DARKTRACE ACADEMY

THREAT VISUALIZER ADMINISTRATION

Training Manual

Threat Visualizer Administration

Training Manual
v4.4.2
Darktrace 6.1

Table of Contents

Table of Contents

1. Learning Objectives

Course Agenda

This course, Threat Visualizer Administration, outlines a range of 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.

The following document serves an educational guide for the key configuration elements of Threat Visualizer interface.

PDF Navigation

To navigate back to the Table of Contents page, click on the Home button.

To navigate back to the chapter's menu, click on the Menu button.

To access related videos from the Customer Portal, click on the Play button.

Some elements can be interacted with by clicking on options, hovering over images or typing in the reserved space.

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

- **Optimize devices and configure subnets**
- **Enhance device tracking configurations**
- **Assign permissions and groups to users**
- **Configure LDAP, SSO, and HTTPS Certificates**
- **Deploy Cloud/SaaS Security Modules**
- **Create and restore from backups**
- **Upgrade the Darktrace Appliance and Model Deck**

2. Device and Subnet Administration

In order to obtain an accurate picture of network architecture, it is useful to understand the devices and subnets being modeled by Darktrace. In this chapter, let's review the device and subnet admin pages.

Device Admin

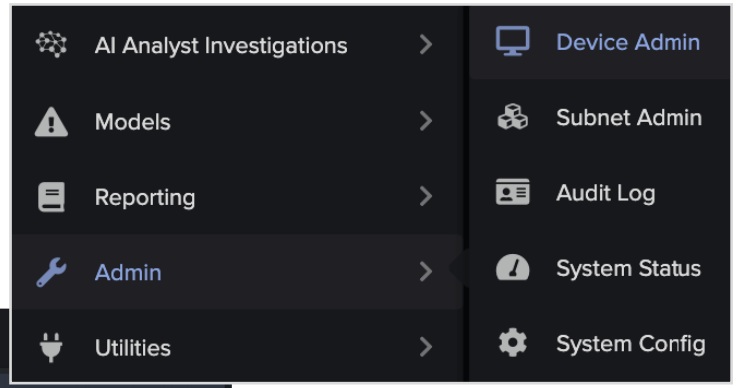
1. Under the main menu, hover over **Admin** and select **Device Admin**.

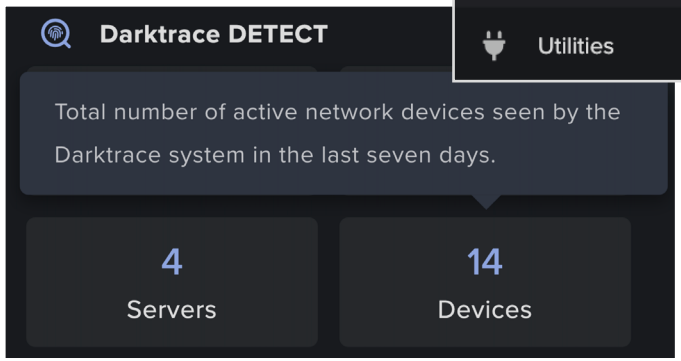
   Alternatively, click the **devices statistic** in the Darktrace DETECT summary.

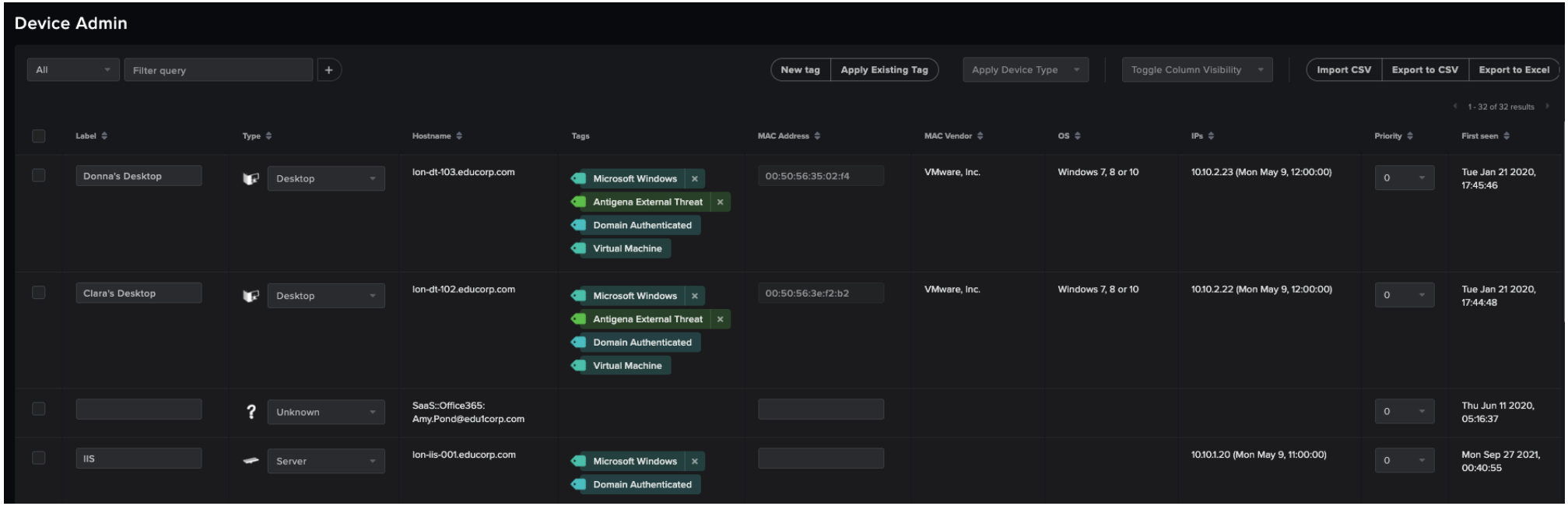
2. This will open the Device Admin interface in a new tab which lists all the devices which have ever been observed on the network since Darktrace was installed.

   For each device on the network, the 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.

   By clicking the headings, the columns can be ordered in ascending or descending order.

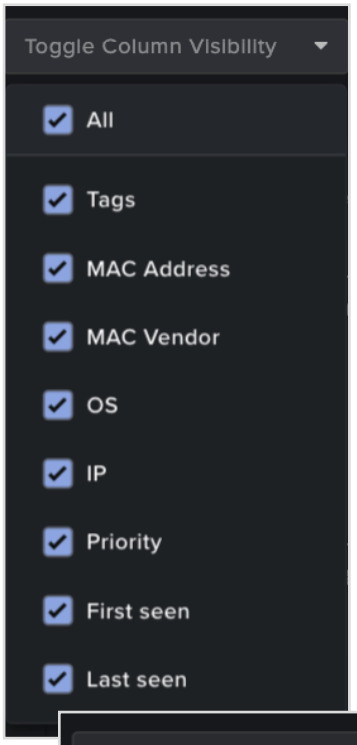






3. The columns displayed can be **limited**. Click the **Toggle Column Visibility** drop-own menu to select/deselect the columns as desired.

   With columns deselected, the table will change. The workspace can be easily reset to show the default columns by checking the **All** option at the top.

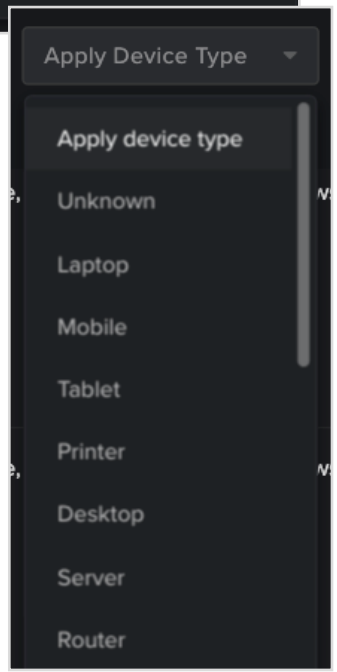


4. **Labels** are nicknames for devices. Examples may include short descriptions to help understand a device's key function, such as DC1, Antivirus, or Darktrace.

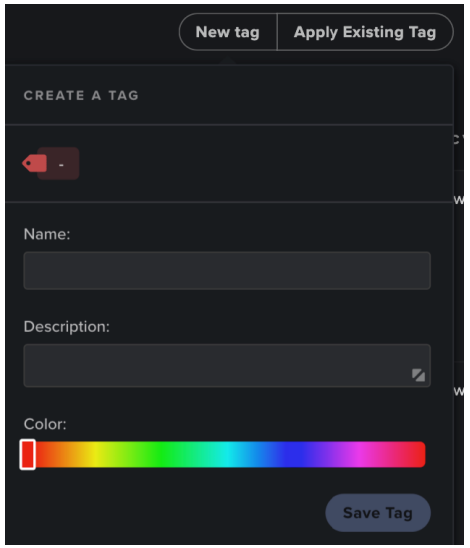
   Labels are particularly useful if hostnames lack clearly defined naming conventions. It is not necessary to label every device, but it is recommended to name key servers or devices, especially those which often cause model breaches.

5. 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.

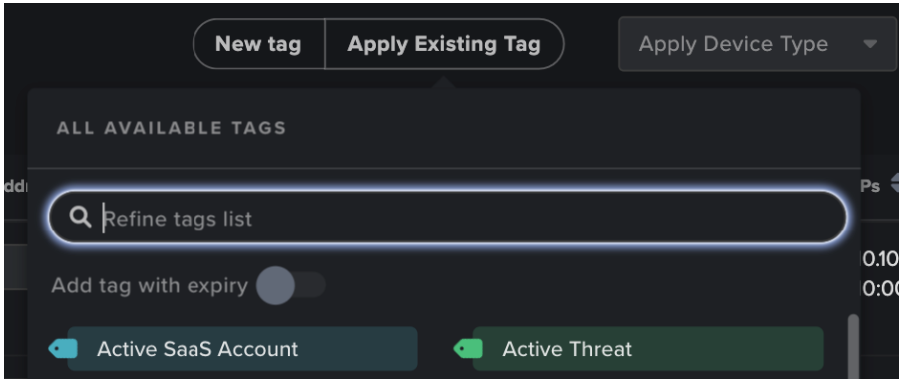


6. **Tags** are like roles for devices. They can be used to group similar devices together. Examples of Tags included DNS servers or Security devices. Tags are defined to facilitate searching for devices and tuning models to only fire if a tag has been set.

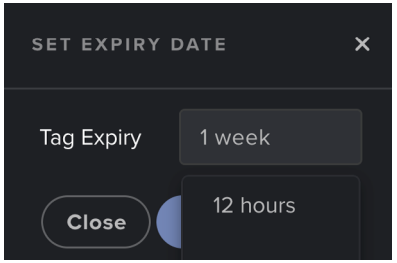


   a. Tags can be created by clicking the **New tag** button and filling out the fields. Upon creation, this tag is available to be applied to devices.

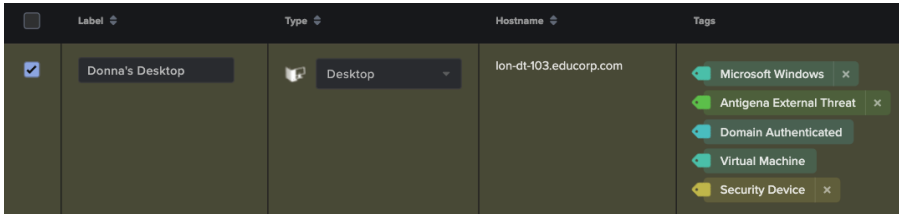
   b. To apply a Tag to devices, click **Apply Existing Tag** at the top of the screen. This will open a selection of available Tags, which can be refined using the search bar



   c. Turning on the **Add tag with expiry** toggle will allow users to add an expiry to the selected tag(s) by clicking on the tag and using the tag expiry drop-down menu.



d. 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.



7. **Priority** is a method to boost the threat score of a device. It ranges from -5 to 5 in increments of 1.

   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.

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.

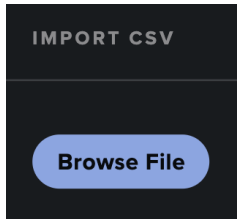
   Click this and enter text in the dialog to add notes. Devices which already have notes can be identified by a similar icon which contains an orange circle.

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. There are multiple **import** and **export** options for the Device Admin.

   a. The options to export to **Excel** or **CSV** creates a copy of the table into a spreadsheet format.

   b. The results can be updated by importing a CSV file. Click the **Import CSV** option to open a window which allows the user to browse files.



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

Top Tip:

By exporting to CSV format, the file can be used as a template for any Device Admin updates which can be carried out by importing a CSV.

Configuring 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.

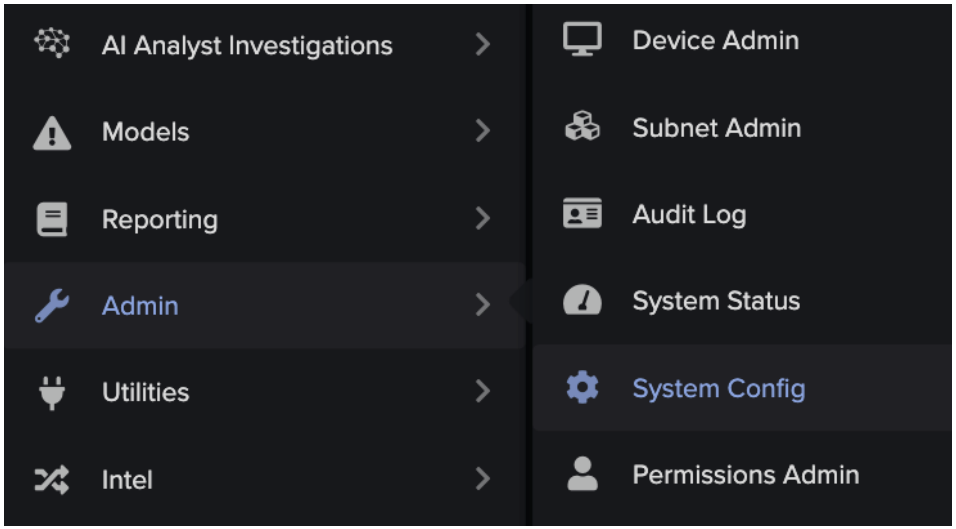
Similar to the method used in the Device Admin page, a more granular type can be set for devices in the Threat Visualizer.

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.

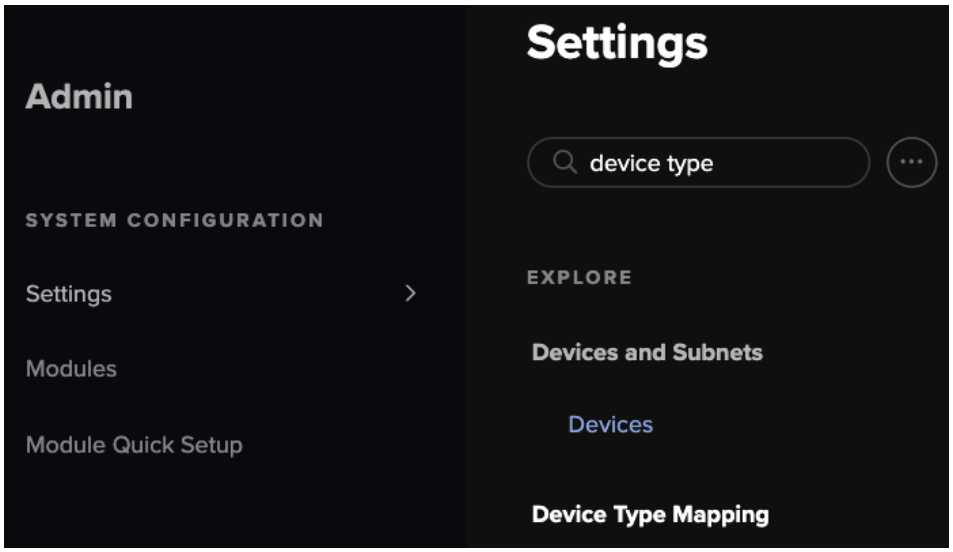
If you desire to be more granular, you can create a model where the Action of the model, if conditions are met, will be to change the device type.

You can set the hostnames that Darktrace should expect to see for: Desktops, IP Phones, Laptops, Mobiles, Printers, Servers and Tablets, as detailed below.

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** and locate the **Device Type Mapping** section.

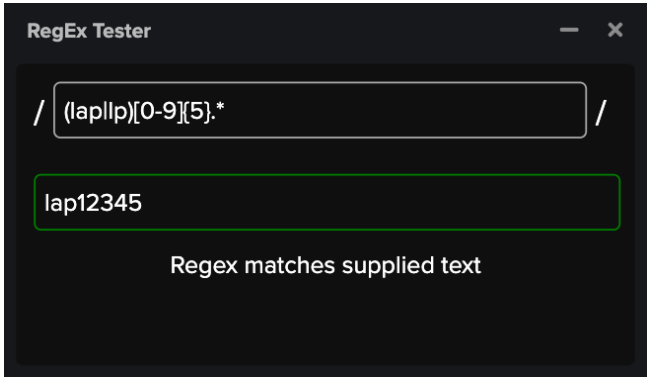


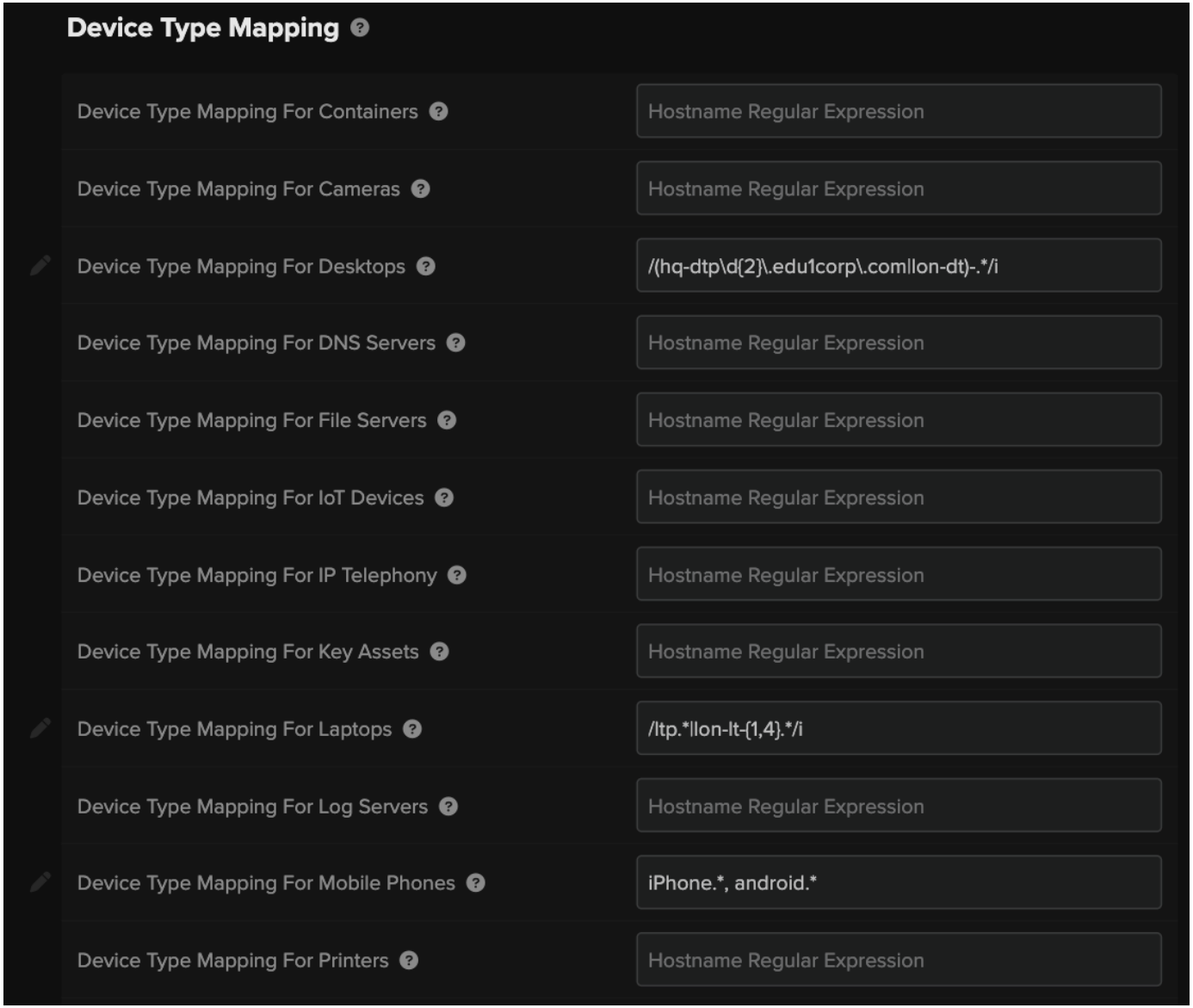
3. The device type mapping fields accept **text or regular expressions**. The table below provides some examples.

SET	REGEX VALUE
Hostname for Desktops	(mac|w7)-dsktp.+\darktrace.corp
Hostname for IP Phones	voice.+\.darktrace.corp
Hostname for Laptops	(mac|w7)-.+\.darktrace.corp
Hostname for Mobiles	iphone.+\.darktrace.corp
Hostname for Printers	print.+\.darktrace.corp
Hostname for Servers	srv\.dc(1|2).+\.darktrace.corp

4. The Device Type Mapping section contains many **fields for different device types**.

   If text or regular expressions are inputted into any of these fields, this takes immediate effect when the device is next seen and will be applied to future devices as well.





Top Tip:

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.

Try the RegEx Tester in the Threat Visualizer Utilities to see if your regular expressions match device names on the network.

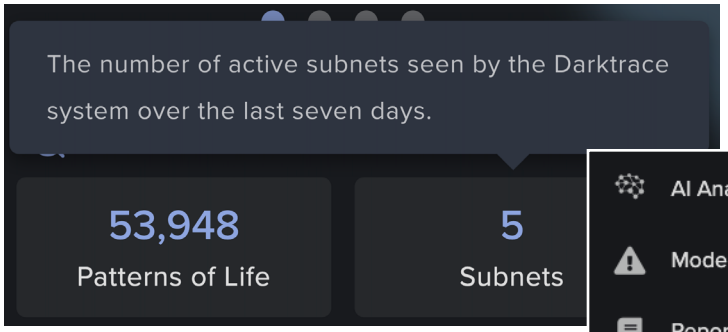
Subnet Admin

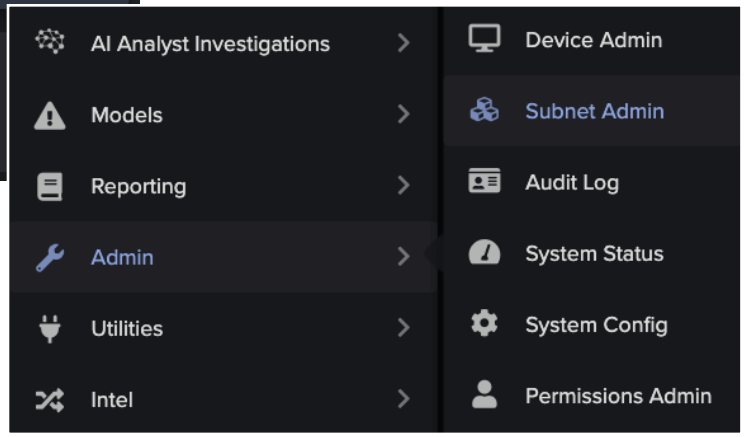
1. Review the **Subnet Admin** page, also found by navigating through the Admin menu.

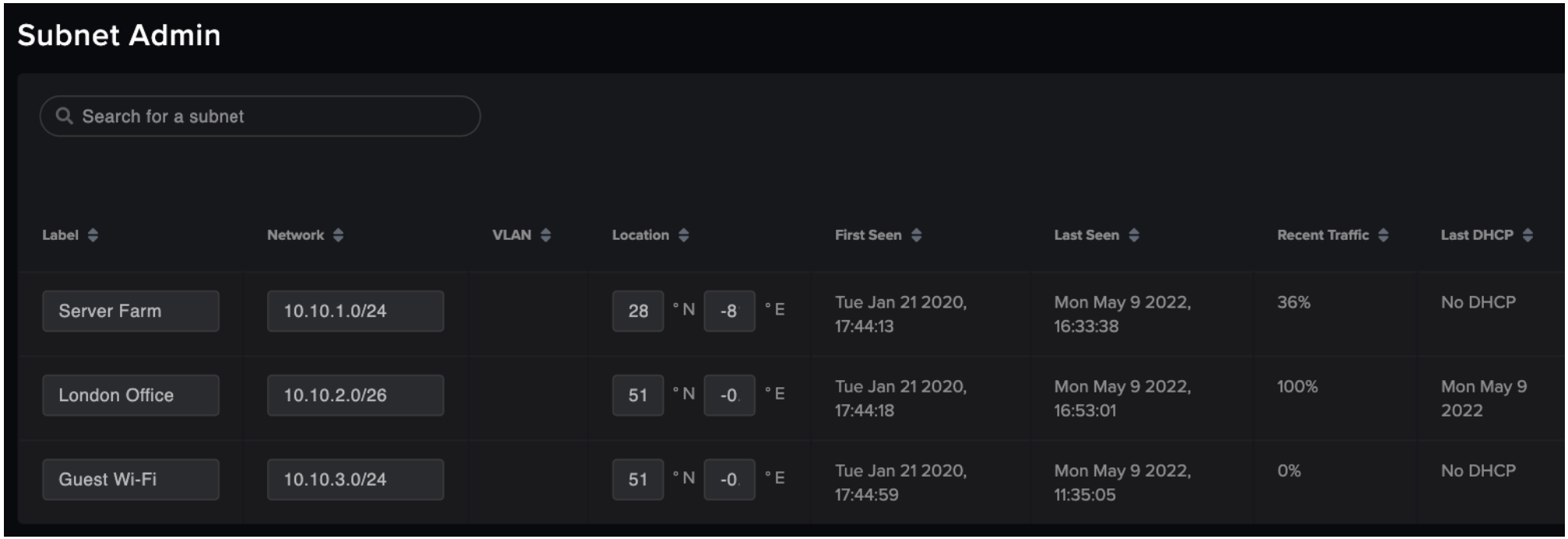
   The alternative way to reach this page is to click the **number of subnets** in the Darktrace DETECT summary view.

2. The Subnet Admin page has a **table** containing the **network ranges** and a plethora of associated useful information.

   By clicking the headings, the columns can be ordered in ascending or descending order.

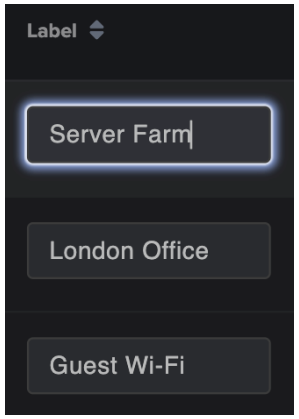






3. By labeling subnets on this page, it can make reading network diagrams much easier.

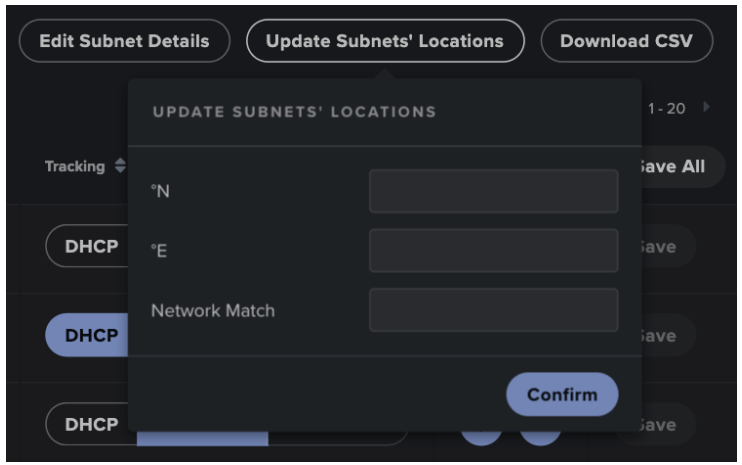
   To add a **label**, click a network range and type in a nickname. These values will then be searchable in the Omnisearch bar and will be presented in the Subnet View.



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.

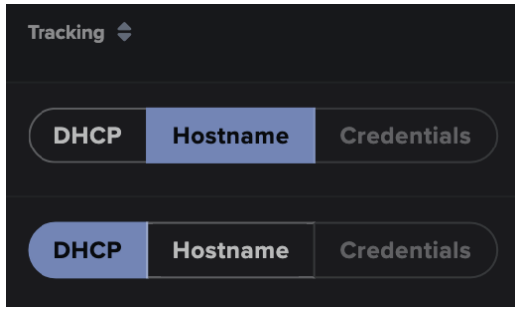
5. To update the latitude and longitude of multiple subnets, click the **Update Subnets' Location** at the top of the page.

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**.

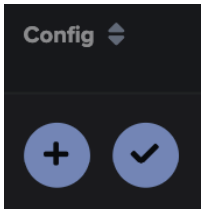
   Most regular dynamic subnets are fine using the DHCP option, but this option should be removed for static subnets.



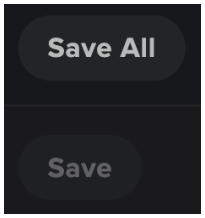
Note: Device Tracking will be covered more in depth in the next chapter.

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.

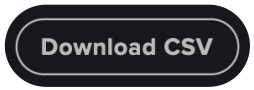
   To prevent Darktrace tracking and triggering model breaches in a Subnet, click the **tick** button.



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.

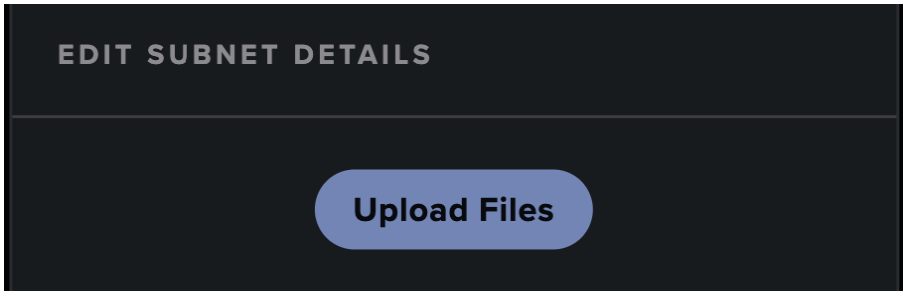


9. To download a copy of the current Subnet Admin table, click **Download CSV**. This will allow easy editing, or it could be useful to maintain a copy of the original table.

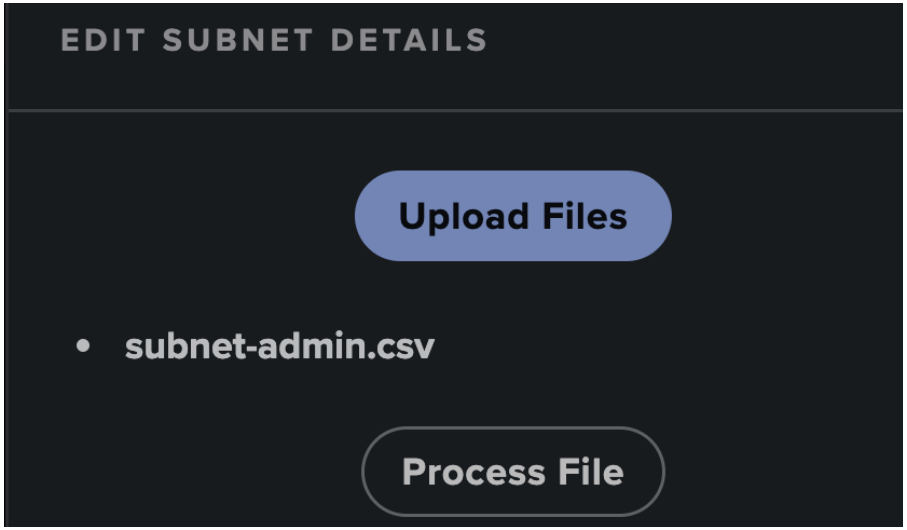


10. Rather than editing details from the Subnet Admin page, it is possible to upload an existing CSV file. Click **Edit Subnet Details**.

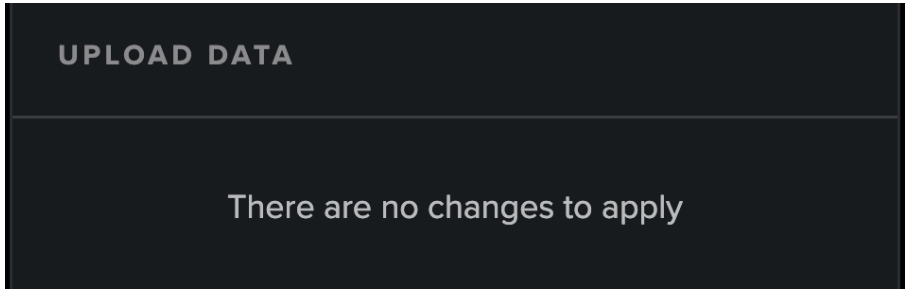
    a. An **Upload Files** option will become available. Darktrace will accept CSV files in the same format as the CSV file that can be downloaded from the Subnet Admin page.



    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 (if any) that will be made. Click **Confirm** to proceed or click outside the dialog to escape.



Top Tip:

If you notice any traffic changes such as the appliance being slower or timing out, check the health of the appliance via the System Status page. This page is discussed more in depth in our Cyber Engineer course.

Device and Subnet Admin Chapter Test

DARKTRACE
Cyber Engineer Certification

This page will test your knowledge and check your understanding of the Device and Subnet Administration section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. Which column is used to set up nicknames for devices?

- [ ] Types
- [ ] Labels
- [ ] Tags

2. What is the possible range of a device's priority score?

- [ ] -5 to 5
- [ ] 0 to 5
- [ ] -5 to 10

3. Which RegEx value will be used to set a hostname for laptops?

- [ ] voice.+\.darktrace.corp
- [ ] (mac|w7)-dsktp.+\.darktrace.corp
- [ ] (mac|w7)-.+\.darktrace.corp

4. On which page can you add specific notes?

- [ ] Device Admin only
- [ ] Subnet Admin only
- [ ] Both

5. It is possible to track subnets using credentials.

- [ ] True
- [ ] False

6. Which subnet geographical coordinates can you modify?

- [ ] Latitude only
- [ ] Longitude only
- [ ] Both

Clear All Answers

3. 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. In this chapter, let's review the different ways that Darktrace might track devices.

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.

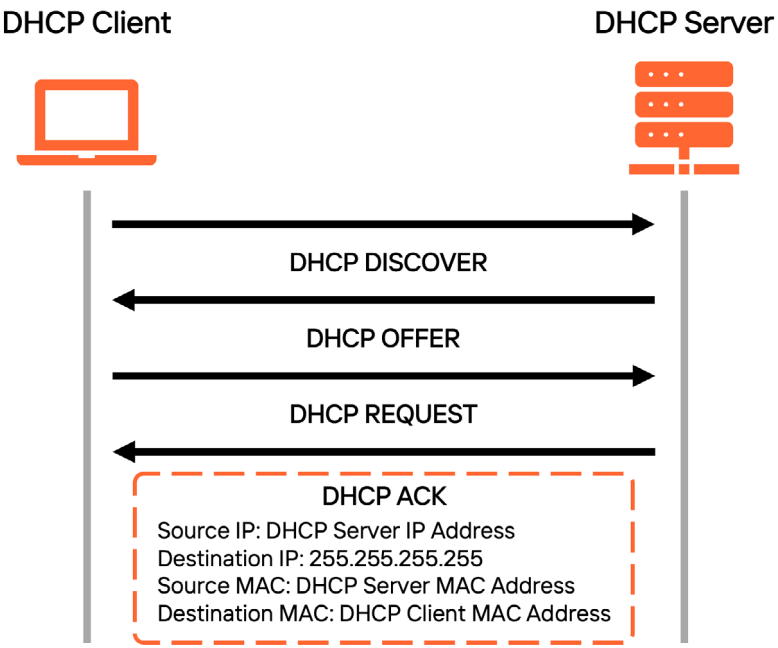
Device Tracking Methods:

There are multiple methods for device tracking in Darktrace:

- Static IP address tracking
- Dynamic IP address tracking via DHCP
- Tracking via DHCP or VPN logs with Syslog Ingestion
- Tracking by hostname from Kerberos or DNS traffic
- Tracking by credentials used on devices

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 receive a DHCP ACK request from the DHCP server. 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.

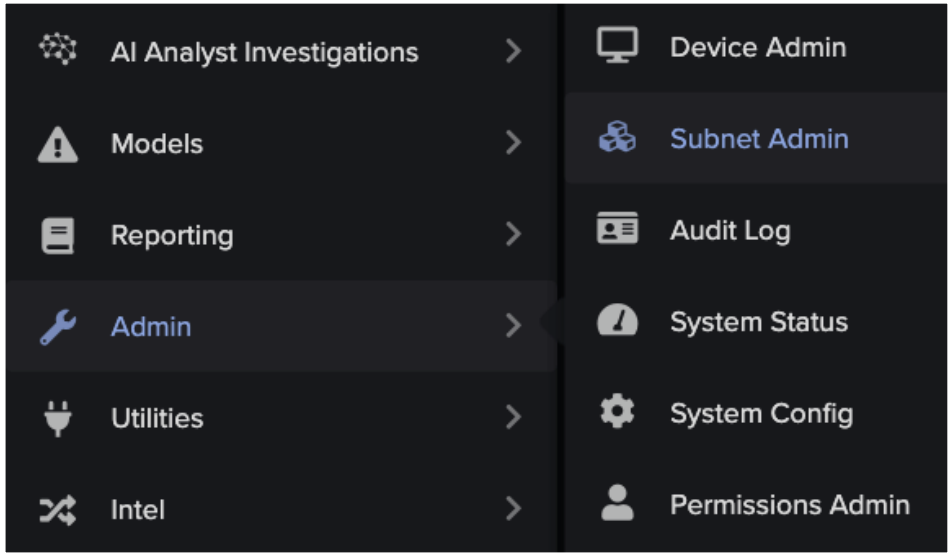
This method can mean a device such as a laptop can be displayed twice in Darktrace. One device for the connection via a physical Ethernet cable, and another for the Wi-Fi network card. Differentiating the two can assist Darktrace learn a pattern of life for a device. For example, typically a user's behavior 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.

By analysing DHCP traffic Darktrace extracts a device's IP, hostname and MAC address to improve its tracking and its identification. By default, DHCP is expected on all subnets. If a subnet does not have any DHCP traffic, such as a network of static IP servers, the Threat Visualizer Status page will show "No DHCP" in red for the offending subnet.

- If DHCP is expected but not observed, this is indicative of missing data. To rectify, traffic mirroring has to be reviewed or, instead, DHCP logs can be ingested directly in syslog format to provide the missing assignment data.
- If DHCP is not expected, it can be disabled to remove warnings. When a subnet is to be tracked by credential, DHCP must be disabled.

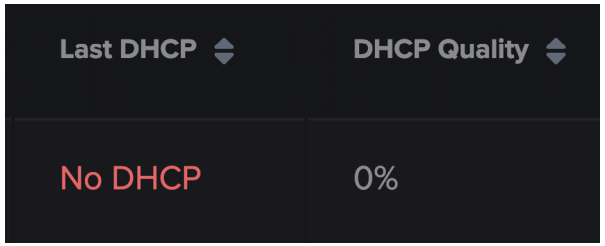
Disabling Subnet DHCP

1. Within the Threat Visualizer, navigate to the **Subnet Admin** page in the main menu under **Admin**.

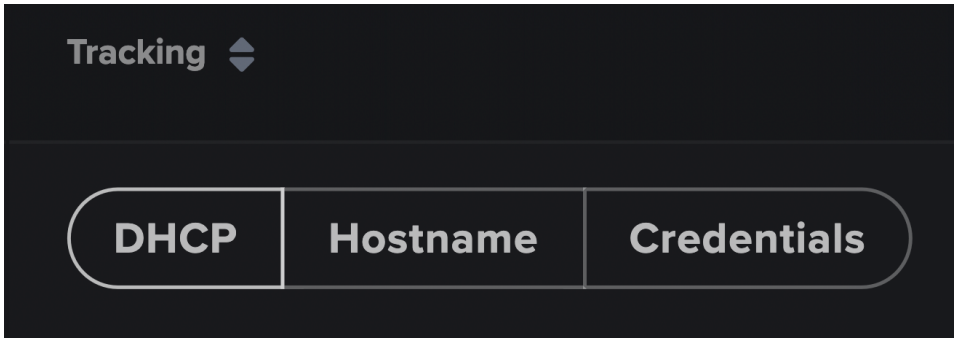


2. Locate any Subnets with **No DHCP** in red.

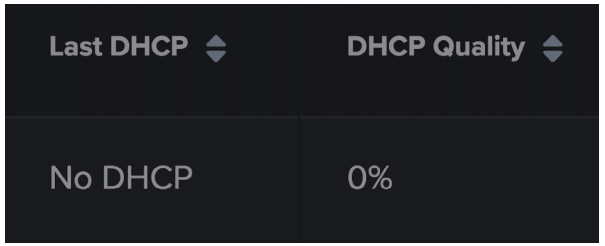
   If this is expected, the warning can be removed. Otherwise, alter the traffic mirroring configuration or setup DHCP log ingestion to provide the missing assignment data.



3. Locate the corresponding entry. Click the highlighted **DCHP** in the **Tracking** column to disable DHCP for the Subnet and save the changes.



4. Confirm that the **No DHCP** warning is no longer in red



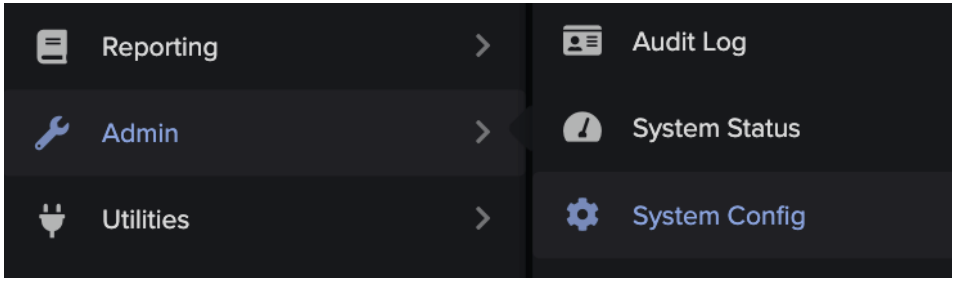
Tracking by Hostname

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.

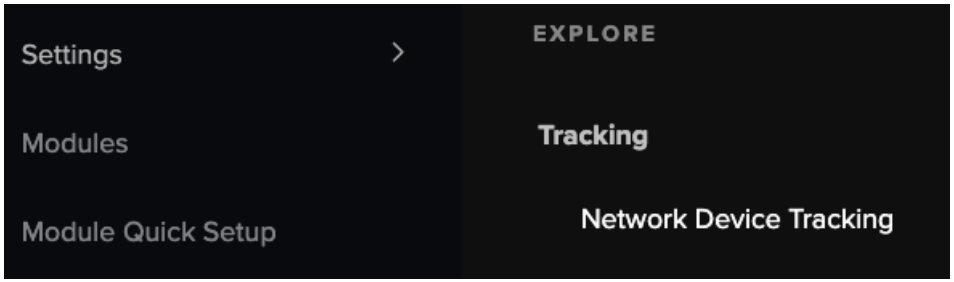
If DHCP is unavailable, Darktrace will default to tracking a device by its IP address. This may mean it will lose track of devices where they have dynamic IP addresses. However, by configuring Darktrace options, hostnames can be appended to a device to better track them. To aid in this process, there are three ways to configure Darktrace to look for hostnames.

Passively Look for Hostnames in Kerberos Traffic

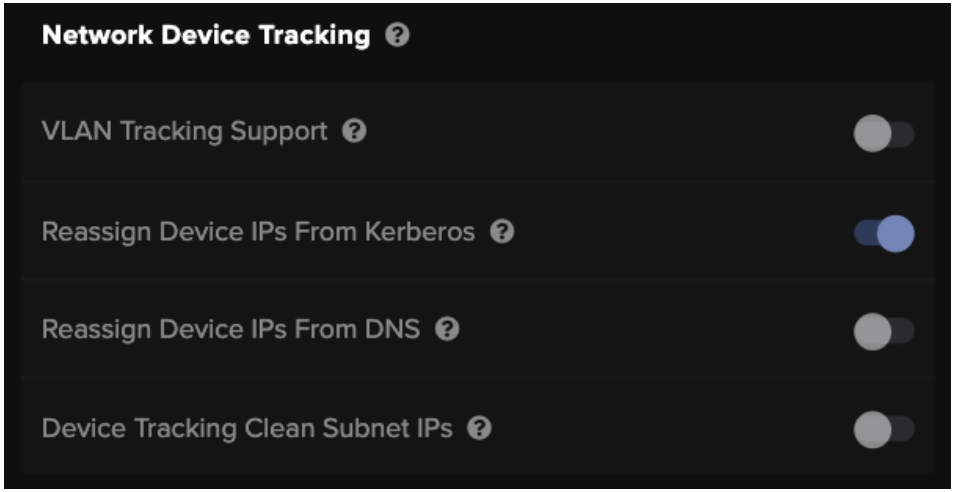
1. Navigate to the **System Config** page.



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



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



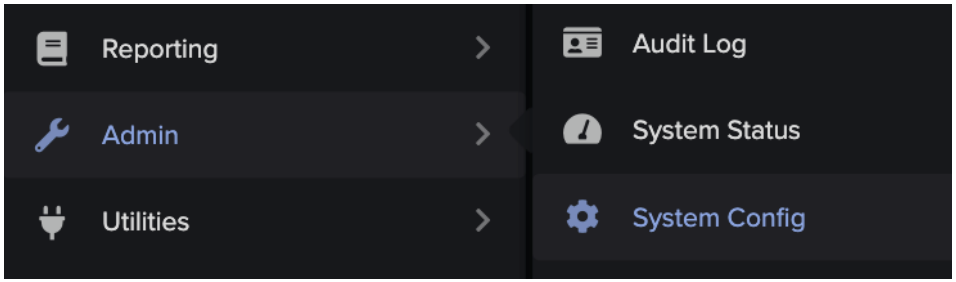
When DHCP is not available, setting this to true will enable Darktrace to append hostnames when performing Kerberos authentication.

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.

