THREATMATE™

INQUISITIVE SECURITY

ThreatMate Platform Guide

Installation and configuration time: 30 minutes

The ThreatMate platform consists of multiple components that work together to discover and continuously monitor assets. The components include:

- **ThreatMate Discovery Agent**. It monitors a subnet by continuously discovering live hosts and running vulnerability analysis on them. It can also perform internal penetration tests. It can be horizontally scaled by adding additional instances of discovery to monitor different networks or a subset of hosts on the same network. A single sensor can monitor any number of hosts based on the hardware resources available. The agent needs to be installed on a persistent machine on the network.
    - **Hardware Requirements**
        - Vulnerability discovery
            - 4 GB of free RAM and 1 CPU core for each batch of 1000 live machines regardless of how large the network is. For example if your network is /16 but only has 100 live machines you can still fit in the original requirements.
            - Bandwidth
                - download: 4MB per live host per hour
                - upload: 10MB per live host per hour
        - Penetration test
            - 8 GB of free RAM at a minimum and 4 CPUs but prefer 16GB of RAM
    - **Supported OS:** Windows/Linux/Mac/Docker/Virtual Machines
- **ThreatMate Endpoint Agent**. It continuously collects endpoint data for:
    - Asset management - the collected data includes all hardware and software on the endpoint device
    - Vulnerability analysis for third party software - find vulnerabilities in third party applications such as Mozilla Firefox or Adobe Acrobat (Authenticated Vulnerability Scan)
    - Vulnerability analysis for the operating system - find missing patches and vulnerabilities in the operating system (Authenticated Vulnerability Scan)
    - Compliance checks - find compliance violations on endpoints. This can be used to enforce best practices or a compliance regime such as CIS or HIPAA.
    - Threat hunting and suspicious behavior - allow advanced research to uncover active attackers on endpoint devices.

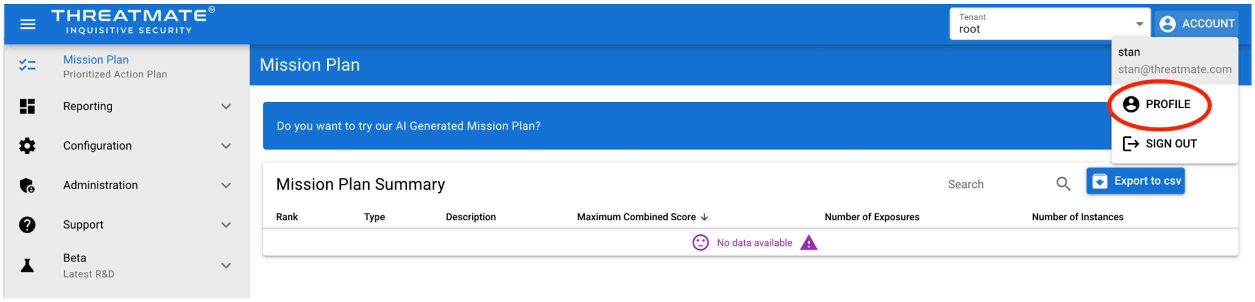
    - **Hardware Requirements:** 50MB of free RAM and 1 CPU core
    - **Supported OS:** Windows/Linux/Mac/Docker/Virtual Machines
- **API Integrations.** ThreatMate integrates with cloud services and third parties. The integrations are used to perform additional security analysis.
    - Google Workspace - cloud service provider
    - Microsoft 365 - cloud service provider
    - ConnectWise - MSP management platform
    - Vanta - continuous compliance
    - PurpleKnight - active directory assessment

After the deployment of the ThreatMate Discovery Agent the initial report takes about 6 hours to complete. The ThreatMate Agent results are available within 5 to 10 minutes.

All data transferred between the discovery agent, the endpoint agent and the cloud instance is encrypted and authenticated using HTTPS.

Managing Your Profile

You can change your password and enable MFA from your profile page:



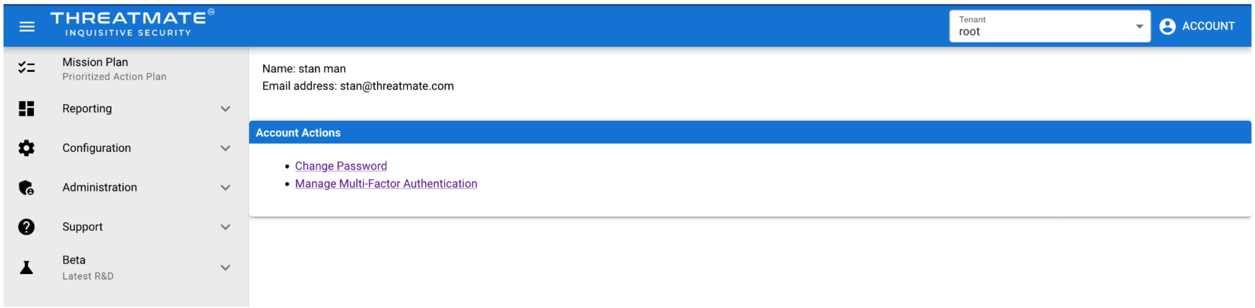
Mission Plan

Do you want to try our AI Generated Mission Plan?

Mission Plan Summary

Rank	Type	Description	Maximum Combined Score ↓	Number of Exposures	Number of Instances

No data available



Name: stan man
Email address: stan@threatmate.com

Account Actions

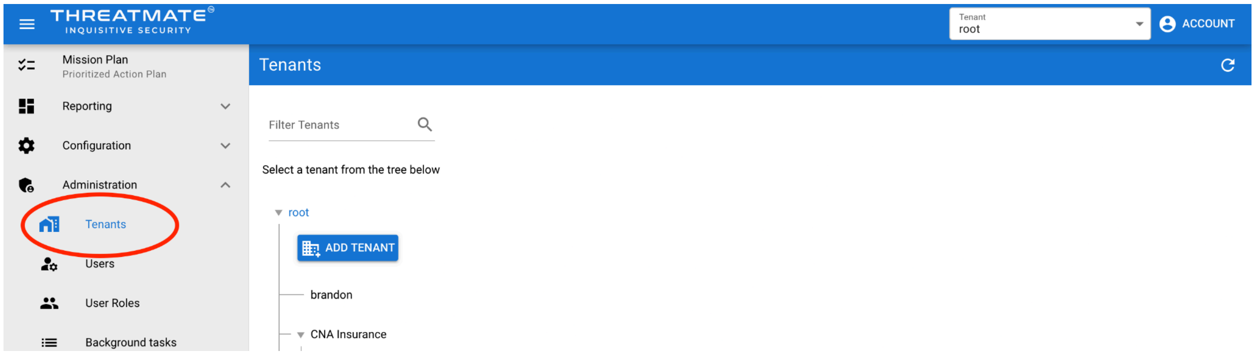
- Change Password
- Manage Multi-Factor Authentication

Managing Tenants

ThreatMate supports hierarchical tenants which allow you to organize your customer base in a flexible manner. Each customer should have their own tenant in order to isolate the data that belongs to different customers. This way you can also do per tenant reporting.

Creating Tenants

In order to create tenants in ThreatMate you need to navigate to **Administration -> Tenants** page.



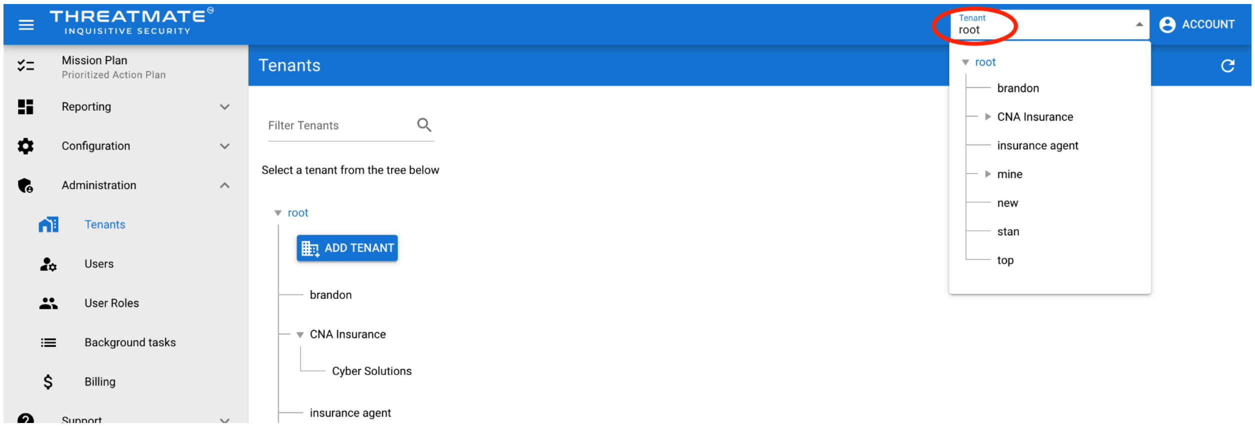
Tenant: root

Select a tenant from the tree below

You can create as many tenants as you need.

Global Tenant Selector

In order to view the data for a particular tenant you need to make sure it is selected in the global tenant selector:



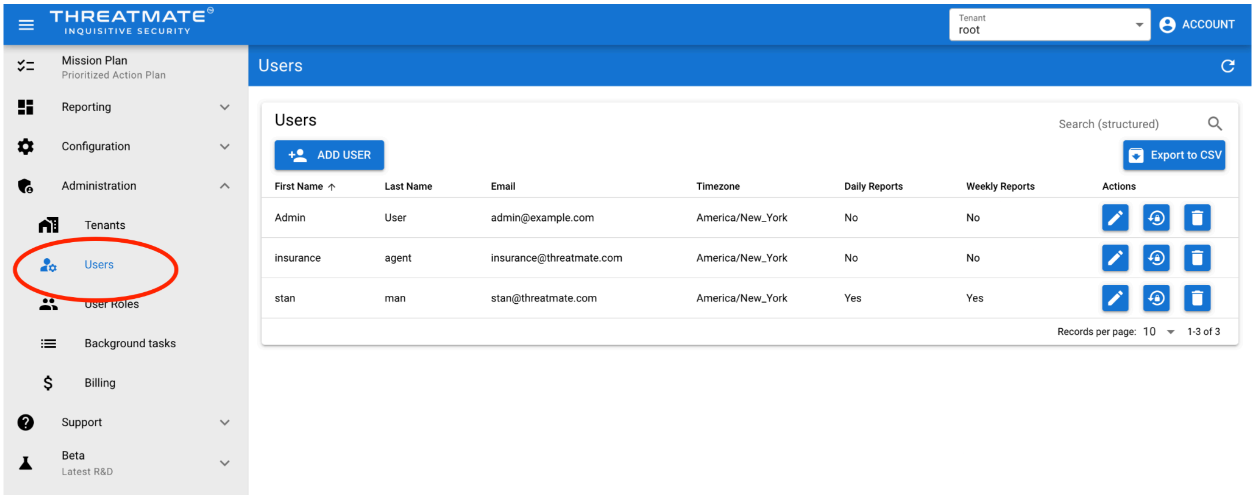
Tenant: root

Select a tenant from the tree below

Every interface in the dashboard respects the selected global tenant. Before adding any discovery agents, endpoint agents or cloud integrations make sure that you're adding them to the correct tenant. Always check the tenant upon login to make sure you are viewing the correct data.

