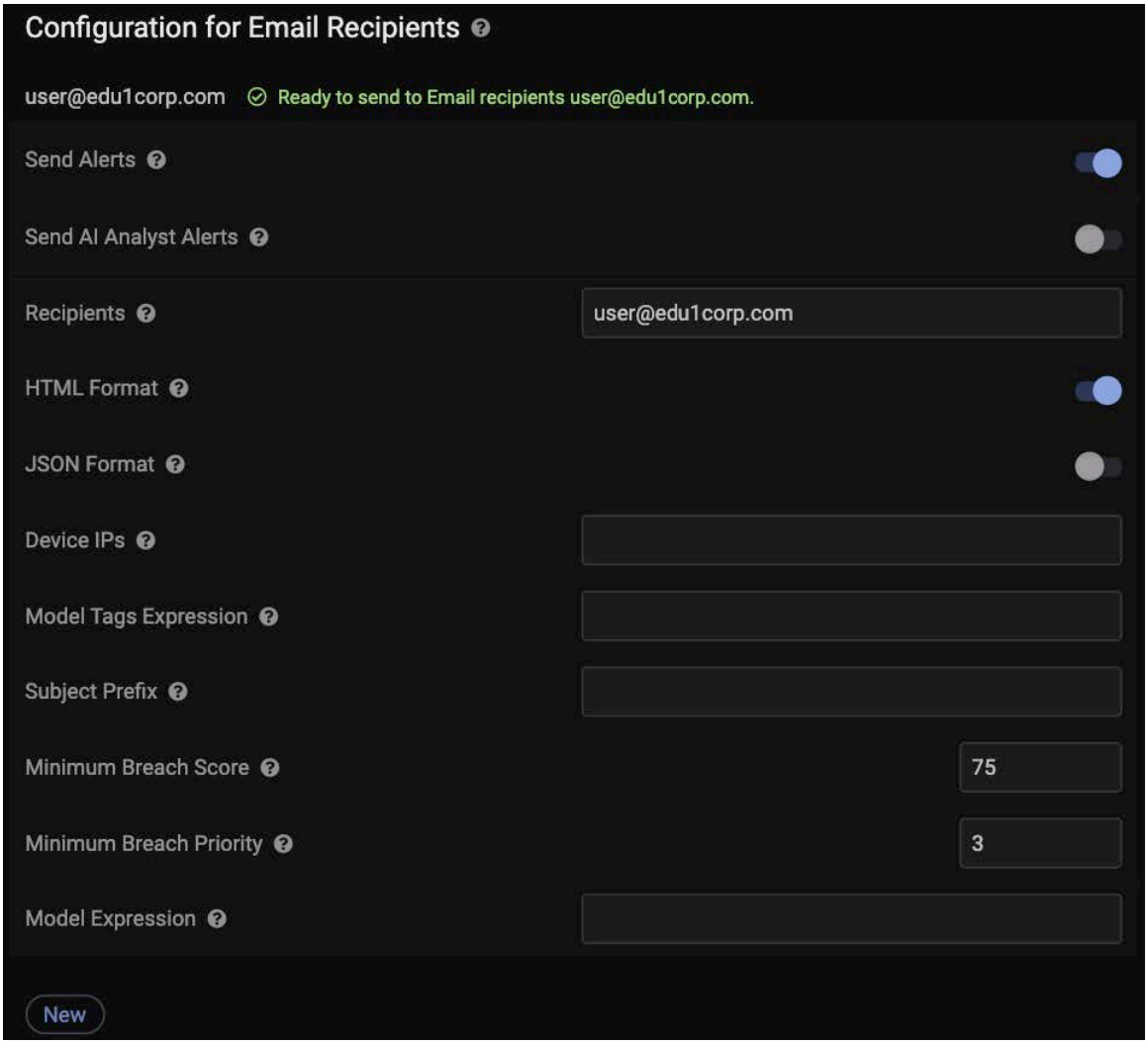
b. Next, provide a **Sender Name** and **Sender Email Address** to set the values which will be observed by the recipient of the alert email.

c. Enter a **Username**, which must match the Sender Email Address, and the associated password so that Darktrace can send email alerts via the server.

d. Finally, the email alerts can use **STARTTLS** or **SSL**. While these mutually exclusive settings are optional, enabling one of them is recommended.

e. Save your changes by clicking **Save** at the top of the window.

6. Multiple alert recipients can be configured in parallel with different restrictions. Once the email server has been configured, click on the Settings tab in the Email Alerts Output window and scroll down to the **Configuration for Email Recipients**.



a. First, decide which email alerts should be sent. It is possible to enable **Model Breach** email alerts and **AI Analyst** email alerts by using the toggles for each respective field.

b. Secondly, enter one or more recipient email addresses into the **Recipients** field. If multiple emails are entered into this field, separate them with a comma.

c. Select a format for email alerts. The options are **HTML Format** or **JSON Format**. If neither are selected, the email will be sent in plain text.

d. By utilizing the **Device IPs** field, it may be useful to configure a list of devices, IPs or network ranges that Model Breaches should be restricted to for the chosen recipients.

e. Another optional filter is the **Model Tags Expression**, which allows you to restrict Model Breaches to those with tags that match the regular expression defined.

f. The **Subject Prefix** field may be utilized for defining a prefix to be used when sending alert emails to the intended recipients.

g. Once the alerting type has been configured, consider what **thresholds** should be breached before being notified.

   i. The **Minimum Breach Score** corresponds to the percentage score displayed when hovered over the colored bar to the left of a Model Breach. These are the scores which can be filtered using the Sensitivity Slider in the Threat Visualizer. Setting the minimum score to 60 will only alert breaches which have a score of 60% or higher.

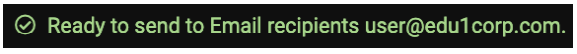
   ii. Every Model has a priority between 0 and 5 which indicates the breach severity. The **Minimum Breach Priority** will restrict alerts to a threshold of greater than or equal to the chosen minimum Model priority.

   iii. The **Model Expression** value can be used to restrict alerts only to Model names that match a certain Regex value.

   Note: *Alerting configuration offers multiple filters which control when an alert should be sent to specific recipients. While it is not necessary to fill out all these values, if more than one alert condition is configured, a Model Breach must meet all selected requirements before alerting can occur.*

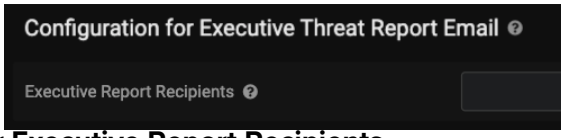
h. **Save** the settings.

If correctly configured, a message will appear to indicate that mail can be sent to the chosen user(s).



7. To add email alert recipients with different conditions, click **New** and repeat the above process.

Within the Email Alerts window, there is an additional option that allows **Configuration for Executive Threat Report Email**. Using the same options as set in the Configuration for Email Server, input the email addresses for **Executive Report Recipients**.

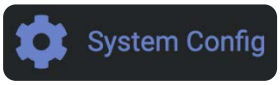


Setting up the Mobile App

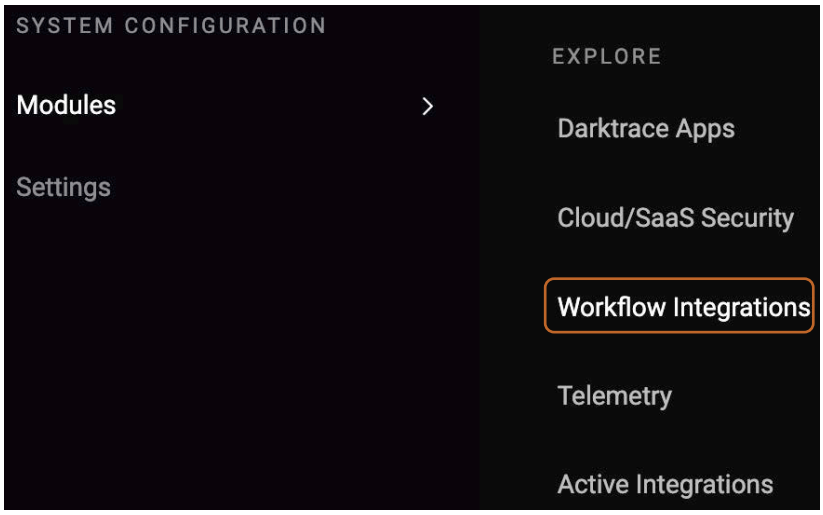
The Darktrace Mobile App, available for iOS and Android, allows users to easily access Darktrace Alerts when they are on the move. In order to associate the Darktrace Mobile app with an existing Darktrace deployment, the Threat Visualizer must be authorized to send alerts. Organizations wishing to use IMAP will experience reduced functionality.

Configuring the App

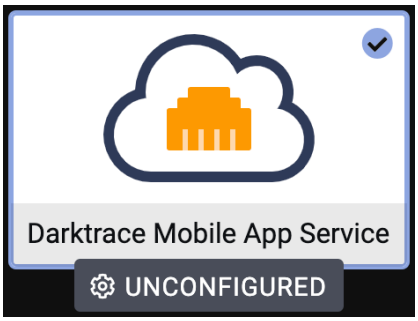
1. In order to configure the Mobile App, the Configuration permission is required to access and change details on the **System Config** page, located under the Admin section of the main menu.



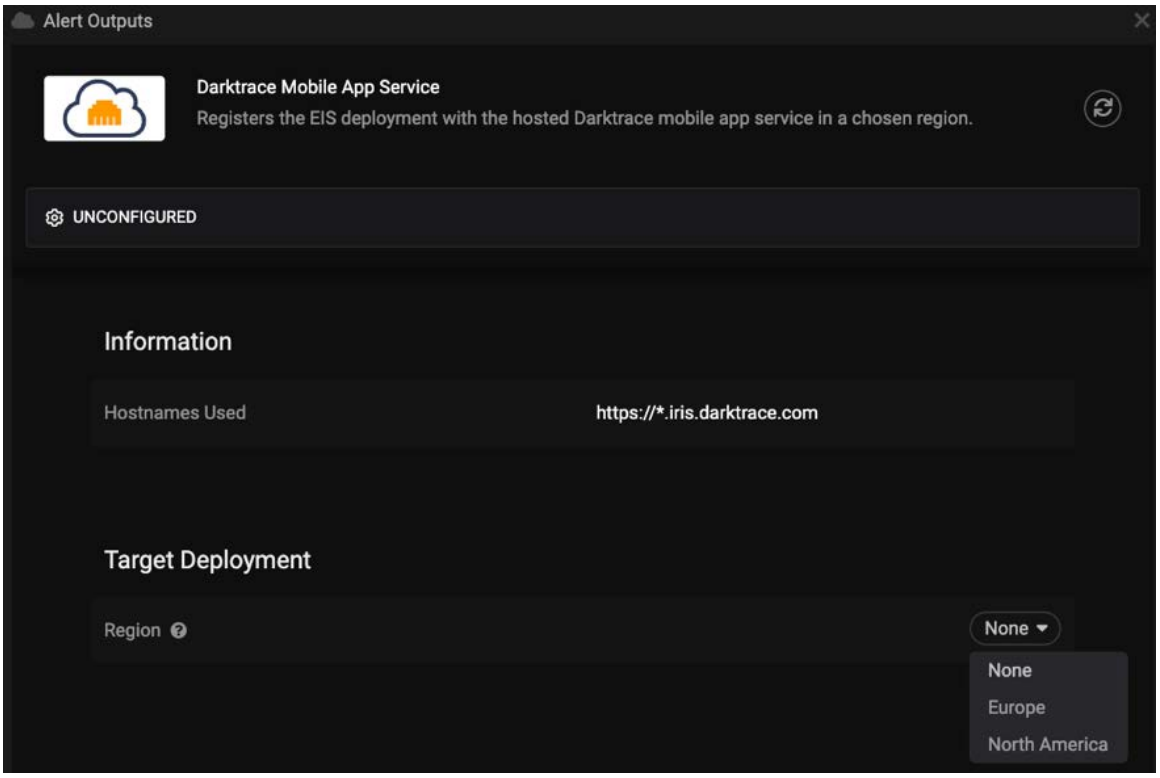
2. From the left-hand menu, select **Modules**.
3. From the Modules options, locate **Workflow Integrations.**



4. Choose the **Darktrace Mobile App Service** module.

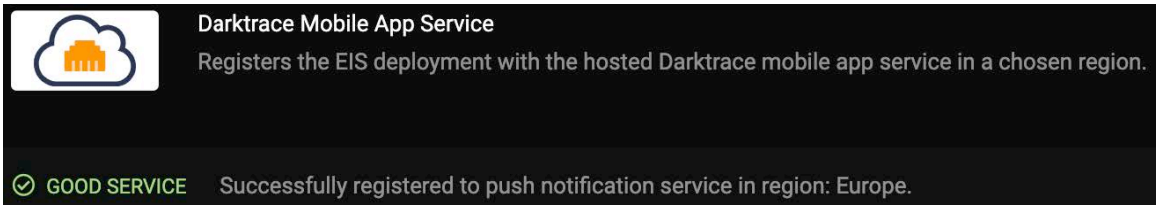


5. A configuration window will open. From the **Region** drop-down menu, select a Target Deployment Region to host the mobile app push notification service.



6. **Save** the change using the button that appears at the top of the window.

7. The **Service Status** should now state that it is **Successfully registered to push notification service in region: [*Chosen Region*]**.



8. The Mobile App service has now been **launched** and is ready for registering and to start receiving alerts.

   Note: *It is imperative to whitelist the hostname https://*.iris.darktrace.com on any existing client firewalls or Darktrace alerts may be blocked.*

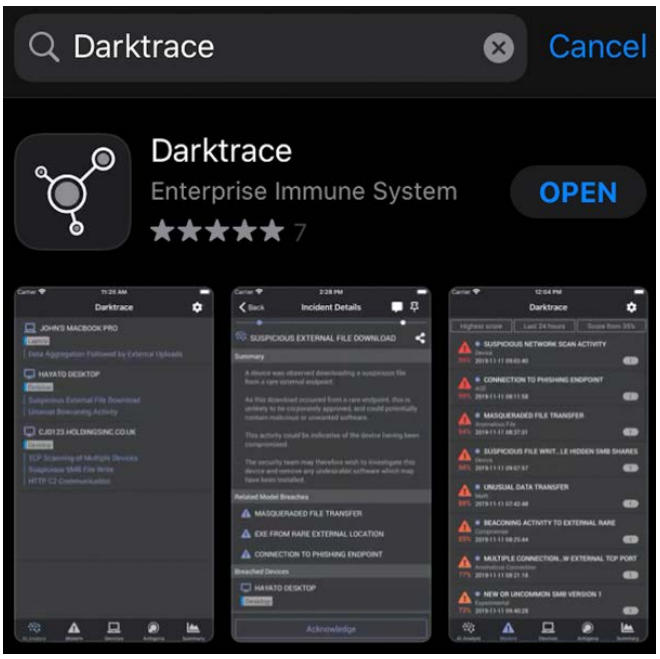
Mobile App Permissions

Mobile App permissions per user can be set by an administrator via the User Admin page. The permission can be revoked at any time. If the administrator revokes Mobile App permissions, the Model Breach, Antigena and summary cached data within the app is deleted for the given user. If a Darktrace user using the mobile app has their Mobile App permission removed, their app will deactivate itself and receive no further data.

Note: *LDAP users must have their app permissions explicitly revoked on a per user basis in the User Admin page. Removing the permission from an LDAP Group in the Group Admin page is not sufficient.*

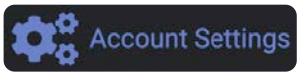
Registering the App

1. On a smartphone, open the appropriate **app store** and search for **Darktrace**. The Darktrace iOS app is available on the App Store and the Android app is available on Google Play. Download the Darktrace app.



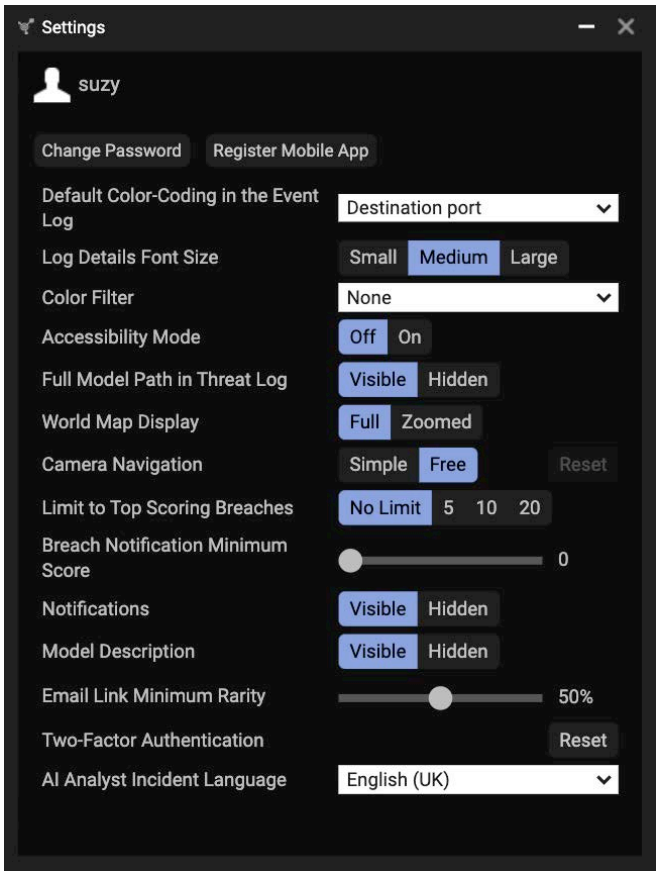
2. Make sure the **Mobile App** is ready and to hand for the next few steps...

3. Navigate to **Account Settings** from the main menu.



4. Click **Register Mobile App** at the top of the dialog.

5. A **QR code** will open in a dialog on the Threat Visualizer.



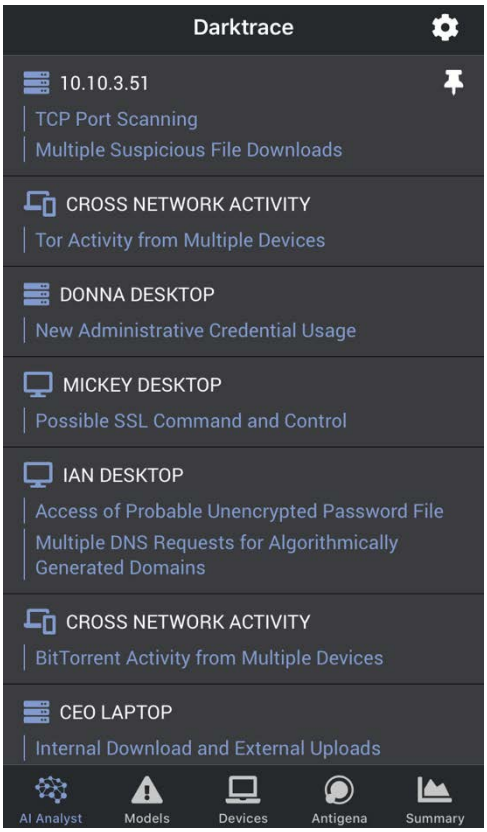
   a. In the app, click Next in order to authenticate with the Darktrace appliance.

   b. The app will request permission to use the smartphone camera. Use the camera to scan the QR code on screen in the Threat Visualizer.

   c. The app should authenticate.

   d. Move between screens using the guided overlay to understand the functionality. This guide can be re-enabled at any point from the app config page.

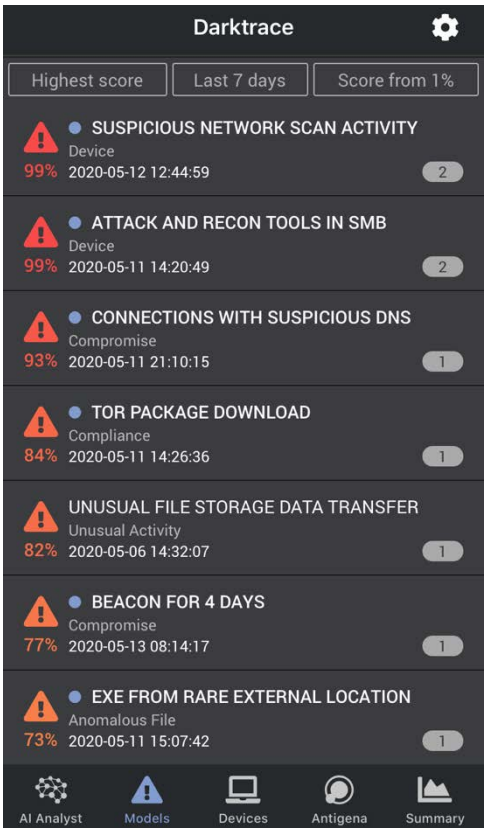
AI Analyst



This screen displays AI Analyst incidents.