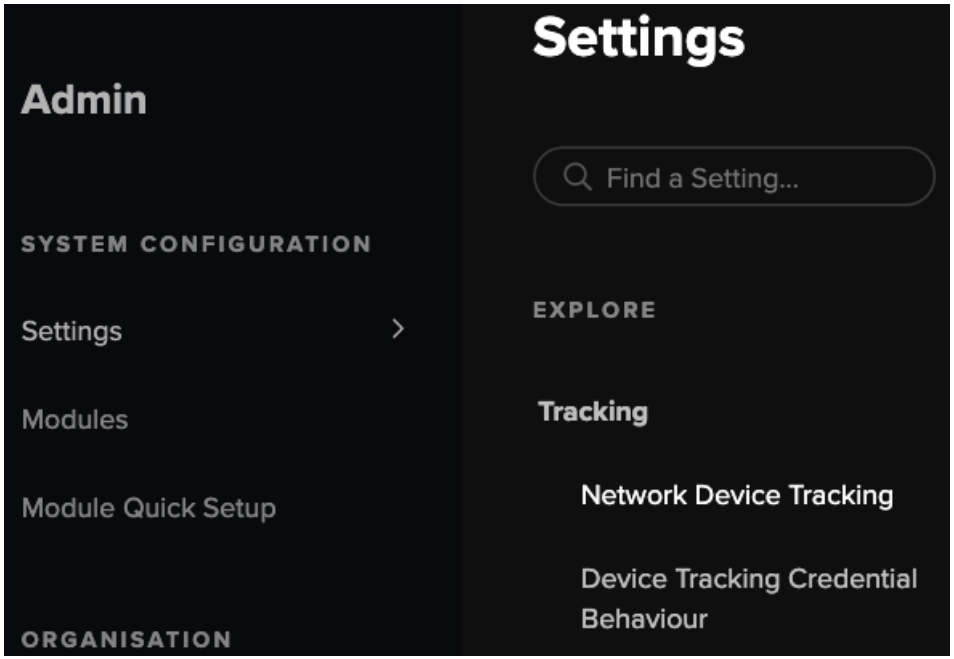
Passively Look for Hostnames in DNS Traffic

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

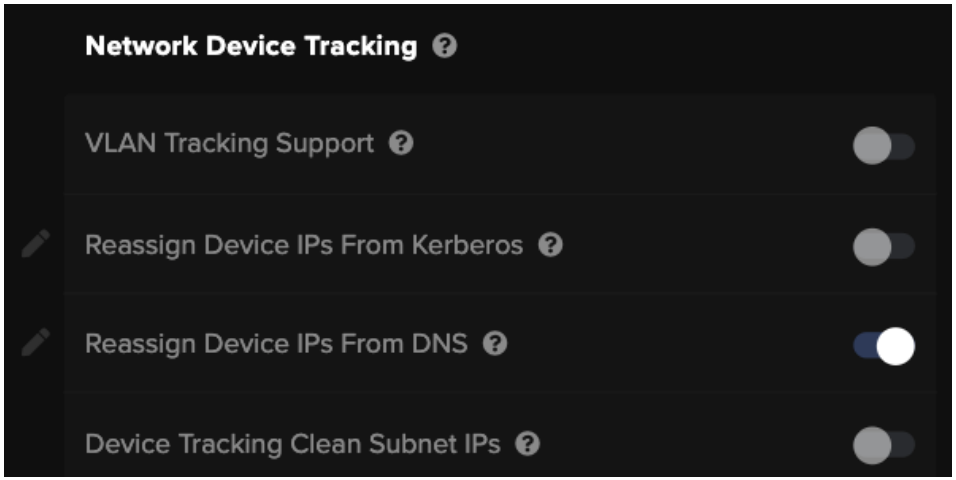
1. Open of the **System Config** page from the main menu.



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



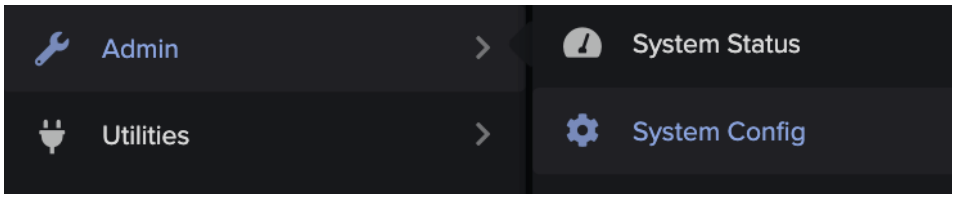
3. Review the **Reassign Device IPs From DNS** setting. By default, this option is disabled. Typically enabling this setting is not recommended, so only enable this setting if all other options have been exhausted.



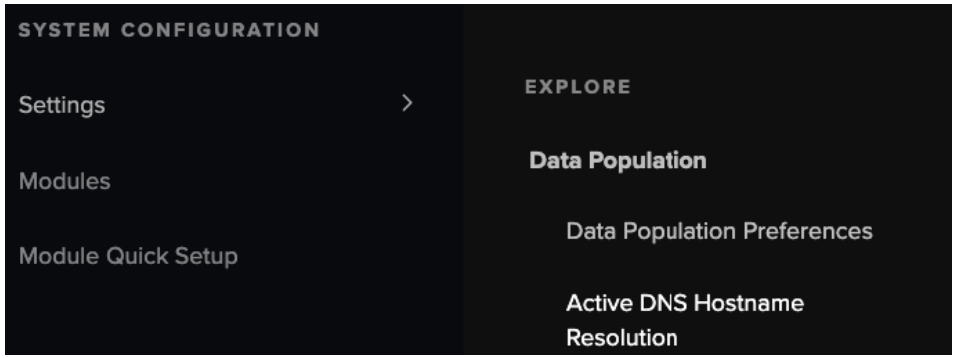
Polling DNS Servers to Append Hostnames

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.

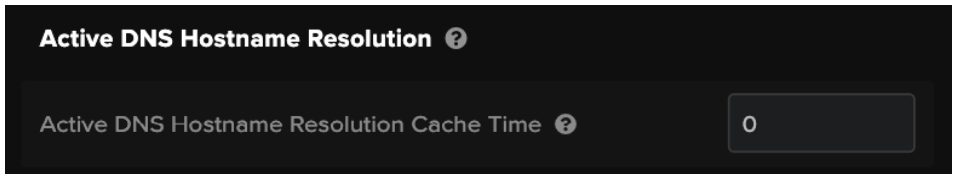
1. Open of the **System Config** page from the main menu and access Settings.



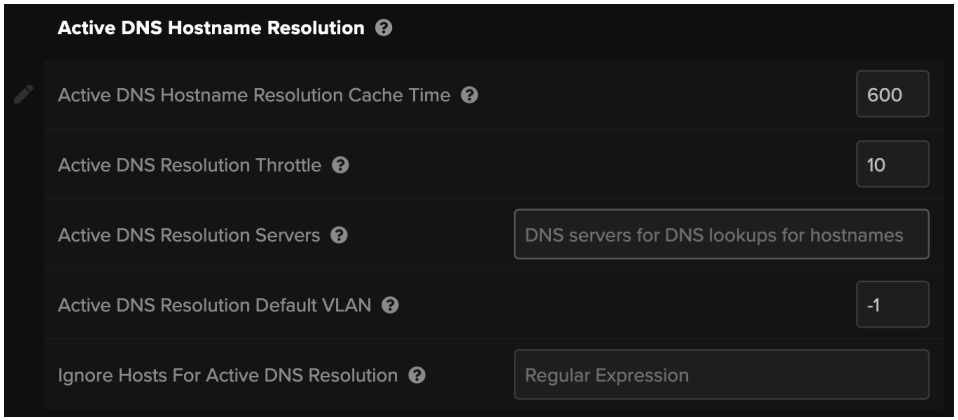
2. Locate the **Data Population** section and navigate to the **Active DNS Hostname Resolution** subsection.



3. Within the **Active DNS Hostname Resolution** section, there is a Cache Time field with a default value of 0.



4. 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.



Note: A value of 7200 seconds (2 hours) is typical, but a minimum of 600 seconds (10 minutes) is required to reveal additional options.

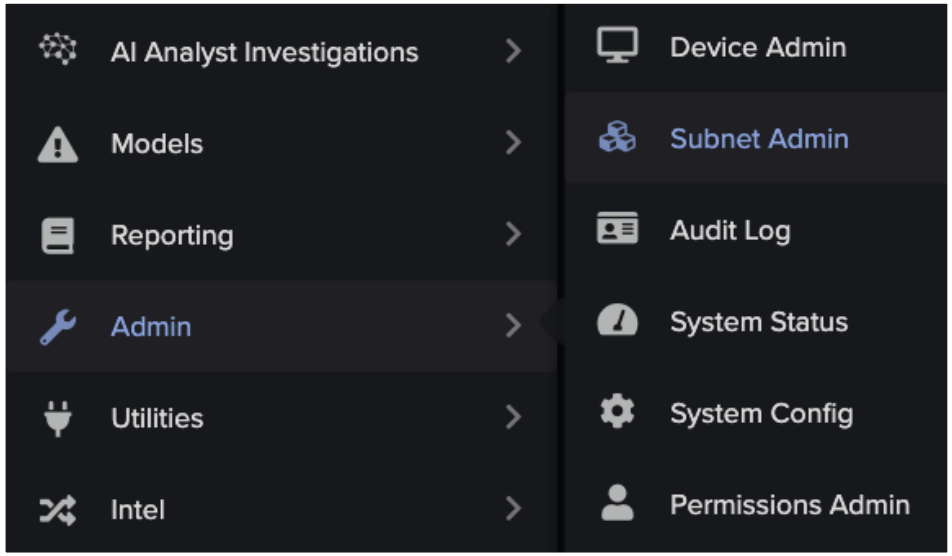
a. When performing DNS resolution, the **Active DNS Resolution Throttle** value limits the maximum frequency of requests per millisecond. The default value is 10 but can be altered if desired.

b. 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.

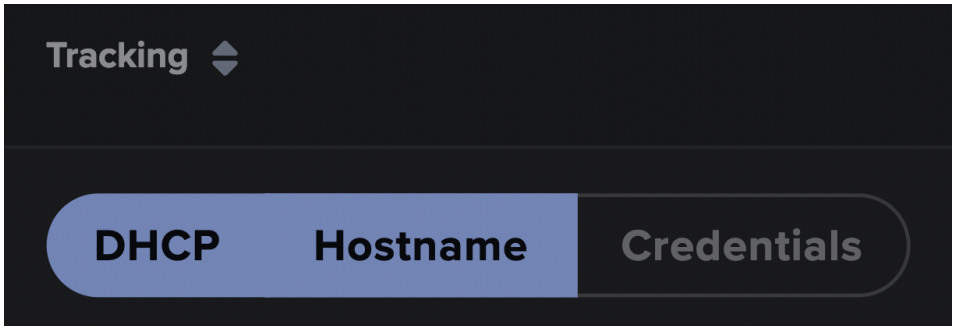
5. **Save Changes** by clicking the button which will be displayed at the top of the screen when values are entered.

Configuring a Subnet to Track by Hostname

1. In the main Threat Visualizer, navigate to the **Subnet Admin** page in the main menu under **Admin** and locate the corresponding entry.



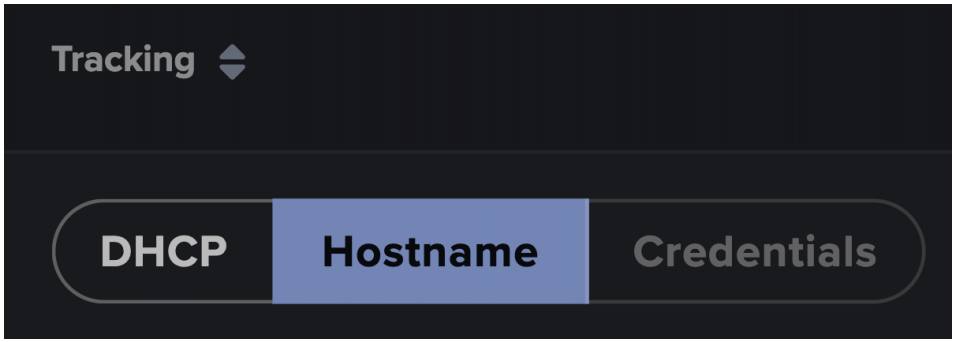
2. Review the **DCHP** setting in the **Tracking** column.



The DHCP subnet setting controls if Darktrace should track devices by DHCP. When tracking by hostname, enabling DHCP will look at hostnames in DHCP traffic as the most authoritative source, falling back on Kerberos or DNS if unavailable.

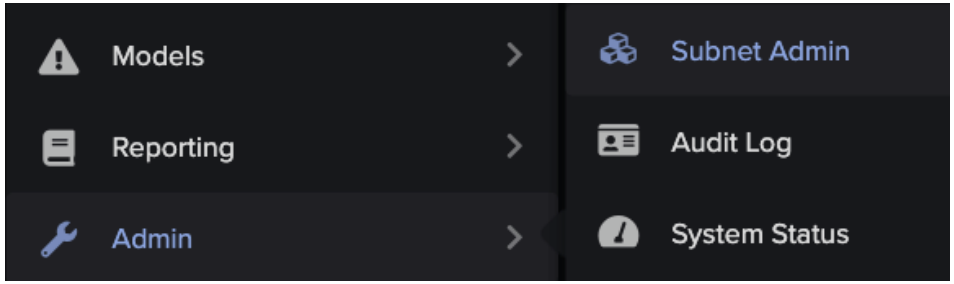
If disabled, Darktrace will use Kerberos and DNS as the primary source for hostname information.

3. Review the **Hostnames** setting. Enabling this setting will begin tracking the subnet by hostname and save the changes.

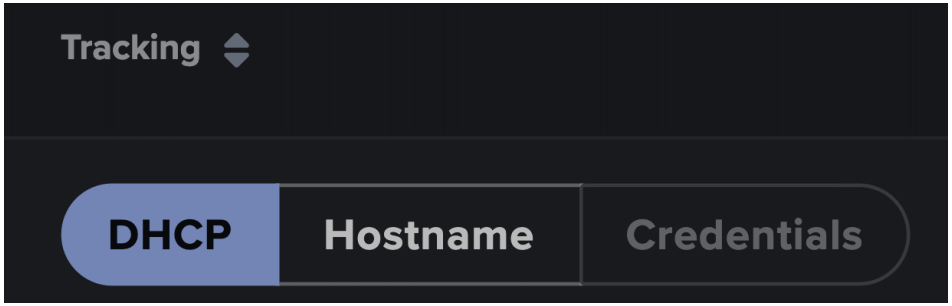


Tracking by Credentials

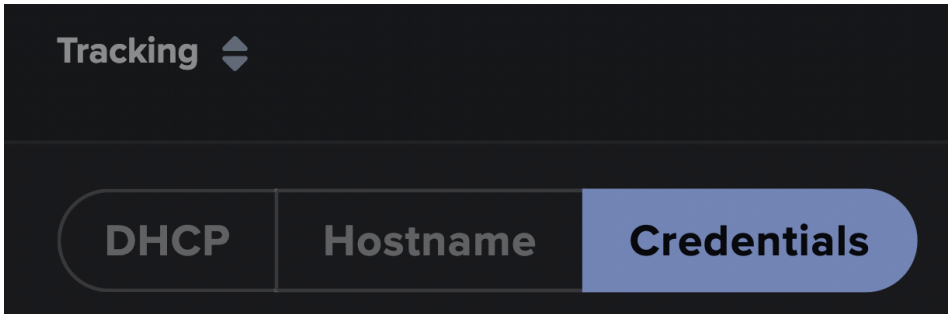
1. In the main Threat Visualizer, navigate to the **Subnet Admin** page in the main menu under **Admin** and locate the corresponding entry.



2. Review the **DCHP** setting in the **Tracking** column. If Tracking Credentials is to be enabled, DHCP must be disabled.



3. Review the **Credentials** setting. Enabling this setting will begin tracking the subnet by credential.

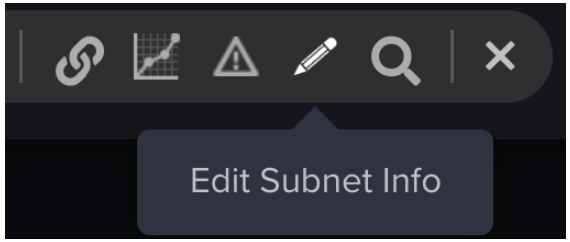


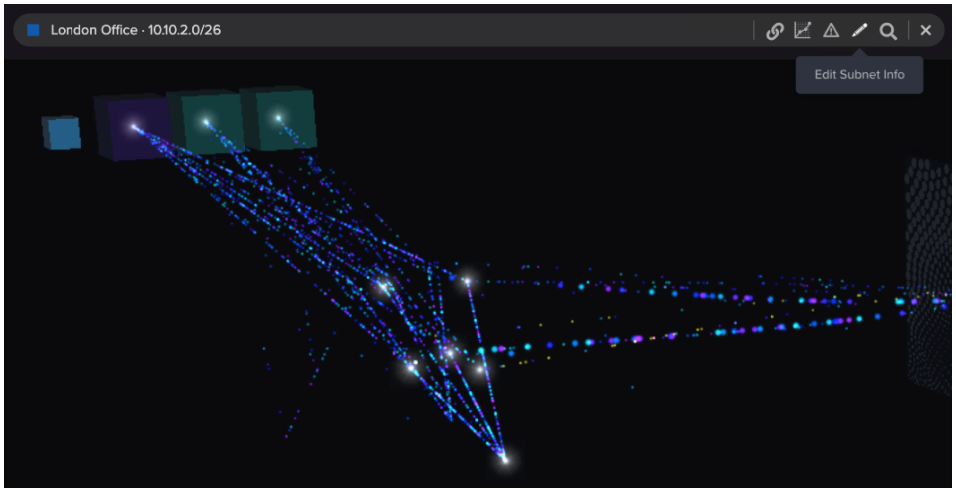
Editing Subnet Info

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).

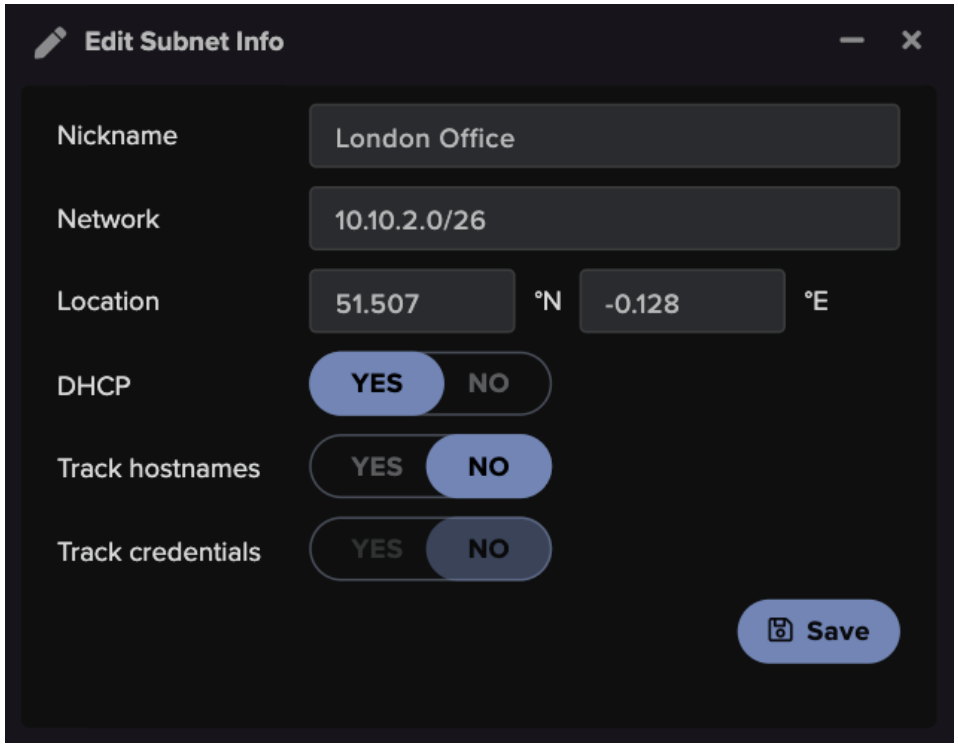
1. In the Subnet View, i.e. with a subnet populated in the Omnisearch bar, click the **Edit Subnet Info** symbol, indicated by the **pencil icon**.





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

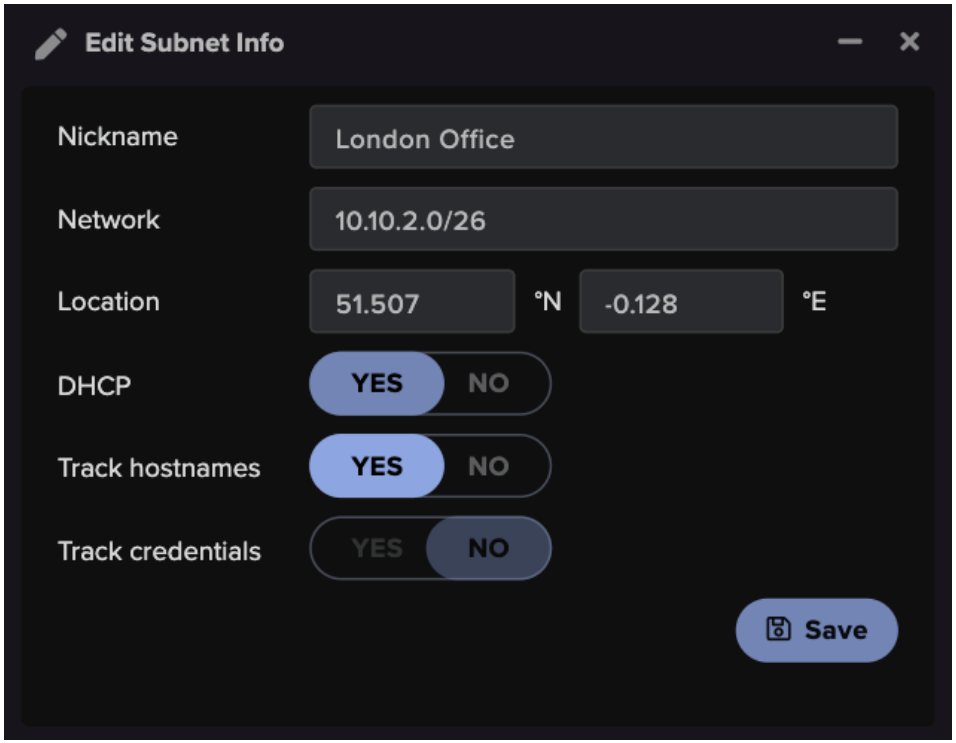
   When **disabled**, Darktrace will track all devices in a subnet by their **IP addresses**.



   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.

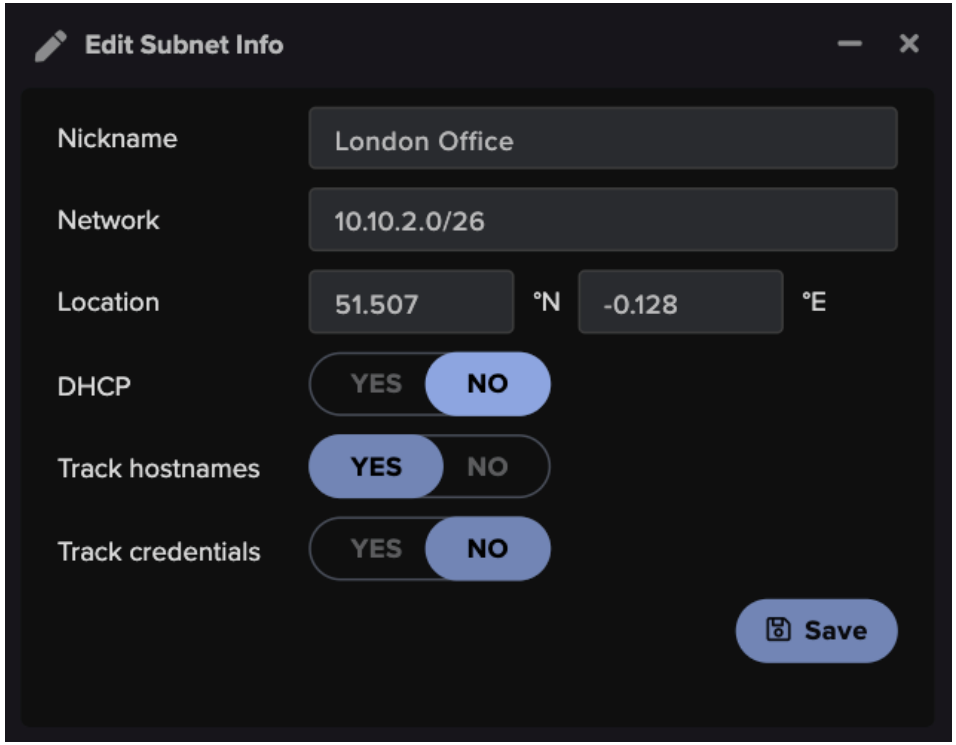
3. It is possible to have **multiple tracking methods** employed for a subnet.

   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**.



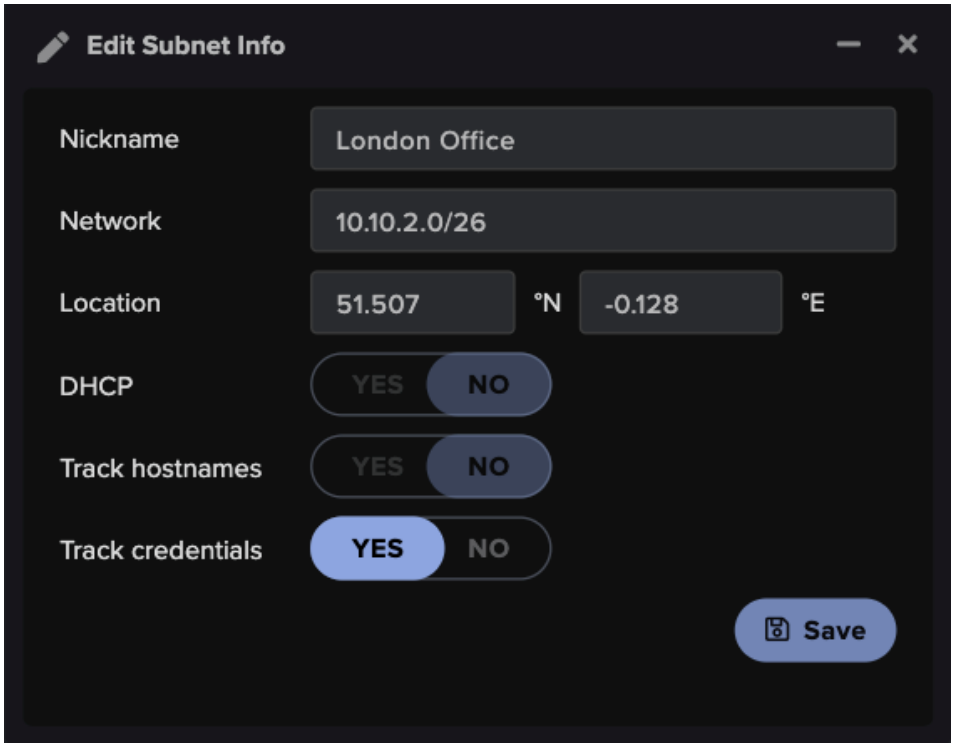
Tracking devices by hostname will assist Darktrace in distinguishing between the various devices which may share the same IP.

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.

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.

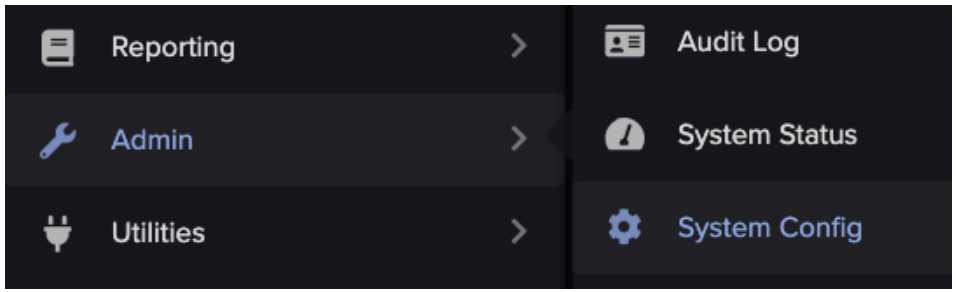
Logs should be sent in syslog format. Encrypted and unencrypted log ingestion is available along with multiple forwarding methods. Darktrace provides support for multiple log feeds into an appliance:

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

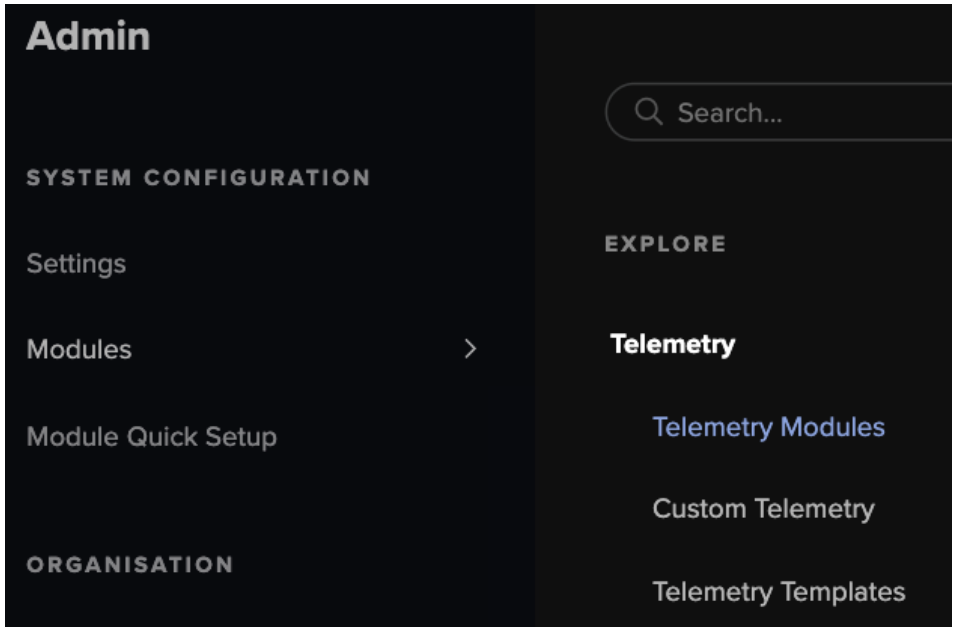
In addition to processing and transmitting network traffic, hardware probes and vSensors are able to ingest and forward syslog format logs to the Darktrace master. Pattern matching is configured on the master and propagated to the vSensor. Matching/Discarding is performed at the vSensor level where valid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

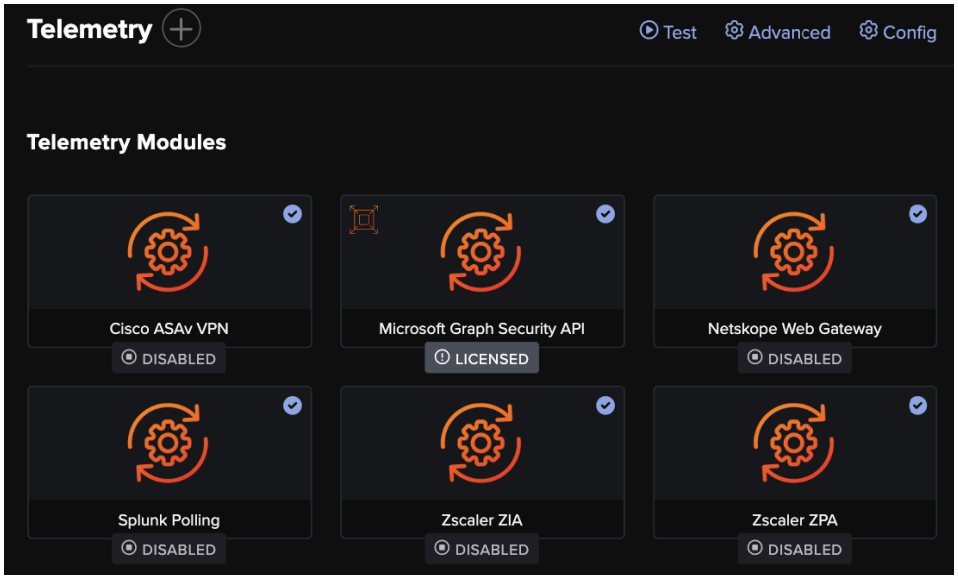
2. From the Darktrace master appliance intended to receive the logs, navigate to the **System Config** page from the Admin section of the Threat Visualizer Main Menu.



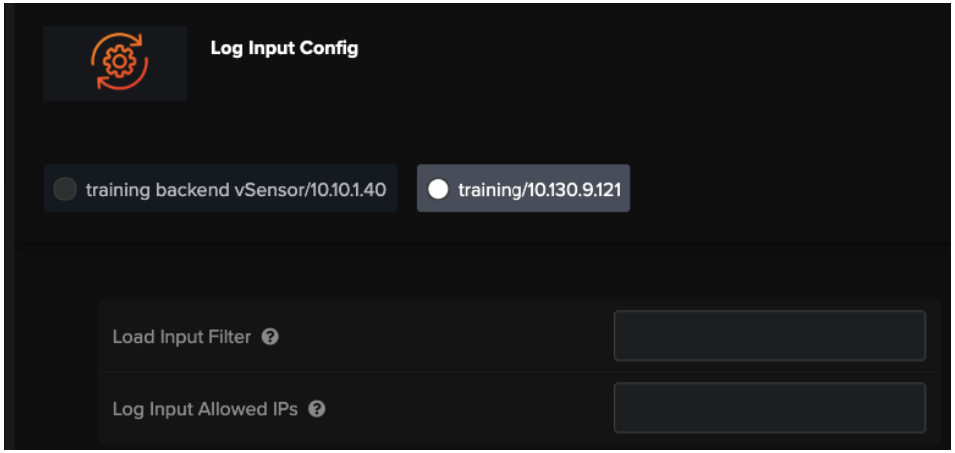
3. Select the **Modules** option from the left-hand menu and locate the **Telemetry** section.



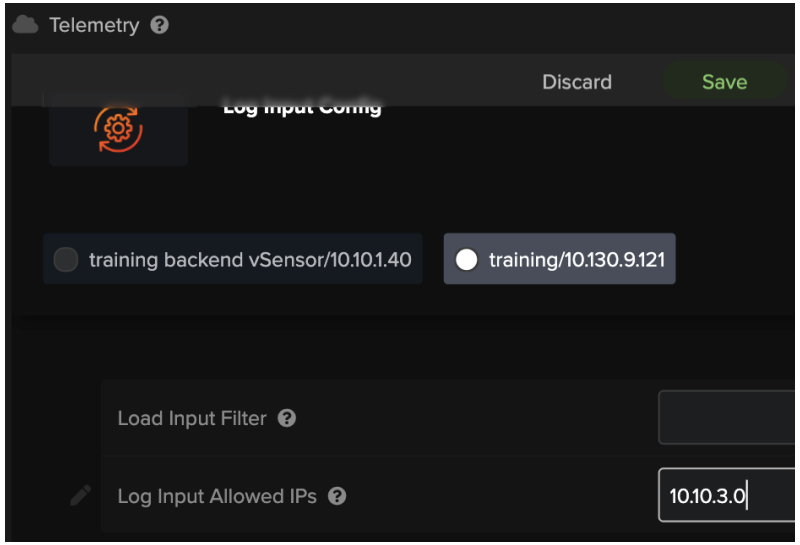
4. From the top right-hand corner of this section, select the **Config** button.



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.



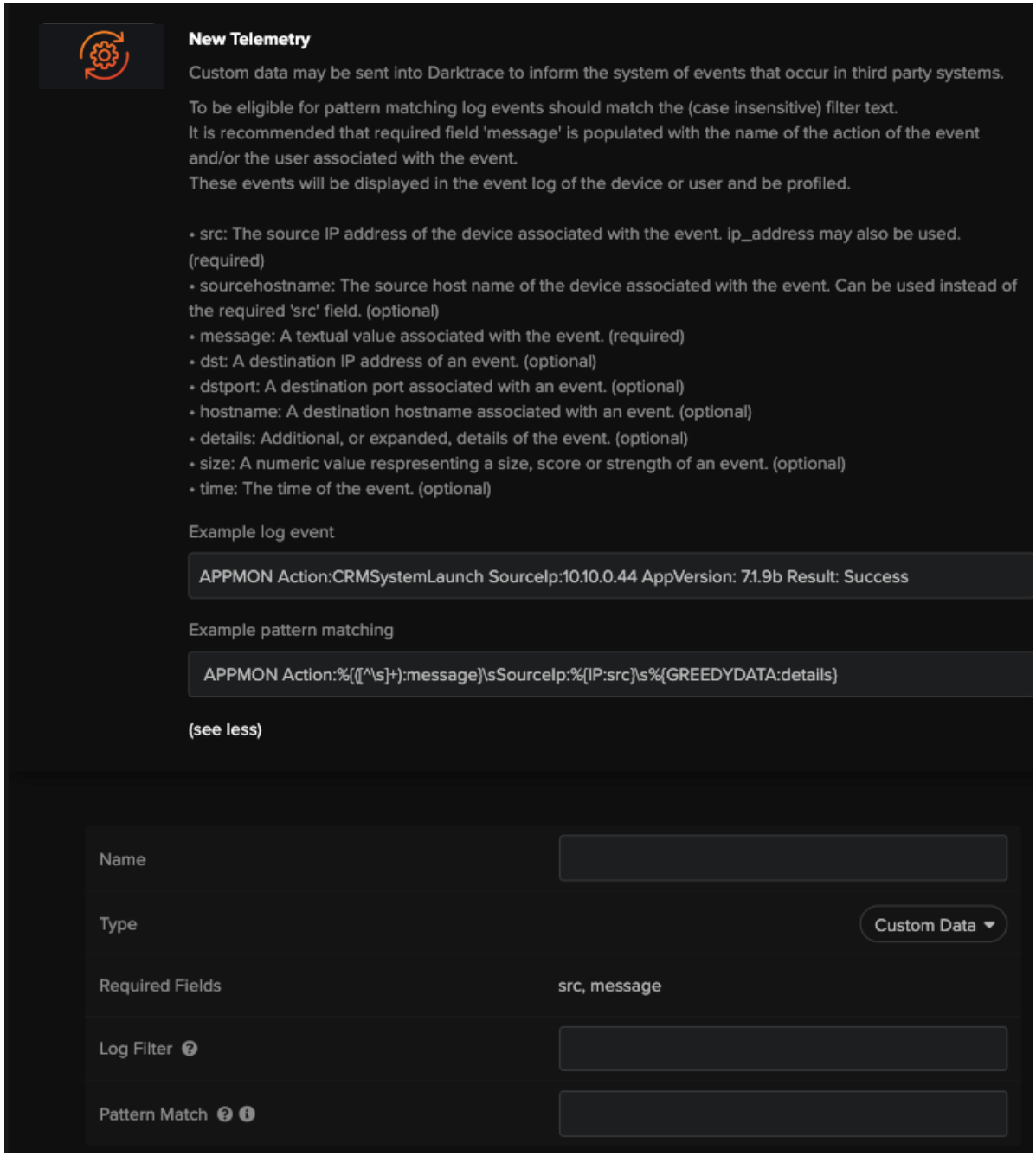
7. In order for logs to be parsed, a **template** must now be defined. To begin this process, **exit the Config dialog**.

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

9. A **New Telemetry** 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.

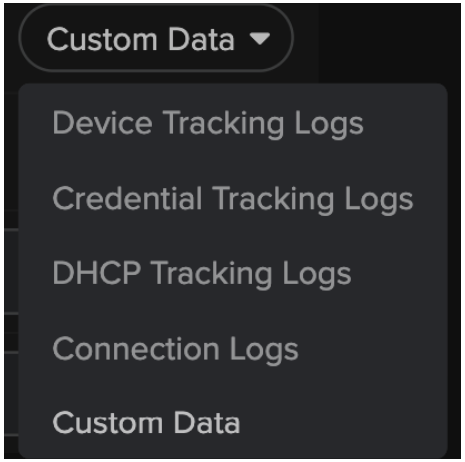
   Log entries are matched against each applicable configured pattern until a match is found. Once a match is found and data is extracted by the associated pattern, no further pattern matching will be attempted.

   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 worked example.

What is Grok?

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.

Log Input Worked Example

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

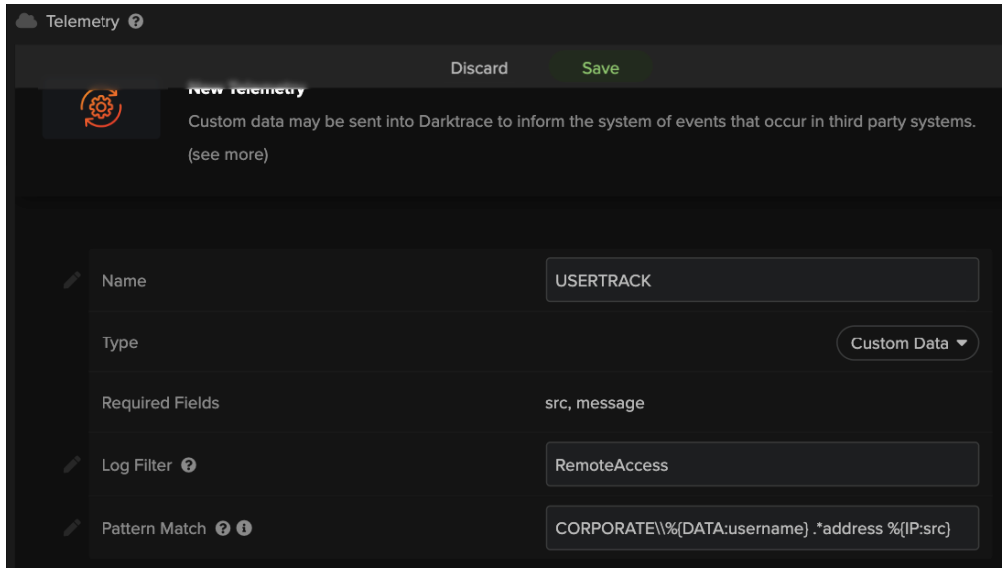
The following log line is an example VPN server log and is intended for use in a subnet tracked by credentials.

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.

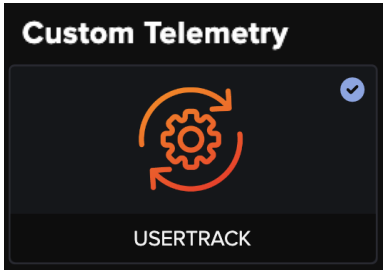
Credential tracking logs require a username and IP address, as indicated by the username and src required fields. It is also possible to obtain a timestamp, but this is optional. The following pattern should extract the username and IP address:

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

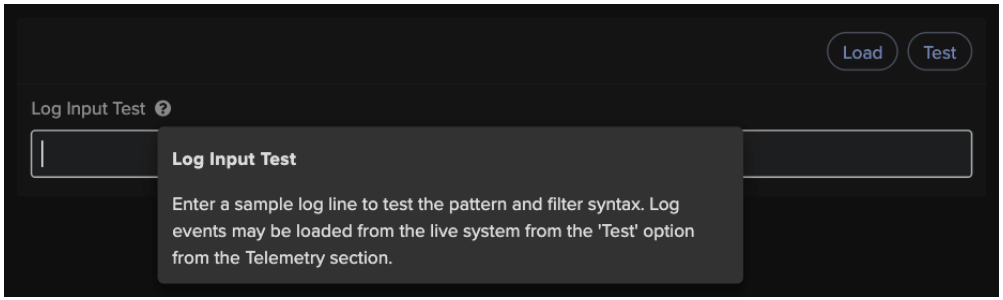


The USERTRACK example will take any log that contains RemoteAccess. In this case, it will look for a string of the form CORPORATE\username, where the username part of the string will be assigned to the username value. It will then look for the value for the source address and will return an IP address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

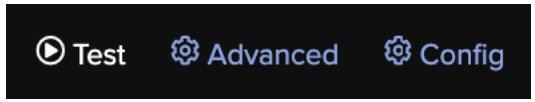
Once a template has been configured and saved, it can be found under **Custom Telemetry**.



Selecting an existing telemetry allows users to utilize the Log Input Test functionality to compare log lines with the configured pattern. Input can be loaded from lines seen or pasted into the field.



Note: Patterns can be also be tested using the Test button beside to Telemetry heading.

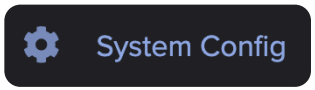


Encrypted Log Input TLS Certificates

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. It is also possible to add a custom certificate.

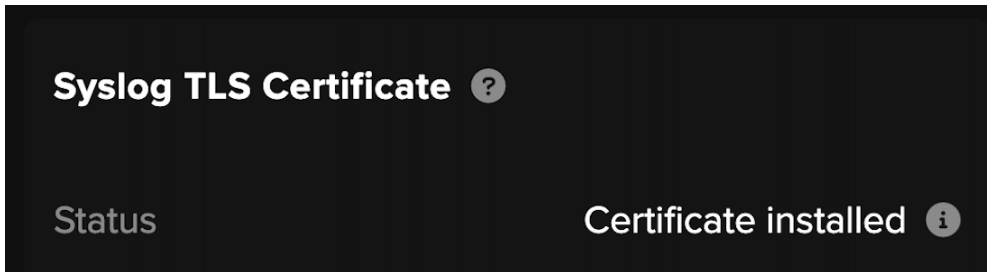
Note: This section only applies to on-premise appliances.

