DARKTRACE

CYBER ENGINEER

Training Manual

Darktrace Cyber Engineer

Training Manual
v2.1.1
Darktrace Version 5

Table of Contents

Table of Contents

1. Learning Objectives

Course Agenda

This course outlines how to install, configure and deploy Darktrace's Cyber AI Platform.

It is designed for an audience interested in the installation and implementation of Darktrace, including IT Security Manage, It Security Architects, Engineers and Darktrace Partners.

The following document serves an educational guide for the key elements of the Darktrace Console with respect to configuring Darktrace appliances.

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

- **Understand how components are employed for varying deployment scenarios**
- **Have knowledge of how to size a Darktrace installation**
- **Navigate the Darktrace Console**
- **Connect and configure the appliance to ingest traffic**
- **Review the System Status in the Threat Visualizer and Advanced Search**
- **Describe how to configure vSensors, osSensors, and cSensors**
- **Understand how to install Darktrace Terminal Service Agents (TSAs)**
- **Deploy Darktrace as a Managed Security Service Provider**

2. Architecture and Deployment

Darktrace can be deployed to cover a variety of network architectures. It does not matter if a network is physical, virtual, cloud-based, or even a hybrid - Darktrace can provide visibility in all coverage areas. This chapter outlines how Darktrace can be installed and what components may be necessary for different scenarios.

Network Architecture

The type of Darktrace appliances needed to achieve full visibility for an organization will completely depend on the network architecture. It is important to take note of how different appliances and sensors can be used to shine a light into all corners of the network.

Darktrace Appliances

For on-premise installations, Darktrace will ship an appliance. These are available in different sizes depending on the performance required, specifics of which can be found in the *Darktrace Appliance Specifications* Technical Brief. Darktrace appliances are highly tuned, high performance pieces of hardware that host the Darktrace platform including the Threat visualizer and Advanced Search interfaces.

The appliance passively monitors network traffic and operates at the core of a network such as at a central switch. The ingestion of network data is typically performed by one of three methods, although depending on infrastructure and the environment, there may be other options available.

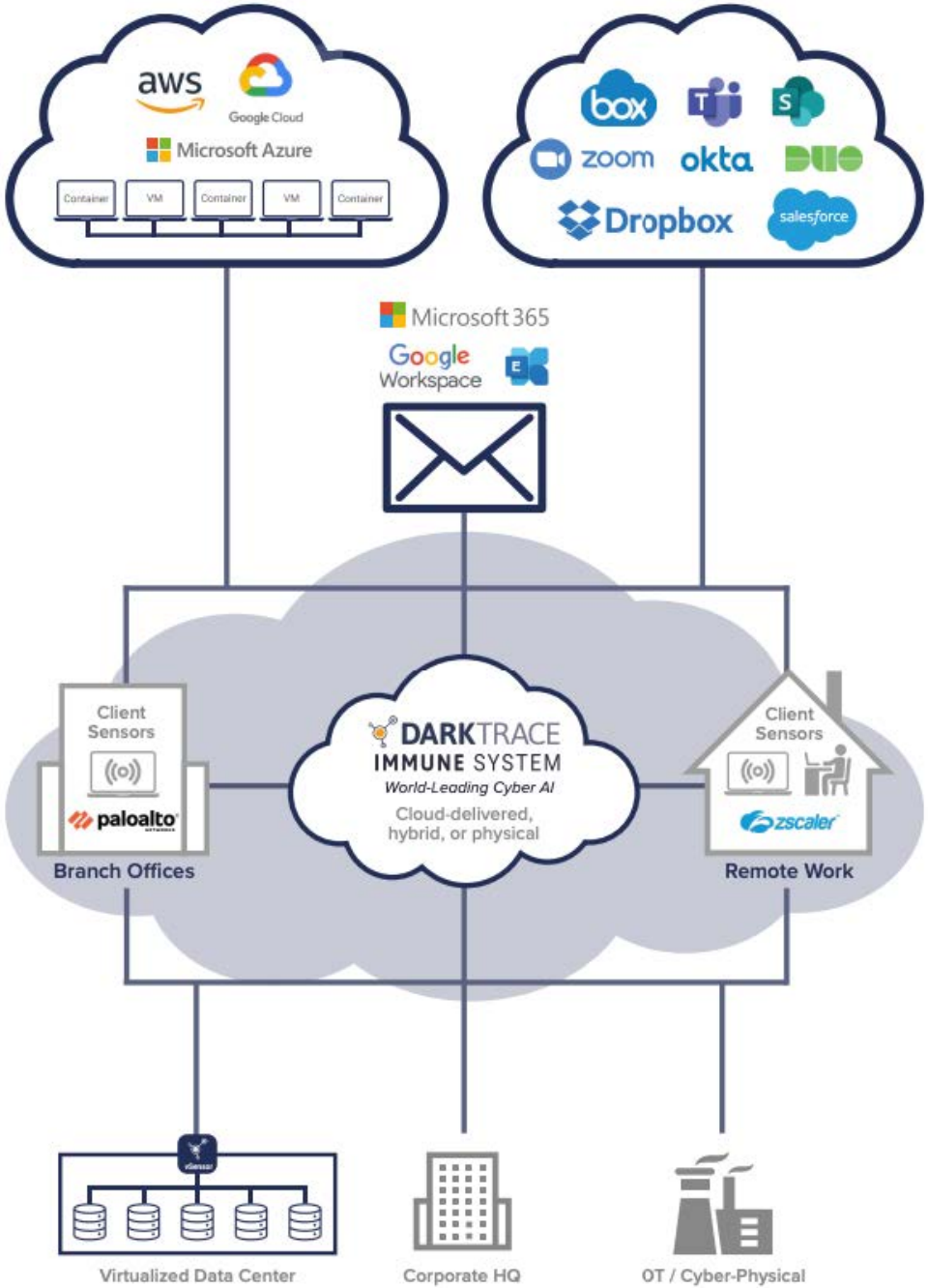
These options are not mutually exclusive, and any combination of these methods may be used:

- Layer 3 (VLAN mirroring)
- Layer 2 (Port mirroring)
- Network tap

Essentially, the Master appliance passively receives a copy of raw network traffic from the switch or tap.

All physical devices such as laptops, servers, tablets, mobile phones and printers can be captured including sensor traffic on OT environments.

As described later, a series of Probes and additional Master appliances can be combined to scale. It can also be used in conjunction with cloud and virtualized environments.



Darktrace Sensors

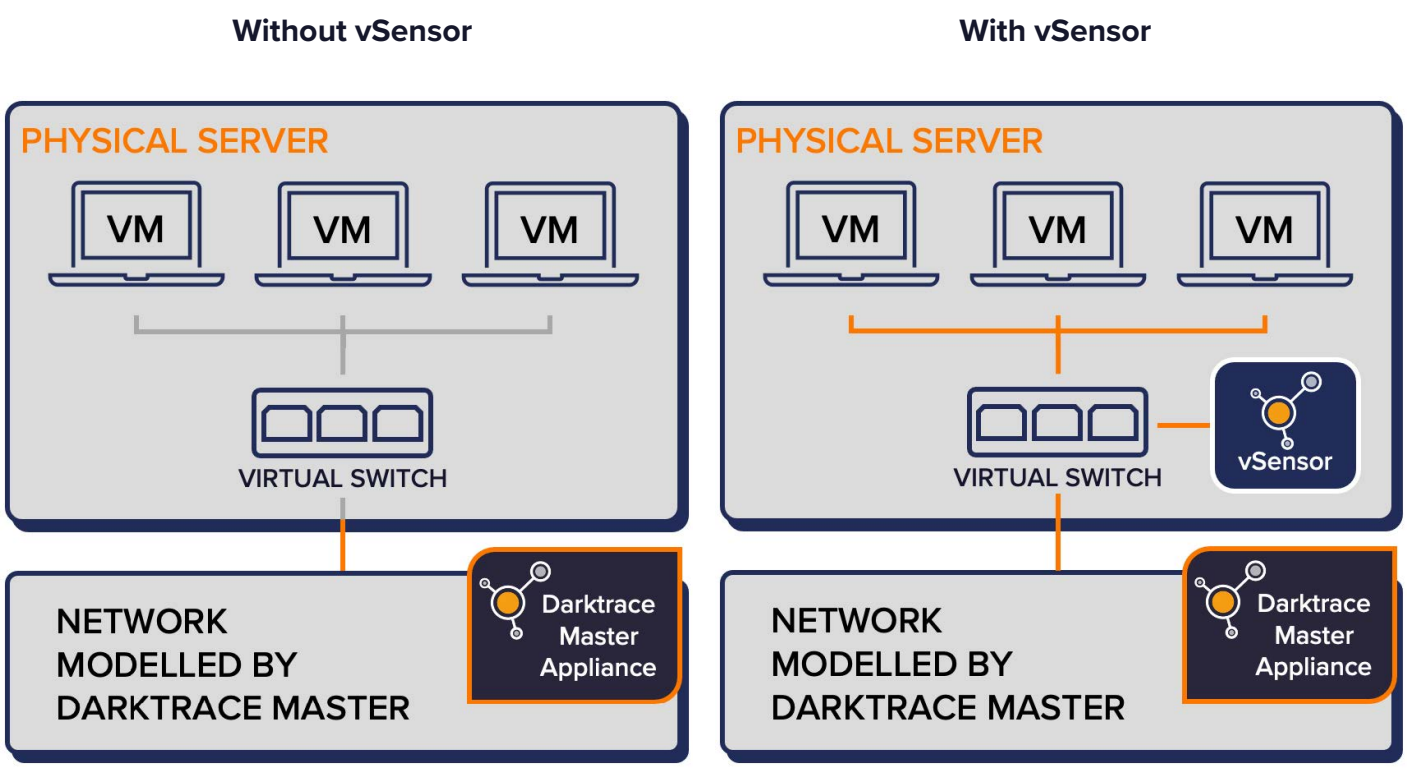
Darktrace vSensors, osSensors and cSensors seamlessly extend the self-learning, real-time threat detection capability of the Enterprise Immune System into cloud, virtualized, and remote environments. Darktrace sensors used in combination can achieve greater and simpler visibility into the network.

Whereas in traditional, physical networks, traffic can be easily 'seen' on the physical wire itself, traffic between virtual machines (VMs) residing on the same host can be difficult to monitor. This is because inter-VM traffic is switched locally on a virtual switch, as opposed to a physical one, and thus never makes it down to the network wire where it can be observed.

While solutions like taps can be used to mirror and access virtual traffic that leaves the virtual environment and travels over the physical network, they are sometimes unable to capture all the traffic that flows between VMs and inside the cloud.

For example, an application may be distributed across both physical and virtual environments, with the database tier residing on the physical server while the web and app tiers are virtualized. In this case, the network traffic between the two VMs may never traverse the physical network and thus will not pass by the TAP or a physical switch mirror port.

VISUAL EXAMPLE



In the first figure, the Darktrace Master can see the physical server, as denoted in orange, but cannot see any of the traffic between the virtual machines contained within the physical server, as denoted in gray.

In the second figure, a vSensor has been connected to the virtual switch. Now all the traffic occurring within the physical server can be distinguished, as depicted by orange lines representing the modeled network traffic.

vSensors

The Virtual Sensor ("vSensor") software is installed as a virtual appliance configured to receive a mirrored connection from the virtual network switch.

This allows it to capture all inter-VM traffic, without a single packet being lost or dropped by the system.

It stores the packet captures on a rolling basis, optimizing disk space and I/O performance, and ensuring that there is minimal impact on the performance of the server. Only one vSensor needs to be installed on each of the hosts, allowing for scalability.

By extracting only relevant metadata, only a fraction of the original raw network traffic is securely sent and ingested by the Master appliance.

The amount of network traffic processed by the vSensor and sent to the DCIP master is approximately 1-4% of the incoming bandwidth of the vSensor. Data can be "pulled" from the vSensor by the master, or "pushed" to the master appliance from the vSensor. All communication methods use HTTPS over port 443. Using the Pull or Push token modes, the vSensor can communicate securely via a pre-shared token, making them suitable for use over untrusted networks such as the internet or behind a NAT.

Darktrace vSensors are distributed in industry-standard formats, representing a virtual (software) appliance. They have been developed for VMWare ESXi, Microsoft HyperV and any other virtualized environment that supports Open Virtualization Formats (OVF), such as VirtualBox / VMware vSphere.

osSensors

An OS Sensor ("osSensor") is a lightweight, host-based server agent that is easily installed onto virtual machines in the cloud.

These sensors do not perform on-host Deep Packet Inspection. Instead, they intelligently create single copies of network traffic in a non intrusive manner and are capable of dynamically configuring themselves to streamline bandwidth use and avoid data duplication.

This data is aggregated within the local vSensor and fed back to the Master appliance via a secure connection. Therefore, osSensors cannot be deployed as a standalone solution.

The most suitable host-based sensor will differ depending on the deployment scenario and the network device for monitoring. The osSensor is available for a large range of operating systems and can be deployed in containerized environments.

Available for Linux and Windows, Darktrace osSensors are robust and resilient, allowing organizations to enhance visibility and deliver Enterprise Immune System monitoring to cloud environments, wherever they are hosted.

The vSensor image and osSensor agent can both be downloaded from the Darktrace Customer Portal Software Downloads page.

cSensors

The Client Sensor ("cSensor") extends the visibility of Darktrace's Cyber AI Platform via endpoint agent software that monitors devices' network activity and delivers key data and metadata to the Enterprise Immune System.

This can include remote working devices and those that cannot be seen adequately using bulk network traffic mirroring or existing Darktrace sensors. It is ideally used in combination with other Darktrace virtual sensors and deployment options to achieve a combination of greater and simpler visibility.

The cSensor is suitable where traffic mirroring is not viable and can potentially see East/West traffic that may not be reaching existing mirroring locations. It can be installed on host machines via existing management systems.

The cSensor communicates securely to Darktrace cloud-based infrastructure. Bandwidth consumption is restricted by performing a combination of on-endpoint DPI and cloud-based processing. In comparison to vSensors, cSensors perform slightly less deep packet inspection overall and will only transmit processed metadata.

Deployment Scenarios

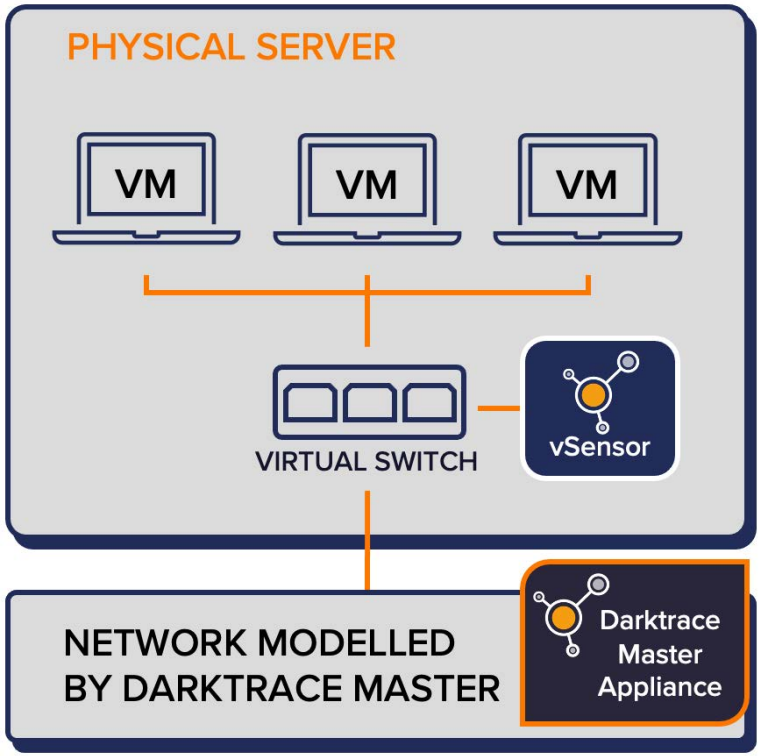
VMs on a Server

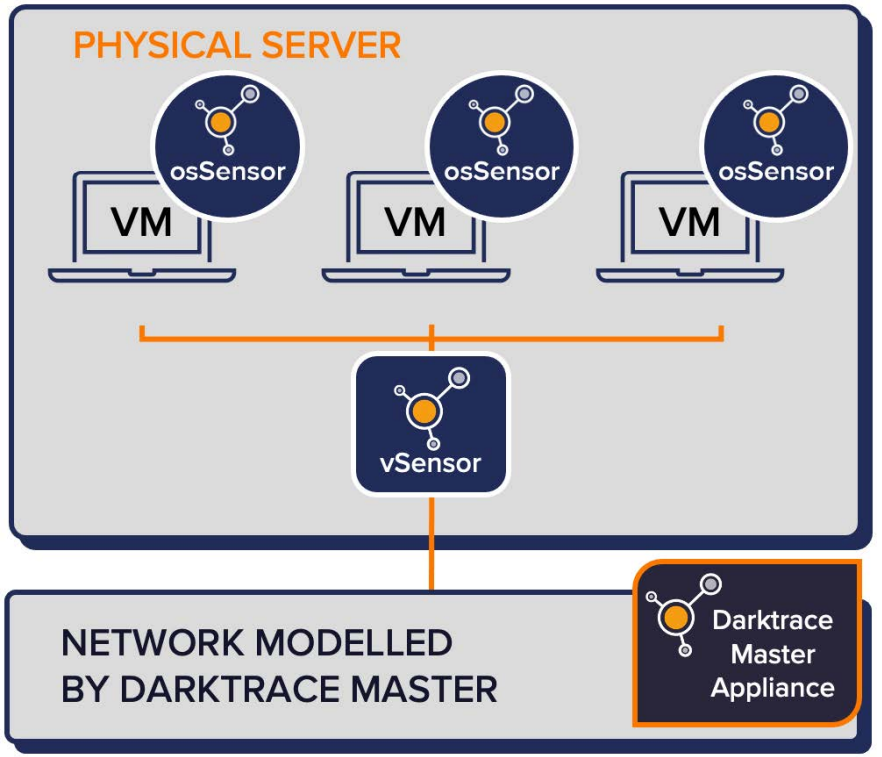
A standard deployment of the Darktrace Enterprise Immune System involves the capture of all traffic from a virtual server within one hardware appliance to a virtual server in another hardware appliance. This is because the traffic traverses the physical network connection.

With the vSensor installed into the hardware server, acting as just one more VM, visibility is extended to traffic between the VMs within the same physical appliance.

Note it is possible to port mirror a physical switch when it is not possible to mirror a virtual switch. In a similar fashion to as previously described, an osSensor can be installed on each VM to individually collect traffic for every device. The monitored traffic is sent to the vSensor for analysis. One vSensor can receive traffic from multiple osSensors before sending the data to the Darktrace appliance.

Instead of mirroring a distributed virtual switch, a vSensor can also be installed on every physical hypervisor host. In a similar fashion to a cloud environment, it can passively capture network traffic traversing the VMs and replay it to the Darktrace Appliance. In addition to the OVA format for VMware, QCOW2 (KVM/QEMU) and VHD (Hyper-V) are also supported for vSensor installations.





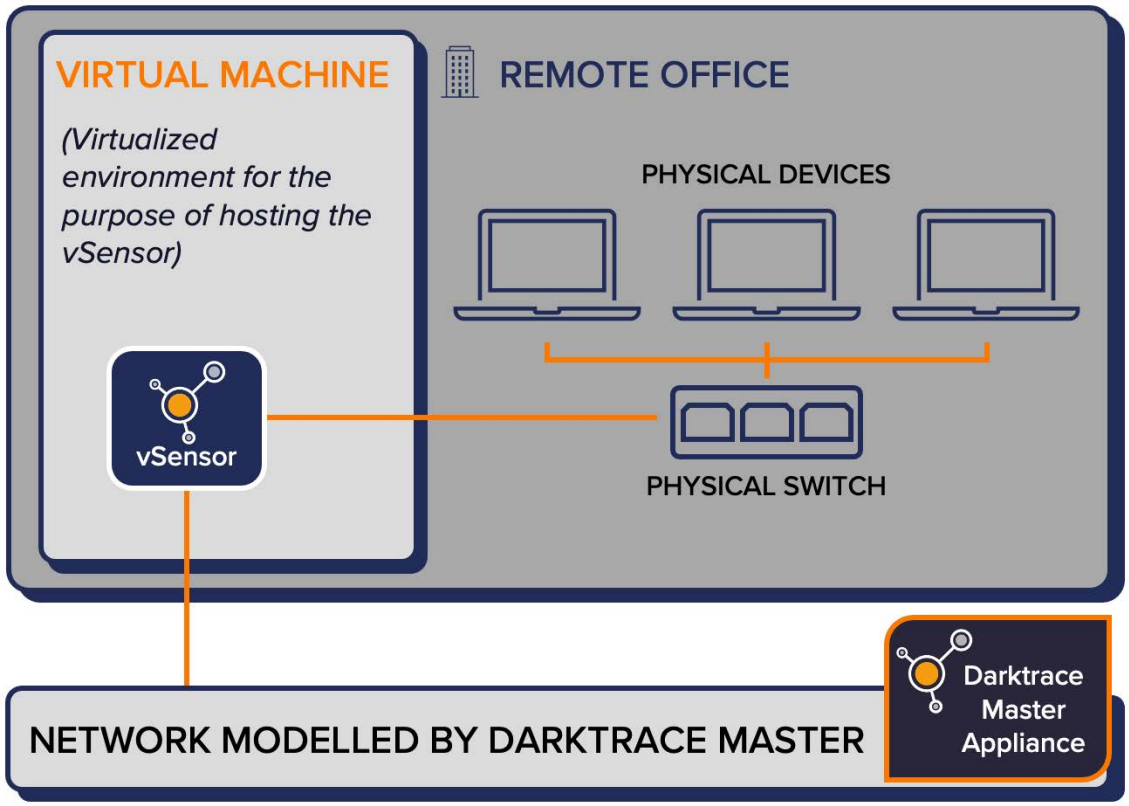
Remote Locations

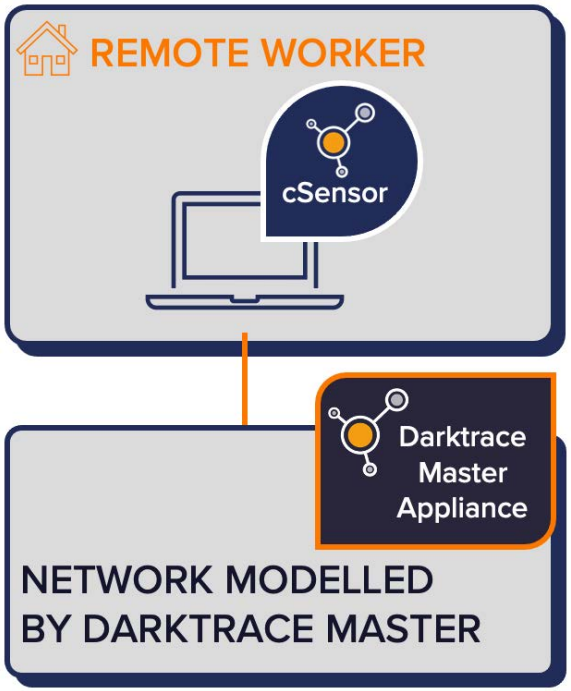
Remote Office

An organization may have remote offices or locations with several machines at each one.

A typical scenario might be a distribution of 300 small sales offices or retail stores, with 5 machines in each. It may not be practical for an organization with this infrastructure to deploy 300 Darktrace appliances into each individual location.

Using Darktrace vSensors, these multiple deployments are not necessary. If the relevant traffic is mirrored into a virtual environment hosting the vSensor, Darktrace can capture their intercommunications, and obtain insights into the data moving within each location. The data is sent back to the master appliance, where advanced analysis is performed.





Remote Worker Devices

In the situations where traffic mirroring is not viable, cSensors can also be used for tiny offices or remote workers.

Due to their host-based nature, cSensors can be rolled out across a fleet of remote devices using an existing remote management system. The devices monitored by the cSensor must be able to contact the cSensor infrastructure over HTTPS/443 for network traffic monitoring.

These cSensors will then securely communicate back to the Darktrace master appliance. Depending on the Enterprise Immune System Deployment type, the master appliance may be physical hardware or may be part of a virtualized set up.

Managed Third-Party Cloud Provider

One of the benefits of using a managed third-party cloud is enabling access from non-corporate sites, such as from home or whilst traveling. However, this environment necessarily creates blind spots from a security point of view. Darktrace is able to address this scenario even if you do not have direct access to the physical cloud server.

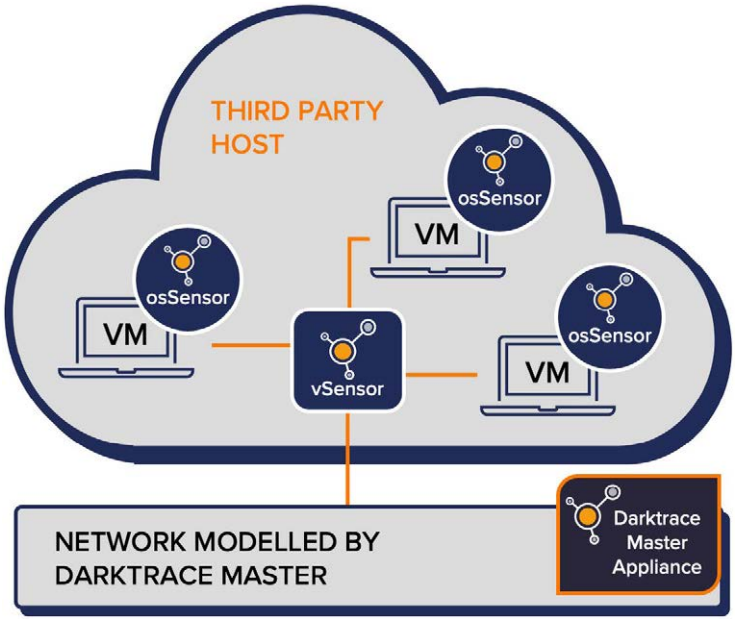
The master Darktrace appliance, connected to the physical network, already captures the activity of a user or client accessing data within the cloud data center. Supported by vSensors, it gains visibility of lateral information flow within the cloud too.

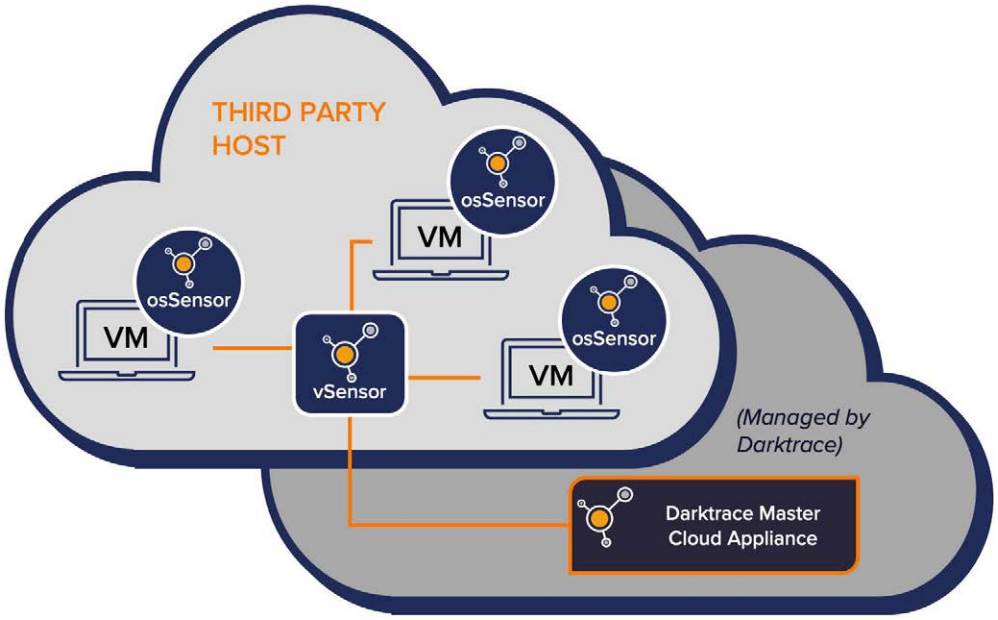
Darktrace is also able to capture virtual network traffic thanks to its osSensors, allowing you to achieve visibility of all cloud activity without requiring access to the hypervisor and with minimal performance impact.

Cloud-Only Environments

If your organization has internal users that access data in the cloud, and does not have on-premise network, Darktrace is able to deliver and manage a cloud-only deployment. In this scenario, Darktrace's Enterprise Immune System technology runs entirely in the cloud, without a physical appliance.

A cloud-only deployment includes the full service offered on the physical appliance, from data collection, mathematics, and detection, through to the Threat Visualizer and our expert Cyber Analyst services. Instead of installing a physical appliance, Darktrace runs a dedicated service for your organization, and vSensors and OS-Sensors are installed onto your existing cloud.





3. Sizing the Appliance for Deployment

There are set procedures for configuring Darktrace's Cyber AI Platform. The first task is to deploy the platform, then configure the console and finally access the Threat Visualizer to complete the setup. Before any of this can take place, the deployment needs to be sized. In this chapter, learn about the installation workflow and considerations before deploying Darktrace.

Darktrace Installation Workflow

1. **Size the deployment** for on premise, cloud and hybrid installations or a POV trial.

2. **Install the Platform** (Can include Appliances, vSensors, osSensors, cSensors and Modules).

3. **Log in to the Appliance via the console**:

   a. Check data is ingested.

4. **Review traffic ingestion in the Threat Visualizer**:

   a. Check network bandwidth and protocols ingested correctly.

   b. Review traffic types in Advanced Search.

5. **Final configuration changes in the Threat Visualizer page**:

   a. Restart POV timer.

   b. Tag key subnets and devices.

   c. Complete DHCP configurations for each Subnet.

6. **Additional changes within the console**:

   a. Schedule backups.

   b. Upgrade Darktrace.

Credentials for installation:

For console configuration, use the **console** account.

For Threat Visualizer configuration steps, use the **darktrace** account.

Darktrace's Cyber AI platform can be deployed in many ways. For on-premise, virtual and cloud hybrid installations a Darktrace appliance and components are typically required to store and process network traffic. Pure cloud deployments can utilize Darktrace's own appliances in AWS and only cloud components are required to be deployed.

Depending on the deployment, Darktrace recommends a no-fee no-obligation trial called a "Proof of Value" (POV) as an easy way to discover the value of Darktrace's unique technology. Spanning over 30 days, Darktrace will visualize a network's activity in real time, and detect in-progress threats or anomalies that would otherwise remain undetected.

During the POV, world-leading cyber analysts provide detailed analysis of what we find through three weekly Threat Intelligence Reports (TIRs). These explain incidents and anomalies that have been uniquely discovered by the Enterprise Immune System. They will help better understand a network environment, share new intelligence within an organization, and identify potential threats before they do damage.

A POV can be deployed in multiple ways.

- **On-premise network**

  Requires the installation of a Darktrace appliance. This is shipped to a customer on-site location. Darktrace employs a series of appliances to capture network traffic. These appliances are highly tuned, high performance pieces of hardware that host the Darktrace platform. There are multiple Darktrace appliance sizes, with different throughput capacities and options for data ingestion.

- **Darktrace IaaS environments**

  Works directly with digital infrastructure. By deploying a Darktrace probe, customers can gain full visibility of their cloud and SaaS environments.

  Darktrace deploys a local 'vSensor' (virtual probe) in each cloud environment. The vSensor captures real-time traffic in AWS, Azure, and GCP, from AWS VPC Traffic Mirroring, the Azure vTAP, and GCP Packet Mirroring, respectively. The receiving vSensor processes the data and feeds it back to the cloud-based Darktrace instance.

- To cover other **IaaS environments** (e.g. Alibaba Cloud, Rackspace, and others).

  Darktrace's lightweight host-based 'OS-Sensors' are installed on each cloud endpoint and configured to send intelligent copies of cloud traffic to the local vSensor deployed in the same cloud environment, which then feeds it back to the cloud-based Darktrace instance for analysis.