- Swipe right to pin.
- Swipe left to acknowledge.
- Tap to review.
  - See timeframe of events.
  - Move between events.
  - Comment on incident
  - Pin incident.
  - Acknowledge single or multiple breaches.
  - Create a short message including a link to the Mobile App incident to be shared or stored as a reminder.
  - Read summary of events.
  - View attack phases involved.
  - List related Model Breaches and devices.
- Drag down to refresh.

Models

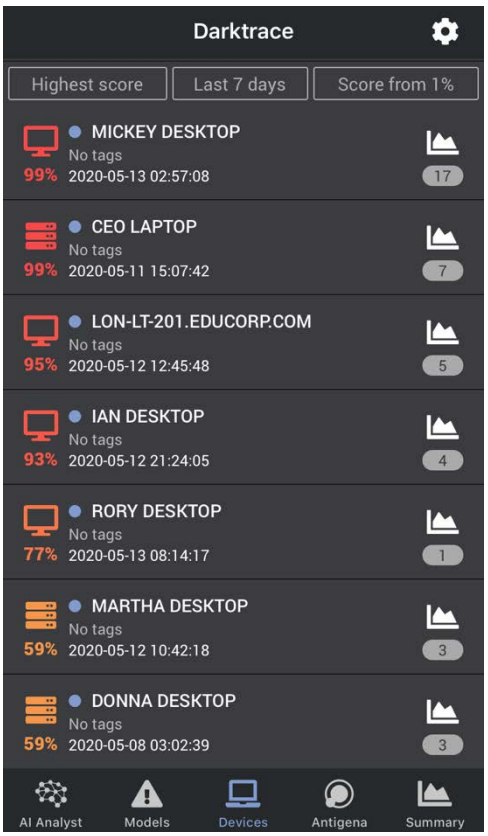


This page lists Models with recent breaches, where each Model is presented on a separate row.

- Visualize how many breaches have occurred for a Model.
- See which breaches are unread.
- Drag down to refresh and reveal a search bar.
- Review Model and Breach details.
  - Mark breaches as read/unread.
    - Swipe left/right to read/unread breaches.
  - List all breaches for a device.
  - Swipe left to acknowledge breaches.
  - Create a shareable link to the Mobile App breach.
  - Comment on breach.
  - Derive geolocations for external locations.
  - View related Antigena Actions.

Devices

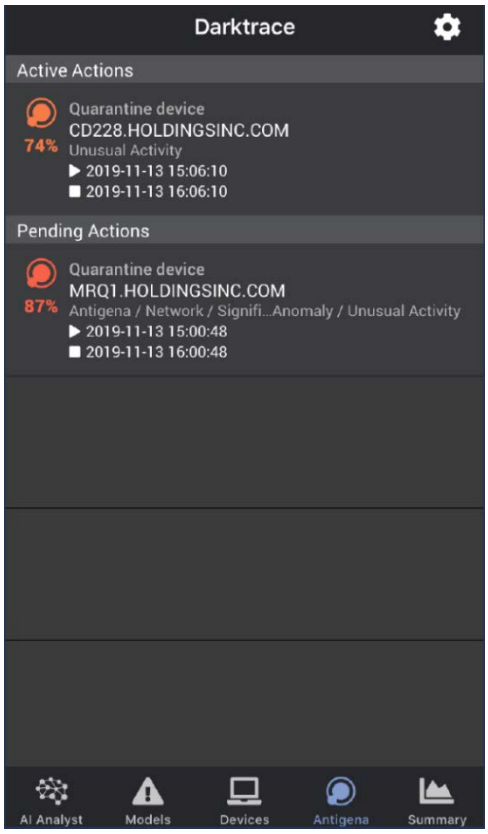
This page lists devices with recent breaches, where each device is given a different row.



- Visualize how many breaches have occurred with respect to a device.
- Swipe right on unread breaches to mark as read.
- Drag down to refresh and reveal search bar.
- View breaches graphically of time frame against breach severity.
  - Click breach dots to view summary.
  - Zoom with two fingers or reset graph.
- Review Device and Breach details.
  - Mark breaches as read/unread.
  - List all Models breached by device.
  - Acknowledge breaches.
  - Create shareable links to the breach.
  - Comment on breach.
  - View related Antigena Actions.

Antigena

The Antigena screen displays Active, Pending, Cleared and Expired Actions.



- View Active devices, currently being controlled by Antigena.
  - Inactive devices are not yet controlled by Antigena.
- Tap an action to review details.
- Swipe left on an Action to make changes.
  - Extend the Antigena Action for a specified time.
  - Activate Antigena to start controlling the device the action specified.
  - Clear the action to stop Antigena controlling the device.
  - Choose time periods to decide how long the Antigena Actions should be Extended, Activated or Cleared.

Summary

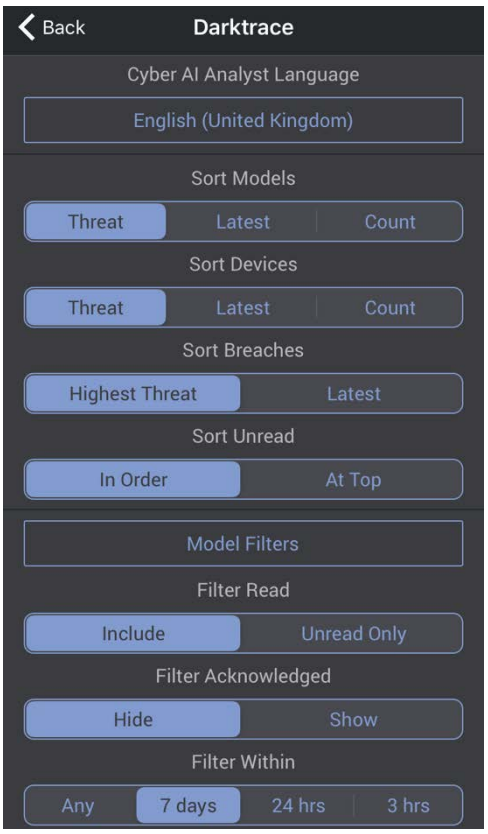
The summary screen mirrors the high-level summary presented on the left of the Threat Visualizer home page.

- View metrics about traffic and devices across the enterprise.
- Number of Antigena actions are indicated.
- Pull down page to trigger manual refresh.

Config

Multiple filtering options and customization for how data is displayed in the app are available on this screen, obtained by clicking the cog in the top right of the app.

- Change the Cyber AI Analyst language.
- Sort Models/Devices and Breaches
- Sort unread in order or highlight them at the top.
- Filter Model Breaches by folder and include read or acknowledged breaches over a set time period.
- Set notification threshold for local, on screen notifications.
- Fetch notifications at controlled intervals.
- Store data on the application on the device.
- Reset tips to familiarize with app.
- Authenticate with Threat Visualizer.
- Set a minimum four-digit pin code.
- Set time required between logins.



Integrating Darktrace: SIEMs and the API

Darktrace can be configured to export information about Model Breaches as they occur, including via syslog to an existing forwarder or indexer for consumption by your organization's SIEM solution. To ensure compatibility with a wide variety of SIEM technologies, the contained information can be formatted as JSON, Common Event Format (CEF), or Log Event Extended Format (LEEF).

Each of these formats provides a corresponding level of detail regarding the Model Breach. The most comprehensive of the above-listed formats is JSON, whose level of detail is most comparable to the output of the following API call:

/modelbreaches?minimal=false&count=1

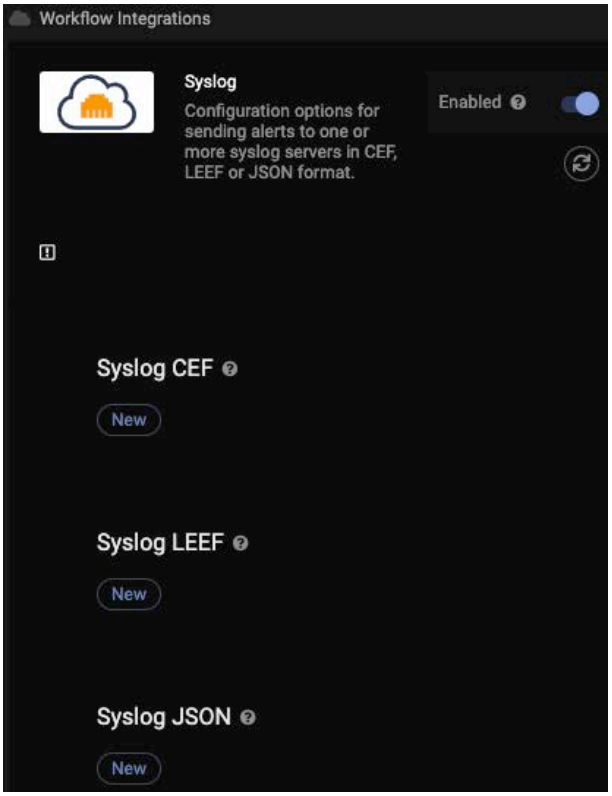
The above can be called in a browser during an active session. For comparison, the CEF and LEEF output is structured as follows:

CEF:0|Darktrace|DCIP|<dcip-version>|<model-id>|<model-name>|<model-breach-severity>|<extra-metadata>

LEEF:1|Darktrace|DCIP|<dcip-version>|<model-name>|externalId=<model-breach-id> src=<source-ip> dst=<dest-ip> shost=ip-<source-ip> srcMAC=<source-mac> message=<model-message> srcType=<device-type> cat=<?> sev=<breach-severity> dhost=<destination-hostname> pid=<policy-id> darktraceUrl=<breach-url> message=<message>

Note that the LEEF format includes the Model Breach URL, facilitating subsequent investigation of the event in the Threat Visualizer.

The exporting of Model Breach details is configured in the Workflow Integrations Module of the System Config page located under Admin in the Main Menu or can be navigated directly to by visiting the ***/sysconfig#modules*** path in the browser. The Syslog Module details options for enabling export to various formats. Setting up JSON/CEF/LEEF alerting via Syslog is similar to the setup for email or mobile app alerts.



Within the Syslog Module on the System Config page, click "New" under one or more of the following:

- Syslog CEF
- Syslog LEEF
- Syslog JSON

Multiple syslog alert formats can be configured in parallel. Furthermore, each entry can have entirely different filters (including one export type with multiple destinations), making syslog exports conveniently customizable.

When choosing a Syslog export type to configure, the selected format(s) will display additional fields for specification of the syslog server, desired port and additional details such as custom field mappings within the output content. The Minimum Score, Minimum Priority, and Model Expression will affect which Model Breaches are exported. When exporting to a SIEM, an organization will often leave these three fields blank to ensure all Model Breaches will be exported.

For more flexible integration, the Darktrace API can be used. The API enables you to poll and retrieve information from your deployment including but not limited to Model Breaches. A full list of programmatically accessible API calls and parameters can be found on the Customer Portal in the Expanded Darktrace API guides.

As in the case of ***/modelbreaches***, an API endpoint that uses the GET method can be triggered by visiting the corresponding URI during an active browser session. Review of the JSON response is often helpful in planning and testing. Some endpoints use the POST method - these perform actions within the Darktrace software. An example is ***/acknowledgeevent***.

In order to make use of the API outside of an active browser session, you must generate a pair of API keys. This process is described in the *Acquiring the API Token Pair* section of the *API Product Guides* which also lists programmatically accessible API calls and their parameters. This process is carried out in the System Config page.

While the meaning of many of the key-value pairs returned from an API call will be apparent or can be derived from context, a few are worth specific mention. A number of unique identifiers can be found in the returned data structures, a partial list of which follows:

did	Device ID, unique per device.
sid	Subnet ID, unique per subnet.
cid	Component ID, unique per component.
chid	Component history ID, unique per historical version of a component.
pid	Policy ID (model ID), unique per model.
phid	Policy history ID (model history ID), unique per historical version of a model.
pbid	Policy breach ID (model breach ID), unique per model breach.

These unique identifiers are primarily useful as avenues to retrieving further information. For example, given a particular device ID, you can request various information associated with the device, including those details normally found in the corresponding Event Log or Graph in the Threat Visualizer:

- ***/details?did=1&count=50&eventtype=unusualconnection***
- ***/metricdata?did=1&metric=connections&from=2020-04-01T00:00:00&to=2020-04-15T00:00:00***

Using multiple API calls, and retrieved IDs as part of subsequent requests, one can quickly aggregate a comprehensive data set around a group of devices, a series of events, a portion of the network, or breaches from a specific Model etc.

Once you are familiar with the individual calls and the information they return, you can decide how best to combine them. As an example of API use, the Threat Tray retrieves the summary information of Model Breaches grouped by Model, device, and user credential, but leaves it to the user to decide which additional information to view next, if any.

The Dynamic Threat Dashboard goes on to retrieve a predefined set of data for each Model Breach. These two examples reflect a balance between flexibility and anticipation of need, but both are geared toward universal utility among a variety of users. For your own more specific use cases, you may take a more targeted approach.

A script that generates a report for internal use might operate on a static set of parameters, thereby involving as little user interaction as desired, and still retrieve detailed information specific to your organization's need. A custom dashboard or modifications to the existing dashboard with a custom browser extension can help standardize sequences of actions commonly performed by members of your team.

The following are examples of API calls that can be performed via the browser during an active session as a way of becoming familiar with the content and format of responses (adjust time frames, and IDs as necessary):

- ***GET /modelbreaches?from=2020-05-01T00:00:00&to=2020-06-01T00:00:00 &includebreachurl=true***
- ***GET /details?pbid=12345***
- ***GET /details?did=1&count=100&eventtype=connection&intext=external***
- ***GET /mbcomments?pbid=12345***
- ***GET /network?metric=datatransfervolume&from=2020-05-01&to=2020-06-01***
- ***GET /metricdata?did=1&metric=datatransfervolume&from=2020-05-01&to=2020-06-01***

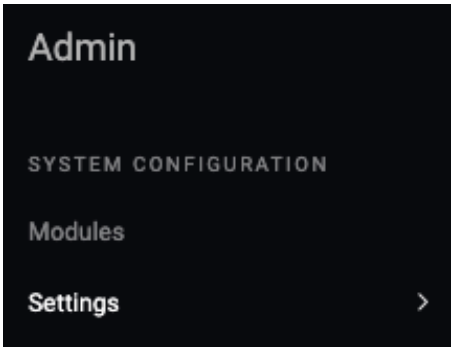
API Exercise - Try This:

- Consult The Threat Visualizer API Product Guide on the Customer Portal to craft a GET request URI to retrieve each of the following:
  - A list of all Models.
  - A list of all devices modeled by Darktrace in the last 30 days.
  - A list of all subnets modeled by Darktrace in the last 30 days.
  - Information on an external endpoint, including a list of network devices that have recently communicated with it.
  - A list of the last 10 Model Breaches that occurred on a specific device.
  - A list of the last 20 comments made on Model Breaches.
  - The metric data needed to graph a specific device's internal and external data transfer.

10. Configuring Darktrace Settings

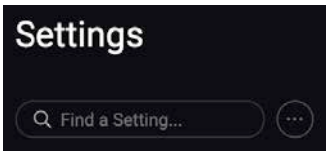
Again, within the System Config page, there are many configurable elements.

This section outlines configurable which are outside of the Modules page – in the Settings page.



Due to the sheer number of fields, it may be preferable to narrow down the page to relevant sections.

Notice the search bar at the top of the page. Utilize this to make the following workflows easier to carry out.

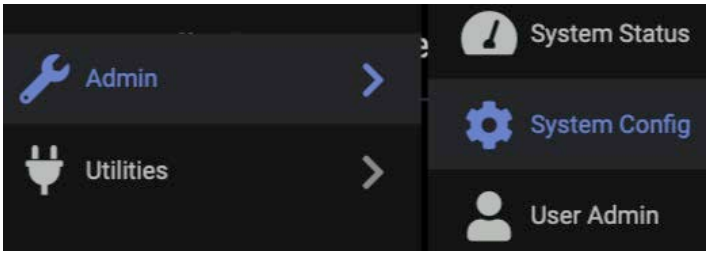


LDAP Configuration

The Threat Visualizer supports connections to LDAP servers such as Active Directory. This integration can be configured to provide additional functionality. Firstly, it can enable authentication to the Threat Visualizer interface by using credentials from an LDAP server. Secondly, it can enrich the device details observed within the Threat Visualizer by providing LDAP attributes for users.

1. From the main menu, navigate down **Admin** and locate the **System Config** option.

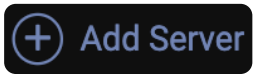
   This will open the System Config page in a new tab.



2. With the **Settings** submenu selected, scroll down to locate the **LDAP/Active Directory** section.

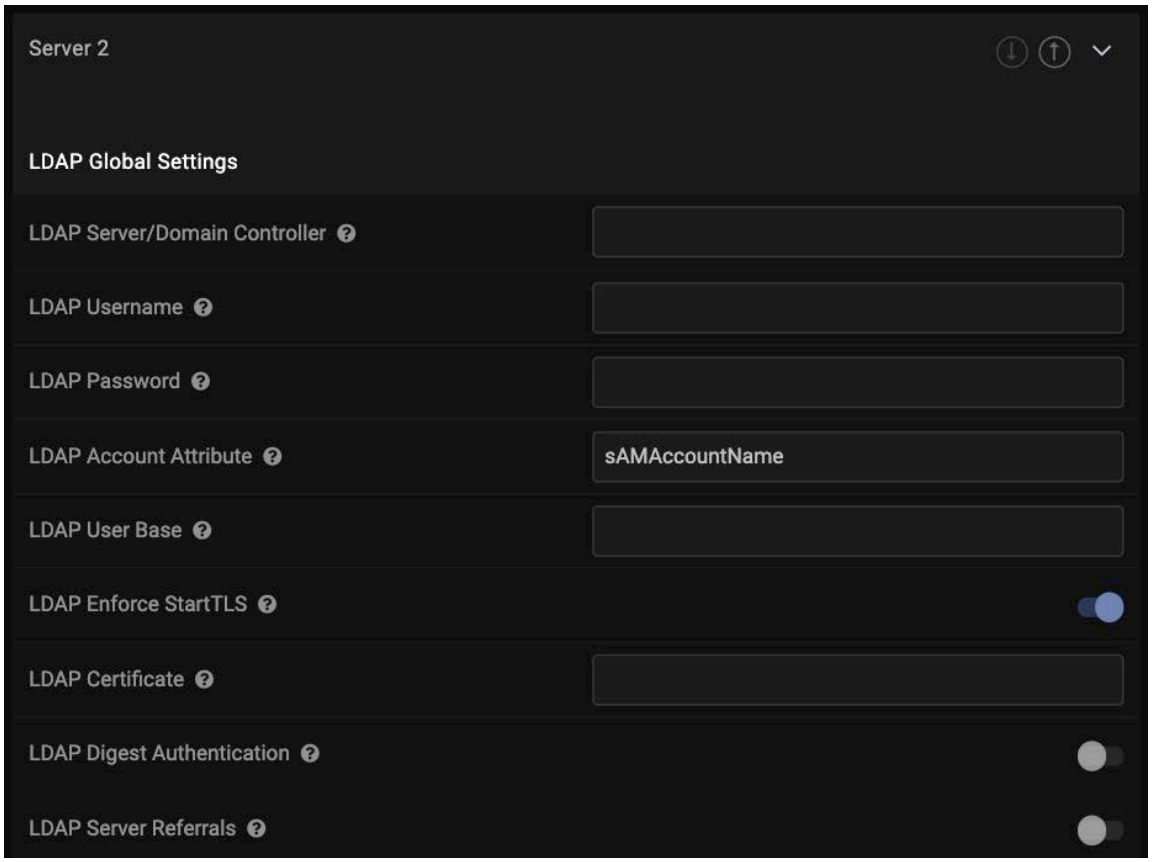
3. **Existing servers** which have been previously configured will be displayed here. Click the minus icon at the end of the row to expand and review the details.

4. To configure a new server, click **Add Server** to open up a new dialog containing a range of fields to be filled out.