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



2. On the Settings page, use the **search bar** to look up TLS.

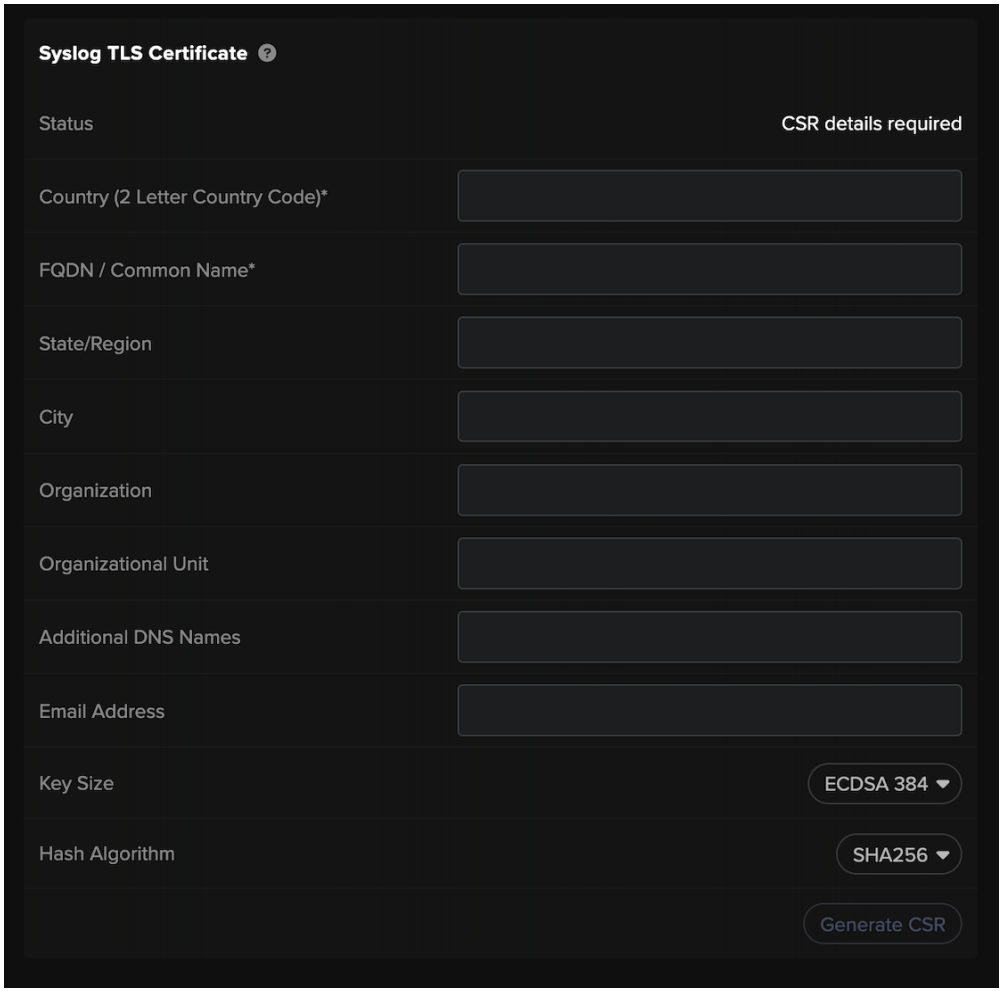
3. Locate the **Syslog TLS Certificate** field. If the certificate is to be changed for a master, probe or vSensor, be sure to select the correct field from the correct subsection.



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

5. 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.

6. With the minimum fields entered, notice the **Generate CSR** button. Click this to generate a CSR which can be exported and signed.



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 it 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.

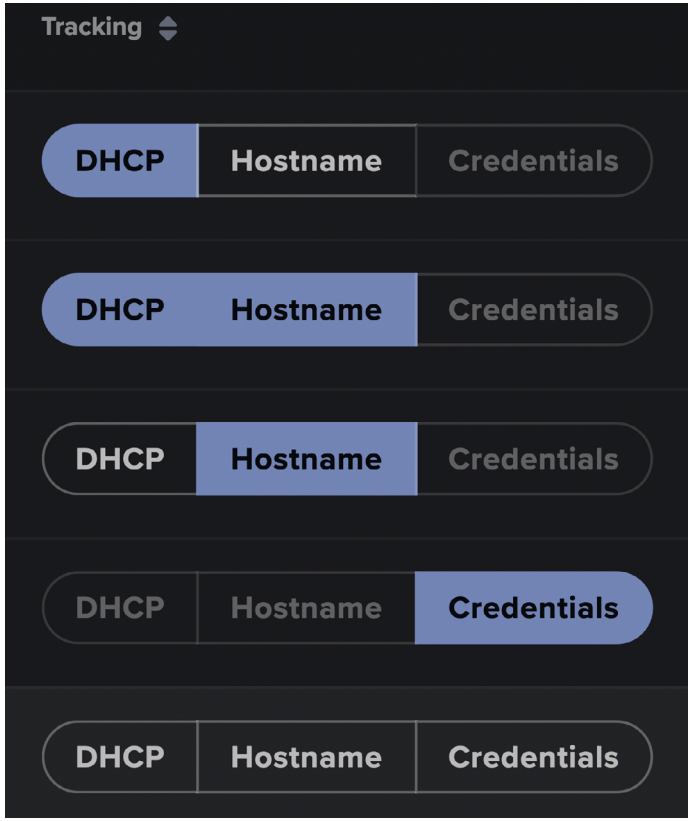
Tracking Summary

The table below is a useful summary of tracking options for the Threat Visualizer and which result can be achieved depending on the options enabled.

DHCP	TRACK HOSTNAMES	TRACK CREDENTIALS	METRIC	RESULT
Yes	No	No	**MAC**	Devices tracked based on MAC address, unless there is no DHCP data for the entire subnet, in which cases it will failover and track based on hostname using **Kerberos/DNS data.**
Yes	**Yes**	No	**Hostname**	Devices tracked based on hostname, using the hostnames in DHCP data, unless there is no DHCP data for the entire subnet, in which cases it will use **Kerberos/DNS data**.
No	**Yes**	No	**Hostname**	Devices tracked based on hostname using **Kerberos/ DNS data**.
No	No	**Yes**	**Username**	Devices tracked based on username using **Kerberos/ NTLM/Radius data**.
No	No	No	**IP**	Tracking disabled. Device objects will be modelled on all data to/from their IP.

Subnet Admin Settings

Combinations of these three tracking settings, DHCP, Hostname and Credential, can be changed via the Subnet Admin page, as outlined earlier.



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

Device Tracking Chapter Test

DARKTRACE
Cyber Engineer Certification

This page will test your knowledge and check your understanding of the Device Tracking section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. What information is necessary for Darktrace tracking?

- [ ] The device's assigned IP address
- [ ] The device's assigned MAC address
- [ ] Both the device's assigned IP and MAC addresses

2. How many servers can be entered as a maximum in the Active DNS Resolution Servers field?

- [ ] 5
- [ ] 10
- [ ] 15

3. What kind of tracking is best for shift workers sharing the same device?

- [ ] DHCP
- [ ] Hostnames
- [ ] Credentials

4. Which metric is used when tracking is disabled?

- [ ] DHCP
- [ ] IP address
- [ ] MAC address

5. It is possible to configure multiple tracking methods for a subnet.

- [ ] True
- [ ] False

6. What default tracking method is used to reassign Device IPs?

- [ ] DHCP
- [ ] DNS
- [ ] Kerberos

Clear All Answers

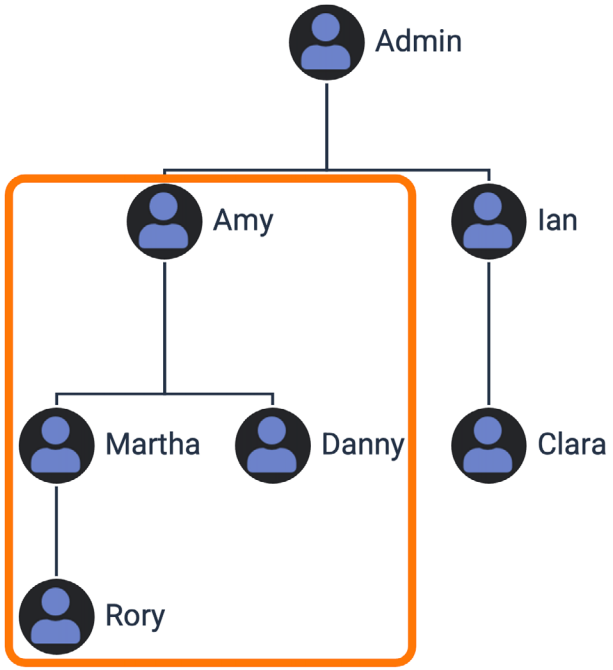
4. User Management

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. Permission administration can be carried out using the Permissions Wizard - let's explore how to use this page in the following chapter.

Permissions Admin

The Permissions Admin is a page where permissions can be set for users of the Threat Visualizer. 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.

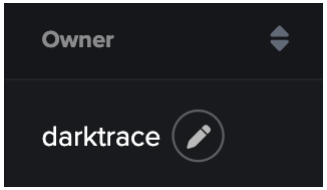


Therefore, Admin can assign permissions to all the users on the right.

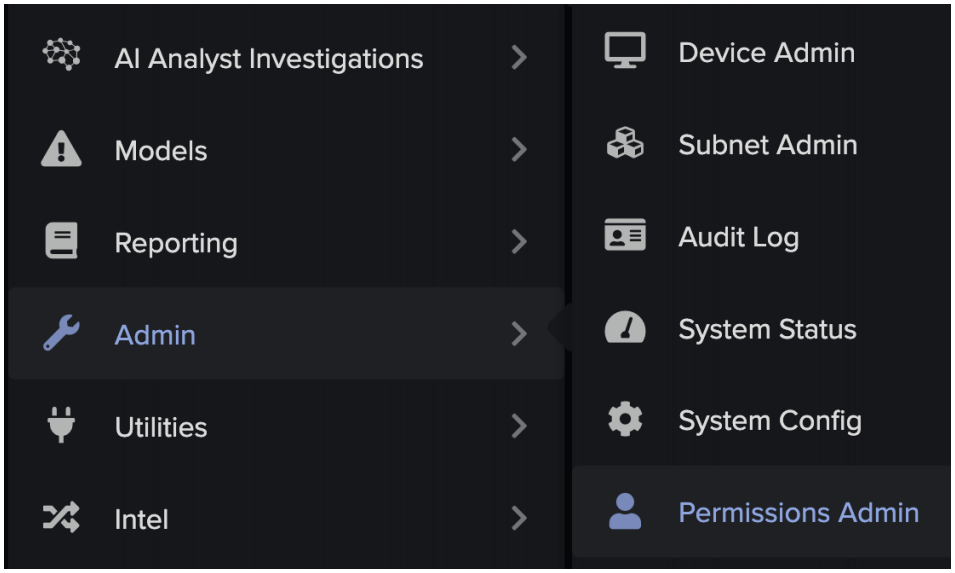
However, if Amy logs in, she will only be able to see and assign permissions to the users highlighted in the orange box. This is because Amy created Martha and Danny's users and Martha created Rory's.

Users are technically "owned" by the user who created them, and it is possible to transfer ownership of users to other users with equivalent or greater access. The user will no longer be visible to the original owner and will only be visible to the new owner. This also applies to any child users they have created. This must be performed by a user who has visibility over both the existing and the desired owner.

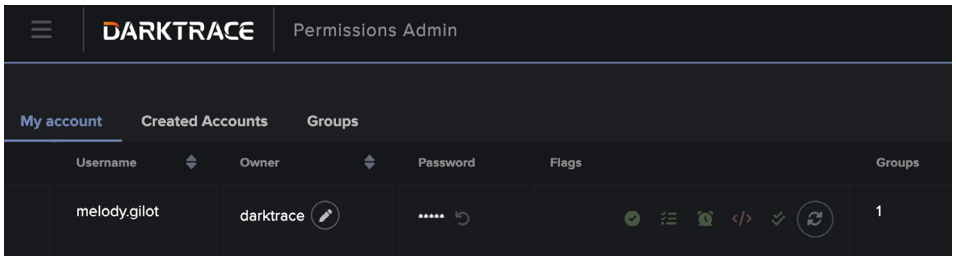
To change the owner of a users, click the **pen icon** beside the name of the owning user in the "owner" column.



1. Within the main menu, navigate down to **Admin** and select **Permissions Admin** from the available options.

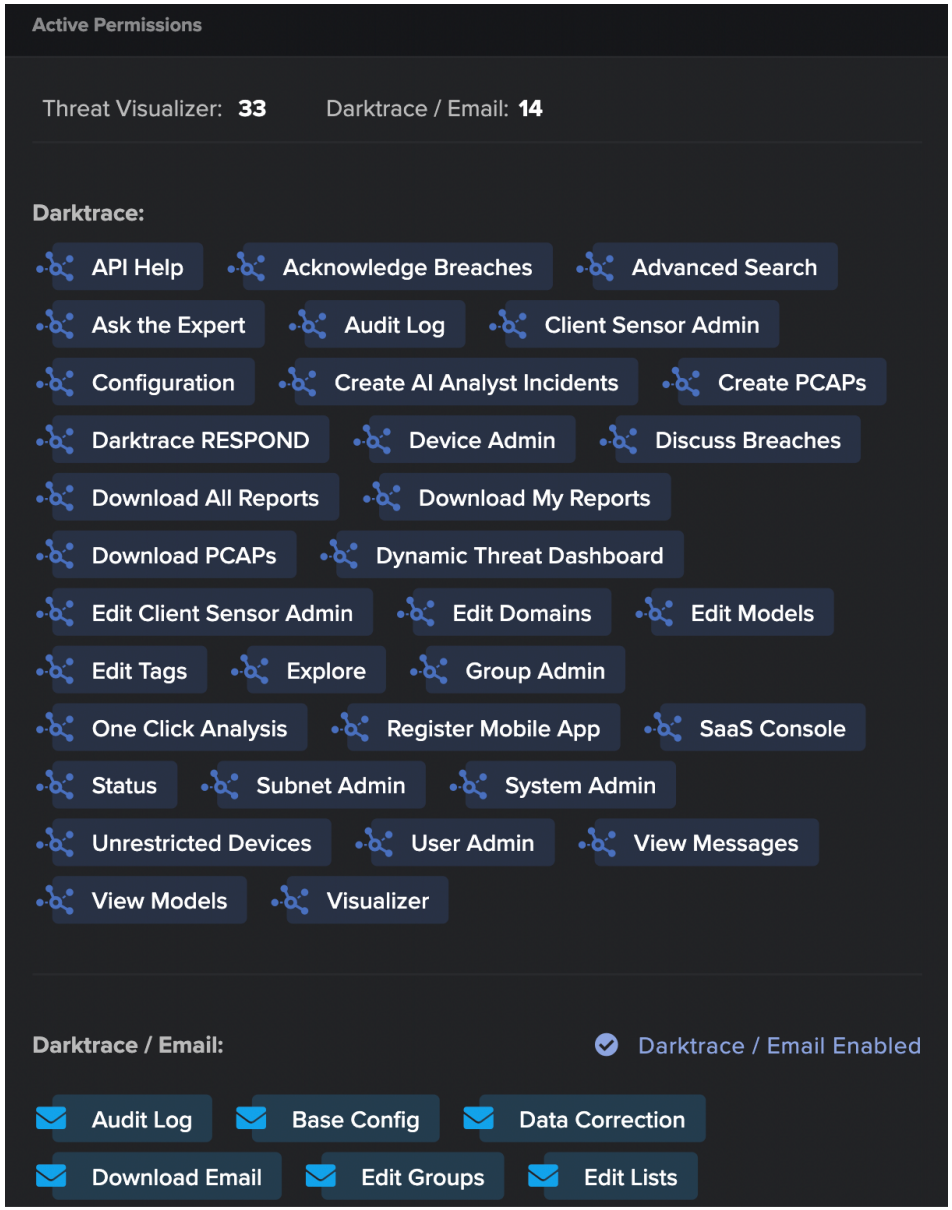


2. Upon opening in a new tab, notice the Permissions Admin displays a **table** of username, owner, password, flags, groups, permissions and Network/ SaaS restrictions (if applicable).

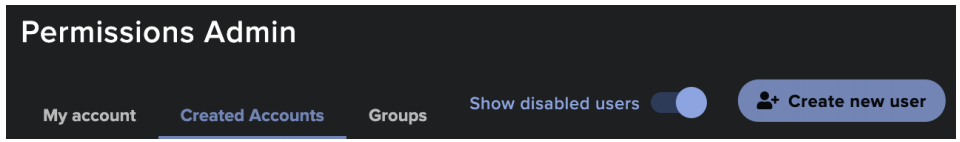


Note: By default, the table will display the account ("My account") of the user who is currently logged in.

The Active Permissions will show a breakdown of Threat Visualizer and Darktrace/Email permissions assigned to the user.



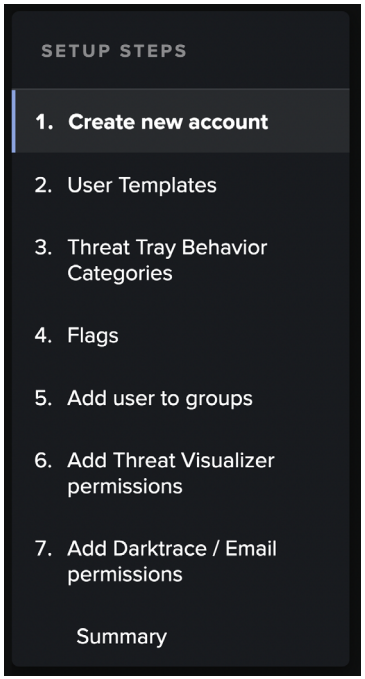
3. As an administrator, it may be desirable to create new users. To do so, navigate to the **Created Accounts** tab and click the **Create new user** button in the top right.



4. Doing so will open a **Permissions Wizard**.

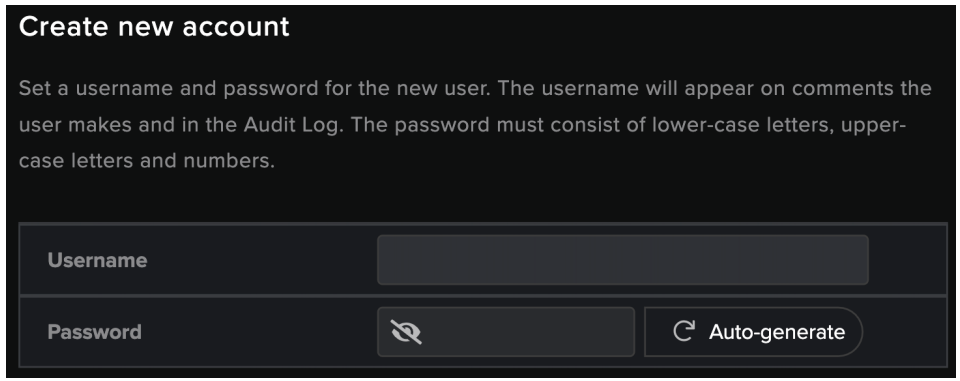
   This will open up a window with a list of setup steps. This walks the creator through setting up a user and applying different types of permissions, either based on suggested job roles, pre-made groups or from scratch.

   For each stage, read the information and fill out the required fields.



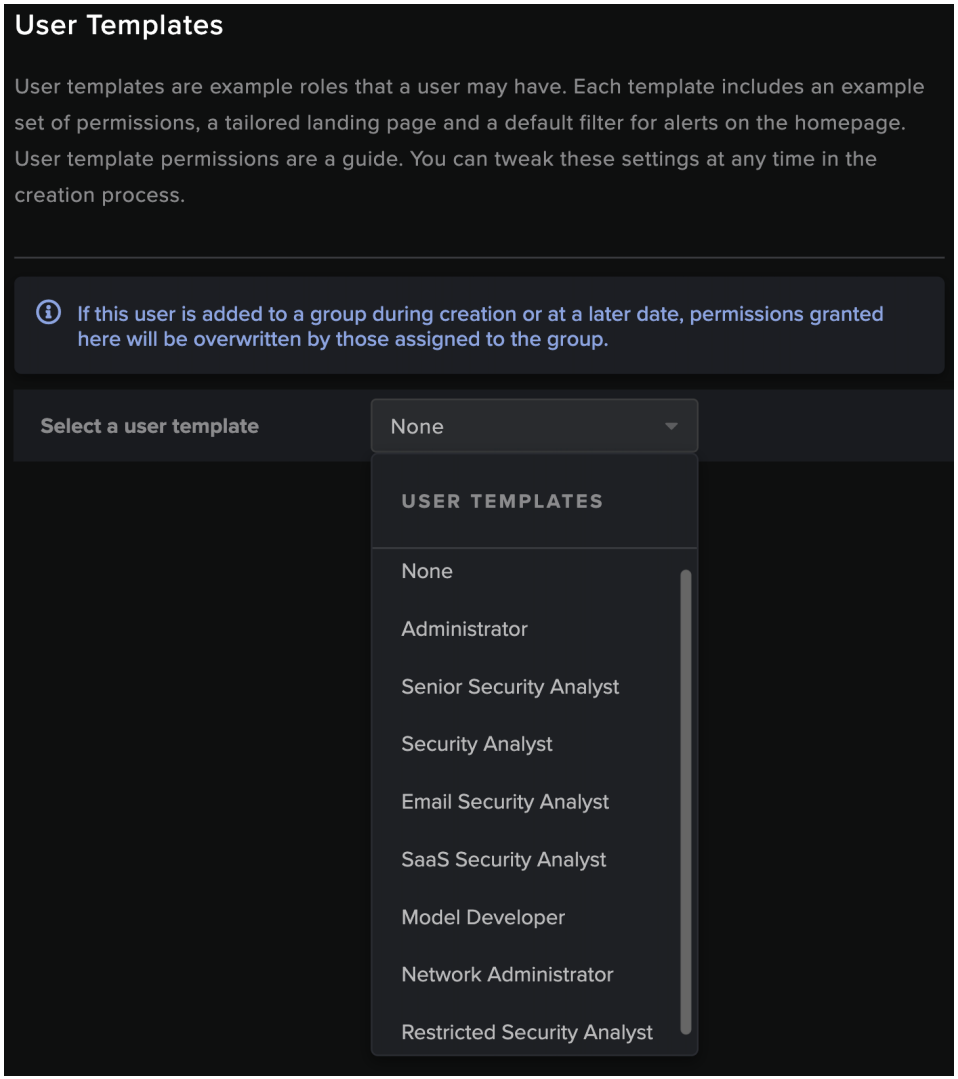
5. First, choose a username for the new user and type this into the **Username** field. This name will appear in the Audit Log.

   Then, create a **Password** containing a mix of lower and upper-case letters and numbers of generate one automatically.

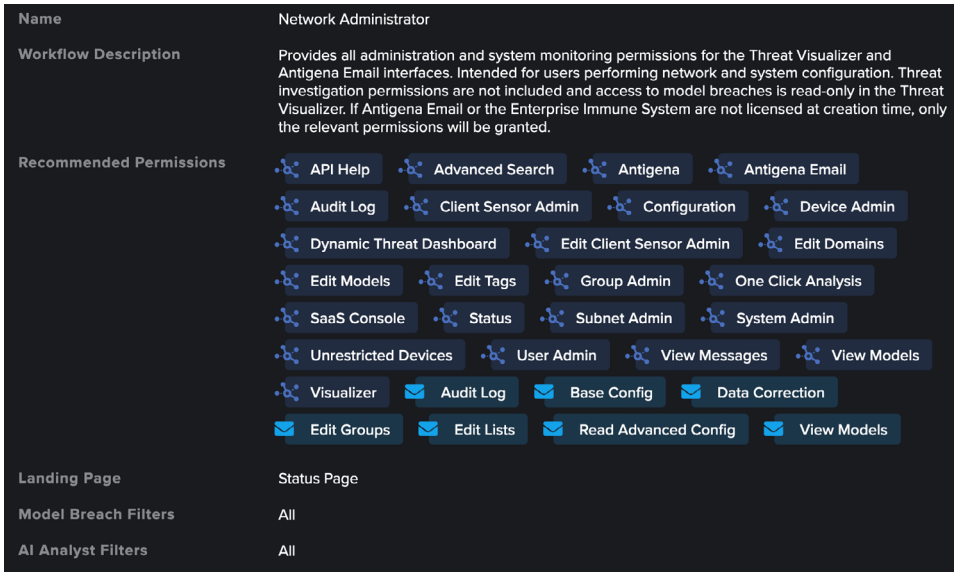


6. Click **User Templates** at the bottom of the page to continue.

7. **User Templates** are an optional feature which allow the creator to select a group of permissions which might suit a job role ranging from Administrators to Security Analysts to Model Developers.



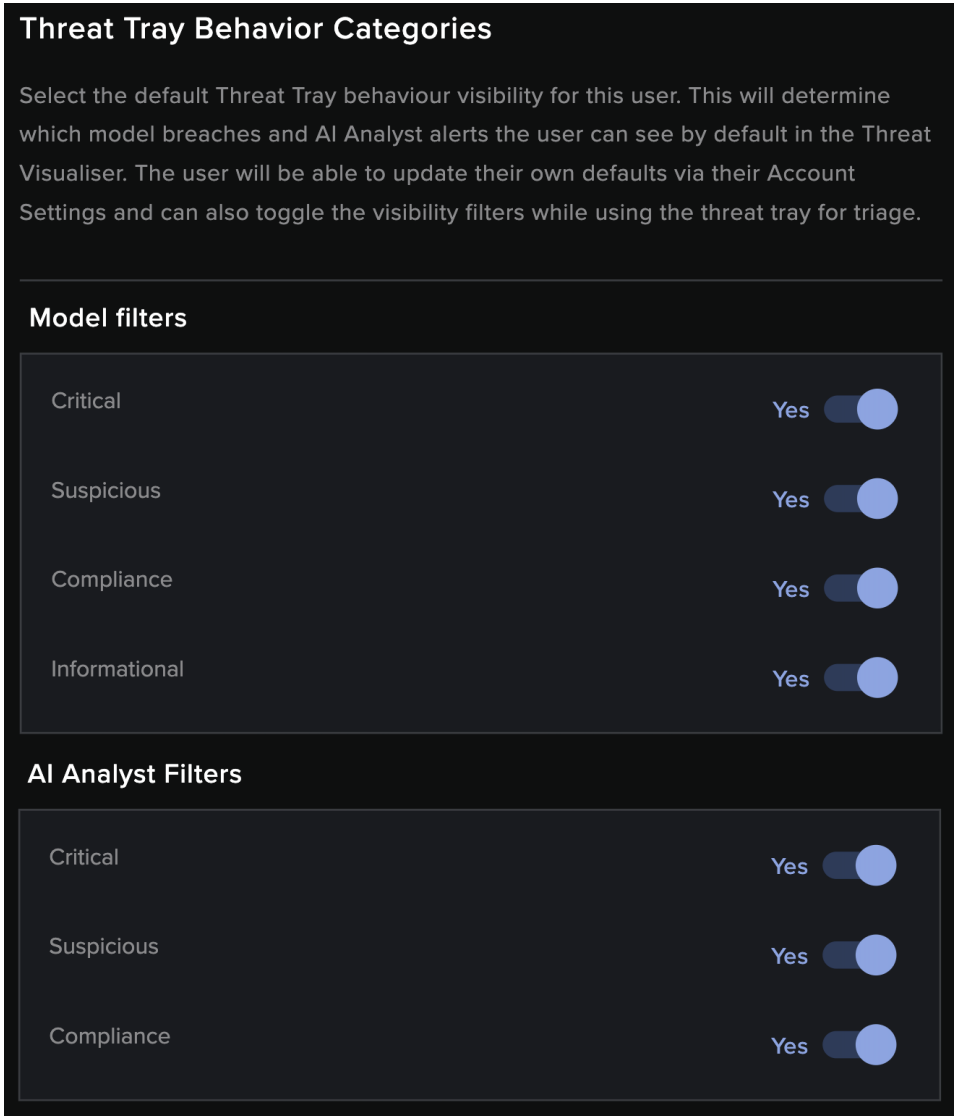
For example, selecting Network Administrator will give a short description of the expected workflow for that role, a list of relevant permissions, the Status page as the landing page opened when logging in and filter visibility.



Note: All User Templates are outlined in a table later in this chapter.

8. Once a template has been selected, if desired, click **Threat Tray Behavior Categories** to move on.

9. Threat Tray Behavior Categories allow the user to determine the **default visibility** a user has over the **Threat Tray** and **AI Analyst Incident Tray**. With all the toggles switched to Yes, the user will have full visibility.



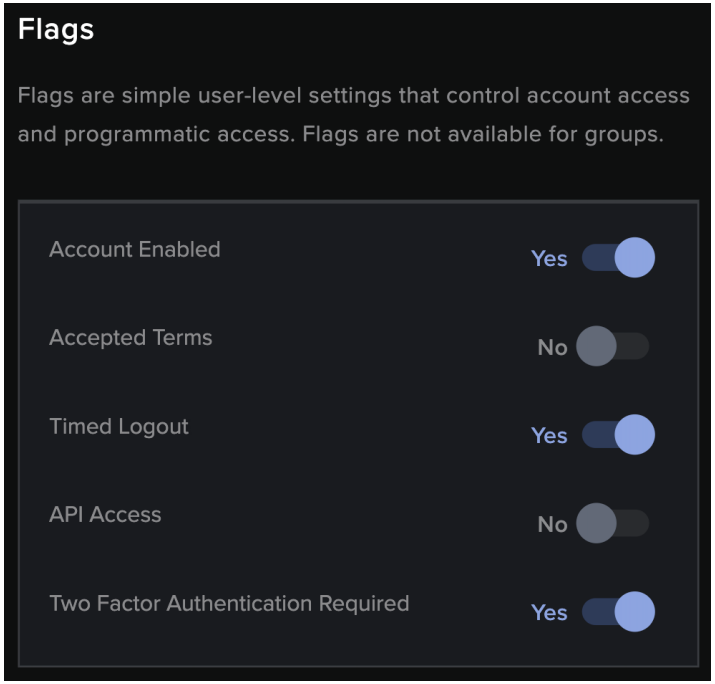
Note: The user is able to update these in their Account Settings, but this method can streamline the triage process when initially logging in.

10. Once the desirable default behavior has been set, click **Flags** in the bottom right to open the next step.

11. **Flags** are applied to individual users to determine account access and security.

    When creating a new account, it will need to be **enabled** for a user to log in.

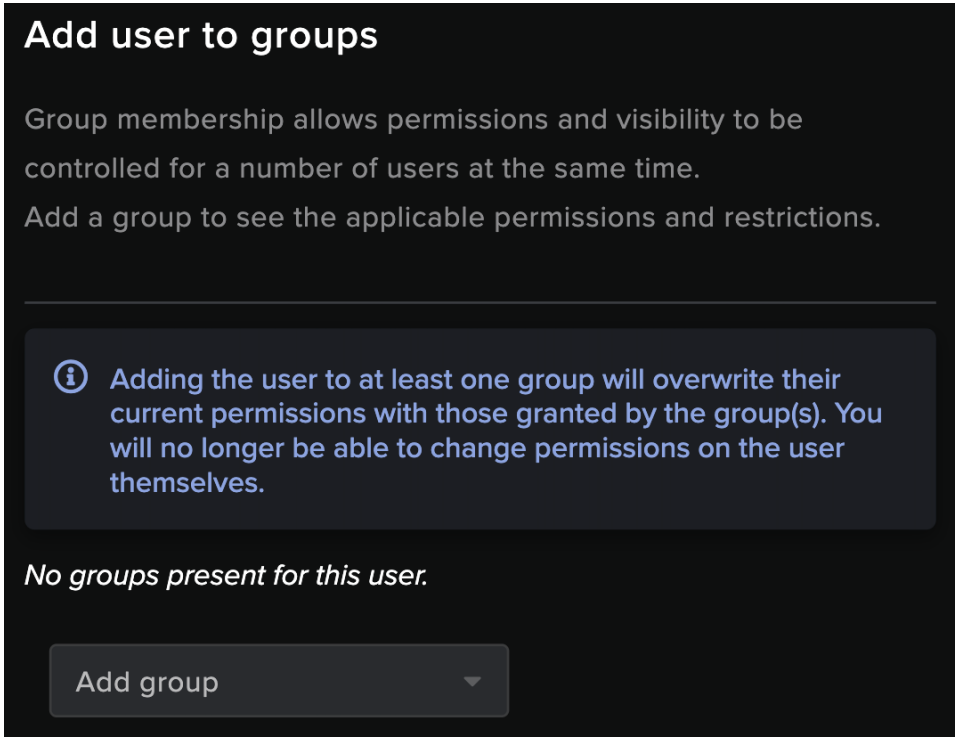
    To ensure a user accepts the terms of use when logging in for the first time, leave **Accepted Terms** off.



Other features such as **timed logout**, **API access** and **2FA** can be enabled/disabled for security purposes. When a user has been created their enabled/disabled flags will be displayed in green/red respectively.

12. Once flags have been applied to the account, click the **Add user to groups** button to move to the next page.

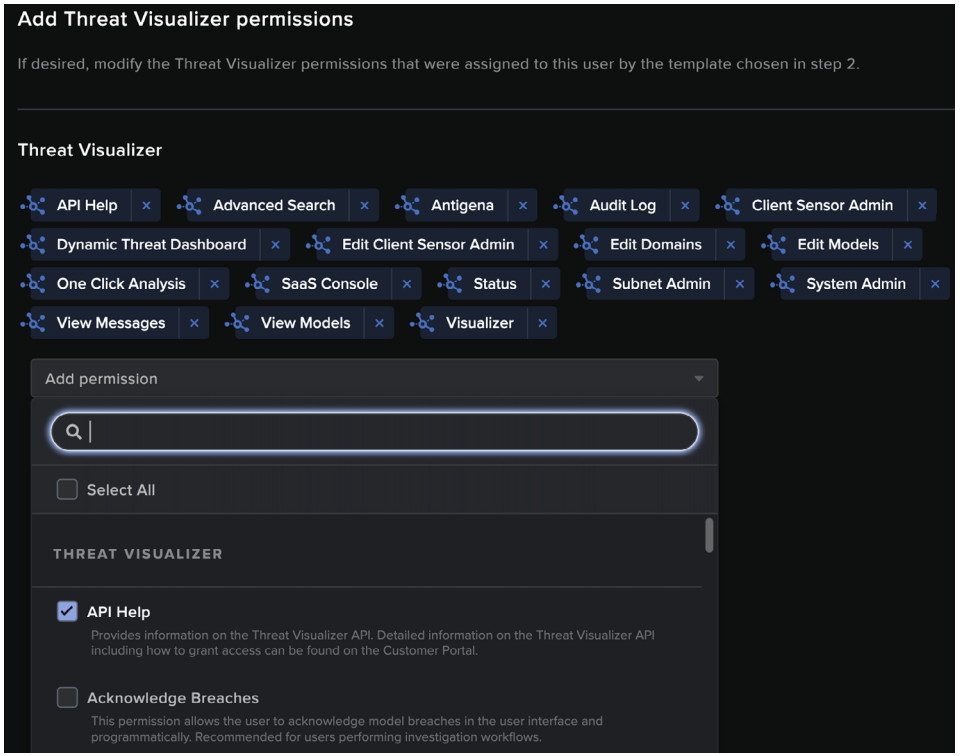
13. This next step allows the creator to add a user to a **group**. Groups are created by Threat Visualizer users rather than Darktrace so can be predefined and used instead of User Templates. Optionally, use the drop-down menu to select an existing group.



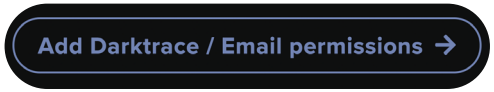
14. To move onto the next step in the set-up process, click **Add Threat Visualizer permissions**.

15. If a User Template has been selected in an earlier stage, some permissions will already be populated on this page. Review the existing permissions.

    They can be removed by clicking the cross beside the name but can also be added/removed by clicking the **check box** beside the permissions in the **Add permission** drop-down menu.

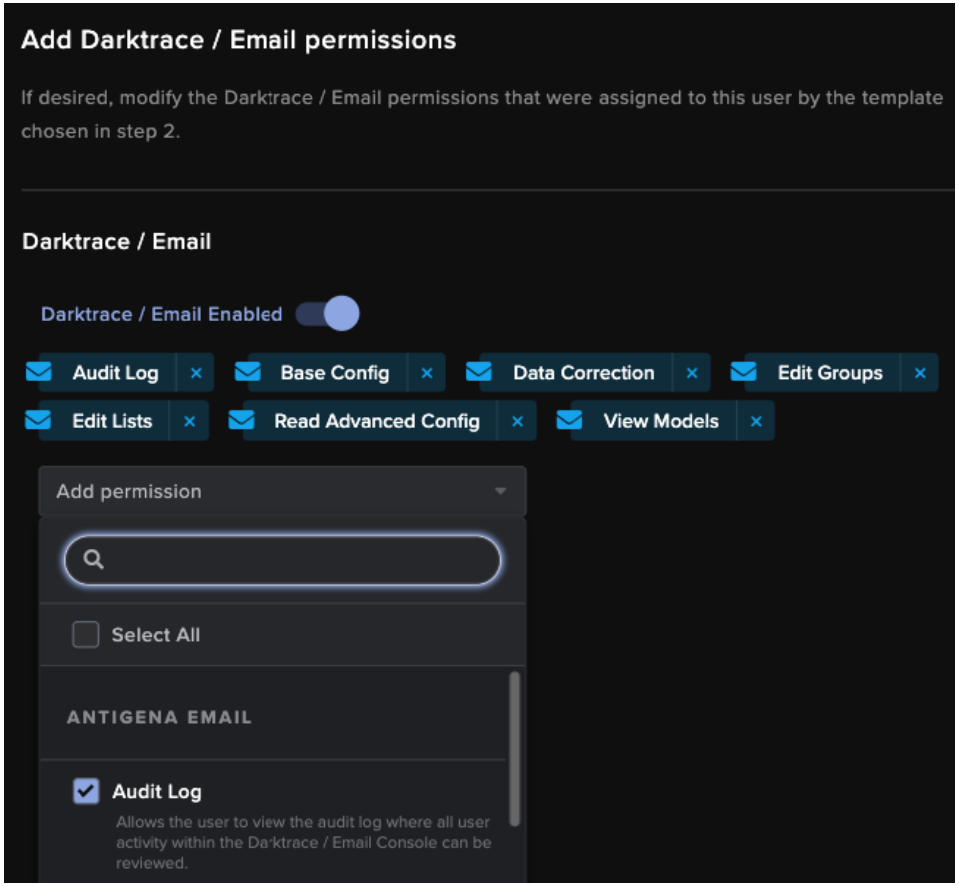


16. Some deployments also have Darktrace/Email. Click the **Add Darktrace/Email permissions** button to review these if relevant.



17. In a similar fashion to the Threat Visualizer permissions, review the **Darktrace/Email permissions**. These may be present due to a template but can be **added or removed** in the same methods as described before.

    Note that the **Access to Darktrace/Email** toggle must be switched **on** for a user to be able to log into Darktrace/Email or have any permissions relevant to that interface.

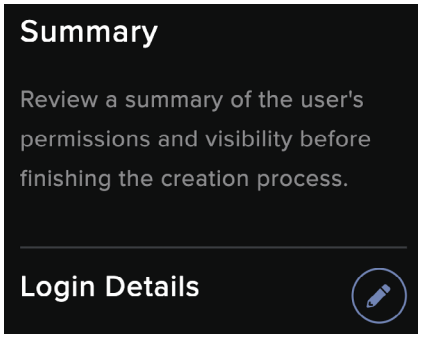


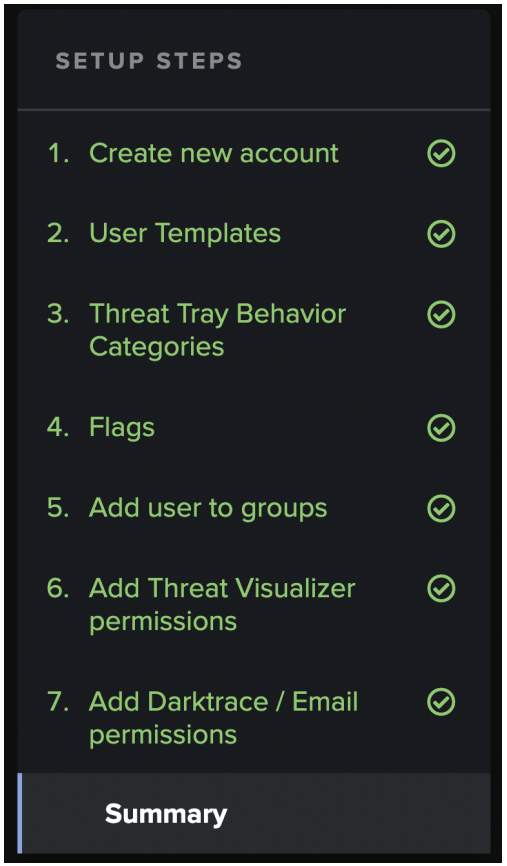
18. Now that all the steps have been followed, click the **Summary** button to navigate to the final page.

19. On the completion of all sections, the **Setup Steps** column on the left of the wizard will show **green ticks** beside each section.

    This page also allows the creator to review each section in one place.

    Beside each heading, a **pencil icon** exists allowing the creator to edit the information for that section. This provides a shortcut to the setup step.

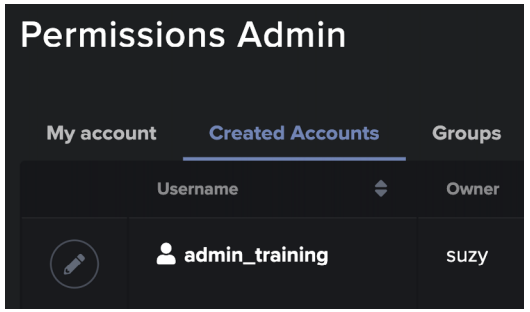




20. Finally, to create the user, click **Create new account** at the bottom of the Summary window.

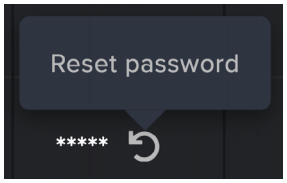
21. Once a user account has been created, it can be found under the **Created Accounts** tab.

    The **owner** can then edit user details in the wizard using the **pencil icon** to the left of the username.



22. Some items can also be edited in the table display:

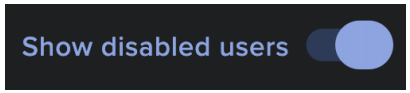
    a. Owners are able to **reset a user's password**.



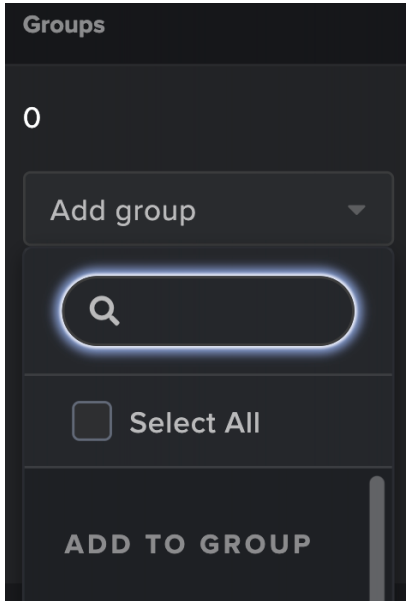
Note: The owner must confirm their own password in a pop up dialog before they can change a user's password.

    b. The **Flags** can be enabled/disabled by clicking the red/green icons.

For example, users can be disabled by clicking the green tick, turning it red. Disabled users can be displayed using the **Show disabled users** toggle at the top of the page.



    c. Users can also be **added to groups** after they have been created.



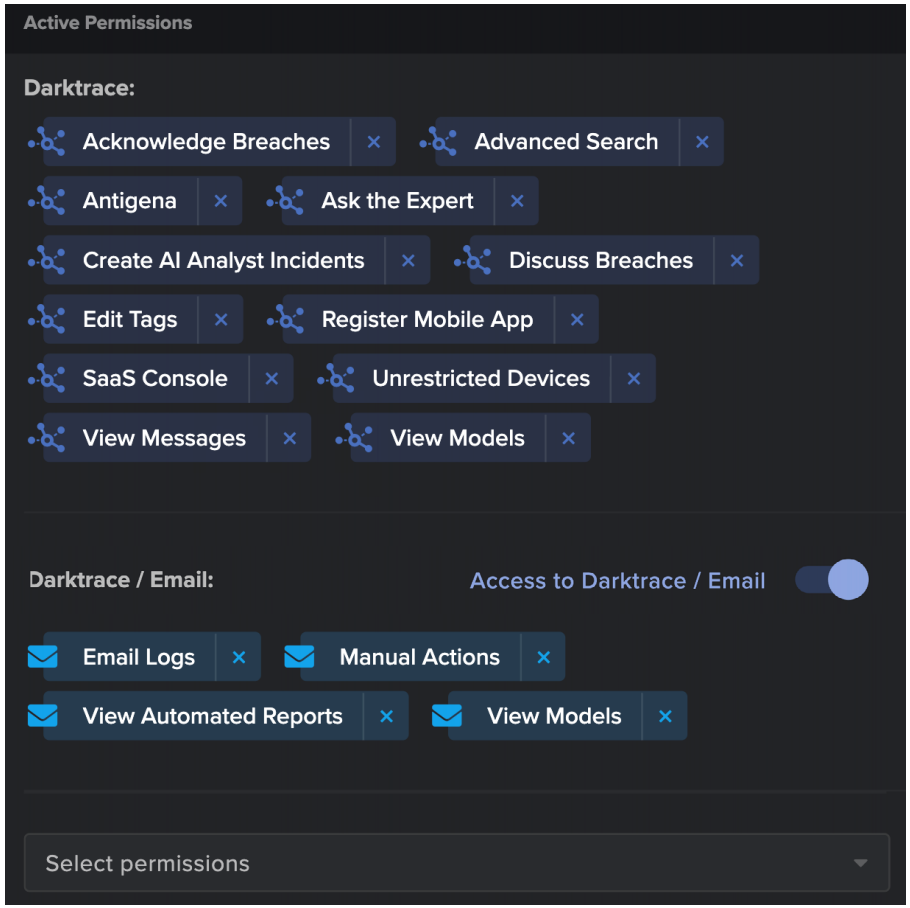
Selecting a group will **remove all existing permissions** and **replace** them with the permissions associated with the selected group.

Any changes made to the groups section will ask the owner to either **save** or **discard** changes.

    d. The **Active Permissions** already assigned to a user can be reviewed by clicking on the row to expand it.

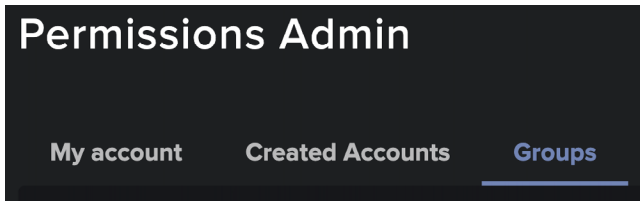
Individual permissions can be **removed** by clicking the **cross** beside the permission name. In a similar way to the permissions wizard, permissions can also be **selected/deselected** using the check boxes in the **Select permissions** drop-down menu. Finally, note that **Darktrace/Email** permissions can be **revoked** by turning off the toggle.