Adding users to tenants

Each tenant can have its own users that are able to login to that tenant and see all child tenants. The users are allowed to see only the data in the tenant they are added to and any child tenants of their tenant. In order to add users to a tenant first make sure the current tenant is selected in the Global Tenant selector and then go to **Administration -> Users**.



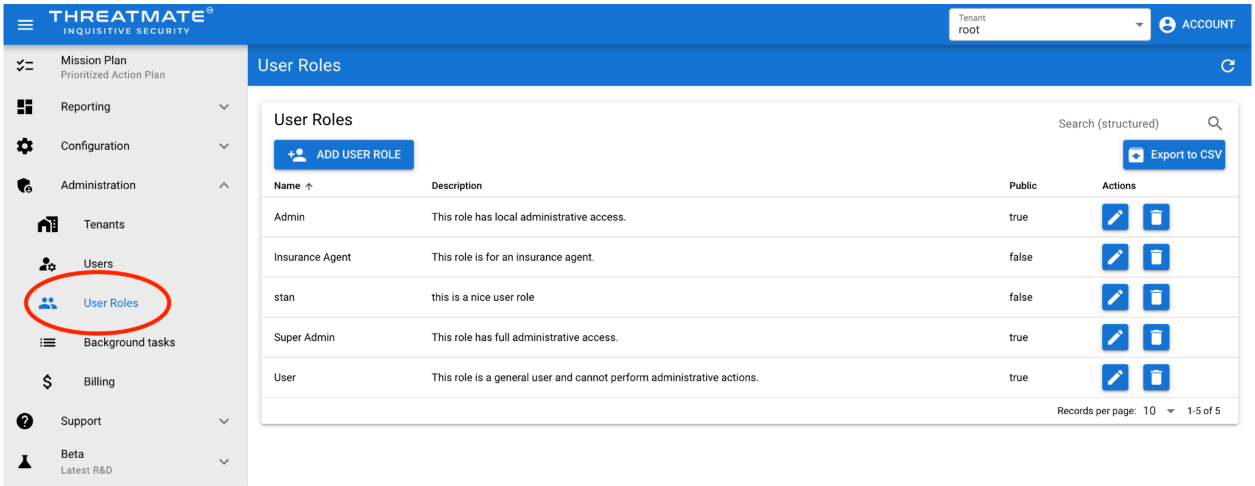
Users

First Name	Last Name	Email	Timezone	Daily Reports	Weekly Reports	Actions
Admin	User	admin@example.com	America/New_York	No	No	
insurance	agent	insurance@threatmate.com	America/New_York	No	No	
stan	man	stan@threatmate.com	America/New_York	Yes	Yes	

Records per page: 10 1-3 of 3

User Roles

ThreatMate supports custom user roles. They can be defined under **Administration -> User Roles**.



User Roles

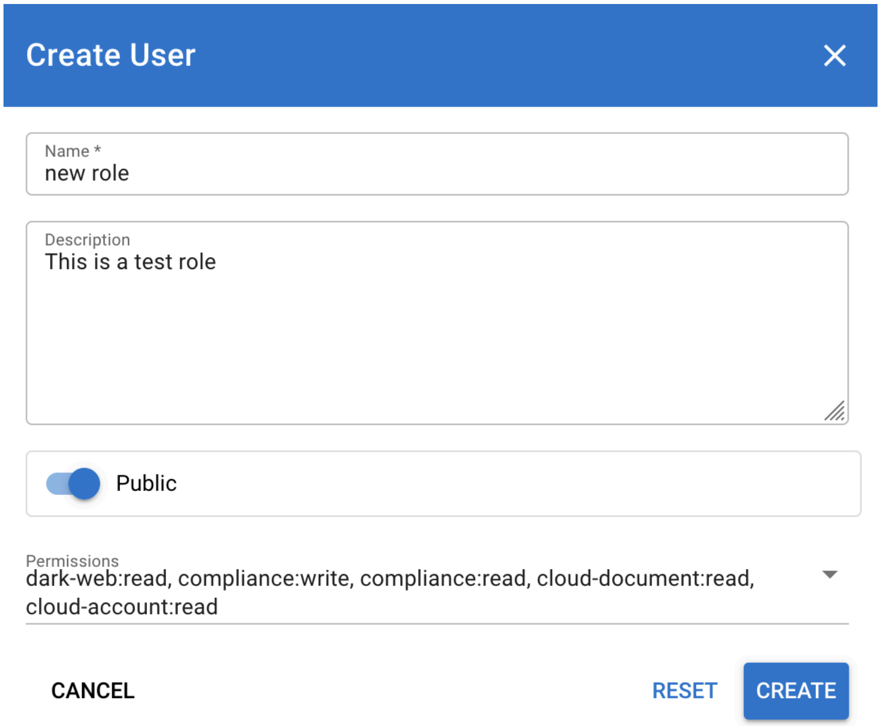
Name	Description	Public	Actions
Admin	This role has local administrative access.	true	
Insurance Agent	This role is for an insurance agent.	false	
stan	this is a nice user role	false	
Super Admin	This role has full administrative access.	true	
User	This role is a general user and cannot perform administrative actions.	true	

Records per page: 10 1-5 of 5

By default 4 user roles exist:

- Admin
- Insurance Agent
- Super Admin
- User

You can add any number of user roles:



Name *
new role

Description
This is a test role

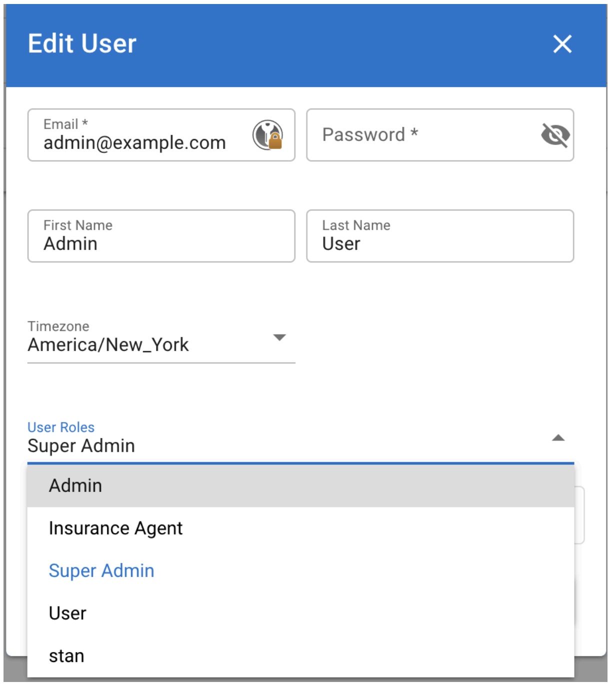
Public

Permissions
dark-web:read, compliance:write, compliance:read, cloud-document:read, cloud-account:read

Making the role **Public** means child tenants will inherit the role and can use it. Note that if the users are lacking specific permissions they will receive a **Forbidden** error message in the UI. You can test user roles by logging in as the new user and making sure the permissions are what you expect.

The UI will also change based on the available permissions. If a page requires a permission which the user doesn't have it will be hidden from the menu. This way the minimum UI will be displayed to the user based on the selected permissions.

You can assign multiple user roles to a user which will be the unique union of permissions across the user roles. This will allow you to create user roles that can be easily reused depending on the access requirements.



Edit User

Email * admin@example.com

Password *

First Name Admin

Last Name User

Timezone America/New_York

User Roles Super Admin

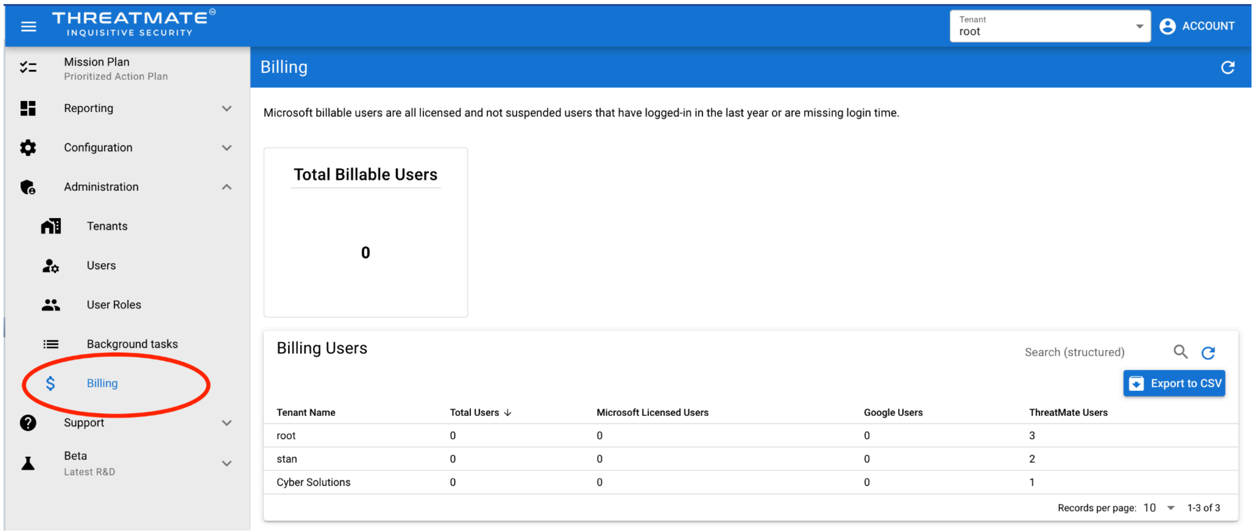
User Roles Permissions

The permissions for the User Roles can be viewed in this spreadsheet:

User Roles Permissions

Billing

To see the billing all child tenants you can navigate to Administration -> Billing:



Microsoft billable users are all licensed and not suspended users that have logged-in in the last year or are missing login time.

Total Billable Users

0

Billing Users

Tenant Name	Total Users ↓	Microsoft Licensed Users	Google Users	ThreatMate Users
root	0	0	0	3
stan	0	0	0	2
Cyber Solutions	0	0	0	1

Records per page: 10 1-3 of 3

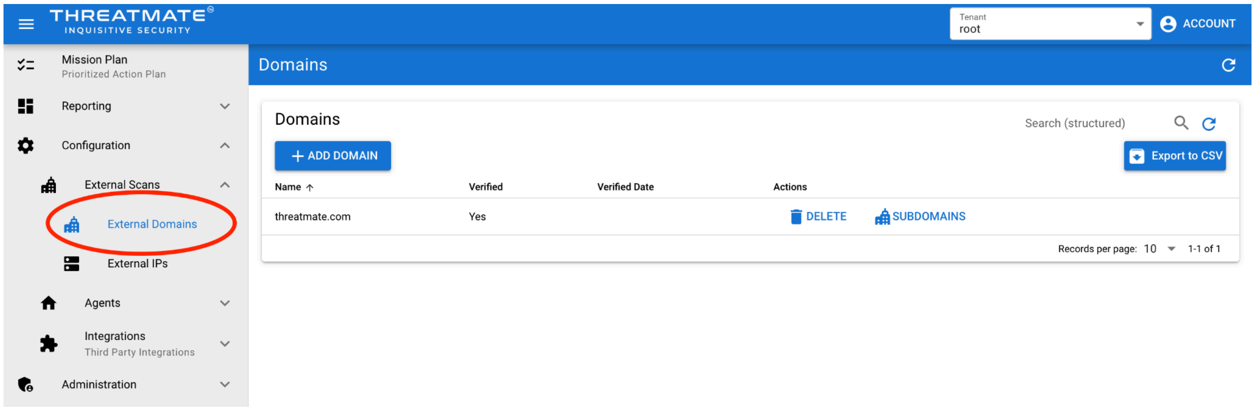
The billing users are calculated using all of the Google Workspace users and a subset of the Microsoft users which are licensed, not suspended and have logged in in the past year. The ThreatMate users are not counted as billable users.