   Note: *Existing servers which may have already been configured will be displayed as an entry. Click existing entries to view the fields.*

5. Within the resulting **LDAP Global Settings** window, a range of options are available. Hover over each **tooltip** icon when working through the fields to fill out the information.



a. Fill out the **LDAP Server/Domain Controller** with an IP address or hostname. The path to the LDAP Server location can be set at ldap://hostname. If using SSL, the input can be of the form ldaps://hostname. With this option, ensure that LDAP Start TLS is set to false.

   Note: *Port numbers can also be configured, for example, ldapserver.darktracetraining.com:1389. Hover over the tooltip icon for more information.*

b. For the **LDAP Username**, specify a username with credentials that Darktrace can utilize to access the LDAP server. For example, *darktrace@examplecompany.com*, *cn=darktrace, cd=examplecompany, dc=com.*

c. Enter a corresponding password into the **LDAP Password** field for this user which can be used to log in and connect to the LDAP server.

d. In the **LDAP Account Attribute** field, provide an LDAP attribute to match user credentials with. By default, this will be sAMAccountName, but a user search field is also supported. A replaceable string example is for doing this is outlined in the tooltip.

e. Set the **LDAP User Base** path to identify the users in the LDAP tree. For example, *ou=users, dc=company, dc=com*.

f. Darktrace supports multiple methods of secure LDAP integration: **LDAPS** (LDAP over SSL) or LDAP with **STARTTLS**. While these settings are optional, having a secure method is strongly recommended. Note that only one of the two modes can be enabled at a time.

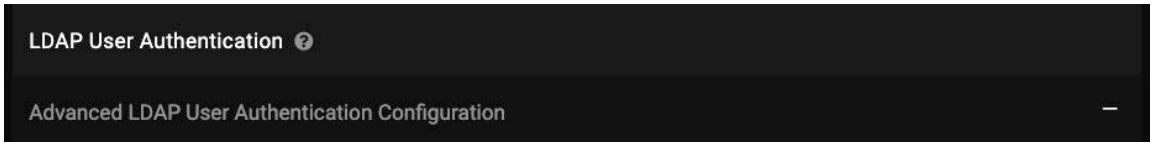
   If LDAPS has been configured in the LDAP Server/Domain Controller field, LDAP Enforce StartTLS must be disabled. If not, the **LDAP Enforce StartTLS** can be enabled using the toggle.

g. An **LDAP Certificate** is optional for both forms of encryption. Omitting a value disables certificate validation.

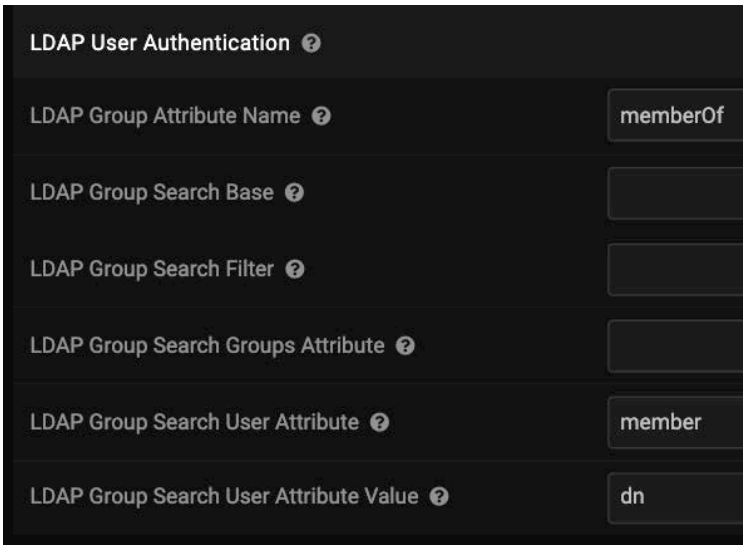
h. Another optional field allows you to enable **LDAP Digest Authentication** if SASL authentication desired.

i. Enable the **LDAP Server Referrals** field if they are in use.

6. Below the Global Settings for the new server is a **LDAP User Authentication** section. This configurable section allows your department to log in to Darktrace using Active Directory or LDAP credentials. Click the minus sign at the end of the row to expand advanced settings.



__Note:__ Advanced Settings are typically not required for standard Active Directory deployments.



7. Again, fill out the appropriate values.

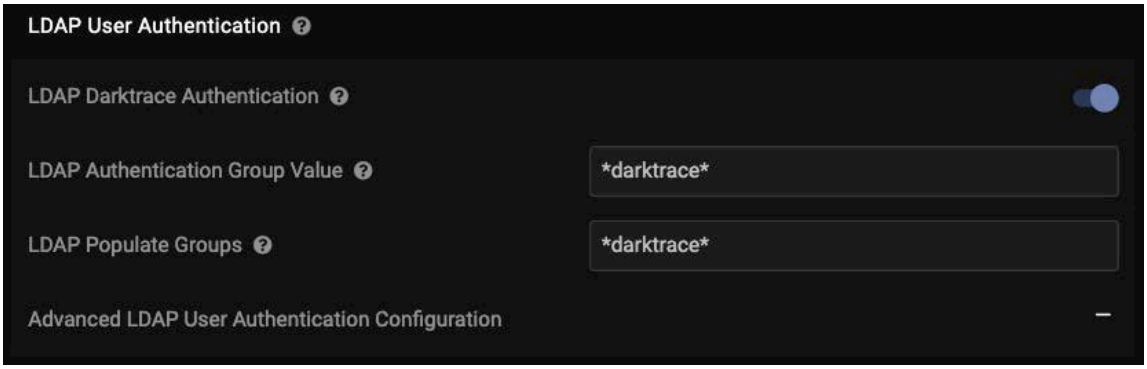
   Some of the fields have **pre-populated default values**. Use the tooltips next to each field if you choose to modify any of them.

   Remember to **Test LDAP** after any changes have been made.

8. With any changes made, remember to click the **Save Changes** button presented at the top of the screen.

9. At this point, it is advisable to use the **Test LDAP** button at the top of the **LDAP/Active Directory** section.

10. Moving down the page, notice a separate **LDAP User Authentication** subsection, under the **LDAP/Active Directory** section.

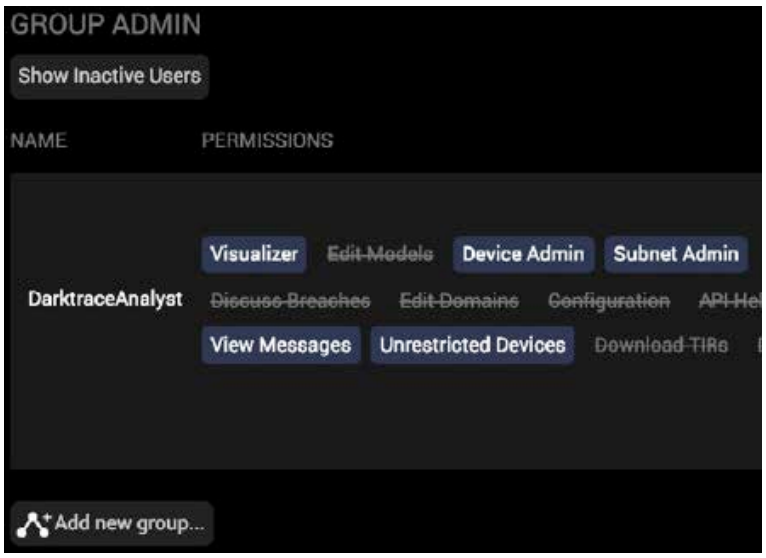


a. Enable **LDAP Darktrace Authentication** to allow users to login to Darktrace using their LDAP credentials. Note that this option can only be used for encrypted connections.

b. Use the optional **LDAP Authentication Group Value** field to restrict usage of LDAP authentication for logging into Darktrace to specific groups. This field is not case sensitive and will also support wildcards.

c. The **LDAP Populate Groups** field can retrieve and present groups in the Group Admin page. If an LDAP user meets the correct criteria to access Darktrace, the Threat Visualizer can retrieve other groups they are a member of. These other groups can be used to assign permissions and network visibility. This can be useful for security teams who are divided into different regions or platforms.

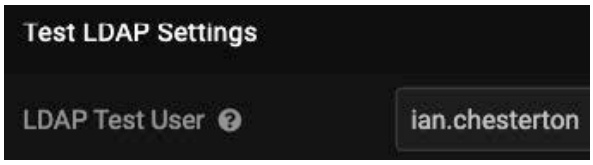
When logging into the interface for the first time after LDAP is enabled, navigate to **Group Admin**. Any groups for a user in LDAP matching the LDAP Authentication Group value will be automatically created. When a new Group is created, ensure that user permissions for the group are updated in Group Admin to match to desired authorization.



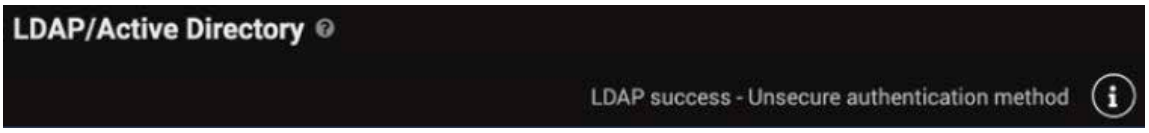
d. Click the minus button to expand the **Advanced LDAP User Authentication Configuration**.

The **LDAP Metrics** field should now be visible. Enter metrics, separated by commas, to be sent to LDAP in order to enrich credentials.

11. Before changing the any of the **LDAP User Attributes** values in the next section from their default, set a valid and identifiable **LDAP Test User**, as seen in the Threat Visualizer.

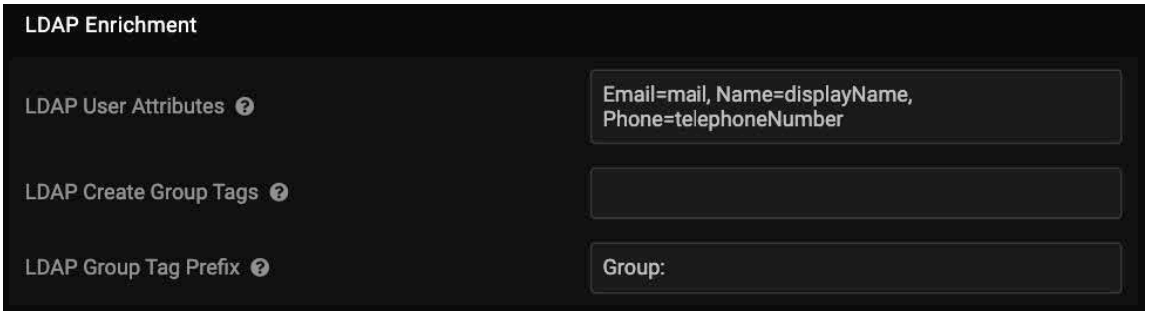


12. Click the **Test LDAP** button at the top of the LDAP section to perform a test of the settings which have been configured so far. If the test was successful, a message will be displayed. Unencrypted connectivity can also be highlighted here.



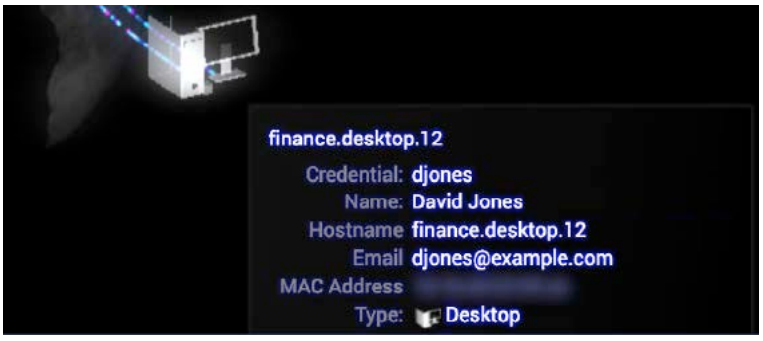
13. Click the **tooltip** icon to review the list of **attributes**. (If the test user is not valid or unidentifiable, the tooltip icon will not appear.) Both mapped and unmapped attributes will be listed, where mapped attributes are the pieces of information presented in the user interface. However, all attributes are available for appending to the information displayed in the Threat Visualizer.

14. Now, navigate to the **LDAP Enrichment** heading of the LDAP/Active Directory section.



a. Review the **LDAP User Attributes** field to begin appending details. Attributes are set as key-value pairs, for example, Email=mail, where the first part (i.e. Email) can be any term shown in the interface, but the second term (i.e. mail) must be specifically returned by LDAP or no value will be found.

The **Threat Visualizer** will not display these details until the user next logs in and their credentials are captured. Once refreshed, the new user LDAP attributes will be visible by hovering over a device in the Device View.



b. Within the same LDAP Enrichment section, locate the **LDAP Create Group Tags** field. The value of this field is used to match LDAP groups. Groups that match the value will generate tags and users in the matching group will be tagged automatically. This field supports wildcards, multiple comma-separated values and is not case sensitive.

c. When tags are created, a prefix is inserted before the group name to indicate the tag refers to an LDAP group. By default, this prefix is “Group:”, and as an optional step, this can be modified in the **LDAP Group Tag Prefix** field.

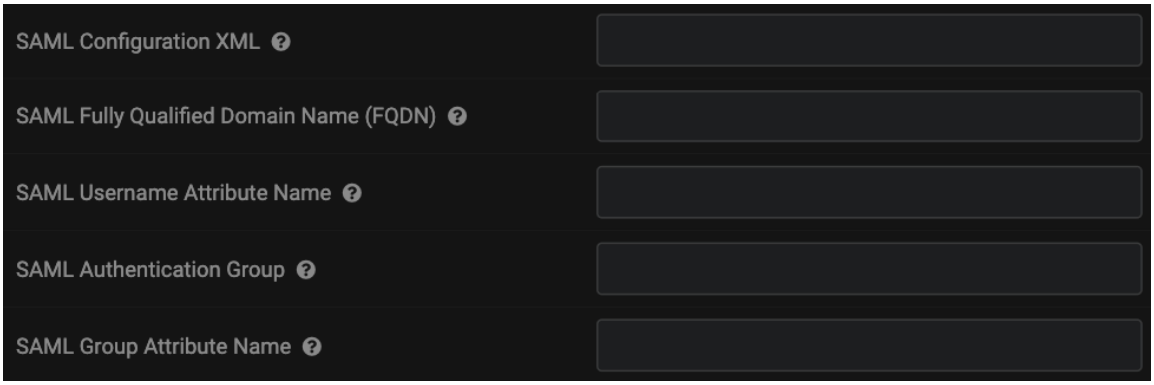
15. Once LDAP configuration is complete, remember to click **Save Changes** at the top of the section.

SSO Configuration

The Threat Visualizer supports SAML2 SSO. Single Sign On can be configured within the Threat Visualizer System Config page. Please note that SSO is not compatible with the Mobile App.

1. Navigate to Settings section of the **System Config** and scroll down and locate **SSO Configuration**.

2. There are five fields to be filled in.



   a. Begin by entering the SML metadata XML from your ID provider into the **SAML Configuration XML** field.

   b. Next, enter a valid domain into the **SAML Fully Qualified Domain Name (FQDN)** field. This must correspond with the FQDN of the Darktrace instance which SSO is configured for. This value is the entity id in the SAML SSO ID Provider.

   c. Enter the **SAML Username Attribute Name**. The expected NameID format is outlined in the tooltip.

   d. Input the **SAML Authentication Group** to restrict usage of single sign on to specific groups of users.

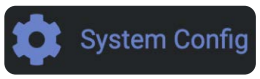
   e. Finally, enter the **SAML Group Attribute Name**.

Configuring HTTPS Certificates

Darktrace Appliances are shipped with a self-signed certificate for the hostname “dt-XXXX-YY” - the internal appliance hostname as designated by Darktrace. Self-signed certificates are often not trusted by web browsers and therefore a warning which needs to be dismissed may be displayed before accessing the Threat Visualizer interface. Additionally, it is common practice for companies to have their own appliance naming conventions, and it is likely the Darktrace designated name will not fit into such a scheme. Uploading a valid HTTPS certificate will prevent web browser warnings that the connection uses an invalid certificate.

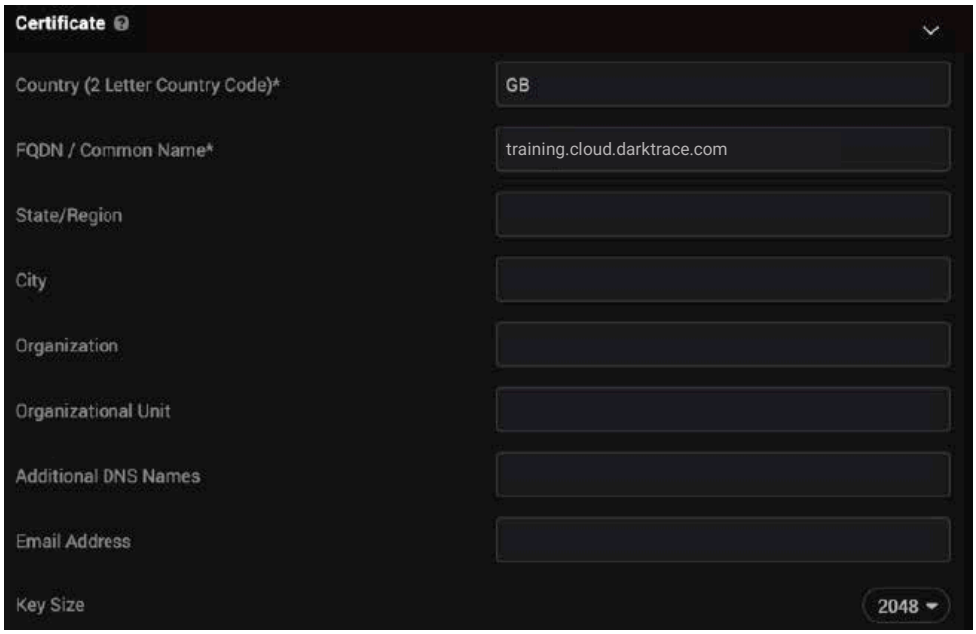
Note: *In some browsers, this warning may be indicated by a red line through the https part of a URL.*

1. Within the Threat Visualizer, navigate to **System Config** within the Admin section of the main menu and open the Settings page.

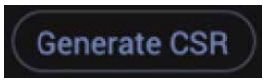


2. Scroll down the page, locate the **Certificate** section and click **New**.

3. A series of fields will appear requesting additional information. Complete as much information as possible with at least the **Country** and **Fully Qualified Domain Name** (FQDN) populated.



4. With the minimum requirements filled in, a **Generate CSR** button will appear. Click this to use the supplied information to generate a Certificate Signing Request in PEM format.



5. **Copy the CSR** to a file and provide it to a **Certificate Authority**, such as DigiCert or GoDaddy, who will provide a certificate in return for a nominal fee. A local Certificate Authority may be used provided the facility is available and users of the appliance are likely to have the root certificate present on their connecting clients.

6. Upon receiving the certificate back from the Certificate Authority, return to the HTTPS Certificate section and paste the PEM encoded contents of the certificate into the **Certificate** field.

7. Click **Save** to apply the change. Reload the Threat Visualizer and confirm that the invalid certificate warning has gone.

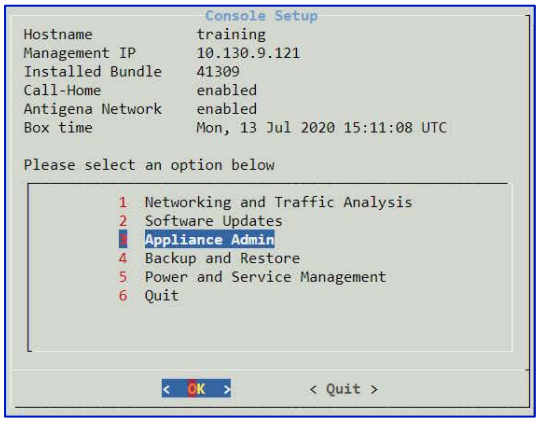
11. Exporting Advanced Search

The logs presented in Advanced Search are rich in information and can be exported from a Darktrace appliance to external log storage. The export is performed at a stage between Deep Packet Inspection and data insert into Advanced Search, so logs will only be exported from the point of configuration onward. This means that system notices will not be included. Following the next steps enables you to export the Advanced Search data to Elasticsearch (v.6 and v.7) or TCP JSON format (suitable for SIEMs or Splunk environments).