Any permission changes can be **saved** or **discarded**, much like the groups.



Creating Groups

1. To create new or view existing groups, navigating to the **Groups tab** from the Permissions page.



Existing groups each have a row each outlining the assigned permissions.

2. To follow the process of creating a new group, click the **Create new group** button in the top right of the page.

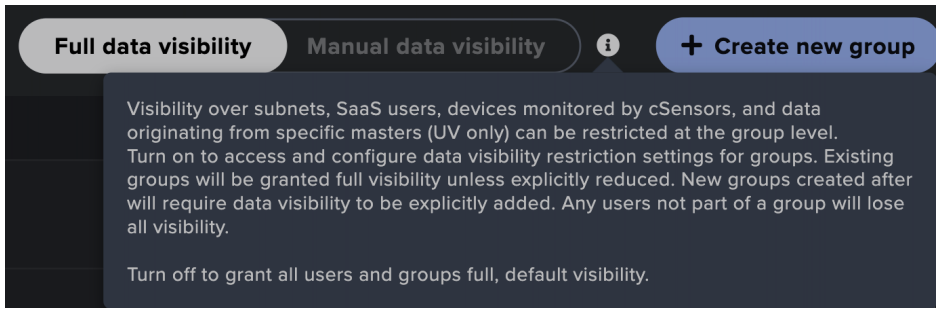
Restricting Data Visibility

The default setting in the Groups tab will allow full data visibility over subnets, cSensor monitored devices and SaaS users.

This setting can be changed to manual data visibility which gives Administrators more granularity over individual group visibility restrictions.

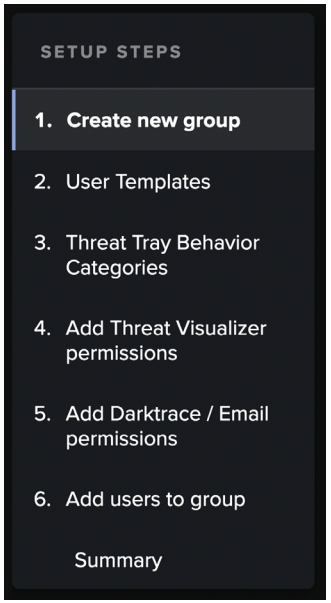
If the setting is changed to manual, existing groups are granted full visibility, but new groups will need visibility to be defined during creation.

Note: Any users who are not part of a group will lose all visibility.

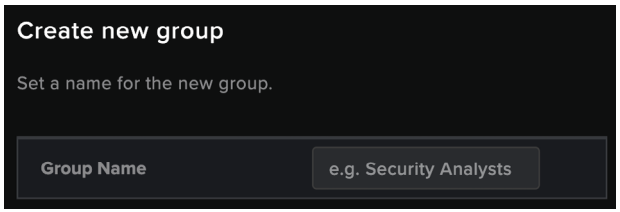


3. As with the new user creation wizard, there is also a **group creation wizard** of a similar format.

This will open a dialog which walks through the steps outlined in the image on the right.

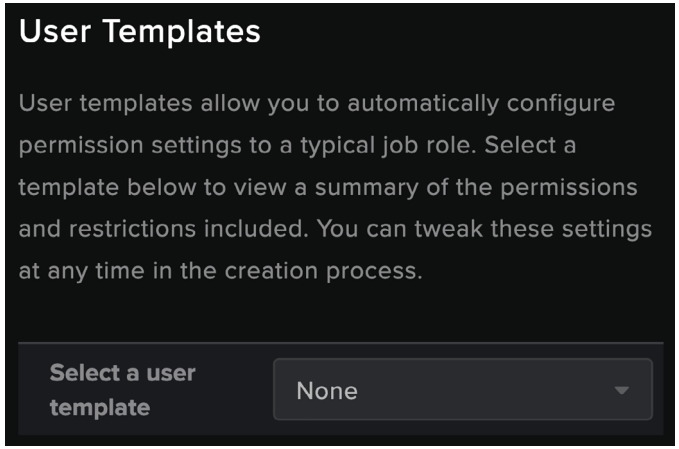


4. First, type a name into the **Group Name** field.



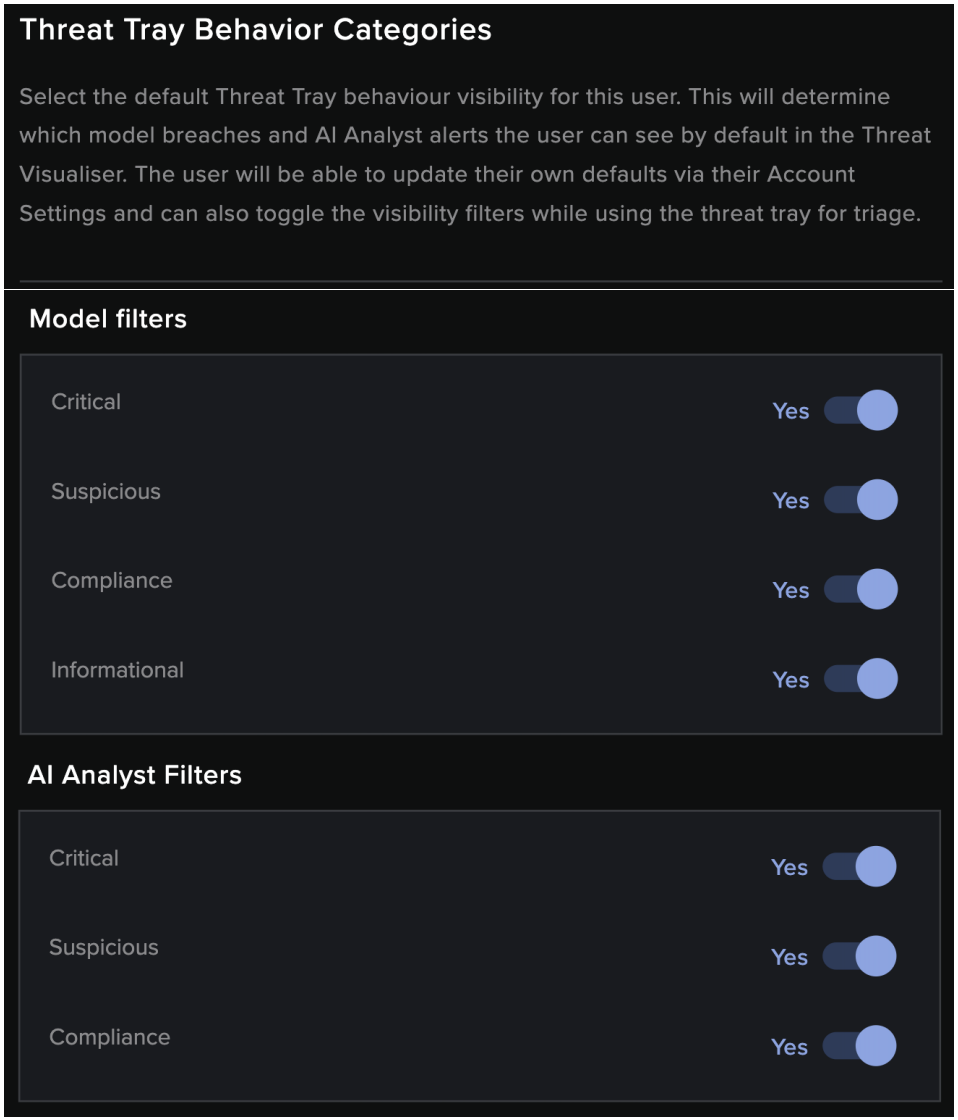
5. Click the **User Templates** button to move to the next page.

6. Groups can be based on pre-existing templates and tweaked to better reflect roles in an organization. Use the drop-down menu to select a **user template**, if necessary.



7. Move onto the next page by selecting **Threat Tray Behavior Categories**.

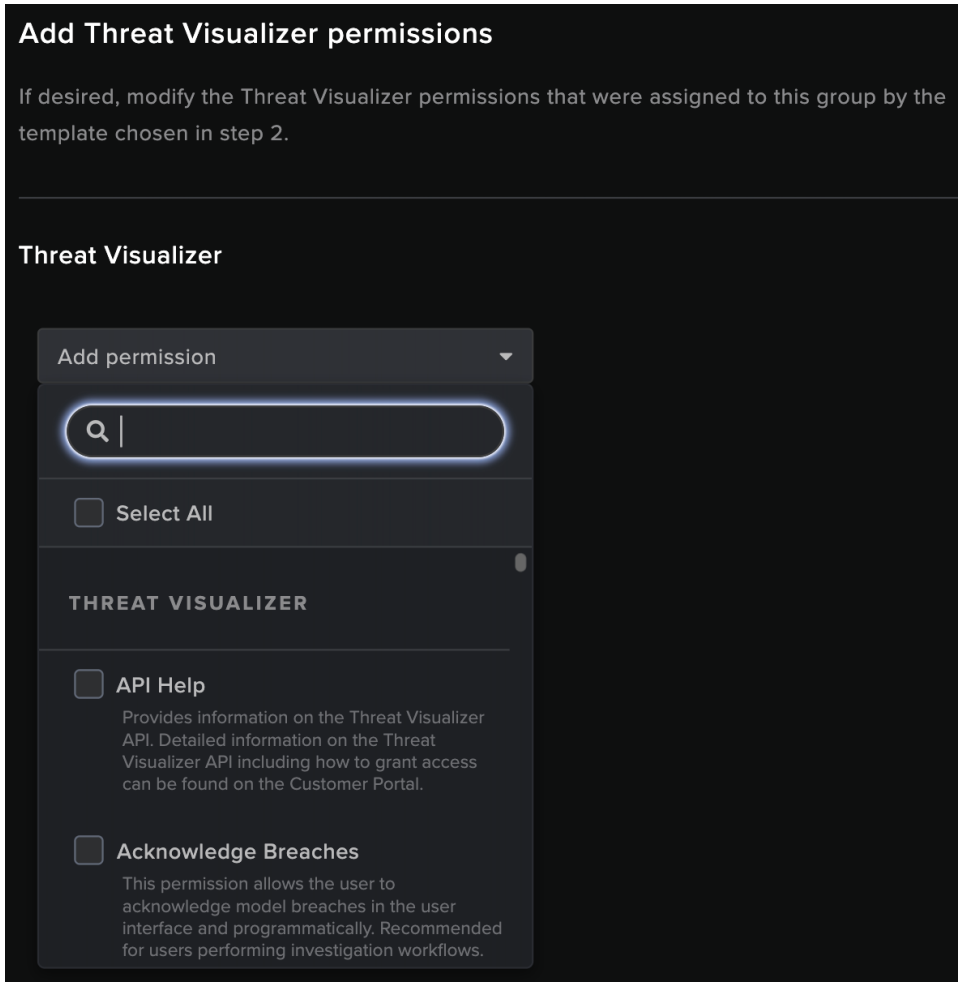
8. In the same way as described in the user setup steps, **Threat Tray Behavior Categories** can be assigned on a group level.



This can be useful to divide up tasks between teams based on the severity of threats highlighted in the interface.

9. Click **Add Threat Visualizer permissions** to move on.

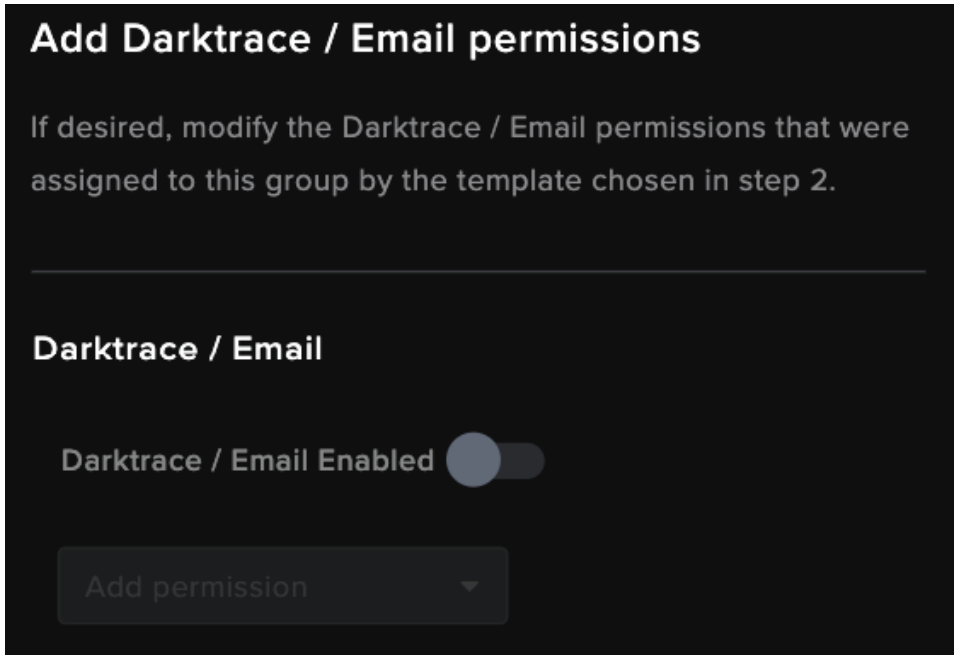
10. Search for or scroll through the permissions and use the **check box** beside any permission that is to be added to the group.



11. Click **Add Darktrace/Email permissions** to move to the next step.

12. Groups can have additional Darktrace/Email permissions if desired.

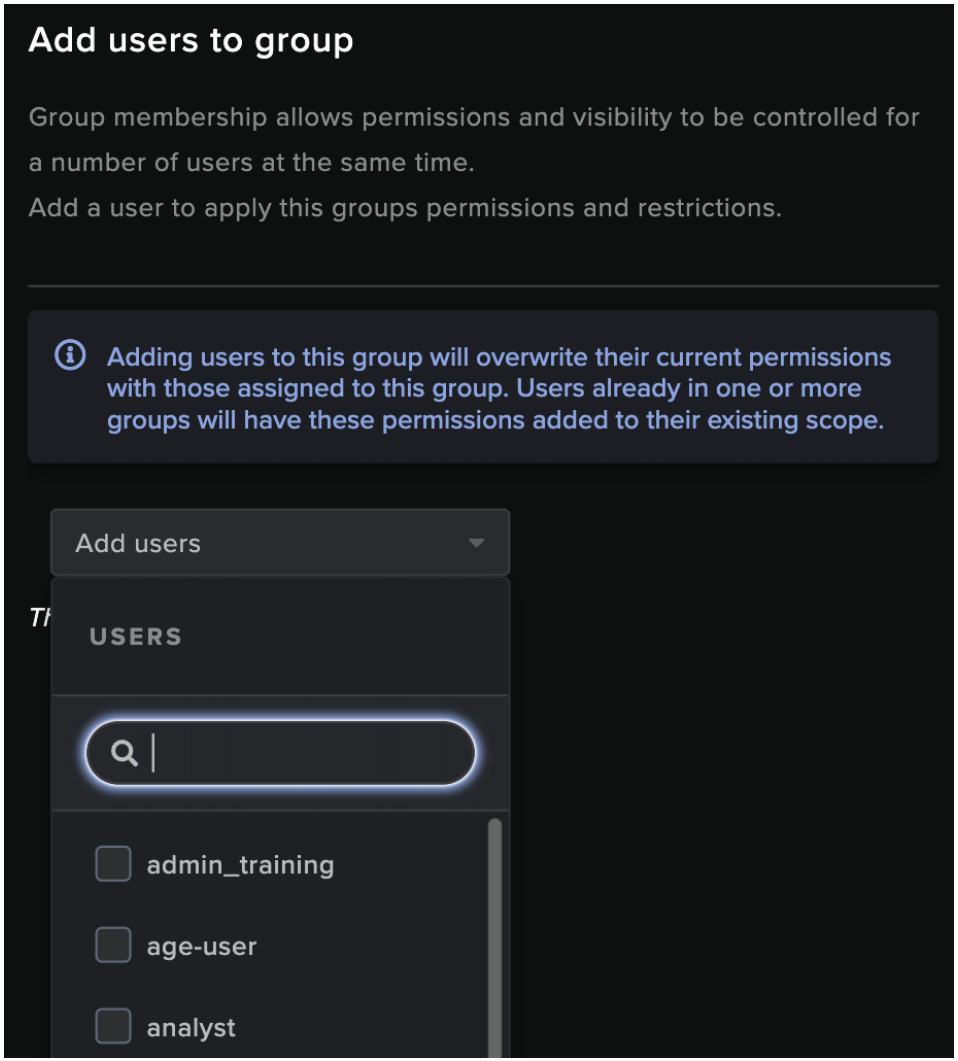
    For an administrator, it might be useful to have oversight over all interfaces.



    As an Darktrace/Email specialist, these might be the only relevant permissions, so make sure the toggle is on so permissions can be selected.

13. To begin applying these configurations to individual users, click **Add users to group**.

14. Rather than applying groups to users in the user creation/editing stage, users can be applied to groups in the group creation phase. Simply search for and add existing users to the group from the **Add users** drop-down menu.



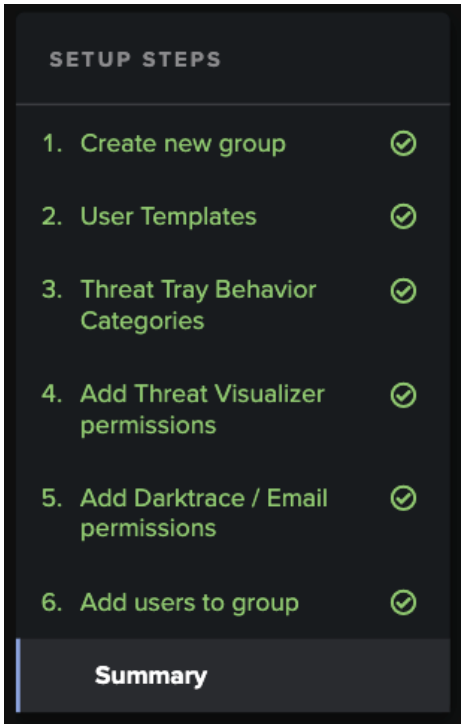
15. Click **Summary** to review the final page of the dialog.

16. With each step complete, review the settings on the **Summary** page.

    Down the left of the dialog, the setup steps should show **completed** items, as depicted by the green coloration and ticks.

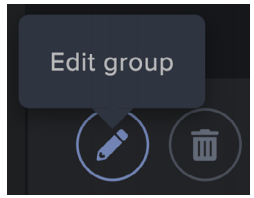
    As with the user creation wizard, any group settings can be edited by clicking the pencil to the right of the heading.

17. Click the **Create new group** to save the settings.



18. New groups will appear on the Groups tab listing the **name**, **number of users**, **permissions** and any **restrictions**.

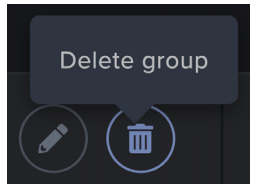
19. Groups can be edited in the same way as users by clicking the **pencil** to the left of the group name.



    This reopens the wizard and allows for navigation through the aforementioned steps.

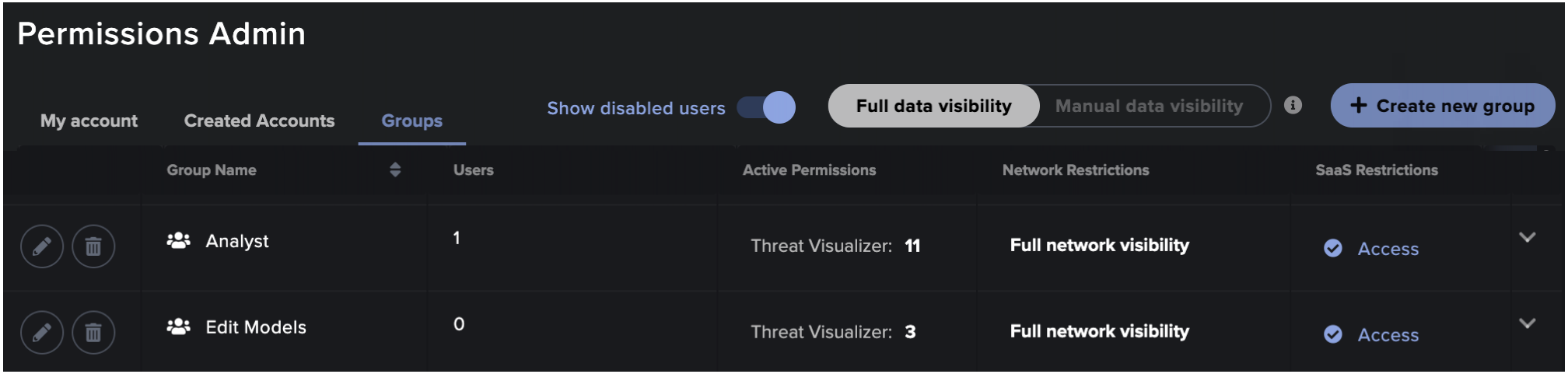
    Furthermore, individual columns can be **edited** and **saved** in table view with the option to discard changes.

20. Unlike users, groups can be **deleted**. This can be achieved by clicking the **trash can icon** to the left of the group name.



Top Tip:

Using user templates as a base, groups can very quickly be created and tweaked to best reflect the different teams in an organization.



Permissions Breakdown

Full permission descriptions can be found in the permissions wizard when creating a user, or by hovering over a permission in a created user row. The following table summarizes all the available Threat Visualizer permissions and provides a short breakdown for each one as well as a recommendation for which level of access the user is expected to have. *Note: Darktrace/Email permissions are outlined in the Darktrace/Email Part 2 - Customization course manual.*

PERMISSION	DESCRIPTION	RECOMMENDED USER
API Help	Provides information on the Threat Visualizer API. Detailed information on the Threat Visualizer API including how to grant access can be found on the Customer Portal.	Admin, Developers
Acknowledge Breaches	This permission allows the user to acknowledge model breaches in the user interface and programmatically. Recommended for users performing investigation workflows.	Admin, End User, Super User
Advanced Search	Grants access to the searchable detailed metadata logs produced by network traffic and event analysis. Key for investigation and is recommended for all users operating without anonymization.	Admin, End User, Super User
Darktrace RESPOND	Allows the user to create and modify active RESPOND actions. One or more valid RESPOND component licenses is required to take actions.	Admin, Super User
Ask the Expert	Ask the Expert allows user to send queries to a Darktrace Cyber Analyst for expert assistance during live threat investigations. This component requires an Ask the Expert license to appear in the Threat Visualizer. Recommended for senior analysts.	Admin, End User, Super User
Audit Log	This permission allows the audit log to be accessed. The log captures user actions like changes to configuration settings, model breach interaction and successful logins. Typically for administrators only.	Admin
Client Sensor Admin	Client Sensor Admin displays the status of current endpoint agents and allows configuration changes to be made. This permission provides read-only access and is recommended for administrator users.	Admin
Configuration	Provides access to view and configure system settings on the System Config page. Typically for administrators only.	Admin
Create AI Analyst Investigations	Allows the user trigger AI Analyst investigations into devices and SaaS users. Recommended for users performing investigation workflows.	Admin, End User, Super User
Create PCAPs	Enables users to create packet captures in the Threat Visualizer. Should be combined with Download PCAPs to retrieve created data. Recommended for users performing investigation workflows who are operating without anonymization.	Admin, Super User

PERMISSION	DESCRIPTION	RECOMMENDED USER
Device Admin	The Device Admin interface allows changes to devices to be made on an individual or bulk basis. Access is granted by the Visualizer permission but configuration changes cannot be made. This permission is required to modify the device label, priority, and type. Typically for administrators only.	Admin
Discuss Breaches	This permission is required to comment on model breaches within the user interface and programmatically. Recommended for users performing investigation workflows.	Admin, End User, Super User
Download All Reports	Provides full visibility over reports generated by all users and automated processes on the 'Download Reports' page. The user must also possess the 'Unrestricted Devices' permission (not operating in an obfuscated mode) to review and generate reports	Admin, Super User
Download My Reports	Provides limited visibility on the 'Download Reports' page to self-generated reports only. Recommended where the user is subject to visibility restrictions that may differ from other users. The user must also possess the 'Unrestricted Devices' permission (not operating in an obfuscated mode) to review and generate reports.	Admin, End User, Super User
Download PCAPs	Allows the user to download created packet captures. Must be combined with Create PCAPs. Recommended for users performing investigation workflows who are operating without anonymization.	Admin, Super User
Dynamic Threat Dashboard	Allows the user access to the Dynamic Threat Dashboard, an alternative threat investigation interface. Recommended for users performing investigation workflows.	Admin, End User, Super User
Edit Client Sensor Admin	This permission provides access to configure agents and change their policy membership on the Client Sensor Admin page. Recommended for administrator users only.	Admin
Edit Domains	This permission controls access to and modification of Intel pages including TAXII Config, Watched Domains and Trusted Domains. These pages list suspicious (Watched) and frequently seen (Trusted) endpoints respectively and are used in modeling. Recommended for senior analysts or system administrators.	Admin, Super User
Edit Models	Allows existing models to be edited or custom models to be created. Required for 'One click defeats' in the Model Breach log. Users must also be granted View Models. Recommended for senior analysts and model developers only.	Admin, Super User
Edit Tags	Tags can be added to devices, SaaS users or models; user with this permission can add, modify or remove tags in a number of interfaces. Tags are used to control Darktrace RESPOND/Network eligibility, therefore, this permission is recommended for more experienced users performing investigation workflows.	Admin, Super User
Explore	Provides access to the Explore functionality that allows playback of communication between Subnets or Tags at a given point. Fixed positions can be provided and set. Recommended for most analysts.	Admin, End User, Super User

PERMISSION	DESCRIPTION	RECOMMENDED USER
Group Admin	Groups allow permission sets and visibility to be controlled for multiple users at once. This permission is required to create and modify groups and group membership on the Permissions Admin page. Typically for administrators only.	Admin
One Click Analysis	Provides a quick view of the model breach to assist in identifying and investigating model breaches. Recommended for users performing investigation workflows.	End User, Super User
Register Mobile App	Allows the user to register the Darktrace Threat Visualizer mobile app on their iOS or Android mobile device. Enabling this permission will add the required settings to the user's Account Settings window.	End User, Super User
SaaS Console	Controls access to the SaaS Console, a specialized user interface for investigating SaaS and Cloud activity. Recommended for users performing investigation workflows.	End User, Super User
Status	The System Status page contains detailed information about system health and any active system alerts. This permission grants access to view the interface and interact with or acknowledge System Status alerts. Typically for system administrators only.	Admin, Super User
Subnet Admin	Allows access to Subnet Admin, an interface where subnets are listed and changes can be made to their configuration. Typically for administrators only.	Admin
System Admin	Permits the user access to administrative features also available within the console application. Please note, some administrative features may not be available due to deployment type. Recommended for system administrators only.	Admin
Unrestricted Devices	Users without this permission will operate in an anonymized mode where credential and client device information is obfuscated. Access to Device Admin is removed and Executive Threat Reports cannot be generated. It is recommended this permission is granted to almost all users unless anonymization is desired.	Admin, End User, Super User
User Admin	Allows the user access to create and edit user accounts on the Permissions Admin page. Users can only edit users they have created (or child accounts of those users) and add permissions equal to or less than their current permission scope. Typically for administrators only.	Admin
View Messages	Allows the user to view system messages on login (such as reboot notifications) and those sent by Darktrace to the instance. Recommended for administrators.	Admin, End User, Super User
View Models	Darktrace models are a logical framework built upon the output of complex anomaly detection. This permission allows read-only access to view and understand model logic. Edit Models is required to make changes.	Admin, End User, Super User
Visualizer	Grants access to the main Threat Visualizer interface and read-only access to Device Admin and the RESPOND Actions window. Users without this permission will not be redirected to the Threat Visualizer on login.	End User, Super User

User Templates

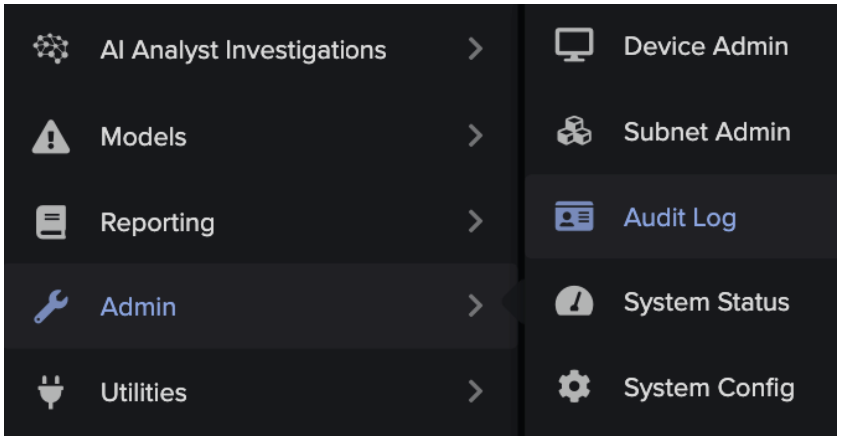
User Templates can form a good foundation for applying permissions to users who may fit under outlined roles. Note that if Darktrace/Email or the Threat Visualizer are not licensed at user creation time, only the relevant permissions will be granted from these templates. Remember, permissions can be manually added after the template stage but templates will be overwritten by groups.

TEMPLATE NAME	WORKFLOW DESCRIPTION	LANDING PAGE	DEFAULT FILTERS
Administrator	Provides all Threat Visualizer and Darktrace/Email permissions granted to the default "admin" user.	Threat Visualizer	All
Senior Security Analyst	Includes all required permissions to perform threat investigation workflows and higher-level privileges to modify and retrieve data in the Threat Visualizer and Darktrace/Email interfaces. Users with this template can activate or clear RESPOND actions.	Threat Visualizer	Critical Suspicious
Security Analyst	Includes all required permissions to perform threat investigation workflows. Users with this template can activate or clear RESPOND actions.	Threat Visualizer	Critical Suspicious
Email Security Analyst	Includes all required permissions to perform threat investigation workflows in the SaaS and Darktrace/Email Consoles. The Email console will be set as the default landing page and access to the main Threat Visualizer interface is not available. Users with this template can activate or clear RESPOND actions.	Email Console	Critical Suspicious
SaaS Security Analyst	Includes all required permissions to perform threat investigation workflows in the SaaS Console and Darktrace/Email console. The SaaS Console will be set as the default landing page and access to the main Threat Visualizer interface is not available. Users with this template can activate or clear RESPOND actions.	SaaS Console	Critical Suspicious
Model Developer	Grants privileges to create and edit models in Threat Visualizer and Darktrace/Email interfaces. Permissions to perform threat investigation and interact with model breaches is included to allow users to identify behavior of interest and control models currently under their development. Users with this template can activate or clear RESPOND actions.	Threat Visualizer	All
Network Administrator	Provides all administration and system monitoring permissions for the Threat Visualizer and Darktrace/Email interfaces. Intended for users performing network and system configuration. Threat investigation permissions are not included and access to model breaches is read-only in the Threat Visualizer.	Status Page	All
Restricted Security Analyst	Grants a restricted set of Darktrace Environment permissions that cause users and client devices to be anonymized. It provides limited access to some interfaces and allows interaction with model breaches. Users do not have access to Advanced Search or privileges to change administration settings.	Threat Visualizer	Critical Suspicious

Further Options

Audit Log

Once a user has been created, the Audit Log will capture the user's actions such as changes to configuration settings, model breach interaction and successful logins.

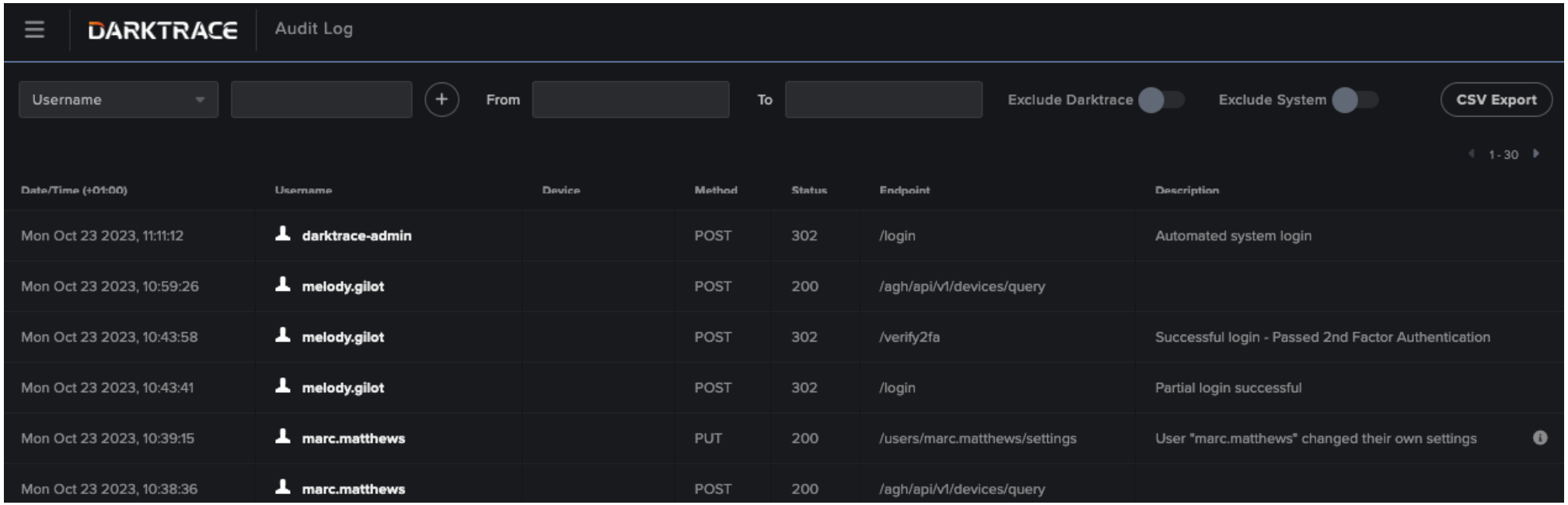


1. Click **Admin** and then **Audit Log** from the Threat Visualizer main menu.

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. The **method**, **status** and **description** of each event is also tabulated.

   Along the top of the table, filter options are available for reducing the number of events presented on screen at any time. The results can be paged through using arrows in the top right of the screen.



a. Notice the **username icon** for each event.

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

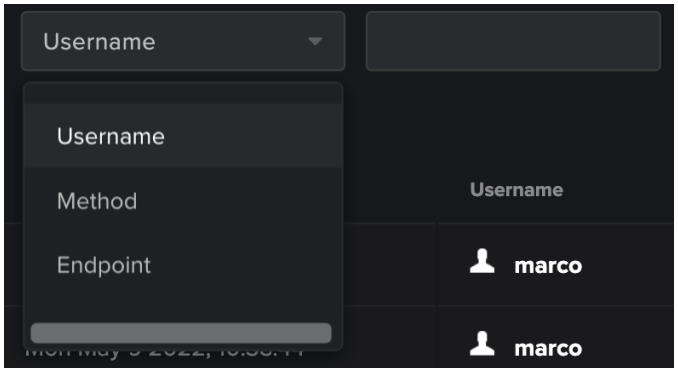
ii. The **monitor** icon is related to command line or SSH access, e.g. when a user uses the console app.

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.

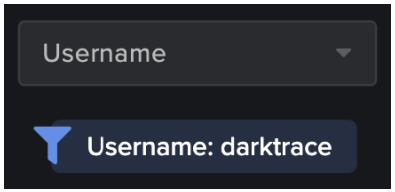
3. The **search bar** at the top of the page can restrict results to individual **users**, **methods** or **endpoints**.

Note: The user interacts with the UI via four available HTTP Methods: PUT, GET, POST or DELETE. These actions occur with respect to the results displayed in the Endpoint column.

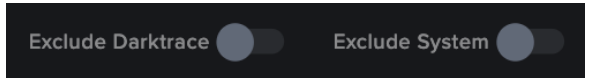


a. Select a mechanism to restrict results, type in the search bar and press the **plus icon** to the right of the search bar to filter the Audit Log.

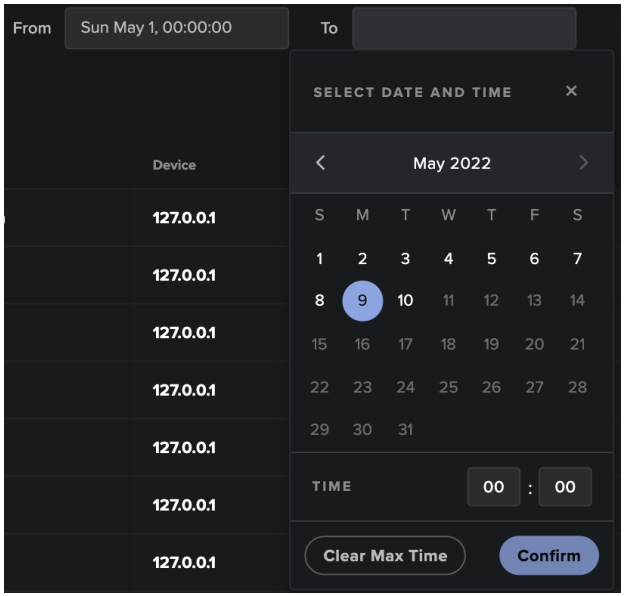
b. Applied filters will appear under the search bar in blue. To remove a filter, **click it**.



4. To **exclude Darktrace** or **System** events from the Audit Log results, use the **toggles** at the top of the page.



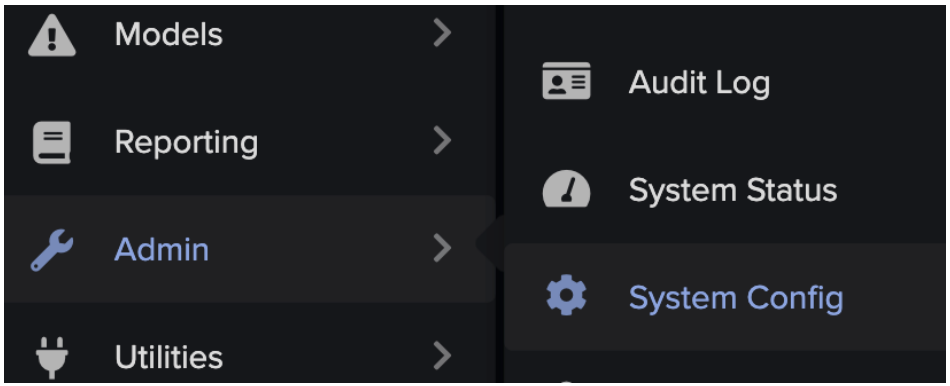
5. Checking accesses to the Threat Visualizer can be done by **time frame**. Click the **From** and **To** time selectors, remembering to click on the Confirm buttons when selecting the date / time ranges.



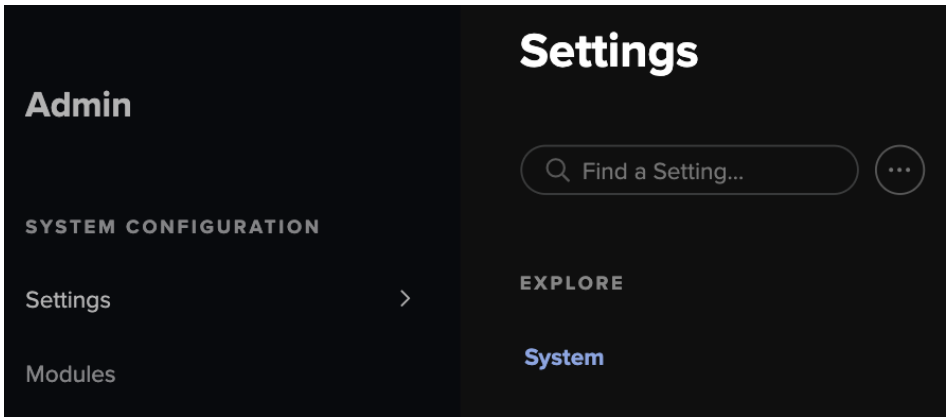
6. It is also possible to export the selected elements in a CSV file format by clicking on the **CSV Export** in the top right of the page.

Session Expiry

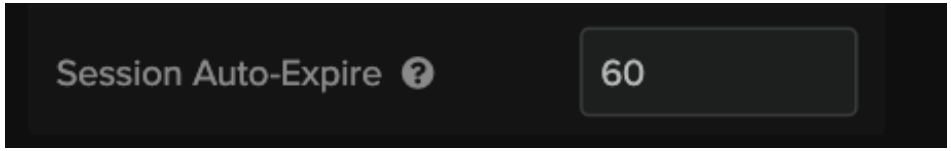
1. Users with the "System Administration" permission can modify the default session length by accessing the **System Config** page from the main menu, under Admin.



2. From the left-hand side, choose the field **Settings > System.**



3. Input the desired **Session Auto-Expire** duration in its dedicated field. By default, it is 60 minutes.



User Management Chapter Test

DARKTRACE
Cyber Engineer Certification

This page will test your knowledge and check your understanding of the User Management section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. Which of the following is NOT an AI Analyst Filter?

- [ ] Critical
- [ ] Suspicious
- [ ] Informational

2. Users part of the same group can have different permissions.

- [ ] True
- [ ] False

3. Which of the following permissions provides detailed information about the system's health?

- [ ] Device Admin
- [ ] Subnet Admin
- [ ] Status

4. Which user template is recommended to conduct threat investigation workflows?

- [ ] Administrator
- [ ] Security Analyst
- [ ] Network Administrator

5. Account owners CANNOT be changed.

- [ ] True
- [ ] False

6. Which icon appears on the Audit Log when a Darktrace user logs in ?



- [ ]
- [ ]
- [ ]

Clear All Answers

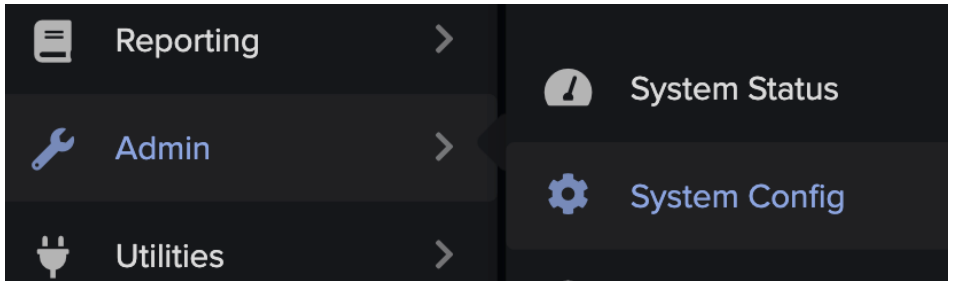
5. Configuring Darktrace Settings

Again, within the System Config page, there are many configurable elements. However, this chapter outlines configurable elements 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 so make sure to utilize the search bar at the top of the System Config page to make workflows easier to carry out.

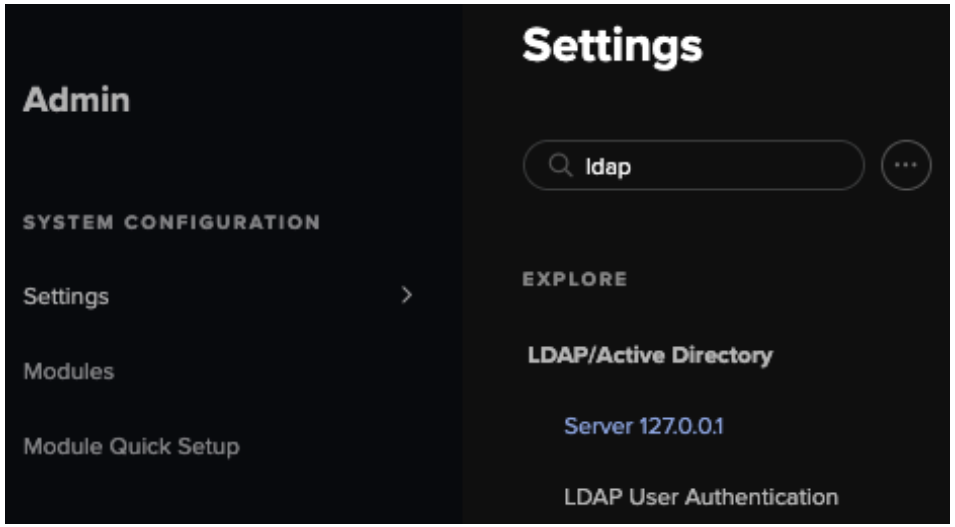
LDAP Configuration

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.

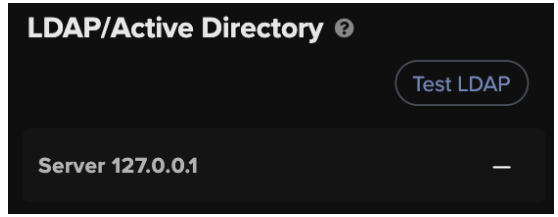
1. From the main menu, navigate down **Admin** and locate the **System Config** option. This will open the System Config page in a new tab.



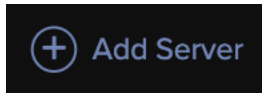
2. With the Settings submenu selected, scroll down to locate the **LDAP/ Active Directory** section.



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.

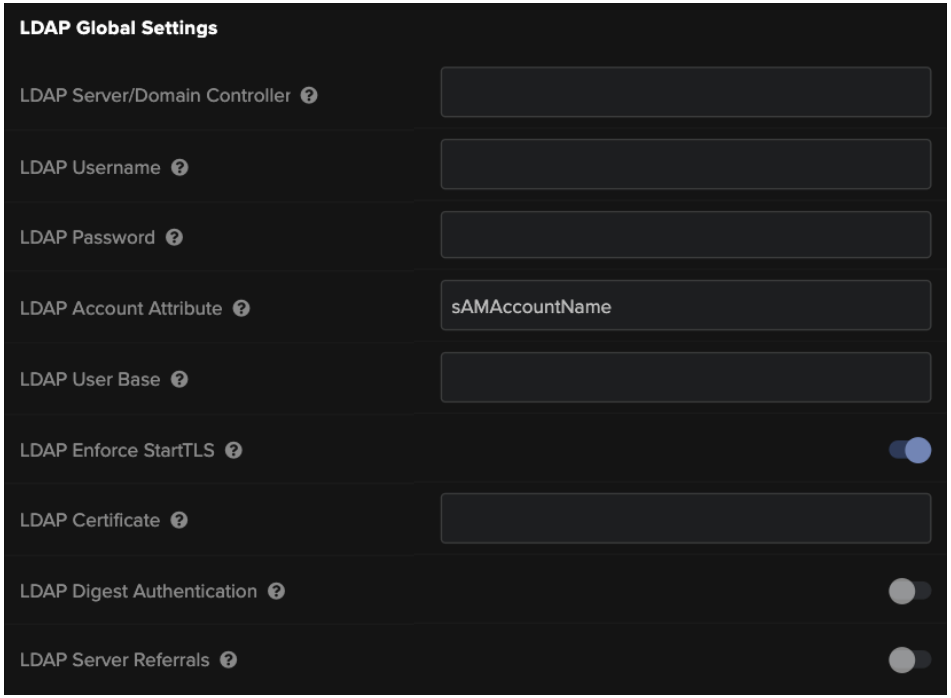


4. To configure a new server, click **Add Server** to open up a new dialog containing a range of fields to be filled out.