ThreatMate External Attack Surface Scan

ThreatMate can scan any number of top level domains externally without the need to install the discovery agent. ThreatMate uses its own cloud infrastructure to conduct the scans. The scans are scheduled to run every 12 hours.

External Domains

In order to add domains to scan navigate to the **Configuration -> External Scans -> External Domains** page:



Domains

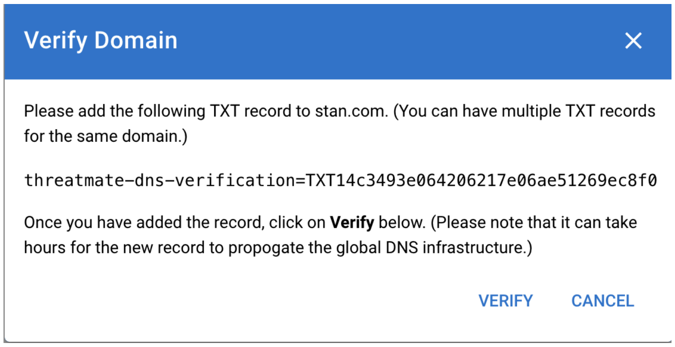
Name ↑	Verified	Verified Date	Actions
threatmate.com	Yes		DELETE SUBDOMAINS

Records per page: 10 1-1 of 1

Note that when you add a domain it will be scanned immediately upon adding and it will take about 5 minutes to complete. The domain will be added to the currently selected tenant. Make sure you have the correct tenant selected before continuing.

You can add any number of top level domains. They will be enumerated for their subdomains and each subdomain will be scanned for vulnerabilities.

The external domains can also be verified. This will enable us to perform full port scan on verified domains and an external penetration test. To verify a domain you'll need to add the corresponding TXT record to your DNS configuration:



Verify Domain

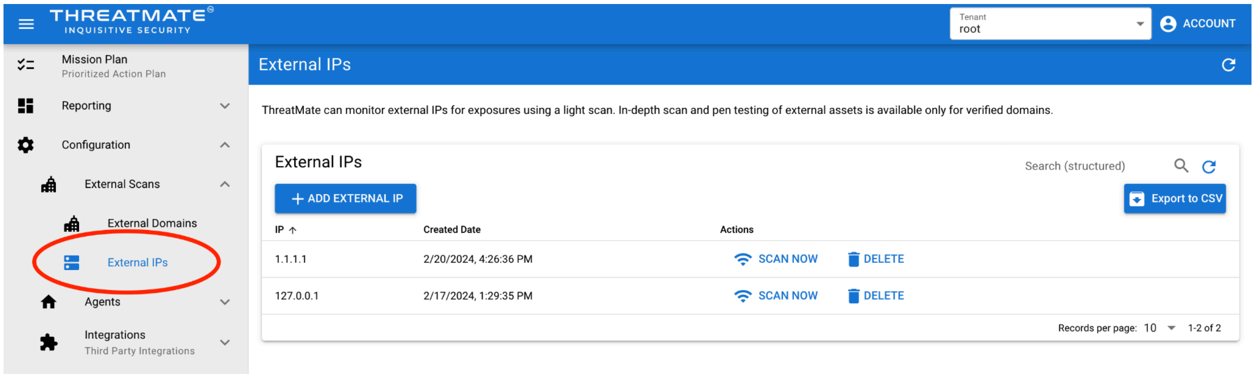
Please add the following TXT record to stan.com. (You can have multiple TXT records for the same domain.)

```
threatmate-dns-verification=TXT14c3493e064206217e06ae51269ec8f0
```

Once you have added the record, click on **Verify** below. (Please note that it can take hours for the new record to propogate the global DNS infrastructure.)

External IPs

You can also scan external IPs that don't have an associated domain. In order to prevent abuse we don't allow full port scan or pen testing on the external IPs. In order to pen test them you can create a DNS record for them and verify them.



Tenant: root

ThreatMate can monitor external IPs for exposures using a light scan. In-depth scan and pen testing of external assets is available only for verified domains.

IP ↑	Created Date	Actions
1.1.1.1	2/20/2024, 4:26:36 PM	SCAN NOW DELETE
127.0.0.1	2/17/2024, 1:29:35 PM	SCAN NOW DELETE

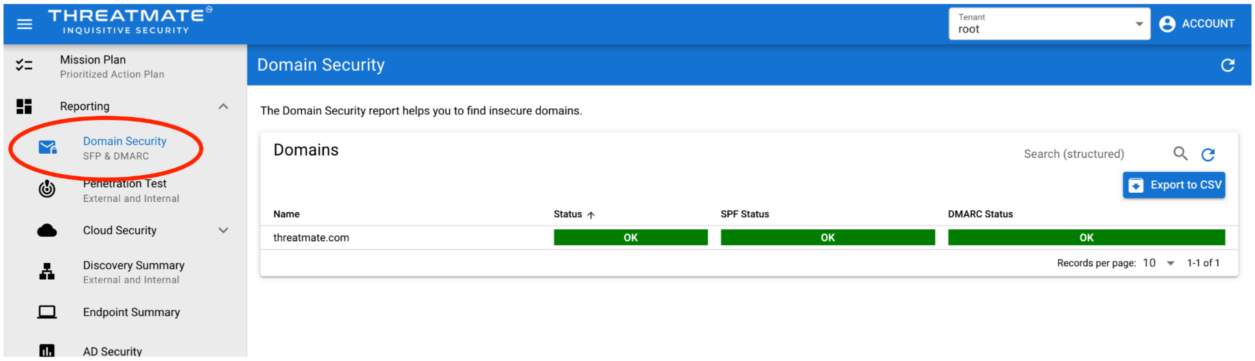
Records per page: 10 1-2 of 2

External Scan Results

There are a couple of reports that can show a different set of external scan analysis.

Domain Security

The first report that is generated for the external domains is the Domain Security report which you can find in Reporting -> Domain Security:



The Domain Security report helps you to find insecure domains.

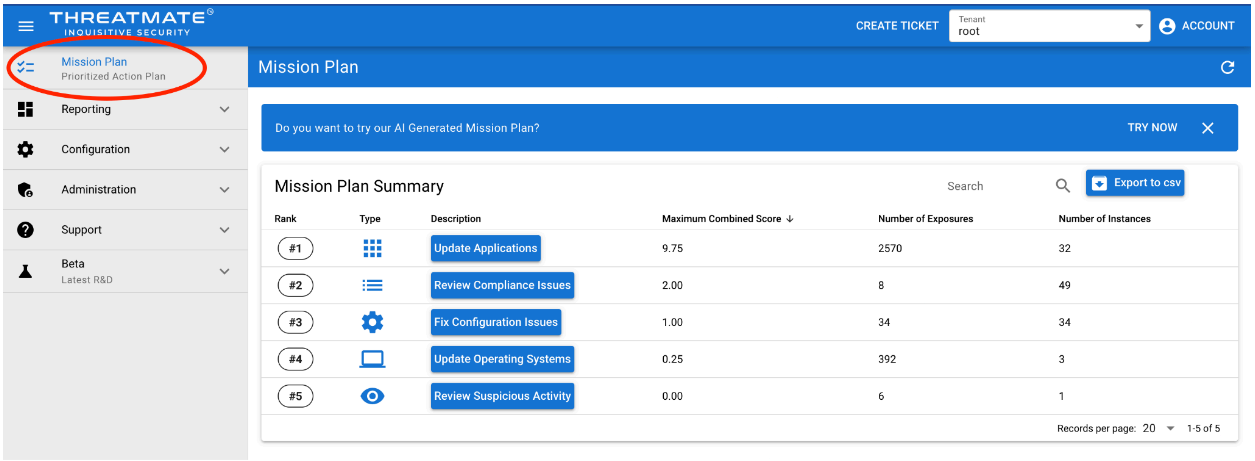
Domains

Name	Status ↑	SPF Status	DMARC Status
threatmate.com	OK	OK	OK

Here you can quickly see which subdomains have correct SPF and DMARC entries. All subdomains that have an MX record will be analyzed.

Mission Plan

The Mission Plan will contain the external scan results (alongside other results):



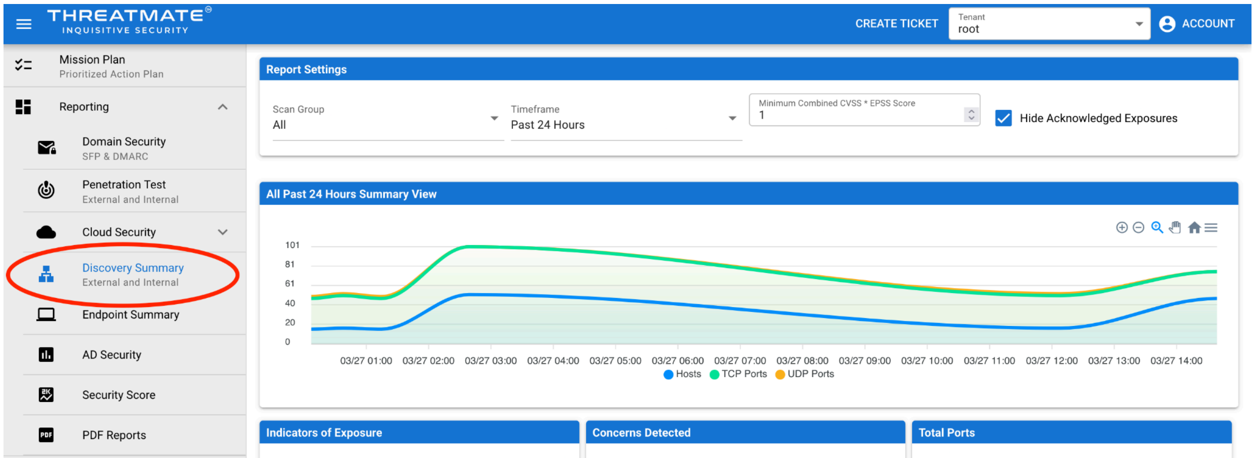
Do you want to try our AI Generated Mission Plan?