- **Darktrace SaaS applications**

  Provider-specific Darktrace Security Modules are enabled on the Darktrace cloud-based instance and will interrogate the security APIs of the relevant SaaS solutions. SaaS solutions covered include Salesforce, Office 365, OneDrive, SharePoint, Box, Dropbox, G Suite, Jumpcloud, and Egnyte.

- **Cloud environments**

  Darktrace platform manages a cloud-based Darktrace instance hosted in Darktrace's own AWS environment. It receives traffic from sensors deployed in the customer's IaaS and/or SaaS environments.

Cloud Deployment POVs

Cloud based POVs do not require a Darktrace appliance and can be installed in 5 easy steps:

1. **Darktrace Customer Portal activation**

   Prospect receives an email with a link to activate a Darktrace Customer Portal account.

2. **Download vSensors**

   Prospect downloads Darktrace virtual sensors from the Customer Portal (vSensor and osSensors)

3. **Install vSensors**

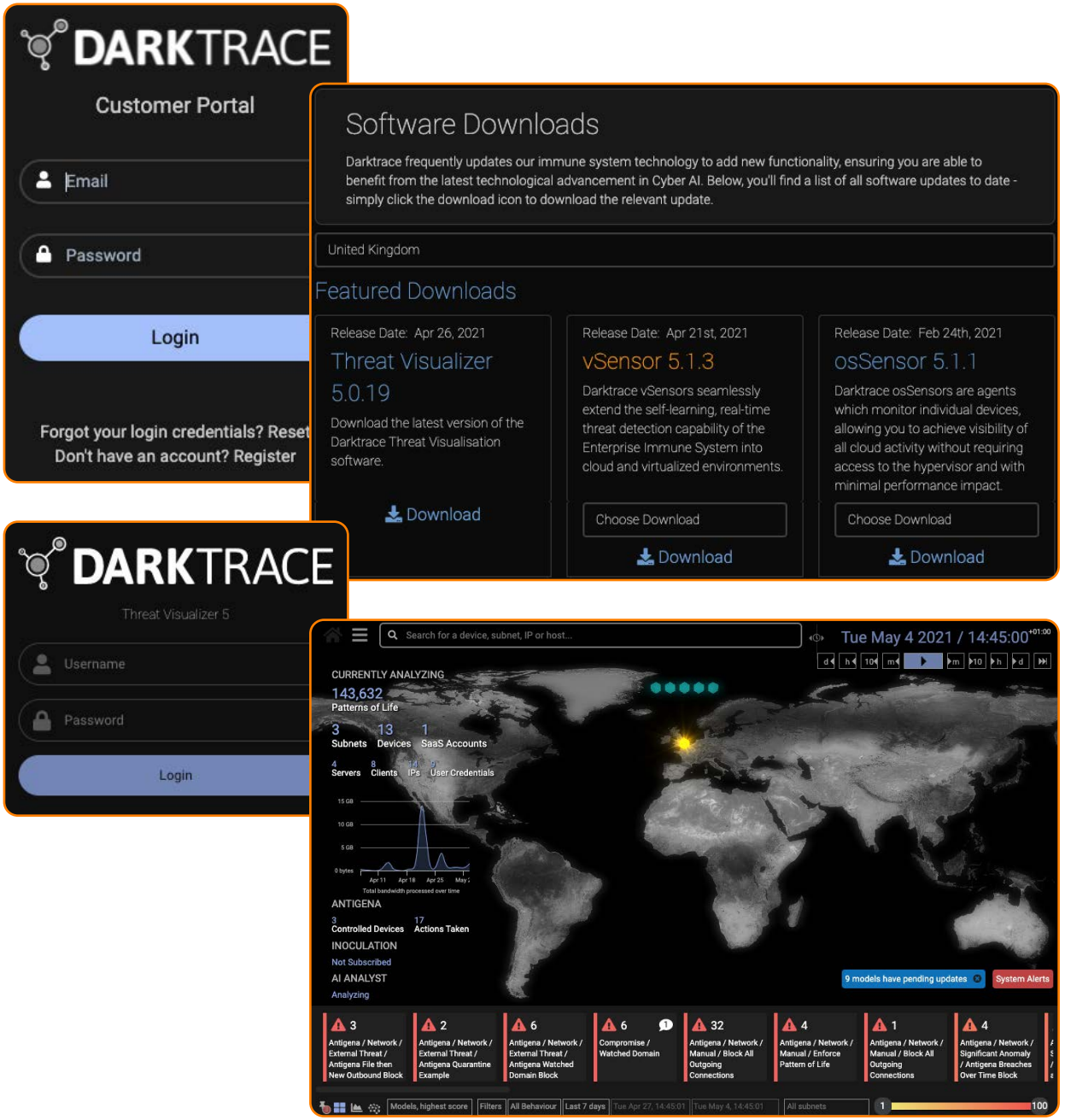
   Darktrace Cyber Engineer assists installation of virtual sensors into chosen environment (covering either a physical office location, a cloud environment or both.) Data can now be ingested into the virtual sensors, and a connection is made between those sensors and the private customer master hosted in the Darktrace Cloud.

4. **Install Antigena Email and/or SaaS modules**

   If the POV includes either Antigena Email or coverage of a SaaS application, your prospect will receive a relevant link to the Darktrace Customer Portal, where they can install these modules.

5. **Access to Threat Visualizer**

   Installation is now complete. After POV Session 1, your prospect receives a link and credentials to access the Threat Visualizer.



On-premise Network Appliance POVs

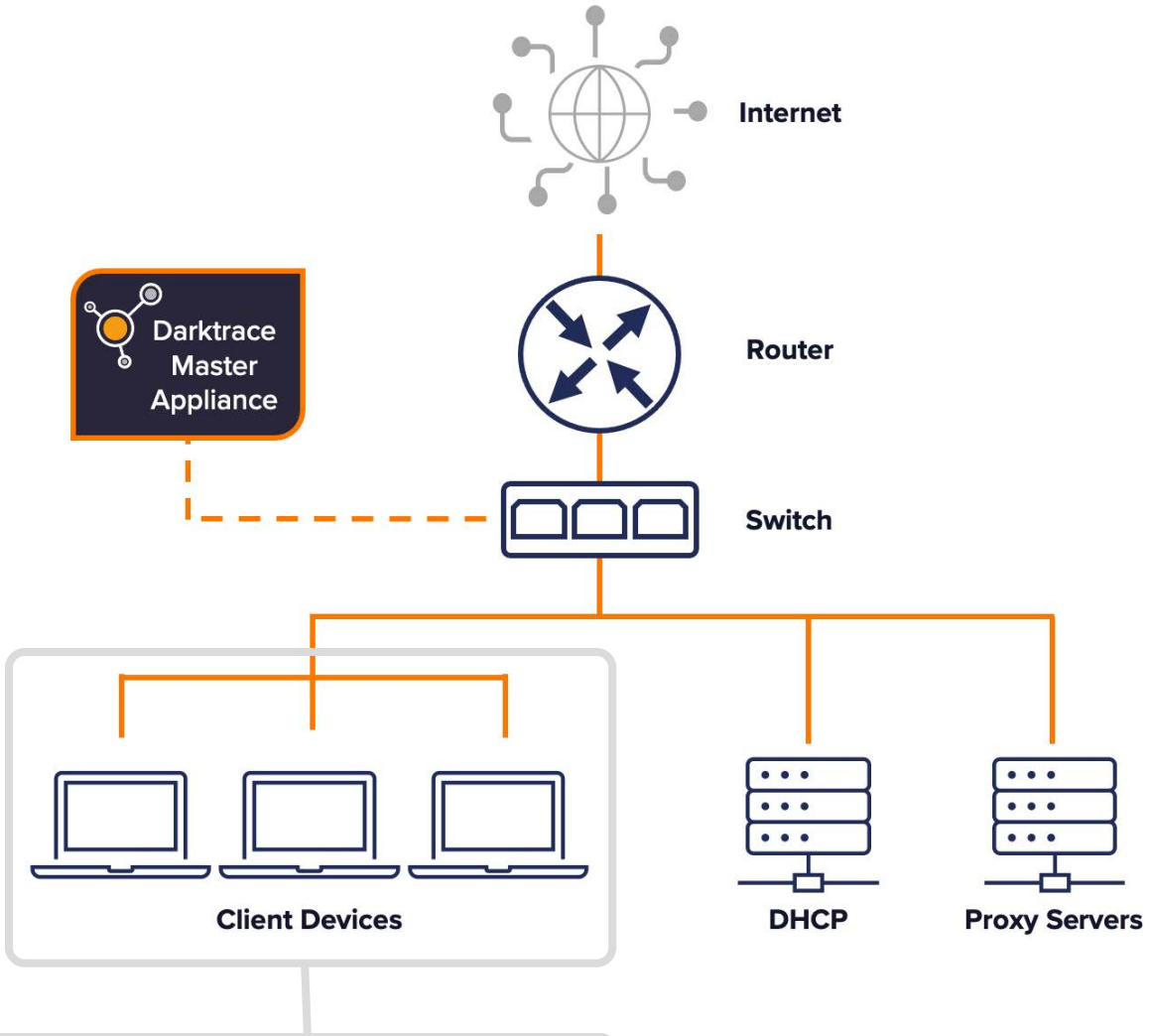
During the POV, depending on the size and complexity of a network, it may not be effective to ingest traffic from all subnets. Instead it is recommended to select a number of subnets where full duplex traffic is available. This will minimize unidirectional traffic and provide the best insight into a network.

Upon completion of the POV, it is recommended the Appliance is installed at the core of a network to capture all internet bound client and server traffic.

In many situations, it is preferable to configure multiple points of data capture. The aggregation of these data capture points may necessitate passing duplicate packets to the Darktrace appliance. The Darktrace platform is aware that some packets may be duplicates and methods are in place which mean that duplicate packets do not affect the behavioral models.

The Darktrace platform will de-duplicate TCP packets and consolidate these in any front-end representation of data. It should be considered that although the existence of duplicate packets of any type is handled by Darktrace internally, there is still a hardware overhead associated with their capture.

An easy way to understand how Darktrace captures data is to think about what traffic is being sent over a core switch. Darktrace can only model packets which are passively monitored.



In this figure, the appliance installed at the core of the network will capture all client to server communications and internet bound traffic.

However, traffic occurring between the client devices (i.e., in the gray box), such as direct FTP or SSH connections between the laptops, will not be visible as it does not pass the core switch.

To capture and monitor this traffic, an additional appliance or vSensor will be required.

Appliance Operation

Data Capture

Darktrace is designed to operate on network data without any pre-configuration of specific data types. In more complex single-site or multi-site enterprise environments, the ability to provide data capture can be limited to the practicalities of network administration and pre-existing infrastructure configuration. When selecting where to position the Darktrace appliance, it is important to consider which data will best enable Darktrace to determine a pattern of life for the objects in your network. Organizations may choose to limit the scope of data capture to those containing the most 'information-rich' flows, to reduce the infrastructure demand of packet capture. Very often this requires a balance between the hardware resources needed to capture and analyze the traffic, and the importance of that traffic in determining a pattern of life.

In many corporate environments, network traffic that is considered 'information-rich' includes:

- Direct internet-bound traffic
- Internet-bound traffic that goes via a proxy or sequence of proxies
- DNS resolution
- DHCP traffic
- Internal access to server application services *(such as file services, web portals, payroll systems and print servers)*
- Authentication traffic *(such as Active Directory authentication)*
- Any other traffic between two internal devices

In some corporate environments, information that provides some relevant data, but which requires greater resources to capture and analyze, might include:

- Inbound access from public IP addresses to intensive server farms, for example, a heavily used web server farm.
- Traffic where neither end of the communication can be ascribed to a specific location, such as transient traffic between two devices where both sides of the communication are subject to network address translation.

Information that is considered 'information-poor' might include network traffic that connects storage area networks and controllers, such as Fiber Channel over Ethernet (FCoE) technologies. This high-volume traffic places great demands on packet capture technologies yet provides little ascribable information.

Organizations wishing to restrict data capture should adopt a 'exclude list' policy, selectively removing data segments from the data capture rather than selectively adding them. For example, you may not wish to monitor a guest network, as this could generate a large number of anomalies with different devices and apps communicating on the network. Also, you may not be concerned with developer networks and therefore not wish to monitor them. However, as a general rule, as much data should be captured as is possible for the infrastructure or for analytical processing.

Encrypted Traffic

Although the payload of encrypted traffic is unreadable, it still provides very valuable information. For example, the time of day, source, destination, and the size of transfer can be used during analysis if the connection is suspicious. Therefore, this traffic is considered 'information-rich'.

Desired Data

To determine what is the best data to capture and the required capture points, it may be helpful to consider the daily life cycle of an average Windows desktop.

Depending on your network topology, you may require more than one Darktrace appliance at more than one location. There are a number of types of Darktrace appliance which, depending on your network, may perform different functions.

The following network topology examples describe where to site a Darktrace appliance or multiple appliances within your network. In the following examples, a master appliance may provide end-to-end Darktrace functionality to act as either a standalone unit or part of a Master/Probe distribution. A probe will provide deep packet inspection and pass relevant metadata to the master. The master will behaviorally analyze the data and provide all user interfaces for the Darktrace technology.

A network topology that requires one Darktrace appliance to perform capture of the required data has the following features:

- Clients, DHCP infrastructure and proxy servers exist on separate sub-nets
- Communication between any of these segments passes through a central network device

In this environment, a Layer 3 port mirror may be configured on this network device to pass all traffic (TX and RX) from this network device to a Darktrace appliance. This data capture point is indicated in the diagram.

In some networks, a single data capture point for a single network device is insufficient to provide full awareness of the network behavior of internal devices. In the example above, it is unlikely that network devices see the transmission of DHCP data from the DHCP servers to client devices. In this instance it is preferable to perform data capture at both network devices and the Data Capture Point.

Model Blurring

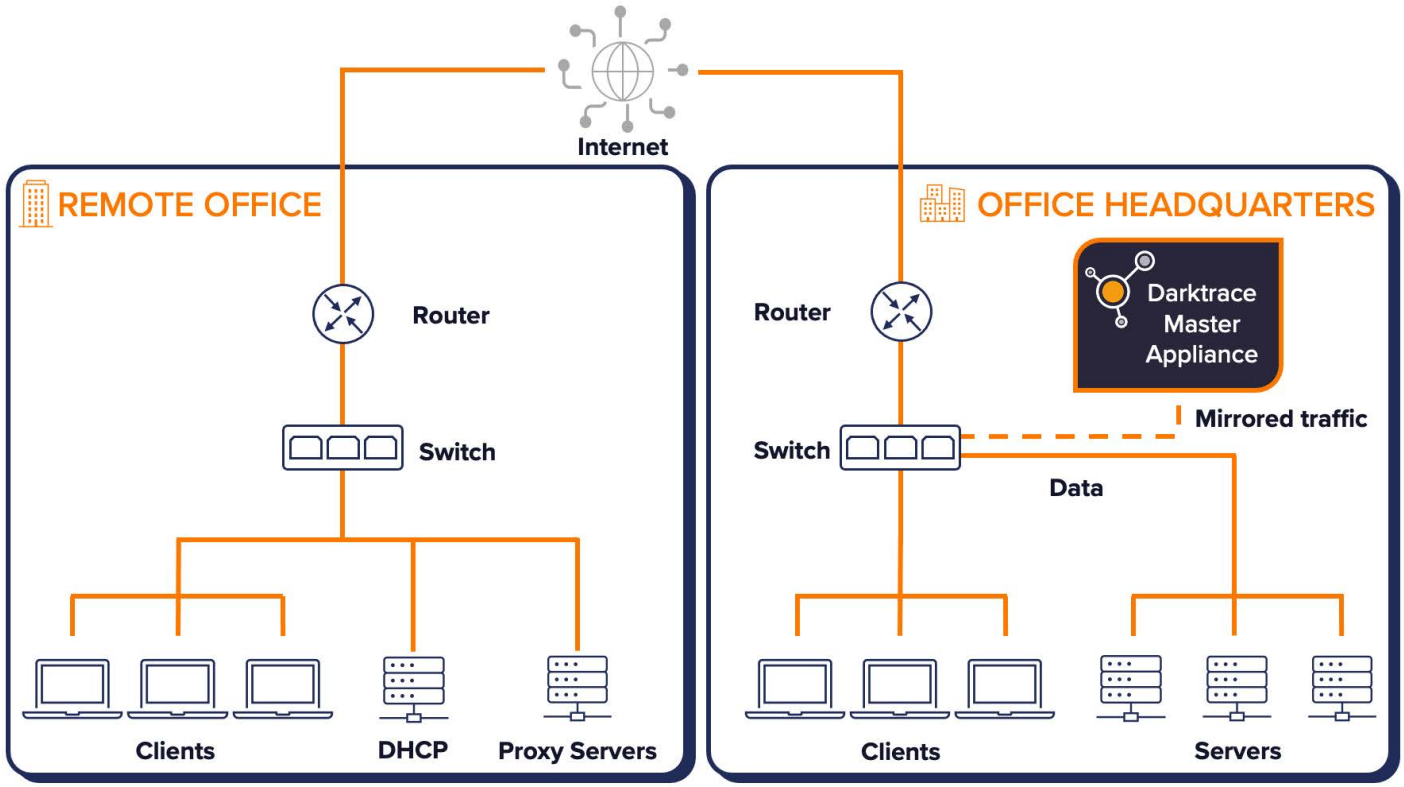
When Darktrace does not have mapping data available for DHCP devices, such as those existing at an unmonitored remote site where IP addresses are allocated at the remote site, a situation called ‘model blurring’ may occur. If Darktrace is not provided with the information to track different devices on the same IP address, the behavioral models at the remote site become blurred with each other.

Instead of constructing behavioral models for each specific device, Darktrace constructs a complex model that refers to the behavior of the remote subnet as a whole. This is sometimes the desired effect with BYOD or guest networks; sometimes organizations wish to be alerted when any device breaches the normal activity of a normal user on that network. However, it should be noted that these blurred models take longer to construct than device-specific models, and while the models are being constructed, more alerts will be generated than for those on equivalent networks where mapping data is available.

Possible Architectures

Multiple Capture Points

The following diagram represents a Master/ Probe distribution architecture with a central head office and a remote site.



Features of this architecture:

- The two locations are connected by a site-to-site VPN.
- The IP ranges of all machines are within the ranges that Darktrace has been configured to analyze.
- Each location has a local egress point to the internet.
- At the remote location, client devices are allocated DHCP addresses from a local DHCP server.
- The devices at the remote office will access the application servers at the Head Office.

A Darktrace appliance is located optimally at the Head Office location, as shown in the diagram. In this scenario Darktrace will behave as follows:

- All traffic at the Head Office will be analyzed as expected.
- Darktrace will attempt to create sparse behavioral models for the devices at the remote site, based on a limited subset of information. The behavioral models will only be calculated based on the remote office's connections to head office application servers.
- Model blurring will occur for devices at the remote site.

If this is not the desired behavior, one or more of the following actions are suggested:

- Configure the remote office network infrastructure to forward packet captures to the Head Office.
- Set up VLAN tagging at remote office level so that the Master can differentiate between the devices.
- Place a Darktrace probe at the remote office to feed into the master Darktrace appliance at the Head Office.

Distributed Architecture

Many aspects of the internal structure of a Darktrace system are modular, and thus may be distributed across two or three appliances, while still permitting a single packet capture route and single user interface.

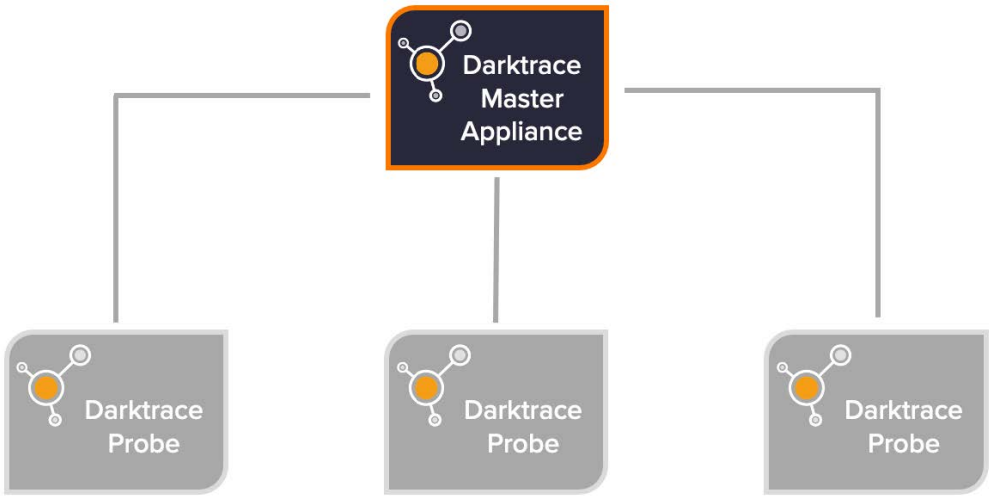
Components may be distributed so as to increase data write/read speeds and reserve dedicated appliances for deep packet inspection and mathematical anomaly detection. Appliances participating in shared component systems must be connected by high speed, low latency links; typically, this is performed with devices in the same location.

Environments that may benefit from shared component configuration include those with high numbers of small connections, those operating as master devices for multiple probes, or any other situation where the capacity of a single device would be exceeded.

Since a single user interface is displayed, the existence of a shared component configuration is largely invisible to an ordinary operator of the system.

A simple Master/Probe distribution of Darktrace appliances involves one or more appliances configured as probes, which forward key metadata to a single master appliance. The single master appliance may or may not be configured in shared component mode.

A Darktrace appliance operating as a probe may be placed in the same location as the master to increase raw packet capture capability, or at a geographically separate location for geographically dispersed topologies.



Features of this type of distribution:

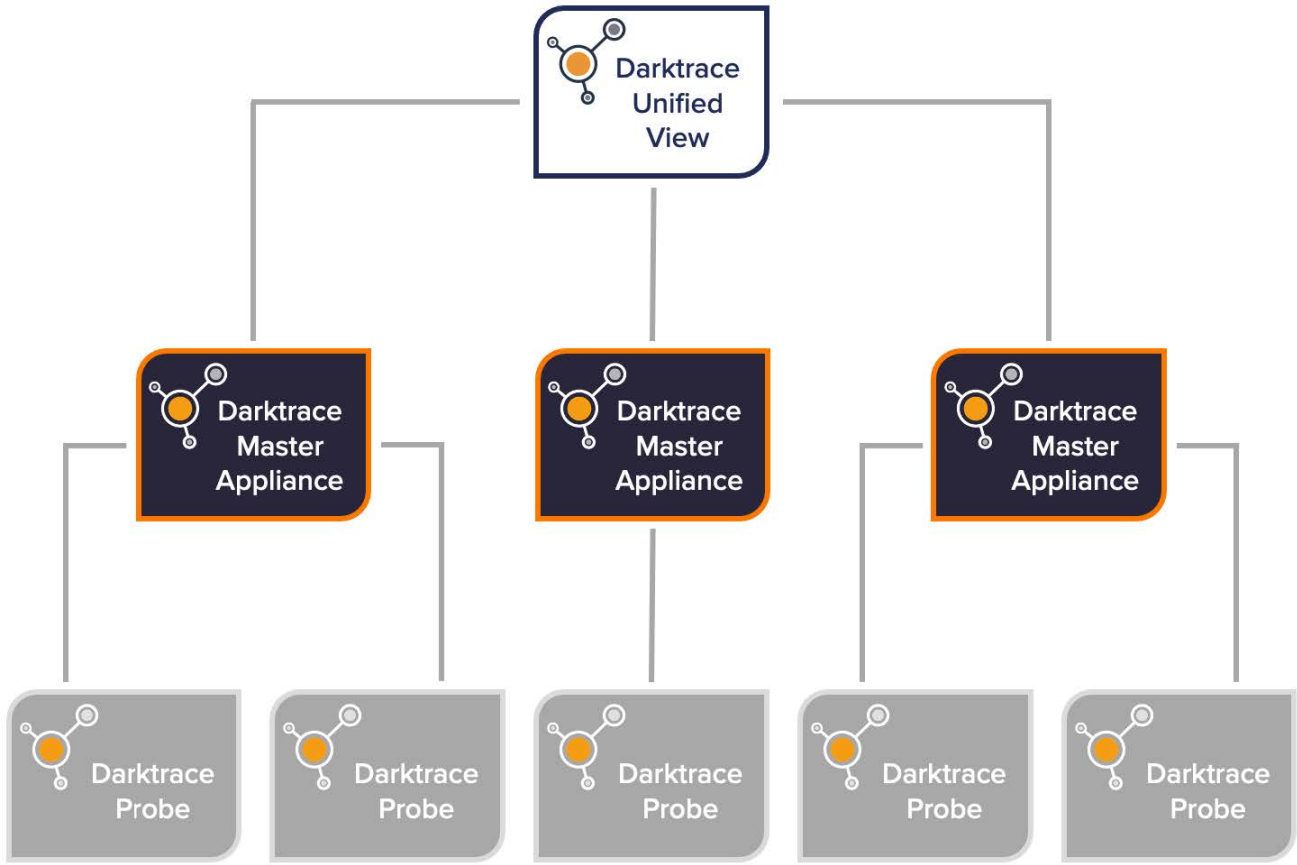
- The probe will offload much of the local processing and storage from the master appliance. The Master/Probe distribution is designed such that only metadata derived from a probe will be forwarded to the master appliance.
- Data that is infrequently used after generation, such as raw packet capture, will be maintained locally at the probe and will only be recalled to the master upon user demand.
- The master appliance serves up the user interface, and for an ordinary operator of the system the existence of the Master/Probe configuration is invisible.
- Many probes may be configured to report to a single master.
- This distribution is suitable for environments with high bandwidth or for geographically distributed infrastructures.
- The appliances in this type of distribution communicate with each other over encrypted IPsec protocols.

Complex Master/Probe Distribution

A more complex Master/Probe distribution involves one where multiple Darktrace instances (each potentially formed of shared component or Master/Probe distributions) are connected by one master presenting a single user interface.

Each instance is aware of the others at the user interface level alone. This is deliberate and is intended to restrict sustained bandwidth utilization between appliances to a negligible level. Bandwidth transfer between these instances is on demand only.

Communications between browser and appliances, and between appliances, is over HTTPS. Since there is negligible sustained communication between appliances, behavioral profiles are not shared between instances and careful excluding/including must be performed to prevent multiple device profiles being created, if this is the desired behavior.



Sizing Questions and Considerations

Before installing an appliance, it is essential to have a sizing call to confirm a customer's requirements.

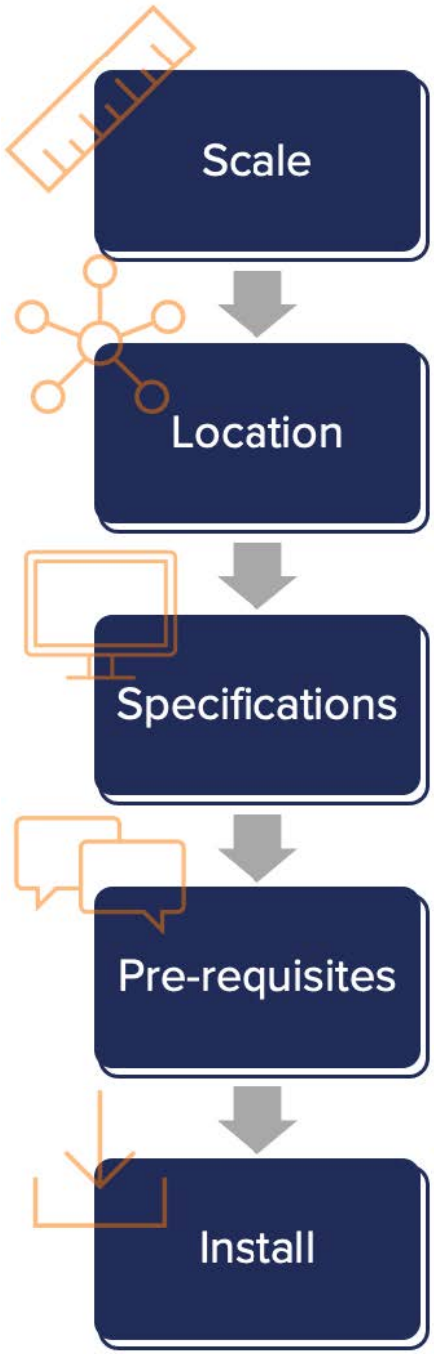
The Darktrace appliance can be delivered in different sizes and it will depend on the amount of network traffic as to which is best suited for a particular environment.

It is also important as part of the sizing call to discuss where the appliance will be installed on the network and to confirm that the infrastructure is in place in preparation for the installation.

As part of a sizing call the following factors should be considered by discussing the following points.

Objective:

- Understand the network and its scale.
- Identify the best location in the network, where we will see the most 'rich' traffic, to place the appliance for the POV.
- Identify the specifications of any hardware and software required (usually aiming for just one physical appliance).
- Ensure the prospect understands the pre-requisites for the POV.
- Get a shipping address and agree on an install date.



1. **Obtain a high level overview of what the network looks like**

- Check the following:
  - How many sites have IT infrastructure?
  - How do the sites connect together? *(MPLS, VPN, etc)*
  - Where are key servers hosted? *(DNS, DHCP, AD, DC, Internet Breakout)*
  - Is there any Cloud/SaaS? *Obtain details later in the call.*
- Once we have this overview, we can then dive into a specific site (usually a large office) to ask more specific questions about how that site fits together.

2. **Determine the best/most practical location for an appliance**

- There are many different factors and scenarios that govern where the appliance would be best located, but generally we are aiming for:
  - A large (or the largest) office location.
  - To be at the heart of the network and likely hanging off the core switch
  - However, there are exceptions to this, such as:
    - Inability to deploy (i.e. shared infrastructure)
    - Future office moves.

- The types of traffic that we are looking for are:
  - Bi-directional network traffic between clients-servers, server-server, server-internet and client-internet.
  - Traffic between an internal client and an internal web proxy as well as any other internet bound traffic that might bypass this web proxy.
  - Rich user-server traffic, particularly DHCP, DNS and authentication traffic (i.e. Kerberos).
  - General network traffic related to common protocols, including but not limited to HTTP, TLS, SMB, SSL etc.

- There are certain situations where we generally will not see very good network traffic. In particular:
  - If we are located at the border or perimeter of the network as we are likely to miss client-server traffic.
  - If we are located in a DMZ.
  - If we are located in a data center
    - There are exceptions to this, but generally we are only going to see server-server traffic and some, but not necessarily all, client-server traffic.
    - Investigate what network traffic can be ingested from all devices. Certain devices may require more effort to ingest effectively.
    - Confirm you are only modelling devices that breakout to the internet through the data center and that also receive DHCP, AD etc. from a domain controller in the data center rather than from a local domain controller.

3. **Identify hardware/software specifications**

- In order to size a physical appliance, we will need to know:
  - Number of devices the appliance is likely to model (anything with an IP address) and, if they know, the throughput the appliance is likely to see.
  - The type and number of network interfaces required for the analysis ports on the Darktrace appliance (Copper (1/10Gb, Fiber SFP+ MM/SM, etc.)
  - If in any doubt as to what size appliance we should be deploying, it is best to size up rather than down. If we need to swap the appliance out when moving to a contract, then we can do that. However, if we need to swap the appliance out pre-POV then this will slow down the sales cycle.

4. **Sizing of Virtual/Cloud/SaaS**

- To monitor the intra VM traffic on a hypervisor, we will need to deploy a vSensor per physical host (unless using a Virtual Distributed Switch).
  - How many Hypervisor physical servers?
  - How many VMs?

- Is there any virtual desktop infrastructure (VDI) being used, such as Citrix XenApp / Virtual Apps?
  - How many hosts?
  - NATted?

- Cloud: AWS, GCP, Azure
  - How many VPCs/vNets?
    - 1 vSensor/VPC
  - How many instances (VMs)?
    - 1 osSensor/instance depending if traffic mirroring available

- SaaS: Are any of the following being used with the license level requirement?
  - Office 365
  - G Suite
  - AWS
  - Azure
  - Dropbox, Box, Egnyte

5. **Explain pre-requisites**

- IP information for the appliance
  - One internal static IP address to be bound to the Darktrace appliance management port along with its relevant network mask and default gateway.
  - The IP addresses of the DNS and NTP servers.
  - A KVM switch (keyboard, video and mouse) or monitor (with VGA) and USB keyboard available on the day of the installation.