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.

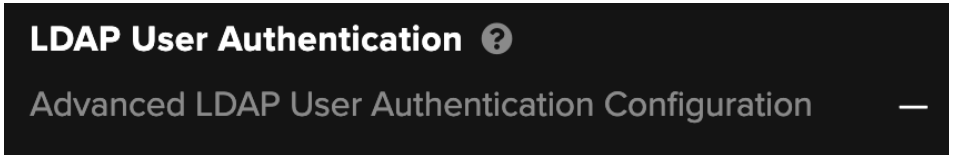
If LDAPS has been configured in the LDAP Server/Domain Controller field, LDAP Enforce StartTLS must be disabled. If not, the **LDAP Enforce StartTLS** can be enabled using the toggle.

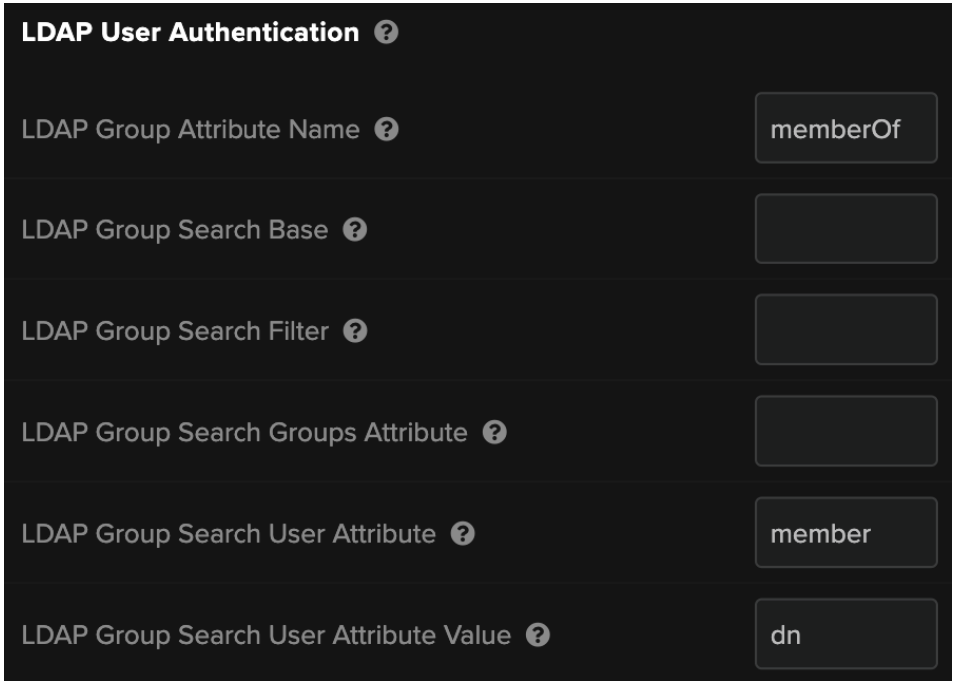
g. An **LDAP Certificate** is optional for both forms of encryption. Omitting a value disables certificate validation.

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.

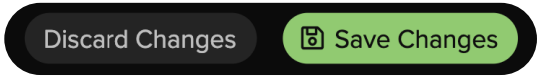




Note: Advanced Settings are typically not required for standard Active Directory deployments.

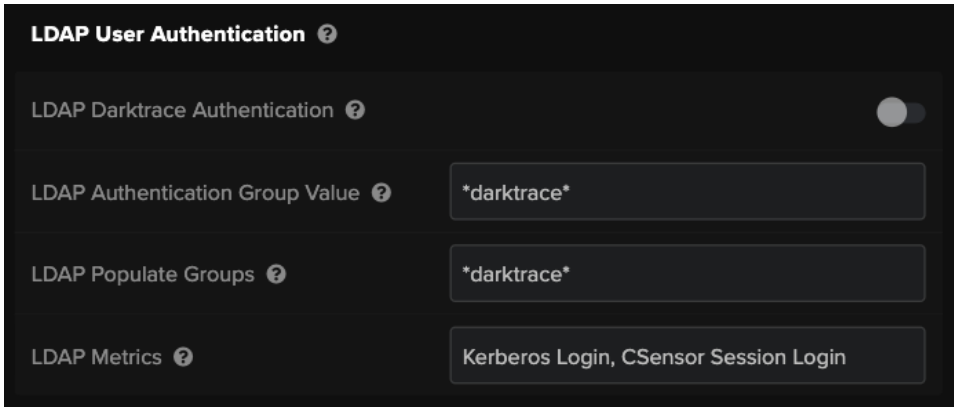
7. Again, **fill out the appropriate values**. Some of the fields have **pre-populated default values**. Use the tooltips next to each field if you choose to modify any of them.

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.

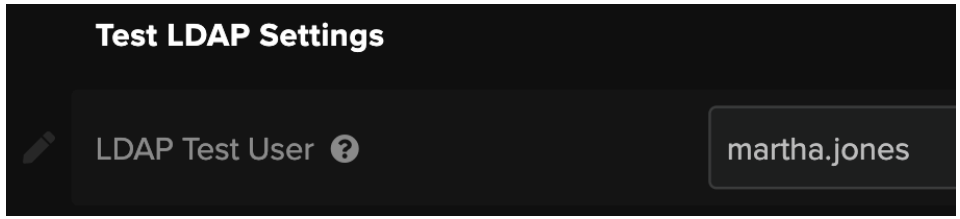
b. Use the optional **LDAP Authentication Group Value** field to restrict usage of LDAP authentication for logging into Darktrace to specific groups. This field is not case sensitive and will also support wildcards.

c. The **LDAP Populate Groups** field can retrieve and present groups in the Permissions 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.

Note: When logging into the interface for the first time after LDAP is enabled, navigate to Permissions 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. The **LDAP Metrics** field should be visible. Enter metrics, separated by commas, to be sent to LDAP in order to enrich credentials.

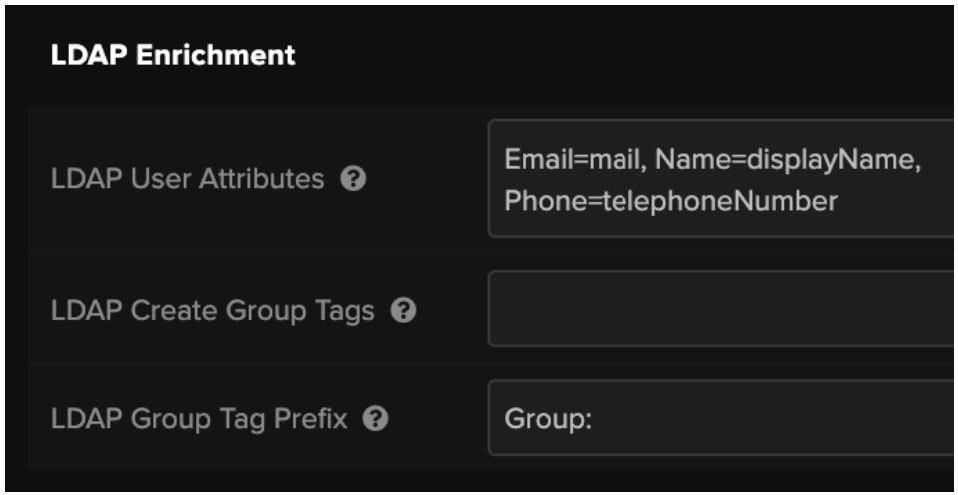
11. Before changing any of the LDAP User Attributes values in the next section from their default, set a valid and identifiable **LDAP Test User**, as seen in the Threat Visualizer.



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 in the bottom right of the page. Unencrypted connectivity or missing data 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.

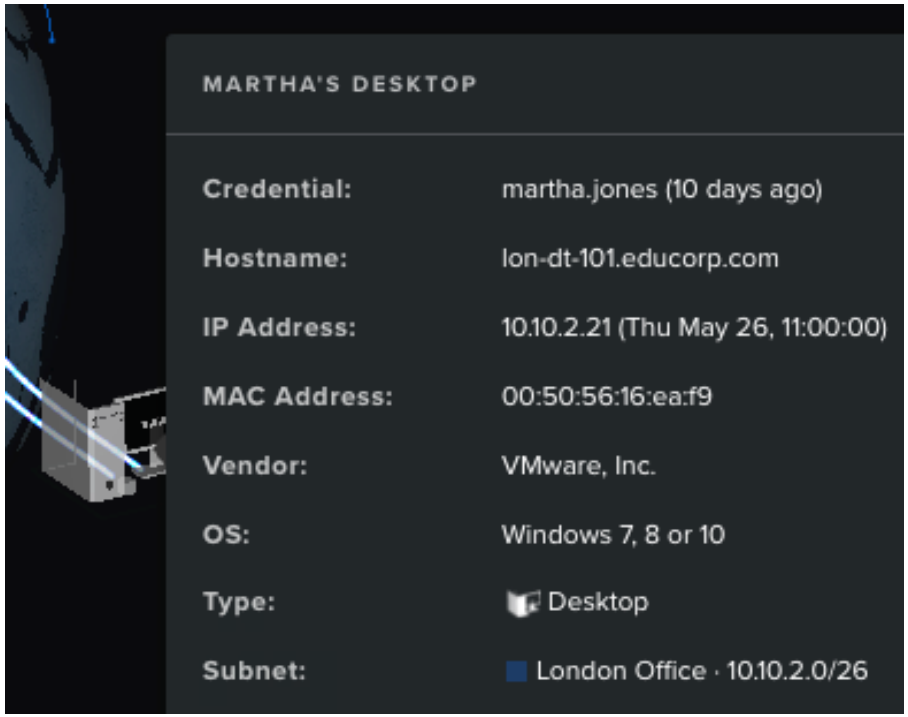
14. Now, navigate to the **LDAP Enrichment** heading of the LDAP/Active Directory section.



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.



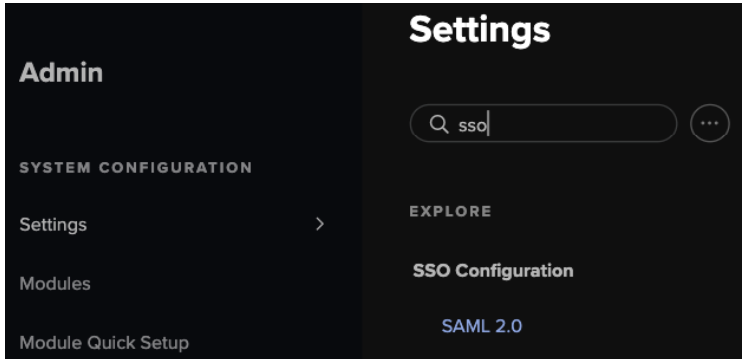
b. Within the same LDAP Enrichment section, locate the **LDAP Create Group Tags** field. The value of this field is used to match LDAP groups. Groups that match the value will generate tags and users in the matching group will be tagged automatically. This field supports wildcards, multiple comma-separated 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 screen.

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. Alongside some pre-populated information, there are five fields to be filled in and two optional toggles.

   Note: The login and logout URLs will need to be provided to your ID Provider.

   a. Begin by entering the SAML 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.

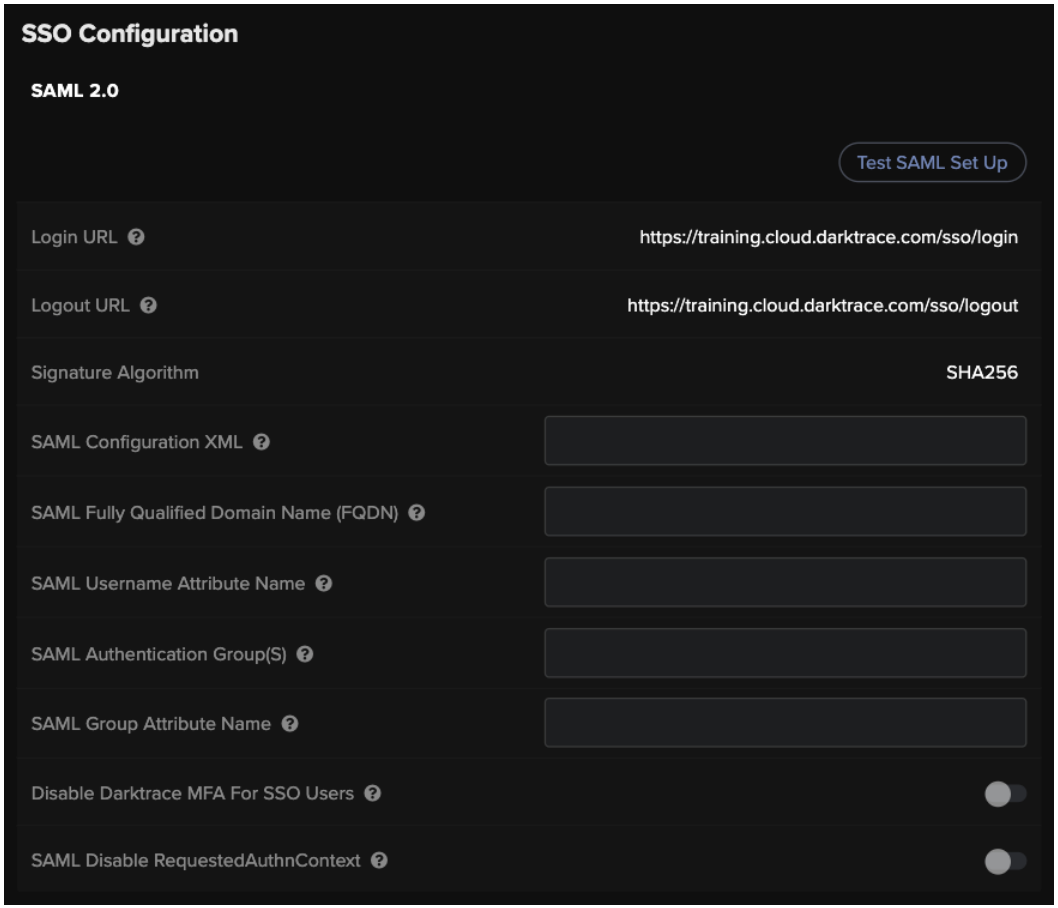
   c. Enter the **SAML Username Attribute Name**. The expected NameID format is outlined in the tooltip.

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

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

   f. If multifactor authentication is already required by the SSO provider, additional Darktrace MFA can disabled using the **Disable Darktrace MFA for SSO Users**.

   g. The final toggle, **SAML DIsable RequestedAuthnContext**, can disable requests for specific authentication context.



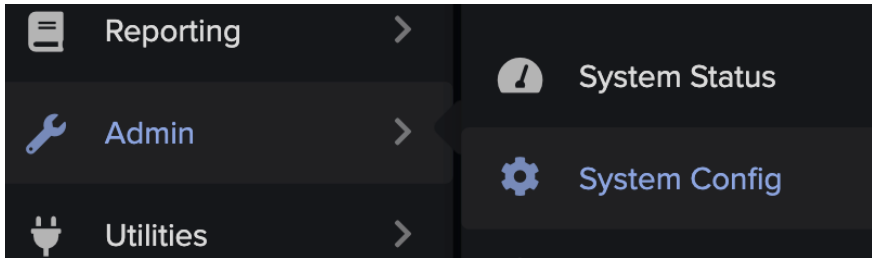
Configuring HTTPS Certificates

Uploading a valid HTTPS certificate will prevent the web browser warning that the connection to the Threat Visualizer uses an invalid certificate. This is indicated in some browsers by a red line through the 'https' part of the URL and may also present the user with a warning that must first be dismissed before accessing the Threat Visualizer interface.

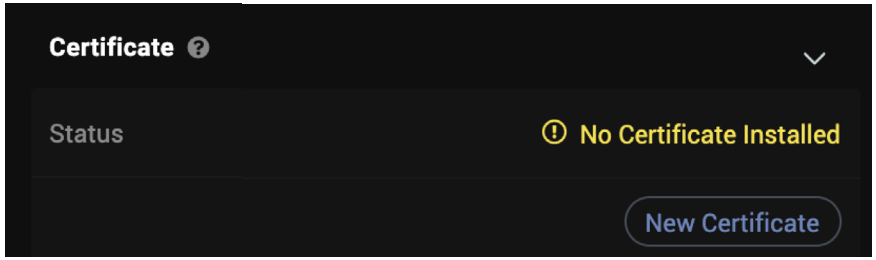
Darktrace Appliances are shipped with a self-signed certificate for the hostname "dt-XXXX-YY" - the internal appliance hostname as designated by Darktrace. Self-signed certificates are often not trusted by web browsers and therefore a warning may be displayed when accessing the appliance. Additionally, 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.

Note: This section only applies to on-premise appliances.

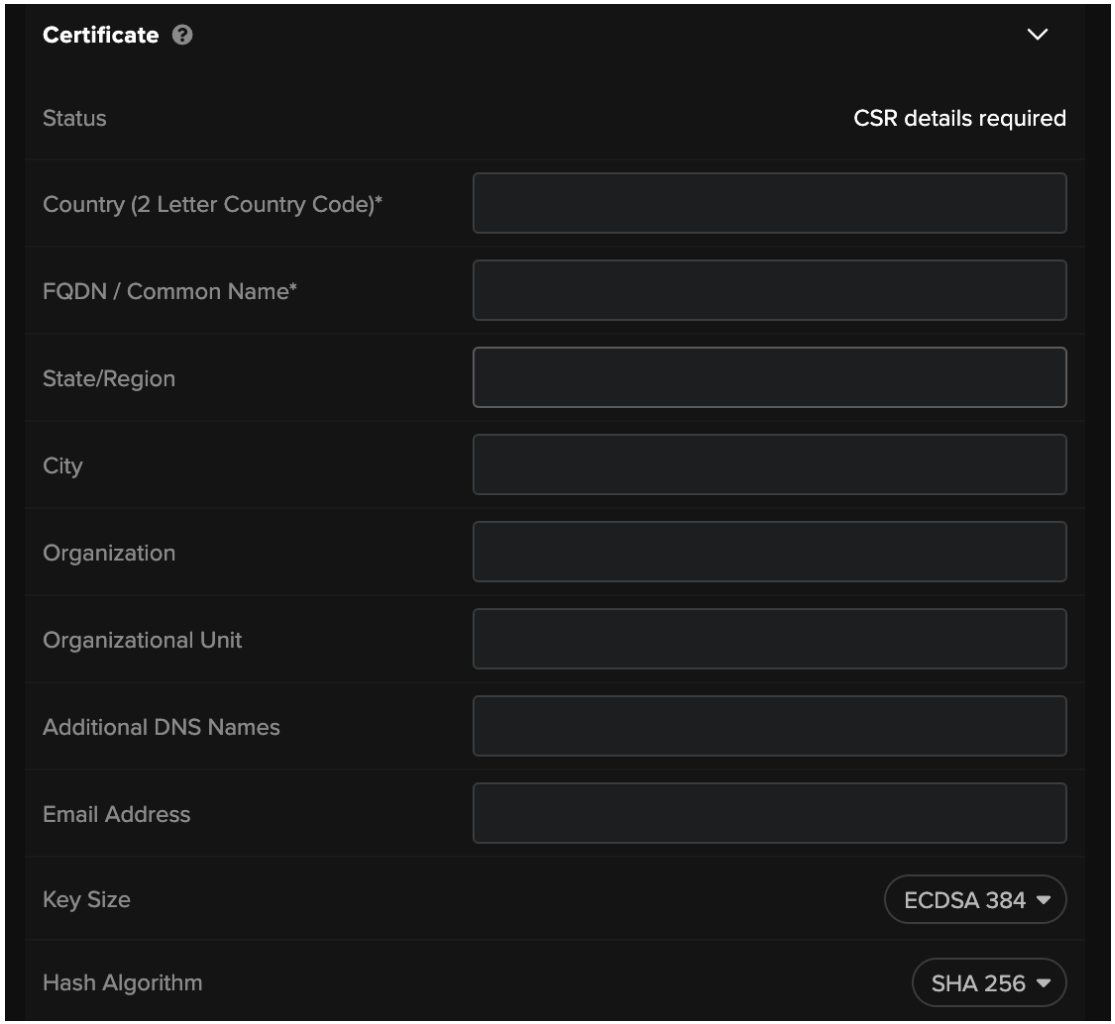
1. Within the Threat Visualizer, navigate to **System Config** within the Admin section of the main menu and open the **Settings** page.



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



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.



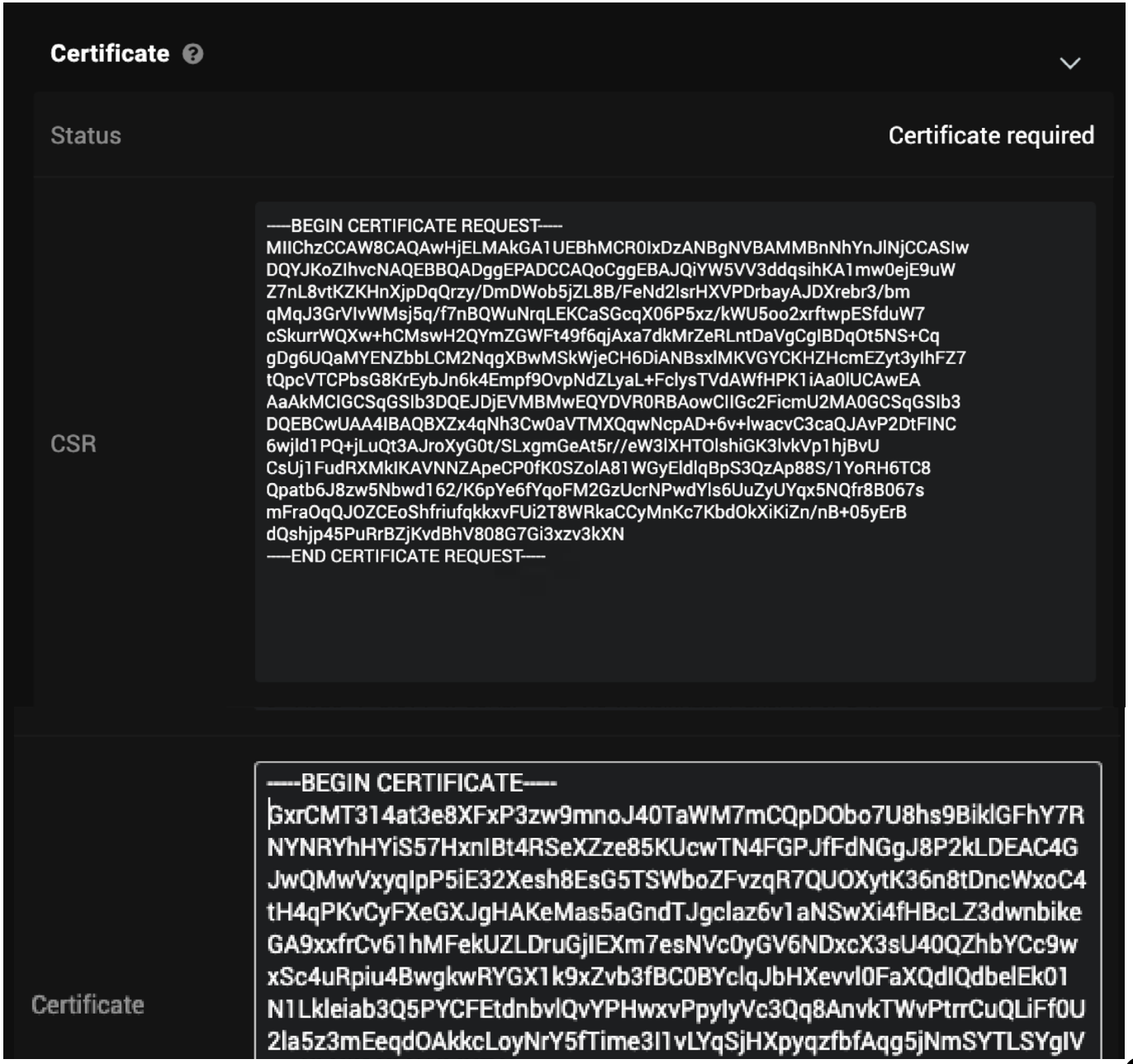
4. With the minimum requirements filled in, a **Generate CSR** button will appear. Click this to use the supplied information to generate a Certificate Signing Request in PEM format.

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.



Configure Darktrace Settings Chapter Test

DARKTRACE
Cyber Engineer Certification

This page will test your knowledge and check your understanding of the Configure Darktrace Settings section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. Which field will allow to identify the users in the LDAP tree?

- [ ] LDAP Username
- [ ] LDAP User Base
- [ ] LDAP Certificate

2. Where should you add the user's name information?

- [ ] LDAP User Attributes
- [ ] LDAP Create Group Tags
- [ ] LDAP Group Tag Prefix

3. What is the default prefix for LDAP tagged groups?

- [ ] LDAP
- [ ] LDAP Group
- [ ] Group

4. The Threat Visualizer supports SAML2 SSO.

- [ ] True
- [ ] False

5. Who will provide the login and logout URLs for SSO?

- [ ] Your Darktrace Representative
- [ ] Your ID Provider
- [ ] Your ISP

6. Which deployment does HTTPS Certificate apply to?

- [ ] Cloud
- [ ] On-Prem
- [ ] Hybrid

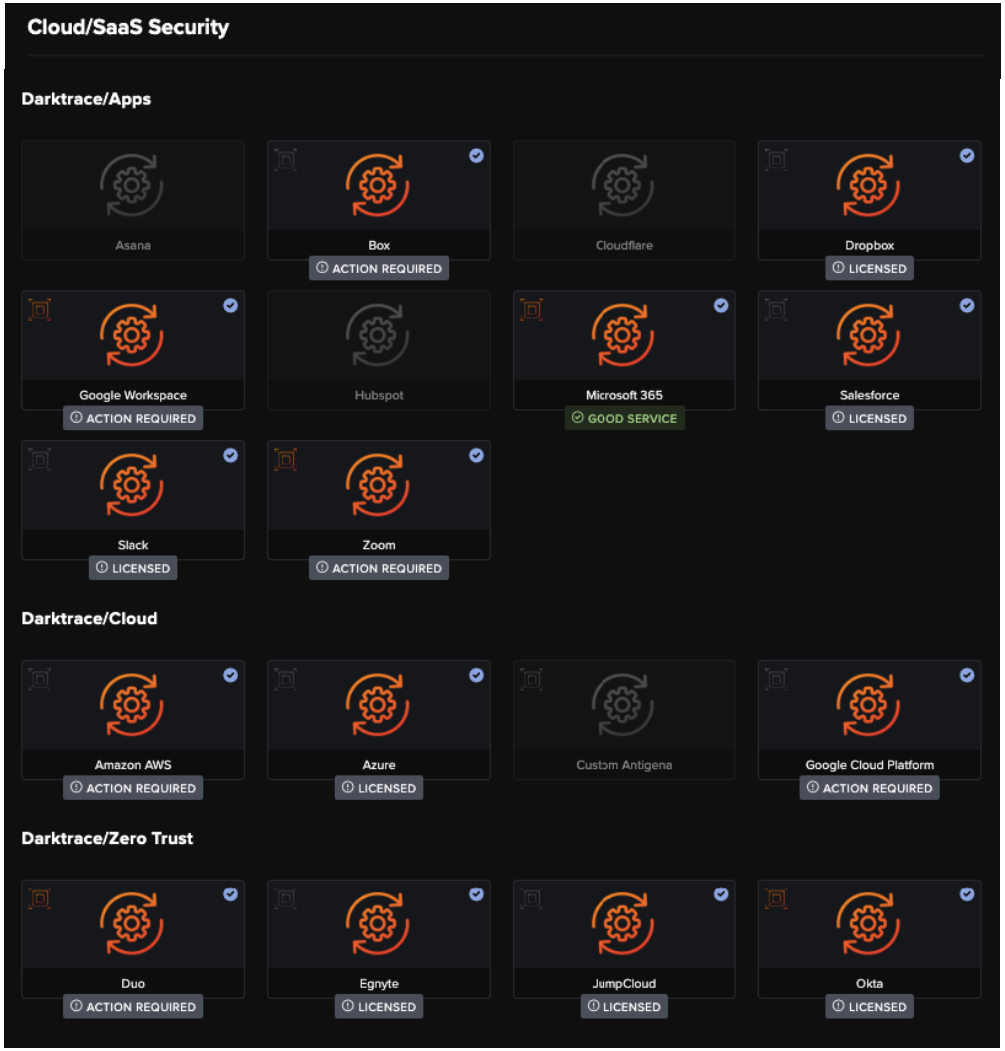
Clear All Answers

6. Configuring Darktrace Modules

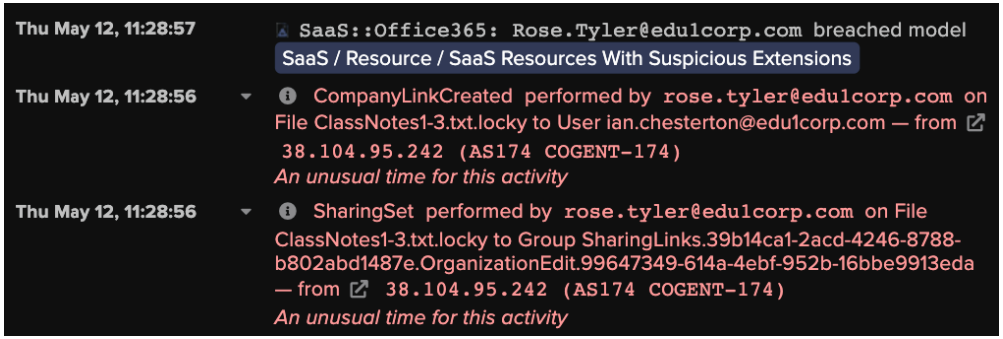
Within the System Configuration page, there is a Modules section, which provides a visual way of understanding what is and what is not enabled on your Darktrace deployment. It instantly outlines which products make up your Darktrace suite but can also highlight additional telemetry and workflow and integration modules that you may wish to enable and configure. In this chapter, let's look at configuring a variety of modules ranging from SaaS to alerting and even the Darktrace Mobile App.

Cloud/SaaS Security Modules

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, SaaS and Zero Trust Modules, 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 modules, a license is required.



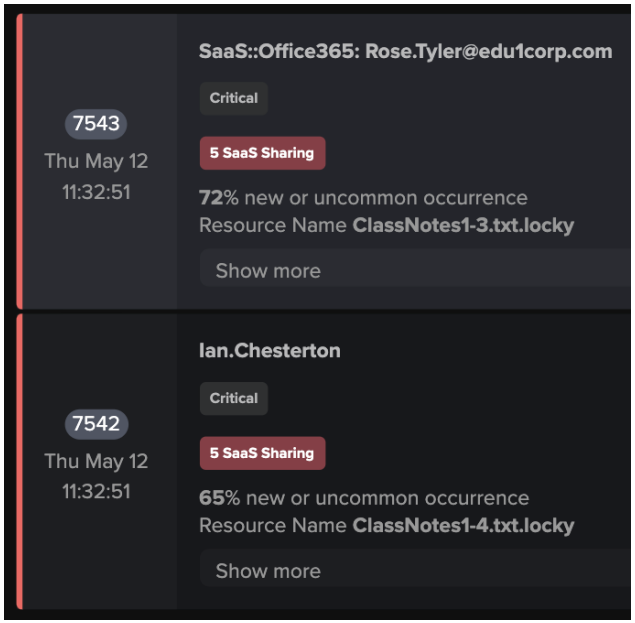
Without a SaaS connector, Darktrace will see traffic to these solutions, but it will be encrypted. For example, the Event Logs will show encrypted communications on port 443, but the credential used, and which files are uploaded, downloaded or deleted will not be identifiable.



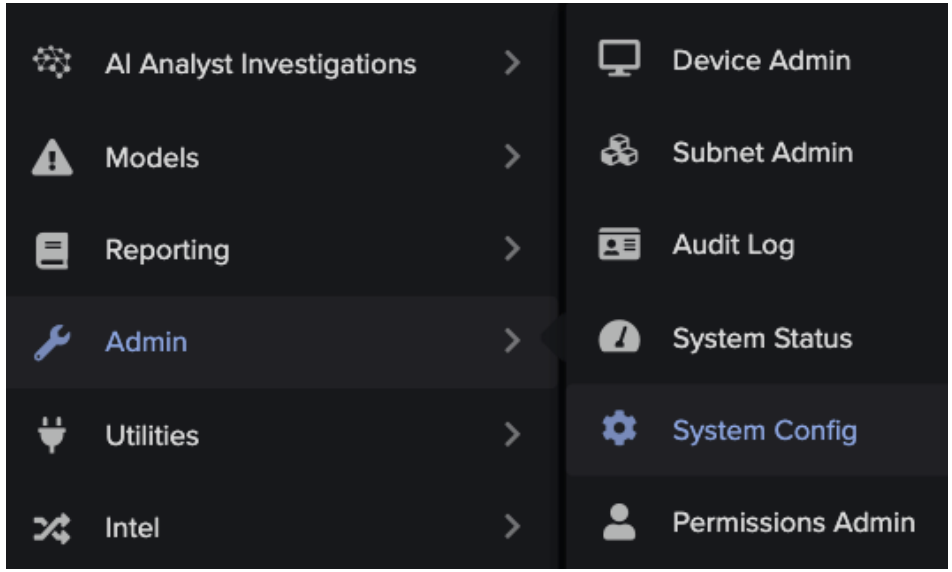
Connectors, such as the Office 365 Connector, can monitor a range of categories:

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

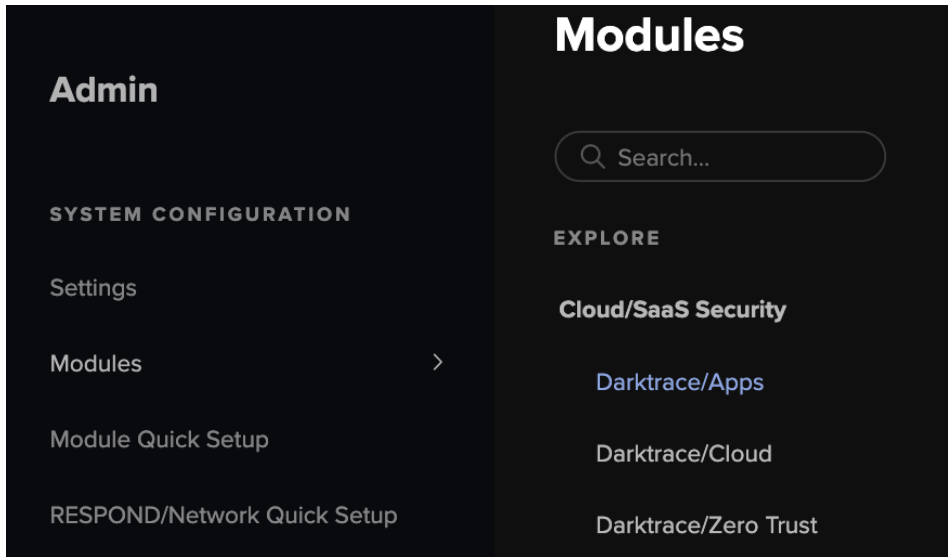
An easy way to deploy Cloud/SaaS Security Modules within Darktrace are outlined below. Note that different Module settings may vary slightly.



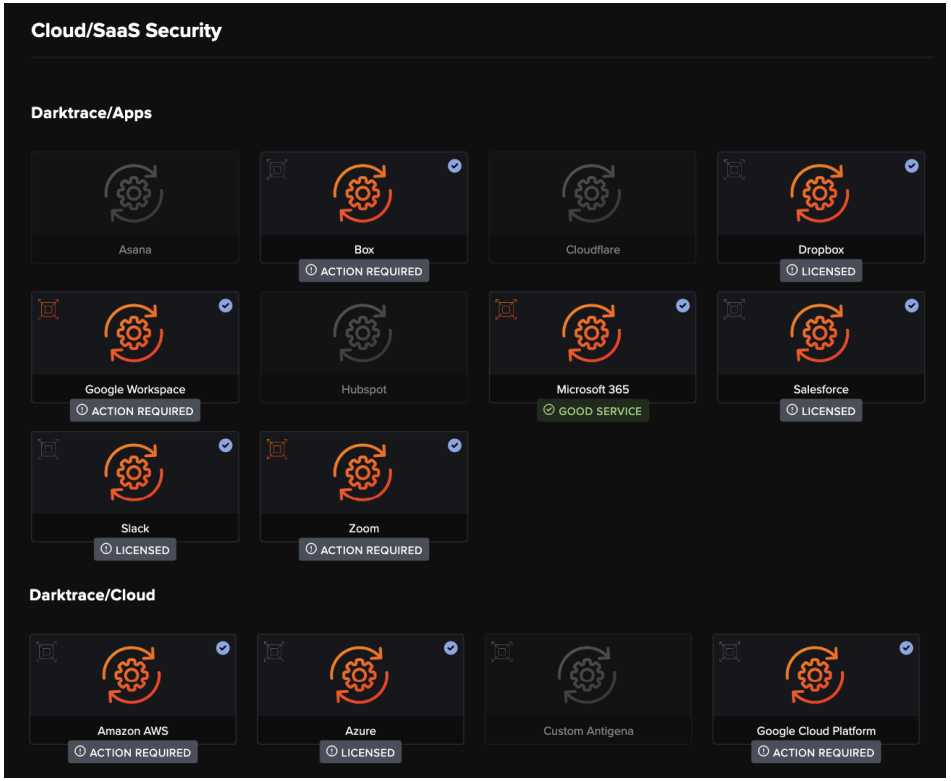
1. Navigate to the **System Config** page.



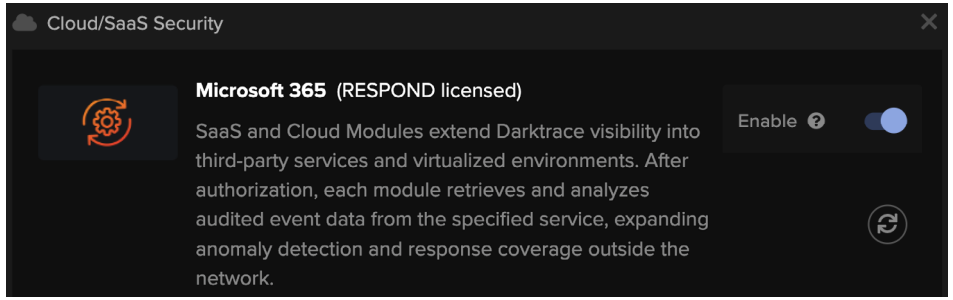
2. Within the Modules menu, navigate to the **Cloud/SaaS Security** subsection which will show modules for Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust.



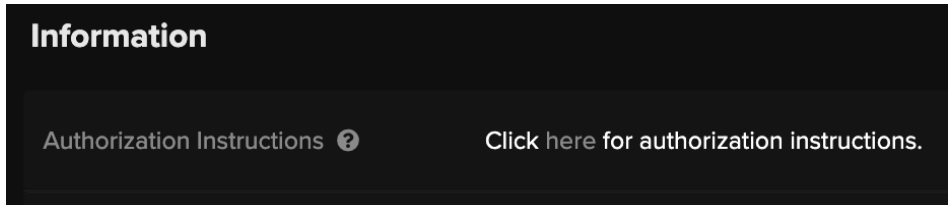
3. Highlighted modules in the **Cloud/SaaS Security** section are licensed, or in use. Click the appropriate module from the available options to open a window allowing for further configuration.



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

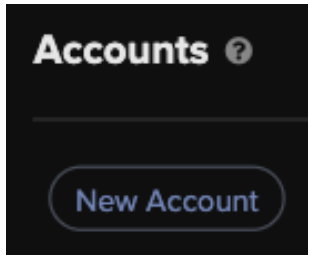


5. Under the Information heading, next to the field labeled **Authorization Instructions**, click the link for further instructions.

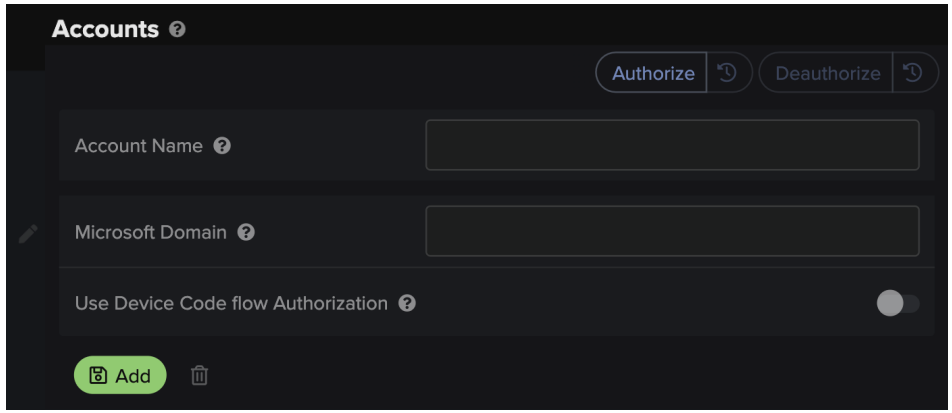


6. Follow the module specific steps on the page and **log in to the SaaS provider**.

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



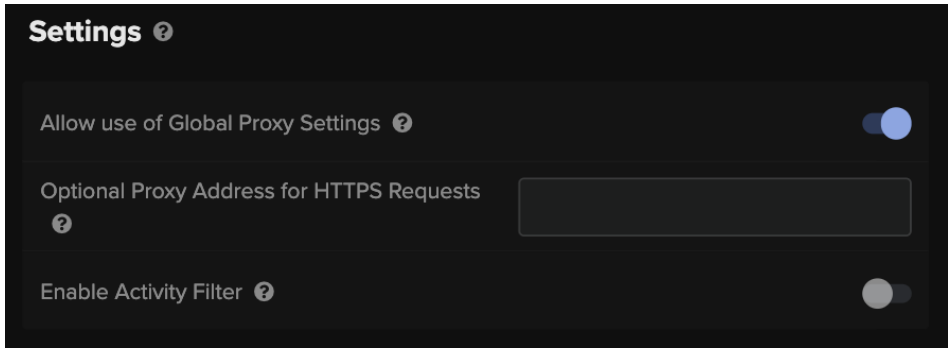
8. Clicking on the New Account button will open up more **fields**. Fill these out using the **tooltips** for assistance.



9. Click the **Authorize** button above these fields to begin monitoring your Cloud/SaaS environment.

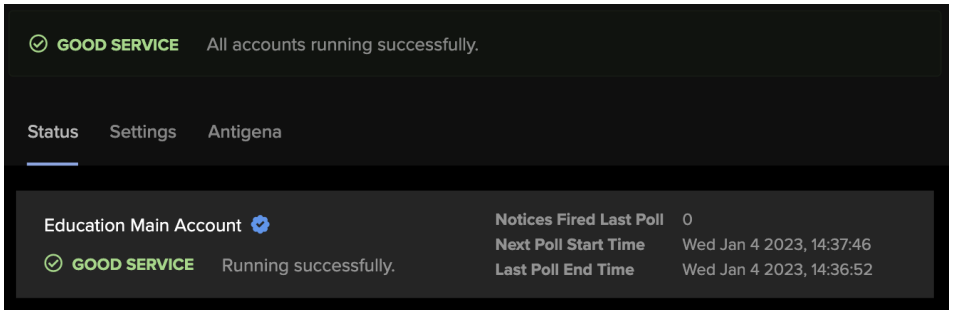
After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful or if any errors occurred.

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



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

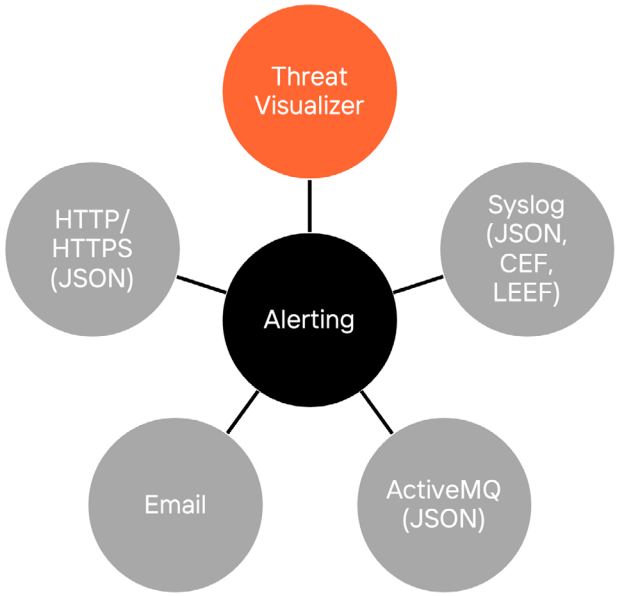
11. Once the module has been successfully configured, a message will appear within the **Status** section of the window.



Configuring Alerts

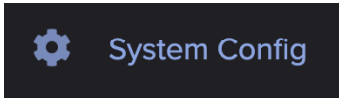
1. Darktrace can interact with an organization's existing alerting or security information system.