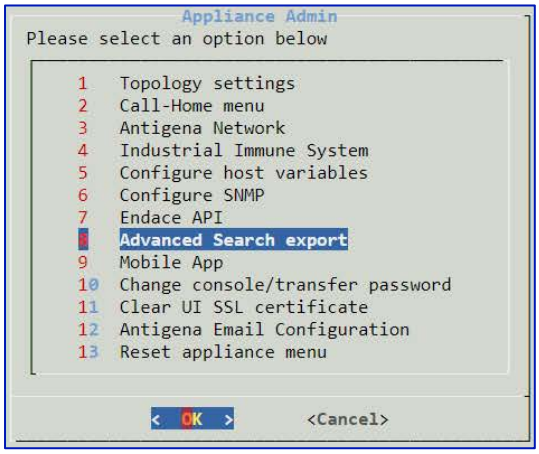
To export Advanced Search, you must have a Darktrace Appliance running at least version 4.0, access to the appliance console, a configured Elasticsearch cluster or external log server and, if necessary, a relevant firewall exception which allows Darktrace to connect to the external log location. Advanced Search export can be removed by re-attempting configuration and providing a blank value in the hostname field in the first prompt.

Note: *In order to configure HTTP and Kafka exports, you must get in touch with your Darktrace representative as this can only be carried out by a member of Darktrace support.*

1. Log in to the **Console** interface and view the options displayed. Using the keyboard, go down to the third option, **Appliance Admin**, and select OK to proceed.



2. Under the Appliance Admin option, select option 8, **Advanced Search export**, before clicking OK.



3. There are two export options available. Follow the appropriate steps below for the different export types.

   Note: *Advanced Search logs can be sent to external tools, but if there are multiple masters/probes generated such data, the same process will need to be carried out on them all.*

4. With both options, there will be a window which asks, "**Would you like to set a customer filter on outgoing messages?**". This may be desirable to prevent duplication and reduce the volume of messages exported to the external log server where some types of traffic are already being ingested from other sources (e.g. VPN logs, DNS queries).

   Configuring filters can be tricky and the supported syntax must be followed.

   a. Each field can be filtered on **Fields[<fieldname>]**. Single quotes (') should be used for variable names.

      Example: **Fields[@type] == 'conn'**

   b. **Regular expressions** must be enclosed by **forward slashes**.

      Example: **Fields[dest_ip] !~ /^192\.168\.10\./ && Fields[dest_ip] !~ /^10\./**

   c. When specifying a value, the **type of data matters**. For example, *Fields[dest_port] != '53'* will not work because the data type is numeric. However, *Fields[dest_port] != 53* will work.

   d. The **relational operators** that can be used are:

==	equals
!=	does not equal
>	greater than
>=	greater than or equal to
<	less than
<=	less than or equal to
=~	regular expression match
!~	regular expression negated match

   e. There are three **logical operators** which are supported:

()	Parentheses for grouping expressions
&&	AND (higher precedence)
||	OR

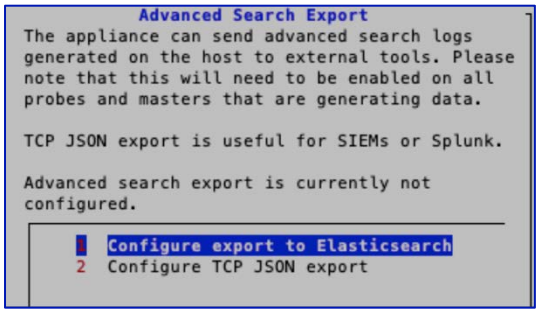
   f. **Special syntax** that can also be used are TRUE, FALSE and NIL, where the latter can be used to test the existence or non-existence of a field variable.

   Further examples:

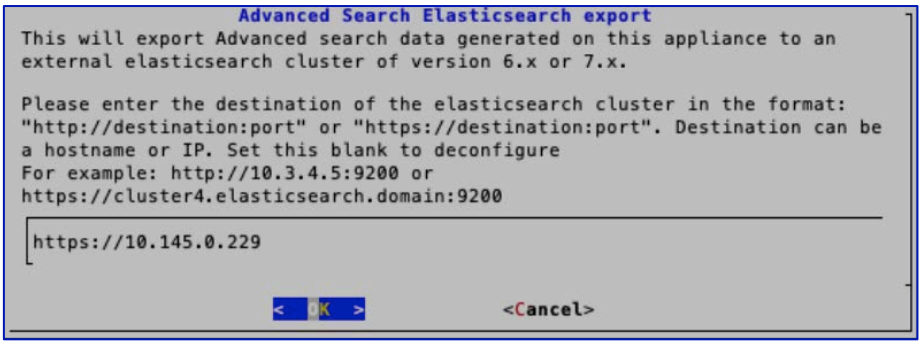
```
Fields[@type] == 'conn' || Fields[@type] == 'conn_long'
Fields[dest_port] != NIL
Fields[source_ip] =~ /^10\./ && Fields[dest_port] != 53 && Fields[@type] != 'ssl'
```

Configure Export for Elasticsearch

1. Select option 1, **Configure export to Elasticsearch**, to begin the process of configuring Advanced Search to send logs from the current appliance to Elasticsearch.



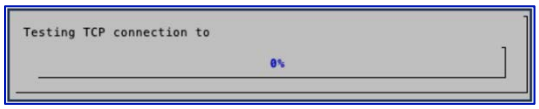
2. You will be prompted to enter the **destination of the Elasticsearch cluster** where the logs are to be exported into the empty field.



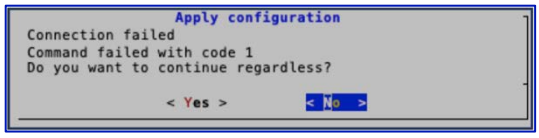
   Insert the HTTP or HTTPS destination of the cluster in the format of http(s)://destination:port. If using HTTPS, the connections will be encrypted, but certificate validation is not performed. Once inserted, select OK.

   Note: *Mapping files for Elasticsearch version 6 and 7 will be placed in the transfer directory of the Darktrace appliance; please retrieve the mapping file for the relevant version. The mapping template assumes that the default index name will be used for exported logs. If you plan to use a custom index name, please adjust the mapping template appropriately.*

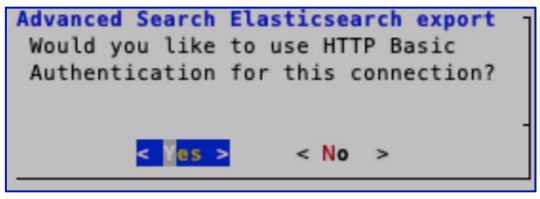
3. A **progress bar** will appear to indicate the **TCP connection** to the Elasticsearch cluster is being **tested**. Ensure that any necessary firewall exceptions have been made to allow communication.



   Failed connections must be resolved before logs can be successfully exported but you may still proceed with the configuration at this stage.

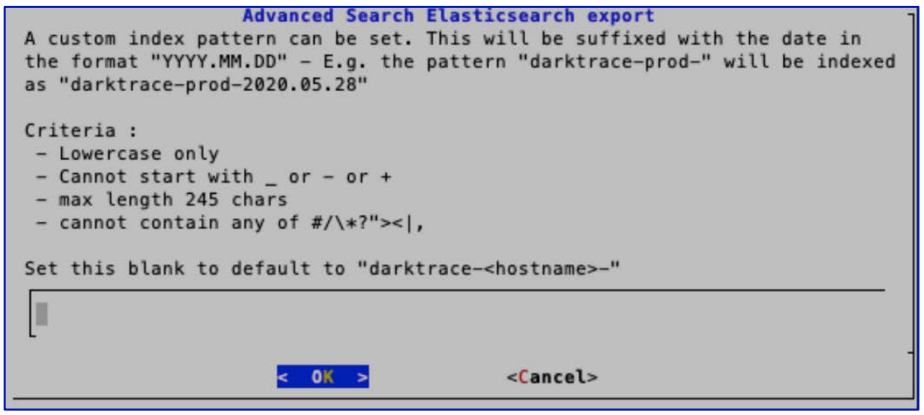


4. You will be asked if you would like to use **HTTP Basic Authentication** for the connection. Darktrace recommends using this authentication for best security practice. If selecting Yes, you will be prompted to input a username and password, where the credentials must be valid for a user with permission to index data in the Elasticsearch cluster.



   Note: *The password must not contain double quote characters (“).*

5. At this point, you will be prompted to input a **custom index pattern**. All patterns will be suffixed with the date in the format "YYYY.MM.DD".



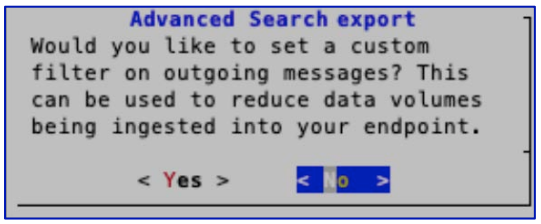
Example: The pattern "darktrace-123-" will be indexed as "darktrace-123-2020.07.15".

Index patterns have a few rules; they must be lowercase with a maximum of 245 characters, cannot begin with _,- or + and cannot contain special characters *(# / \ * ? " < > | , .)*.

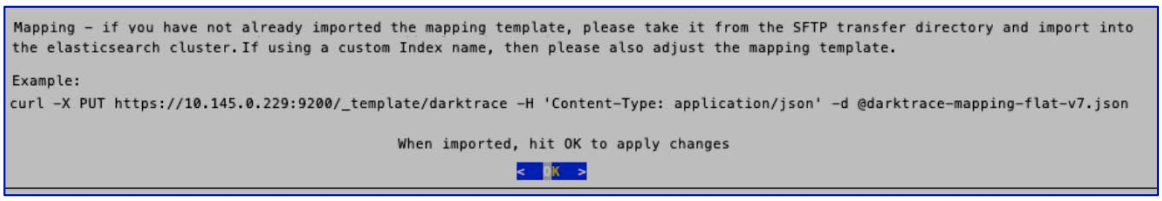
A blank index pattern will default to "darktrace-<hostname>-". Select **OK** to proceed.

6. An optional step is creating **custom filters**.

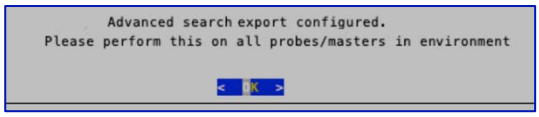
   Click Yes and follow the guidance on filter syntax to apply filters or click No to proceed without.



7. Now, a prompt will appear. Confirm you have **imported the mapping file** provided earlier into your Elasticsearch cluster and made any necessary changes to the default index specified in the file. Click **OK** to confirm.



8. Finally, the configuration will be applied. Click **OK** to close.

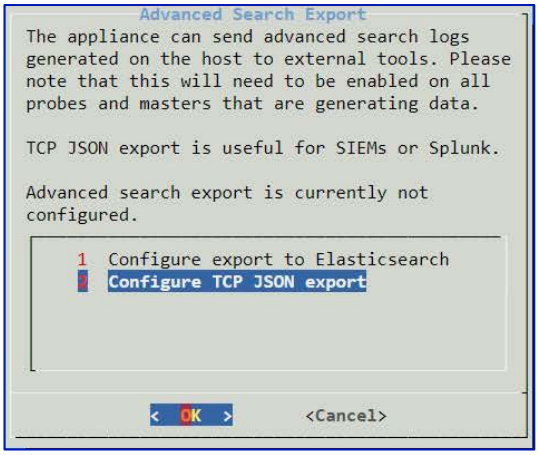


Configure Export for TCP

1. Select option 2, **Configure TCP JSON export,** to begin the process of configuring Advanced Search to send logs from the current appliance to a third-party tool.

   This option is useful for integrating with SIEMs or Splunk.

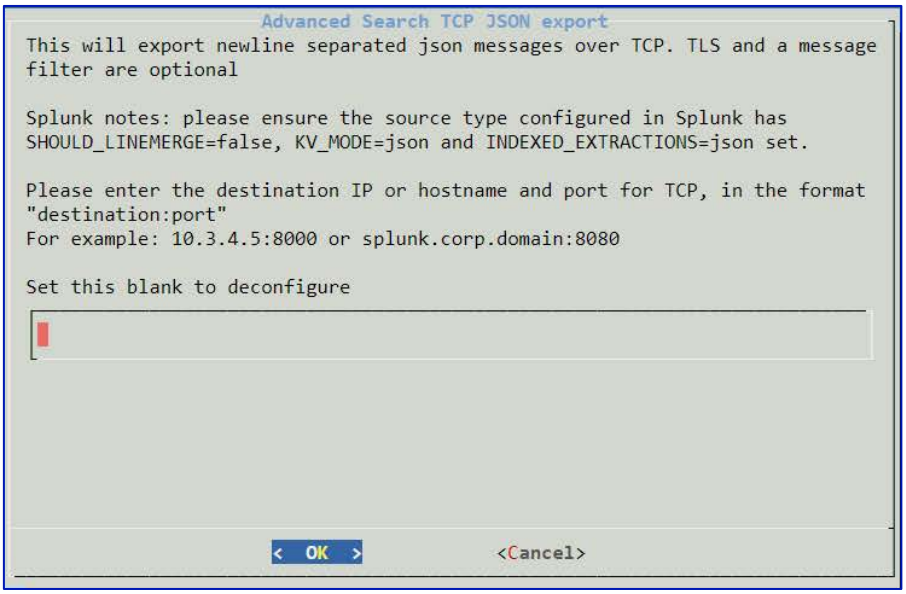
   Press **OK**.



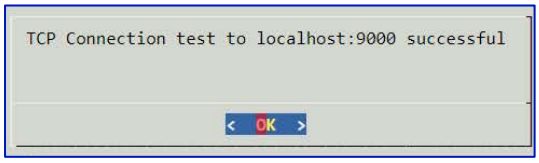
2. A message will appear on the screen. Suggested inputs are noted on this page, such as destination:port.

   Input a value, for example, your **server name followed by the appropriate number**.

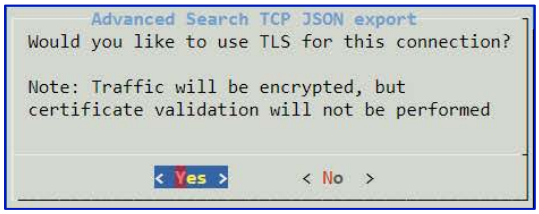
   Then click **OK**.



3. If the **TCP connection test** is successful, a message will appear. If it is unsuccessful, you can still proceed, but will not be able to export logs until the connectivity issues have been resolved. Click OK to proceed.

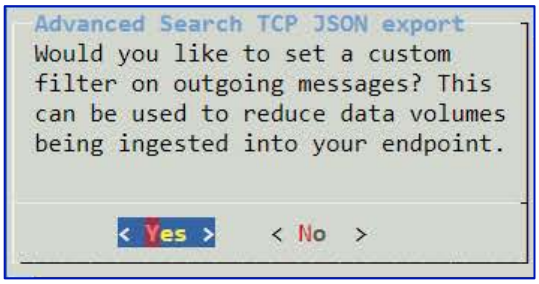


4. Next, the console will ask, **Would you like to use TLS for this connection**? Darktrace recommends using TLS for best security practice. Selecting Yes will encrypt the traffic. Note that certificate validation will not be performed at this stage.

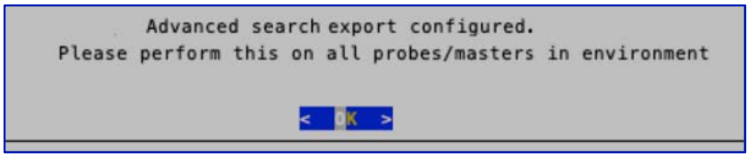


5. Another question will be presented; **Would you like to set a custom filter on outgoing messages?**

   Selecting Yes can reduce the data volumes being ingested into your selected endpoint, but you must follow the filter syntax guidelines to apply them. Select Yes or No as appropriate to proceed.



6. After the optional filter has been configured, a final window will show. Select **OK** to proceed and apply the changes. **Configuration is now complete**.



12. Backing up and Restoring Darktrace

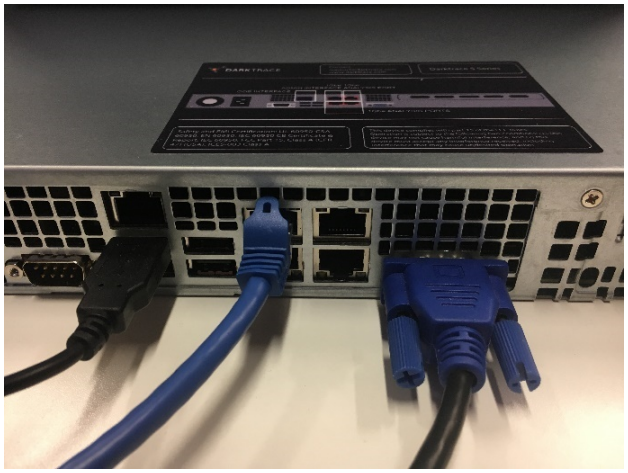
The Darktrace Threat Visualizer application includes configuration options to back up Darktrace appliances. A backup includes all Darktrace machine learning, Models, breaches, as well as subnet and device information, and configuration settings on the Threat Visualizer GUI. On the other hand, it does not include transactional data such as connections in the Event Log, Advanced Search entries and PCAP files, nor configuration settings on the Console menu. A backup will take approximately 2GB of storage space, although actual size can vary.

You do not need to backup all appliances. Only the Master appliance needs to be backed up, as no data backed up is stored on the Probe (the data mentioned earlier is stored only on the Master). Make sure to back up all Masters, if more than one is being used.

A backup file can be created either manually or automatically on the daily schedule as specified.

Create an Immediate Backup

1. The **Console** interface can be accessed by using a VGA monitor and USB keyboard connected to the Darktrace appliance. Alternatively, the application can be remotely accessed via the appliance management interface (Ethernet port eth0) by means of any ncurses-capable SSH client (such as PuTTY).

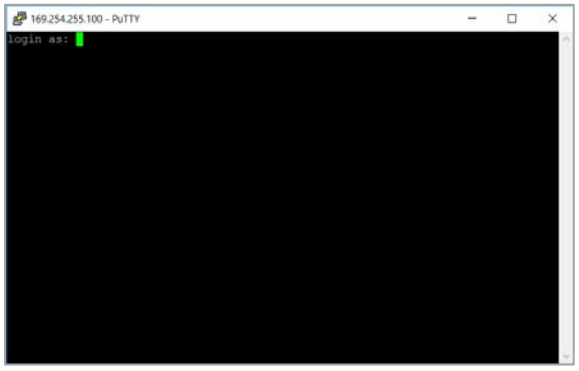


   Darktrace recommends plugging in a VGA monitor and keyboard to view the boot sequence. This can help diagnose issues such as hard drive failures during transport, or errors with the BIOS.

2. By default, the appliance is shipped with the IP **10.0.0.2**.

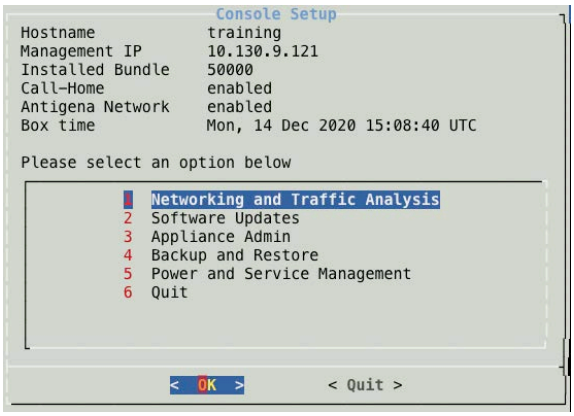
   If the plan is to install the appliance on a different subnet, it is necessary to change the IP address via the console.

   In the example screenshot to the right, an SSH connection has been directly made by plugging an Ethernet cable to the Admin Interface port.

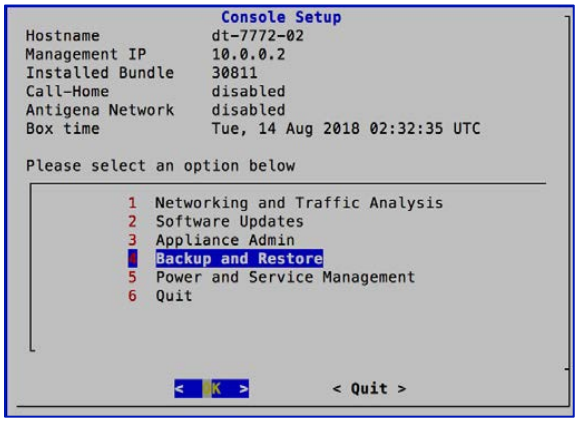


3. Log in as the **Console** user and enter the password provided by Darktrace. Confirm the **Console Setup** options are displayed.