- Mirrored network traffic to be analyzed by the appliance.
  - Bi-directional network traffic between client-servers and client-internet.
  - Traffic between an internal client and an internal web proxy and also any other internet bound traffic that might bypass this web proxy.
  - Rich user-server traffic, particularly DHCP, DNS and authentication traffic (i.e. Kerberos).
  - General network traffic related to common protocols, including but not limited to HTTP, TLS, SMB, SSL etc.

- Call-Home
  - Must allow outbound TCP traffic on port 443 or 22 from the appliance's internal IP to our four static IPs in Cambridge.
  - Call-Home is fully audited so that you can see when we have established connections.
  - The connection is encrypted using the ChaCha20 cipher.
  - There are alternatives to this solution, which should be discussed with the customer.

4. Console Configuration

When installing appliances, there are many configurable elements in the Darktrace Console. Let's explore call-home and data ingestion.

Appliance Installation Prerequisites

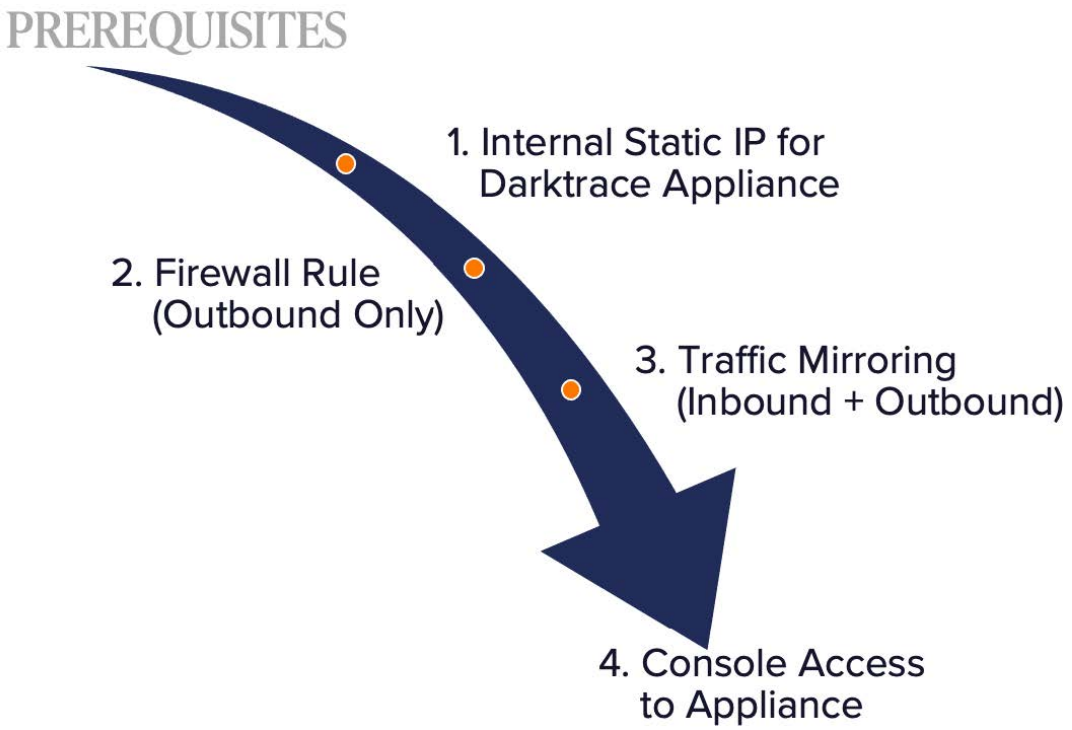
Before commencing the installation of a Darktrace appliance, check the following prerequisites are in place. Some of these details should be confirmed as part of the sizing call.

1. Allocate an **internal static IP address for the Darktrace Appliance**. The appliance will require connectivity through a management or admin port with an NTP server, DNS server(s), subnet mask, and default gateway settings.

2. Create a **new Firewall rule that allows ONLY outbound TCP** from <**darktraceApplianceStaticIP**> to **212.250.153.80**, **212.250.153.81** and **194.72.254.216**, **194.72.254.217** on port **22** [SSH] or **443** [SSL].

3. Set up appropriate **traffic mirroring feeds** that include all bidirectional (inbound + outbound) traffic, including any client-server internal and internet traffic (HTTP), Active Directory, Kerberos, DNS, and most importantly DHCP traffic.

4. A valid **user account** has been provided to access the Appliance's console. It is recommended that this password be exchanged via a secure channel such as text message, or embedded in an encrypted email attachment. Credentials are not sent in clear text to avoid password sniffing.



Installing a Darktrace Appliance

If a customer installs the Appliance and enables Call-Home, all additional configuration can be completed remotely by Darktrace or a Partner.

1. Begin by unpacking the Darktrace appliance. It must then be racked with power for the UPS and appliance.

   Do not plug in network traffic from the Switch yet.

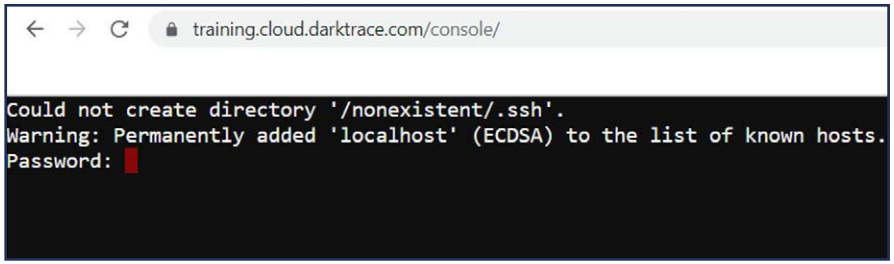
   The Console interface can be accessed by using a VGA monitor and USB keyboard connected to the Darktrace appliance. Alternatively, the application can be remotely accessed via the appliance management interface (Ethernet port eth0) by means of any ncurses-capable SSH client (such as PuTTY).

   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 you plan to install the appliance on a different subnet, you will need to change the IP address via the console.

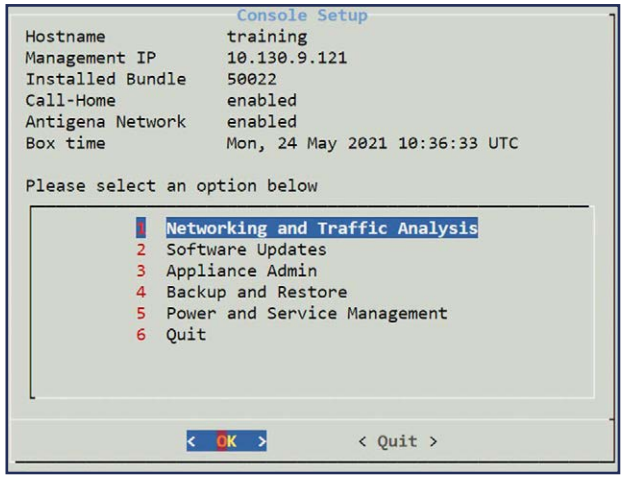
   In the example screenshot (left), an SSH connection has been directly made by plugging an Ethernet cable to the Admin Interface port.



3. Log in as the **Console** user and enter the password provided by Darktrace.

   Confirm the **Console Setup** options are displayed.

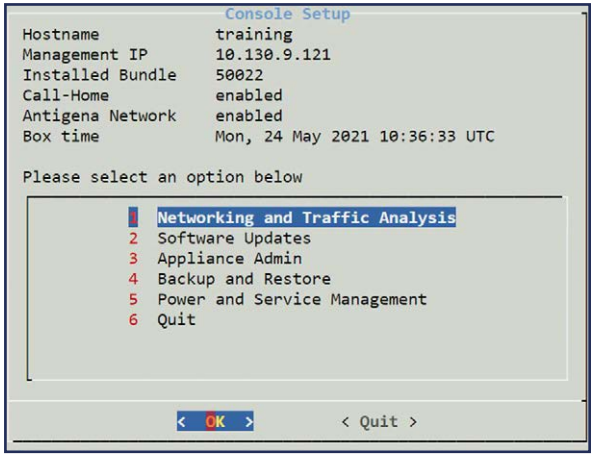
   The console is a CLI (command line interface) which allows only keyboard controls. Arrow keys work as expected, and the Cancel option returns to the parent menu. Numeric hotkeys can also be used to jump to specific menu options, and the Enter key selects the currently highlighted option.



Set the Appliance IP Address

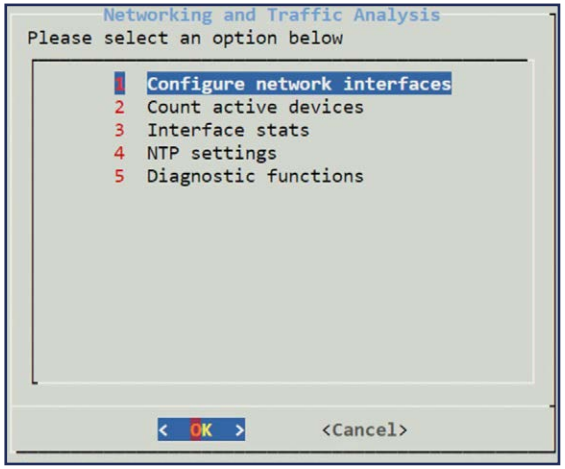
Unless the Darktrace appliance has been shipped with pre-configurations, it may be necessary to change the static default IP address of 10.0.0.2. For example, you may wish to move the appliance to a different subnet.

1. If you wish to change the IP of the appliance, select option **1. Networking and Traffic Analysis** on the Console homepage and press **OK**.

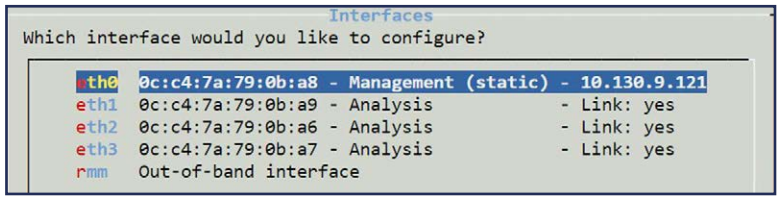


2. Within the Network Settings options, choose **1. Configure network interfaces**.

   Click **OK**.

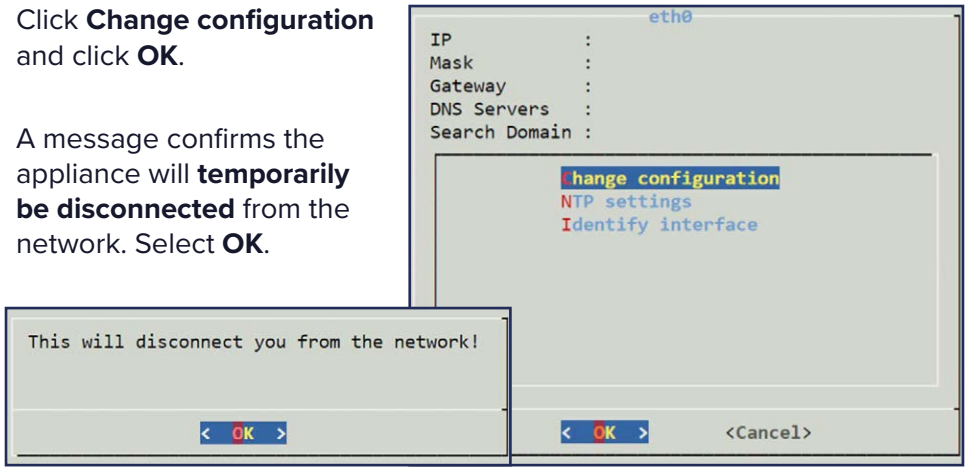


3. **Select an interface** to configure.

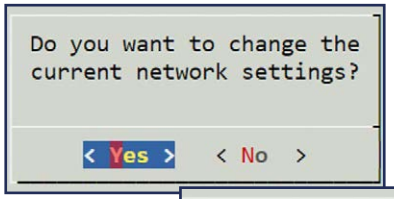


4. Click **Change configuration** and click **OK**.

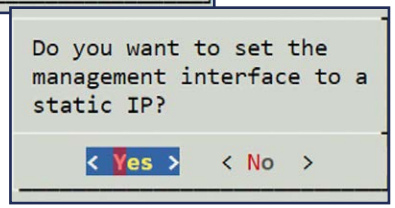
5. A message confirms the appliance will **temporarily be disconnected** from the network. Select **OK**.



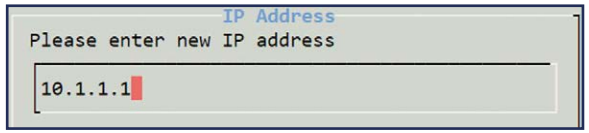
6. Choose **Yes** to confirm you wish to change the current network settings.



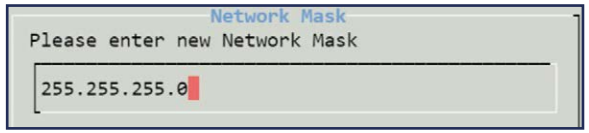
7. Select **Yes** to configure a static IP. It is strongly recommended to set the Darktrace appliance with a static IP. Alternatively, DHCP will be used.



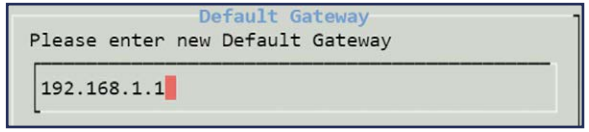
8. Enter a **new IP address** and press **OK**.



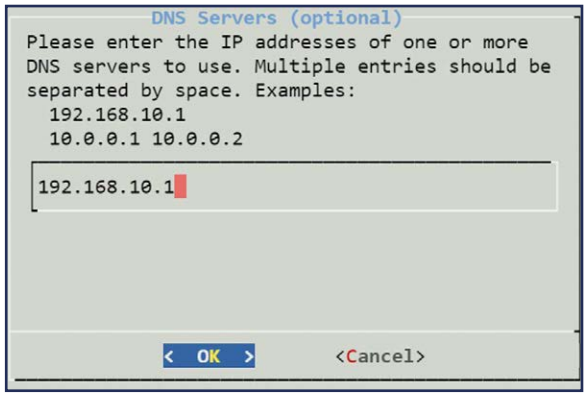
9. For the next step, enter a new **Network Mask**. Press **OK**.



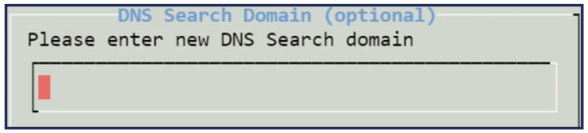
10. Enter a new **Default Gateway**. Click **OK**.



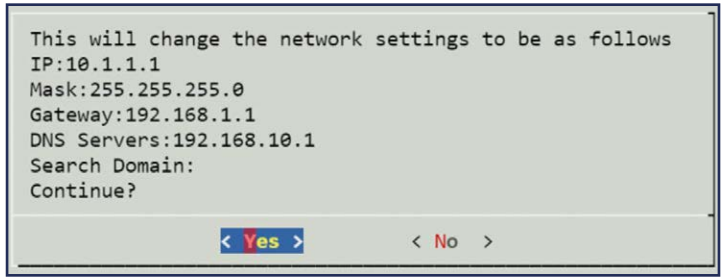
11. Enter a **DNS Server**. Additional DNS Servers can be appended with a space between IP addresses.



12. Unless you plan to use a DNS service to resolve hostnames that are not fully qualified, leave the domain **blank** and press **OK**.



13. Before saving your changes, a **review screen** will display your changes. Confirm the details are correct by choosing **Yes**.

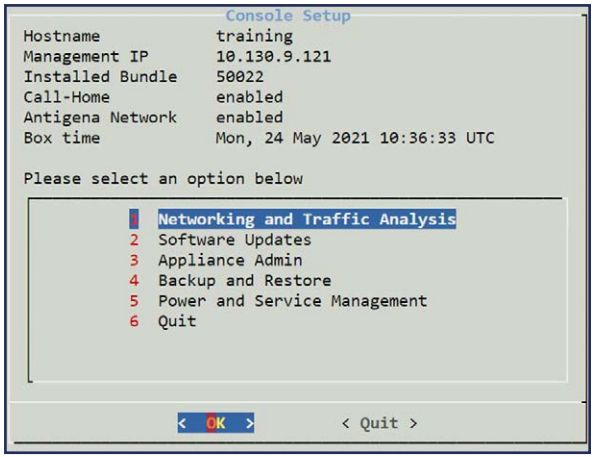


14. Press **Done** and then select **Cancel** to navigate back to the Home screen.

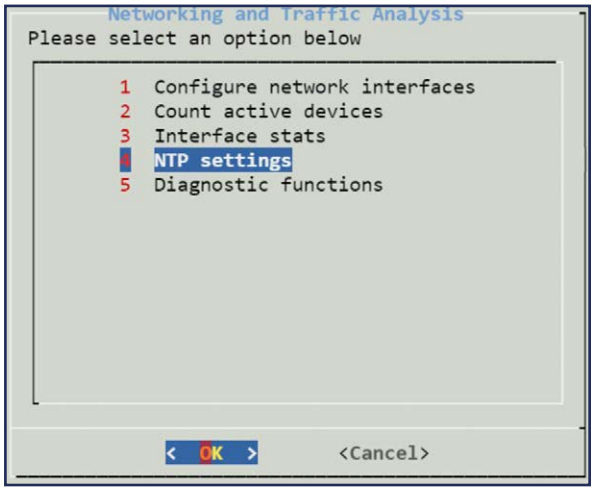
Configure NTP settings

Unless preconfigured, a valid NTP server must be set. This enables the appliance to accurately record events and logging information.

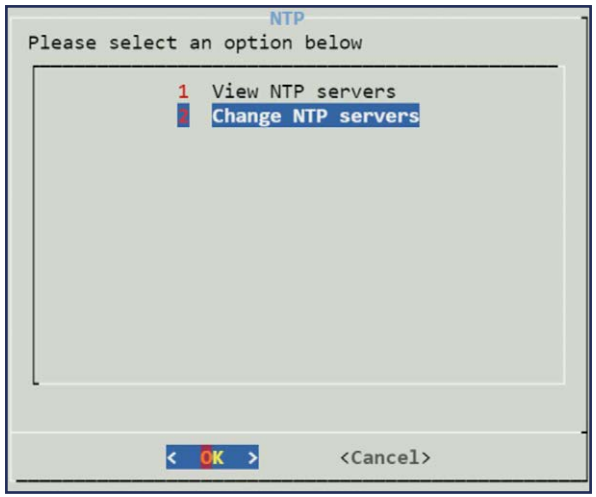
1. From the Console homepage, select option **1. Networking and Traffic Analysis** and click **OK**.



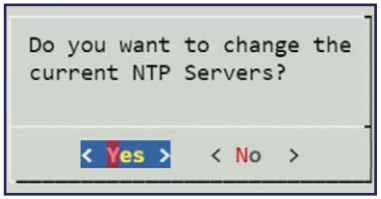
2. Select option **4. NTP Settings** and press **OK**.



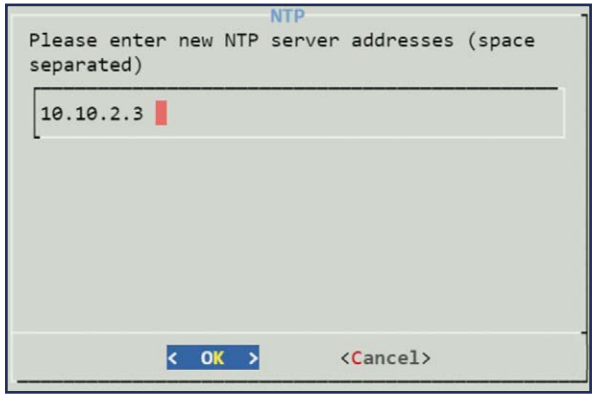
3. Select option **2. Change NTP servers** and press **OK**.



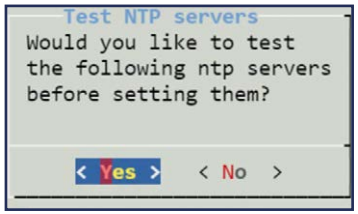
4. Press **Yes** to confirm you wish to make changes.



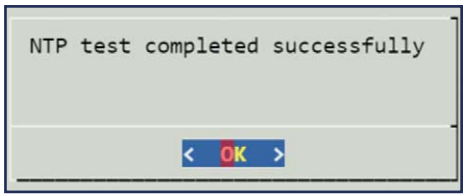
5. Enter a **new address for your NTP Server**. Additional servers can be appended by using a space as a delimiter. Press **OK**.



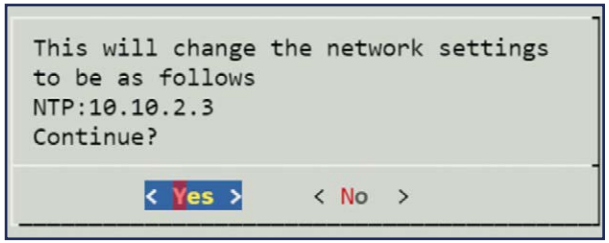
6. Confirm if you would like to **test** that Darktrace can access your NTP Server.



7. Check it **connects successfully** and click **OK**.



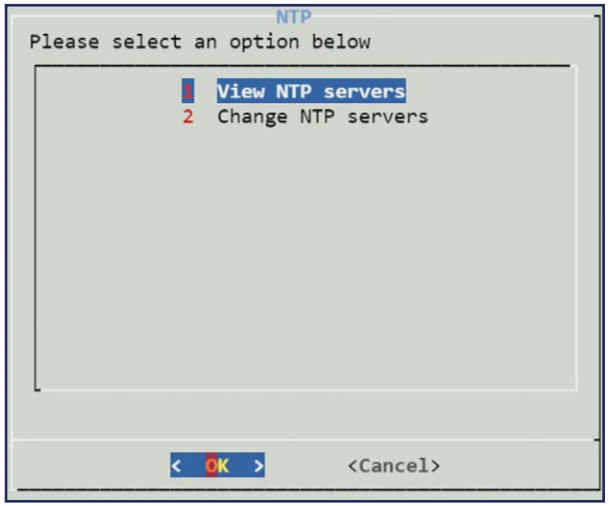
8. Read through the new network settings and **confirm your changes** by pressing **Yes**.

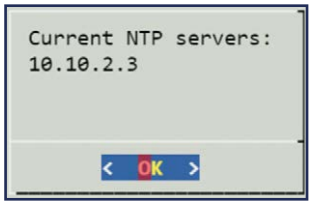


9. Press **Done** to complete changes and set the NTP Server.

10. Select **View NTP servers** to confirm it has been set correctly.

11. **Current NTP servers** will be listed.

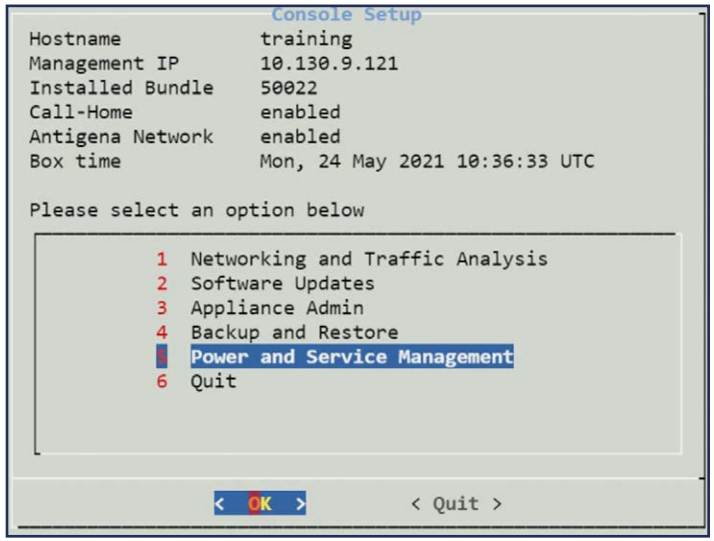




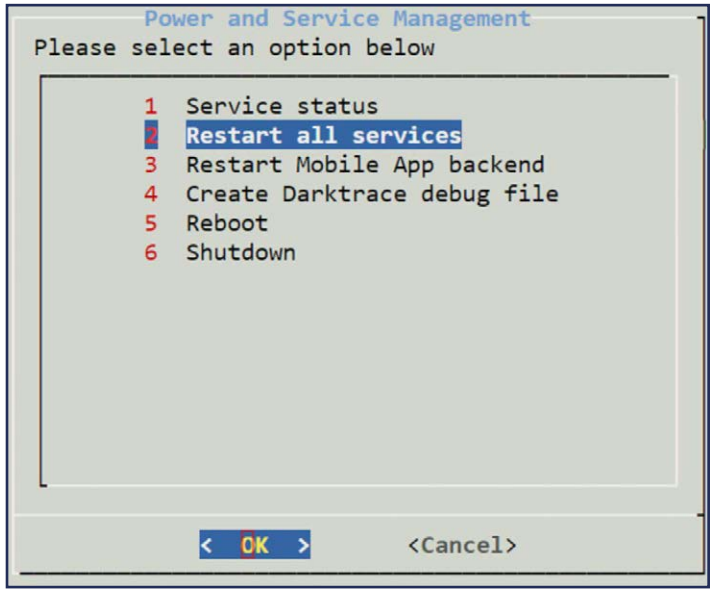
Restart Services

Before completing any additional steps, it is recommended to restart Darktrace Services.

1. From the Console home screen, click **5. Power and Service Management** and press **OK**.

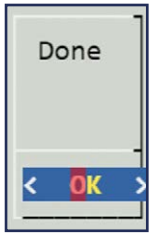


2. Select option **2. Restart all services** and press **OK**.



3. Choose **Yes** and wait for the task to complete.

4. A **Done** dialog will confirm when the operation is complete. Press **OK**.



5. To check the appliance is correctly configured, it is recommended to ping the appliance on the network. Connect the **Admin** port of the Darktrace appliance to the **Switch** and check you can ping the appliance. If you can successfully ping it, you can now proceed to enable Call-Home.

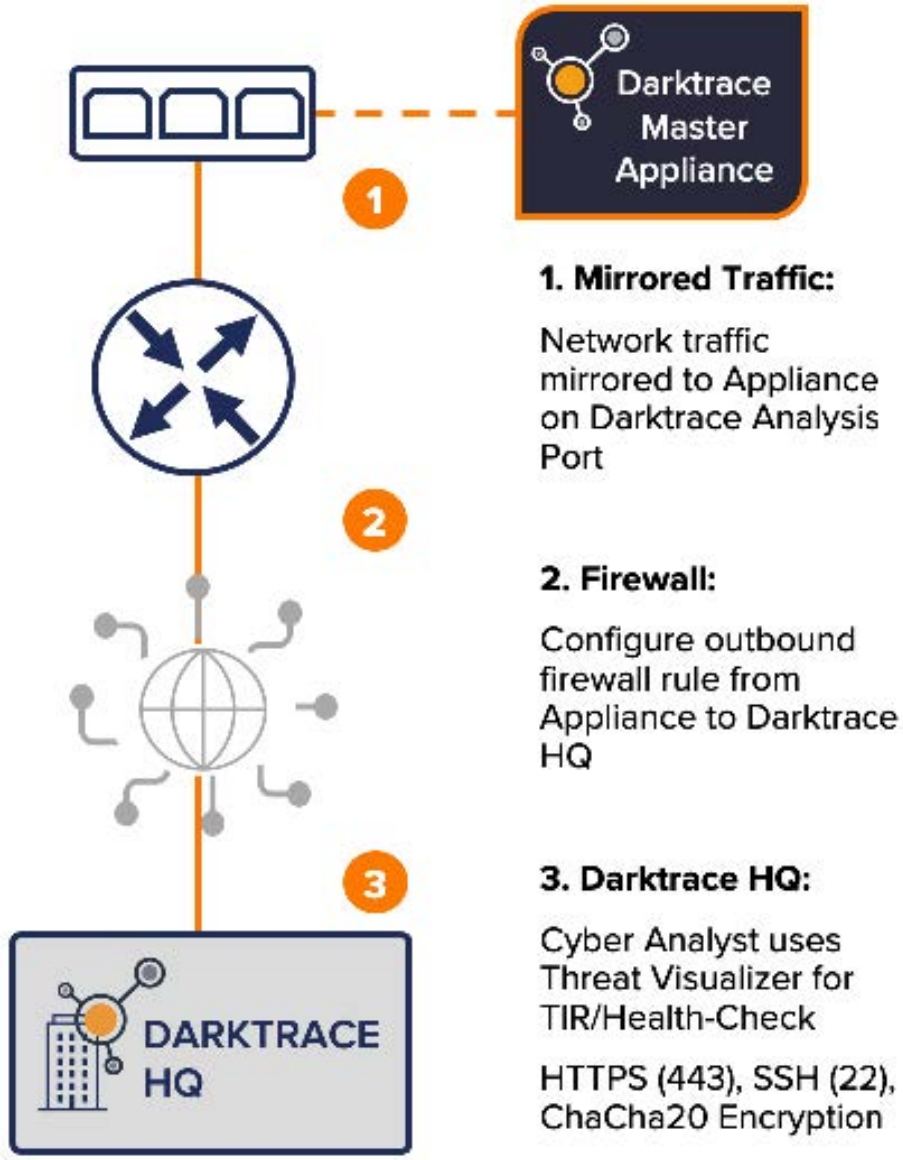
Call-Home

The Call-Home facility allows remote monitoring and troubleshooting of a Darktrace appliance. Darktrace appliances connect back to Darktrace Central Management over a secure and encrypted channel to receive patches and updates.

For managed deployments and POVs, this also enables Darktrace's Cyber Analysts to review and tune the output from the appliance, and Darktrace Support to investigate the appliance when necessary. This secure connection is called Call-Home.

Call-Home requires your network ACLs to permit the appliance outbound access via SSH over port 22 or 443, with SSL wrapping enabled, to the IP ranges of the Darktrace monitoring infrastructure.

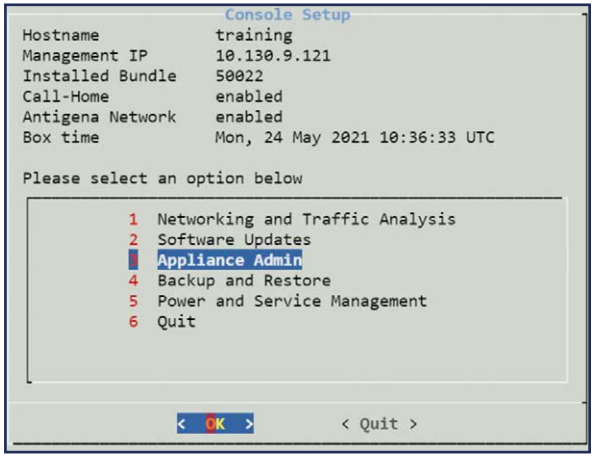
The Call-Home tool also provides the Darktrace Security Operations Centre (SOC) with continued access to the Darktrace Threat Visualizer for the purpose of generating Threat Intelligence Reports.