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



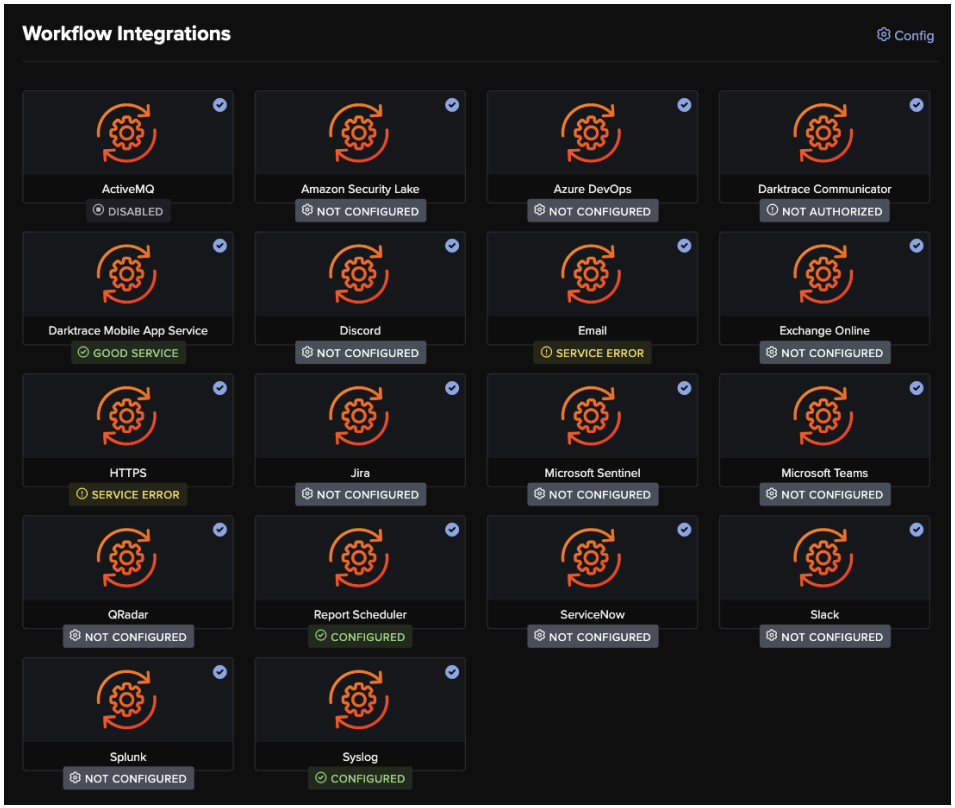
Note: For alerts to contain links back to the Threat Visualizer, the Fully Qualified Domain Name (FQDN) value must be set in the Settings section. This field should contain the resolvable hostname or IP address of the Darktrace Threat Visualizer.

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.

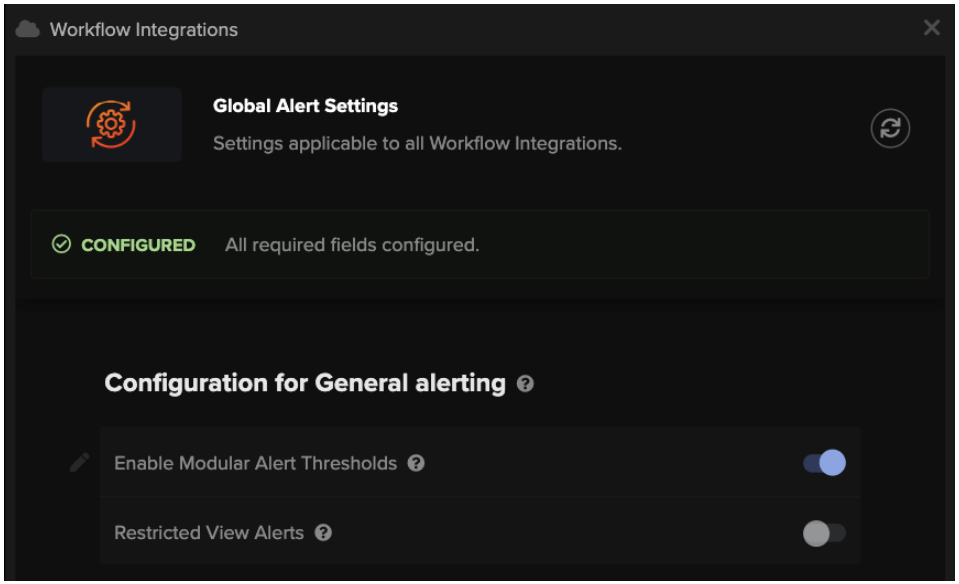
Note: Alerts are only sent for Models where the Action is set to Alert.



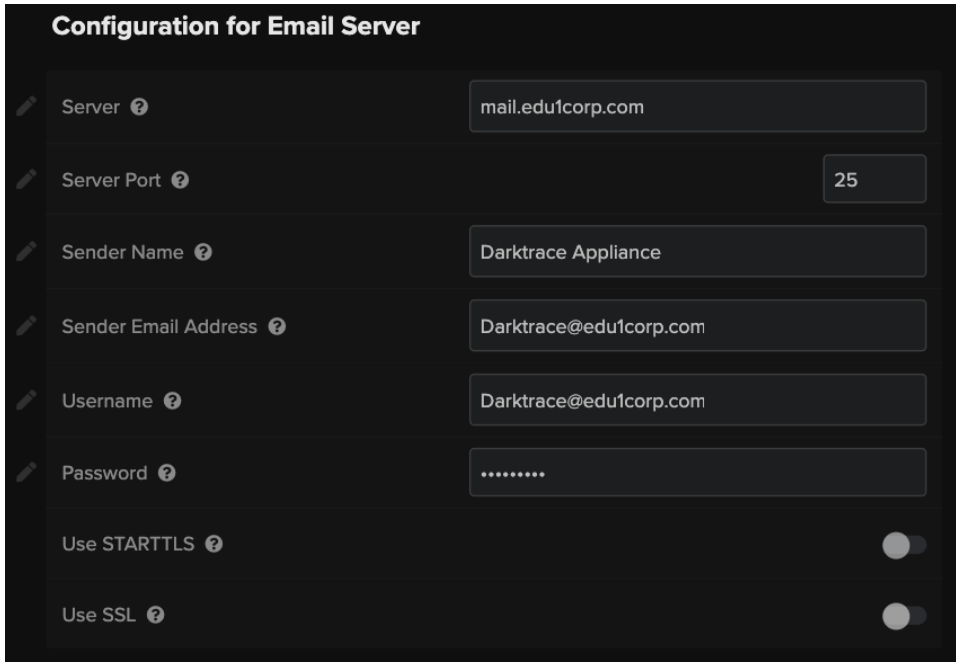
3. In the top right-hand corner of the Workflow Integrations section, click the **Config** button to open a Global Alert Settings option.

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**, and click on the Settings tab to find the **Configuration for Email Server** section.



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

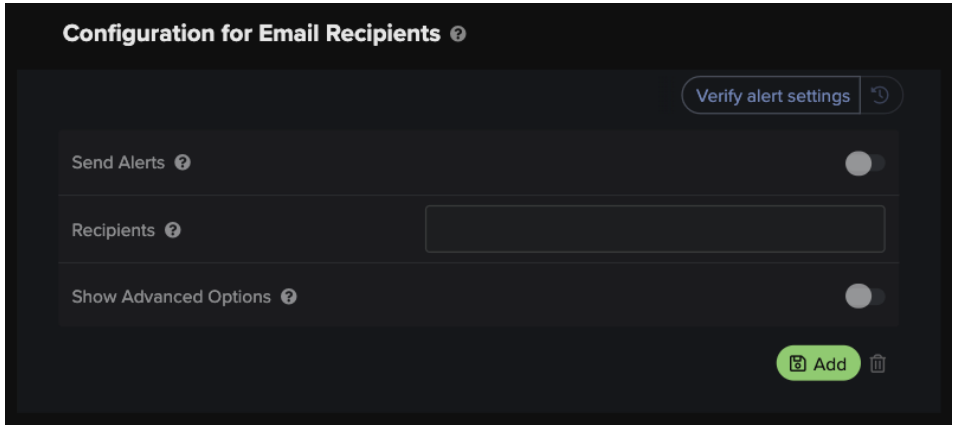
   b. Next, provide a **Sender Name** and **Sender Email Address** to set the values which will be observed by the recipient of the alert email.

   c. Enter a **Username**, which must match the Sender Email Address, and the associated **password** to authenticate with 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, locate the **Configuration for Email Recipients** section.



a. First, turn on the toggle to **Send Alerts** for this configuration.

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.

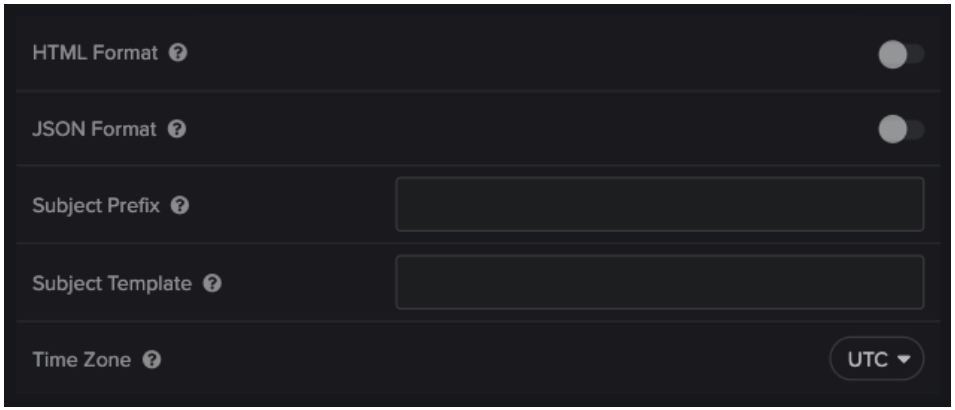
c. Switch on **Show Advanced Options** to see other available fields.

Top Tip:

The Advanced Options are split into multiple categories, including the general alert formatting/template details, AI Analyst alerts, Model Breach alerts and System alerts.

It may be desirable to have different configuration settings for different roles within an organization. For example, resolving System Status alerts may not fall under an Analyst's skill set, but receiving emails about AI Analyst or Model Breach alerts may be more relevant.

7. The first section contains fields which determine the **generic details** of the email alert, such as format and time zone.



a. Using the toggles, 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**.

b. The **Subject Prefix** field may be utilized for defining a string which will be added before the subject of an alert email.

c. The subject itself can be customized using the **Subject Template** field.

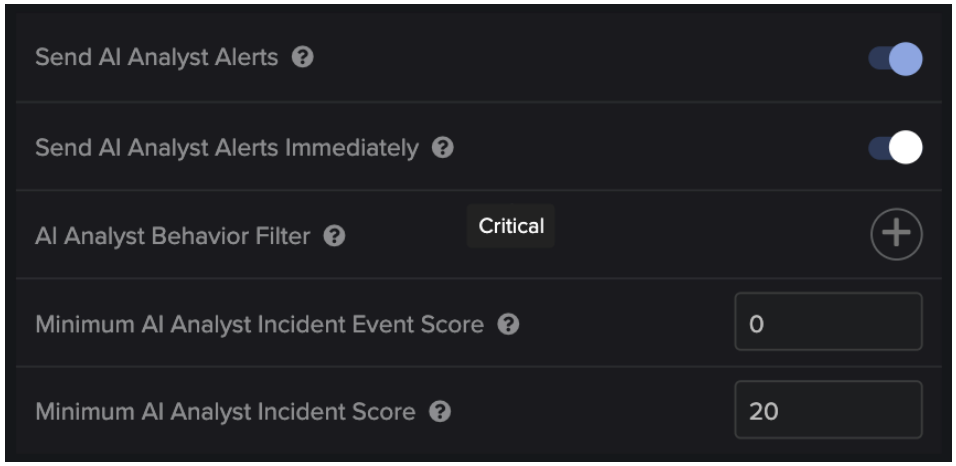
This option supports templates using the available fields time, device, label, hostname, name, score and ip. Combining these, a subject can be created. For example:

Model $(name) breached on $(time) with $(score)

Note: If a field does not return a value, it will be replaced with "unknown". Furthermore, the device field will be replaced with, in order of priority: label, hostname, IP address, or unknown, depending on what is available in the alert.

d. Finally, using the UTC drop-down, select a relevant **time zone**.

8. Next, the alert can be configured to send **AI Analyst information**.



a. First, decide whether **AI Analyst Alerts** should be sent by turning the toggle on. By default, alerts of this type will be sent.

b. The next option, **Send AI Analyst Alerts Immediately**, is on by default and will send an alert as soon as an incident is created. Turning this setting off will send a curated list of interesting incidents once an hour.

c. The recipient will be alerted to **Critical** incidents, as seen in the **AI Analyst Behavior Filter**. Click the **plus button** at the end of the row to add further behaviors or hover over an existing filter to display the trash can which allows the filter to be removed.

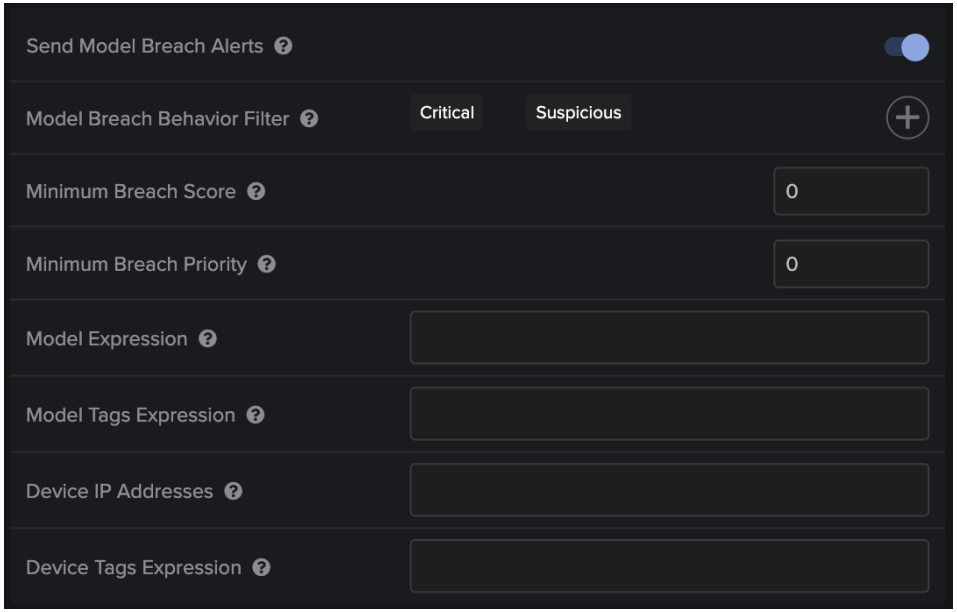
d. Once the AI Analyst fields have been reviewed, consider what thresholds should be breached before being notified.

   i. The **Minimum AI Analyst Incident Event Score** corresponds to the individual events that contribute to an Incident. These individual events are equivalent to the tabs of an incident. If an event has a score greater than or equal to the inputted value, the event alert will be triggered.

   ii. The **Minimum AI Analyst Incident Score** corresponds to the overall score given to an incident in the AI Analyst Threat Tray. These are the scores which can be filtered using the Sensitivity Slider in the Threat Visualizer. The default value of 20 is equivalent to the Sensitivity Slider's default value. This will only alert incidents which have a score higher than 20%.

Note: If more than one alert condition is configured, an AI Analyst event/ incident must meet all selected requirements before alerting can occur.

9. Moving down the window, the alert can be configured to send **Model Breach information**.



a. First, decide if the configured user should be alerted to **Send Model Breach Alerts**.

b. The **Model Breach Behavior Filter** field has **Critical** and **Suspicious** filters applied by default. Click the **plus button** to add further behaviors or hover over a filter to display the trash can to remove it.

c. Once the alerting type has been configured, consider what Model Breach 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. 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.

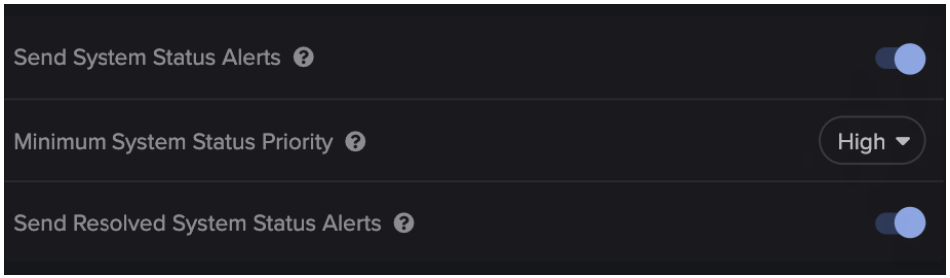
iv. Another optional filter is the **Model Tags Expression**, which allows you to restrict Model Breaches to those with tags that match the regular expression defined.

Note: As mentioned before, 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.

d. By utilizing the **Device IP Addresses** 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. Values can be entered in the form of a comma separated list.

e. By entering a regular expression in the **Device Tag Expression** textbox, users can restrict the sending of a model breach alert to those with device tags matching the regular expression.

10. Finally, the email alert can include **System Status** alert information.

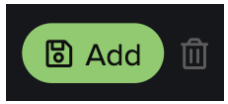


a. First, decide whether **System Status Alerts** should be sent by turning the toggle on. By default, alerts of this type will be sent.

b. Then, using the **Minimum System Status Priority** drop-down, select a minimum priority to be alerted to. The options are as follows: Informational, Low, Medium, High and Critical.

c. The last option, **Send Resolved System Status Alerts** can be toggled on/off. Leaving this on will alert the recipient to all System Status alerts, including resolved ones. However, turning this off will restrict alerts to unresolved only.

11. Once the options for a chosen Email Recipient have been configured, click the green **Add** button below the newly configured fields.



Note: Individual entries of configurations for email recipients can be deleted by clicking the trash icon beside the Add button.

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

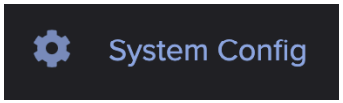
13. To add email alert recipients with different conditions, click **New** and repeat the above process.

Setting up the Mobile App

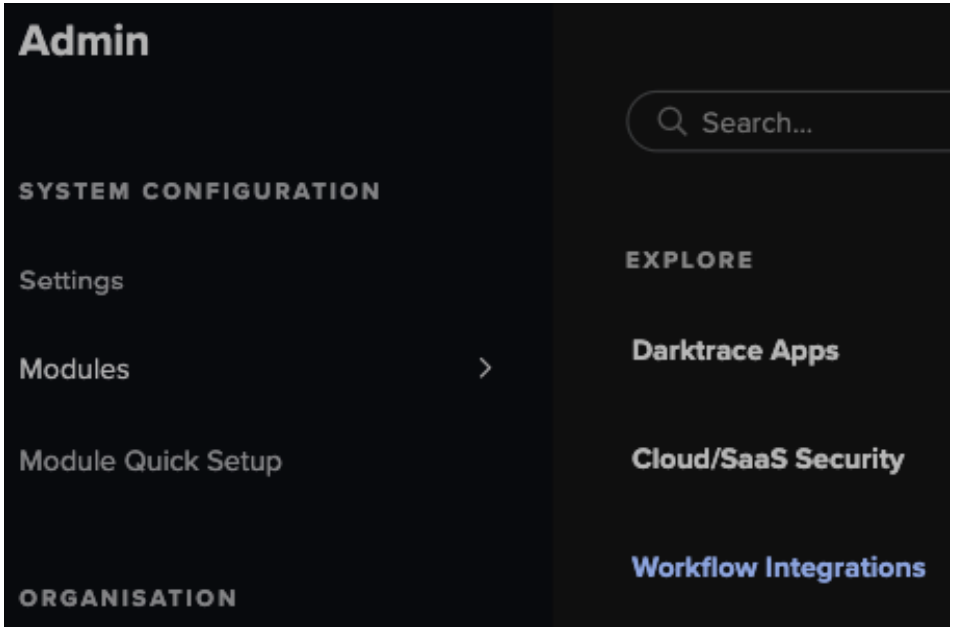
The Darktrace Mobile App, available for iOS and Android, allows users to easily access Darktrace Alerts when they are on the move. In order to associate the Darktrace Mobile app with an existing Darktrace deployment, the Threat Visualizer must be authorized to send alerts. Organizations wishing to use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

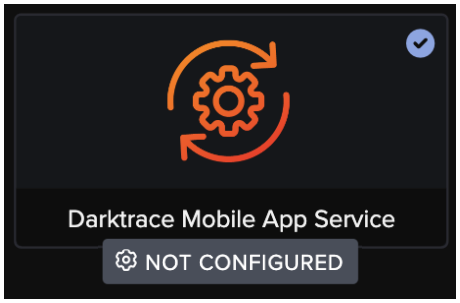


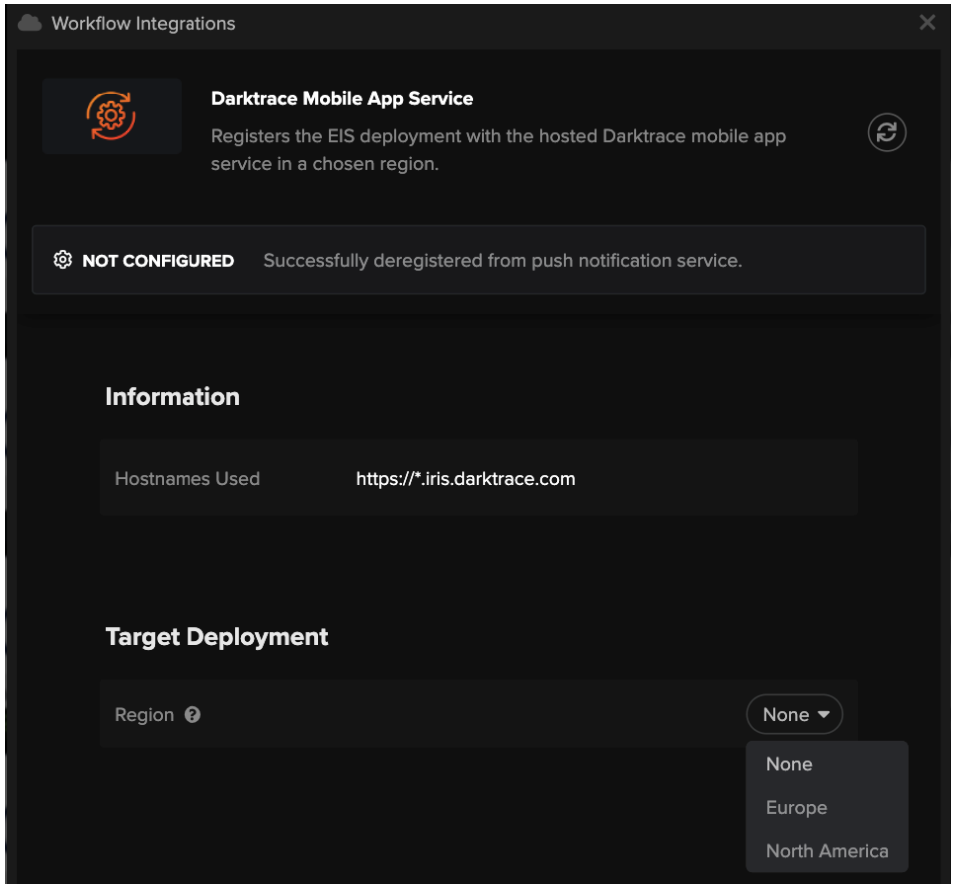
2. From the left-hand menu, select **Modules** and locate Workflow Integrations.



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

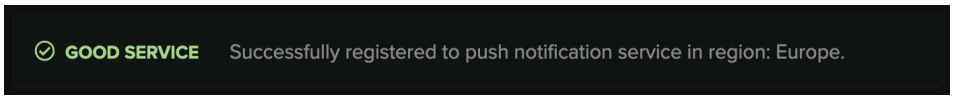
4. A configuration window will open. From the Region drop-down menu, select a **Target Deployment Region** to host the mobile app push notification service.





5. After selecting a region, **save** the change using the button that appears at the top of the window.

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



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

Note: It is imperative to add to a Trusted Domain list 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 Permissions Admin page. The permission can be revoked at any time.

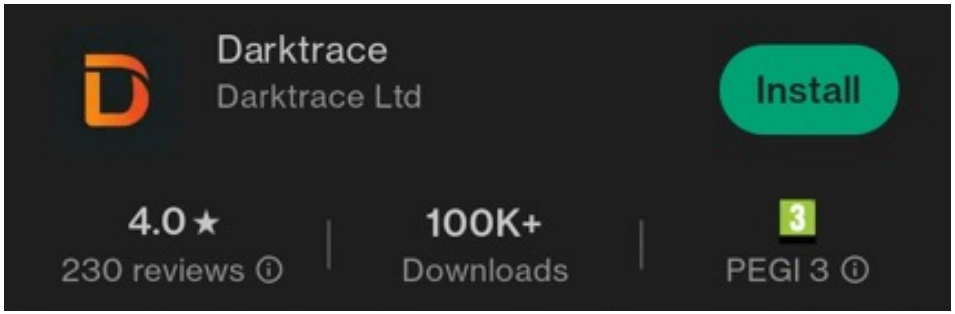
If the administrator revokes Mobile App permissions, the Model Breach, Antigena and summary cached data within the app is deleted for the given user.

If a Darktrace user using the mobile app has their Mobile App permission removed, their app will deactivate itself and receive no further data.

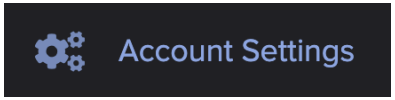
Note: LDAP users must have their app permissions explicitly revoked on a per user basis in the User Admin page. Removing the permission from an LDAP Group in the Group Admin page is not sufficient.

Registering the App

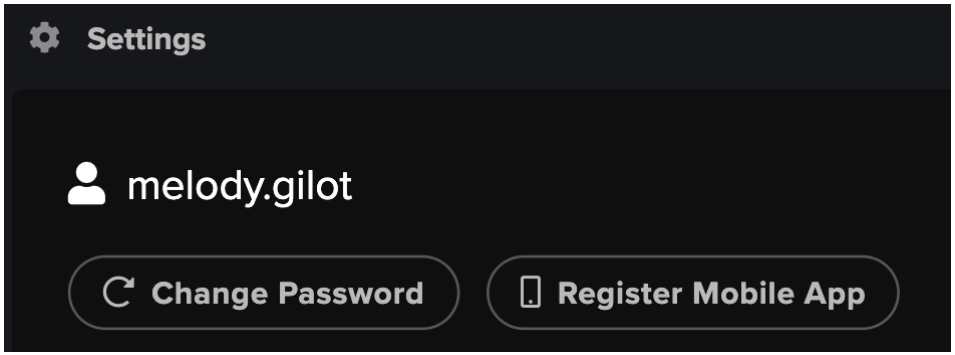
1. On a smartphone, open the app store and search for Darktrace. The Darktrace iOS app is available on the App Store and the Android app is available on Google Play. **Download and open the Darktrace app**.



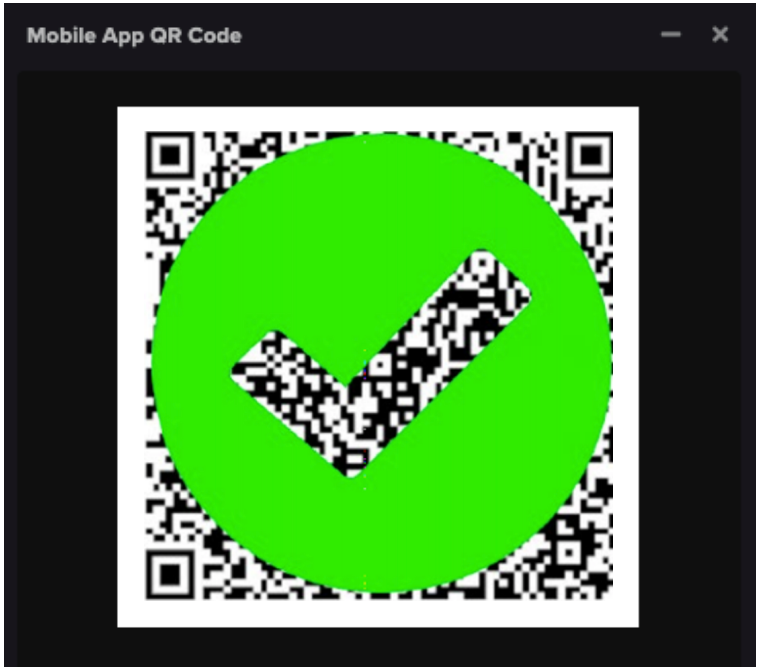
2. Navigate to **Account Settings** from the main menu.



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



4. 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. To finish authenticating, enter your **Darktrace account password**.

d. It is also recommended to provide a **pin code** as an authentication method.

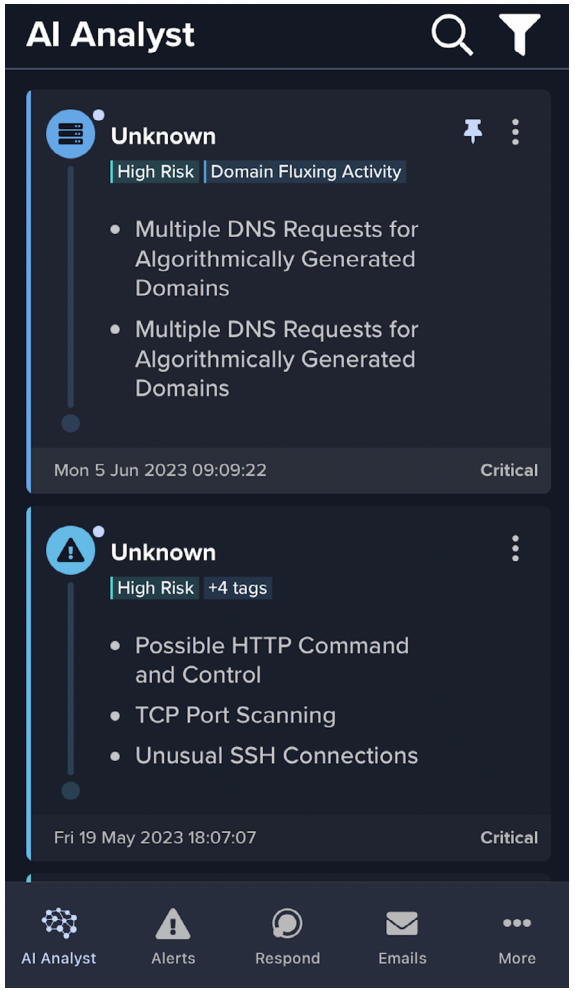
e. Move between screens using the **guided overlay** to understand the functionality. This guide can be re-enabled at any point from the app config page. Using the App

Using the App

AI Analyst

This screen displays AI Analyst incidents.

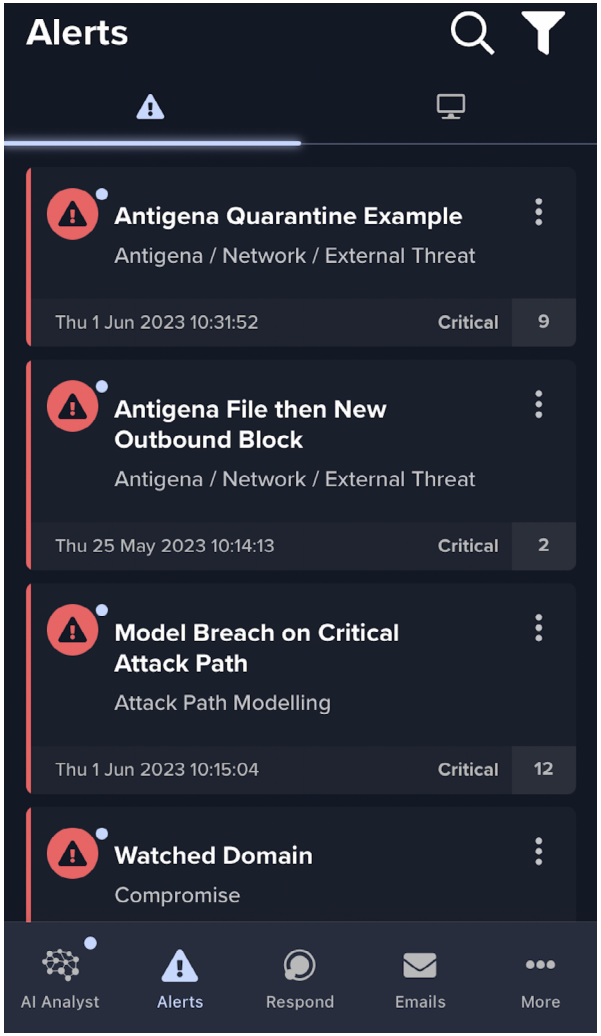
- Tap the more icon to pin an incident.
- Swipe left to acknowledge an incident.
- Tap to review Cyber AI Analyst incidents:
  - Open the left tab to view incident events and information.
  - Swipe left on an incident event to acknowledge it.
  - Open the middle tab to view incident devices.
  - Open the right tab to view incident comments.
  - Tap the pin icon to pin or unpin the incident and its events.
  - Tap the tick icon to acknowledge or unacknowledge all events for this incident.
  - Shre a link to the Mobile App incident.
  - Read summary of events. and view attack phases involved.
- Drag down to refresh.



Alerts

This page lists Model Breaches.

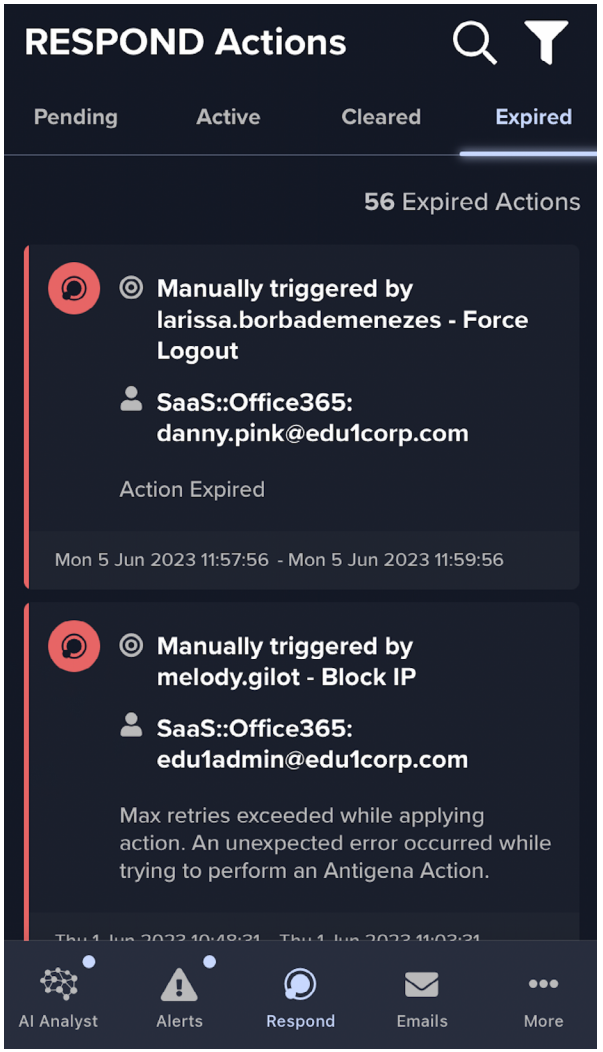
- Tap to modify the alerts page filter settings
- Open the left tab for model breaches by model
- Open the right tab for model breaches by device
- Tap on the more icon to pin or mark read a model or device
- Drag down to refresh and reveal a search bar.
- Review Model and Breach details.
  - Swipe left on a model breach to acknowledge it
  - Swipe left and right to view other model breaches
  - Swipe up from the bottom to view quick actions
  - Open the left tab to view a summary
  - Open the middle tab to view events within the model breach
  - Open the right tab to view related RESPOND actions
  - Tap on an event to view details



RESPOND

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

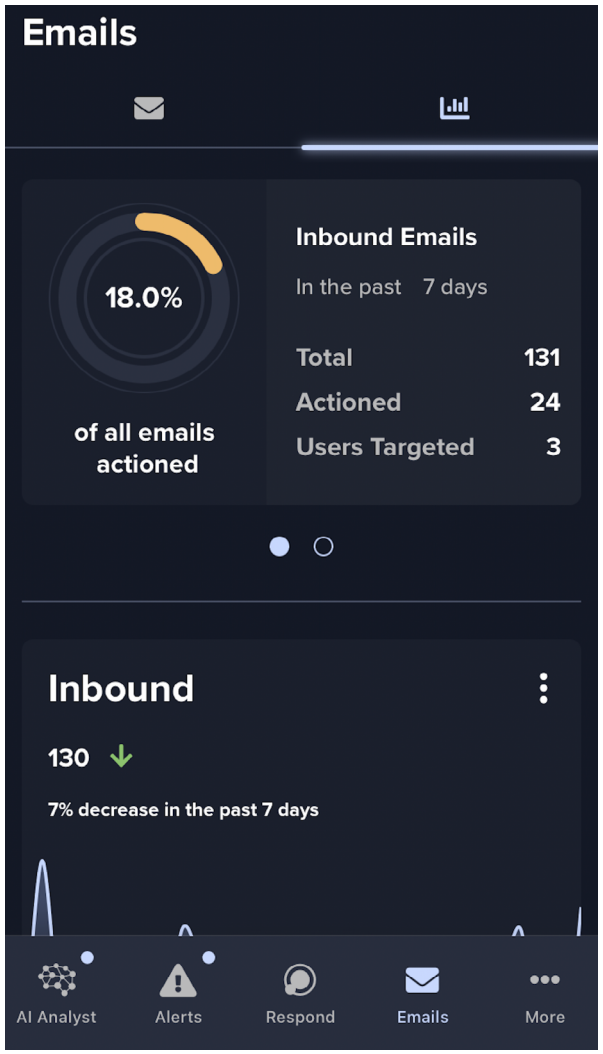
- Use the tabs to filter by action status
- Swipe left on a RESPOND action for actions
- The Pending, Active, Cleared and Expired actions will be shown in different tab
  - Tap an action to review details.
  - Swipe up from the bottom to view quick actions such as Extend, Clear or Activate
  - Open the left tab for information about the action
  - Open the right tab for related model details



Emails

The Email screen displays ounbound and inbound emails.

- Use the Email tab to filter and find emails
- Use the Graph tab for an overview of emails
- Swipe left on an email to manually hold it
- Swipe right on an email to manually release it
- Click on an email to have access to the Overview and more actions at the bottom
  - Tap Release Email to release it.
  - Once an email has been released, the option to add a Learning Exception will appear.
  - Tap Hold Email to hold it.
  - Tap Investigate Campaign to view similar emails from the same sender.



More

Dashboard

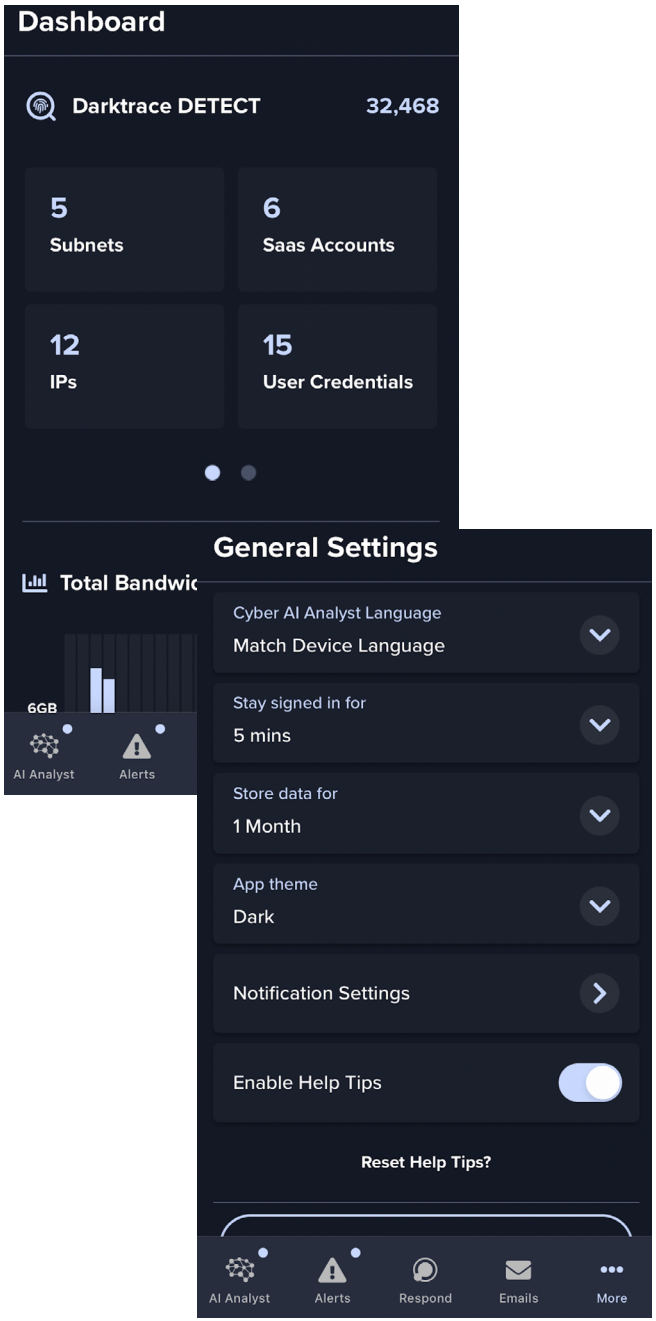
The Dashboard screen mirrors the high-level summary presented on the left of the Threat Visualizer home page.

Settings

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

Notifications

Notifications can be seen from this page. The notification types include Model breaches, RESPOND actions, AI Analyst incident events and System alerts.



Integrating Darktrace: SIEMs and APIs

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>

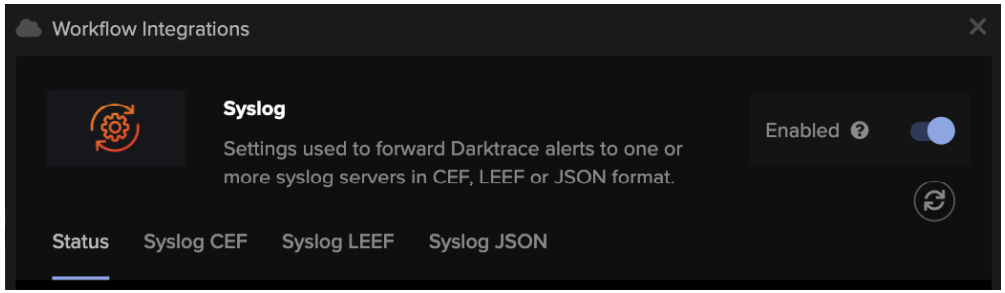
Note that the LEEF format includes the Model Breach URL, facilitating subsequent investigation of the event in the Threat Visualizer.

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, open the relevant tab and 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

Consult The Threat Visualizer API Product Guide on the Customer Portal to craft a GET request URI to retrieve each of the following. Using the text boxes below, paste your results for future reference.

- 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.
- Any SMB1 sessions seen in the last 7 days

Configure Darktrace Modules Chapter Test

DARKTRACE
Cyber Engineer Certification

This page will test your knowledge and check your understanding of the Configure Darktrace Modules section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. What would happen without a SaaS connector?

- [ ] Darktrace cannot see SaaS traffic
- [ ] SaaS traffic will be encrypted
- [ ] There is no SaaS connector

2. Which of the below is NOT a Cloud/SaaS Security subsection?

- [ ] Darktrace/Office365
- [ ] Darktrace/Apps
- [ ] Darktrace/Zero Trust

3. For email alerts, SSL and STARTTLS can be used together.

- [ ] True
- [ ] False

4. Which hostname is used to receive alerts on Darktrace Mobile App?

- [ ] https://*.mobile.darktrace.com
- [ ] https://*.iris.darktrace.com
- [ ] https://*.rose.darktrace.com

5. Darktrace/Email is available in Darktrace Mobile App.

- [ ] True
- [ ] False

6. What does the API key-value “pid” mean?

- [ ] Public ID
- [ ] Policy ID
- [ ] Policy History ID

Clear All Answers

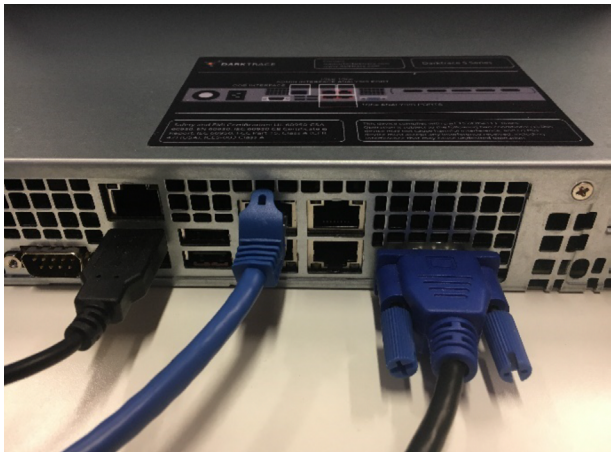
7. Backing up and Restoring Darktrace

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 on-premise Master appliances need to be backed up, as no data 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

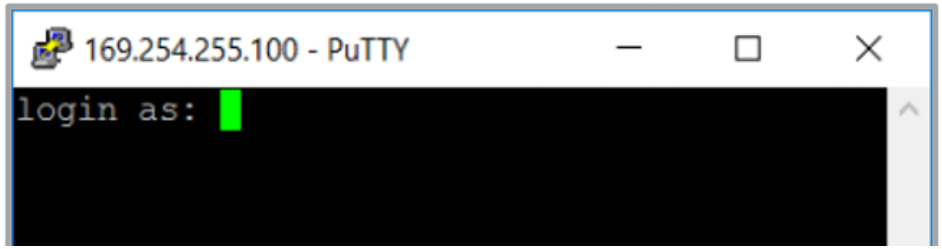
1. The **Console interface** can be accessed by using a VGA monitor and USB keyboard connected to the **Darktrace appliance**. Alternatively, the application can be remotely accessed via the appliance management interface (Ethernet port eth0) by means of any ncurses-capable SSH client (such as PuTTY).



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.