   The console is a Command Line Interface (CLI) which allows only keyboard controls. Arrow keys work as expected, and the Cancel option returns to the parent menu. Numeric hotkeys can also be used to jump to specific menu options, and the Enter key selects the currently highlighted option.



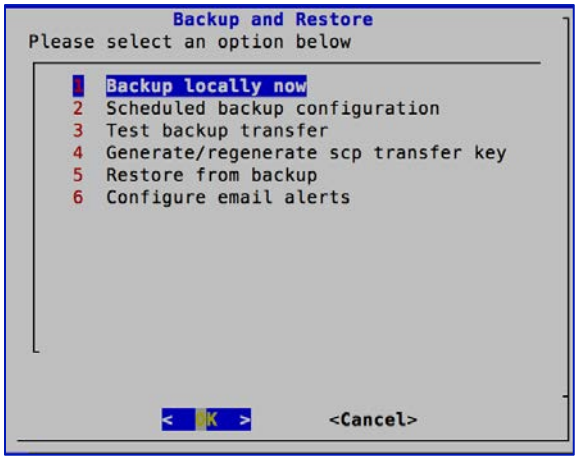
4. On the Master appliance, login to the Console menu, select **4. Backup and Restore**, and then press **OK**.



5. A range of backup options are available.

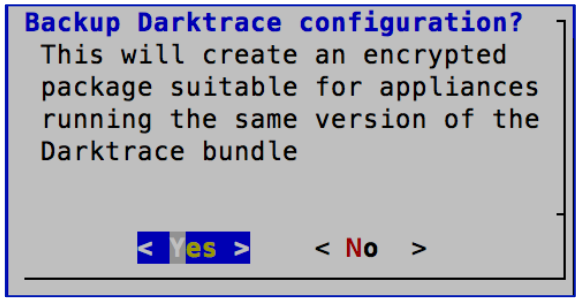
   Select option **1. Backup locally now**.

   Choose **OK**.



6. Note that backups can only be restored to the same version of the Darktrace software.

   Select **'Yes'** to proceed.

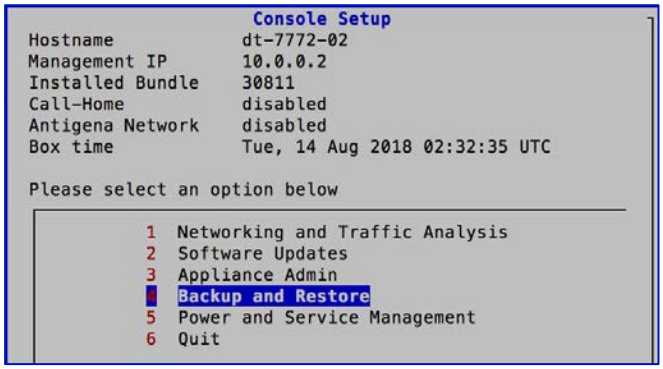


7. The Backup file is created in the ***/files*** directory, which can be accessed by the ***transfer*** user via SFTP.

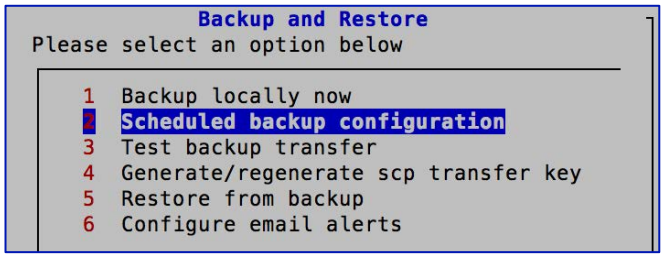
Create Scheduled Backups

The Darktrace Threat Visualizer application includes configuration options to backup Darktrace appliances in multiple ways via SCP, SMB or S3. In Master/Probe architectures, only the Master appliances need to be backed up. In Unified View deployments, or if multiple Master appliances are in use, it is necessary to back up all Masters.

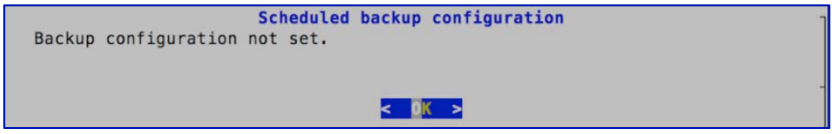
1. On the Master appliance, login to the Console menu, and select option **4 Backup and Restore.**



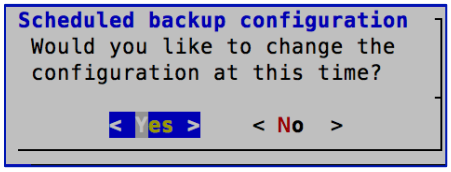
2. Select option **2** for **Scheduled backup configuration**.



3. A display may state that a backup configuration is not set yet for the first time.

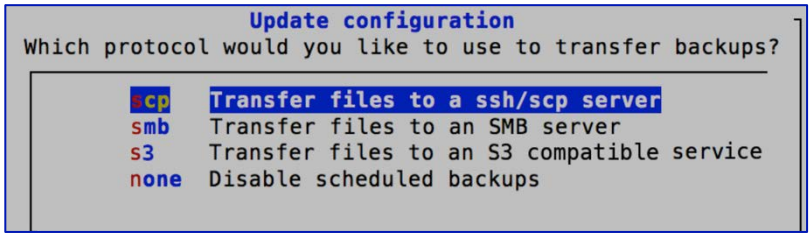


Select '**OK**'.



Another window will pop up - select '**Yes**' to proceed.

4. Select either **ssh/scp**, **smb** or **s3** to transfer backup files depending on the server that receives them. Note that selecting **none** disables scheduled backups.

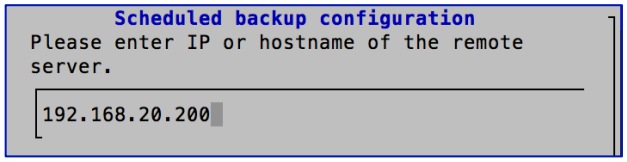


Please follow the path outlined below for the appropriate server for your network.

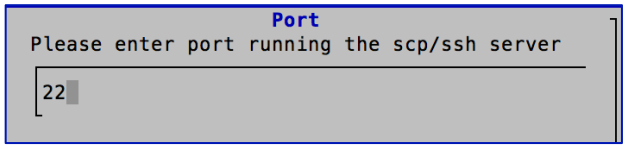
Backup via SCP

1. When using **SCP**, enter the following values and choose **OK** to confirm each one.

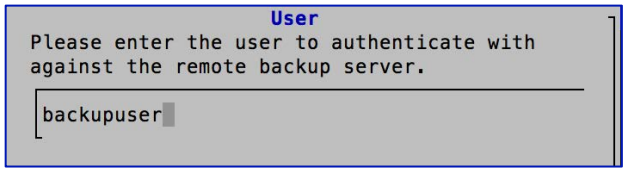
   a. Enter the **IP address** or **hostname** of the remote server that receives the backup files.



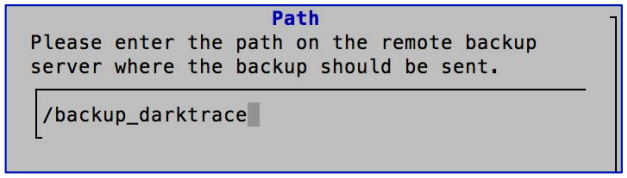
   b. Input the **port** for the backup server.



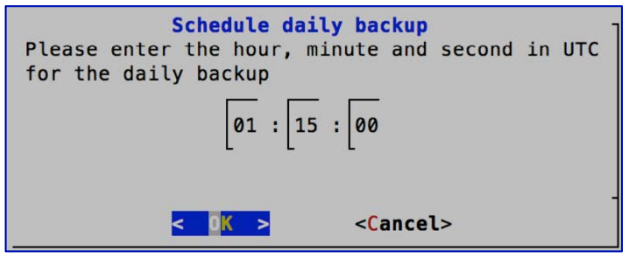
   c. Type in the **username** of the server.



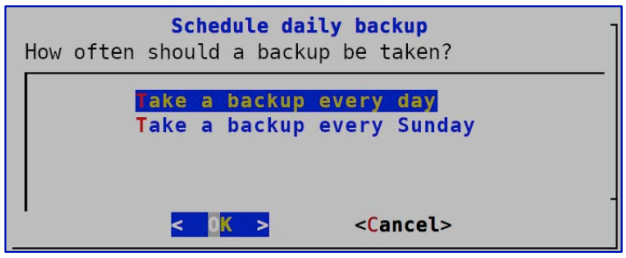
   d. Finally, type the **path** on the server where the backup will be sent.



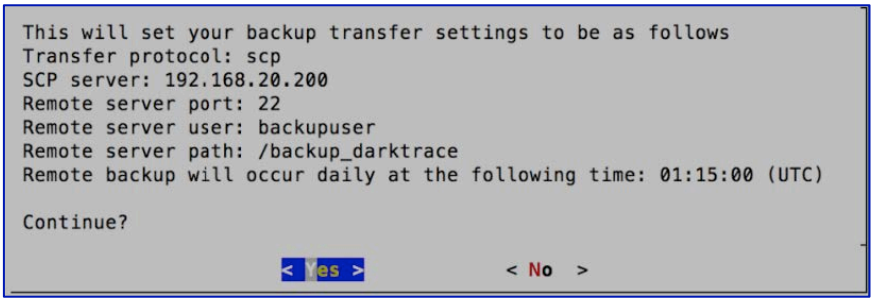
2. Enter the **hour**, **minute** and **second** in **UTC** for the SCP backup and press OK to confirm.



3. Select whether SCP backups should occur **daily** or be performed **every week** at a specified time.

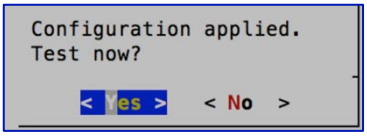


4. Confirm the **configuration settings** and select **Yes** to proceed.



Please note, the public key is generated in the /files directory, which can be accessed by the transfer user via SFTP. The key must be added to the .ssh/authorized_keys file for the configureated user on the remote backup server. The key can also be regenerated from **Generate/regenerate scp transfer key** under the Backup and Restore submenu.

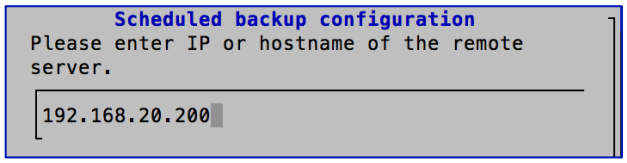
5. As an optional step, **test** the configuration. This can be performed at any time from the **Test backup transfer** under the Backup and Restore submenu.



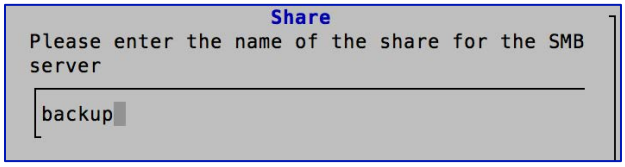
Backup via SMB

1. For **SMB** enter the following details and click OK to move onto the next step each time:

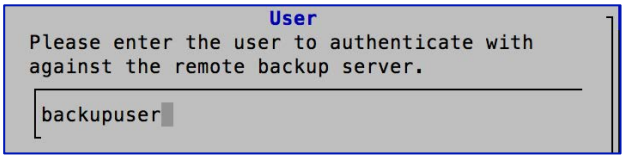
   a. The **IP address** or **hostname** of the remote SMB server which is the intended destination for backup.



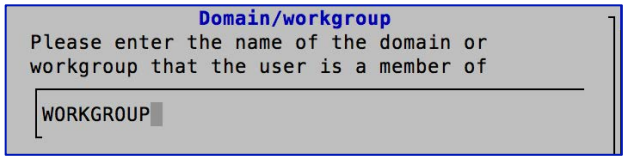
   b. Name of the **share** on the SMB server.



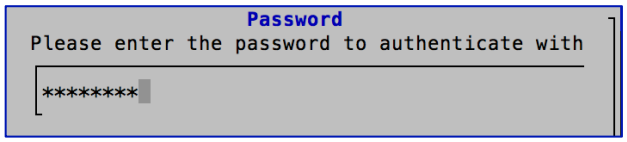
   c. Enter the **user** on the server.



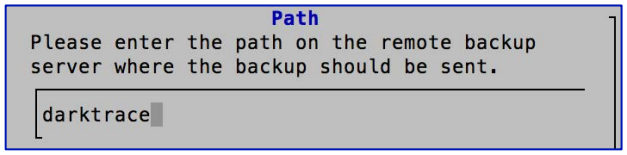
   d. Set the **domain** or **workgroup** that the user is a member of.



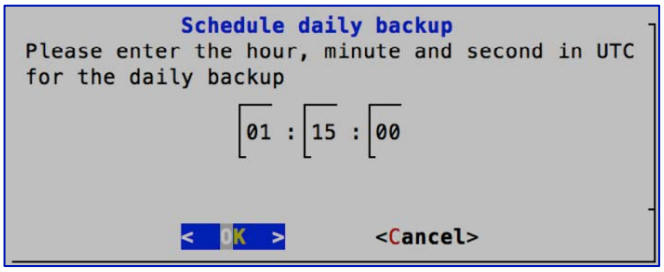
   e. Enter a **password** for the user for authentication.



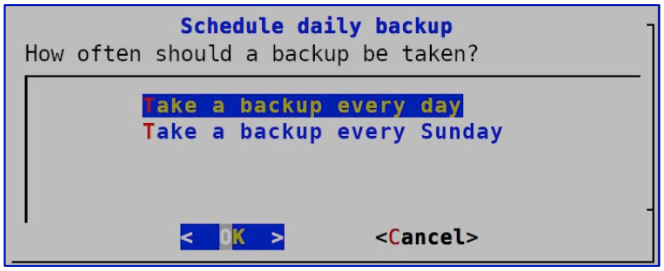
   f. Input the **path** on the server where the backup will be sent.



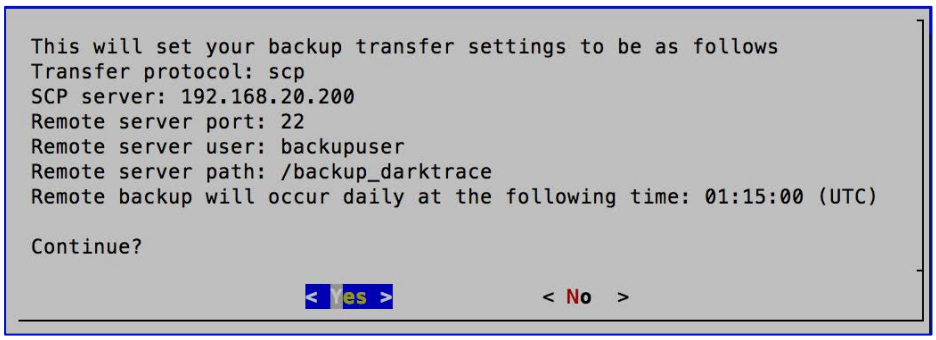
2. Enter the **hour**, **minute** and **second** in **UTC** for the SMB backup and press OK to confirm.



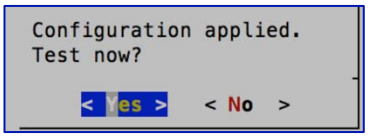
3. Select whether SCP backups should occur **daily** or be performed **every week** at a specified time.



4. Confirm the **configuration settings** and select **Yes** to proceed.



5. As an optional step, **test** the configuration. This can be performed at any time from the **Test backup transfer** under the Backup and Restore submenu.



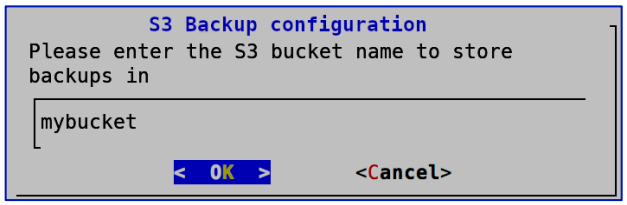
Backup via S3

1. Enter the **URL** of the **S3-compatible service** which is intended to receive the backup files.

   Do not include the bucket name in the URL at this stage.

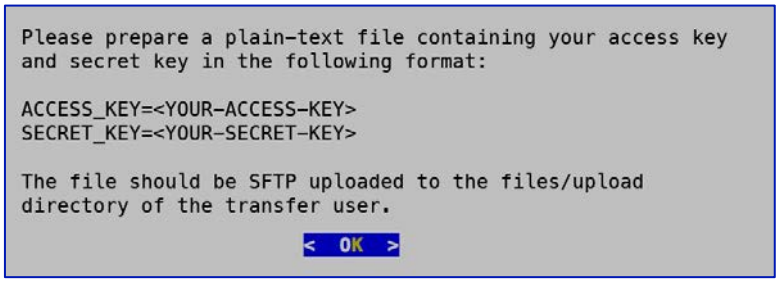
   Click **OK** to proceed.

2. Enter a **bucket name** where the backups are to be stored.



3. Enter the **authentication details for S3**. These can be **uploaded** in a compatible file by the transfer user using SFTP, which can be carried out by selecting the first option or entered **manually** using the second option.

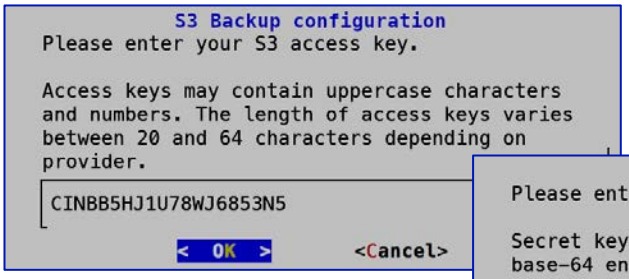
   a. To **load S3 authentication details** from a file, create a plain text file with the Access Key and Secret Key in the format:

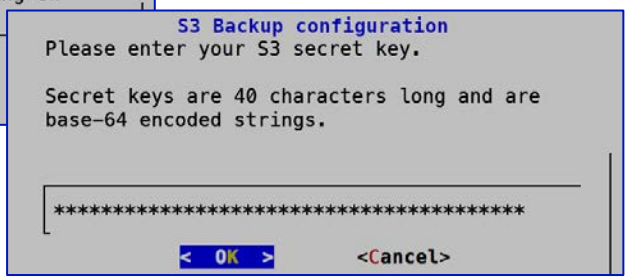


   ACCESS_KEY=key
   SECRET_KEY=key

   Upload this file using the transfer user into the files/upload directory. Proceed when the file is uploaded and load the authentication details.

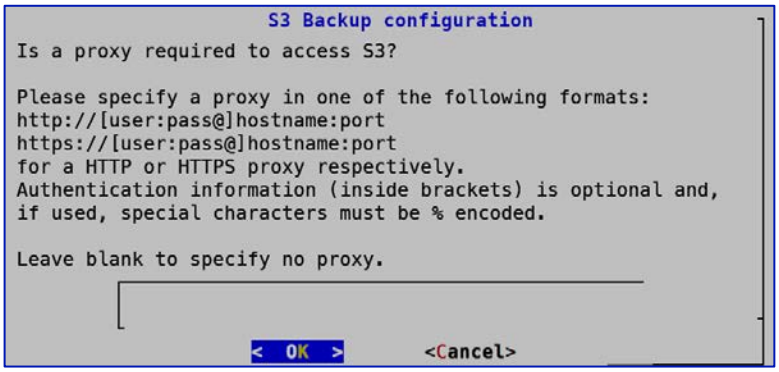
b. To enter the details **manually**, first, enter the S3 **Access Key** and proceed by selecting OK. Then, enter the **Secret Key** into the second prompt and proceed again.



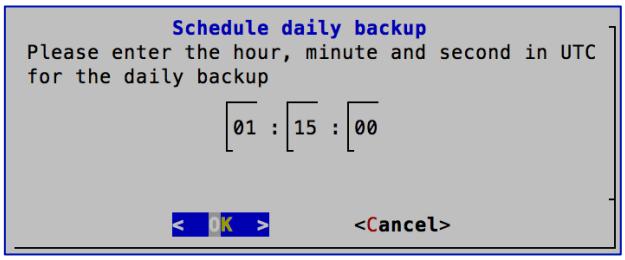


4. If a **proxy** is required to access the S3 service, enter the details described in the prompt which appears on screen.