Mission Plan Summary

Rank	Type	Description	Maximum Combined Score ↓	Number of Exposures	Number of Instances
#1		Update Applications	9.75	2570	32
#2		Review Compliance Issues	2.00	8	49
#3		Fix Configuration Issues	1.00	34	34
#4		Update Operating Systems	0.25	392	3
#5		Review Suspicious Activity	0.00	6	1

Discovery Summary

The discovery summary report can provide more information on the found exposures and domains. It can be found in **Reporting -> Discovery Summary**:



Tenant: root

Report Settings

Scan Group: All

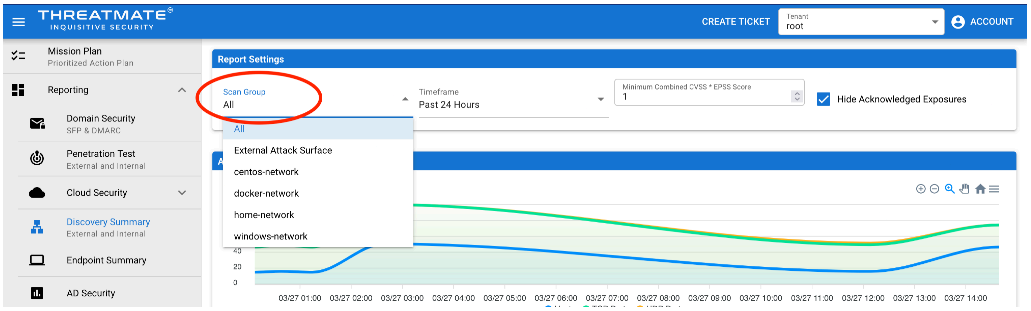
Timeframe: Past 24 Hours

Minimum Combined CVSS * EPSS Score: 1

☑ Hide Acknowledged Exposures

All Past 24 Hours Summary View

In order to only see the external results you'll need to select the **External Attack Surface** scan group:



Tenant: root

Report Settings

Scan Group: All

Timeframe: Past 24 Hours

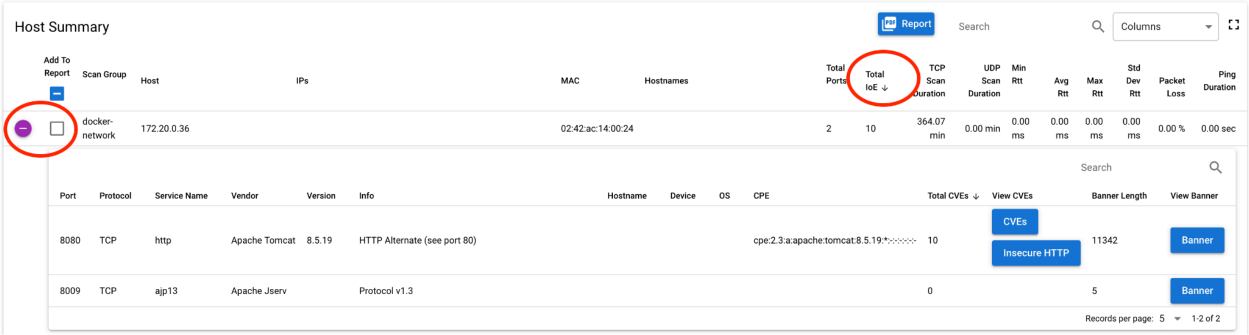
Minimum Combined CVSS * EPSS Score: 1

☑ Hide Acknowledged Exposures

The discovery summary dashboard is organized in 3 sections:

- Indicators of Exposure - shows the found issues sorted by the Maximum Combined Score
- Port Summary - the open ports found on all scanned subdomains
- Host Summary - a summary of all found subdomains and their data

The host summary includes all the results for each subdomain which can be accessed by clicking on the purple button + at the beginning of each host row:



Host Summary

	Add To Report	Scan Group	Host	IPs	MAC	Hostnames	Total Ports	Total IoE ↓	TCP Scan Duration	UDP Scan Duration	Min Rtt	Avg Rtt	Max Rtt	Std Dev Rtt	Packet Loss	Ping Duration
−	□	docker-network	172.20.0.36		02:42:ac:14:00:24		2	10	364.07 min	0.00 min	0.00 ms	0.00 ms	0.00 ms	0.00 ms	0.00 %	0.00 sec

Port	Protocol	Service Name	Vendor	Version	Info	Hostname	Device	OS	CPE	Total CVEs ↓	View CVEs	Banner Length	View Banner
8080	TCP	http	Apache Tomcat	8.5.19	HTTP Alternate (see port 80)				cpe:2.3:a:apache:tomcat:8.5.19:*:-:-:-:-:-:-	10	CVEs Insecure HTTP	11342	Banner
8009	TCP	ajp13	Apache Jserv		Protocol v1.3					0		5	Banner

Records per page: 5 1-2 of 2

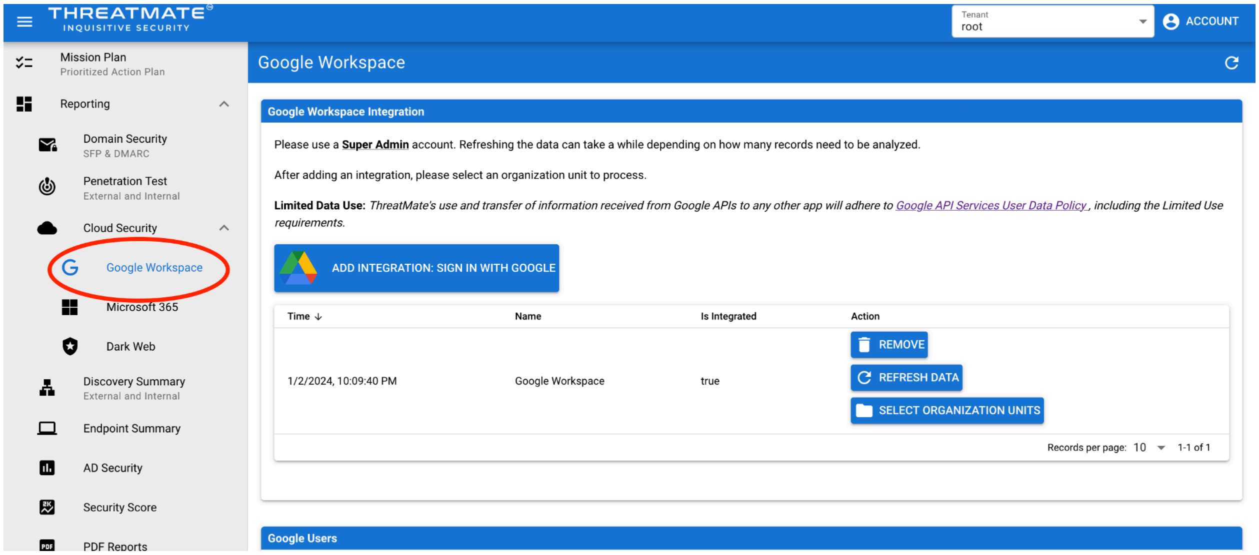
The table is sorted by the **Total IoE** column which stands for Total Indicators of Exposure.

ThreatMate Cloud Security

ThreatMate can analyze your customer’s Cloud Security provider for security issues. We support **Google Workspace** and **Microsoft 365**. You will need to add an integration in order to run the analysis. The integration requires a super admin account.

Google Workspace Integration

You can navigate to Reporting -> Cloud Security -> Google Workspace in order to add an integration and view the analysis:



Google Workspace Integration

Please use a **Super Admin** account. Refreshing the data can take a while depending on how many records need to be analyzed.

After adding an integration, please select an organization unit to process.

Limited Data Use: *ThreatMate's use and transfer of information received from Google APIs to any other app will adhere to Google API Services User Data Policy , including the Limited Use requirements.*

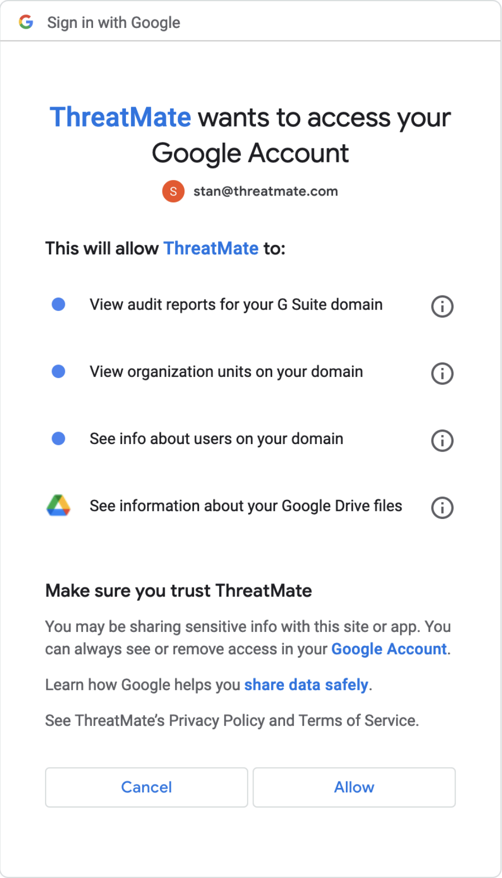
ADD INTEGRATION: SIGN IN WITH GOOGLE

Time ↓	Name	Is Integrated	Action
1/2/2024, 10:09:40 PM	Google Workspace	true	REMOVE REFRESH DATA SELECT ORGANIZATION UNITS

Records per page: 10 1-1 of 1

Google Users

First click on **Add Integration** in order to start the integration. You will be presented with the following consent screen



Sign in with Google

ThreatMate wants to access your Google Account

stan@threatmate.com

This will allow ThreatMate to:

- View audit reports for your G Suite domain
- View organization units on your domain
- See info about users on your domain
- See information about your Google Drive files

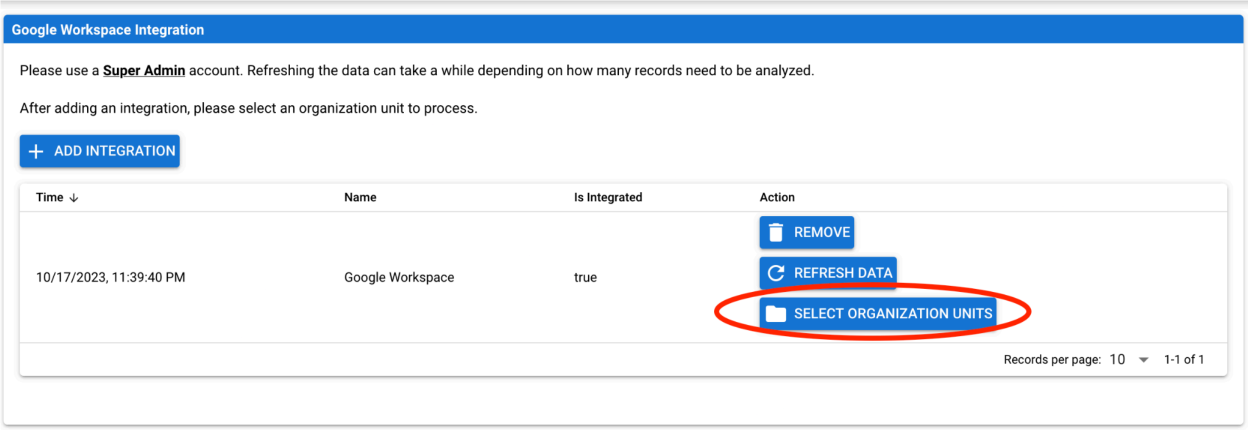
Make sure you trust ThreatMate

You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.