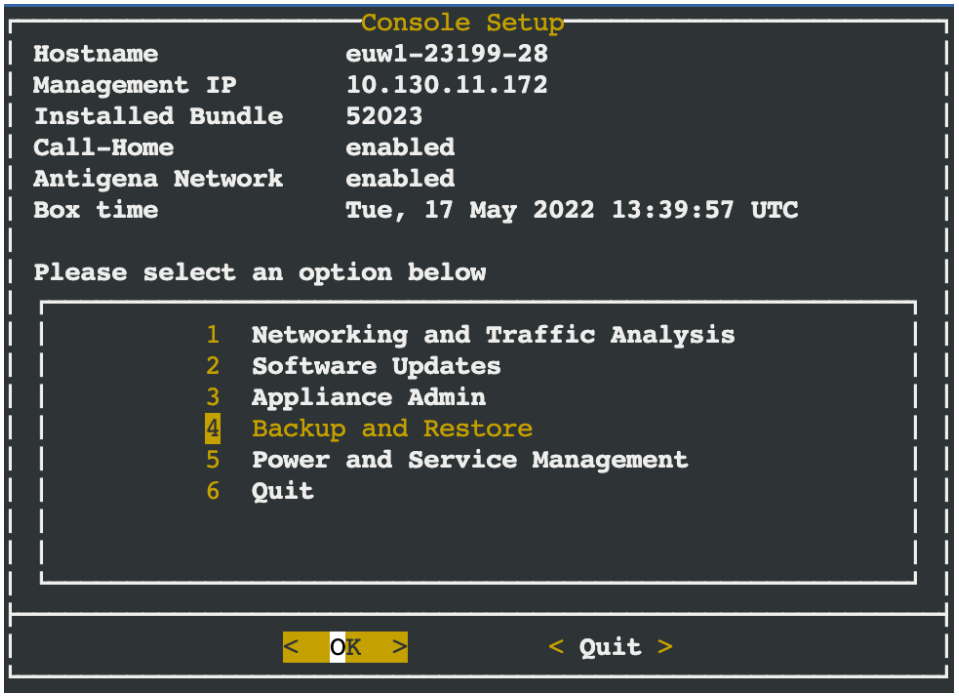


Console Usage

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.

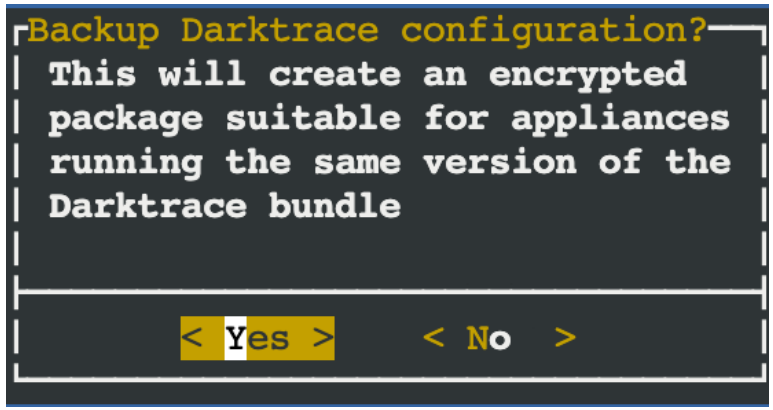
3. Log in as the **Console user** and enter the **password** provided by Darktrace. Confirm the Console Setup options are displayed.

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



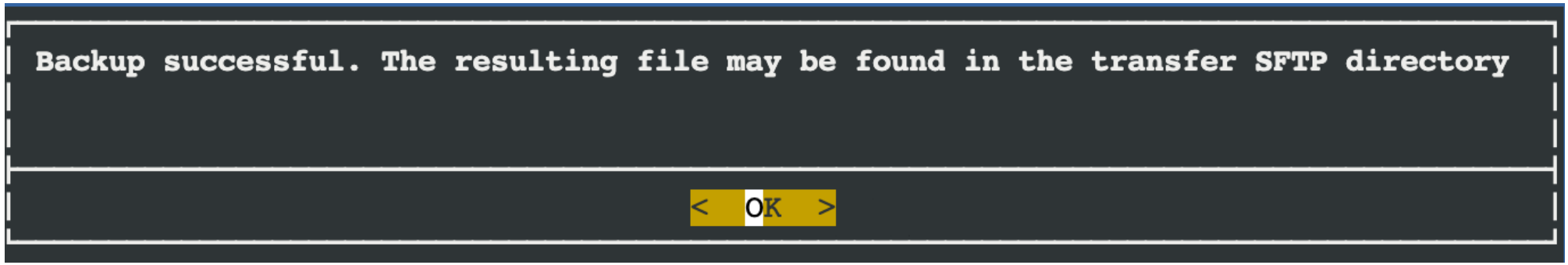
2. A range of backup options are available. Select option **1. Backup locally now**. Choose **OK**.

3. Note that backups can only be restored to the same version of the Darktrace software. Select '**Yes**' to proceed.



Note: The backup file name will contain the bundle version number.

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



Create Scheduled Backups

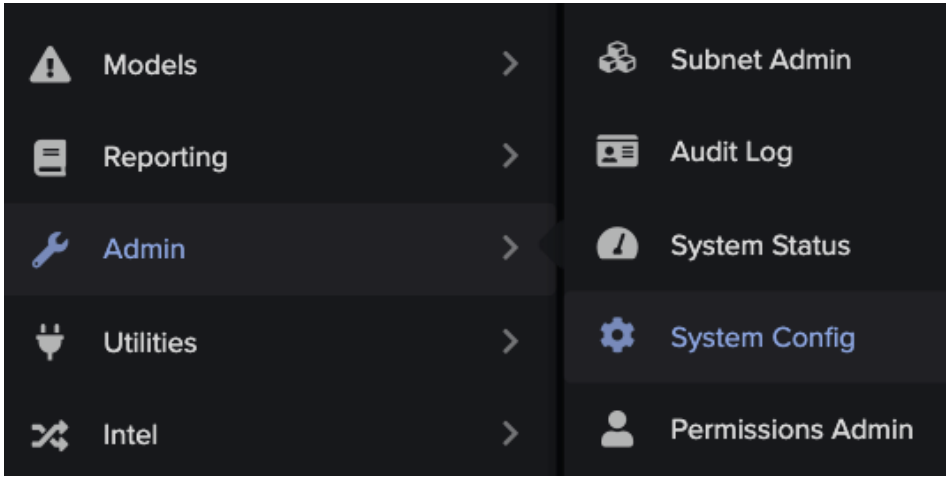
The Darktrace Threat Visualizer application includes configuration options to schedule backups for your Darktrace appliances. A backup includes all Darktrace machine learning, models, breaches, as well as subnet and device information, and configuration settings on the Threat Visualizer GUI. It does not include transactional data such as connections in the Event Log, Advanced Search entries and PCAP files, nor configuration settings on the console menu.

In networks with Probe and Master appliances, only the Master appliance needs to be backed up. In Unified View deployments, or if more than Master is being used, make sure to back up all Masters. Darktrace Threat Visualizer 5.2 allows scheduled backups and scheduled backup alerts to be configured from the Threat Visualizer System Config page (physical appliances only) by users with the "System Admin" permission.

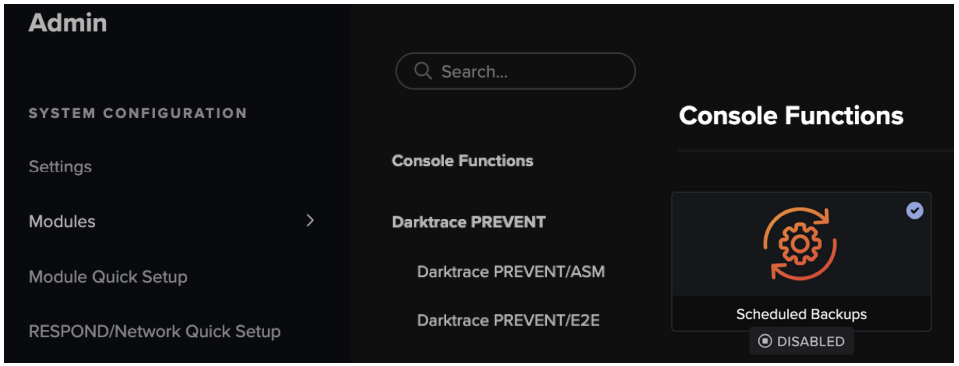
Note: Scheduled backups can also be configured from the console. For more information on the process, follow the relevant Customer Portal links: SCP, SMB and S3.

Global Settings

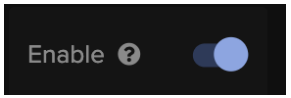
1. Open the Threat Visualizer and navigate to the **System Config** page (Main menu > Admin).



2. From the left-side menu, select **Modules**, navigate to the **Console Functions** section, and choose **Scheduled Backups**.

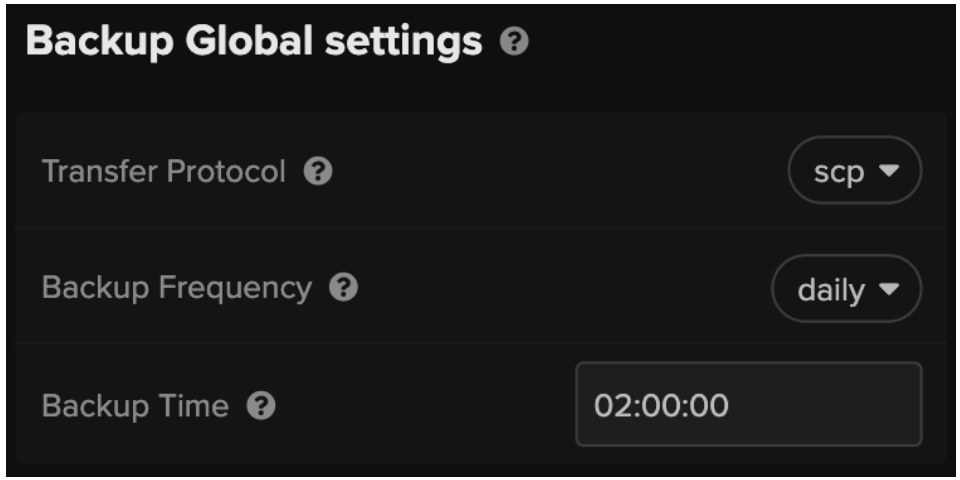


3. Turn on **Enable** in the top right to begin scheduled backup configuration and show new sections.



4. First, configure the settings under **Backup Global settings**. Select the transfer protocol from **SCP**, **SMB** or **S3**. Each protocol has different configuration requirements.

5. Choose the **frequency** of backups (weekly or daily) and set a **time** in UTC at which backups should be created (for example, 02:00:00)



The next steps for configuration are now dependent on the transfer protocol selected in step 3. Please proceed to configure SCP, SMB or S3.

Backup via SCP

Under "Transfer protocol settings", configure the SCP specific settings:

1. First, use **SCP Username** to enter a user to authenticate against for the server.

   The username may contain alphanumeric or specific special (_,.or-) characters. The first character must be alphabetical or _. Dollar characters ($) are not permitted.

2. In the **SCP Host** field, enter the IP address or hostname of the remote server intended to receive the backup files.

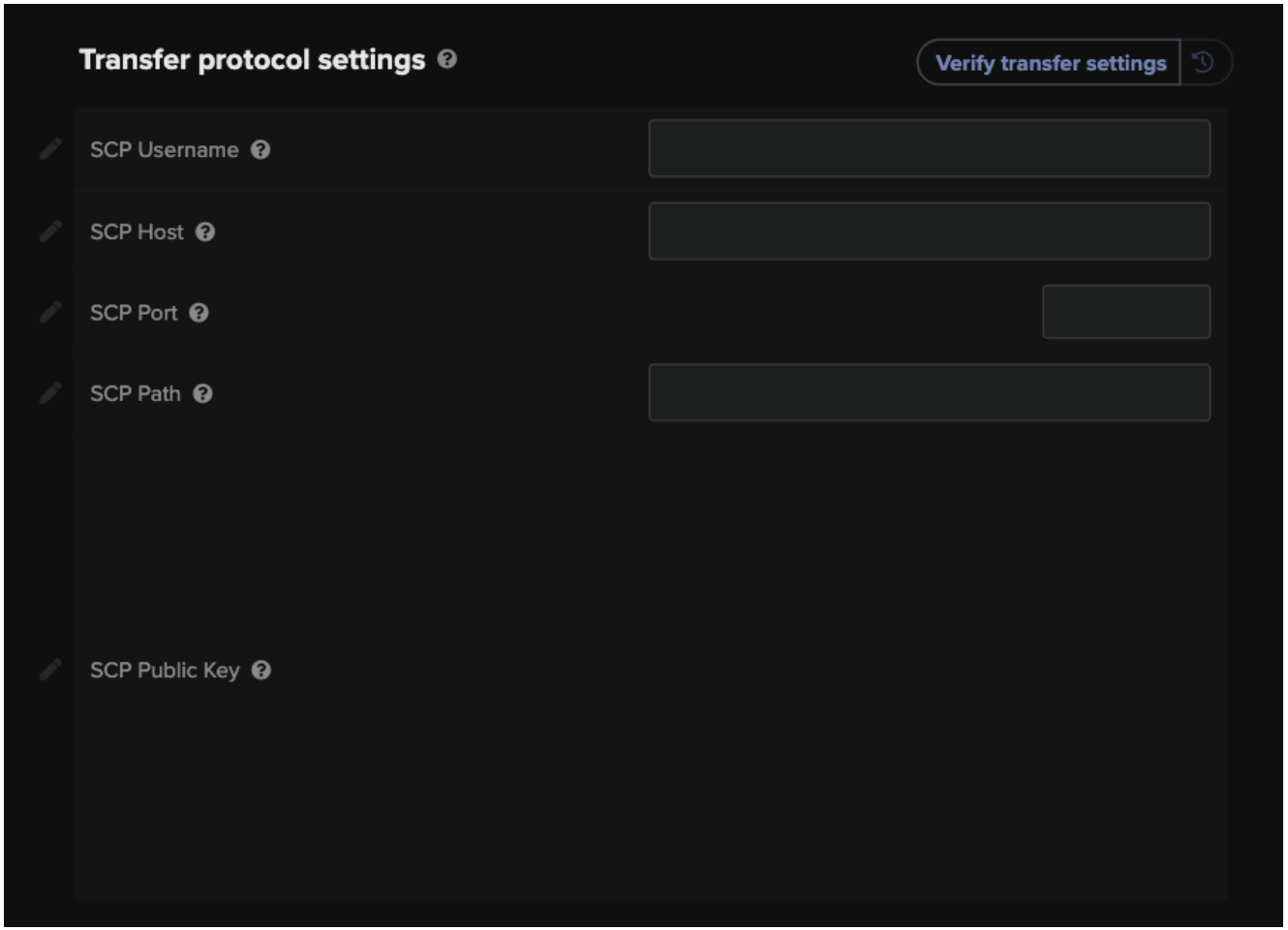
3. Enter a port on the backup server in the **SCP Port** field.

4. Enter an **SCP Path** on the server where the backup will be sent.

5. **Save** the changes.

6. Add the public key displayed in the **SCP Public Key** field to the .ssh/authorized_keys file for the configured user on the remote backup server.

7. Return to the System Config page and optionally test the configuration by clicking **Verify Transfer Settings**.



Backup via SMB

Under "Transfer protocol settings", configure the SMB specific settings:

1. First, use **SMB Host** to enter the IP address or hostname of the remote server intended to receive the backup files.

2. Under **SMB Share** enter the name of the share on the SMB server.

   This share name cannot contain the character \ followed by n and that it cannot start or end with / or \.

3. In the **SMB Username** field, enter a user to authenticate against for the SMB server.

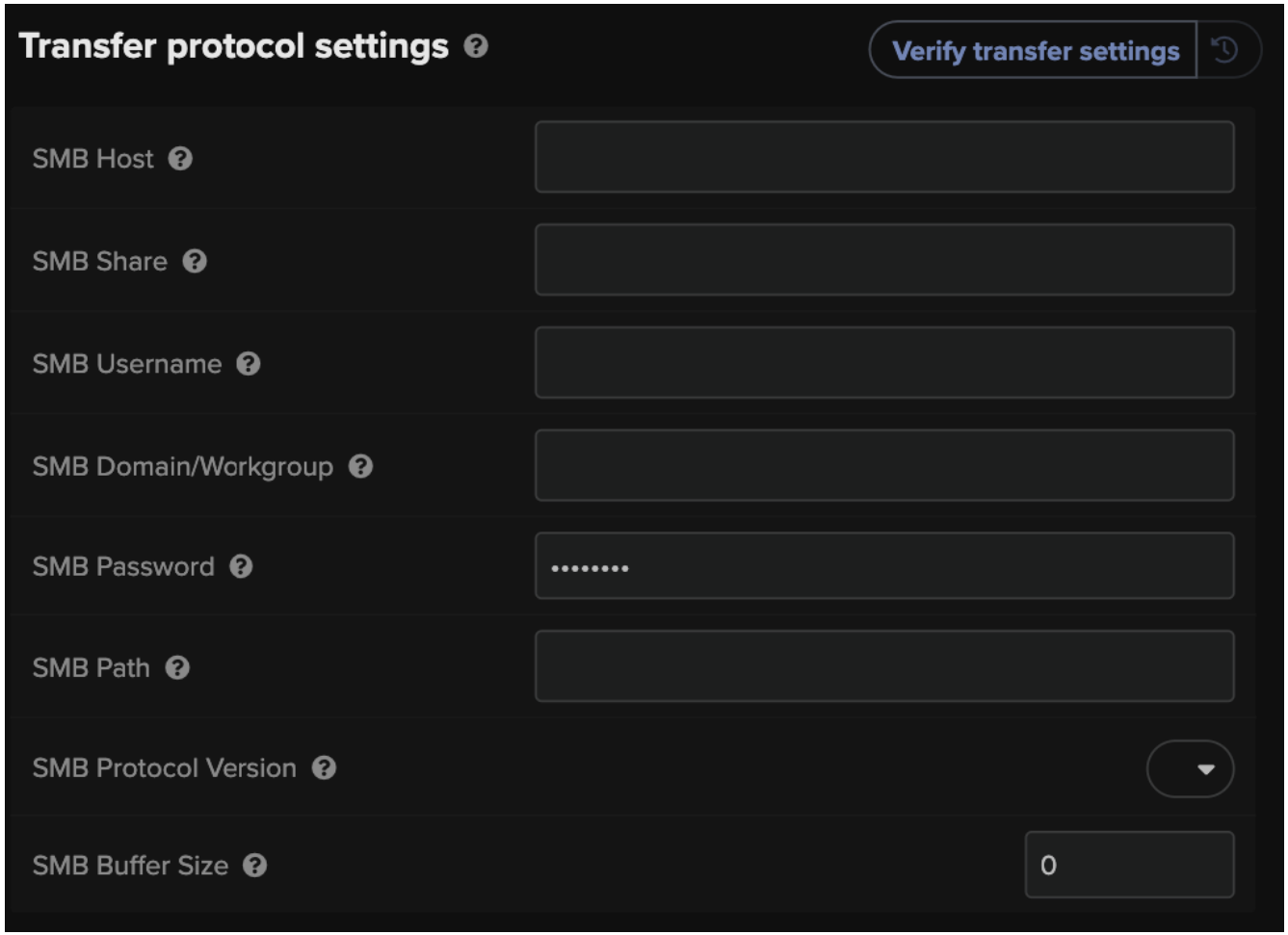
   The username may contain alphanumeric or specific special (_,.or-) characters. The first character must be alphabetical or _. Dollar characters ($) are not permitted.

4. Use the **SMB Domain/Workgroup** to specify the domain or workgroup that this user is a member of.

5. In the **SMB Password** field, enter a password for the user for authentication.

6. Set the **SMB Path** on the server where the backup will be sent.

   This path name cannot start with ./ please use / instead to denote the root of the share.



7. Select the maximum **SMB Protocol Version** - SMB1, SMB2 and SMB3 are supported. The use of SMB3 is recommended.

8. **Save** the changes and optionally test the configuration by clicking **Verify Transfer Settings**.

Backup via S3

Under "Transfer protocol settings", configure the S3 specific settings:

1. First, use **S3 Service URL** to enter the URL of the S3-compatible service intended to receive the backup files. Do not include the bucket name in the URL.

2. Provide an **S3 Bucket Name** where the backups should be stored.

3. Enter the **S3 Access Key** and **Secret Key** values for authentication.

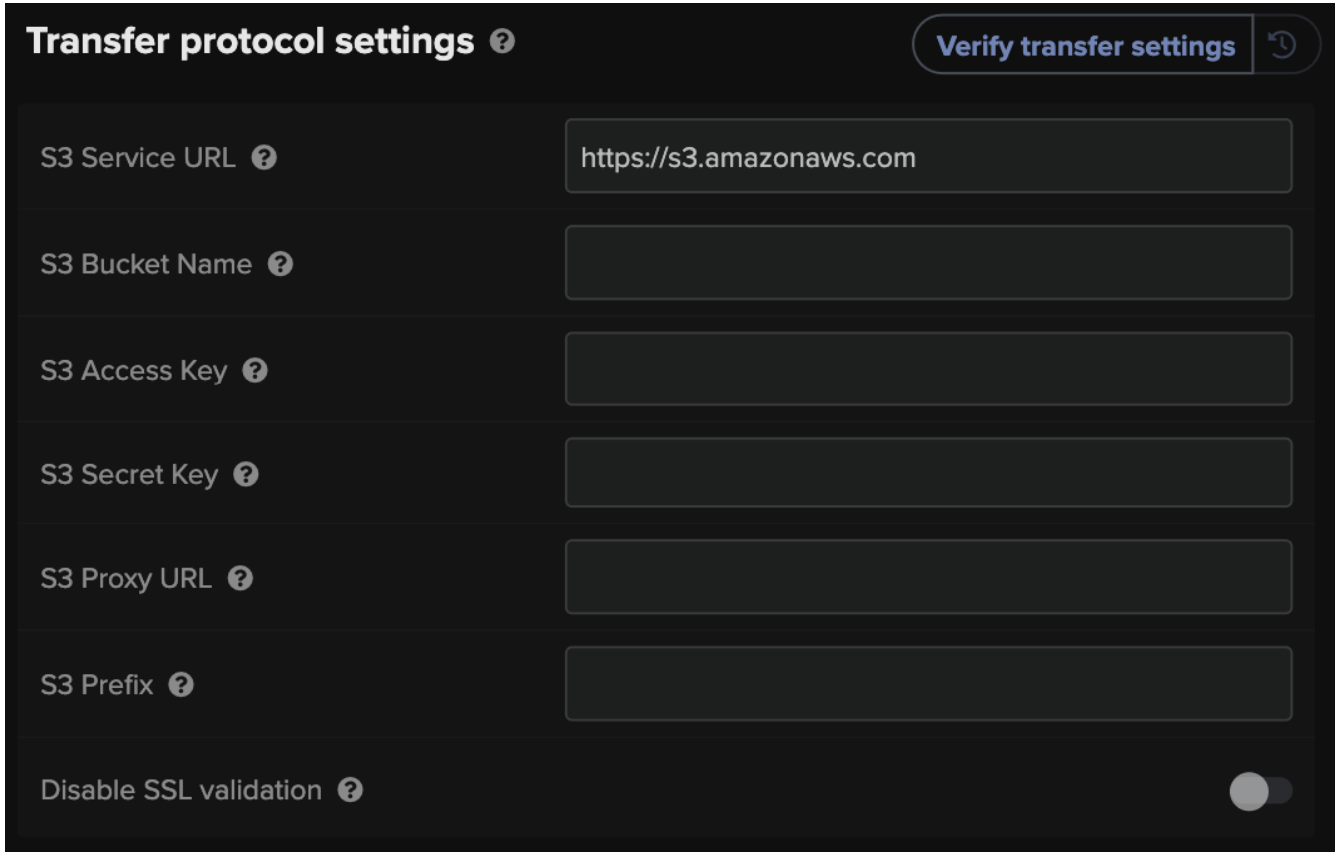
4. If a proxy is required to access the S3 service, enter the details in the **S3 Proxy URL**. Leave the field blank if no proxy is required.

5. Optionally add an **S3 Prefix** to specify the backup location within the bucket.

   If the backups are to be stored at the top level of the bucket, leave this field blank.

6. **SSL validation** can be optionally disabled if experiencing issues with self-signed certificates on a local S3 compatible service. SSL validation should not be disabled if a public S3 provider such as AWS or GCP is in use.

7. Finally, save the changes and optionally test the configuration by clicking **Verify Transfer Settings**.



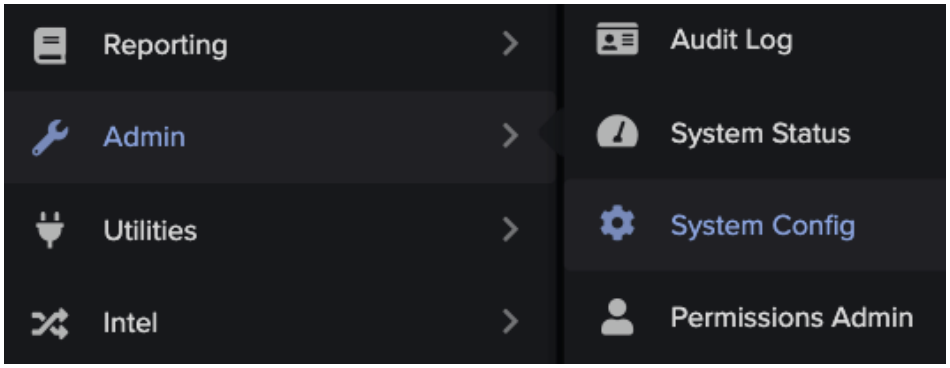
Note: Minimum IAM policies for AWS S3 backups and guidance on encryption are covered in Example IAM Policy for S3 Backups.

Scheduled Backup Email Notifications

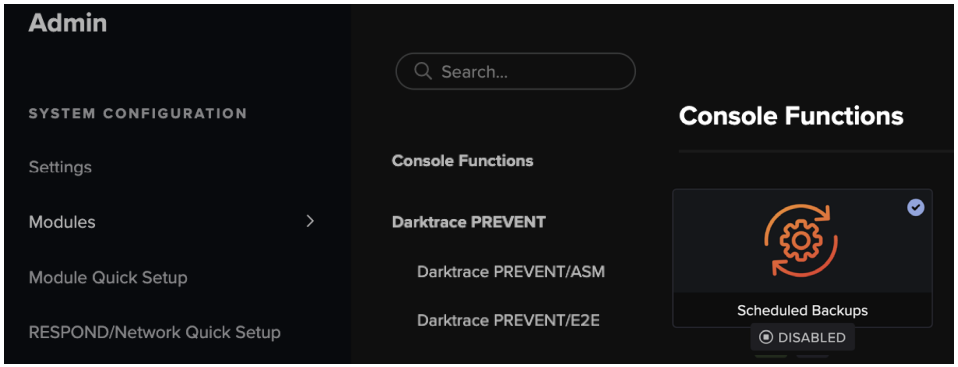
Darktrace provides the option to receive email notifications about the success or failure of daily scheduled backups. Scheduled backups must already be configured for email notifications to be set.

Darktrace Threat Visualizer 5.2 allows scheduled backups and scheduled backup alerts to be configured from the Threat Visualizer System Config page (physical appliances only) by users with the "System Admin" permission.

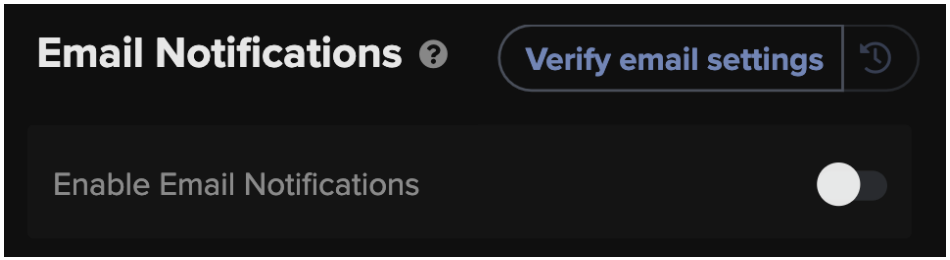
1. Open the Threat Visualizer and navigate to the **System Config** page (Main menu > Admin).



2. From the left-side menu, select **Modules**, navigate to the **Console Functions** section, and choose **Scheduled Backups**.



3. Scroll to the Email Notifications subsection and turn on **Enable Email Notifications** to reveal additional configuration fields.

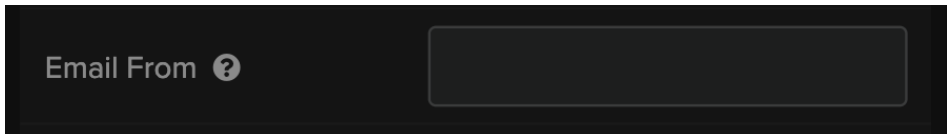


Note: By default, email notifications are sent when a backup fails.

4. Notifications can also be sent when a backup is successful. If this is desired, turn on **Email on success**.

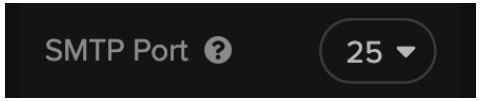
5. Enter an email address in the **Email To** field to receive notifications.

6. Optionally enter an email address in the **Email From** field to send notifications from.

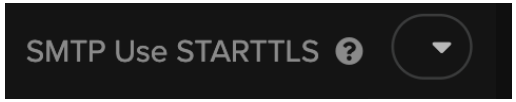


7. In the **SMTP Host** field, enter the hostname or IP address of an SMTP server to send emails via.

8. Select a port for SMTP in the **SMTP Port** option.

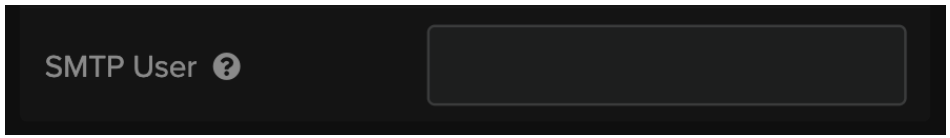


9. Choose whether STARTTLS is to be used using the **SMTP Use STARTTLS** drop-down menu.



   If "yes" is selected, STARTTLS will always be required. If "auto" is selected, STARTTLS will be used if available. If "no" is selected, STARTTLS will not be required.

10. The last field is the **SMTP User**. Enter a username to configure SMTP authentication. If entered, an additional password field will appear to complete.



11. **Save the changes**. Optionally send a test email to confirm the configuration process was successful.

Restore from a Backup

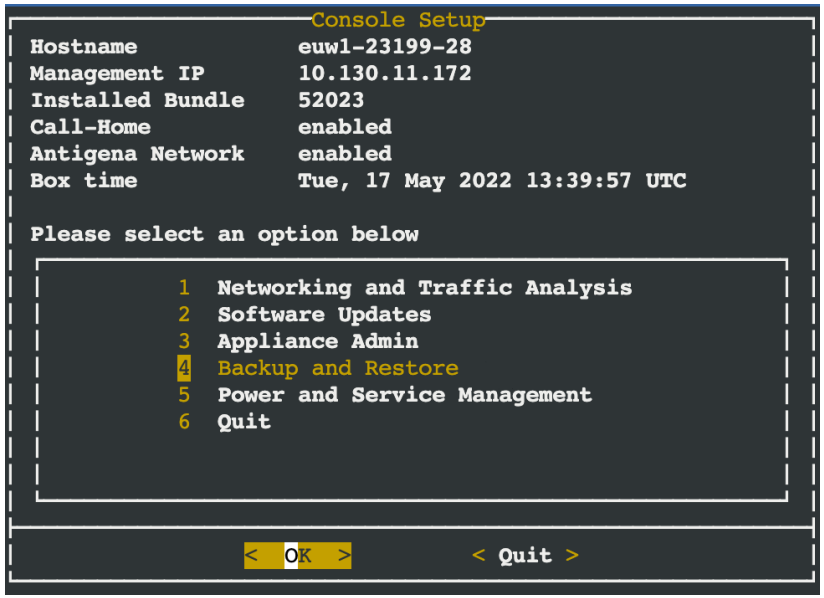
The option to restore from a backup is available in the console menu. Transactional data such as connections in the Event Log, Advanced Search entries, and PCAP files are not restored.

Before restoring from a backup, carry out the following:

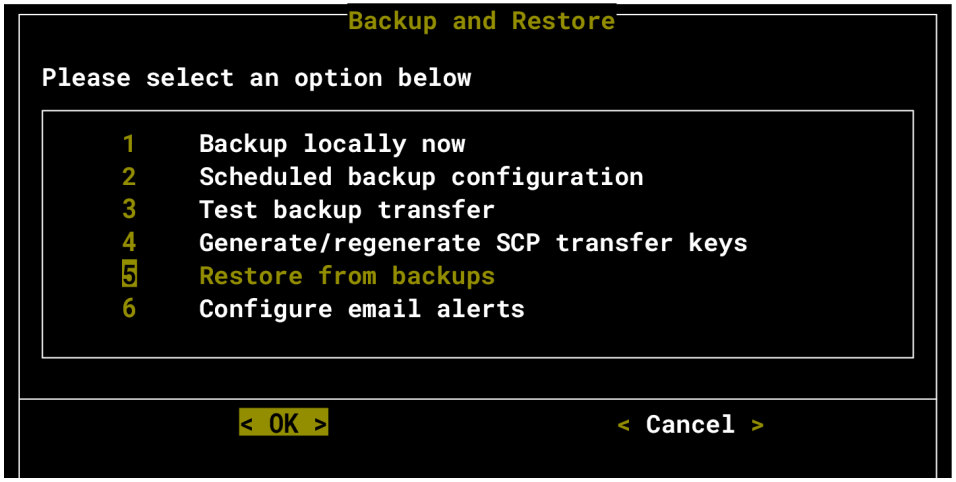
- Confirm the version of the appliance is the same as the backup file. These must be the same version.
- Upload the backup file to /files/upload in the transfer user directory via SFTP, if not done so when creating a backup.
- Make sure the appliance is no longer ingesting data. Unplug the cable(s) from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

To restore from a backup, perform the following steps:

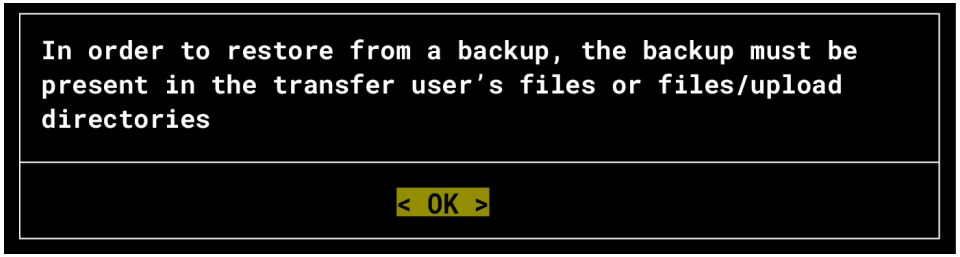
1. On the Master appliance, login to the **Console menu**, and select 4. Backup and Restore.



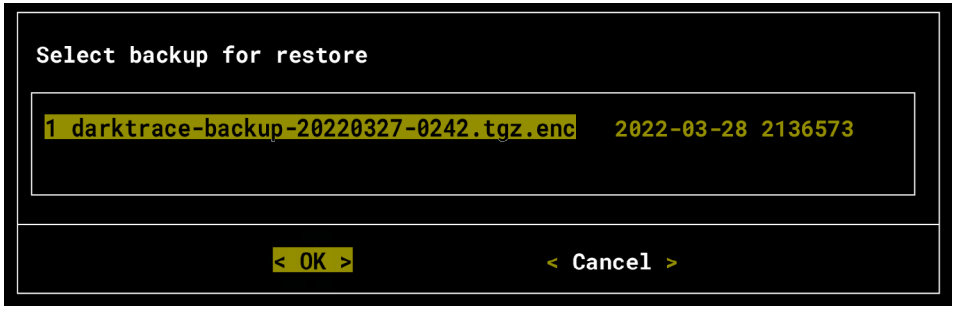
2. Then select option **5. Restore from backup**.



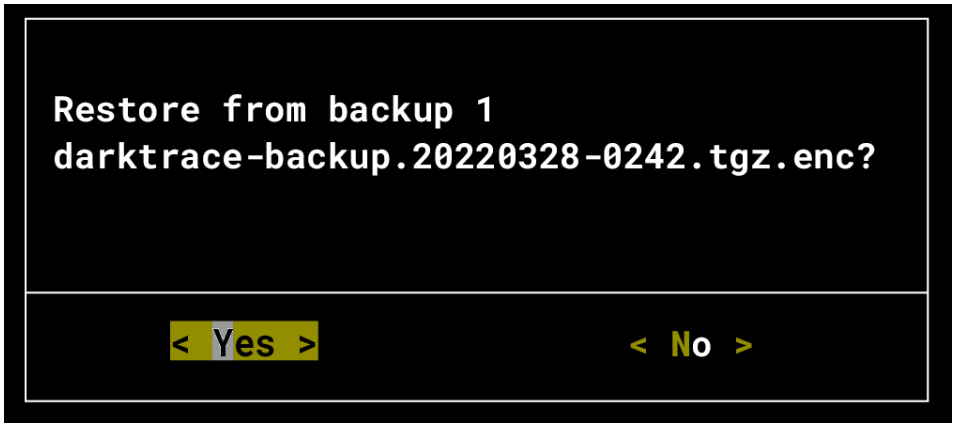
3. A **warning dialog** will open to explain that a backup must be present before a restoration can occur. Press **OK** to continue.



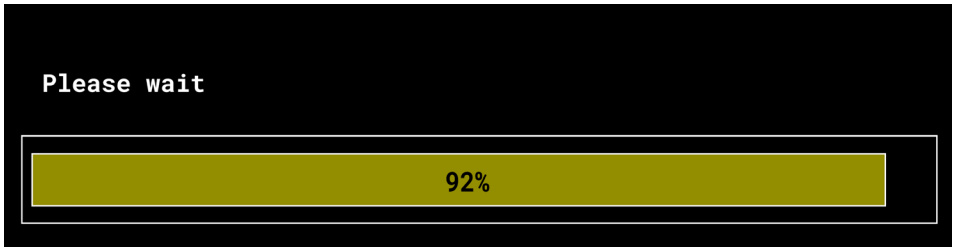
4. **Select** a backup to restore from the list.



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**.

Backing up and Restoring Chapter Test

Cyber Engineer Certification

This page will test your knowledge and check your understanding of the Backing up and Restoring Darktrace section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. Where can you create an immediate backup from?

- [ ] Threat Visualizer interface
- [ ] Console interface
- [ ] System > Config page

2. Which transfer protocol is NOT available for scheduled backups?

- [ ] S2
- [ ] S3
- [ ] SMB

3. Which permission do you need to enable email backup alerts?

- [ ] Device Admin
- [ ] Configuration
- [ ] System Admin

4. What is the default timezone for scheduled backups?

- [ ] GMT
- [ ] UTC
- [ ] CDT

5. Scheduled backups can also be configured from the console.

- [ ] True
- [ ] False

6. Which file directory should you upload a backup to before restoring from a backup?

- [ ] /files/backup
- [ ] /files/upload
- [ ] /files/restore

Clear All Answers

8. Upgrading Darktrace

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 the Darktrace Appliance

Upgrading to the latest version of the Threat Visualizer application is quick and easy.

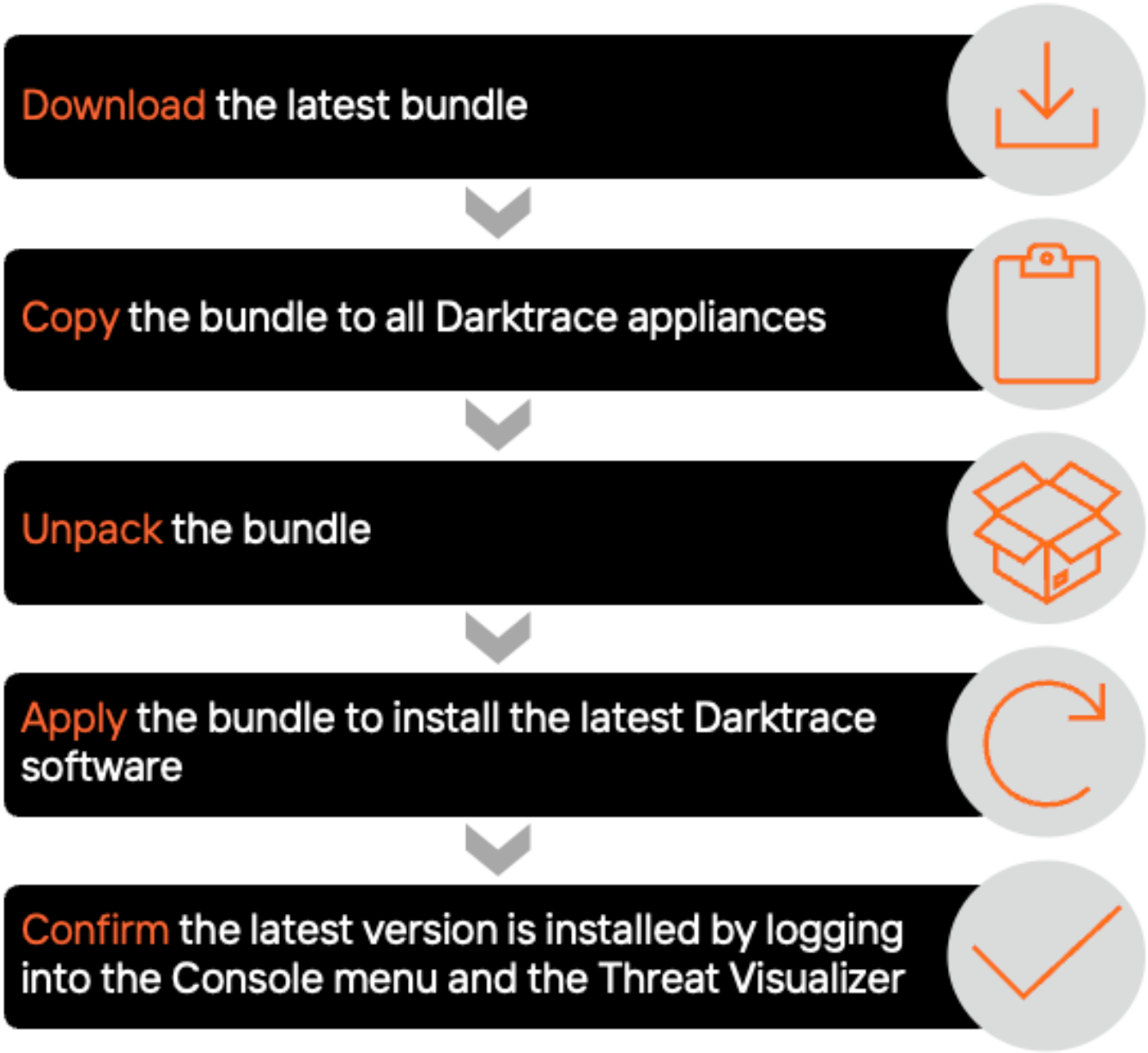
Review the summary of the steps presented on the right-hand side.

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.

When upgrading an appliance, we need to consider the types of bundle file, the download methods for bundle files and the upgrade procedure.

These considerations are outlined in the next three subsections.



Types of Bundle File

There are two 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:

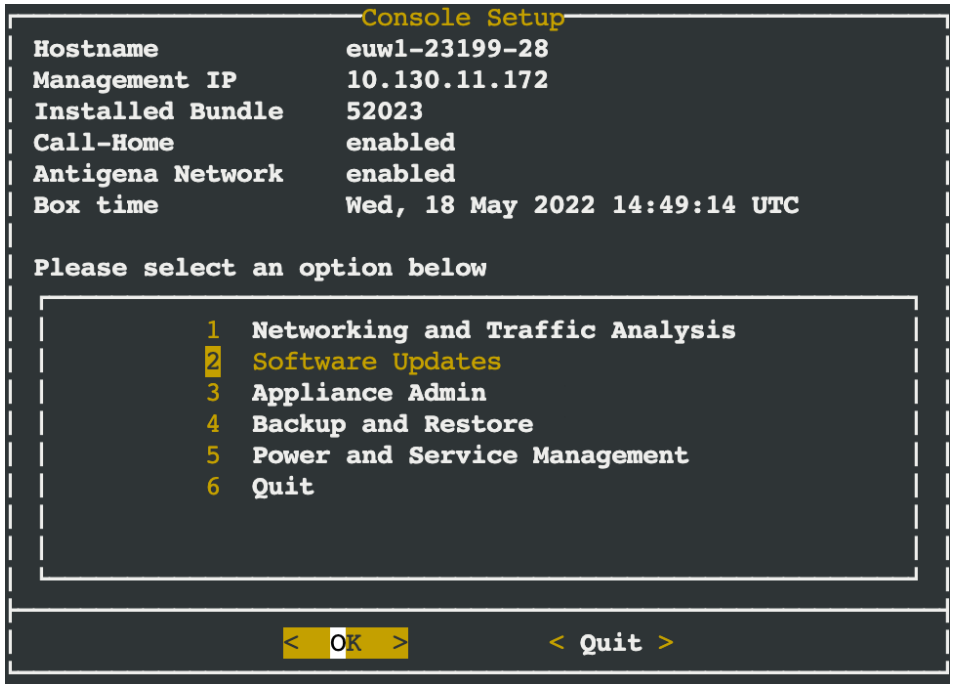
2 Software Updates > Guided mode > 1 Check for updates now
Customer Portal

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.

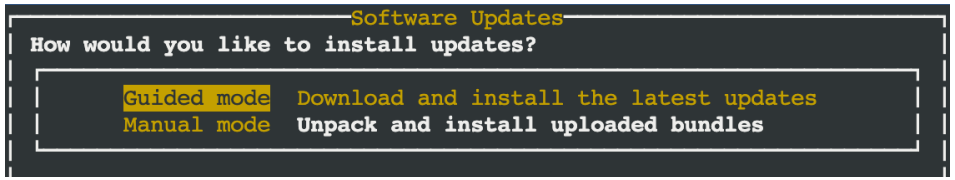
Upgrade Procedure

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.

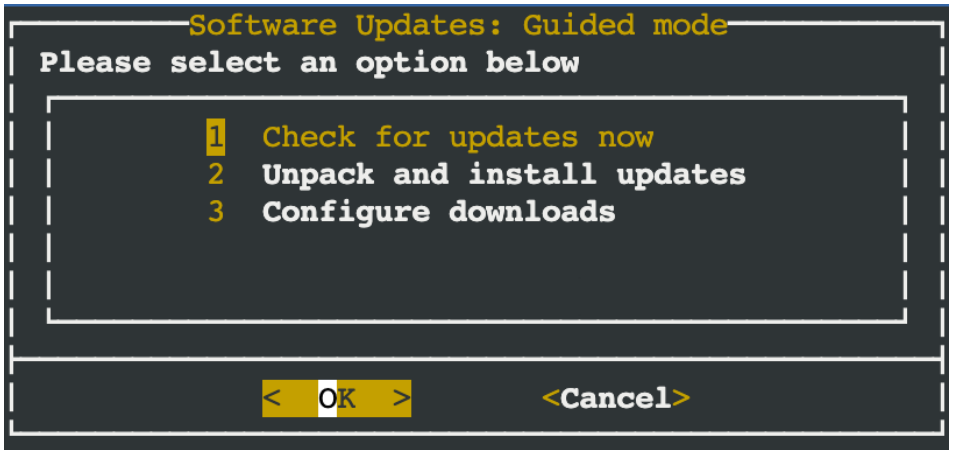
1. Log in to the Console menu and select "**2 Software Updates**".