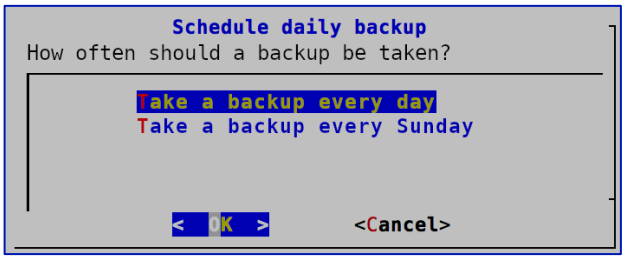
   Leave the field **blank** if no proxy is required and proceed by selecting OK.



5. Enter the **hour**, **minute** and **second** in **UTC** for the backup and click OK to confirm.

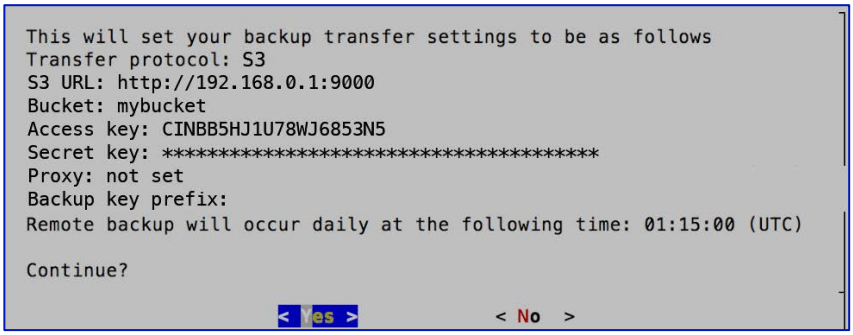


6. Select **how often** the S3 backup should be performed: **daily** or **weekly** at the specified time.



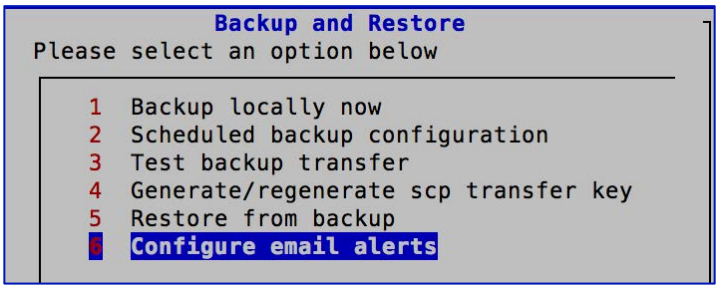
7. Finally, **confirm the configuration options** and select Yes to proceed.

   At this point, you can **test the configuration** or do it later using the Test backup transfer under the Backup and Restore submenu.



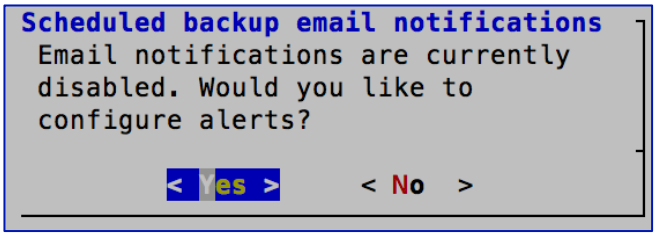
Send Email Notifications for Scheduled Backup Status

1. Under the **Backup and Restore** submenu, select option **6. Configure email alerts**.

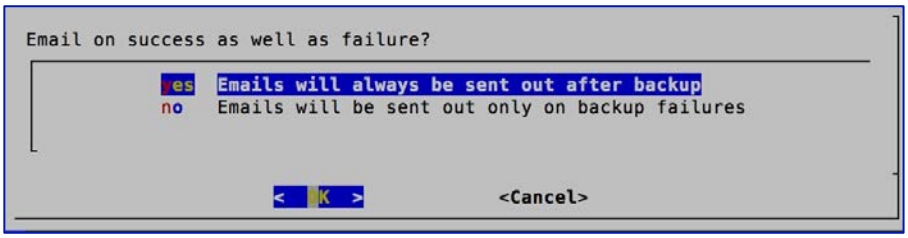


2. A confirmation will be displayed. Press '**OK**' to proceed.

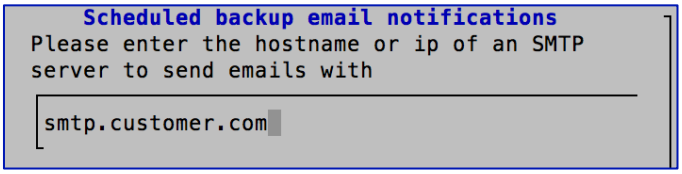
3. Choose '**Yes**' to enable notifications.



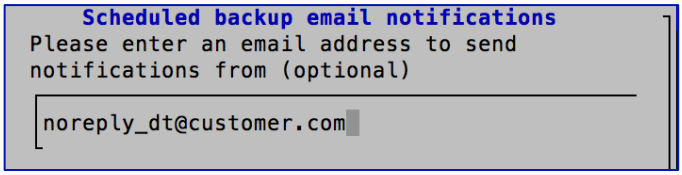
4. Select whether **emails** will be sent out regardless of the result of the backup.



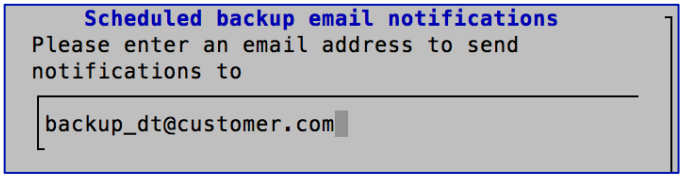
5. Enter an email address to **send notifications to**.



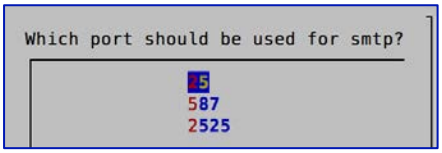
6. Enter an email address to **send notifications from** (optional).



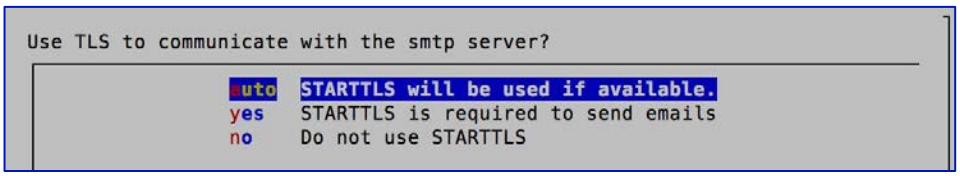
7. Enter the hostname or IP address of an **SMTP server** to send emails with.



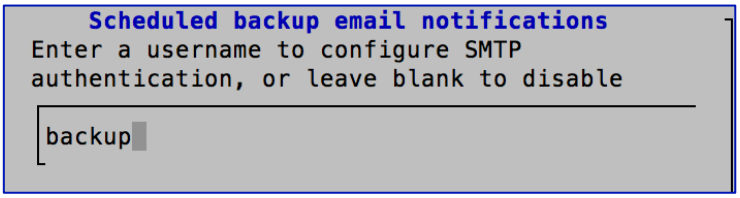
8. Select port for **SMTP**.



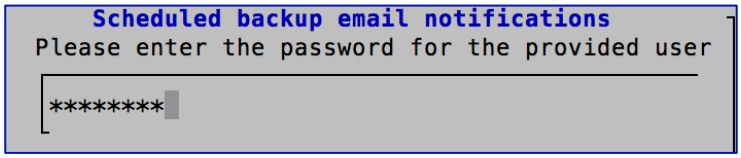
9. Select whether **STARTTLS** is to be used.



10. Enter a username to configure **SMTP** authentication (leave blank to disable the email notification).

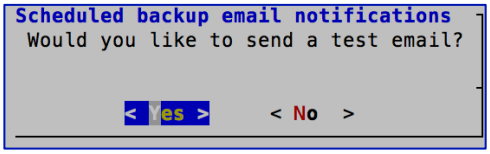


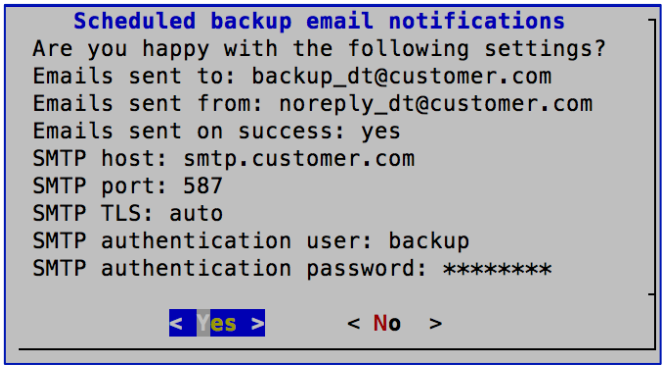
11. Enter the **Password** of the user.



12. Confirm the configuration and select **Yes** to proceed.

13. Select **Yes** to send a test email.





Restore from a Backup

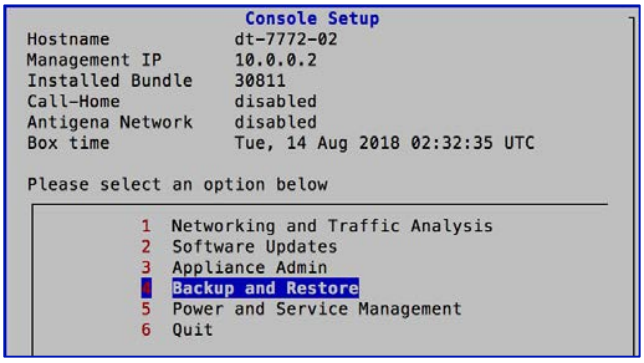
The option to restore from a backup is available in the console menu. Transactional data such as connections in the Event Log, Advanced Search entries, and PCAP files are not restored.

Before restoring from a backup, carry out the following:

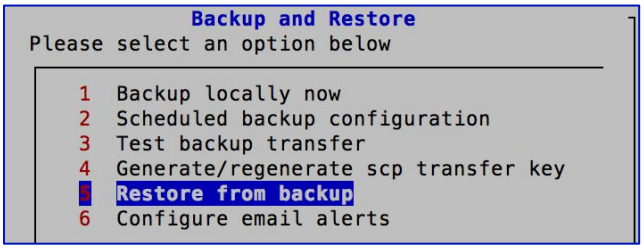
- Confirm the version of the appliance is the same as the backup file. These must be the same version.
- Upload the backup file to */files/upload* in the *transfer* user directory via SFTP, if not done so when creating a backup.
- Make sure the appliance is no longer ingesting data. Unplug the cable(s) from analysis port(s) before deleting captured date, and restoration.

To restore from a backup, perform the following steps:

1. On the Master appliance, login to the Console menu, and select **4. Backup and Restore**.

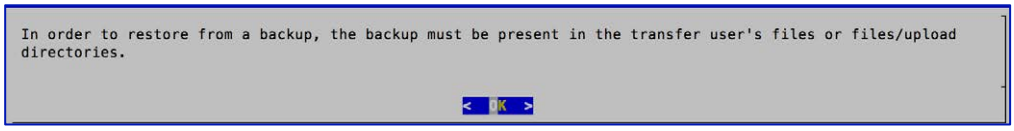


2. Then select option **5. Restore from backup**.



3. A warning dialog will open to explain that a backup must be present before a restoration can occur.

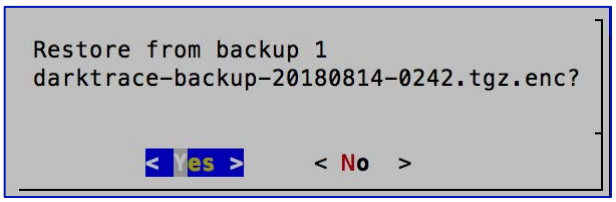
   Press **OK** to continue.



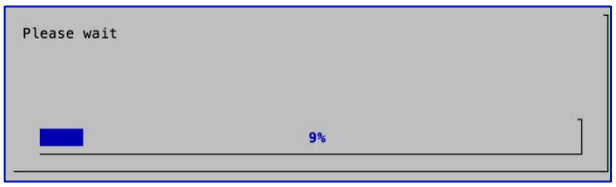
4. Select a backup to restore from the **list**.

5. A confirmation box will request that you confirm your selected choice of backup to restore.

   Choose **Yes**.

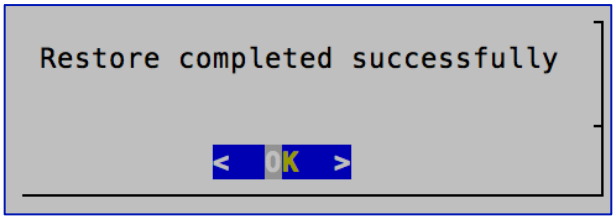


6. Please **wait a while** for the restoration to complete. The time this takes to complete depends on the size of the backup file.



7. A “restore completed successfully message” will appear.

   Press **OK** to return to the **Backup and Restore** submenu.



13. Upgrading Darktrace

Upgrading the Darktrace Appliance

This section describes the process for manual upgrades for the software version running on a Darktrace appliance. When Call-Home is enabled, Darktrace appliances will automatically be upgraded by Darktrace to the latest release. Otherwise, unless you inform your Darktrace representative of not using it or when Call-Home is disabled, a manual upgrade is required.

Upgrading to the latest version of the Threat Visualizer application is quick and easy. Review the summary of the following steps:

- Download the latest bundle.
- Copy the bundle to all Darktrace Appliances.
- Unpack the bundle.
- Apply the bundle to install the latest Darktrace software.
- Confirm the latest version is installed by logging in to the Console menu and the Threat Visualizer.

As a Darktrace installation may involve multiple appliances, it is important that all appliances are upgraded to the same version. Upgrading an appliance will not change any previous settings or overwrite any model breaches currently stored in the application. Outlined below are three things that should be considered when upgrading.

Types of Bundle File

There are two following types of software upgrade file: full package and differential package.

Full package

This can be applied on any older version to upgrade an appliance. The full package file is named as follows:

darktrace-bundle-*<upgrade version>_<release date>-<alphanumeric>-x*.dat

Differential package

This can be applied only on the specific older versions to upgrade an appliance. While it has such a constraint, it has a smaller file size than a full package. The differential package file has the following naming convention:

darktrace-bundle-*<upgrade version>*-xdelta*<specific old version where it can be applied>_<release date>-<alphanumeric>-x*.dat

Example: *darktrace-bundle-30811-xdelta30801_20180726T1426Z-5c186-x.dat*

By using this, it is possible to upgrade an appliance running version 30801 to 30811.

Also, some differential packages contain ‘delta’ instead of ‘xdelta’ in their file name. A ‘delta’ package can be applied not only to the specific version indicated in the filename, but also to newer versions:

Example: *darktrace-bundle-30811-delta30700_20180726T1426Z-5c186-x.dat*

Download Methods for Bundle Files

Software upgrade bundle files are provided by either of the following methods: automatic download, manual download via Call-Home or from the Customer Portal.

Automatic download

A differential package file is automatically downloaded every weekend (if available) when one of the following options under **2. Software Updates** > **Guided mode** > **3. Configure downloads** has been enabled:

- Download updates via Call-Home

  Update bundle files are downloaded via Call-Home. (Call-Home must be established to select this). This is enabled by default.

- Download updates over the internet

  Apart from the Call-Home SSH connection, Darktrace provides another channel for appliances to automatically download over the internet via HTTPS. The appliance needs access to packages.darktrace.com (or the cloudfront.net content delivery network, if you prefer) over port 443. A proxy can be configured if required. Note that this requires a bundle key, which can be requested from Darktrace Support.

To disable this, select ***None (disable guided updates)*** under the submenu.

Manual download via Call-Home

Download the latest differential package using the following option in the Console menu:

2 Software Updates > **Guided mode** > **1 Check for updates now**

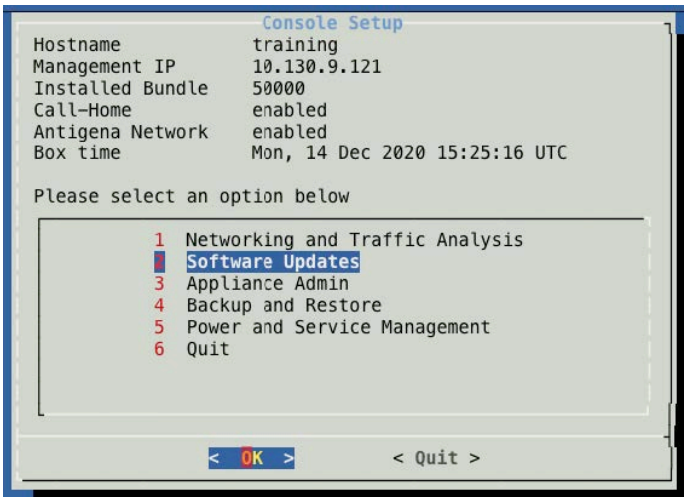
Customer Portal

The latest bundle file is available in the Customer Portal. Download it from the website and copy it to your appliance via SFTP with the *transfer* user.

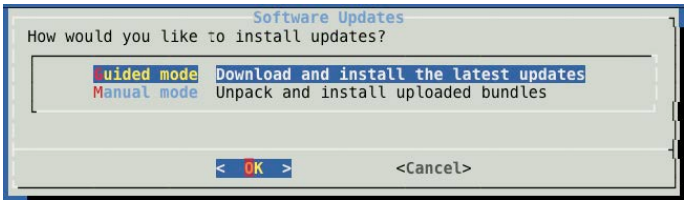
Upgrade Procedure

It is possible to manually upgrade an appliance using the following procedure. Please ensure that the upgrade bundle file is placed on the appliance before the upgrade process. If the bundle was downloaded from the Customer Portal, login to the appliance as the *transfer* user via SFTP and upload your upgrade bundle file to the */files/upload* directory.

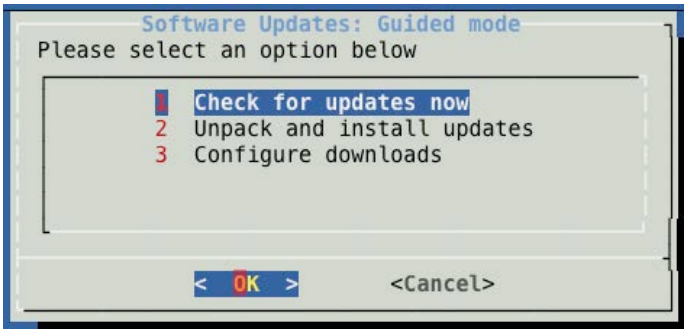
1. Log in to the Console menu and select "**2 Software Updates**".



2. There are two options: **Guided mode** and **Manual mode**.



3. Selecting the **Guided Mode** reveals a corresponding menu.



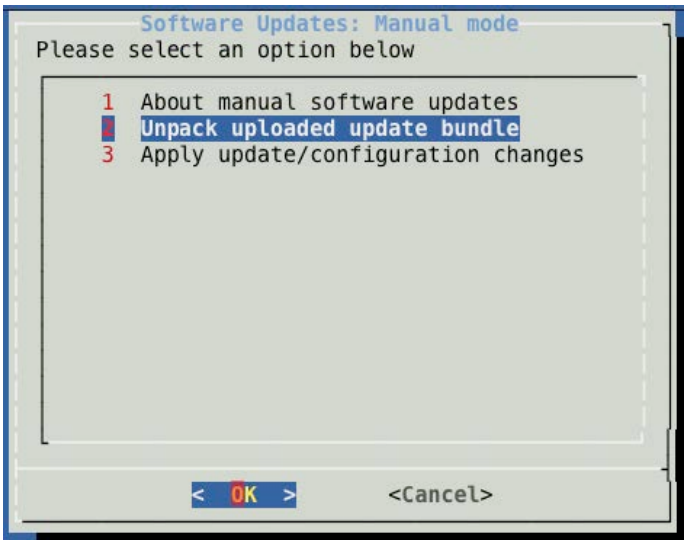
"1 Check for updates now" will check if there are any new available updates. If an update is available it will download and proceed to unpack and install it, prompting before each step begins.

"2 Unpack and Install updates" will run through the update process, asking for confirmation before each step.

"3 Configure downloads" allows you to select how you would like to fetch the latest bundles. Disable this option if you do not wish to use this feature. Please refer to the previous subsection of ***Download methods of bundle files***.

4. **Manual Mode** requires further operations to unpack the downloaded bundle and then install it.

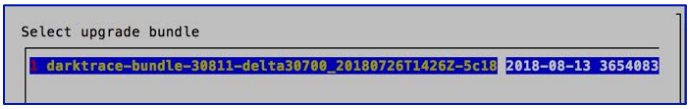
   In the Manual Mode submenu, select "**2 Unpack uploaded update bundle"** to show the list of the available bundles stored in the appliance.