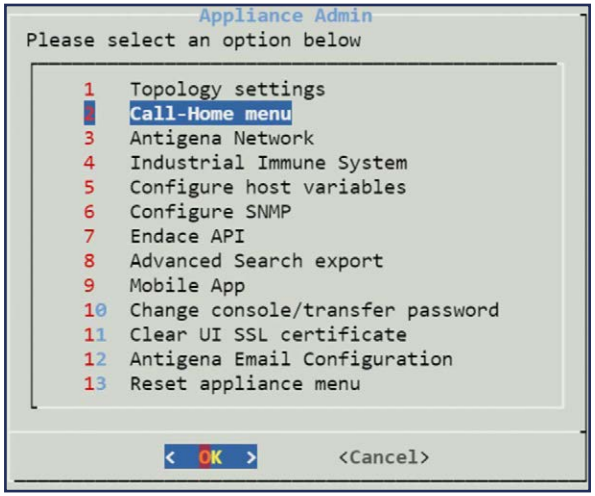
Configure Call-Home Settings

If Call-Home is required, the Darktrace appliance is typically preconfigured before it is shipped to a customer. To view your configuration, follow the following steps:

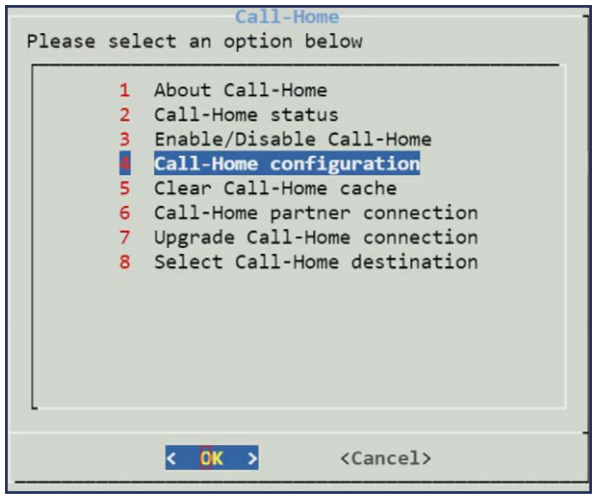
1. On the console menu, select option **3. Appliance Admin**.



2. Navigate to the Call-Home menu by selecting option **2. Call-Home menu**.



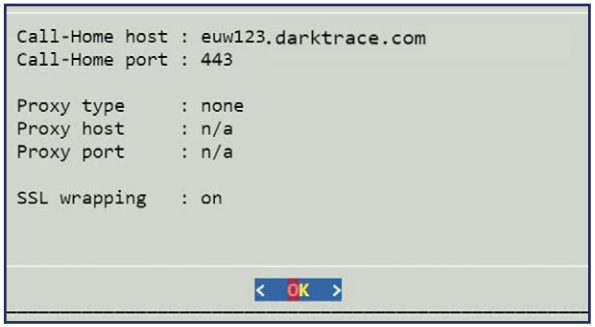
3. Click **4. Call-Home configuration**.



Review your Call-Home configured details.

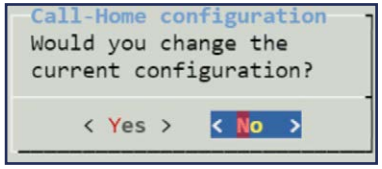
Call-Home is technically SSH, but you can wrap the connection in an SSL stream for the regulations applied on your firewall or proxy. You can also employ a proxy server via HTTP or SOCKS depending on the proxy protocol required.

On boot, Darktrace instances will call home over port 22. If the default Call-Home configuration is applied in the console, the instance will begin calling home over port 443 with SSL wrapping enabled.



Click **OK**.

4. To edit the Call-Home configuration, click **Yes** and complete your changes. Otherwise, select **No** to return to the Call-Home menu.

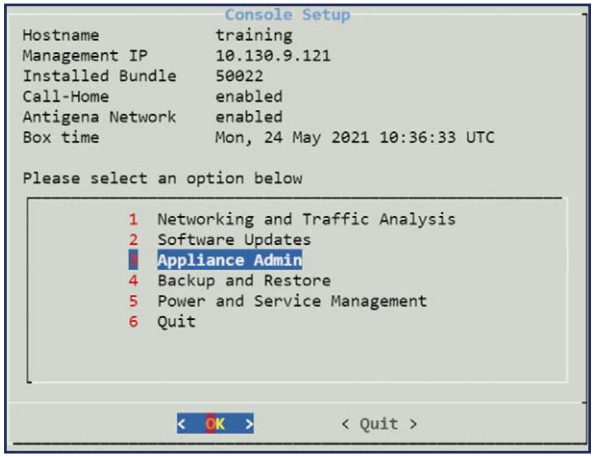


Enable Call-Home

To make changes to an Appliance's Call-Home status, complete the following steps.

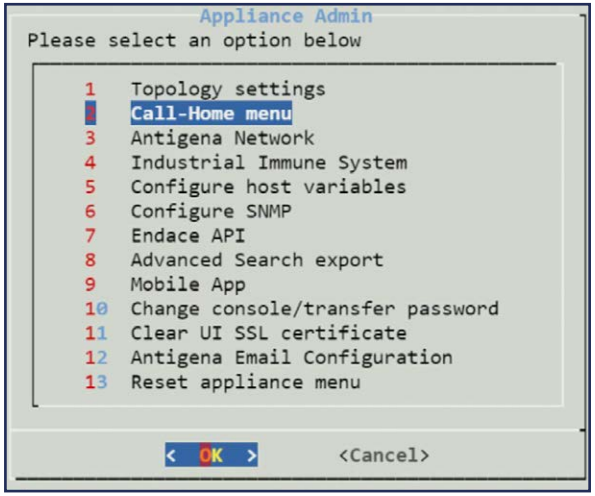
1. If Call-Home is required, select **3. Appliance Admin** from the console home screen.

   Click **OK**.

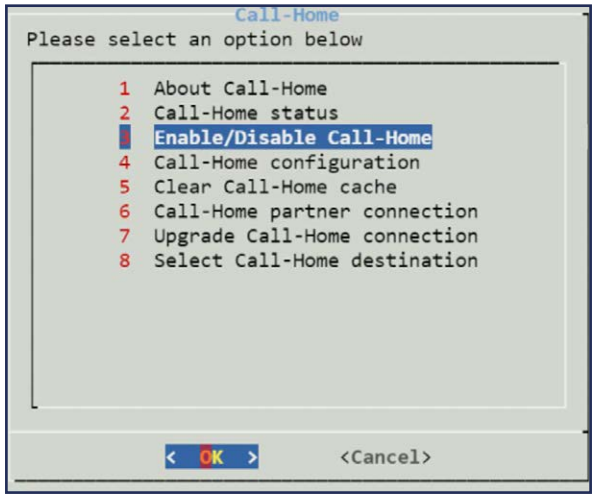


2. Then select option **2. Call-Home menu**.

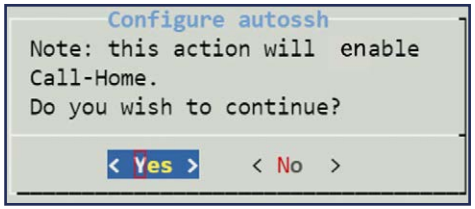
   Click OK.



3. Within the Call-Home options, select **3. Enable/ Disable Call-Home**.



4. Choose **Yes** to confirm you wish to enable Call-Home.

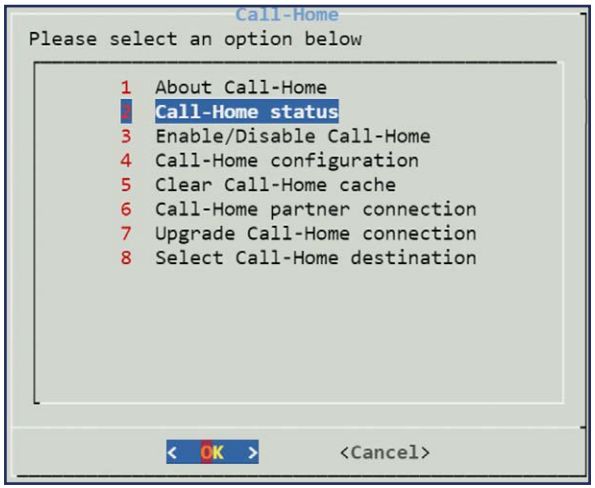


5. A Done dialog will confirm when the operation is complete. Press OK.

   Note: Darktrace will automatically be notified when you successfully enable Call-Home.

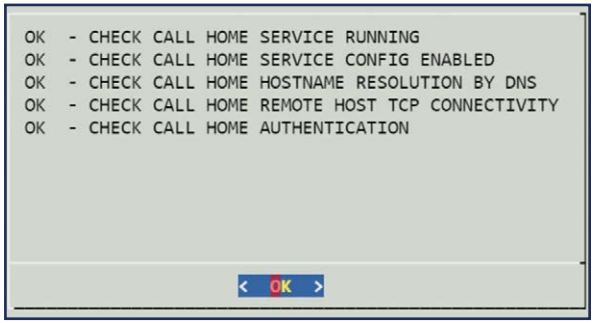
Test Call-Home

1. To test your Call-Home settings, click option **2. Call-Home status** in the Console Call-Home screen. If the configuration is correct, a dialog window will pop up, stating “Call-Home is enabled, checking connection”.



2. If everything is configured correctly, you will see another dialogue box. All the required services **must return OK**.

   If all five rows read OK, the appliance is call-ing home.



If this does not happen, **check the firewall rule** change. Press **OK** to return to the console menu.

Troubleshoot Call-Home

1. If any of the following issues occur the appliance will not be able to Call-Home.

Call-Home Status Fails:

FAIL -> Check Call-Home Service running
Likely the appliance is not working or there is an issue with the cables.
Check the cables. The Admin must connect to Management.
Does it have internet connection?
Check Control Access List.

FAIL -> Check Call-Home Service Config Enabled
This indicates a problem with the Call-Home setting.
Call-Home is disabled. Enable it in the Console.

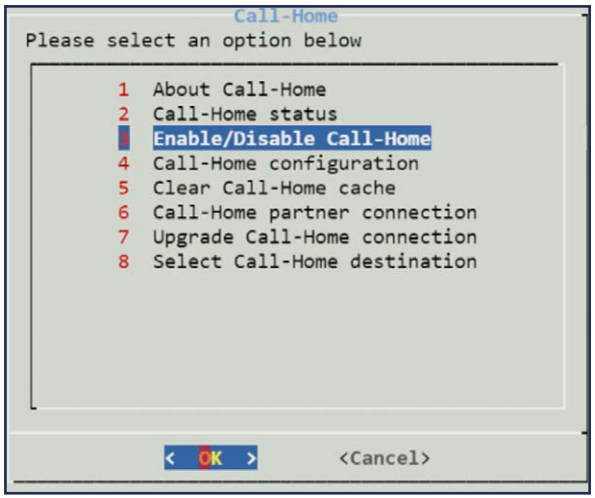
FAIL -> Check Call-Home Hostname Resolution by DNS
Indicates the DNS servers are incorrectly configured.
Check your DNS server connection and details.

FAIL -> Check Call-Home Remote Host TCP Connectivity
Suggests a Firewall is blocking the connection.
Enable a new rule for the firewall to accept it.

FAIL -> Check Call-Home Authentication
Indicates an issue with the network configuration, using the incorrect gateway, or the wrong IP and subnet has been set. The IP and gateway have to have same subnet (for example, on the 192, 10 ranges).

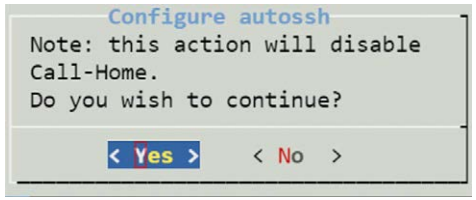
2. Note if there still are issues, the cache may need to be cleared.

   First, **disable call-home** by selecting option 3 from the call-home menu.



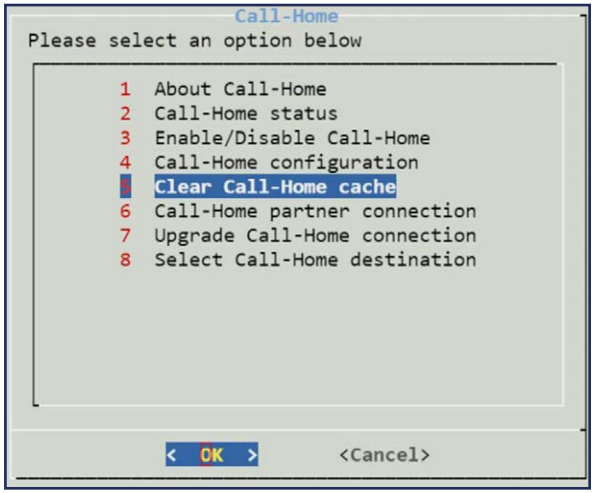
3. The console will ask if you wish to continue.

   Select **Yes** to disable call-home.



4. From the Call-Home menu, select option **5. Clear Call-Home cache**.

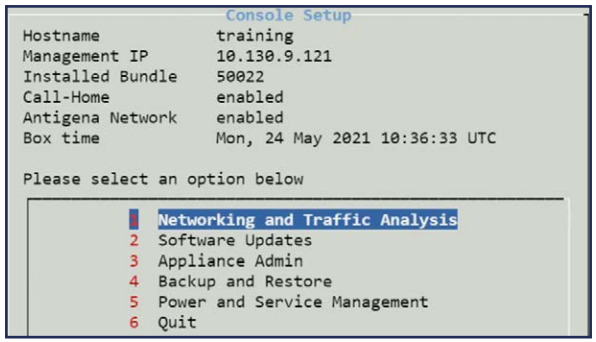
   This will delete the .ssh/known_hosts file, used by call-home SSH authentication, and may help in solving some issues.



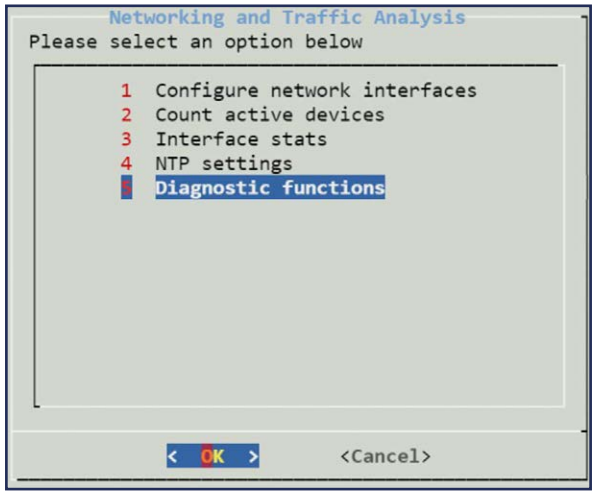
5. A **Done** dialog will appear to confirm the cache has been cleared. Click OK to dismiss.

6. If after following the above steps there still are issues, you might want to use the Diagnostic Functions provided with this application.

   Go back to the main menu, select **1. Networking and Traffic Analysis**.

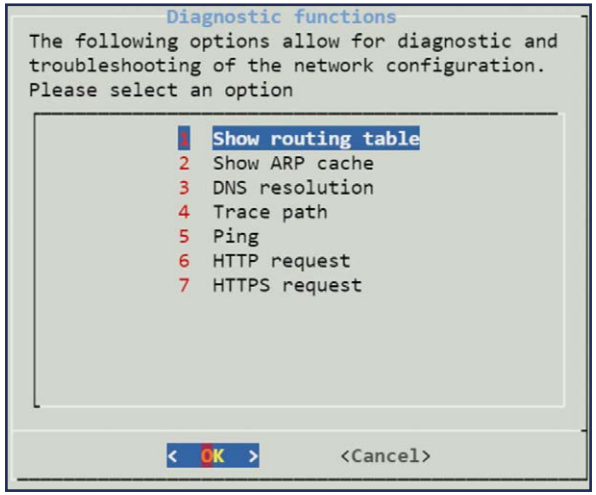


7. Select **5. Diagnostic Functions**.



8. This menu offers various ways to **troubleshoot** networking issues.

   You should already be familiar with these commands.

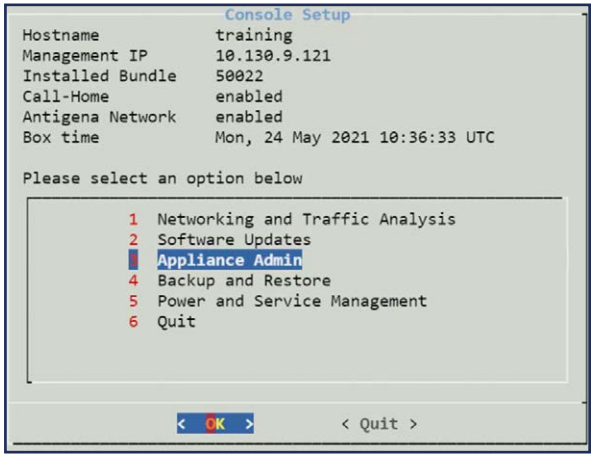


Restart the Call-Home Connection

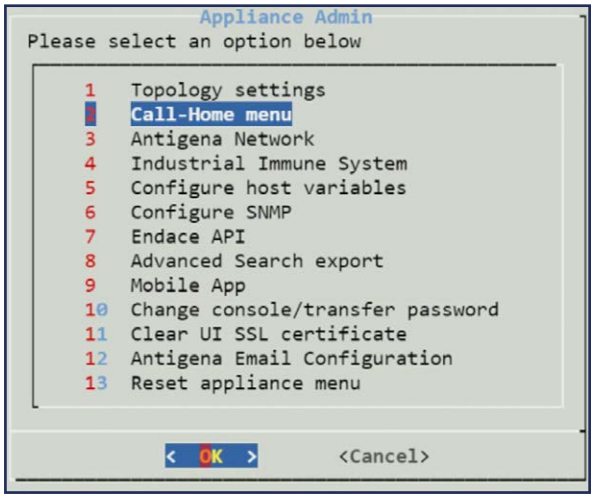
In the eventuality that the Call-Home connection goes down, it may require restarting. This is completed via the console application.

1. Navigate to the Appliance Console menu.

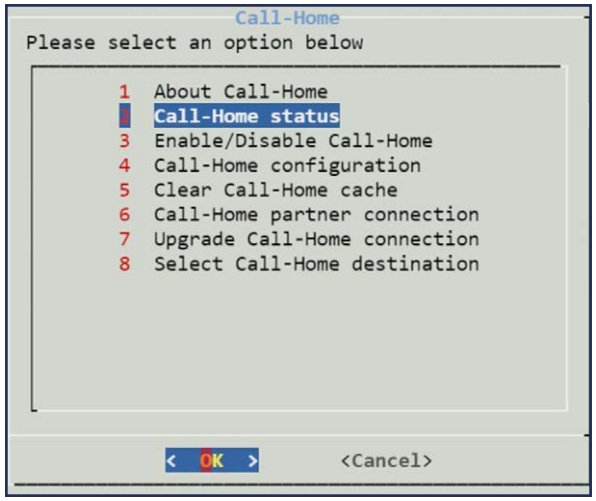
   To access Call-Home connection options, select menu **3. Appliance Admin**.



2. From the Darktrace Admin menu, choose **2. Call-Home menu**.

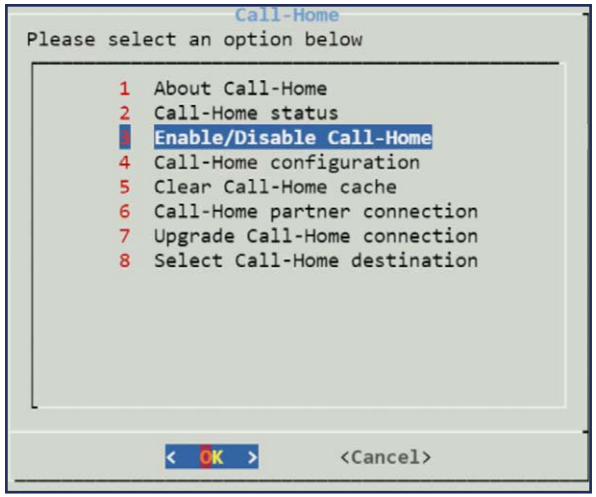


3. At this point, it is advised that you check the status of Call-Home through menu **2. Call-Home status**.



4. The connection status can be changed (connection enabled/ disabled) via option **3. Enable/Disable Call-Home**.

   If the status is set to “enabled”, choose the option, 3. Enable/Disable Call-Home, twice to restart Call-Home.



Partner Call-Home

Partner Call-Home enables partners to have the same ability as Darktrace to remotely access an appliance. This allows partners to service and support their customer Darktrace deployments.

There are two main methods for partners to access customer Darktrace appliances.

1. **VPN and IPSec tunneling**

   The customer provides access to their appliance on their network. From a partner perspective this requires minimal effort to configure as the emphasis is on the customer to provide a connection. The customer controls how to access their appliance and determine setup access policies software required such as VPN clients. This method can be very useful for partners during a POV as quick and easy way to access an appliance. However, there can be delays waiting for a partner to enable access.

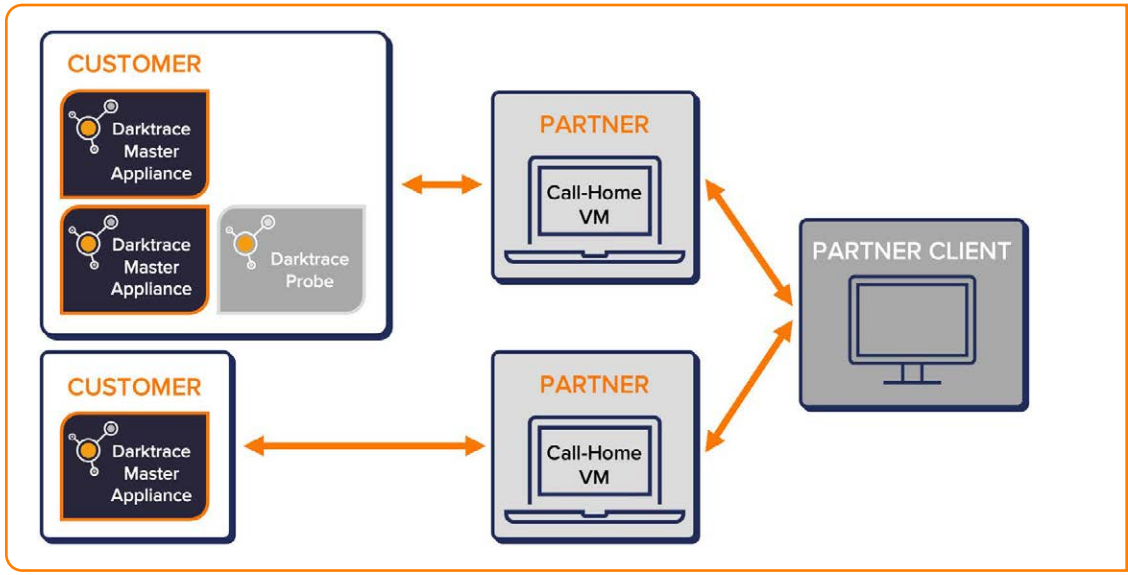
2. **Partner Call-Home**

   The partner must configure a VM to reverse SSH into a customer's appliance. This may initially require more effort for the partner to setup a VM and achieve a connection, however it can facilitate the monitoring and support of a customer's appliance. It can also improve security as partners do not require access to a full network, just the Darktrace appliance.

Partner Call-Home Overview

Technically speaking, Call-Home is reverse port forwarding through SSH, which enables you to reach the destination with an internal IP address that is not normally accessible from outside a network.

The example below demonstrates how an appliance can be accessed through the Call-Home server from anywhere outside the customer's network. A Darktrace appliance connects to a VM over SSH and then in turn is connected by a client device to access the appliance's console or Threat Visualizer application.



A separate Call-Home VM is required for each customer. However, only one Call-Home VM is required for multiple Master appliances or probes.

Partners must install a server to run SSH such as on a Linux VM to enable Call-Home. You need to configure the Darktrace appliance to autossh to the partner's SSH server and establish an SSH tunnel so that the partner can access the appliance remotely on a client device such as a laptop.

Call-Home must be enabled on the customers appliance console menu, so it can connect to the external IP of the partner. After allowing the connection at the firewall, it forwards to the Call-Home server and the SSH connection between the appliance and the server is established. This connection works as an SSH tunnel through which the Call-Home server can access the HTTPS and SSH port of the appliance using port forwarding.

The ports are assigned as follows:

- SSH (22):
  - 10000 + 10 x <Up to the hundred's place of the middle part of appliance hostname> + <The last part of appliance hostname>
- HTTPS (443):
  - 30000 + 10 x <Up to the hundred's place of the middle part of appliance hostname> + <The last part of appliance hostname>

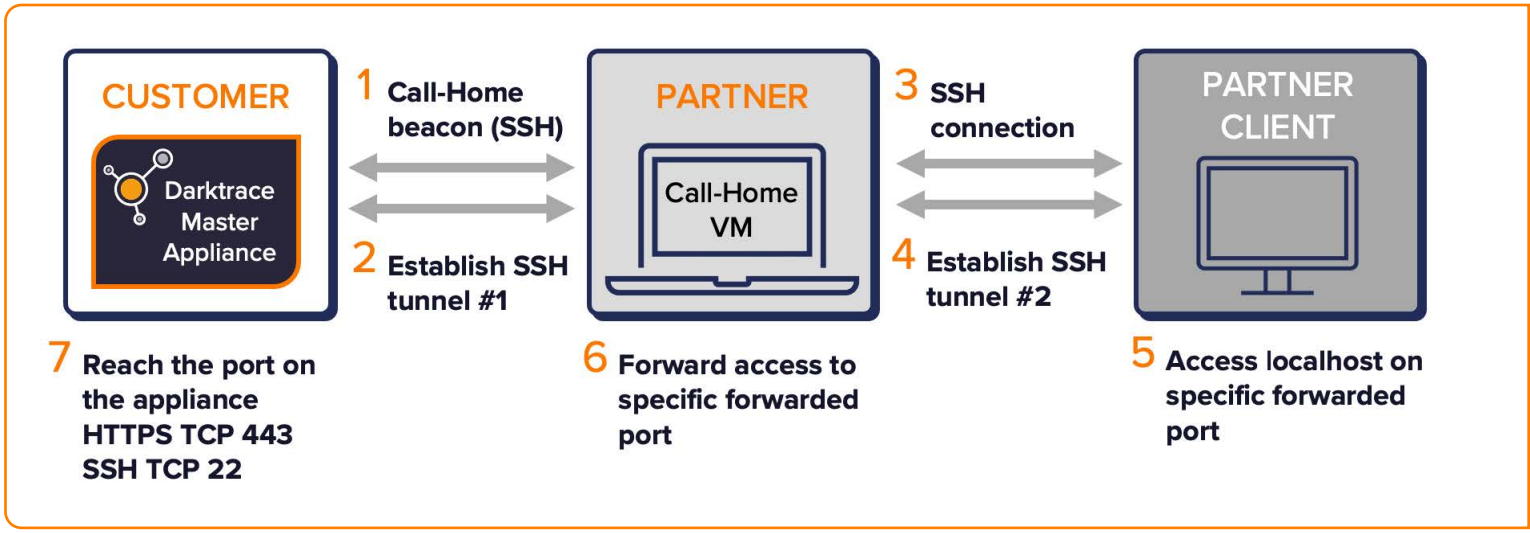
Here are some examples:

- dt-123-01
  - SSH: 10000 + 123 x 10 + 1 = 11231
  - HTTPS: 30000 + 123 x 10 + 1 = 31231
- dt-4839-01
  - SSH: 10000 + 839 x 10 + 1 = 18391
  - HTTPS: 30000 + 839 x 10 + 1 = 38391
- dt-1234-12
  - SSH: 10000 + 234 x 10 + 12 = 12352
  - HTTPS: 30000 + 234 x 10 + 12 = 32352

For example, when the call-home server connects localhost on the specific forwarded port (e.g. if appliance number is dt-123-01, the forwarded HTTPS port and the SSH port are 31231 and 11231 respectively), it is forwarded to the correspondent port on the appliance.

Similarly, you can connect to the call-home server via SSH and then establish an SSH Tunnel for port forwarding. You can decide the forwarded port on your client by yourself. For example, if you use the command ssh –L 1443:localhost:31231 <your ID>@<VM IP> and access localhost on TCP 1443 port, you are forwarded to TCP 31231 on the appliance.

Through the two SSH tunnels, you can eventually connect to the appliance. Taking the above case as an example, you first access localhost on 1443 for HTTPS and you are forwarded to TCP 31231 port on the VM. As the port is also forwarded to TCP 443 port on the appliance, you finally reach it via the multi-hop route.



Configuring Partner Call-Home

There are three steps to setting up Partner Call-Home:

1. **Request a public key to be saved on the partner's SSH server for authentication.**

    - Request to Darktrace Support via a ticket to get the Public Key of the Darktrace appliance. The key format is the following:

      ssh-rsa
      aloadofrandomlettersnumbersandtheoccasional+or/butnospaces
      autossh@dt-xxx-yy

    - Make sure that there is no space or line break on the second line

2. **Setup a Linux SSH server and configure it to allow the Darktrace appliance's SSH to access the LinuxSSH server.**

    - Create autossh user and it's home directory
    - Add the appliance's public key to <autossh home directory>/.ssh/authorized_keys
    - The authorized_keys file stores public keys for clients that are authorized to login to the server as autossh user without password authentication.
    - Set the appropriate permission of the .ssh directory and authorized_keys file so that autossh user can read the file
    - Edit /etc/ssh/sshd_config file to enable public key authentication PubKeyAuthentication yes

As explained so far, once you successfully configure both the appliance and the SSH server, the appliance automatically connects to the SSH server and SSH tunnel is established, which enables you to access the appliance through the SSH server.

Needless to say, the server should be secure since it becomes a critical problem if unauthorized users can access the appliance, which contains detailed information of the customer's network. In general, partners should strictly conduct identity and access management, and network access control for the server.

For example, user credentials for the server must be given to only authorized persons and user authentication should be done in a more secure way such as multi-factor authentication and public key authentication. The server should not be exposed to the external network directly like web server: it should reside in internal network behind firewall and router so as to make access to the server reachable only on the specific port and from the authorized IPs and persons.

3. **Configure the Darktrace appliance to beacon to the Partner's SSH Linux Server.**

    Set the destination IP and port for partner Call-Home on console menu > 5. Darktrace Admin > 4. Call-Home settings > 10. Call-Home partner connection.

Troubleshooting

There are several points you should check when partner call-home does not work.

1. **Check whether the appliance can reach the partner's IP**

   It's the same check for call-home to Darktrace HQ. Typically, it's worth it to check firewall (and/or proxy if used) settings on the customer's site.

2. **Confirm that the appliance is properly configured for the partner call-home setting**

3. **Make sure the public key is valid**

   If the public key is given in a corrupted format, the server doesn't recognize it properly. Check if the public key does not contain unnecessary space and line break.

   If you can see continuous failed accesses from the appliance in SSH access log on the server, it is likely that the public key is not valid.

4. **Confirm that public key authentication is enabled**

   You can try public key authentication from another client to see if it really works. Instead of the public key of the appliance, you add the client's one to authorized_keys file and then access the server from the client. If it works, you can login to the server without password authentication.

5. **Confirm the partner's call-home mapping is properly done**

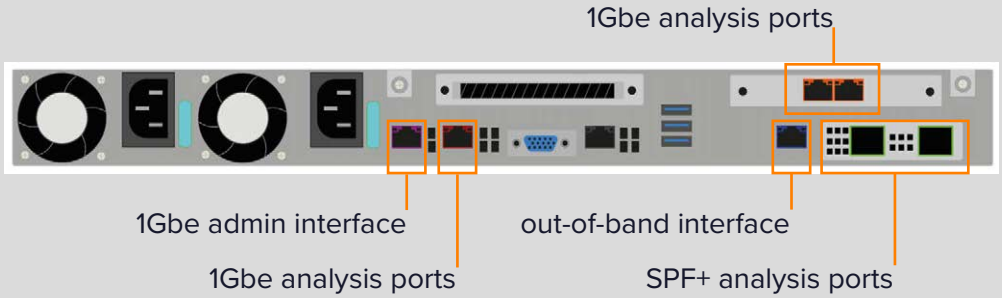
   Partner call-home beacon to the partner's external IP must be forwarded to the SSH server's internal IP.

Ingesting Data

With the previous settings complete, the Darktrace appliance can now be connected to the Mirroring Port.

Darktrace appliances are configured for a range of sizes. Each type of appliance may have different ports.