Learn how Google helps you share data safely.

See ThreatMate's Privacy Policy and Terms of Service.

Please select **Allow** in order to enable the integration. The integration should be successful and before seeing any data you need to select the Organization Units you'd like ThreatMate to scan.



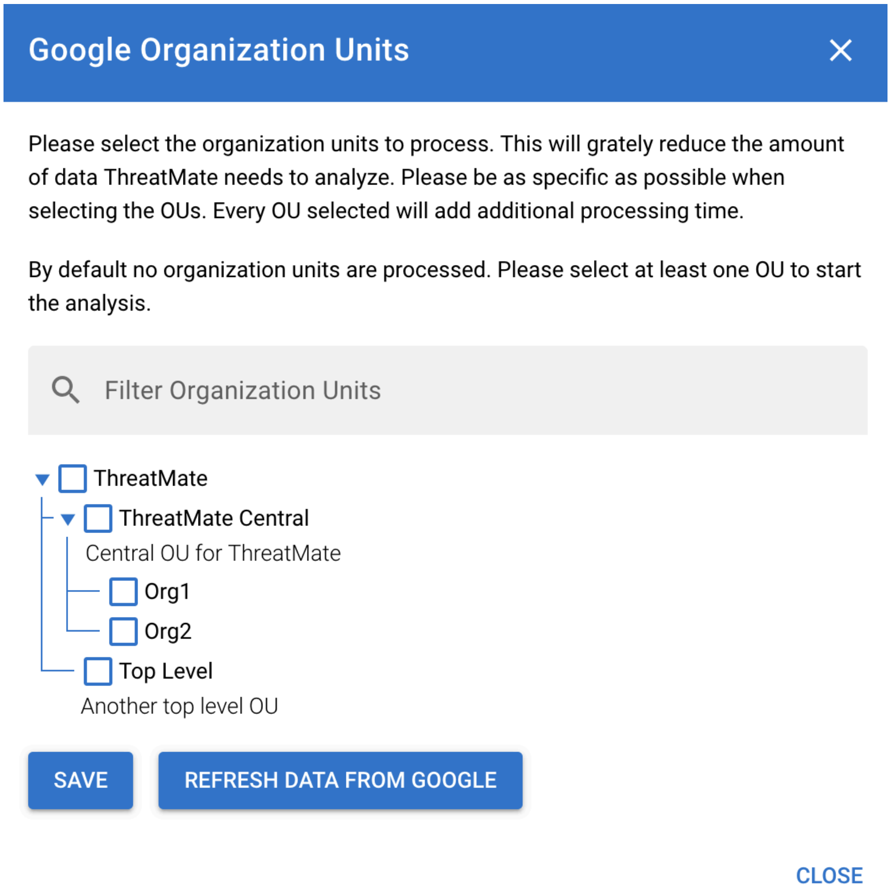
Google Workspace Integration

Please use a Super Admin account. Refreshing the data can take a while depending on how many records need to be analyzed.

After adding an integration, please select an organization unit to process.

Time ↓	Name	Is Integrated	Action
10/17/2023, 11:39:40 PM	Google Workspace	true	REMOVE REFRESH DATA SELECT ORGANIZATION UNITS

Records per page: 10 1-1 of 1



Google Organization Units

Please select the organization units to process. This will grately reduce the amount of data ThreatMate needs to analyze. Please be as specific as possible when selecting the OUs. Every OU selected will add additional processing time.

By default no organization units are processed. Please select at least one OU to start the analysis.

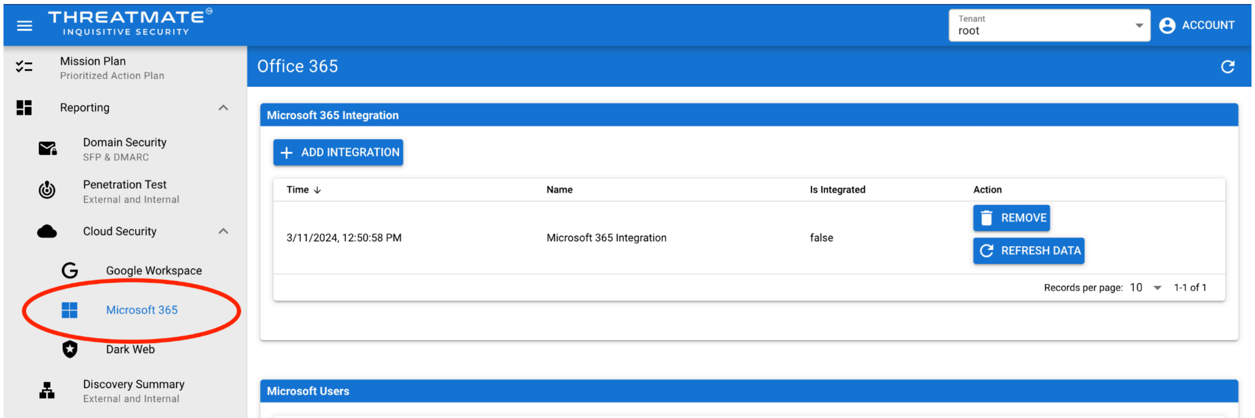
Filter Organization Units

- □ ThreatMate
  - □ ThreatMate Central
    Central OU for ThreatMate
    - □ Org1
    - □ Org2
  - □ Top Level
    Another top level OU

After selecting the organization unit please select **Save**. The analysis will start and take time depending on how large your customer's cloud account is.

Microsoft 365 Integration

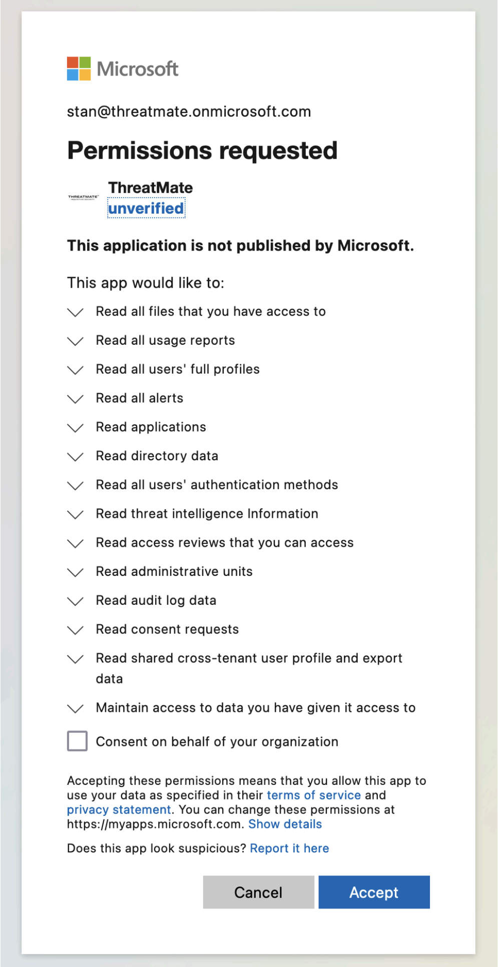
The Microsoft365 integration follows the same principle as the Google Workspace integration. It's located in **Reporting -> Cloud Security -> Microsoft 365:**



Time ↓	Name	Is Integrated	Action
3/11/2024, 12:50:58 PM	Microsoft 365 Integration	false	REMOVE REFRESH DATA

Records per page: 10 1-1 of 1

You need to click **Add Integration** to start the integration. You'll be presented with the following consent screen:


Microsoft

stan@threatmate.onmicrosoft.com

Permissions requested

ThreatMate
unverified

This application is not published by Microsoft.

This app would like to:

- Read all files that you have access to
- Read all usage reports
- Read all users' full profiles
- Read all alerts
- Read applications
- Read directory data
- Read all users' authentication methods
- Read threat intelligence Information
- Read access reviews that you can access
- Read administrative units
- Read audit log data
- Read consent requests
- Read shared cross-tenant user profile and export data
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

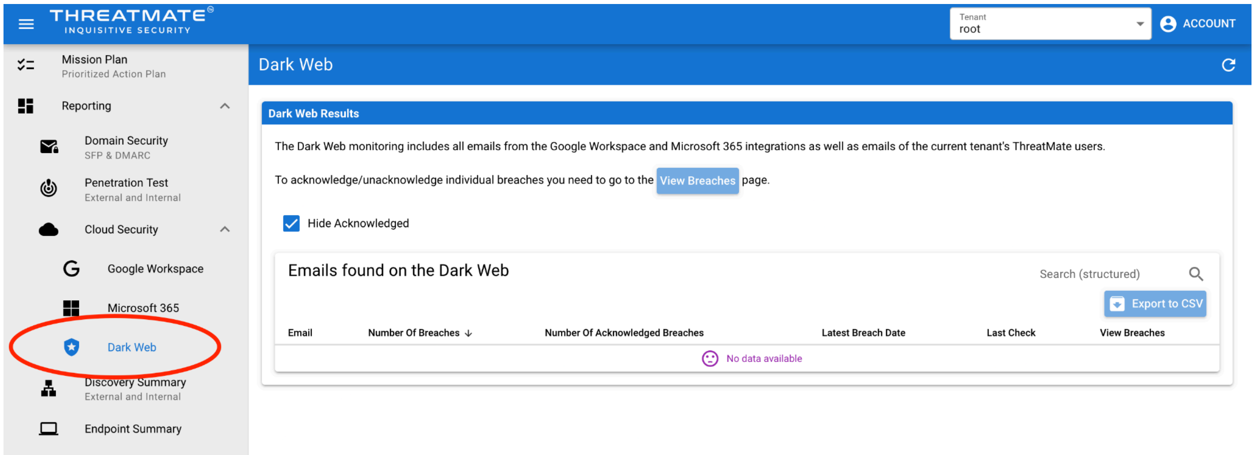
Does this app look suspicious? Report it here

Cancel Accept

Please select the checkbox **Consent on behalf of your organization** and click **Accept**. The analysis will take some time to finish.

ThreatMate Dark Web Monitoring

Once you have the cloud integrations implemented ThreatMate will automatically start scanning your users for breaches found on the Dark Web. you can see the results in **Reporting -> Cloud Security -> Dark Web**:



The Dark Web monitoring includes all emails from the Google Workspace and Microsoft 365 integrations as well as emails of the current tenant's ThreatMate users.

To acknowledge/unacknowledge individual breaches you need to go to the View Breaches page.

☑ Hide Acknowledged

Emails found on the Dark Web

Email	Number Of Breaches ↓	Number Of Acknowledged Breaches	Latest Breach Date	Last Check	View Breaches
No data available					

ThreatMate Discovery Agent

The ThreatMate Discovery Agent is a network monitoring service that scans networks for live hosts and then runs vulnerability scans and penetration tests against them. It runs 24x7 and is able to detect and scan devices continuously around the clock.