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



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



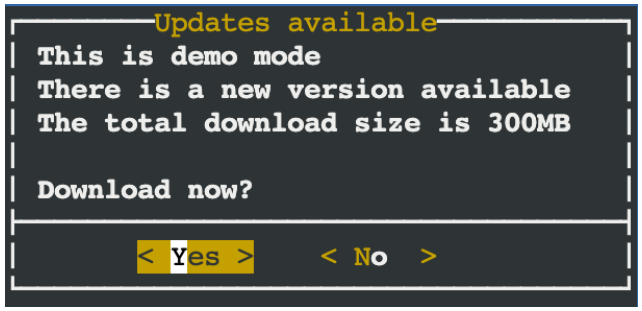
"1 Check for updates now" will check if there are any new available updates. If an update is available it will download and proceed to unpack and install it, prompting before each step begins.

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

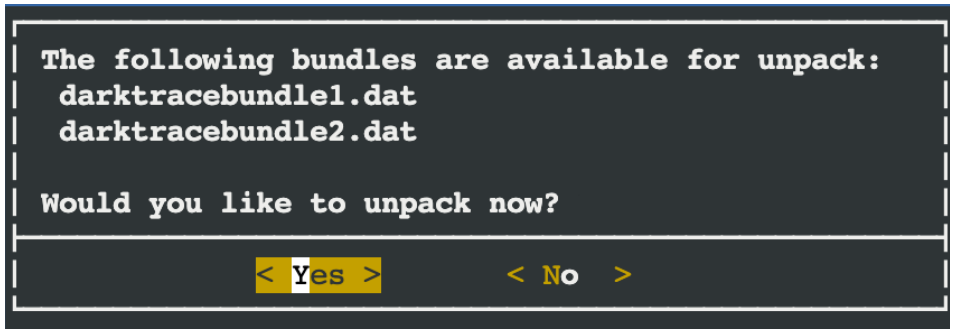
"3 Configure downloads" allows you to select how you would like to fetch the latest bundles. Disable this option if you do not wish to use this feature. Please refer to the previous subsection of **Download methods of bundle files**.

4. If updates are available, a window will show the download size and ask if it should be downloaded now.

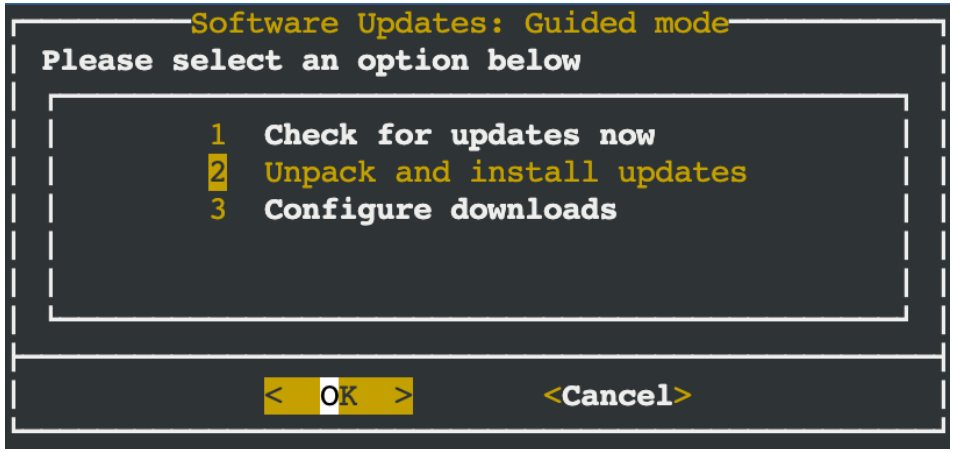
   Click **Yes** to download.



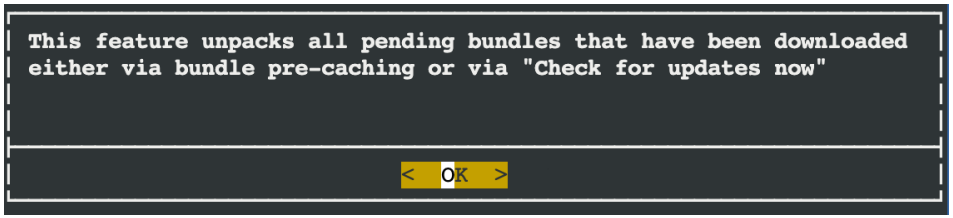
5. After choosing whether to download, available bundles that can be unpacked will be listed. Select **Yes** to unpack now.



6. Updates can also be unpacked from option 2 of Guided mode, **Unpack and install updates**.

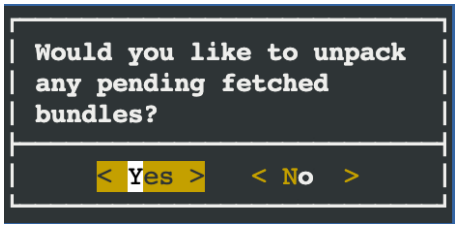


7. A message appears informed the operator that **all pending bundles** will be unpacked, including those found in the check for updates stage. Click **OK** to dismiss.

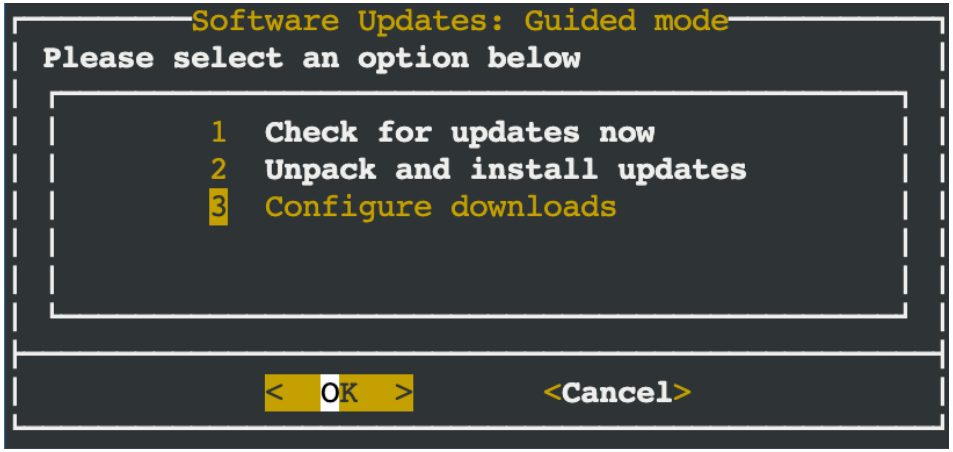


8. Then, the operator will be asked if they would like to unpack any pending fetched bundles.

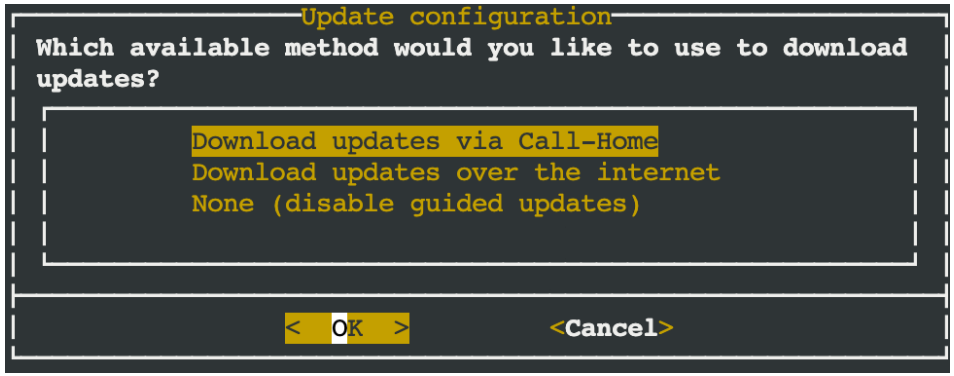
   Click **Yes** to proceed.



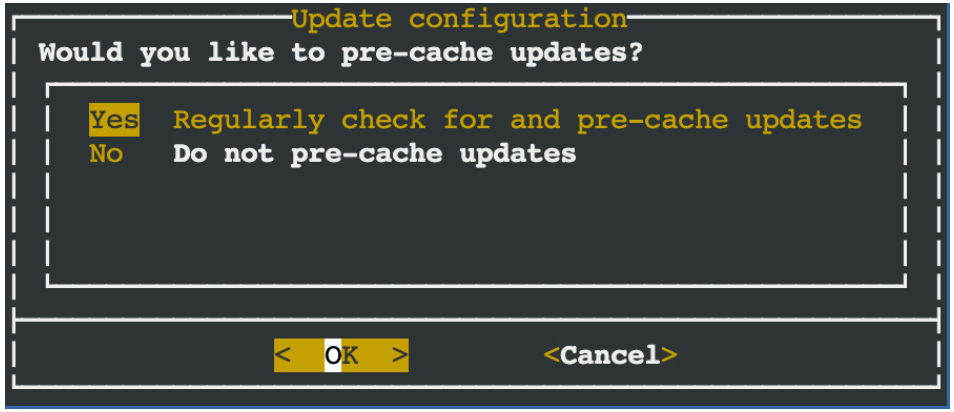
9. In order to install updates, it is important to configure the downloads. Select option **3 Configure downloads** from the Software Updates: Guided mode menu.



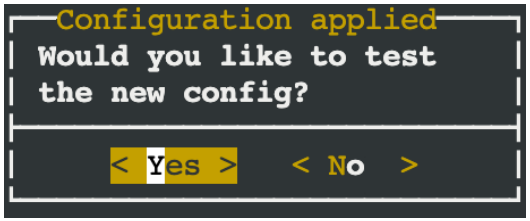
10. Downloads can be carried out using different methods. If Call-Home is available, select **Download updates via Call-Home**.



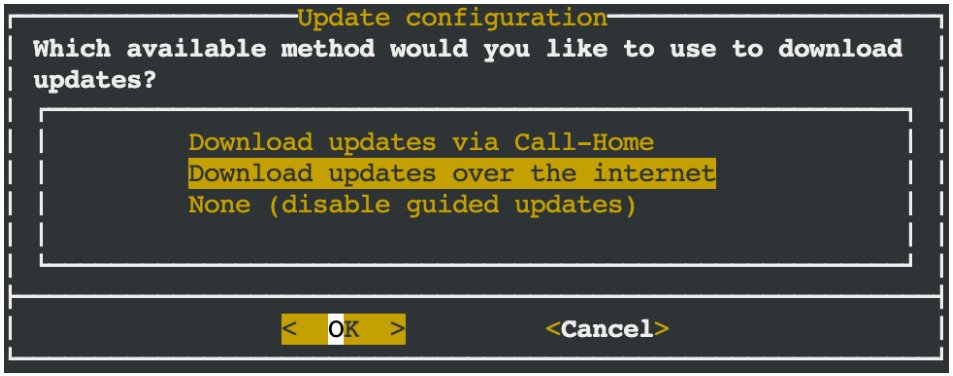
11. At this stage, there is the option to **pre-cache updates**. Select **Yes** or **No**.



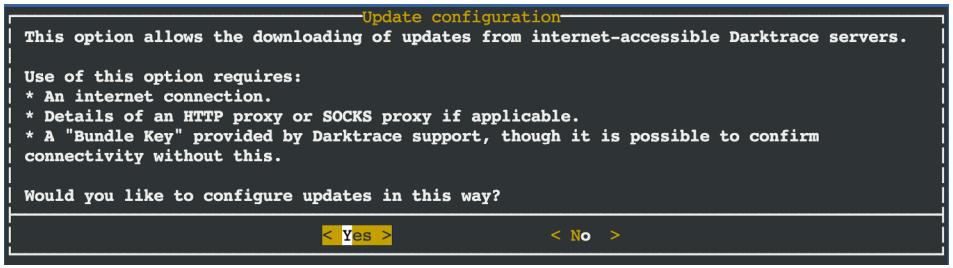
12. After selecting an option and changing the configuration, click **Yes** to **test the new config**.



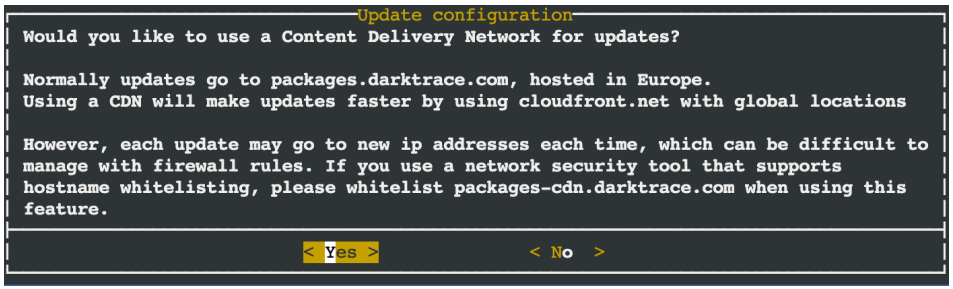
13. For some deployments, Call-Home is not suitable. Instead, the guided option **Download updates over the internet** might be more relevant.



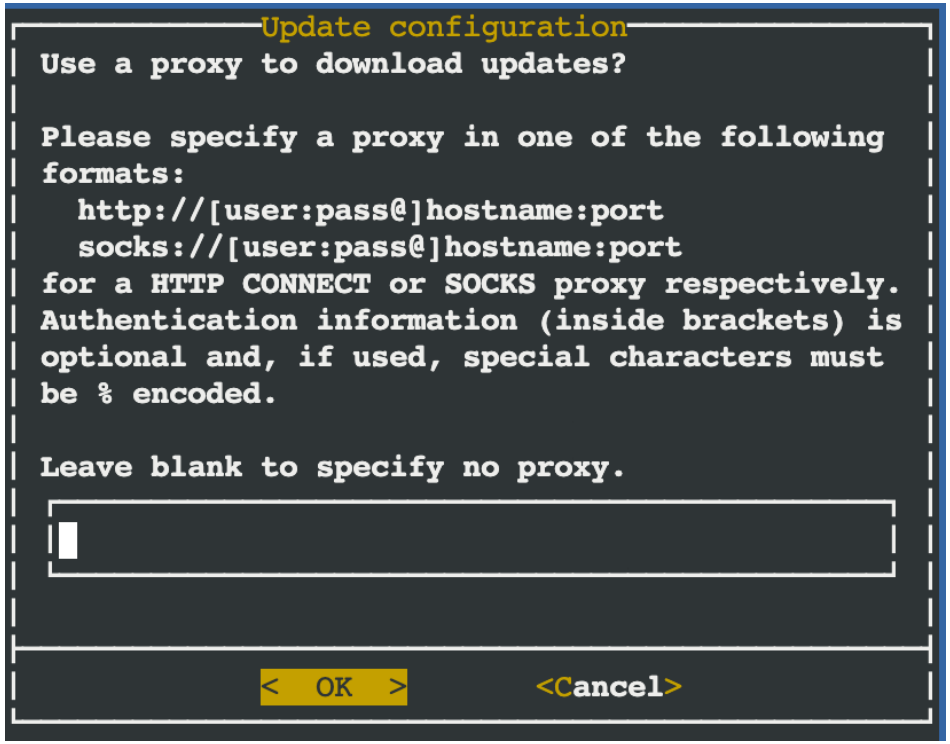
14. Before continuing, a message will appear letting the operator know what is required for downloading updates over the internet. If all of these requirements can be fulfilled, click **Yes** to **configure updates in this way**.



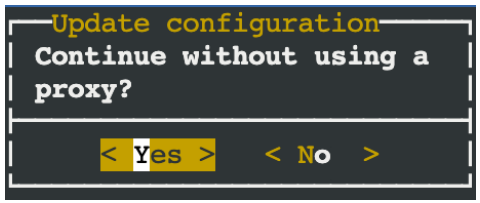
15. Next, the operator will be asked if they would like to use a **Content Delivery Network** (CDN) for these updates. Choose an appropriate response to continue.



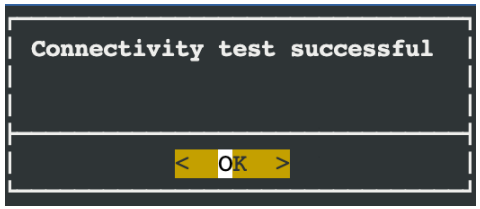
16. As prompted by the Console interface earlier, **proxy details** might be needed if applicable. If there is a proxy, input the details. If not, leave blank and click **OK** to continue.



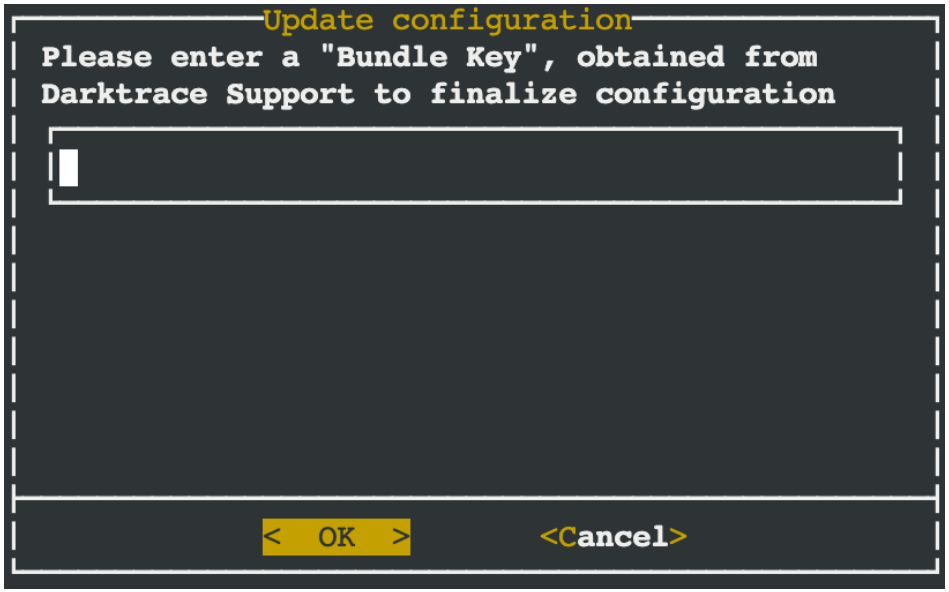
Note: If no proxy is specified, a message will pop up asking the operator to confirm that the process can be continued without using a proxy. Click Yes to proceed and No to return to the previous window and input relevant details.



17. Continuing will test the connectivity. If successful, a **Connectivity test successful** message will be displayed.



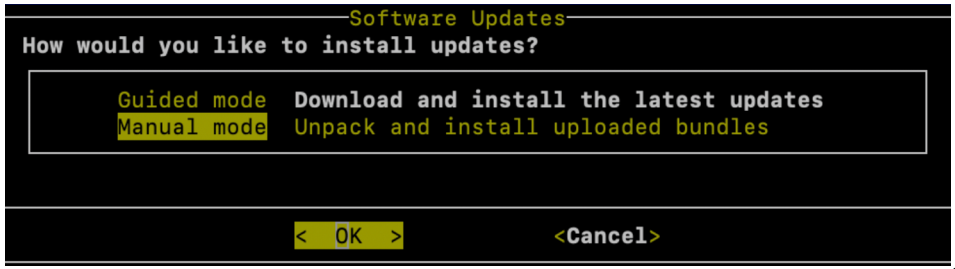
18. Finally, input a "**Bundle Key**" to finish the configuration. This key can be obtained from Darktrace Support.



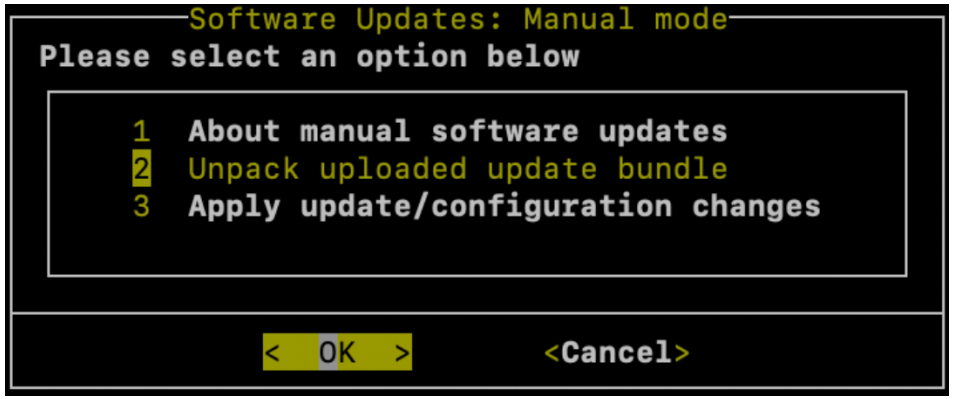
19. After completing this configuration step, downloads can be carried out using guided mode either via Call-Home or over the internet.

Note: If Manual mode is preferable, review the next few steps leading up to verifying a successful download in the Console Interface and System Status page.

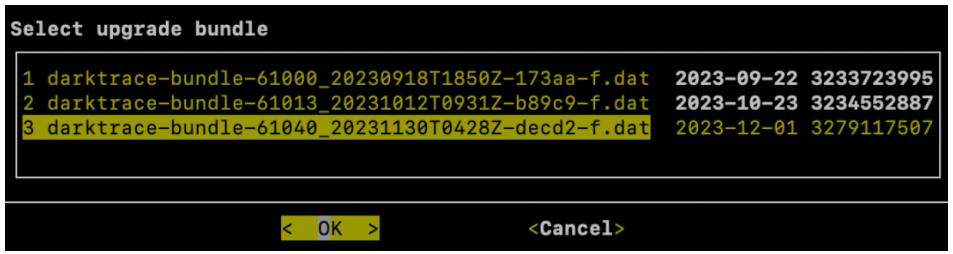
20. **Manual Mode** requires further operations to unpack the downloaded bundle and then install it.



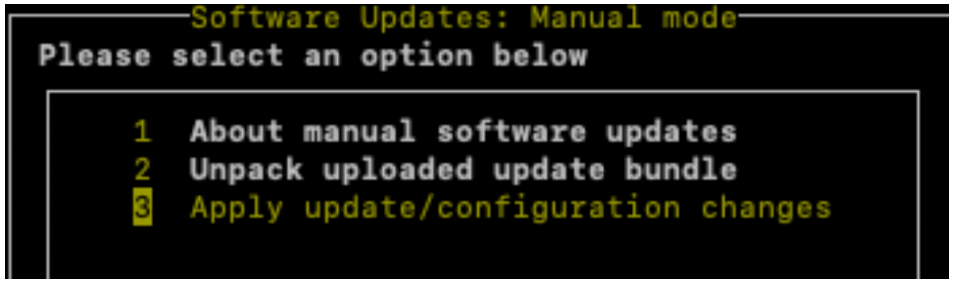
21. In the Manual Mode submenu, select **"2 Unpack uploaded update bundle"** to show the list of the available bundles stored in the appliance.



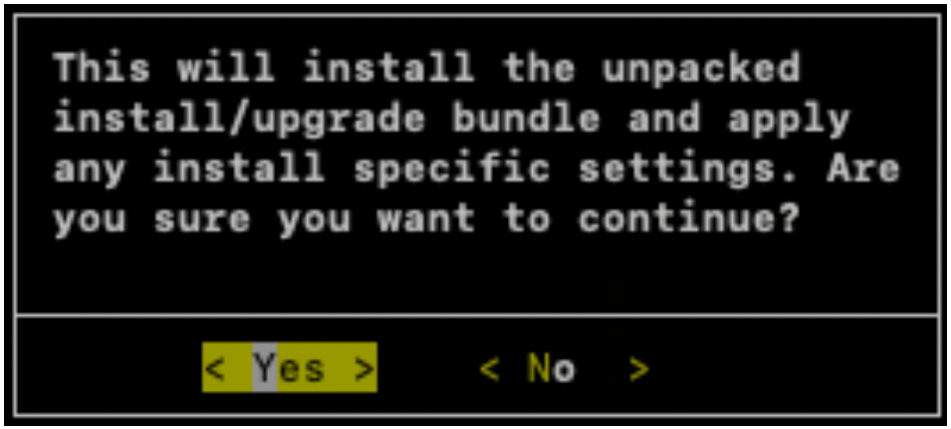
22. Select the newest bundle to install. The latest bundle is always at the bottom of the list. Press **OK** to continue. Then choose **Yes** to proceed. It can take some time for the unpacking operation to complete.



23. Once unpacked, select **3. Apply update/configuration changes**. Select **Yes** to proceed with update.

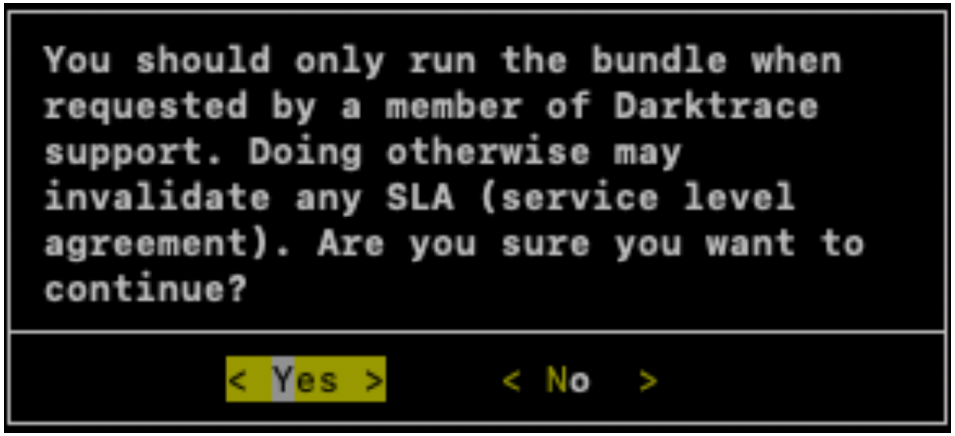


24. A message will be displayed asking for confirmation. Confirm you wish to continue by selecting **Yes**.

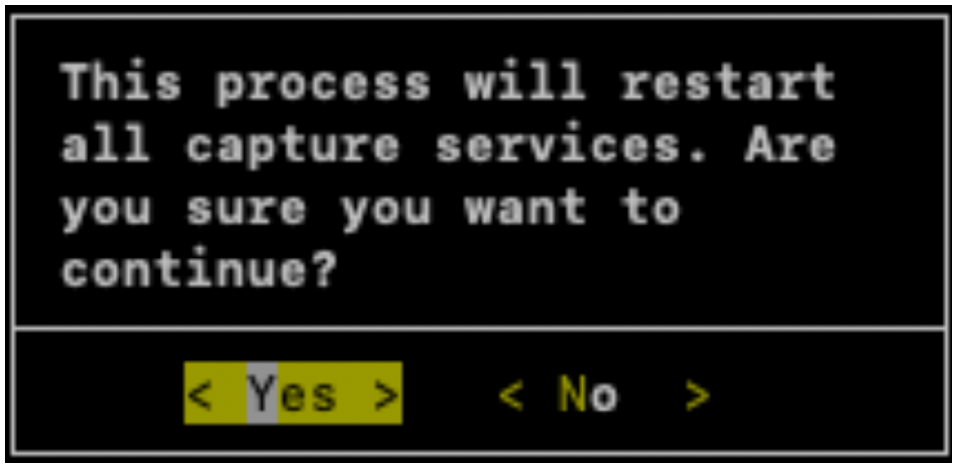


Note: If an error occurs, try applying the latest changes a second time.

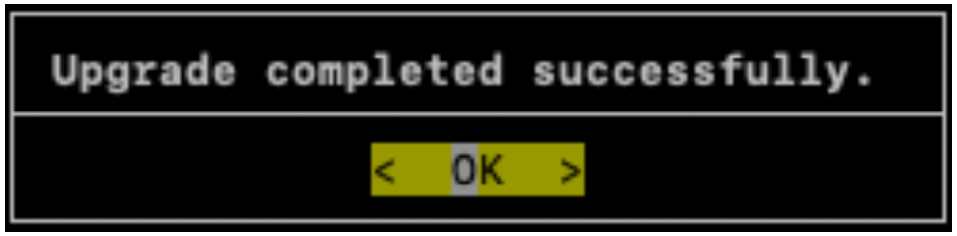
25. A message will appear to make sure the bundle has been requested by a member of Darktrace support. Press **Yes** to continue.



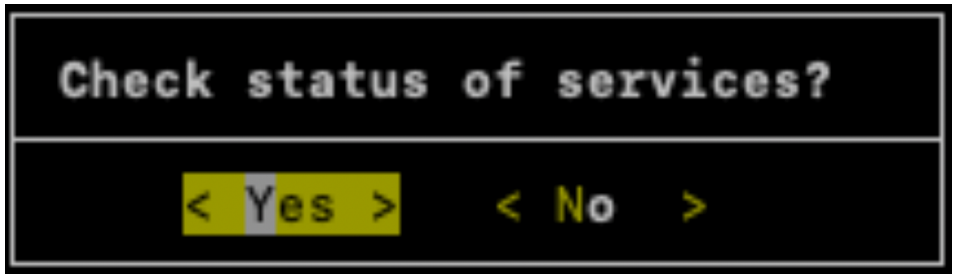
26. A final message will appear. Again, press **Yes** to continue. The update process will begin and a progress bar will be displayed on screen.



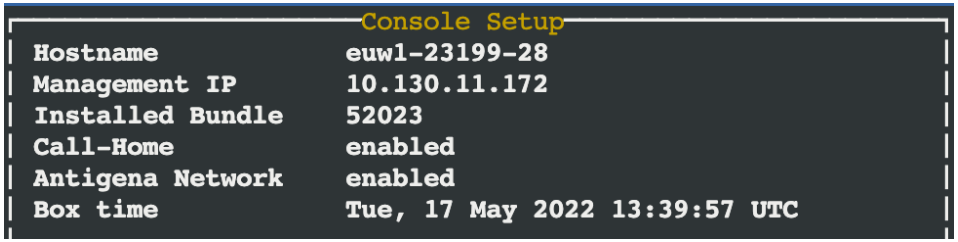
27. When finished and an **Upgrade completed successfully** message appears, press **OK** to complete the upgrade.



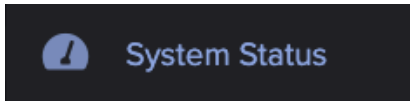
28. You are prompted whether to **check the status of the services**. Select **Yes** if you wish to do so.



29. At the end of the upgrade proceedure, you will be **logged out** of the Console. **Login** to the Console menu again to **confirm** that the software version has been updated by checking the **Installed Bundle** value.

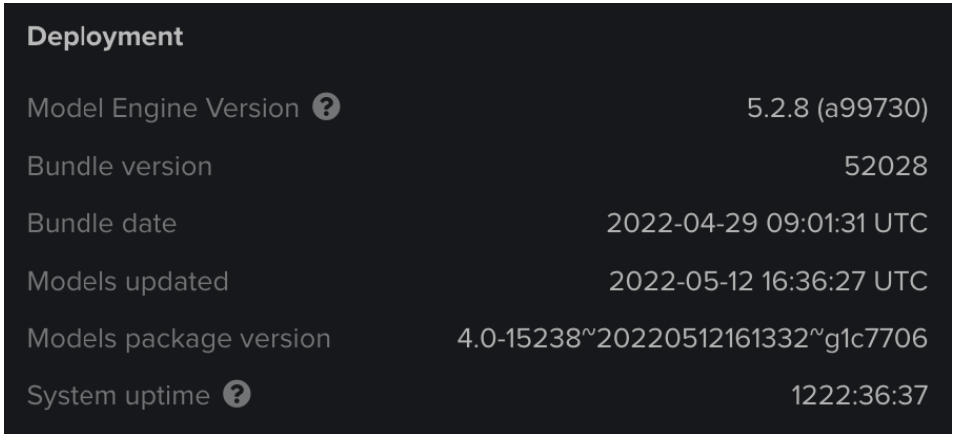


30. Login into the Threat Visualizer web application and navigate to **Admin** > **System Status** under the main menu.



Select an appliance from the **Deployment Health** 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.

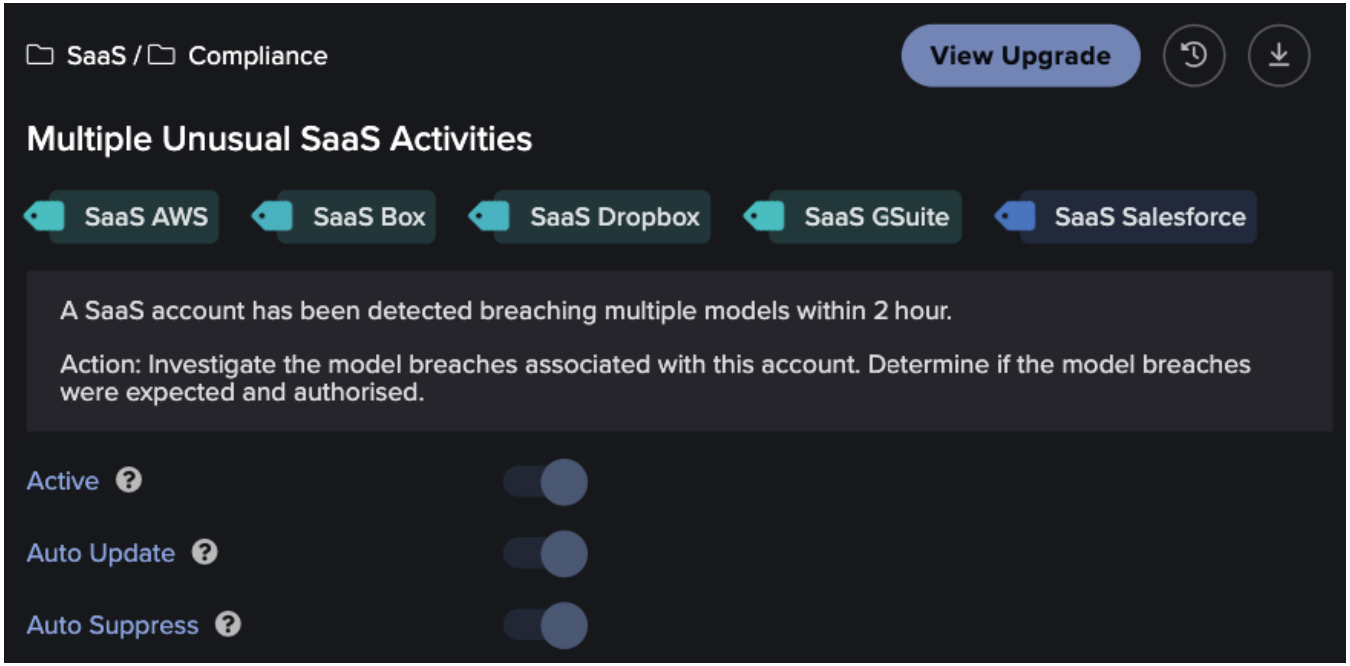


Upgrading Darktrace Models

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.

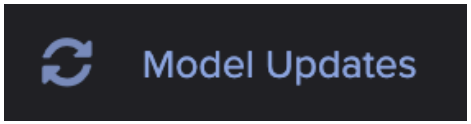
1. View any Model in the Threat Visualizer Model Editor. Note the **Auto Update** function. When set to **Yes**, this will automatically upgrade to the latest version when it is released.

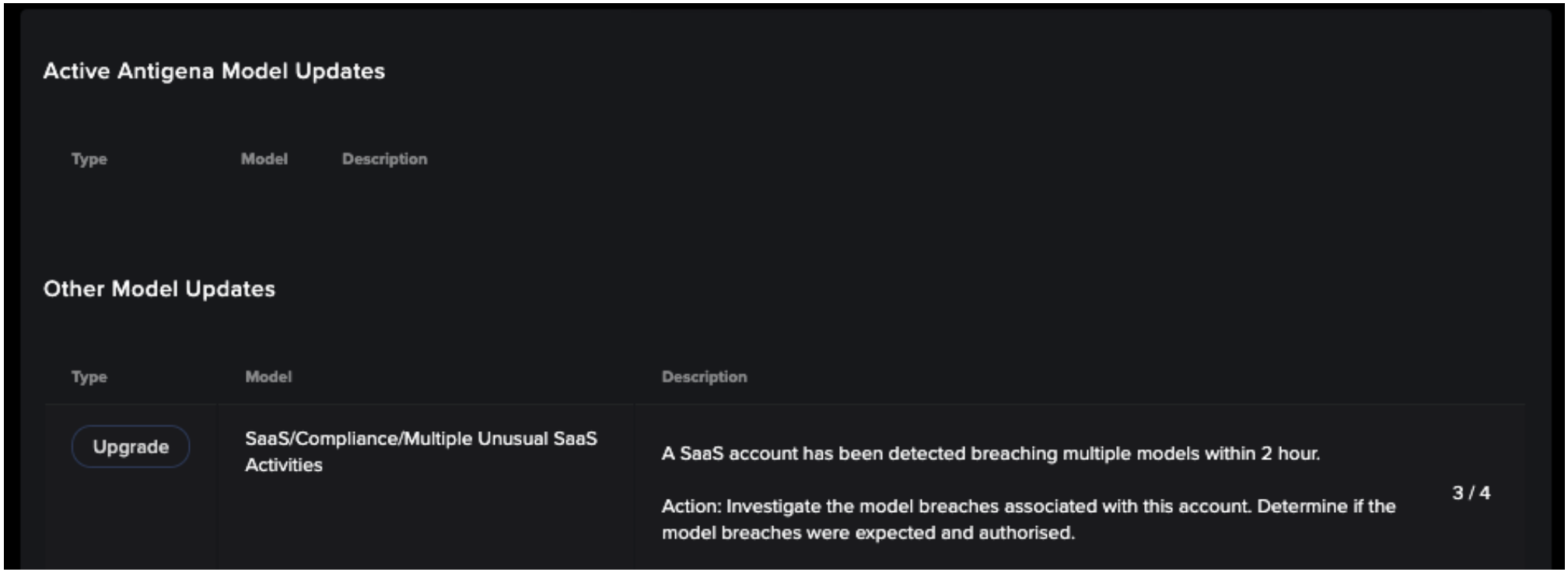
   However, if a Model has been edited, the updates will not overwrite the Model unless the user decides to accept the upgrade. If an edited Model has an available update, there is the option to **View Upgrade**.



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** which are available for review. Any new Models created or duplicated will not be impacted by automatic updates. Clicking this notification will redirect the user to the Model Updates page.

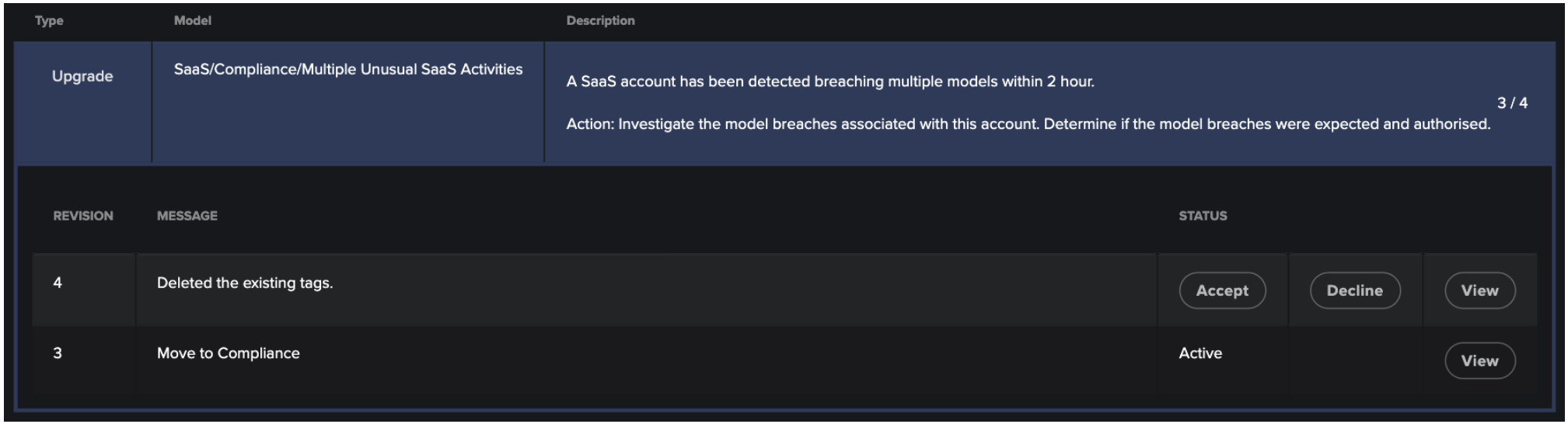
2. The Models Updates page lists all Models which have been customized but have new updates available. This view is also available by selecting the **Model Updates** button under Models from the Threat Visualizer Main Menu.



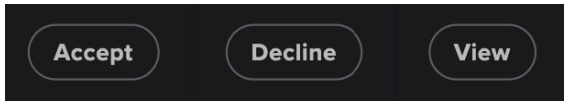


3. If reviewing individual Models is not required, Models Updates can be applied in bulk by clicking **Accept All**.

2. Click on a **Model row** to reveal more options.



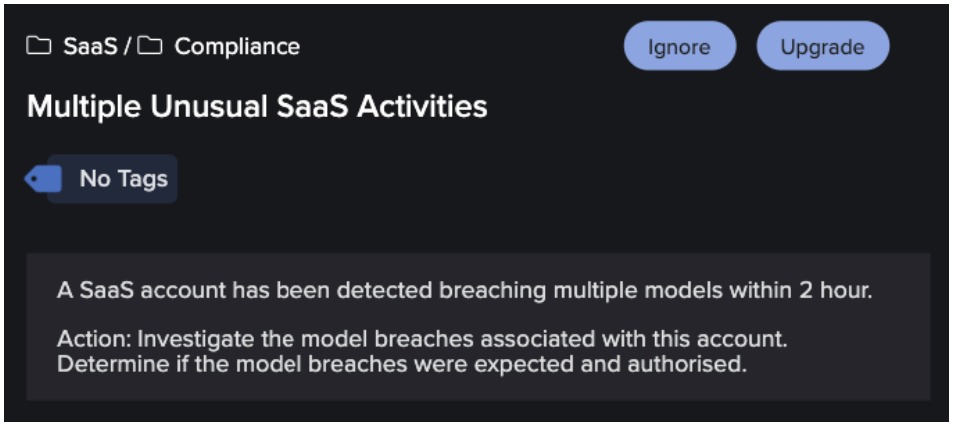
a. Each conflicting Model is listed in a separate row with options to **Accept**, **Decline** or **View** them.



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.

3. 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.



Upgrading Darktrace Chapter Test

DARKTRACE
Cyber Engineer Certification

This page will test your knowledge and check your understanding of the Upgrading Darktrace section. This is the perfect way to work towards your **Darktrace Cyber Engineer Certification**! *Select an answer by clicking on it. Wrong answers are denoted by a red cross and right answers are denoted by a green tick.*

1. Which type of package can be applied on an older version?

- [ ] Full Package
- [ ] Differential Package
- [ ] Both Packages

2. Which configuration allows automatic upgrade downloads?

- [ ] Call-Home
- [ ] Backups
- [ ] Automatic upgrades

3. Which protocol is used when you login as the transfer user?

- [ ] SMB
- [ ] FTP
- [ ] SFTP

4. Which of the below is NOT a software update mode?

- [ ] Guided Mode
- [ ] Manual Mode
- [ ] Independent Mode

5. Updates to Models are automatically delivered on a daily basis.

- [ ] True
- [ ] False

6. Model updates CANNOT be ignored.

- [ ] True
- [ ] False

Clear All Answers

9. Learning Outcomes

Course Agenda Checklist

Thank you for completing this Threat Visualizer Administration course.

We hope this have given you the confidence to tackle a variety of administrative and configuration aspects using the Threat Visualizer for your deployment.

Contact Us

For all further education inquiries, contact:

EMEA: training-emea@darktrace.com
APAC: training-apac@darktrace.com
AMERICAS: training-amer@darktrace.com

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

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

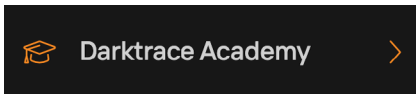
Complete the learning outcomes checklist below:

- [ ] **Optimize devices and configure subnets**
- [ ] **Enhance device tracking configurations**
- [ ] **Assign permissions and groups to users**
- [ ] **Configure LDAP, SSO, and HTTPS Certificates**
- [ ] **Deploy Cloud/SaaS Security Modules**
- [ ] **Create and restore from backups**
- [ ] **Upgrade the Darktrace Appliance and Model Deck**

10. Additional Educational Material

Darktrace Academy Training Resources are designed to maximize your practical skills, understanding, and confidence using Darktrace products. They are available on the Customer Portal at: https://customerportal.darktrace.com/

To access the Training Videos, Courses, and Certification, navigate to Darktrace Academy, and to the resources you require.



Training Courses

We have a wide range of Training Courses available, in multiple languages, all of which are complimentary for our Customers and Partners.

COURSE	AUDIENCE
Darktrace PREVENT/ASM	All end users
Darktrace PREVENT/E2E	All end users
Threat Visualizer Part 1 - Familiarization	All end users
Threat Visualizer Part 2 - Investigation	All end users
Darktrace HEAL	All end users
Cyber Analyst Part 1 – Advanced Analysis	Super Users (Tier 2 Analysts)
Cyber Analyst Part 2 – Model Optimization	Super Users (Tier 2 Analysts)
Cyber Engineer	Partners / Installers
Threat Visualizer Administration	Administrators
Darktrace RESPOND/Network	Administrators and Analysts
Darktrace/Email Part 1 - Familiarization	Email Administrators and Analysts
Darktrace/Email Part 2 - Customization	Email Administrators
Darktrace/Apps	All end users

Training Videos

Our new self-access Training Videos can be accessed at any time to support your learning.

Darktrace Certification

Darktrace offers Customers and Partners who have attended the appropriate webinars and passed the attendance tests, the opportunity to become officially Darktrace certified through multiple certification paths, as shown below.