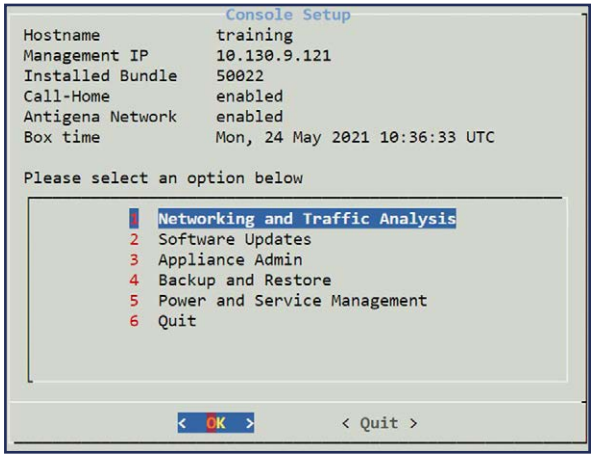
Example: DCIP-M (Medium sized appliance)



1. Connect the **Mirroring Port** to an **Analysis Port** on the Darktrace Appliance. Darktrace will immediately begin capturing and analyzing packets to learn the patterns of life for devices and subnets on your network.

2. On the console home page, select **1. Networking and Traffic Analysis**.

3. Note there are **Count active devices** and **Interface stats** options.



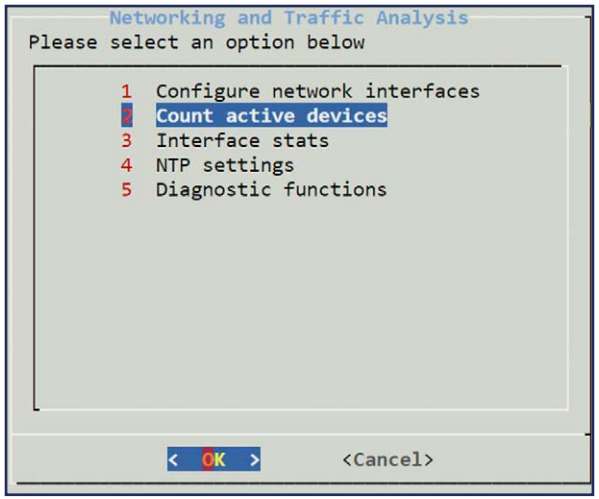
These are useful functions for checking that data is flowing to the appliance from your traffic mirroring port or tap connection.

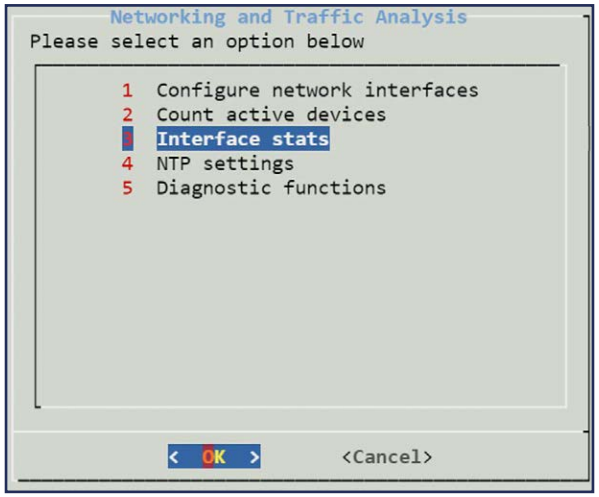
Select option **2. Count active devices**.

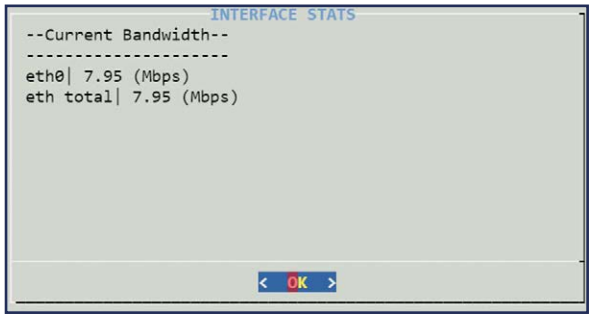
4. This displays all devices which Darktrace has recently seen running on the network. The number will rapidly jump as Darktrace identifies new devices. Check the number of devices is greater than zero. Choose **OK** to return.

5. Next, select **3. interface stats** to review current bandwidth usage.

6. If the throughput remains lower than expected, check the data is plugged into the correct port on the appliance. Select **OK** to return.







5. Reviewing Traffic Status

After installing an appliance and carrying out the necessary configuration in the Console, it is recommended to review the traffic status using a handful of key pages in the Threat Visualizer interface.

Threat Visualizer

Before logging into the Threat Visualizer, Darktrace recommends waiting 15 minutes to allow enough time to check if data is being ingested correctly, particularly for longer connections. It may take up to a week for Darktrace to build up a “pattern of life” for the majority of network devices.

1. Navigate to the **IP address** of the appliance in a web browser:

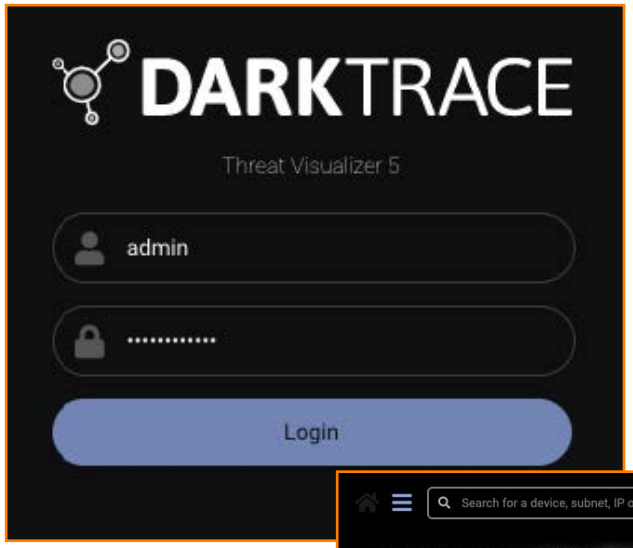
   https://<appliance IP address>

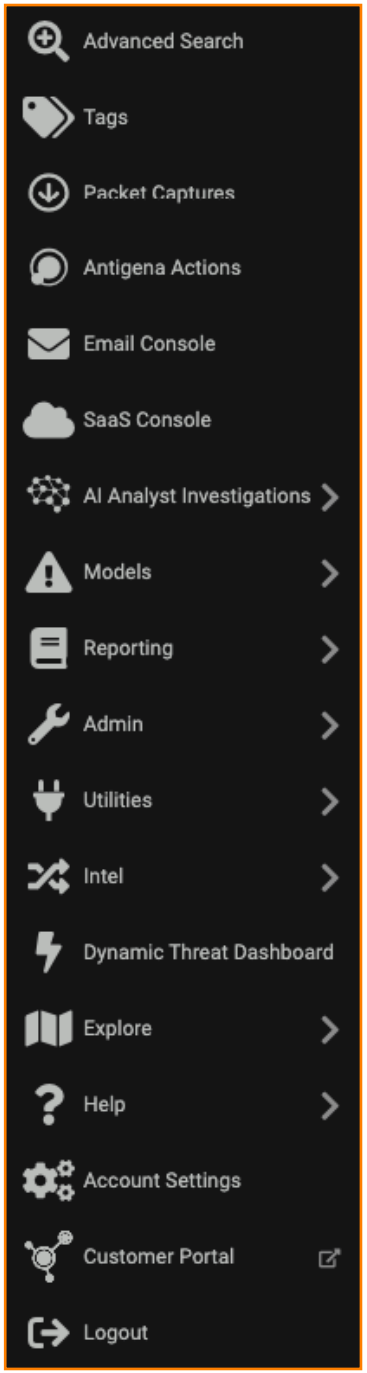
2. Check that the Threat Visualizer **login screen** loads.

3. Login with the **admin** username.

   Note: You should have received an administration password from Darktrace.

4. Make sure you have full access to the items Threat Visualizer **main menu**.

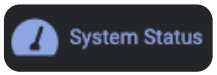


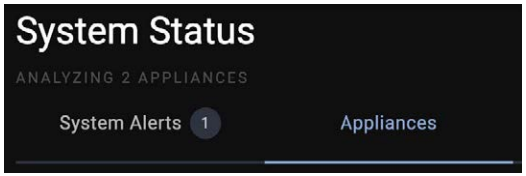


System Status

A few simple checks can quickly confirm that the Darktrace appliance is ingesting data as expected.

1. From the Threat Visualizer **Main Menu** navigate to Admin and select **System Status**.

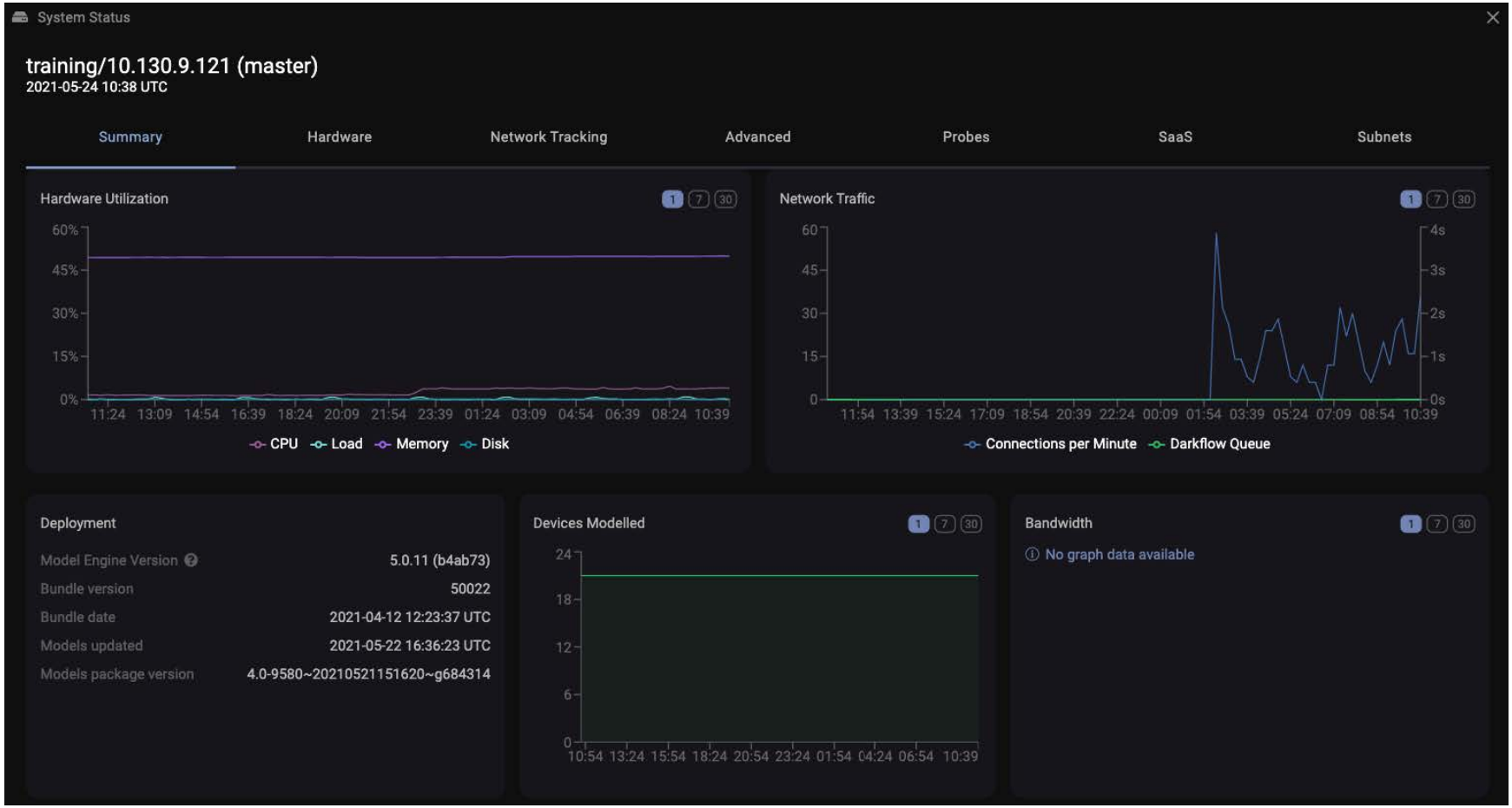




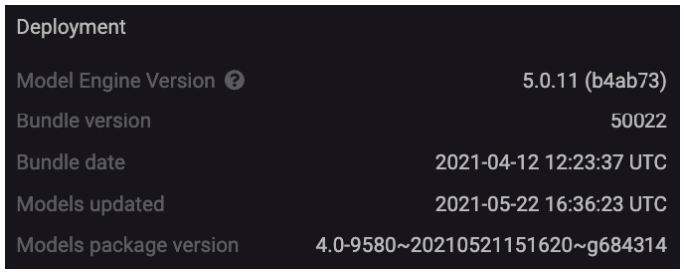
2. The System Status page will open in a new browser tab. On this page, select the **Appliances** tab.

3. Multiple appliances may be listed, including masters and probes. Select the **Master** appliance.

4. A new window opens showing a **Summary** of the selected appliance. Glance over these status values.

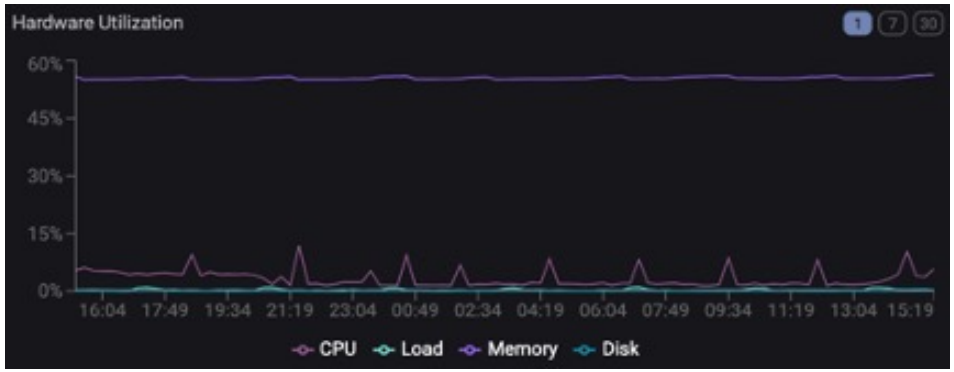


5. It is recommended to always install the latest version. The current version can be confirmed by viewing the **Deployment** section on the Summary page.



Similarly, the **Version Information** can be viewed in the **Advanced** tab.

6. Next, review the **Hardware Utilization** graph in the Summary page. Check the **CPU**, **Load**, **Memory** and **Disk** values for the last day, week or month. Large values may indicate the component is overloaded.

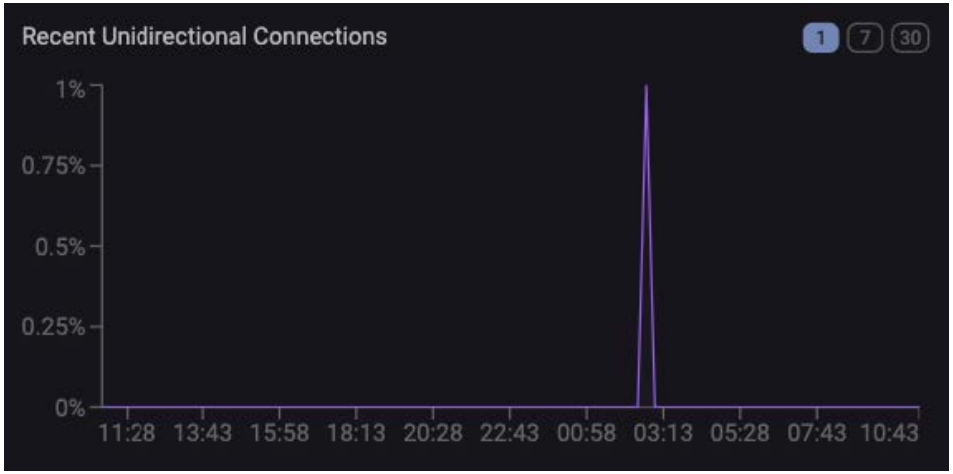


Note: The same graph can be viewed in the Hardware tab.

7. The **Bandwidth** graph in the Summary page can provide a useful snapshot of the ingested data flow. This same graph can be found in the **Hardware** tab.

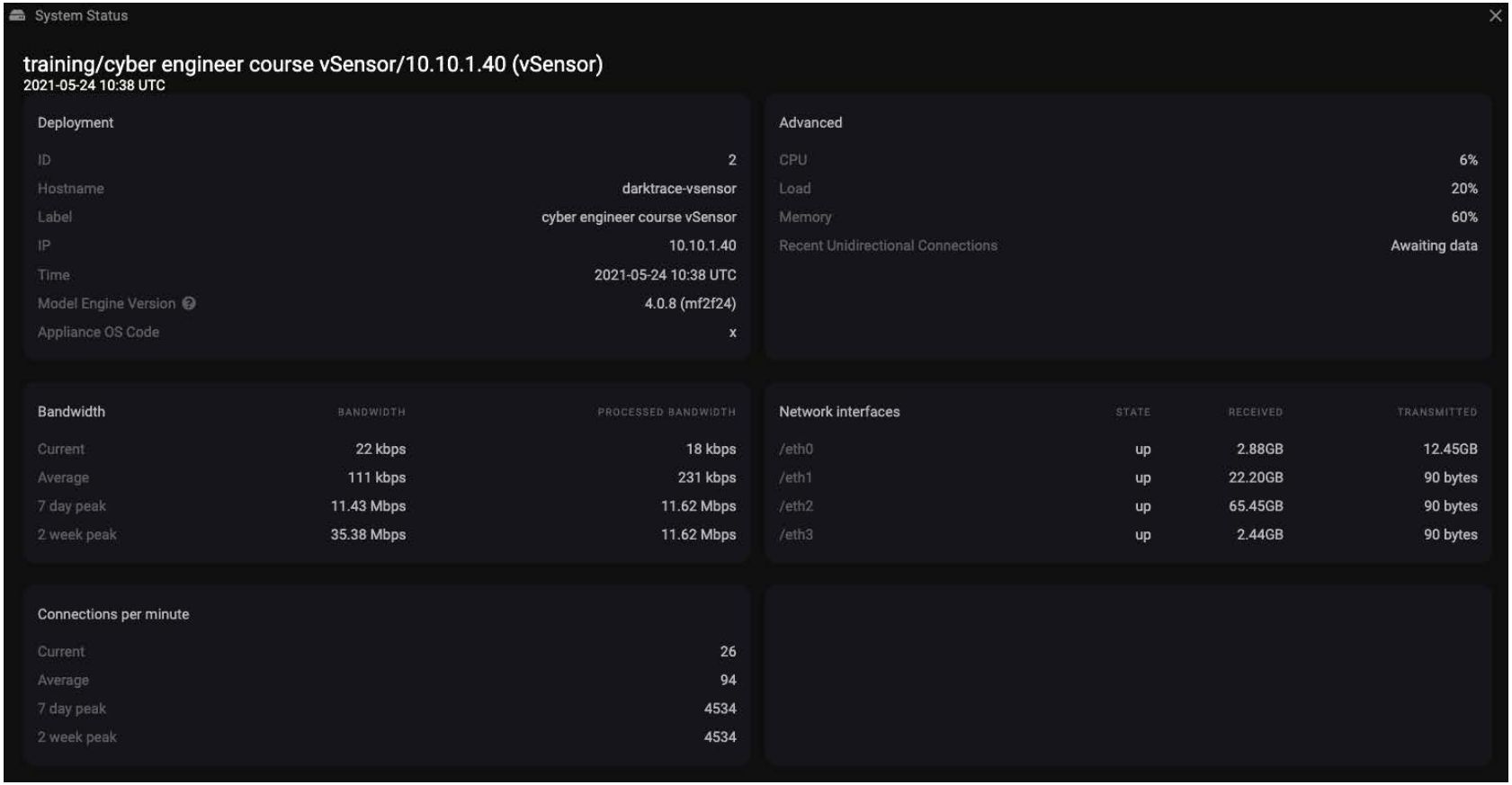
Further information about the bandwidth is tabulated in the **Network Tracking** tab. Process bandwidth occurs after the deduplication of packets. Check that the current bandwidth is at expected levels.

8. Another useful value to review is the **Recent Unidirectional Connections**. This data is graphed in the Network Tracking tab and can be viewed over a day, week or month. Check to see if the value remains below 10%.
Recent unidirectional connections are commonly caused by split routing, load balancers or a misconfigured/overloaded mirrored port such as SPAN. The value is typically between 0% to 10%.



Too much unidirectional traffic means significant amounts of network traffic could be missed, such as an extra Core Switch or missing VLANs. It can also be caused by forgetting to mirror both Rx and Tx streams of network traffic or failing to mirror the traffic from all relevant capture points such as from load-balanced core switches.

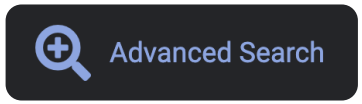
9. Finally, it is recommended to check the same settings for the probes also. Close the Systems Status window for the appliance and **select a probe from the Appliances tab**. This opens a similar window where probe specific data can be reviewed.



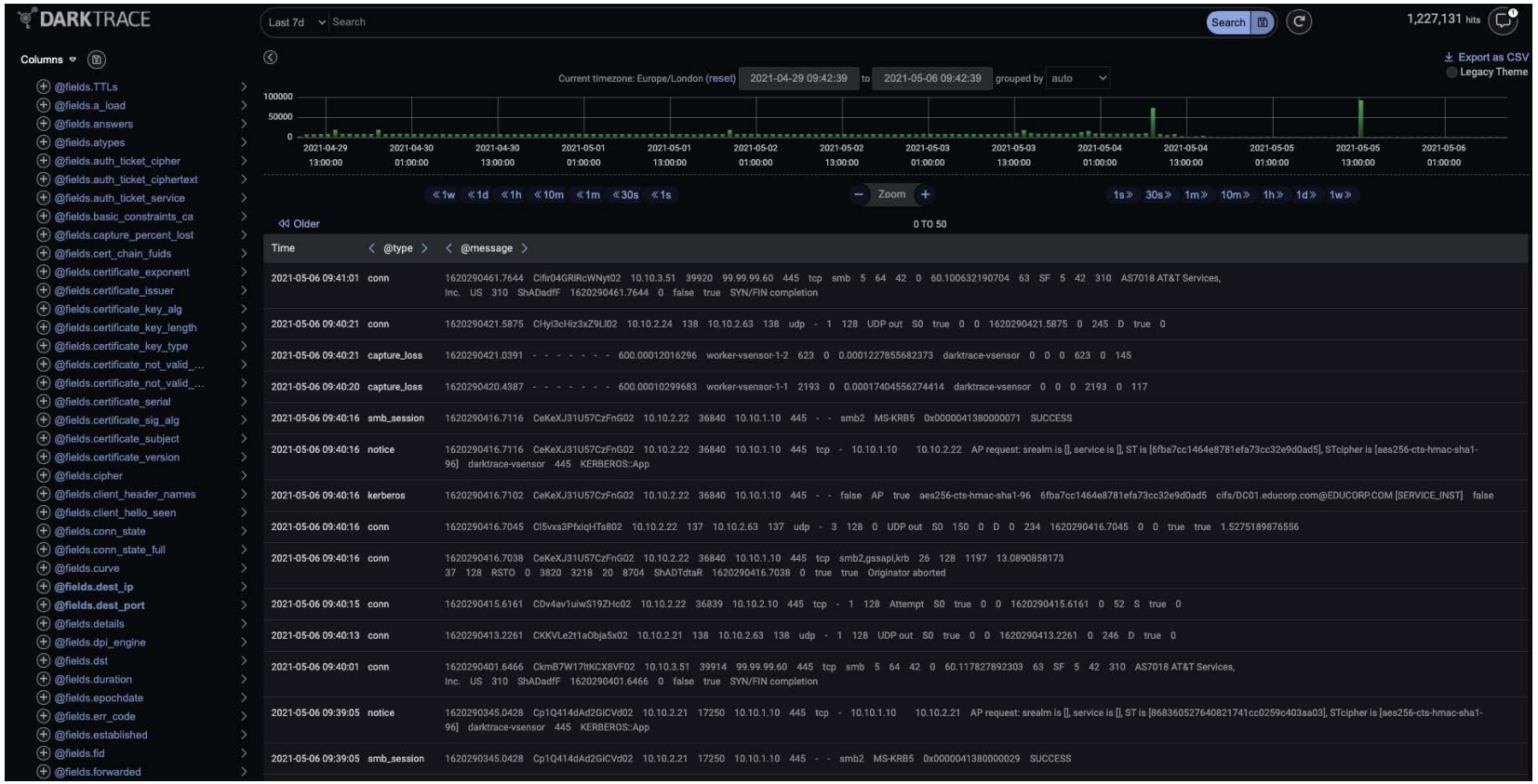
Advanced Search

In addition to the Threat Visualizer, the Advanced Search interface can provide useful information about the health of a network and the data ingestion process. For best results, it is recommended to wait seven days to allow for the tracking of more network traffic and protocols. For example, on some networks, RDP or SSH sessions may not be a common occurrence. However, it is advisable to do a quick check over the last 24 hours to confirm traffic is instantly being ingested.

1. Under Menu, select **Advanced Search**.



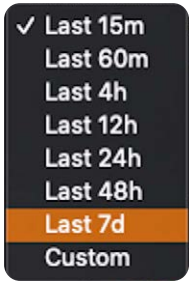
2. Set the date range to **Last 24h** and do not enter any search criteria.



3. Check that data is **initially being ingested** after the appliance install.

Note: This is only an initial test and Advanced Search should be reviewed again following install.

4. At a later stage, once Darktrace has had time to learn the network, come back and perform the same check but over the **last 7 days**. Without inputting any queries into the search bar, look for any obvious gaps in traffic on the graph.



5. Use the table on the following page to **perform a variety of checks** on the traffic.

Advanced Search Check	Advanced Search Query
Searching for all connection events with "0" IP bytes on the response field is a good indicator of unidirectional traffic. Occasionally a TCP request receives a rejection. This is a bidirectional request that was turned away at the door such as at the Firewall. This will show events defined as not completing a Syn-Ack handshake, but also limits it to connections not heard from again.	**@type:conn AND @fields.resp_ip_bytes:0**
This connection query will find missed TCP handshakes. The last operator will remove all normal termination connections, which just leaves the connections that have been missed. It may be useful to click the arrow by the Source IP filter in blue and select the "Score" function. This will show if a particular IP address is the cause of many of the missed connections.	**@type:conn AND @fields.proto:tcp AND NOT @fields.conn_state:ShA*** **@type:conn AND NOT @fields.conn_state:ShA***
Change the Advanced Search time range to the last 24 hours and look for events relating to Kerberos traffic. Check you can see login requests for users by reviewing the @fields.principal_name value. Appending AND @fields.success:"False" may help highlight and diagnose any login issues.	**@type:kerberos**
Searching for HTTP will confirm whether web traffic has been ingested in to the appliance. Check for both internal and external traffic. For example, search for @fields.host:www.google.* to review external requests. Check for an appropriate number of events; a typical mid-sized network of 4,000 devices would usually return well over a million HTTP hits in 24 hours.	**@type:http** **@type:http AND @fields.host:www.google.***
In addition to HTTP traffic, TLS/SSL events are also expected in significant volume. Often, the number of events is approximately half that of http events.	**@type:ssl**
A search for port 445 will reveal SMB 2 and/or SMB 3 traffic. On many networks, SMB can represent a significant proportion of traffic on a network.	**@fields.dest_port:445**
A query for DHCP will reveal hostname and domain information found on the network.	**@type:dhcp**
Notice events reveal all sorts of information about network traffic, including printer, Kerberos, and SMB events. Review the @fields.note field for a description of each event.	**@type:notice**

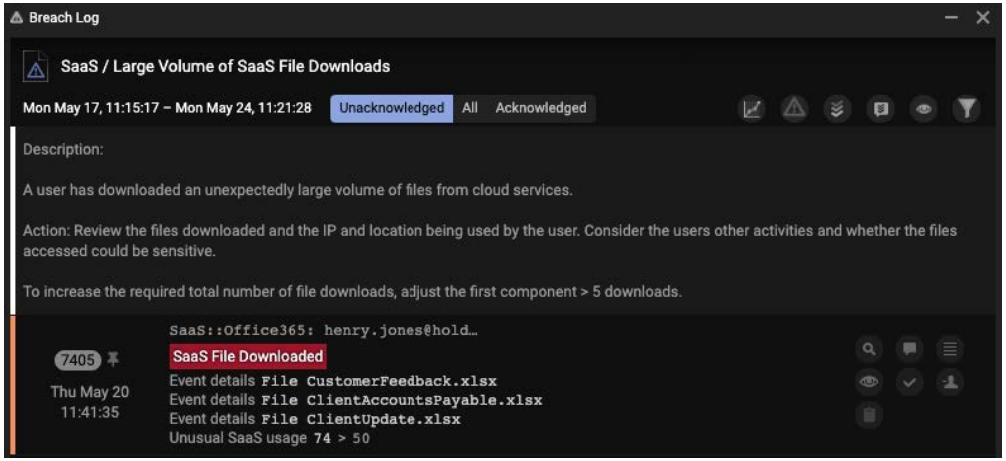
6. SaaS Modules

Whether in the cloud or physical, the Darktrace Master will interrogate the security APIs of the relevant Cloud/SaaS solutions. These include AWS, Azure, Salesforce, Office 365, Box, Dropbox, G Suite, Jumpcloud, Egnyte and Zoom.

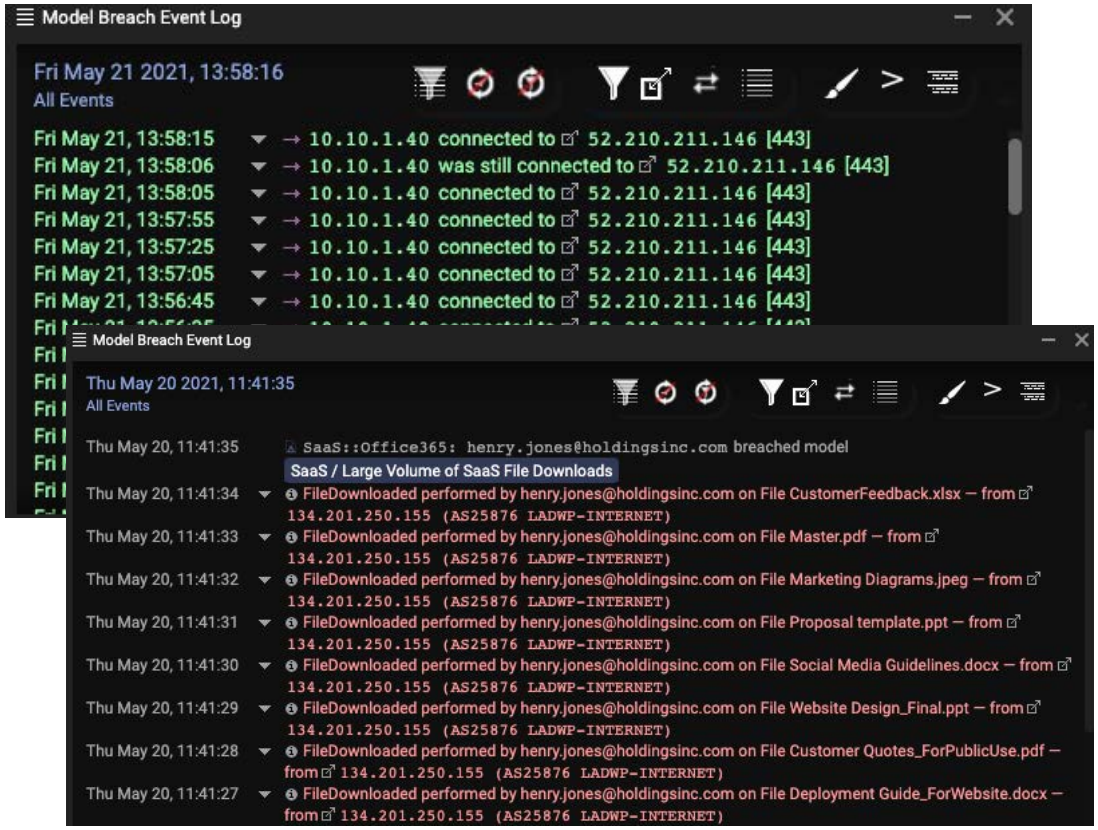
Without a SaaS module, Darktrace will see traffic to these solutions, but it will be encrypted. For example, the event logs will show encrypted communication over port 443, but you will not be able to identify which credential is used, which files are uploaded, downloaded or deleted.