The deployment instructions depend on your operating system. The general hardware requirements for the default discovery settings are:

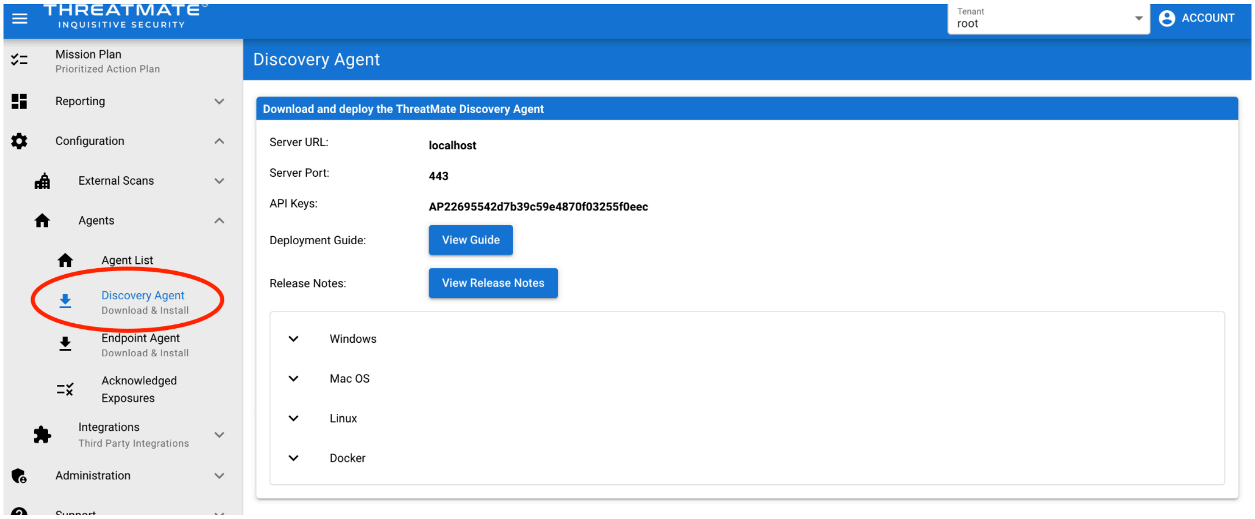
- 1 CPU for each batch of 1000 live hosts
- 2GB of RAM for each batch of 1000 live hosts

If you want to enable penetration testing you'll need the following hardware requirements:

- 4 CPUs
- 8GB of RAM

The recommended deployment is to have a single discovery agent scan a single network where the discovery agent is located on a persistent machine on the target network. The sensor can scale horizontally by running additional instances of it covering separate networks or covering different hosts on the same network in case the network is large. All results are streamed encrypted to ThreatMate's cloud infrastructure using HTTPS.

In order to download the discovery agent you need to navigate to the download page on the left side menu in the web dashboard: **Configuration -> Agents -> Discovery Agent:**



Discovery Agent

Download and deploy the ThreatMate Discovery Agent

Server URL: localhost

Server Port: 443

API Keys: AP22695542d7b39c59e4870f03255f0eec

Deployment Guide: View Guide

Release Notes: View Release Notes

Deployment Considerations

The discovery agent actively scans networks. The default scan interval is twice a day every 12 hours. It can generate network traffic which can be tweaked with custom settings. For best performance and least network disruption we recommend to run the agent on a persistent machine located on the target network. This will avoid scanning across router/firewall/VPN boundaries which can create network congestion and disruption of the network service. This is the preferred way to run discovery scans and allows us to enable ARP scanning which is the 100% guaranteed way to discover live devices on a network. It also allows us to collect the MAC address of any connected device which is an important identification information. Since we don't charge for the discovery agent you are free to deploy it on as many networks as you'd like. The best scan performance we can get is when each discovery sensor scans its own local LAN. This means having a persistent device with our discovery agent on each network we are scanning.

If scanning a local LAN network is not possible then we need to switch from ARP based scanning to ping sweep:

1. The first issue with ping sweep scanning is that it doesn't guarantee we'll find all live devices on a network. Devices which disable ICMP echo responses will not be discovered.
2. The second issue is that ping sweep does not have the ability to collect the MAC address. The MAC address is an important persistent identifier even for devices that change their IPs.
3. The third issue with this architecture is that it will place a significant load on the network infrastructure between the discovery agent and the target network. This can degrade the network performance based on the network architecture. For example if there is a router with a small NAT table it can easily get saturated by the discovery agent and stop serving new connections. If there is a VPN connection over which the discovery agent is scanning it could saturate that network and degrade the performance for other VPN clients.

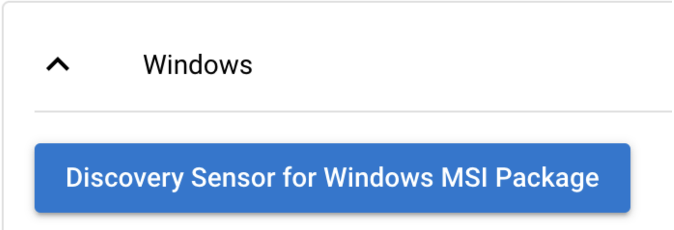
We highly suggest using a per local LAN discovery deployment which will guarantee the best performance for the scans with minimum impact on the network. Scanning across router/firewall/VPN boundaries could cause disruptions based on the network hardware and connection quality.

Scan Groups

Before configuring the discovery agent we need to set a scan group which is a grouping of hosts that will be scanned by the discovery agent. Normally a scan group can be the subnet that is scanned such as “192.168.1.1/24”. But it can also contain multiple subnets or URLs or IPs. The only restriction is to not have duplicate hosts or overlapping networks as part of the scan group. One discovery agent can only handle one scan group at a time. So if you want to scan multiple subnets as separate scan groups you’ll need to use multiple discovery agents.

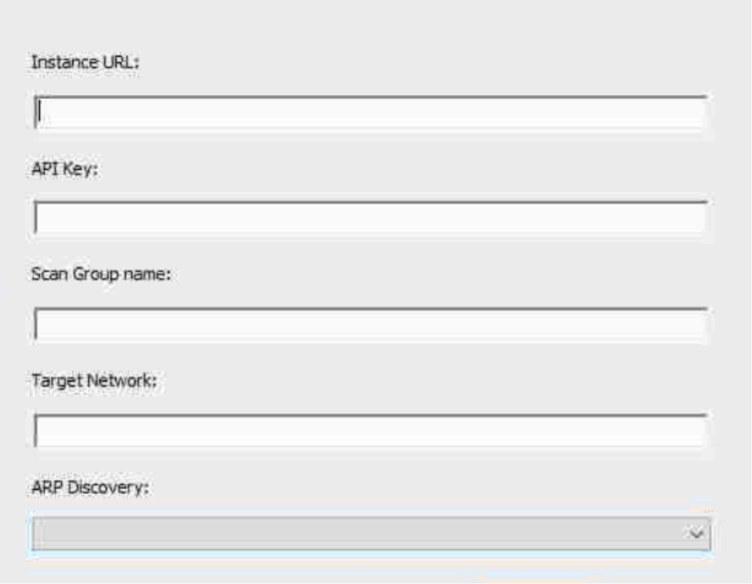
Windows

In order to deploy the discovery agent on Windows you need to click on the Windows drop-down.



You can click on the button to download the Windows MSI package: **threatmate-discovery.msi**

Once downloaded you can install the package. When you run the Windows installer you’ll be prompted to enter the following parameters:



Instance URL:

API Key:

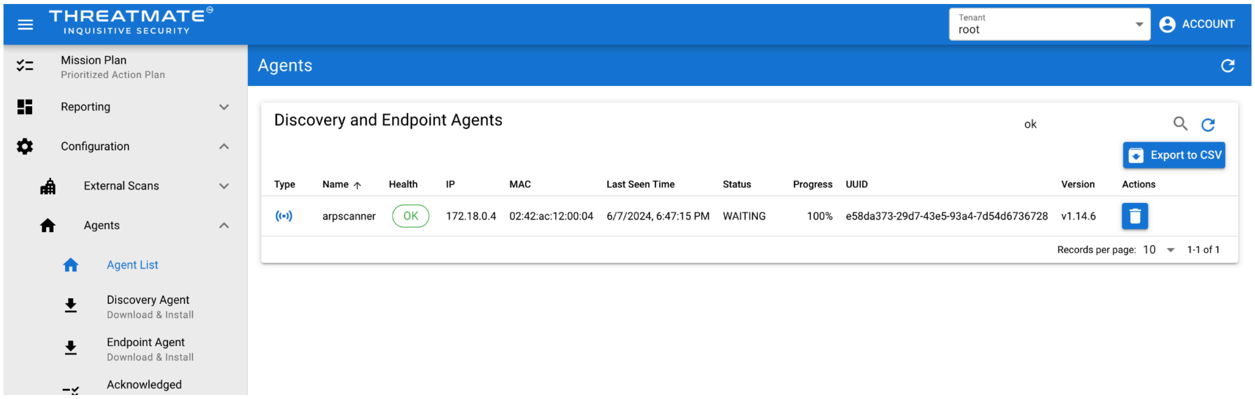
Scan Group name:

Target Network:

ARP Discovery:

- Instance URL: app.threatmate.com
- API Key: the tenant's API key
- Scan Group Name: the name of the network. Normally internal-network or office-network. Sometimes you can have multiple internal VLANs and you want to name them such as datacenter-network or management-network etc.
- Target Networks: the target network CIDR such as 192.168.1.0/24
- ARP Discovery: please select 'Yes' here. For each network that you want to scan you'll need a persistent device on which you'll install a discovery agent and enable ARP scanning for it.

You can verify that the agent is installed by going to **Configuration -> Agents -> Agent List**. The discovery agent will have a different icon.