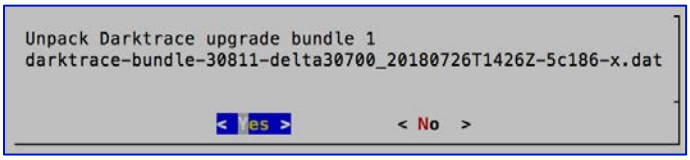


5. Select the newest bundle to install. The latest bundle is always at the bottom of the list. Press **OK** to continue.

   Then choose **Yes** to proceed.

   It can take some time for the unpacking operation to complete.

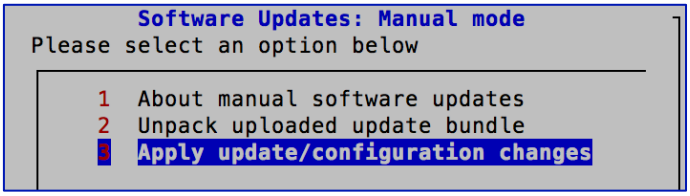


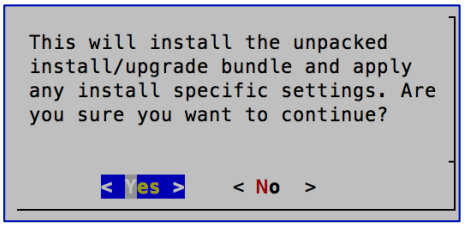


6. Once unpacked, select **3. Apply update/configuration changes**.

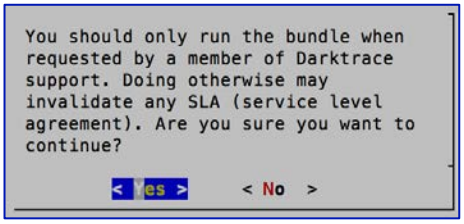
   Select **Yes** to proceed with update.

   If an error occurs, please try applying the latest changes a second time.



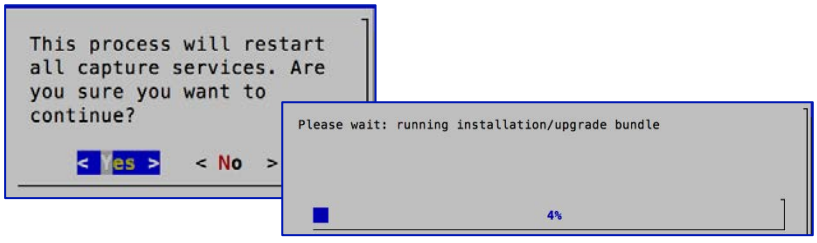


7. Confirm you wish to continue by selecting **Yes**.

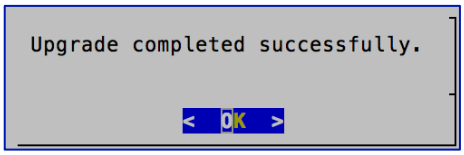


8. Again, press **Yes** to continue.

   The update process will begin.

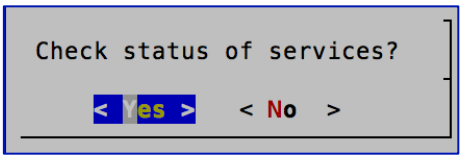


9. When finished, press **OK** to complete your upgrade.



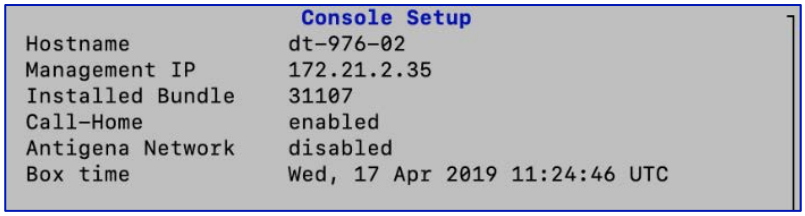
10. You are prompted whether to check the status of the services.

    Select **Yes** if you wish to do so.



11. You will be **logged out** of the Console.

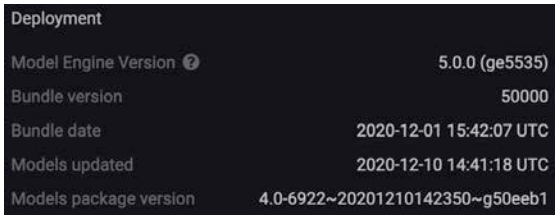
12. **Login** to the Console menu again to **confirm** that the software version has been updated as you applied.



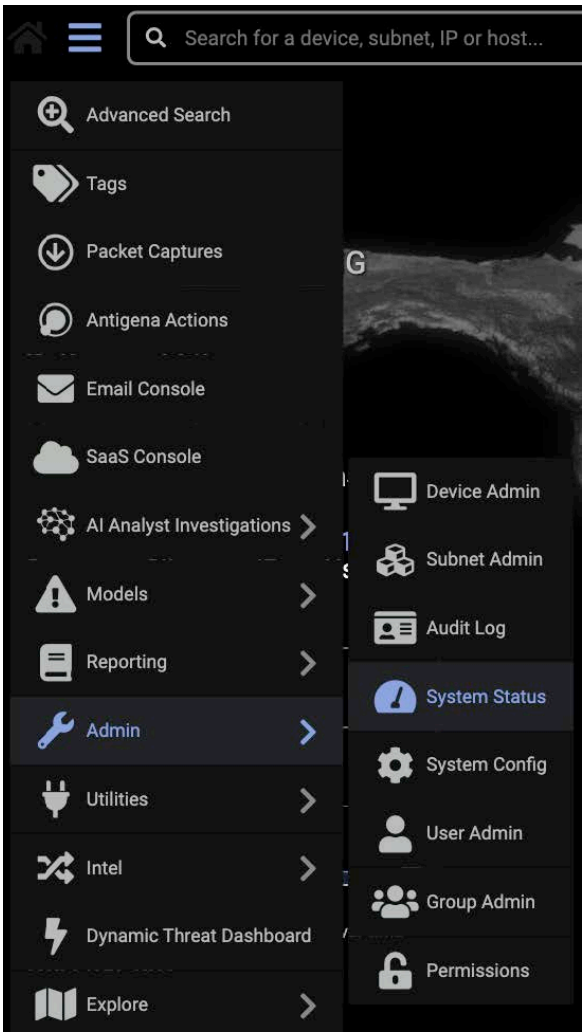
13. Login into the Threat Visualizer web application and navigate to **Admin** > **System Status** under the main menu.

    Select an appliance from the Appliances tab and review the Summary section.

    Confirm that the software version has been updated to the latest version by reviewing the Deployment statistics.



    This indicates whether the upgrade process has been a success.

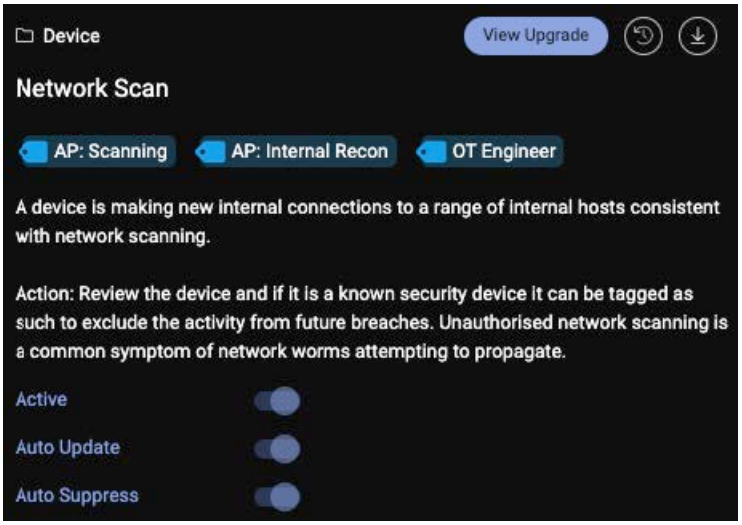


Upgrading Darktrace Models

Besides applying a software upgrade bundle with a set of new or updated Models, updates to Models are automatically delivered on a daily basis. This means that Models can be automatically updated without waiting for a new version of the Threat Visualizer to be released. This auto update feature is enabled by default and works only when Call-Home or Download updates over the internet is enabled.

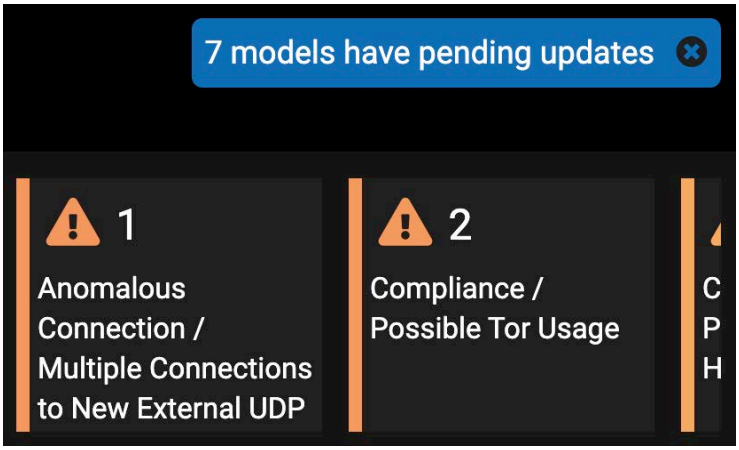
1. View any Model in the Threat Visualizer Model Editor. Note the **Auto Update** function. When set to **Yes**, this will automatically upgrade to the latest version when its released.

   However, if a Model has been edited, the updates will not overwrite the Model unless the user decides to accept the upgrade. If an edited Model has an available update, there is the option to **View Upgrade**.

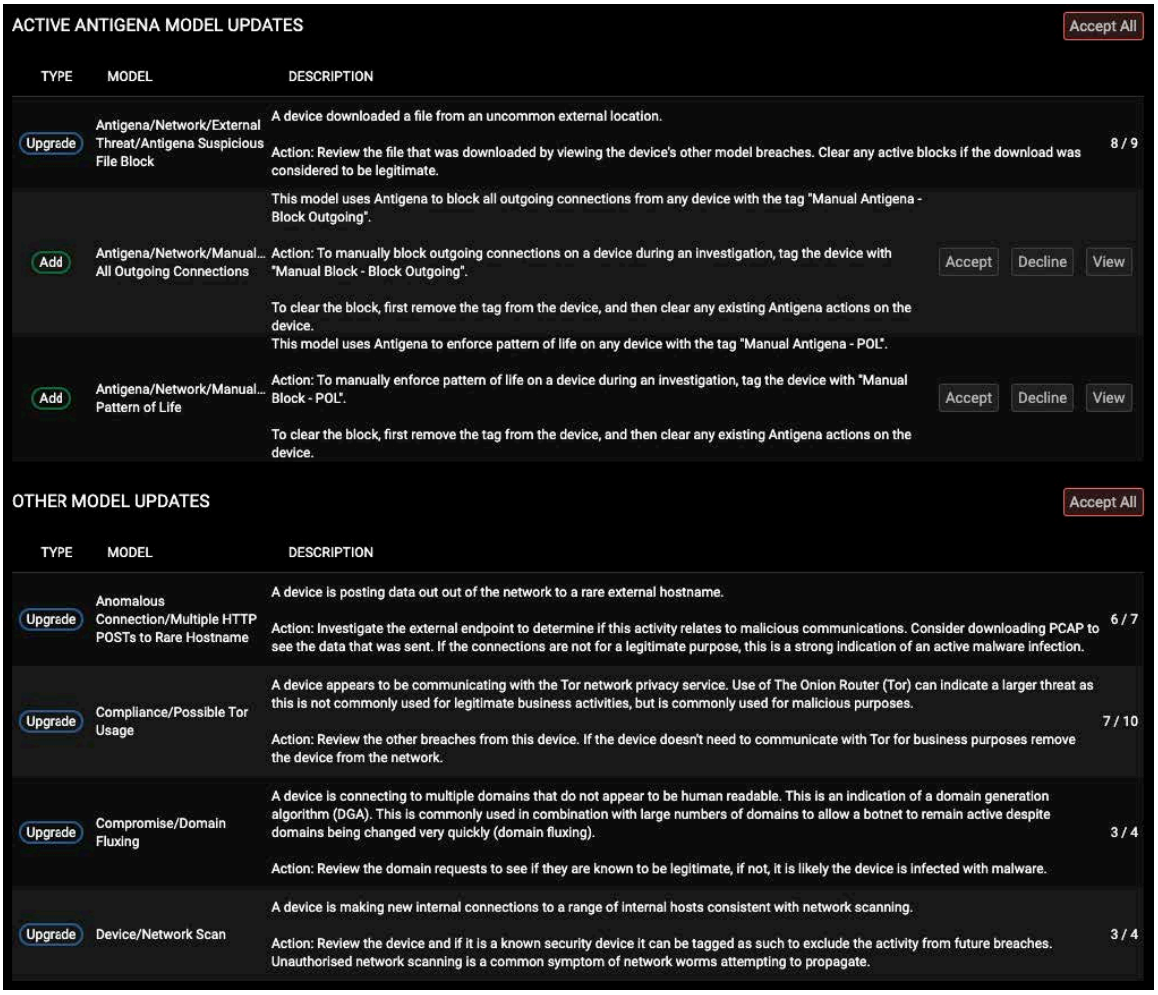


2. Instead of needing to view edited Models individually, a **message will appear** on the home page of the Threat Visualizer stating **a number of models have pending updates** are available for review.

   Any new Models created or duplicated will not be impacted by automatic updates. Clicking this blue notification will redirect the user to the Model Updates page.

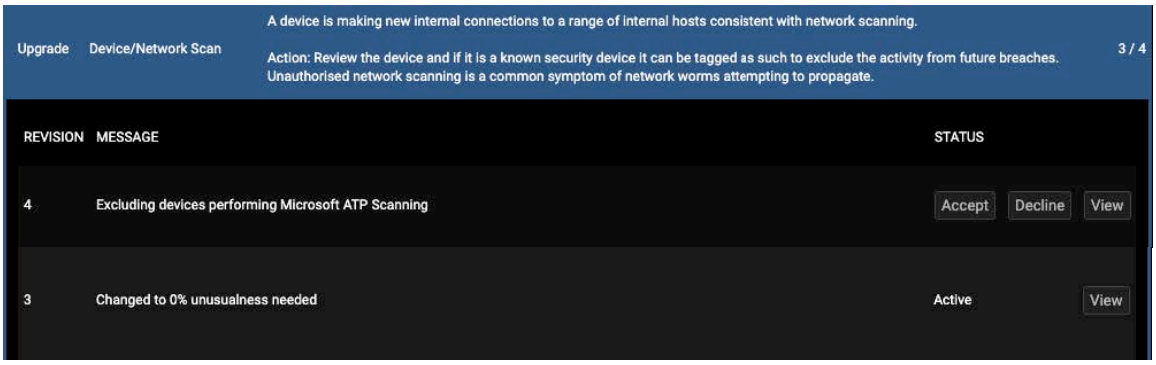


3. The Models Updates page lists all Models which have been customized but have new updates available. This view is also available by selecting the **Model Updates** button under Models from the Threat Visualizer Main Menu.



4. If reviewing individual Models is not required, Models Updates can be applied in bulk by clicking **Accept All**.

5. Click on a Model row to reveal more options.

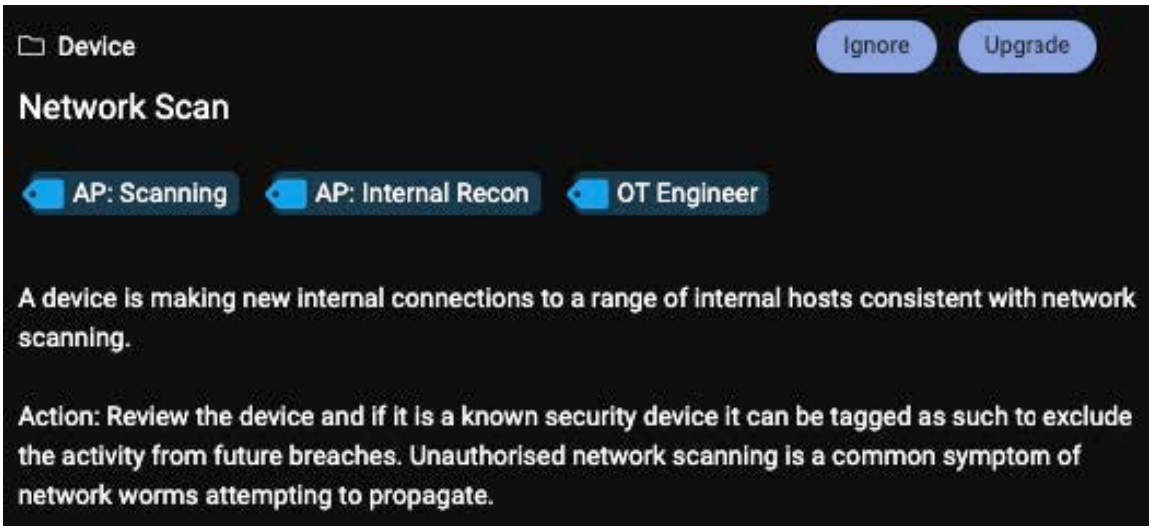


a. Each conflicting Model is listed in a separate row with options to **Accept**, **Decline** or **View** them.

b. For the current active Model, there is also the option to view it by clicking the **View** button on the right.

c. Clicking View for the current active Model and suggested upgrade allows you to **compare them in different tabs**.

6. With the suggested updated Model, it is possible to **Ignore** or **Upgrade** the Model.



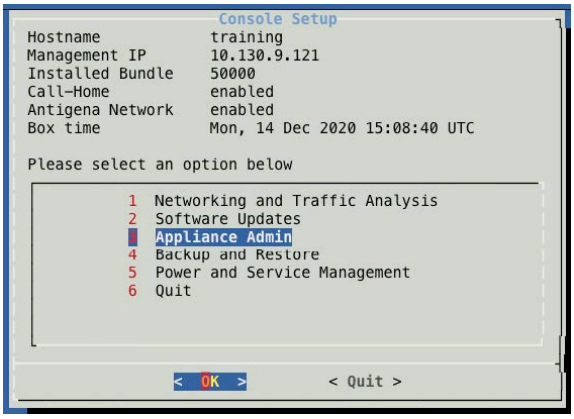
Accepting the changes will permanently update the Model. Be careful not to overwrite any of your changes.

14. Host Variable Configuration

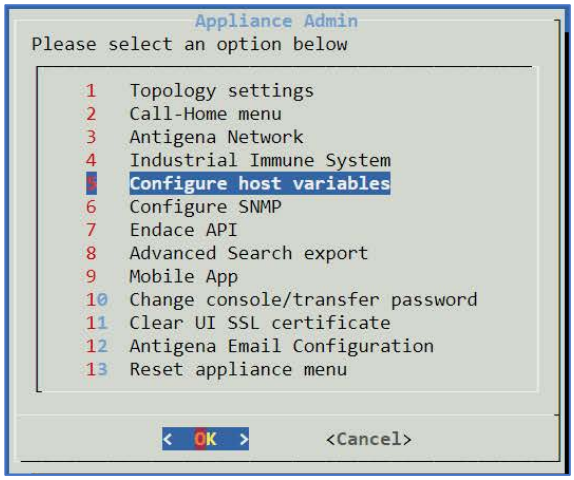
Darktrace provides several custom options which may be appropriate for the network environment. These options will help with accessing, using and administering the appliance and ensure any internal policies are adhered to.

The host variables available to configure may change from version-to-version dependent on requirements. Each option is described in detail when selected from the console menu.

1. Login to the Console menu, choose "**3 Appliance Admin"** and select **OK**.

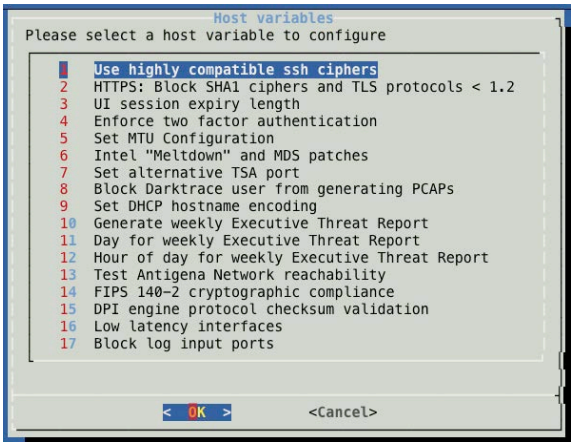


2. Navigate to the option "**5 Configure host variables"** and select **OK**.



3. The Host variables menu will now display all the currently available options. Selecting an option and selecting **OK** will display an explanation of the variable and allow you to set/unset/change the variable.