When configured, you can receive full visibility about which files are being edited. In the example below Darktrace lists all the files deleted quickly helping analysts understand the nature and seriousness of this event.

When combined with Darktrace's Cyber AI, it can even deduce suspicious anomalies. In the example below, Darktrace has triggered a model breach due to the unusual SaaS deletion of files:



View the Threat Visualizer Administration manual and eLearning on the Customer Portal for information about how to configure SaaS modules.



The Office 365 module monitors 11 categories:

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

Without a SaaS module, Accounts can have files deleted without any notification or Antigena response.

7. vSensors

A Virtual Sensor ("vSensor") can be installed as a virtual appliance to receive connections from a virtual switch. In this chapter, we will discuss vSensor installation followed by necessary deployment checks and configuration.

Introduction to vSensors

In order to install Darktrace vSensors and osSensors, you will need to either mirror virtual traffic into a specified VM or to install osSensors onto VMs in a managed hosting service.

You will also need connectivity to the Darktrace master appliance and sufficient bandwidth to transfer 1-4% of original traffic volume mirrored to the virtual appliance.

STATISTIC/REQUIREMENT					
Estimated Devices	50	100	200	400	800
Traffic	100 Mbps	250 Mbps	500 Mbps	1000 Mbps	2000 Mbps
CPUs	2	4	8	16	32
RAM	8 GB	16 GB	32 GB	64 GB	128 GB
Hard Drive	50 GB	100 GB	200 GB	400 GB	800 GB

Note that the vSensor performance may vary by CPU speed and the nature of the traffic and the device limit is for estimation purposes only. It does not constitute a limit on the vSensor, only bandwidth and connections per minute are important. All connections per minute and device counts must fit within sizing recommendations for the master appliance.

Hardware Requirements

Operating System:

- Ubuntu 20.04 Focal

CPU:

- Minimum 2 CPU cores
- Best performance 3+

RAM:

- Minimum 1.5 GB
- 3.75-4 GB recommended

Deep Packet Inspection workers auto scale - each extra DPI worker requires 2 CPU cores and 500 mb RAM

Modes

vSensors can be connected to a Master appliance in three ways:

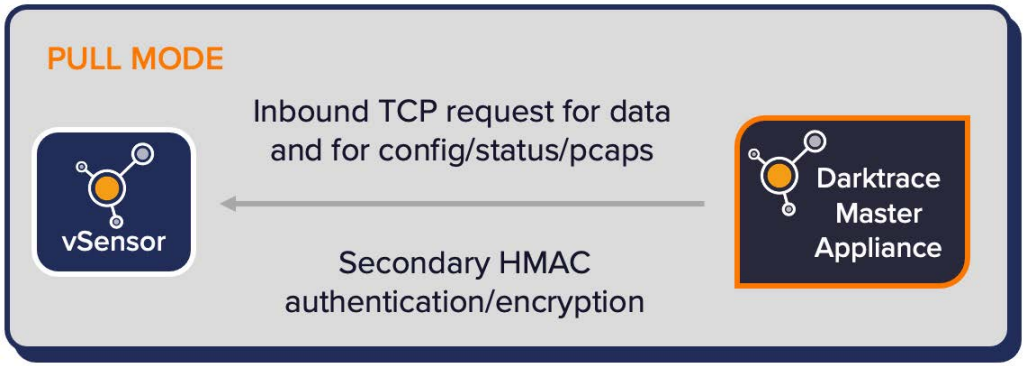
- **Pull Mode**
- **Push Token Mode**
- **Push Legacy Mode** (original Push mode, no longer recommended)

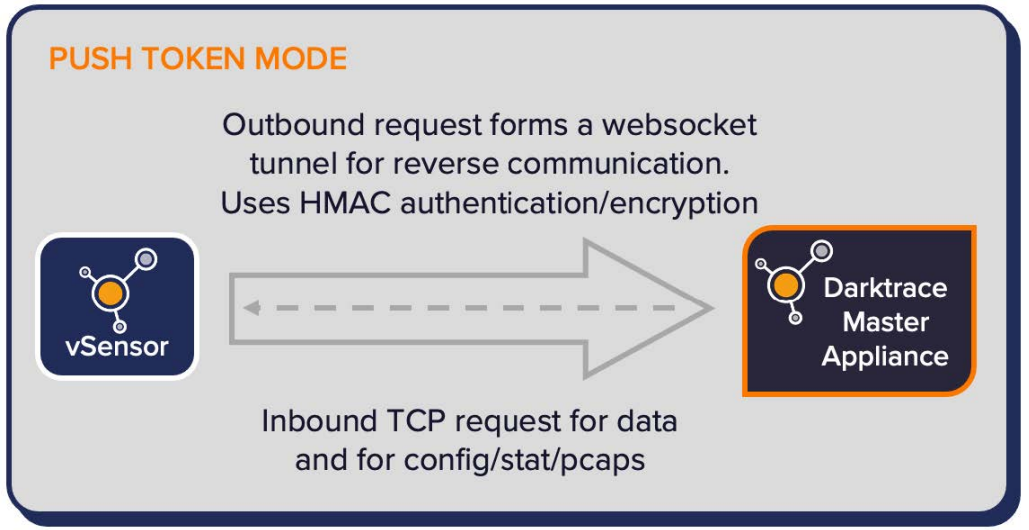
Each mode requires the use of port 443 (HTTPS) for inbound/outbound communication, depending on the mode.

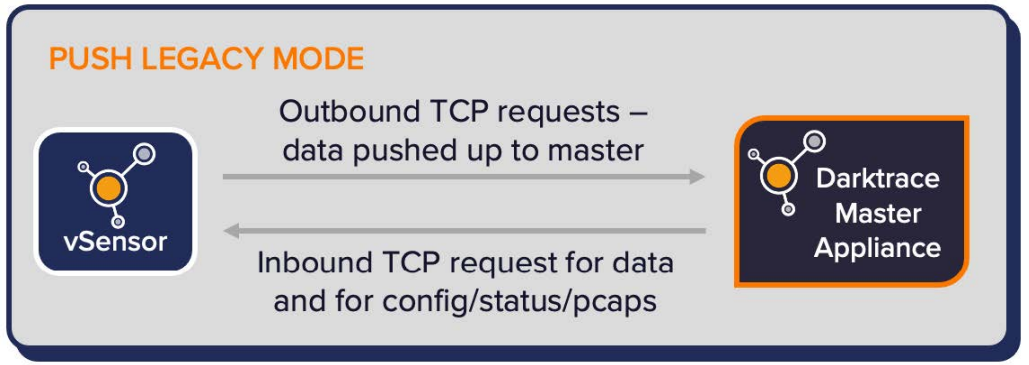
Pull mode and Push Token mode are both approved for cloud-hosted masters.

Push tokens allow the vSensor to communicate securely via a pre-shared token, making this mode suitable for use over untrusted networks such as the internet, and behind a NAT. The Push Token mode is a TCP connection initiated from the vSensor to the master. The Master needs to be reachable by the vSensor.

Unlike Legacy Push mode, the Push Token mode does not require bi-directional communications, so this is ideal when the vSensor is behind a NAT or firewall. For example, this includes most deployments which point to a cloud.darktrace.com hosted master. It uses additional encryption inside the SSL, so is safe to use on untrusted networks if using self-signed SSL certificates. It also supports HTTP proxies for outbound access.





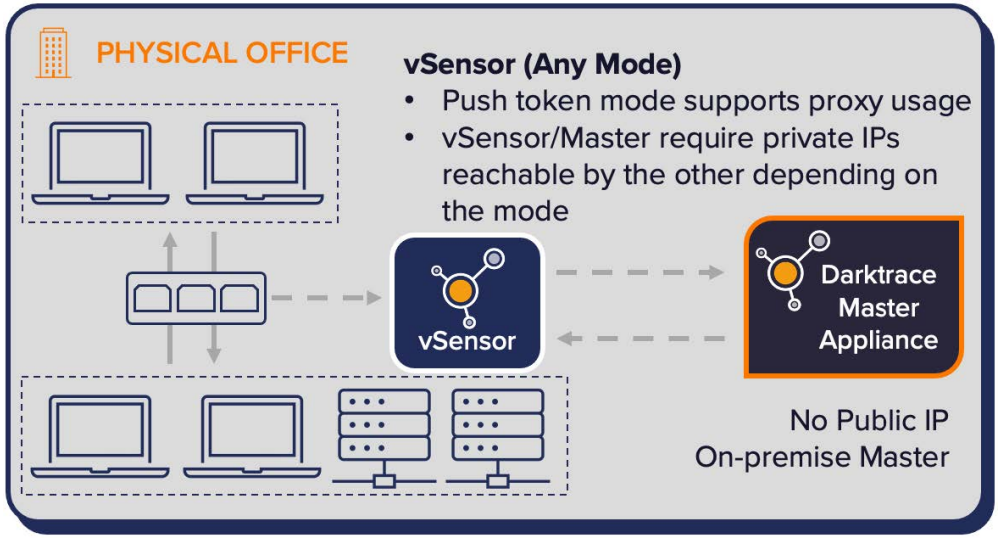


Deployment Examples

The following diagrams demonstrate examples of different methods in varying deployment types.

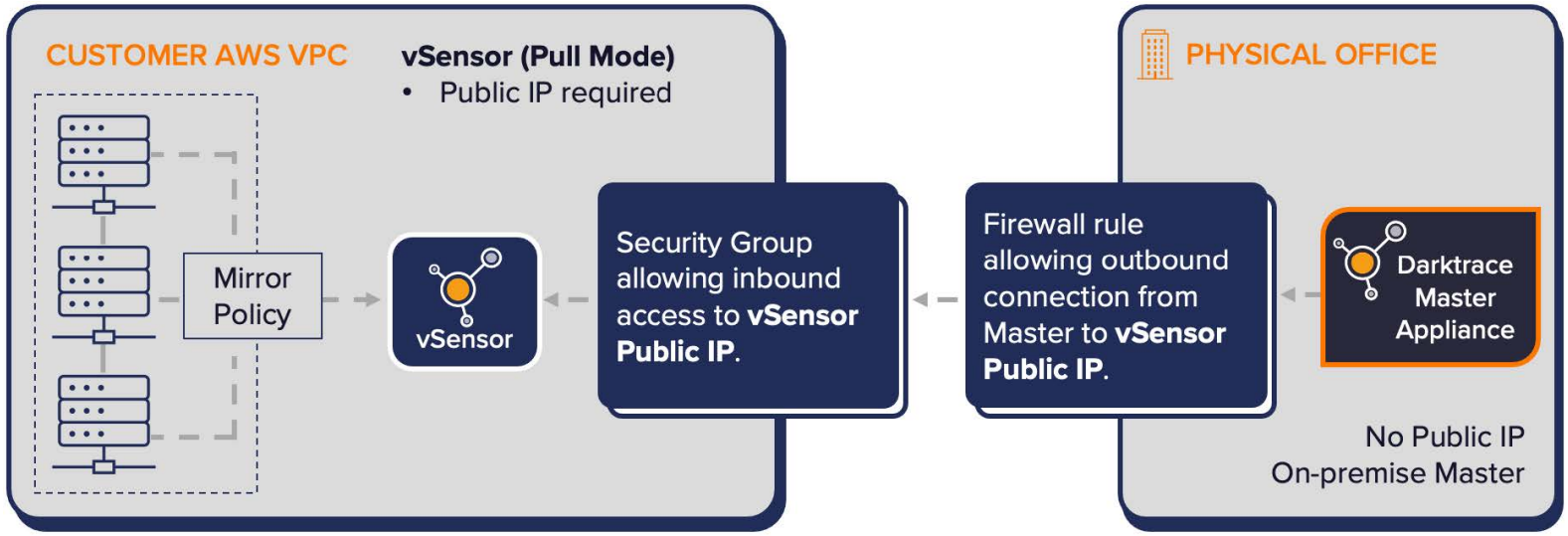
Any Mode with On-Premise Master

The first diagram shows how a vSensor can be deployed on-premise. The vSensor is mirroring traffic from virtual devices via a virtual switch and is communicating the traffic to the Master Appliance. This set-up can use any mode.



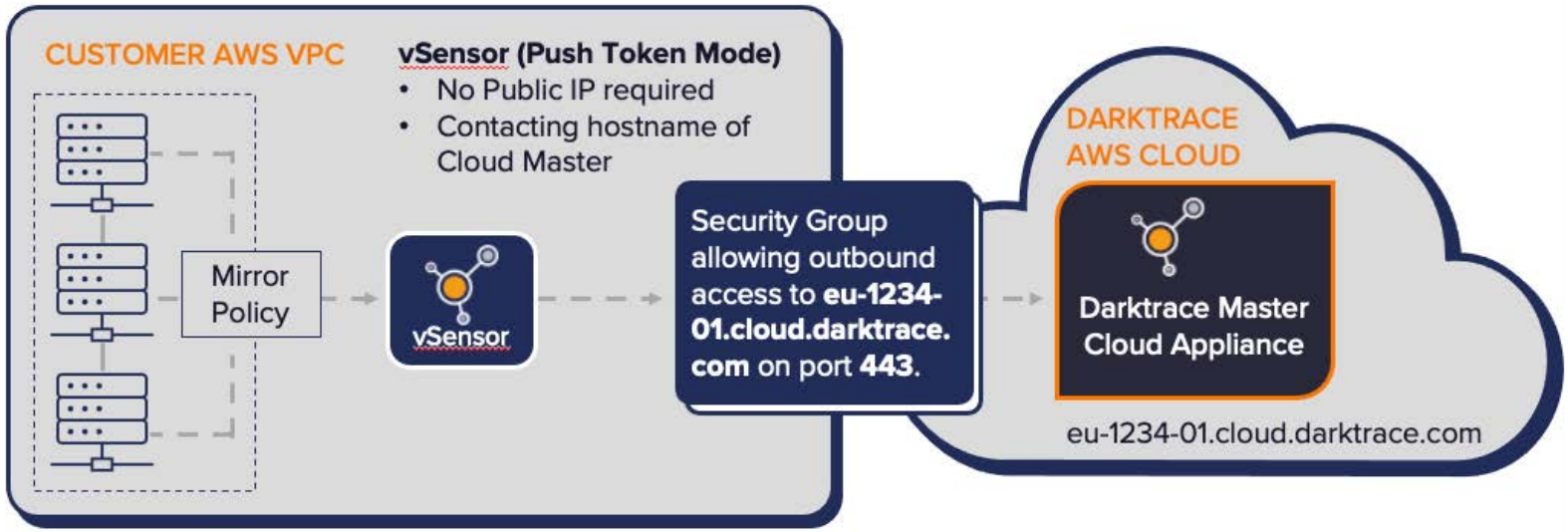
Pull Mode in the Cloud with On-Premise Master

This digram shows the vSensor in a customer AWS VPC mirroring traffic using the appropriate mirror policy. The Darktrace Master appliance communicates externally from the physical office as long as the firewall rule allows. The Security Group in the Cloud allows inbound access to the vSensor's public IP. The TCP connection is initiated by the Darktrace Master to request traffic from the Cloud environment.



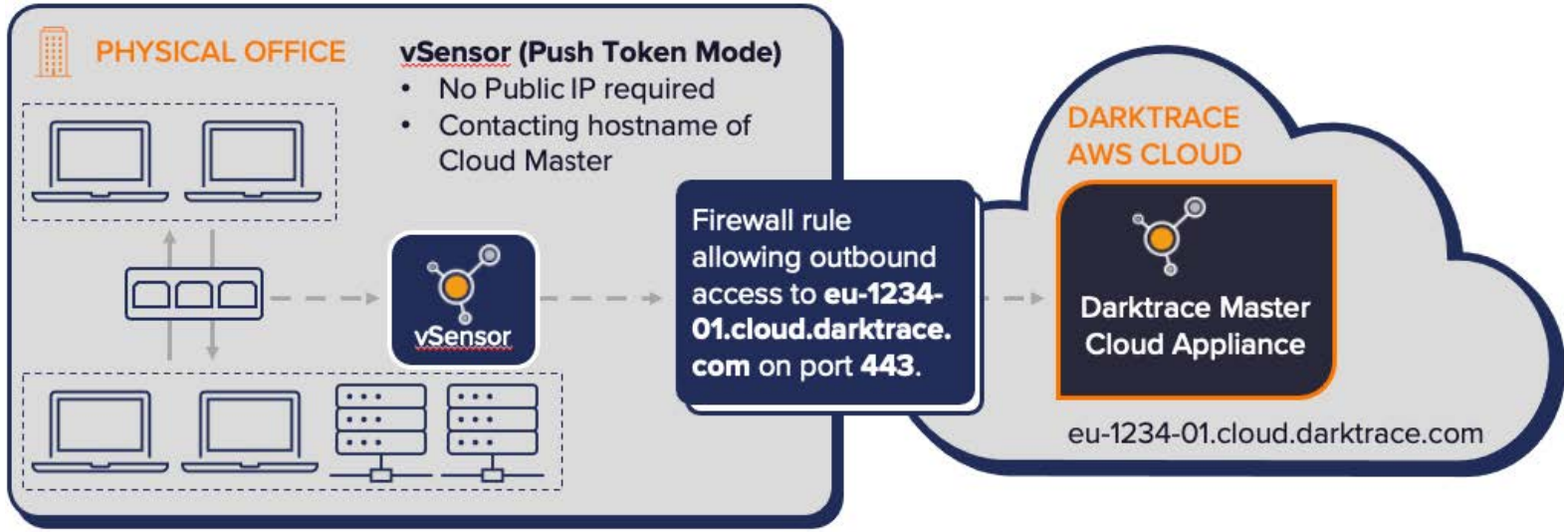
Push Token Mode in the Cloud with Darktrace Cloud Master

Similar to the previous method, the vSensor is mirroring traffic in a customer AWS VPC environment. A TCP connection is initiated by the vSensor to the Cloud Master Appliance, whose hostname is known. Data is transmitted securely using the pre-shared token.



Push Token Mode in a Physical Office with Darktrace Cloud Master

In this instance, the vSensor is situated in a physical office, mirroring virtual device traffic from a virtual switch. In the same way as described above, a TCP connection is initiated by the vSensor to the Cloud Master Appliance, whose hostname is known. A firewall rule from the physical office allows outbound data to be securely transmitted to the Cloud Master using the pre-shared token.



vSensor Installation

vSensor Installation - Standalone Image

1. **Expand the hard disk** to match your sizing (50 GB recommended). The VM will automatically grow its partitions to match.

   Note: The vSensor requires a minimum of 2 CPU cores and 3.75 GB of RAM.

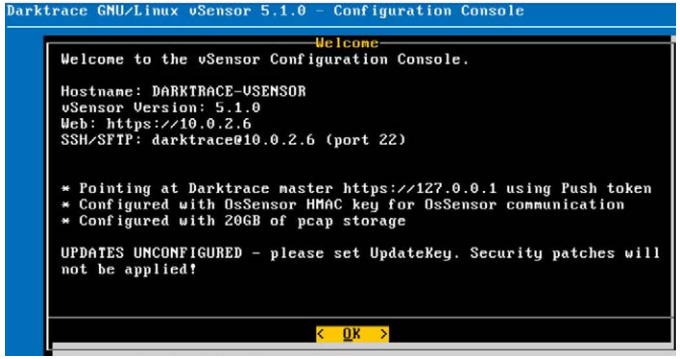
2. **Boot the vSensor**. On first boot, you will be prompted to set a keyboard layout. This is only applicable to the console configuration and will not be applied when using SSH to access the vSensor.

3. Create a new password for the **darktrace** user. This will be the default admin user and the password will be used when accessing the vSensor or performing console actions.

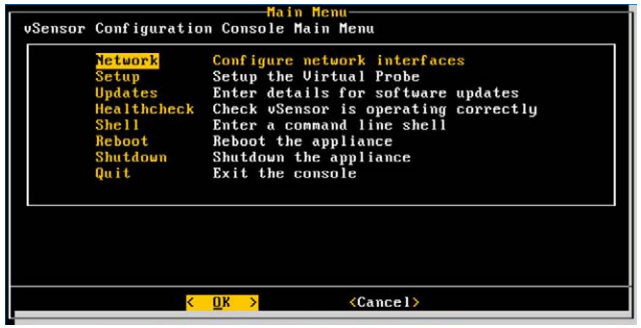
4. Let the vSensor initialize. A screen will display the vSensor's current status. Then proceed to the **main console menu**.

5. Launching the image reveals a welcome screen.

   Click **OK** to proceed.



6. In the vSensor main menu, there are options to configure the network NICs, set up the virtual probe, update the installed software, carry out health checks, enter command line shell commands, reboot, shut down and exit the console.

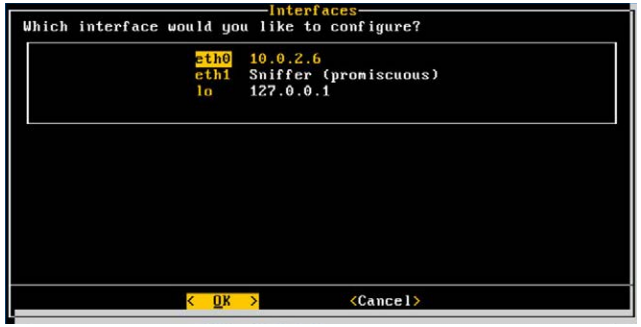


   Begin by selecting the **Network** option and click OK.

7. The Interfaces menu displays available Network Interfaces.

   Assign two network interfaces.

   If the option is given, select **initialize fresh MAC addresses**.



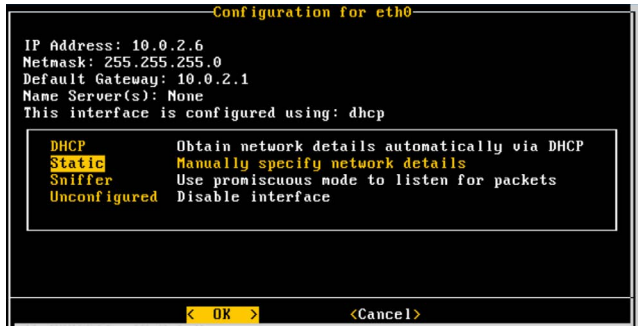
   Select an interface and click OK to configure it.

   a. The first network interface should be able to contact/be accessible by the Darktrace Master over port 443 (HTTPS), depending on the communication mode.

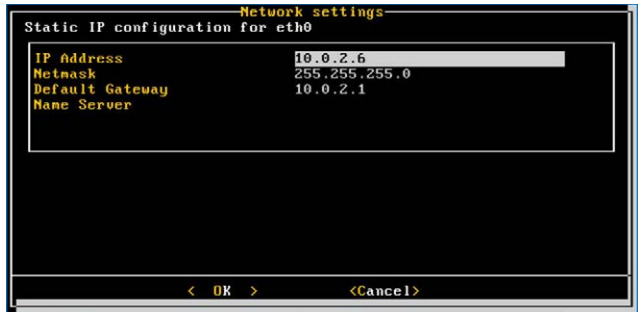
   b. The second network interface should be set to Sniffer mode to receive packets from the virtual switch mirror port, in promiscuous mode.

8. Select **Network** from the main menu and configure the interfaces. Navigating to an interface and pressing enter will provide options to change the interface type.

   a. Set up the main interface (eth0) with a static or DHCP IP.



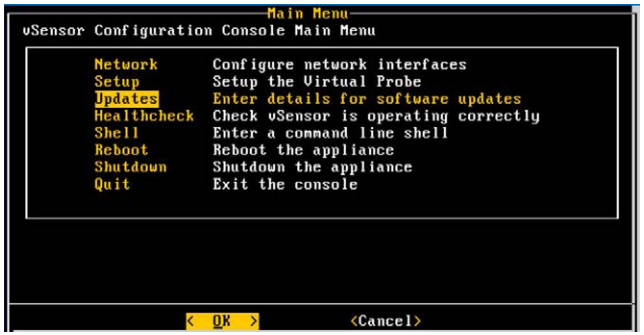
      i. In this example, select Static for eth0.



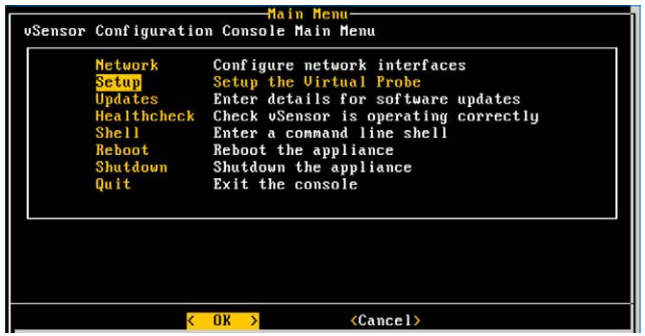
      ii. For the selected interface, configure the IP address, netmask, default gateway, etc.

   b. Set up the second interface (eth1) as a sniffer interface to receive packets.

9. Return to the main menu and select **Updates**. Enter your Update Key and configure optional elements such as a proxy for updates.



10. Finally, enter the **Setup** menu and configure space for PCAP buffer storage, if desired.



vSensor Installation - Cloud

vSensors can be installed in different environments. In this section a quick summary of how they can be installed in the Cloud is outlined. Note that they can also be installed via CLI. For more in depth configuration steps, read the Darktrace vSensor Configuration Guide.

1. Spin up an appropriate virtual machine instance in your Cloud environment. Have your **Update Key** at hand if not installing via CLI.

2. **SSH into the instance** and run the appropriate **install script**, as highlighted in the configuration guide.

3. **Reboot** the instance.

4. **SSH into the instance**, bring up the **configuration console** and enter the **Setup** submenu.

   a. If the vSensor is intended for use with osSensors, set the **osSensor HMAC**.

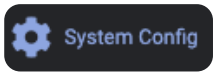
   b. Set **PCAP** buffer storage size if desired.

Communication Mode Configuration

There are three available modes for every interface: Push Token, Pull and Push (Legacy). This can be controlled in the vSensor Setup > Master menu. In the legacy Push mode, the vSensor requires an IP or resolvable hostname. Darktrace recommends employing the PushToken instead. In Pull mode, the appliance will pull data from the vSensor every ten seconds. Push Tokens and Pull mode are implemented slightly differently, as outlined below.

Push Token Mode

1. Log into the Darktrace Master instance UI and navigate to the **System Config** page from the Admin section of the main menu.

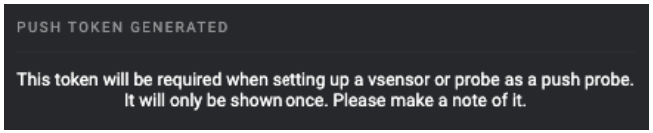


2. Within the Settings page, locate the **Push Probe Tokens** section.

3. Enter a label for the vSensor into the **Push Token Label** field and click **Add**.

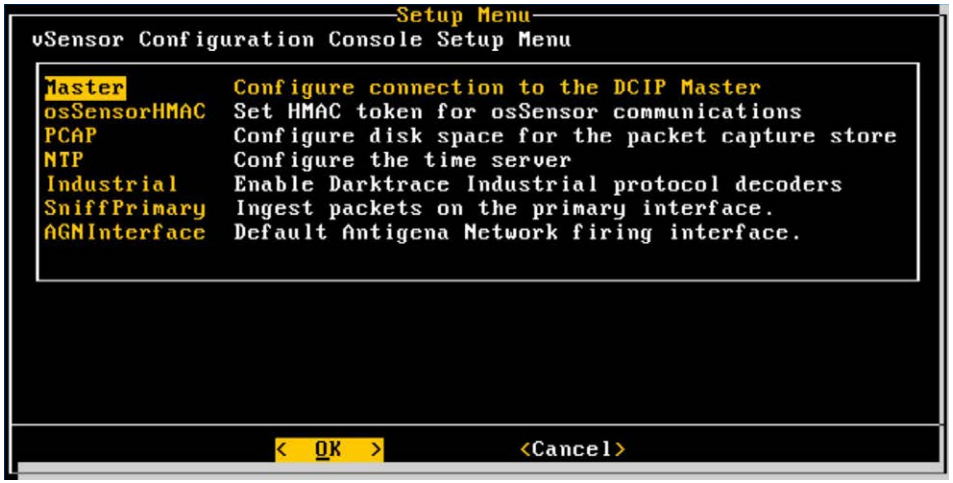
4. A unique token must be generated for each vSensor. It will be generated in the form of [**label:string**].

   This token **will only be shown once** and must be entered into the vSensor. Make sure to take note of this token.

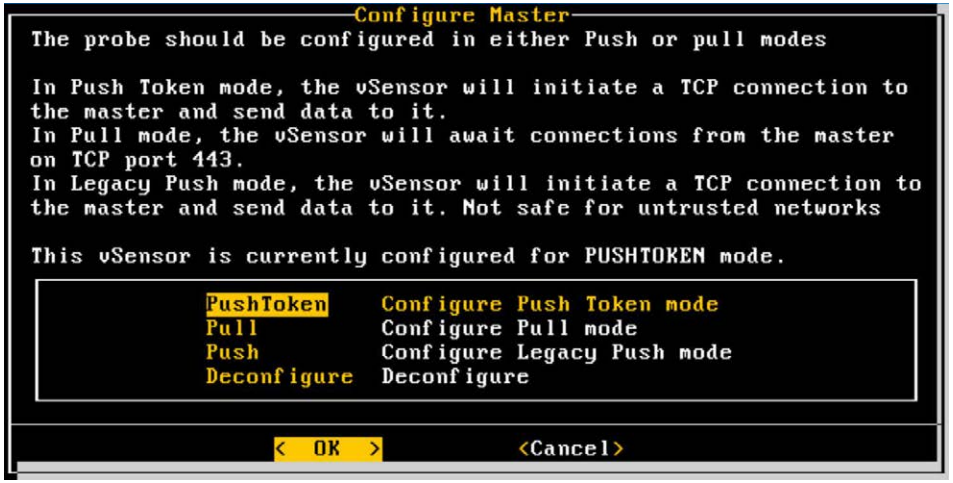


   Note: The label is part of the token. Therefore, if the label is changed, the token must be fully regenerated.

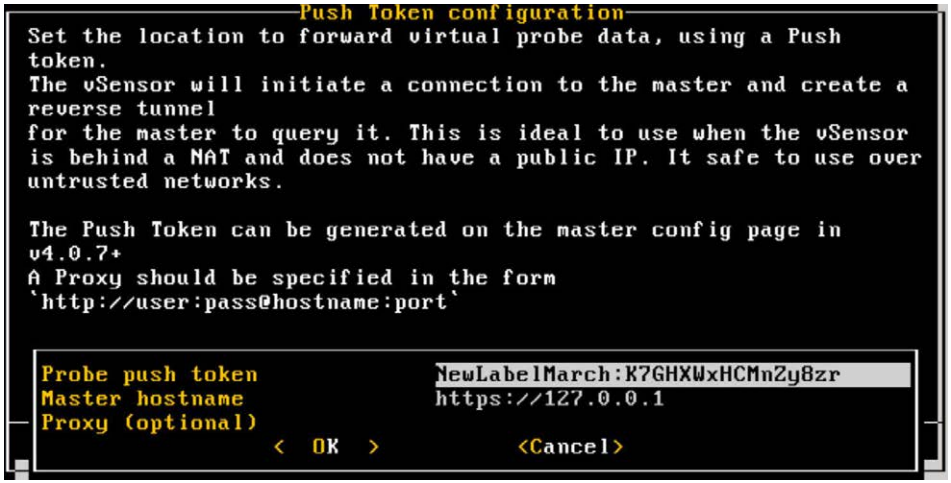
5. Return to the vSensor console and select the **Master** option from Setup sub menu.



6. Choose the **Push Token** mode from the available options.



7. Enter the **token** in full, and enter the **IP or hostname** of the Darktrace Master instance. For cloud-hosted master deployments, the hostname should be used.