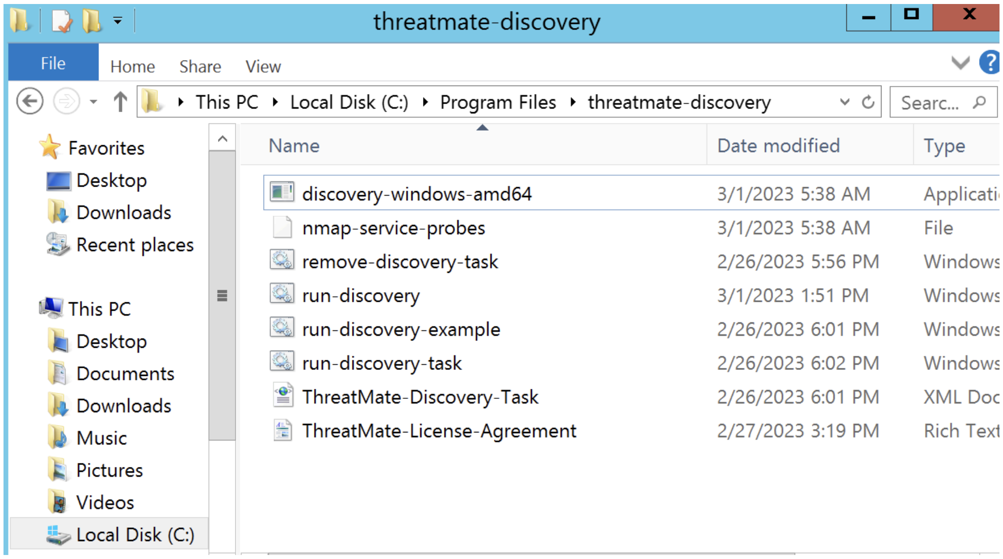
Discovery and Endpoint Agents

Type	Name ↑	Health	IP	MAC	Last Seen Time	Status	Progress	UUID	Version	Actions
((•))	arpscanner	OK	172.18.0.4	02:42:ac:12:00:04	6/7/2024, 6:47:15 PM	WAITING	100%	e58da373-29d7-43e5-93a4-7d54d6736728	v1.14.6	

Records per page: 10 1-1 of 1

Advanced Configuration

Once the agent is installed you can find its files in **C:\Program Files\threatmate-discovery\**



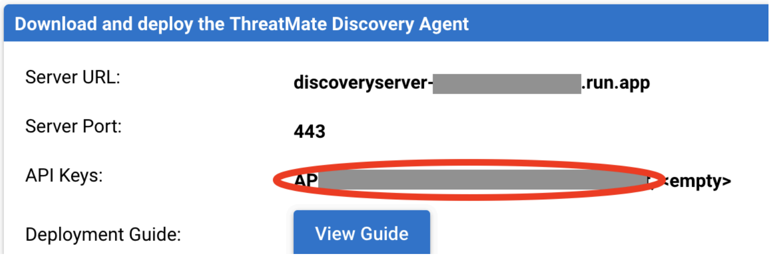
Name	Date modified	Type
discovery-windows-amd64	3/1/2023 5:38 AM	Applicati
nmap-service-probes	3/1/2023 5:38 AM	File
remove-discovery-task	2/26/2023 5:56 PM	Windows
run-discovery	3/1/2023 1:51 PM	Windows
run-discovery-example	2/26/2023 6:01 PM	Windows
run-discovery-task	2/26/2023 6:02 PM	Windows
ThreatMate-Discovery-Task	2/26/2023 6:01 PM	XML Doc
ThreatMate-License-Agreement	2/27/2023 3:19 PM	Rich Text

In order to change the discovery configuration you need to edit the file **run-discovery.bat**

```
"C:\Program Files\threatmate-discovery\discovery-windows-amd64.exe"
--arp-discovery --scan-target 192.168.1.0/24 --scan-group-name
some-network-name --server-host app.threatmate.com --server-port 443
--api-key APXXXXXXXXXXXX
```

Discovery Agent Configuration Options

- `--api-key`: specify the API key for the right tenant. The API key is used to determine the destination tenant. You can get the API key from the Discovery Agent download page in the dashboard.



Download and deploy the ThreatMate Discovery Agent

Server URL:	**discoveryserver-[redacted].run.app**
Server Port:	**443**
API Keys:	**AP[redacted]<empty>**
Deployment Guide:	View Guide

- `--scan-target`: specify the target to be scanned. The target can be a CIDR subnet, an IP address, a URL or a hostname. The sensor needs to be able to reach the target network or host in order to scan it. Multiple targets can be provided with additional **--scan-target** arguments such as: `--scan-target 192.168.1.0/24 --scan-target 1.1.1.1 --scan-target google.com` etc.

- `--arp-discovery`: Enable ARP protocol live host discovery. **We highly recommend enabling this setting!** Using the ARP protocol to discover live hosts is the preferred method as long as the discovery agent is on the same subnet as the live hosts. The ARP protocol discovery guarantees discovering all live hosts on the network regardless if they have ICMP Echo enabled or not. But the protocol is not routable which means it can't be used to discover live hosts across a router boundary such as a different subnet or external domains. If you need to discover live hosts on multiple subnets or on a subnet that is outside of the discovery agent then you shouldn't use the arp discovery. Otherwise the discovery will find no hosts to scan.

- `--exclude-ports:` you can exclude specific ports from being scanned. Some services produce extra alerts when they are scanned and excluding their ports can solve the problem. The excluded ports string follows the following rules:

  ```
  --exclude-ports "1.1.1.1,T:50,U:53,T:900-910,75"
  ```

  - The port string should start with the host followed by a comma and the rest of the port string
  - T: stands for TCP and U: stands for UDP
  - Port ranges can be specified with a dash: T:900-910 means all TCP ports between 900 and 910
  - A port without T: or U: is considered both TCP and UDP
  - Multiple **--exclude-ports** entries can be specified, but each should be for a different host.
  - CIDR networks are not accepted for the excluded ports
  - The excluded hosts should be part of the scan targets. Otherwise an error will be returned. We can't exclude a port or host that we are not scanning.

- `--exclude-service-probes`: you can exclude specific ports from service detection. This means the port will still be scanned if it is open but no further service probes will be sent to it. This will prevent the discovery of vulnerabilities behind the port. Some services crash when being probed so this allows discovery to skip them. The excluded service probes format string is the same as the **--exclude-ports string.** Please refer to it for an explanation. Here is an example:

  ```
      --exclude-service-probes "1.1.1.1,T:50,U:53,T:900-910,75"
  ```

- `--scan-group-file`: A YAML based configuration file that specifies what targets to scan. It can include subnets, IPs, URLs or hostnames:

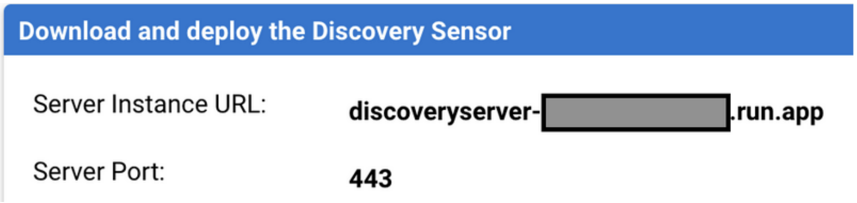
```
scan_group_name:
  hosts:
    - 1.1.1.1
    - 1.1.1.2
    - google.com
    - 192.168.1.0/24
  exclude-ports:
    1.1.1.1: "T:5055,T:5056"
    8.8.8.8: "T:80"
  exclude-service-probes:
    1.1.1.1: "T:5055,T:5056"
    8.8.8.8: "T:80"
```

The YAML configuration file has the following sections:

- `scan_group_name:` This will be the name of the scan group that all hosts will be grouped under. It can use alpha-numeric characters including dashes or underscores and it can't be longer than 32 characters
- `hosts:` this section specifies the scan targets. Refer to --scan-target for more information on the accepted options
- `exclude-ports:` this specifies hosts and ports that should be excluded from the scan. Please refer to the --exclude-ports argument for more details on the port string specification
- `exclude-service-probes:` this specifies hosts and ports to be excluded from service detection. Please refer to the --exclude-service-probes argument for more information on the port string schema

- `--scan-group-name`: this sets the group name for the target network. Groups are important to distinguish different networks with the same IP address space. You can use any human readable name here. For example **main-office-network** or **docker-network**. This is a required parameter unless you're using a YAML file. The command line option overrides the YAML file.

- `--server-host` and `--server-port`: This is ThreatMate's cloud instance server that has been provisioned to you. You can find it on the top of the download page. Copy the server and port from there

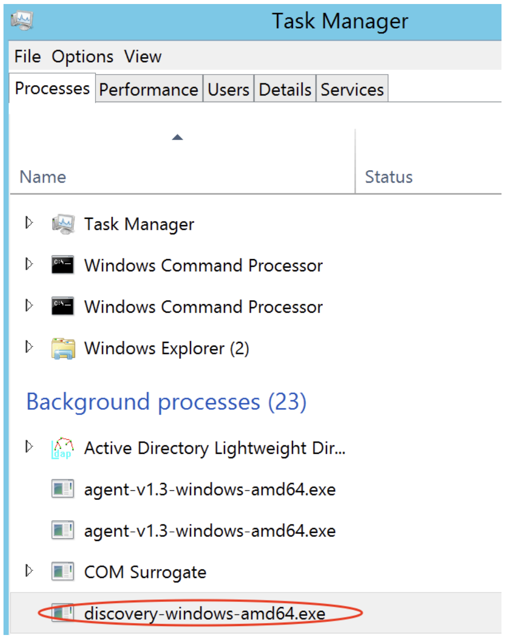


Download and deploy the Discovery Sensor

Server Instance URL: **discoveryserver-[redacted].run.app**

Server Port: **443**

After configuring the running parameters you can execute the bat file and make sure the discovery agent starts correctly. When the bat file is run manually the discovery agent will run in the foreground in a terminal. In order to turn it into a service you can use the **run-discovery-task.bat** file. Run the file as an administrator but make sure discovery is not running, otherwise you'll have two instances of discovery running at the same time. It is used to create a Task that will run as an administrator on system startup. Once the task is installed you can verify that discovery is running by looking in the **Task Manager**.



Task Manager
Windows Command Processor
Windows Command Processor
Windows Explorer (2)

Background processes (23)

Active Directory Lightweight Dir...
agent-v1.3-windows-amd64.exe
agent-v1.3-windows-amd64.exe
COM Surrogate
discovery-windows-amd64.exe

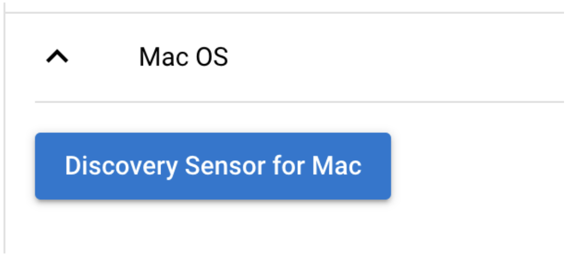
Run discovery quick start

Once you install threatmate-discovery you need to configure it. The following steps should get you started:

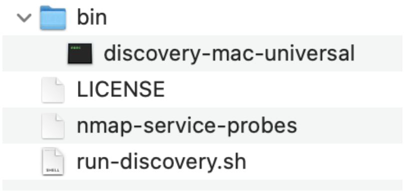
- Go to **C:\Program Files\threatmate-discovery**
- Copy the file **run-discovery-example.bat** to **run-discovery.bat**
- Edit **run-discovery.bat**
- Enter your API key, scan target which can be a CIDR, scan group name such as "internal-network" or "office-network" and please add the option `--arp-discovery` at the end as the last parameter
- Run the agent by executing **run-discovery.bat** as an admin - it should do some work and show a bunch of text in the console.
- Check to see if the discovery agent shows up in the task manager and the ThreatMate dashboard: **Configuration -> Agents -> Agent List**
- Once you confirm that discovery is working, close the open CMD window and install it as a scheduled task by running **run-discovery-task.bat**.

Mac OS

In order to deploy the discovery agent on Mac OS X you need to click on the Mac OS drop-down. Next you can download the discovery **tar.gz** package: **discovery-mac-universal.tar.gz.**



Once downloaded you can untar the package



In order to configure discovery to run you need to open the **run-discovery.sh** file and edit it.