   For more details on "**6 CVE-2017-5754 Intel "Meltdown" patch"**, please refer to *Darktrace Threat Note Meltdown and Spectre.pdf* file which is available to download from the Darktrace Customer Portal.

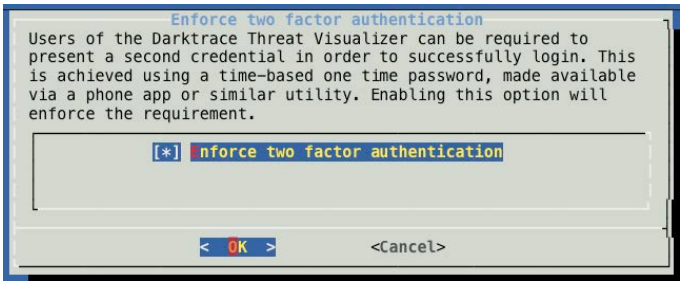


4. The **submenu** allows configuration of the following:

1	**Use highly compatible ssh ciphers**	This option configures the SSH server to use a highly compatible set of ciphers. Disabling this option increases the security of the SSH server.
2	**HTTPS: Block SHA1 ciphers and TLS protocols < 1.2**	Enabling this option restricts the cipher suite in use by the HTTPS server and disables TLS protocols other than TLS v1.2.
3	**UI session expiry length**	This option sets the number of minutes after which UI sessions are logged out due to inactivity.
4	**Enforce two factor authentication**	Enabling this option requires users of the Threat Visualizer to present a second credential in order to successfully login. This is achieved using a time-based password available via a mobile application or similar utility.
5	**Set MTU Configuration**	This option sets the maximum transaction unit (MTU) size that can be communicated over the network.
6	**Intel "Meltdown" and MDS patches**	Enabling this option applies the kernel patch to mitigate the Meltdown vulnerability (Kernel page table isolation). Reboot is required for changes to take effect.
7	**Set alternative TSA port**	This option sets the Terminal Services Agent (TSA) to post data to the appliance on port 1443.
8	**Block Darktrace user from generating PCAPs**	This option restricts the ability to generate PCAPs for the Darktrace user.
9	**Set DHCP hostname encoding**	Changes the encoding for DHCP hostnames. The Windows DHCP client transfers computer hostnames using the system encoding. Organizations with Windows machines configured using to use non-ascii character sets by default may wish to change this setting.

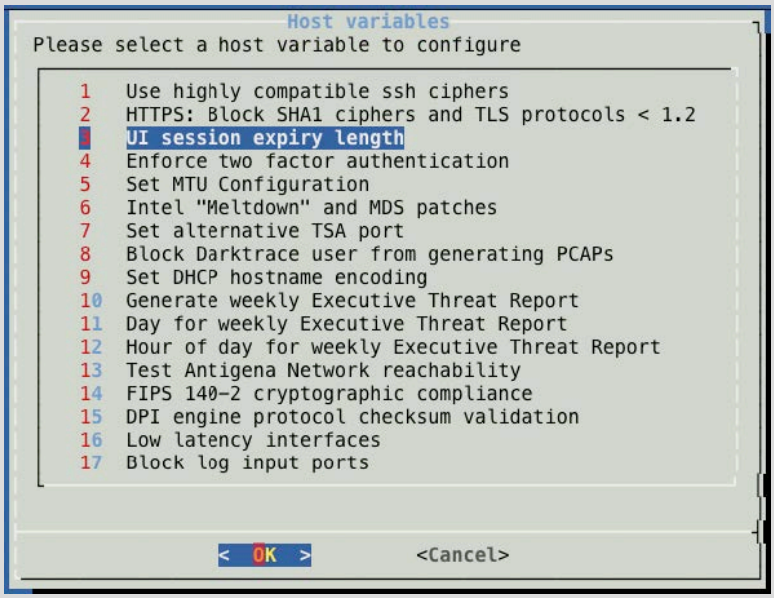
10	**Generate weekly Executive Threat Report**	This option enables the weekly generation of Executive Threat Reports.
11	**Day for weekly Executive Threat Report**	By default, reports are generated on Sunday. This allows an alternative day to be set for weekly Executive Threat Report generation.
12	**Hour of day for weekly Executive Threat Report**	By default, reports are generated at midnight UTC. This allows an alternative hour (UTC only) to be set for weekly Executive Threat Report generation.
13	**Test Antigena Network reachability**	Enabling this option will allow Darktrace support to acquire additional diagnostic information about Antigena Network reachability within your network.
14	**FIPS 140-2 cryptographic compliance**	Enforces FIPS 140-2 encryption on inbound HTTPS connections. When enabled on both Master and Probe, probes will only accept FIPS valid ciphers in inbound connections from the Master.
15	**DPI engine protocol checksum validation**	Checksum validation is performed within the DPI engine to filter out invalid packets that would not typically be accepted by network interfaces. This host variable allows validation to be disabled if invalid checksums are expected within traffic.
16	**Low latency interfaces**	When enabled, packet ingestion interfaces will be polled at a higher frequency to prevent packet mis-ordering when network TAPs send RX and TX packets to different interface ports.
17	**Block log input ports**	By default, the Darktrace appliance ingests syslog entries over a range of ports. This setting will block these ports at the firewall level, which may be required for compliance.

5. Most options can be turned on or off. In these cases, press the spacebar to select or deselect the option and select **OK** to apply changes. When the option is set to on, the option will display [*].

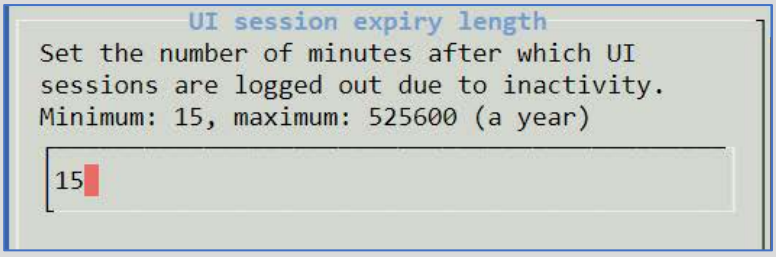


Additional Security Exercise - Try This:

- Within the Host Variables section extend the UI session expiry length



- Set the expiry length to 15 minutes



15. Securely Erasing Darktrace Captured Data

Data erasure is useful when relocating a Darktrace appliance to change its monitoring scope, to start afresh any initial deployment “baselining”, or if data needs to be wiped before returning an appliance to Darktrace.

There are two options for wiping: deleting captured data, or restoring the appliance to factory settings, which involves a full wipe of all storage drives.

The data erasure processes above can be performed onsite, provided access to a Darktrace appliance is available. The processes will not affect the appliance Operating System or any Darktrace proprietary software.

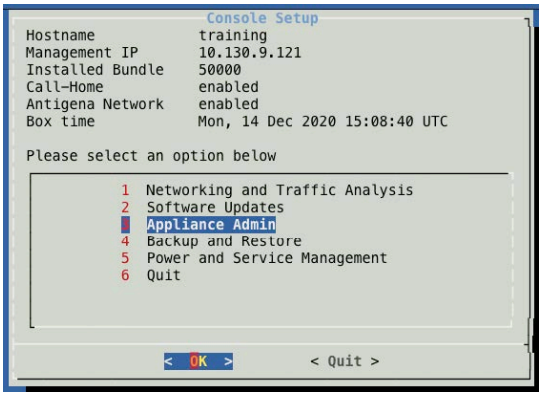
The delete captured data process will include, but may not be limited to, the following data sets: topology settings (connected probes and their IP addresses), hostnames and popularity (rare hostnames etc.), environmental details (proxies, domains etc.), all modelled devices, breaches and partial breaches, device connectivity states, and backups.

Darktrace will also fully erase any information on all storage drives for new or returned appliances.

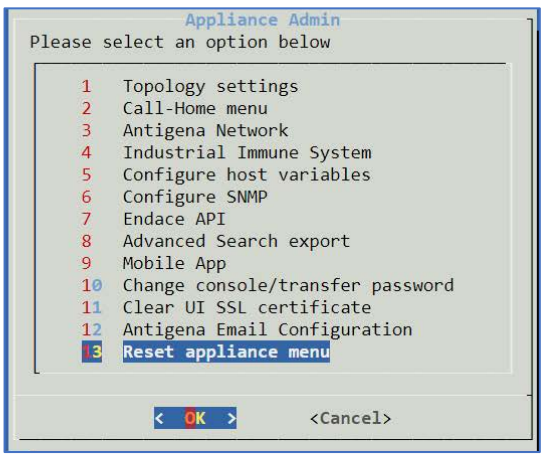
How to Delete Captured Data

Captured data is erased through the console application. This process will also require an unlock code to be provided by a Darktrace representative and exchanged via a secure channel such as text message or the Darktrace Customer Portal.

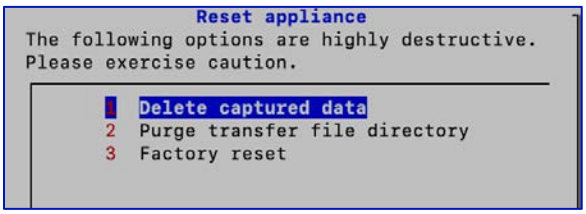
1. Login to the Console menu and select **3. Appliance Admin**.



2. Select option **13. Reset appliance** menu and press **OK**.

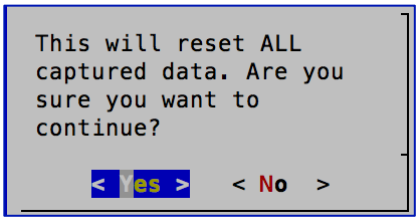


3. Select option **1. Delete capture data** and choose **OK**.



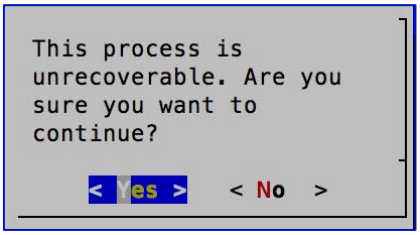
4. At this point, the following warning messages will appear.

   Choose **Yes** to proceed. At this stage, the process can be terminated by choosing **No**.



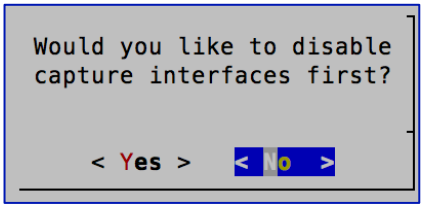
5. The process requires reconfirmation of the decision in order to reset the appliance.

   Choose **Yes** again to confirm this choice.



6. A prompt will open asking whether capture interfaces should be disabled.

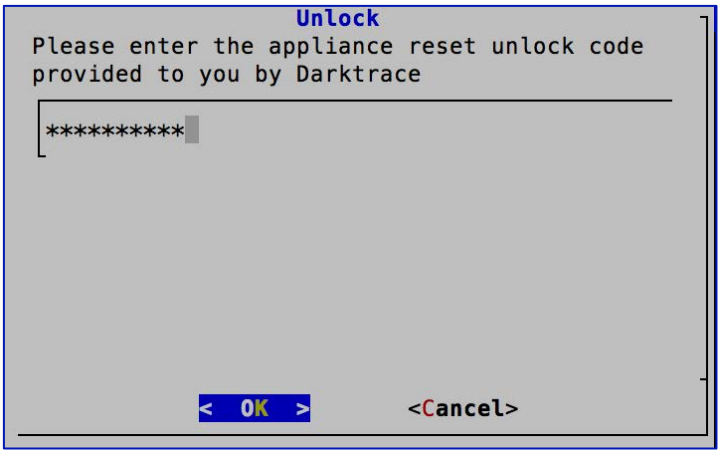
   Selecting **Yes** will allow data to be deleted before removing physical cables. If this is not done, once the wipe is complete, the appliance will start ingesting data again.



   Note: *Capture Interfaces should not be disabled if continued use of the appliance is desired; only Darktrace support can reenable them.*

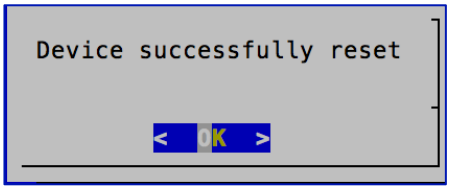
7. Finally, the appliance will request a reset **unlock code** to be input.

   Enter the appliance unlock code provided by Darktrace and press **OK**.



8. A **Device successfully reset** message confirms the erasure process was successful.

   Press **OK**.

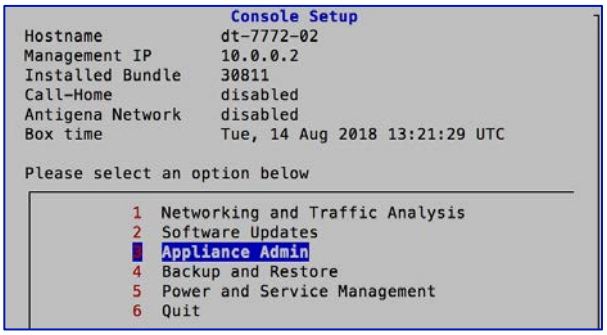


How to Restore to Factory Settings

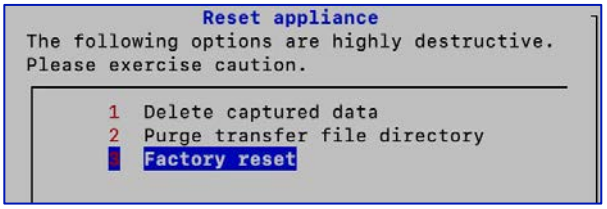
A factory reset is performed through the Console application. As a more stringent data erasure method, this writes zeros to all the disks and then reinstalls the OS and Darktrace software components to totally delete all the data and revert the appliance back to an as-new state. It takes much more time than the Delete captured data option and requires a different unlock code to be provided by a Darktrace representative.

Before proceeding with a factory reset, unplug all analysis port cables (management and RMM cables can remain plugged in). This process will also require a reset code to be provided by a Darktrace representative and exchanged via a secure channel such as text message or the Darktrace Customer Portal.

1. Login to the Console menu and select **3. Appliance Admin** > **8. Reset appliance menu**.



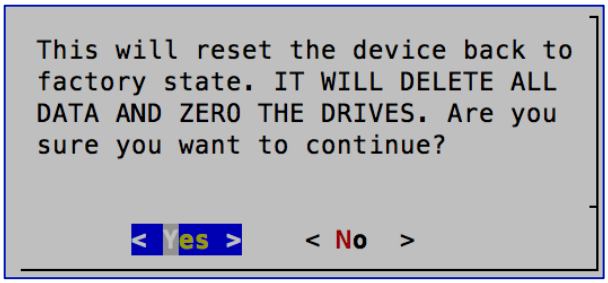
2. Select option **3. Factory reset** and press **OK**.



3. At this point, the following warning messages will appear.

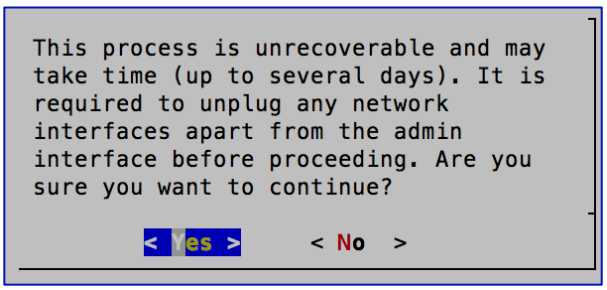
   Select **Yes** to proceed.

   At this stage, the process can be terminated by choosing **No**.



4. The process requires reconfirmation of this decision to restore the appliance to factory settings. This process can take several days, depending on the size of the appliance.

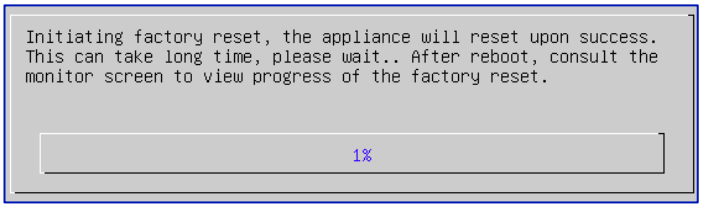
   Press **Yes** again to confirm your choice.



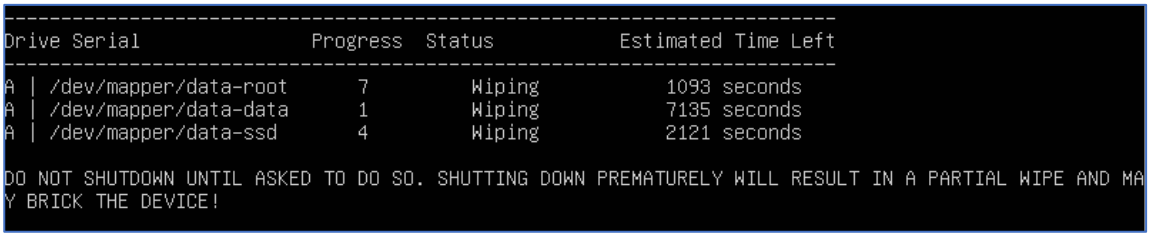
5. Finally, the appliance will request you to input a reset unlock code.

   Enter the factory reset unlock code provided by Darktrace and press **OK**.

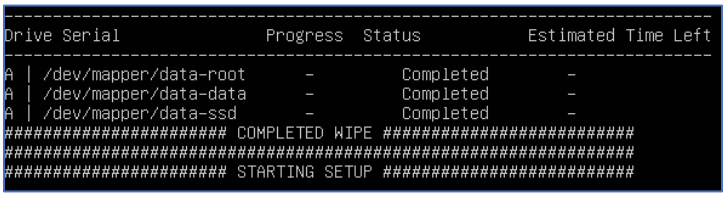
6. During the first part of the process this **message** will appear on the screen. **Do not interrupt the process** or the appliance may be left in an irrecoverable state.



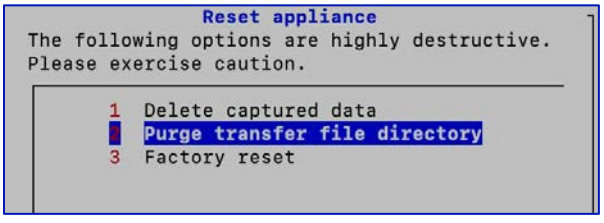
7. After rebooting the appliance, the **terminal** will display the **progress** of the wipe. This will periodically update itself.



8. Once the wipe is **complete**, the terminal will show this message on the screen. After running the setup, it will reboot one further time, at which point the process will be complete.

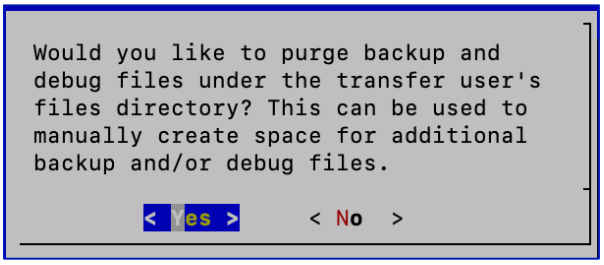


9. Option **“2. Purge transfer file directory”** allows deletion from the appliance’s ‘transfer’ user directory backup and debug files to create space for further newer files.



10. Before proceeding a message will ask whether it should continue or not with the operation which requires confirmation.

    Click **Yes.**



16. Learning Outcomes

Thank you for completing this Threat Visualizer Administration course. We hope this has given you the confidence to tackle a variety of aspects within your deployment.

Complete the learning outcome checklist:

☐	**I understand Darktrace data capture**
☐	**I can confidently configure subnets and optimize devices**
☐	**I am able to assign permissions and groups to users**
☐	**I can follow the Audit Trail**
☐	**I know how to check the health of appliances through the System Status**
☐	**I feel comfortable with deploying SaaS connectors**
☐	**I can effectively configure different types of alerts**
☐	**I understand how to export and integrate alerts with SIEMs and use the API**
☐	**I have set up the Darktrace Mobile App**
☐	**I can successfully configure HTTPS certificates**
☐	**I am able to create backups and restore from them**
☐	**I know how to upgrade the Darktrace Appliance and Model Deck**

For all further education enquires, 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.