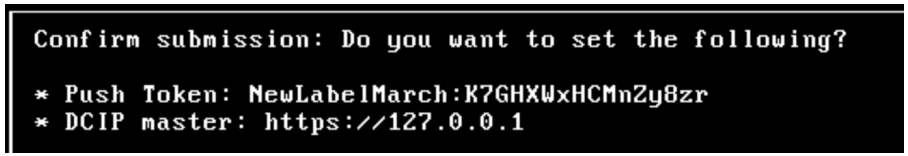


Note: Depending on your deployment environment, you may need to append Security Group or firewall rules.

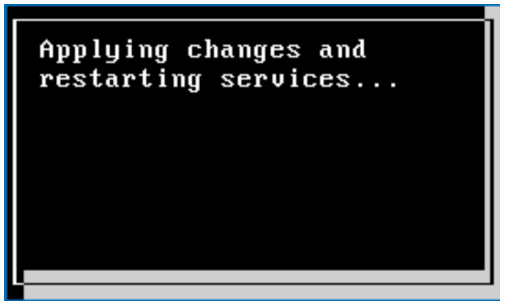
a. After inputting the requested information and selecting OK, you may be prompted to test the connection. Select **Yes** to test or No to ignore.

b. The interface will highlight if the connection was successful. Click **OK** to proceed.

c. Next, confirm these details are correct. If they are, select **Yes** to continue.



d. Finally, this will **apply changes** and **restart services**.



CLI

To instead set the communication mode via CLI, follow steps 1 - 4 of the guide above to generate a push token.

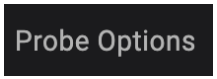
SSH into the vSensor and run:

/usr/sbin/set_pushtoken.sh [pushtoken] [master-hostname] [proxy]

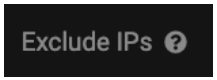
Where **[push-token]** is the token generated on the Darktrace Master instance, **[master-hostname]** is the hostname or IP of the Darktrace Master instance (hostname required for Cloud Masters) and **[proxy]** is an optional parameter available if a proxy is required for the vSensor to access the Master.

8. Returning to the System Config page in the Master Appliance UI, the new vSensor IP should be listed in the probe section. Verify the IP is correct and **confirm the new vSensor**.

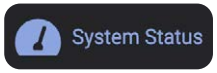
9. Expand the **Probe Options** below any existing vSensors in the Probes/vSensors section.



10. Under **Deployment Scope**, note **Exclude IPs**. This can be helpful to avoid sending unwanted traffic to the Master appliance.



11. Navigate back to the Threat Visualizer homepage, click the Menu button and select the Admin > **System Status** icon.



12. On the **Appliances** tab, **select the probe** directly from the Branch or List View.

13. Check the **CPU, load and bandwidth** are within expected tolerances.

Note: CPU and Load can be found under the Advanced section, but Bandwidth has its own section which can be reviewed.

14. Click back to the homepage and select a **subnet cube**. Confirm data is successfully being read from the vSensor. If not, check the Darktrace appliance can access the vSensor and that the vSensor is ingesting network traffic.

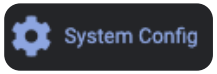
Pull Mode

1. In the vSensor console, select the **Master** option from **Setup** sub menu.

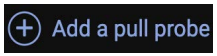
2. Configure the vSensor in **Pull mode**.

3. Set the **Master HMAC token** and click **OK**. The token string can be 5-63 alphanumeric characters, although 20+ is recommended. **Make a note of this key** as it must be entered into the Darktrace Master instance.

4. Log into the Darktrace Master instance UI and navigate to the **System Config** page.



5. Within Settings, scroll down to the **Probes/vSensors** section and click **Add a pull probe**.



6. Enter the vSensor **IP** and the **HMAC token** configured above. Optionally configure any proxy settings. Click the **Add** button. If successfully configured, the page will refresh and the probe will display as active.

CLI

To instead set the communication mode via CLI, SSH into the vSensor and run:

/usr/sbin/set_dcip_hmac.sh [pulltoken]

Where [**pull-token**] is the token to be used for Master-vSensor communications.

Follow steps 3 and 4 of the interactive guide to configure the Darktrace Master instance.

Push Mode (legacy)

Note: Pull mode is no longer recommended by Darktrace.

1. In the vSensor **Setup** sub menu, select the **Master** option.

2. Select **Push** to configure the vSensor in **legacy Push mode**.

3. Enter the **IP or hostname** of the Darktrace Master instance.

   If entering a hostname, ensure the name is resolvable via the DNS server provided to the vSensor.

4. Log into the Darktrace Master instance UI and navigate to the **System Config** page from the main menu.

5. The new vSensor IP should be **listed in the Probes/vSensor section**. Verify the IP is correct and confirm the new vSensor.

Deployment Checks

The following tests can be used to confirm that the vSensor is running and has connectivity with the associated osSensors (if applicable).

- **Check that the vSensor is running**

  To check that everything is running, log in as the Darktrace user (or other sudo user) and run vsensor-health-check.sh. For cloud installs, the sudo user will be the user you started with, usually 'ubuntu'.

- **Check incoming packets**

  Check the Status page of the associated Darktrace master (/sysstatus) or run **bmon** on the vSensor.

- **Check for vSensor overloading**

  Check the Status page of the associated Darktrace master (/sysstatus) for load disk or run **htop** on the vSensor

- **Test connectivity to the Darktrace Master**

  The connectivity to the Darktrace master can be checked by running **wget https://[instance]** and checking that wget connects. The expected output is an error saying that the certificate is invalid, it will contain **issued by /C=UK/L=Cambridge/O=Darktrace/**

- **If the configuration console doesn't appear**

  Run **sudo confconsole**. If it does not appear, reboot the instance. To do so safely, login and type **sudo reboot**.

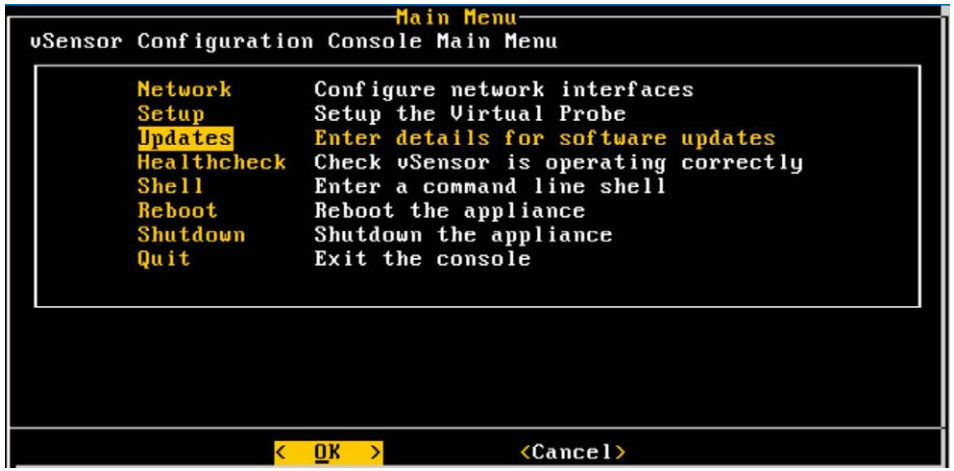
- **If the osSensors can't connect to the vSensor**

  Check port 80/TCP and 443/TCP is open between the osSensor and vSensor.

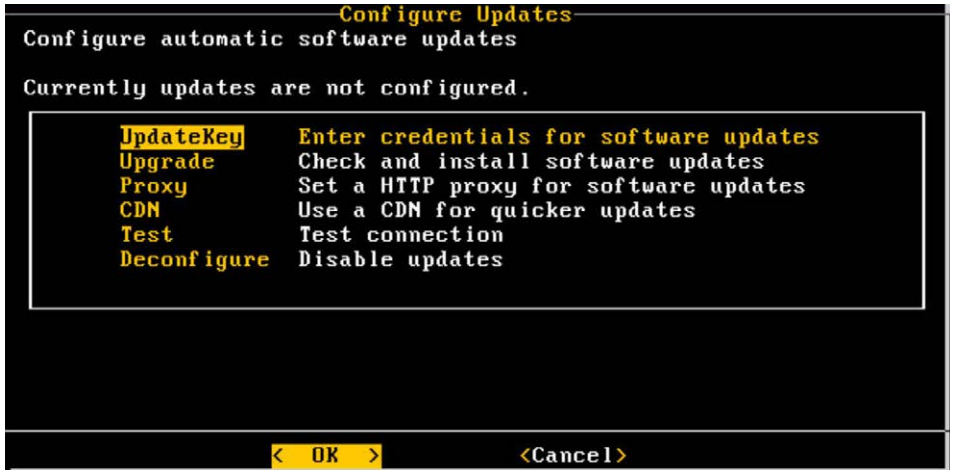
Upgrading a vSensor

Before enabling Packet Capture, it is recommended the vSensor is upgraded to the latest version.

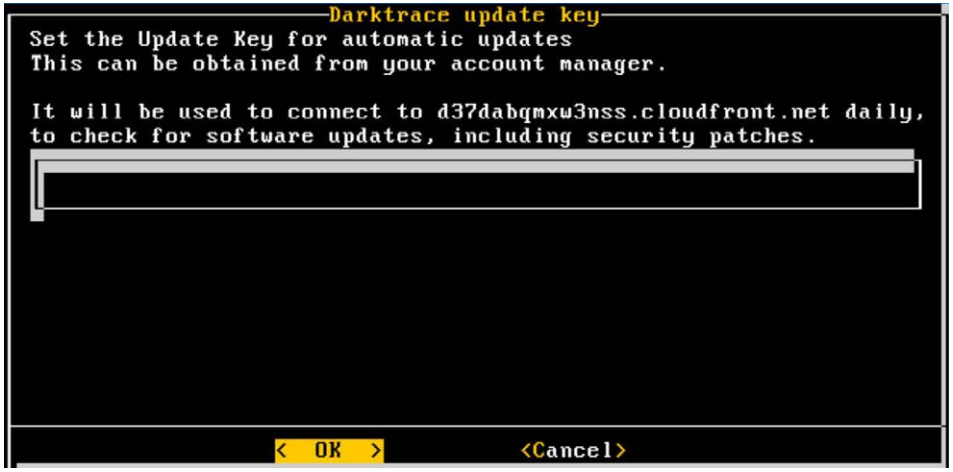
1. Launch the vSensor console, select the **Updates** option from the main menu and click **OK** to continue.



2. Prior to upgrading the vSensor software, a specific Update Key has to be requested from support. Select **UpdateKey** and click **OK**.

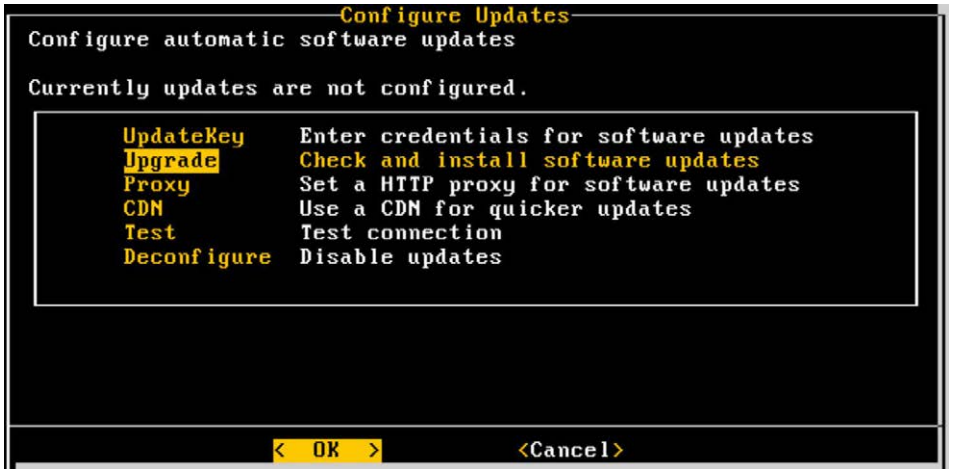


3. **Enter the key** in the field and click **OK**. Follow the instructions on screen.



The first time the installation will be carried out from here. For all other upgrades use the specific menu entry.

4. Now, select **Upgrade** and click **OK**.

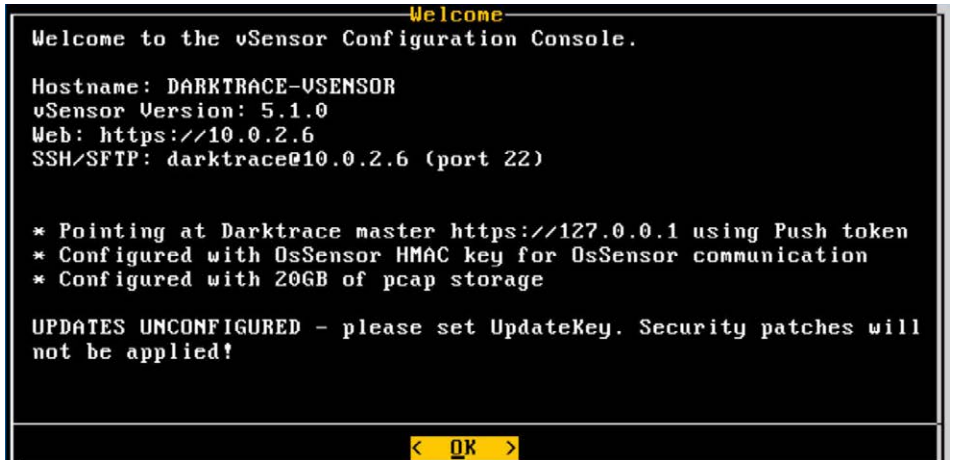


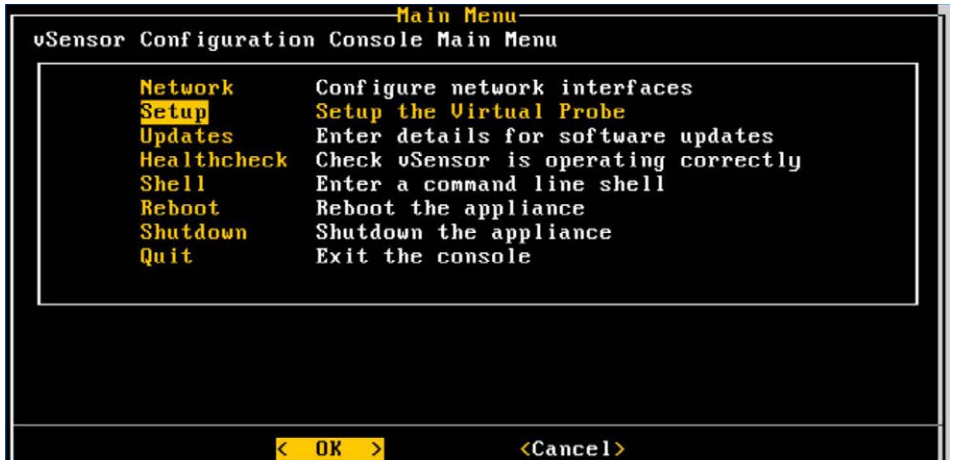
5. Wait a few moments for the package to be upgraded from **packages.darktrace.com**. Once the operation is completed **restart the "confconsole"** and click **OK**.

Enabling PCAP on a vSensor

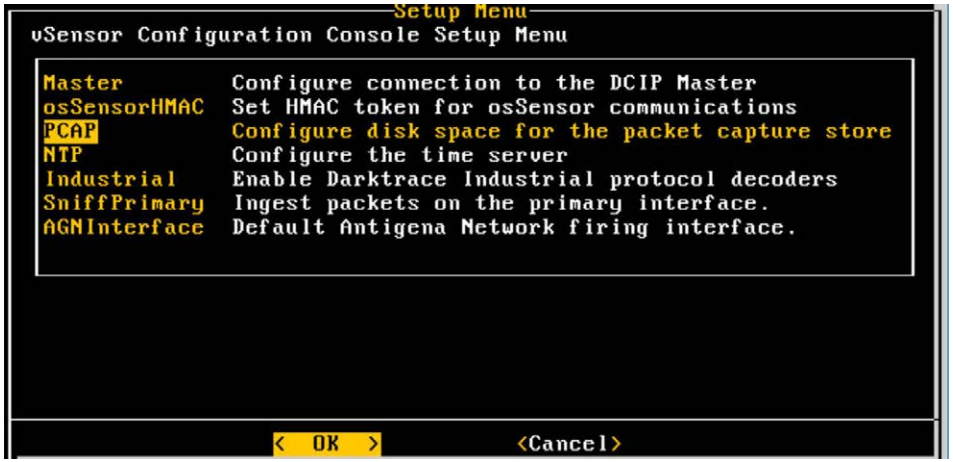
As with a Darktrace Master or Probe appliance, Packet Capture is supported on a vSensor. Packet Capture works by filling up an allotted amount of disk space. When full, it will overwrite the oldest PCAP on a rolling buffer basis.

1. When logging into a vSensor console, the **welcome screen** will confirm if Packet Capture has been enabled. Click **OK** to close the welcome screen.



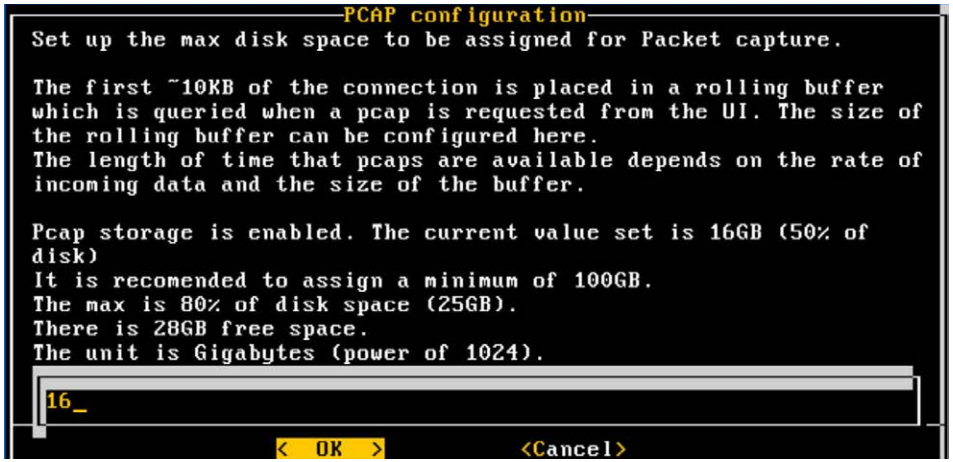


2. Select **Setup** from the main menu option and click **OK**.



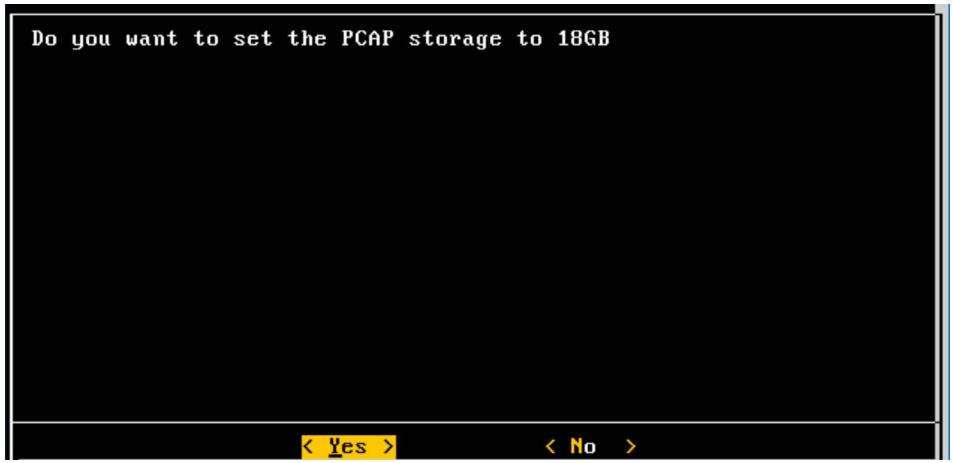
3. Choose **PCAP** and click the **OK** button.

4. The following message will **confirm if Packet Capture is already**

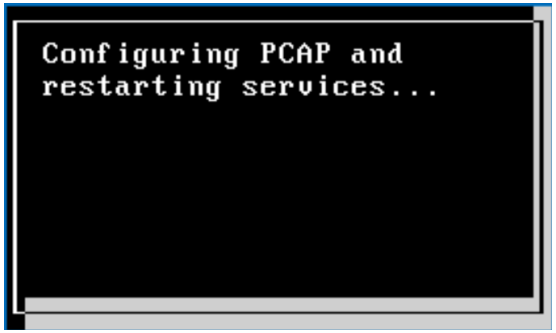


enabled and how much space. In this example, a value of 16 indicates 16 Gigabytes of space will be taken up by saved PCAPs. **Change the value** to your desired level and click **OK**.

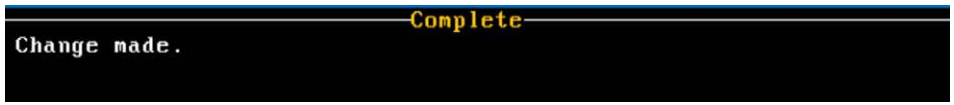
5. A confirmation message will request a confirmation of your option. Click Yes to proceed.



6. Wait a few moments to configure the PCAP storage and **restart the service**.



7. Once complete, a **Change made** message is displayed. Click **OK** to close and return to the console options.



8. osSensors

An OS Sensor ("osSensor") is a lightweight, host-based server agent that is easily installed onto virtual machines in the cloud. In this chapter, we will cover where osSensors are necessary and how to install and configure them.

Introduction to osSensors

When it is not possible to mirror a virtual switch, an osSensor must be installed on each VM. This will capture the VM's network traffic and forward it to a vSensor, which in turn is sent to the Darktrace Appliance.

The osSensor can be installed on Windows and Linux. The osSensor uses libcap / winpcap to read packets from the primary network interface of the machine it is installed on. These packets are then sent to the vSensor, where they are processed by the deep packet inspection engine. Each osSensor registers with a vSensor using a shared HMAC token which must be supplied to both ends.

The vSensor coordinates the osSensors associated with it, so that traffic is captured only once when osSensor devices communicate to each other. The osSensor is provided with a packet filter by the vSensor which instructs it to ignore the flows from other osSensors and data traffic to the vSensor. The osSensor uses outbound port 443 over TCP (HTTPS) for handshake and settings with the vSensor and port 80 over TCP to stream the network data.

osSensor Prerequisites

- A Darktrace Master Appliance running the most recent version of the Darktrace Threat Visualizer.
- The IP of a configured vSensor, intended for communication.
- The vSensor - osSensor HMAC token (also known as Authentication key).
  This is entered on the vSensor and in the osSensor configuration file.

Supported Operating Systems

- Ubuntu 16.04, 18.04 x86 64bit
- Debian Jessie (8), Stretch (9), Buster (10) 64bit
- Redhat Enterprise Linux 6, 7 (including derivatives, e.g. CentOS) 64bit
- Amazon Linux 1, 2 x86 64bit
- Windows 7, 8, 8.1, 10 64bit
- Windows Server 2012, 2016, 2019 64bit

Darktrace osSensors support any Linux distribution running the Docker Engine.

Installing an osSensor for Windows

1. **Log into the virtual server** intended for monitoring.

2. In the Darktrace Customer Portal, **download the osSensor** that corresponds to the virtual server's operating system.

3. The installer is a Microsoft installer file (.msi). Copy the msi file to the VM and **run the .msi installer**. WinPcap will also be installed if it is not installed already. The default install path is **C:\Program Files (x86)\Darktrace**.

4. The .msi installer will proceed through the configuration steps. Complete the following details:

   a. The **IP address** of the **vSensor server**.

   b. The **vSensor Authentication key**, which is the HMAC token created during the vSensor setup for vSensor-osSensor communication.

   c. The **IP address range/Device** used to identify which network device to collect packets from. A range is preferable in case the device IP changes with DHCP. The installer will identify which of the two options was provided and place the value in the **Device**= or **IP**= field of the config file accordingly.

5. A system service, *Darktrace osSensor*, will start on boot and restart if killed. This service runs **C:\Program Files (x86)\Darktrace\osSensor.exe**.

6. The default log path for the Windows osSensor is **C:\Program Files (x86)\Darktrace\osSensor.log** and the default config file location is **C:\Program Files (x86)\Darktrace\osSensor.cfg** if any changes need to be made.

On Windows 10 (and eventually Server 2016), the WinPcap engine can be upgraded to Win10Pcap for performance and stability improvements. It can be found at http://www.win10pcap.org/.

Installing an osSensor for Linux

The rpm and deb packages will install the osSensor, config files and log locations. The service will not start until enabled.

In our training example we have deployed the vSensor and osSensor in Oracle's VirtualBox. Therefore, we have two VMs running in VirtualBox. To run the osSensor, we deployed an Ubuntu 18.04 vdi image file in VirtualBox, then we downloaded and installed the osSensor version for Ubuntu from the Customer Portal. The vSensor OVA file for VirtualBox was downloaded from the Customer Portal.

Locations:

- **binary: /usr/bin/osSensor**
- **config file: /etc/darktrace/ossensor.cfg**
- **service: /etc/init/darktrace-ossensor.conf (Ubuntu upstart) or /usr/lib/systemd/system/darktrace-ossensor.service (RHEL SystemD) /etc/init.d/darktrace-ossensor (RHEL Upstart)**
- **logfile: /var/log/darktrace/ossensor.log**

1. In the Darktrace Customer Portal, download the osSensor that corresponds to the operating system.

2. Move the osSensor file to the virtual machine that you wish to monitor. For example, **scp [directory_from] [User]@[IP]:[directory_to]**.

   Note: If transferring the file in an AWS environment, you may need to specify the -i flag and a path to the relevant identity file.

3. Install the osSensor with **sudo dpkg -i darktrace-ossensor_4.0.0.<extension>** or **yum install darktrace-ossensor_4.0.0.<extension>** for centOS environments.

   a. If any issues arise with dependencies, install them with **sudo apt-get -f install**.

   b. If any additional required dependencies did not install automatically with the above command, use **sudo apt-get install [package_name]**.

   c. If you are still experiencing issues with any dependencies, update all packages with **sudo apt-get update**.

4. After install, the config file must be edited. The default log path for the osSensor is **/var/log/darktrace/ossensor.log** and the default config file location is **/etc/darktrace/ossensor.cfg**, or run **man ossensor.cfg** for help.

   Open the file in your preferred editor, for example **sudo nano /etc/darktrace/osSensor.cfg**.

5. The configuration file contains the following customizable key=value pairs. At a minimum, a **HMAC token**, **vSensor IP** and either **Device or IP** to monitor must be specified.

6. After the configuration file is edited, the service can be started. The service also needs to be enabled so it will **start on reboot**.

   - Ubuntu 14.04/16.04/18.04
     - It will try to auto start on reboot (change this behaviour in /etc/default/darktrace-ossensor)
     - Run: **sudo service darktrace-ossensor start**
   - RHEL 7, CentOS 7, Amazon Linux 2, Ubuntu and Debian:
     - To enable the service between reboots, run: **sudo systemctl enable darktrace-ossensor**
     - To start, run: **sudo systemctl start darktrace-ossensor**
   - RHEL 6, CentOS 6 and Amazon Linux 1:
     - To enable the service between reboots, run: **sudo chkconfig darktrace-ossensor on**
     - Then, to start the service, run: **sudo service darktrace-ossensor start**

osSensor Configuration Files

osSensors are controlled via a configuration file. It is available for both operating systems:

- Windows config file is at **C:\Program Files (x86)\Darktrace\osSensor.cfg**
- Linux config file is at **/etc/darktrace/ossensor.cfg**, or run "man ossensor.cfg" for help

An example of a Linux configuration file can be seen to the right.

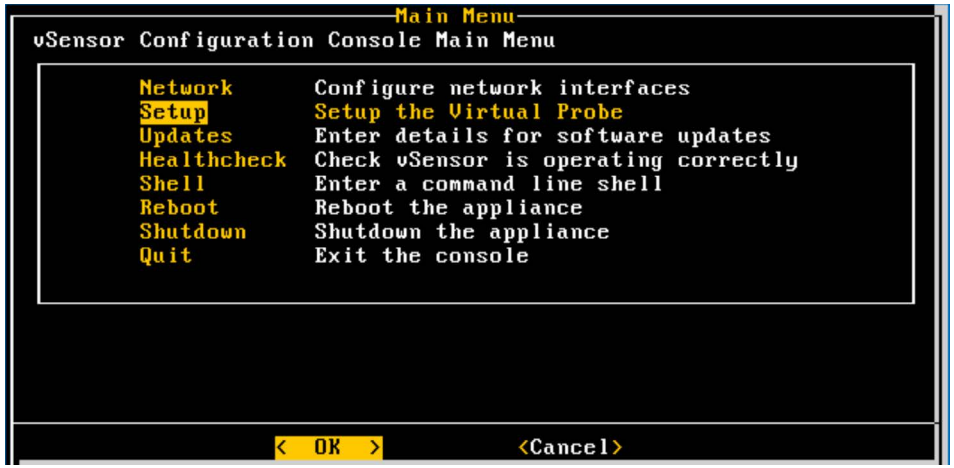
Note: Upgrading or reinstalling the osSensor will reset the config file to the default values. You may wish to take a note of the existing config settings before updating.

```
[osSensor]

# Set from level 0 (info level logging) to 5 (full packet data dumped)
Debug=0

# The host and port of the vSensor instance IP:PORT
vSensor= 10.110.10.1:443

# HMAC key for use with the vsensor
key=YcrattvqYts9Cq7fGoY2s8oNixgT8yyjhJsySE

# Device name from which to capture traffic
#device=

# to detect which device to capture from
ip=192.168.0.0/16

# Enable Antigena capabilities
useAntigena=true

# Enable websocket communication to VSensor
useWebsocket=true

# User to drop privileges to after startup
#user=nobody

# Where to log the output of the osSensor
logfile=/var/log/darktrace/ossensor.log

# A custom bpf filter to use (see man pcap-filter)
# eg Don't count incoming port 80/443 traffic to 172.31.29.42
# but do capture outbound 443/80
bpf=(not port 80 and not port 443) or net 10.0.2.0/24

# Post Antigena actions to vSensor with time delta (in seconds)
sendAntigenaActionDelta=5
```

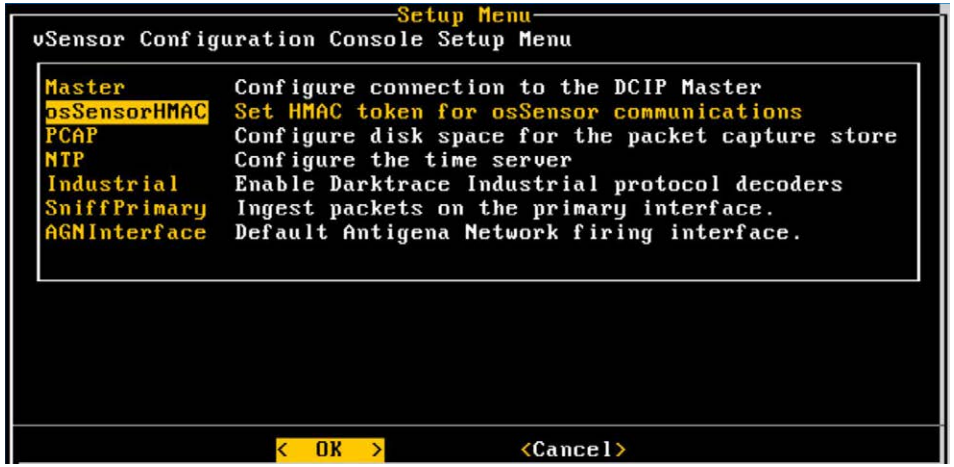
Configuring an HMAC token

The configuration file above requires an HMAC token which is set in the vSensor.

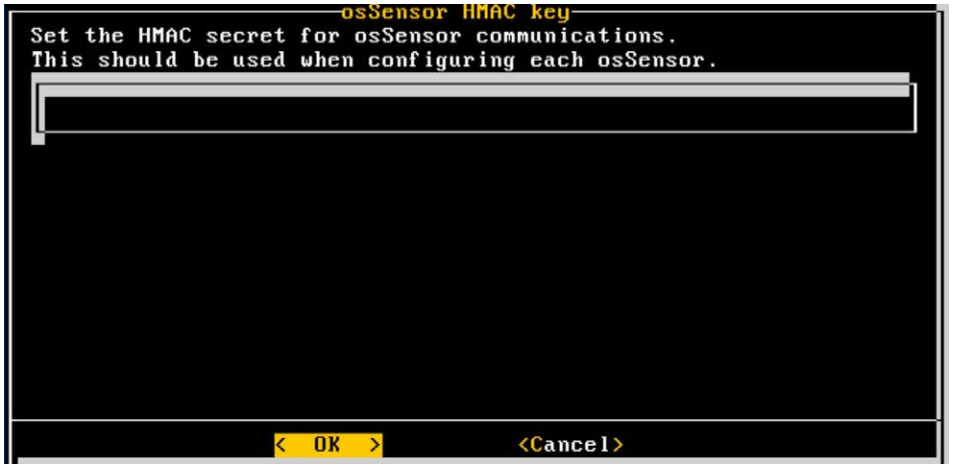
1. Within the vSensor console homepage, select **Setup**.



2. Click the **osSensorHMAC** option. Click **OK**.



3. Enter a suitably **secret key** (20+ alphanumeric characters) and **make a note of it**. Click **OK** to save your changes.



   a. A window will ask if you want to set the osSensor HMAC key to your input. Click **Yes** to set the HMAC key.

   b. Another window will appear to confirm the **change has been made**. Click **OK** to dismiss.

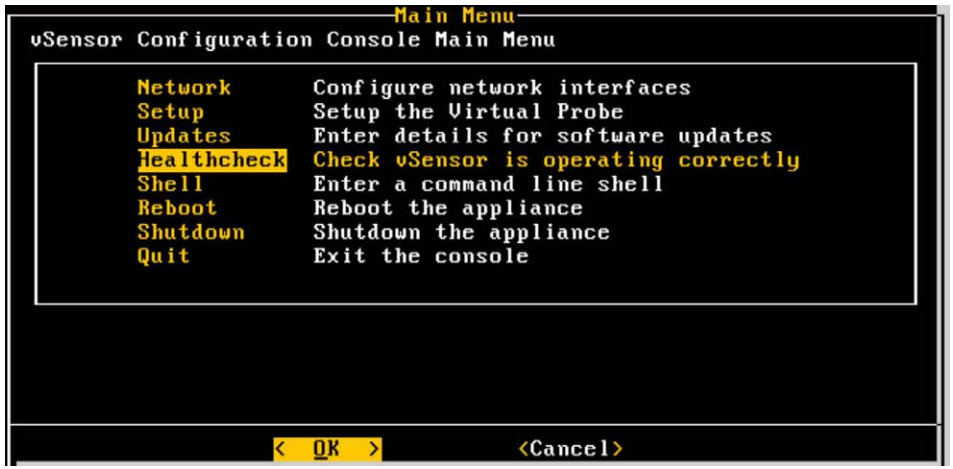
   c. This newly created key must be entered in the Key value of the osSensor configuration file.

4. Once the cfg file is configured, close the editor and start the following service in the terminal window:

   sudo service darktrace-ossensor start

   There are a few methods to check if the osSensor is correctly connected to the vSensor and is sending data.

5. On the vSensor, start the vSensor “confconsole”, from the Main Menu select **Healthcheck**.

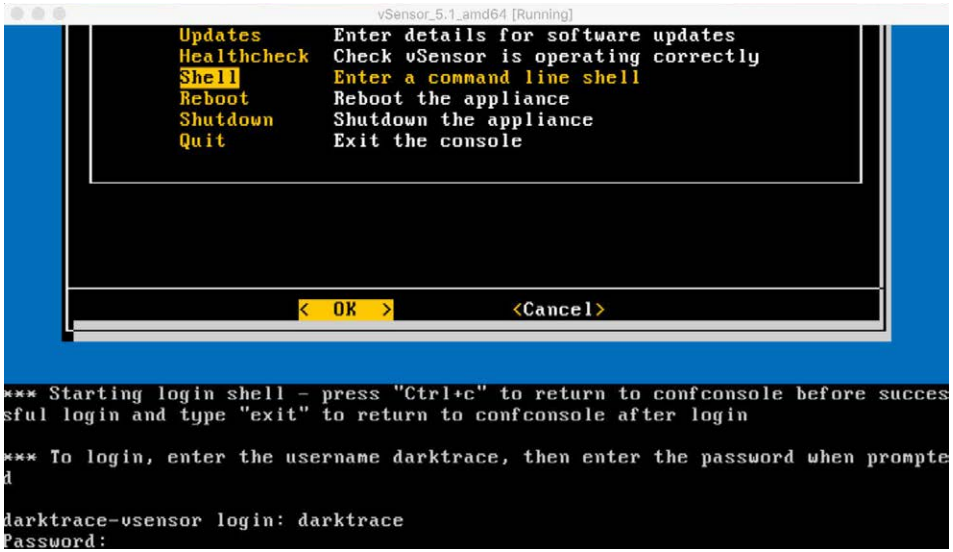


6. In case there is **no communication between the two components** you will get the following result:

Note: This deployment example doesn’t have a Master appliance configured and so the “master_connectivity” error is to be expected.

7. The issue can be due to an incorrectly configured cfg file or the VMs are not on the same network segment. A correct configuration of the VMs and the cfg file will produce an **osSensor count** for the **total** number and **active** number of osSensors.

8. Assuming the connection between the osSensor and vSensor is established, check if data is passing from one to the other by accessing the vSensor’s log file. Launch the “**confconsole**”, select **Shell** from the main menu and **log in**.



9. At this point you can reach the log directory using any command you prefer. Here we use “less”:

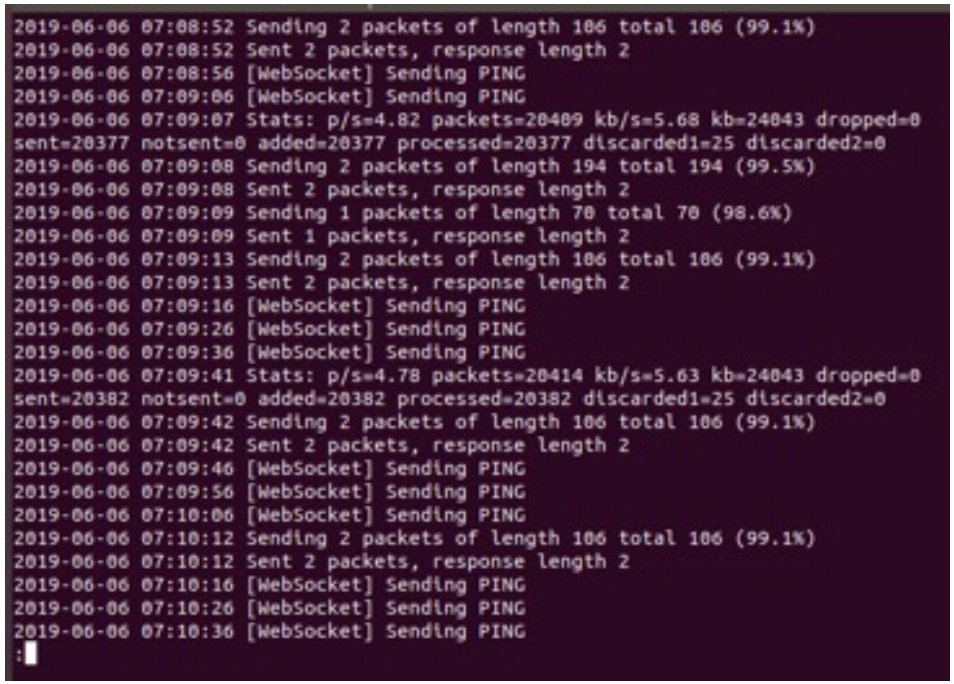
~$ less /var/log/sabreserver/lite/sabreserverlite.log

On the osSensor, the log file is located at:

/var/log/darktrace/osSensor.log

10. Open a **terminal window** and type:

    ~$ less /var/log/darktrace/osSensor.log.



From this we can see that the osSensor is sending data to the vSensor.

9. cSensors

The Client Sensor extends Darktrace's visibility via an endpoint agent software that monitors devices' network activity and delivers key data and metadata to the Enterprise Immune System. This can include remote working devices and those that cannot be seen adequately using bulk network traffic mirroring or existing Darktrace sensors.

Requirements

- An Enterprise Immune System deployments running Threat Visualizer v5.0 or above.
- The device monitored with the cSensor must be able to contact the cSensor infrastructure over HTTPS/443 for network traffic monitoring.
- For physical (hardware) Enterprise Immune System deployments, the master appliance must be able to contact the cSensor infrastructure over HTTPS/443.
- For virtualized Enterprise Immune System deployments, communication with the cSensor infrastructure is handled by Darktrace operations.

Darktrace cSensors can be deployed using the following mechanisms:

- Windows cSensors via CLI
- Windows cSensor via Installer (using a .msi file)
- MacOS cSensor via CLI
- MacOS cSensor via Installer (using a .dmg file)

Supported Operating Systems

- Windows 10, 8.1
- Windows Server 2019, 2016 and 2012R2
- MacOS 11.0, 10.15, 10.14

Host Utilization Requirements

- Bandwidth utilization is minimal, averaging <1kB/s
- Negligible CPU impact, <30MB RAM usage
- Installation Packages: MacOS <30MB, Windows <10MB
- Up to 30MB disk required

Each method requires the FQDN (**FQDN**) of the cSensor cloud infrastructure, a unique authentication token (**UNIQUE_KEY**) and the identifier of the unique authentication token (**KEY_ID**). For detailed configuration methods for each of the above, check the Deploying Darktrace Client Sensors guide on the Customer Portal.

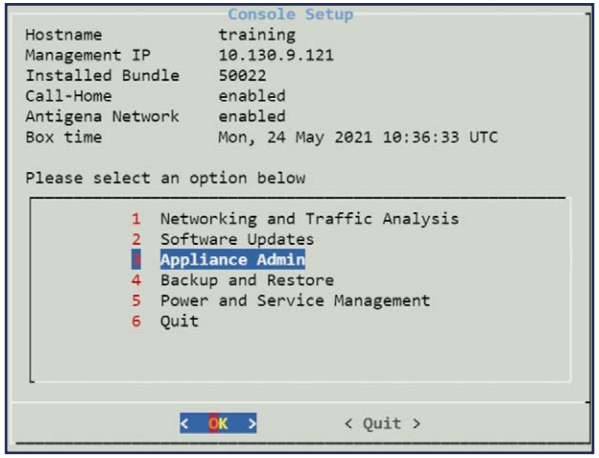
Once Client Sensors are installed, cSensor-monitored devices are modeled as distinct entities by a unique identifier. Traffic on multiple interfaces (such as concurrent Wi-Fi and Ethernet connections) is modeled together as part of the single entity. cSensor devices are aggregated into per-country groups, rather than subnets and displayed on the Threat Visualizer world map accordingly. Monitored devices will display a cSensor icon in the Omnisearch bar to indicate the data source and will show additional information on hover including the OS and installed agent version. Device tracking options are not available for these groups. If network traffic is seen for a monitored device via a different source - for example, a remote worker visits a satellite office and connects to the Wi-Fi - traffic will not be deduplicated.

For long-lived connections, the cSensor performs deep packet inspection analysis on the connection start. Advanced Search data for these connections will be incomplete for connection history and total data transfer over the connection lifetime. Records for short-lived or encrypted connections such as DNS and SSL will be complete.

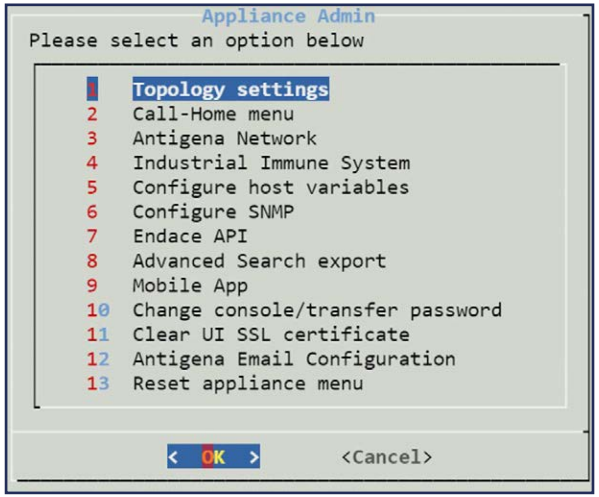
10. Converting to a Probe

After deciding where to place a physical probe within your logical network infrastructure, the Darktrace appliance intended for use as a probe must be converted from its default configuration as a Master. The procedures of the conversion are the following:

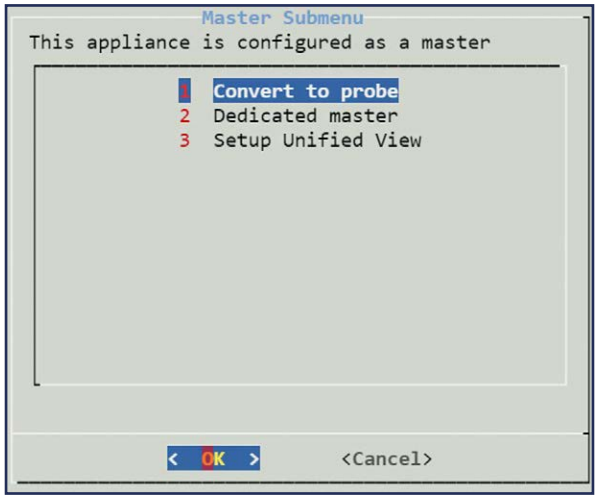
1. From the console main menu, select **3. Appliance Admin**.



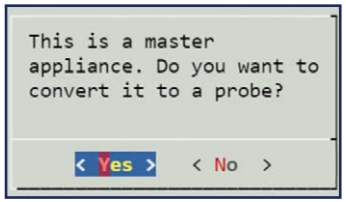
2. Next, select **1. Topology settings.**



3. From the Master Submenu page, select **1. Convert to probe**.

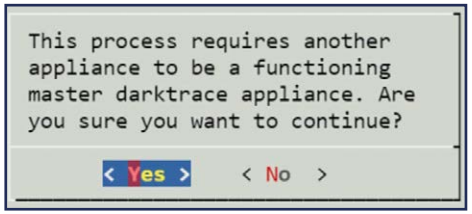


4. Click **Yes** to confirm you wish to convert it.

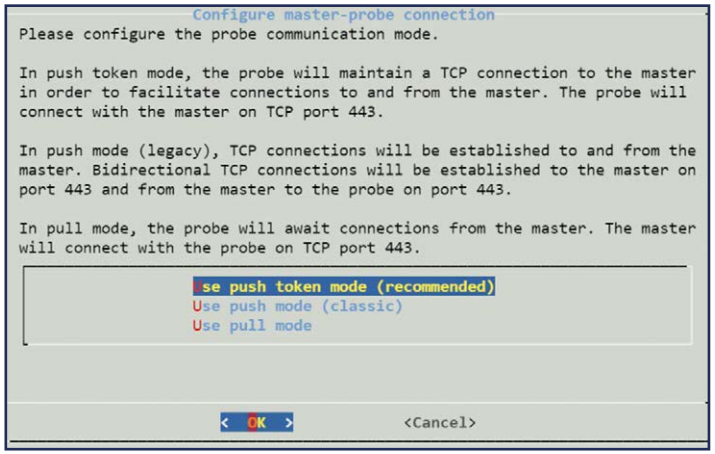


5. A message states a Master appliance is required to use a Probe.

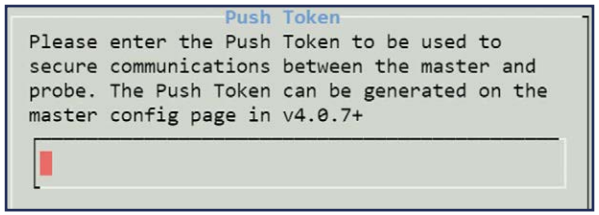
   Click **Yes** to confirm your selection.



6. Select one of the **communication modes**. By choosing push token or pull mode, an HMAC token must be entered for the communication between master and probe.

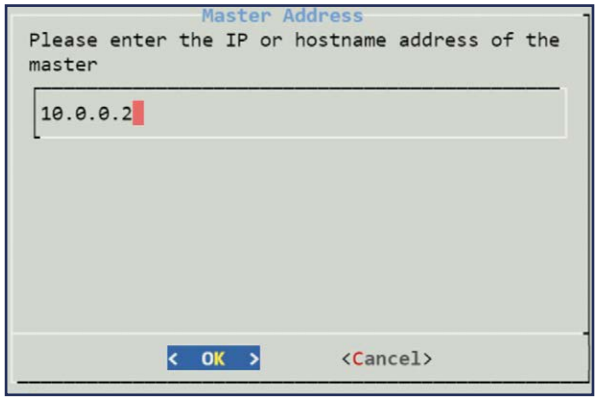


Note: There may be an extra step, depending on which communication mode is selected. For example, if proceeding with Push Token mode, you must input the token generated on the master config page.



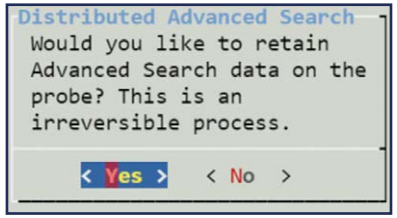
7. Enter the IP address or hostname of the master.

   Click **OK**.

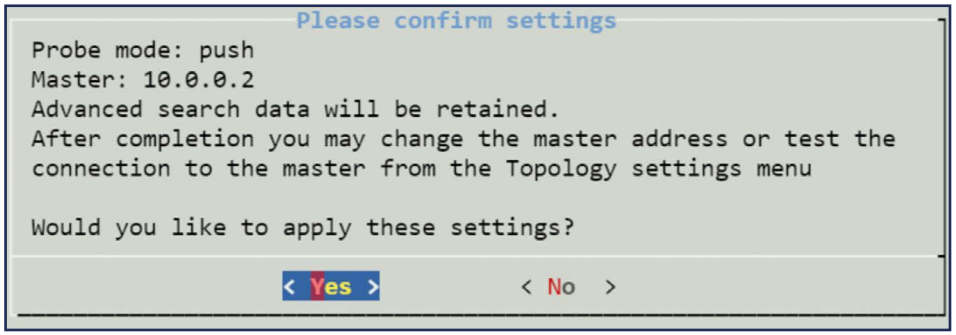


8. Choose whether the probe **retains Advanced Search data**.

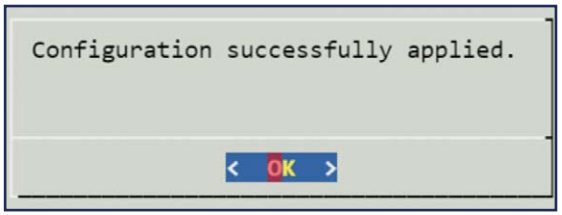
   By selecting No, Advanced Search data will be centrally stored the master.



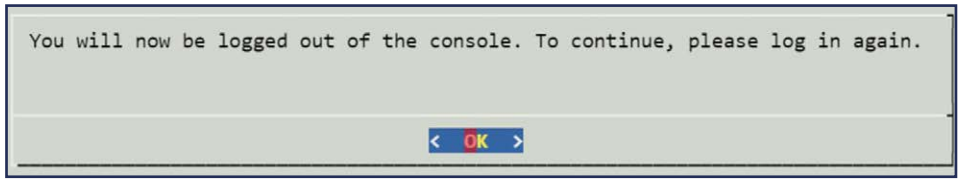
9. Review the settings and select **Yes** to proceed.



10. A dialog will confirm if the configuration has been sucessfully applied.



11. On the completion of these steps, you will be logged out of the console.



12. After the conversion, confirm the connection from the probe you have configured in the **System Config** page under the **Settings** > **Distributed Deployment Settings** > **Probes/vSensors** section in the Threat Visualizer. This action finally allows the probe to connect the master.

11. Terminal Services Agent (TSA)

The Darktrace Terminal Services Agent (TSA) is a lightweight installer which obtains enrichment data for any Windows Terminal Services environment. Windows Terminal Services environments allow centrally hosted Windows applications to be launched and accessed by remote users. For these environments it is not possible to resolve connections initiated from a centrally-hosted application to a specific end user or IP address from raw network traffic. When installed on the Windows Terminal Server host, the TSA enables Darktrace to identify the user accounts initiating connections.

How It Works

The TSA is a signed MSI intended for install on each instance of Windows Terminal Server hosting centralized applications. The agent listens for connections coming from the Windows Terminal Server and maps the source port of the connection to the user account that launched the application. The TSA resolves users for any terminal server environment, such as Citrix Virtual Apps and Microsoft RDSH. Each user is modelled separately from their network activity elsewhere on the network.

The connection information and mapping data, including username, source port and application used for each connection, is provided to the Darktrace Master appliance, which is able to associate these connections with a new 'device' based on each connection's source IP and source port. User connection information is then modeled in the Darktrace Threat Visualizer as individual devices identified as VDI: User.

The connection information is periodically sent via encrypted SSL connection port 443 to the Darktrace Master appliance. The bandwidth requirements are negligible as the TSA does not cause latency and is extremely lightweight.

Supported OS:

- Windows Server 2012
- Windows Server 2016

Supported Environments:

- Citrix Virtual App (formerly XenApp)
- Citrix Virtual Desktop (formerly XenDesktop)

Installing the Terminal Services Agent

Prerequisites

- Access to the Darktrace Customer Portal is required to download the most recent TSA installer.
- The TSA agent must be installed on each instance of Windows Terminal Server hosting centralized applications.
- The TSA location(s) must be able to contact the Darktrace Master appliance in order to send connection information.

Installation

1. **Download** the TSA installer from the Darktrace Customer Portal.

2. On a terminal server, run the **DarktraceTerminalServicesAgent.msi** installer as an **administrator**, and follow the installation instructions.

   Note: For command line installs, refer to the FAQs on the Customer Portal.

3. When prompted, run the installer as **everyone**.

4. On the Darktrace Configuration page, enter the **IP address** or of the **Darktrace Master appliance**. For Cloud Masters, enter the full **hostname** of the master (e.g., *euw1-1234-01.cloud.darktrace.com*).

5. Create a **shared token** for HMAC encryption. Make sure to securely record this HMAC token as it is needed for authentication steps later in the installation process.

   Note: One HMAC token is used to pair all installations of a TSA with a single Master appliance. For multiple Master deployments, see the FAQs on the Customer Portal.

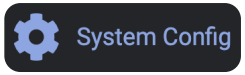
6. The option to customize the location of TSA logs and add an optional proxy to contact the Darktrace master is provided.

7. For **logs**, leave the field blank for the default location, **C:\ProgramData\Darktrace\TerminalServicesAgent**.

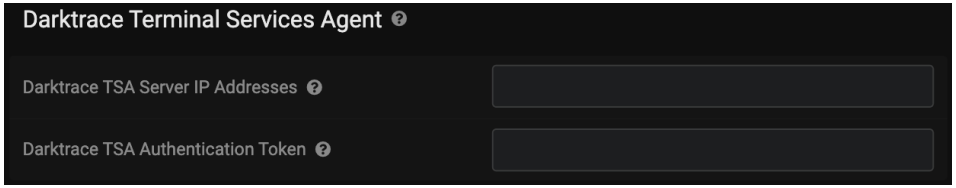
8. For **proxy server**, enter in the format **http://example.proxy:3000** or leave the field blank if not required.

9. On the final Confirm Installation page, click **Next** to install.

10. Access the Threat Visualizer of the Darktrace Master appliance and open the **System Config** page.



11. Select Settings from the left-hand menu and locate the **Darktrace Terminal Services Agent** section.



   a. In the **Darktrace TSA Server IP Addresses** field, enter the IP address(es) or the IP range (in DHCP environments) of the Windows Terminal Servers.

   b. In the **Darktrace TSA Authentication Token** field, enter the HMAC token created earlier and save changes.

Deployment Check

1. To verify the TSA is registered with the Master Appliance, navigate to the /status page and confirm that a new subsection, **TSA**, has appeared with the Windows Server IPs listed.

2. To confirm that the TSA is creating devices, navigate to the Threat Visualizer User Interface and search for **VDI:** in the Omnisearch bar. A list of devices should appear.

3. To confirm that the log files are being populated, check that the log file contains user and port information. By default, this will be located at **C:\ProgramData\Darktrace\TerminalServicesAgent\Log.txt** unless a specific log file location was provided during setup.

If settings such as the Darktrace Master IP need to be altered, edit the config file. The default location is at **C:\ ProgramData\Darktrace\TerminalServicesAgent\ TerminalServiceAgent.config**. The service must be restarted for changes to take effect. For more information, check the Customer Portal TSA FAQs.

12. Darktrace MSSP SOC Integration

MSSP Partner Program

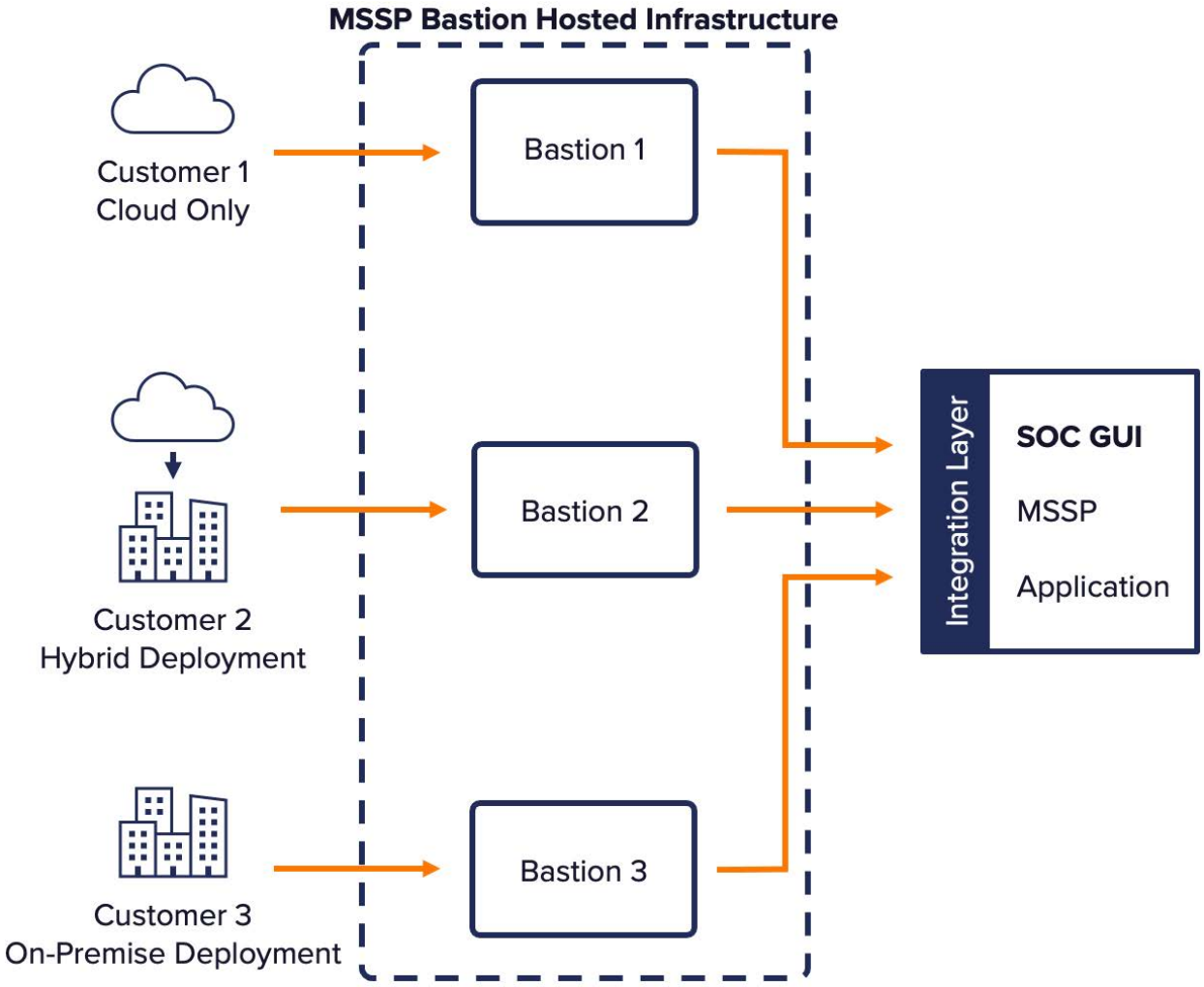
Darktrace's Managed Security Service Provider (MSSP) Partner Program allows organizations seeking to bolster the cyber defense services they offer with Darktrace's Enterprise Immune System.

MSSP partners may choose to manage customer support services on Darktrace's behalf in their own data center, in the end user's data center, or in a third-party cloud environment. After licensing Darktrace's solution, MSSP partners have the opportunity to bundle it with other services at whatever rate they deem appropriate.

Once installed in a customer's environment, Darktrace's self-learning technology works to understand the 'pattern of life' of the environment it is in. As such, data from each customer environment needs to be kept isolated from others, so it is not possible to multi-tenant a single master appliance across multiple customers.

In order to scale service offerings across multiple customers, MSSPs can leverage Darktrace's API to access all the data available within the Darktrace platform and present it through a single custom-built interface.

This allows for rapid customized exporting, integration and orchestration of the Darktrace data directly within you Security Operations Center (SOC).



Dual or Single Call-Home

The Call-Home connection remains within the customer's complete control at all times: it is initiated by your appliance, and you can start, terminate or audit it at any time. Call-Home is fundamental to enable the software communication across the platforms into the SOC. Please note that this communication will not work across dedicated or vendor specific VPN links.

Dual Call Home

A dual Call-Home configuration is the recommended set up as this will abstract the MSSP from the regular service and maintenance that is provided by Darktrace to all Darktrace customers (such as for model updates), while allowing the MSSP to focus on the security monitoring and operations.

Single Call Home

If the customer only allows a single external connection to the MSSP, the MSSP will need to provide for all of services usually managed directly by Darktrace including:

- Health checks
- Software management and updates
- Configurations

Integration with partner SOC environment

SOC integration goals will typically require working with Darktrace Alerts outside of the Threat Visualizer, such as:

- Allowing SOC analysts to triage alerts within a 'one pane of glass' environment without having to support separate access to individual alerting tools
- Combining Darktrace alerts with the output of other tools for the implementation of multi-vendor use cases
- Correlating Darktrace alerts with additional log sources for detection and efficacy gains
- Tracking and recording metrics around alerts and investigations
- Providing context around Darktrace alerts from other data sources, e.g. inventory databases

Two methods of achieving these goals are to implement an API query solution for integrating Darktrace's alerting functionality to output a feed to one or more central logging servers in use within the environment.

Note: For a more detailed insight and suggested workflows, review the Darktrace "Bringing Darktrace into your Managed SOC Services.pdf" document.

13. Learning Objectives

Course Agenda Checklist

Thank you for completing the Cyber Engineer course.

We hope this have given you the confidence to tackle a variety of aspects when deploying the Darktrace Cyber AI Platform.

Contact Us

For all further education inquiries, contact:

EMEA: training-emea@darktrace.com
APAC: training-apac@darktrace.com
US/LATAM: training-amer@darktrace.com

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

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

Using the tick boxes below, complete the learning outcomes checklist:

- [ ] I understand how components are employed for varying deployment scenarios
- [ ] I have knowledge of how to size a Darktrace installation
- [ ] I am able to navigate the Darktrace Console
- [ ] I can connect and configure the appliance to ingest traffic
- [ ] I can review the System Status in the Threat Visualizer and Advanced Search
- [ ] I am able to describe how to configure vSensors, osSensors and cSensors
- [ ] I understand how to install Darktrace Terminal Service Agents (TSAs)
- [ ] I can deploy Darktrace as a Managed Security Service Provider