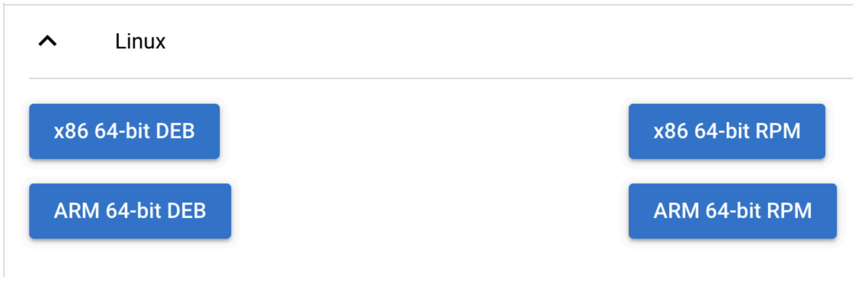
```
 ./bin/discovery-mac-universal --scan-target 192.168.1.0/24
--scan-group-name some-network-group --server-host
cloud-server-localhost --server-port 443 --api-key APXXXXXXXXXXXX
```

Please follow the steps at Discovery Agent Configuration Options for more information on the different configuration options.

After configuring the running parameters you can execute the shell script file and make sure the discovery agent starts correctly. Once you are certain that the sensor is running correctly you can place it in the background.

Linux

In order to deploy the discovery agent on Linux you need to download the installer for your OS from the dashboard: **Agents -> Discovery Agent**



You can download the .deb or .rpm file depending if you're installing on Ubuntu or CentOS. In order to install it on Ubuntu you can use dpkg:

```
dpkg -i ./threatmate-discovery_amd64.deb
```

On CentOS the command is

```
rpm -i ./threatmate-discovery_x86_64.rpm
```

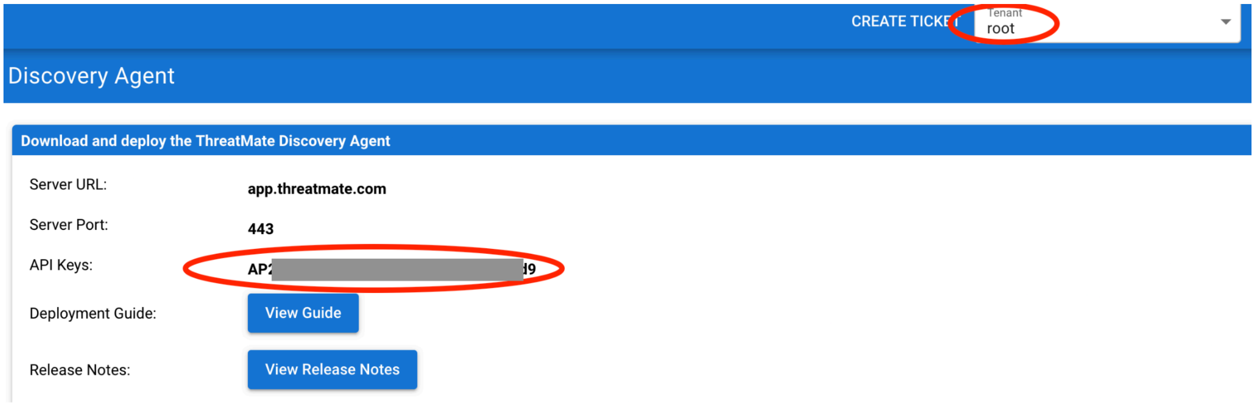
After the installation the following configuration files need to be updated:
Ubuntu: **/etc/default/threatmate-discovery**
CentOS: **/etc/sysconfig/threatmate-discovery**

Please follow the steps at Discovery Agent Configuration Options for more information on the different configuration options.

The initial minimum configuration includes the following arguments:

```
API_KEY=
SCAN_TARGET=
SCAN_GROUP_NAME=
```

You can get the API key from the Discovery Agent page. Please make sure you have selected the correct global tenant in order to use the appropriate API key. Otherwise the data will be sent to the wrong tenant.



Discovery Agent

Download and deploy the ThreatMate Discovery Agent

Server URL: app.threatmate.com

Server Port: 443

API Keys: [redacted]

Deployment Guide: View Guide

Release Notes: View Release Notes

The SCAN_TARGET is the subnetwork you'd like to scan. Multiple subnets can be specified separated by a comma. For example:

```
SCAN_TARGET=192.168.1.0/24,10.10.0.0/24
```

The SCAN_GROUP_NAME is the name that will be used to access the scanned targets.

After you're done configuring the agent you can start it with:

```
systemctl start threatmate-discovery
```

This should start discovery and put in the background. You can check the status with

```
systemctl status threatmate-discovery
```

Docker Container

The discovery agent can also be run as a docker container. You'll need to pull the image from the threatmate docker hub repository. It's important to configure the ulimit parameters in the configuration of the container otherwise the discovery agent could fail.

Here is an example **docker-compose.yml** file that also includes the ulimit parameters:

```
version: "3.8"
services:
  discovery-docker:
    container_name: discovery-docker
    hostname: discoveryscanner
    image: "threatmate/discovery:latest"
    restart: always
    environment:
      - SCAN_TARGET=192.168.1.0/24,192.168.2.0/24
      - API_KEY=APXXXXXXX
    ulimits:
      nproc: 65535
      nofile:
        soft: 999999
        hard: 999999
```

You can save the above file as **docker-compose.yml** and you can run it with:

```
docker compose up -d
```

You can look at the logs to make sure it is running with

```
docker logs -f discovery-docker
```

Or list all currently running containers with

```
docker ps
```

Penetration Testing

Discovery uses the nuclei pen testing framework to deeply scan devices for vulnerabilities, insecurities, default login credentials and web application exposures. The pen tests are based on templates which discovery downloads every time before the test begins. The tests can take longer to complete. The CPU and memory utilization will vary and should be monitored while a test is running. The recommended hardware requirements are:

- 4 CPUs
- 8GB of RAM

The default pen testing frequency is 168 hours (1 week) but it can be extended if needed. A reasonable architecture is to have a separate discovery agent that only does pen testing on a pre-scheduled interval. This way the network impact will be minimal and it will not interfere with the regular vulnerability scans.

In order to do an internal pen test you'll need to enable it in the discovery configuration. Please make sure you're running the latest discovery version. You can upgrade easily by installing the latest version downloaded from the dashboard. It will preserve your discovery settings but you'll need to start discovery manually after the upgrade. If you're running it on a Windows device you can edit **C:\Program Files\threatmate-discovery\run-discovery.bat** and add the following parameters:

```
--enable-nuclei-scan
```

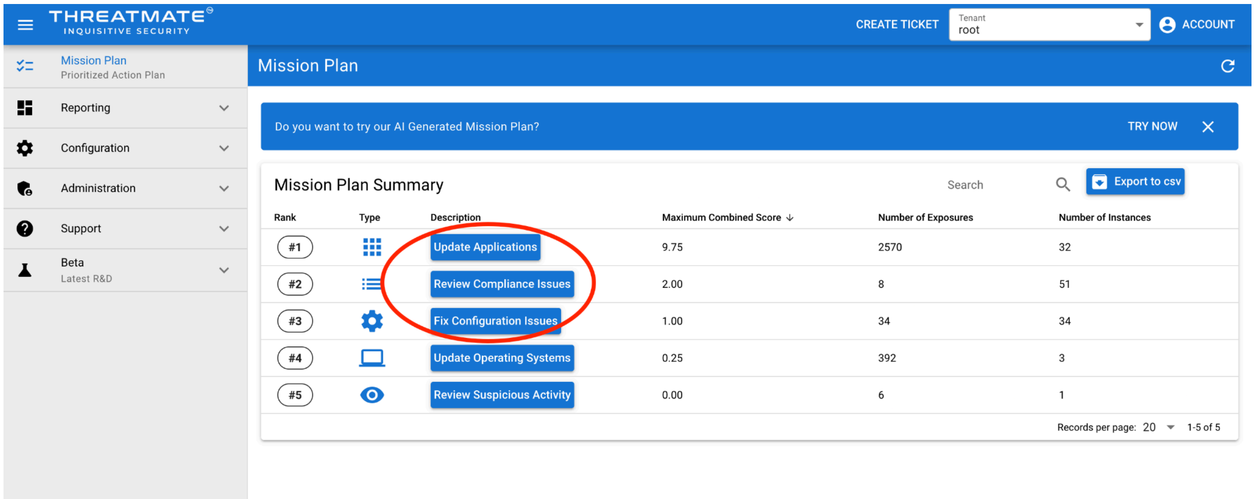
The pen test can take a long time to complete depending on how many devices you have on the network. We suggest running a separate discovery agent that can do only the pen test. In that case you'll need to disable the regular port scan with this setting:

```
--enable-port-scan=0
```

Please keep an eye on the resource utilization and let us know if you experience any issues.

Discovery Results

The discovery results can be seen in the Mission Plan under the **Update Applications**, **Review Compliance Issues** and **Fix Configuration** Issues categories.



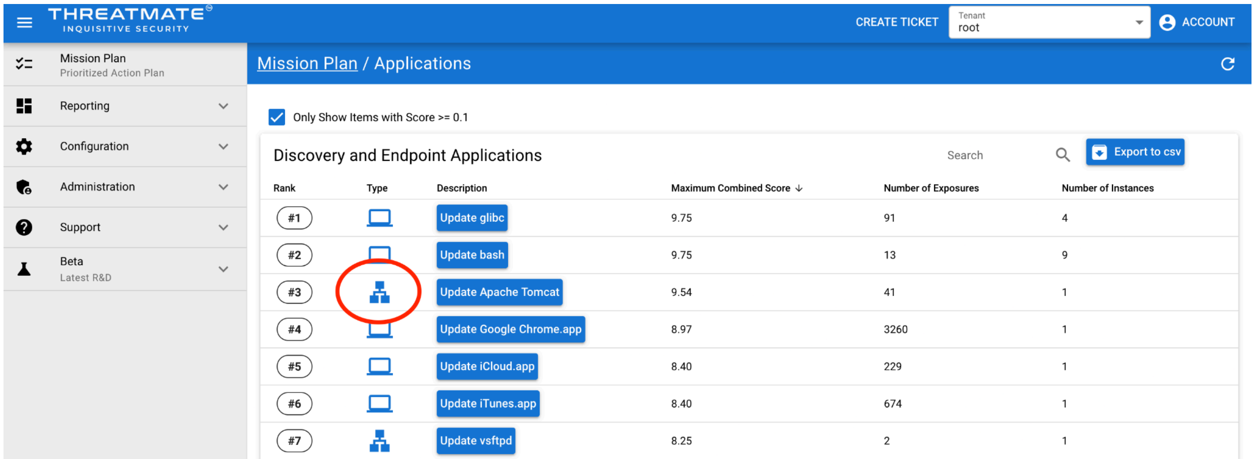
Do you want to try our AI Generated Mission Plan?

Mission Plan Summary

Rank	Type	Description	Maximum Combined Score ↓	Number of Exposures	Number of Instances
#1		Update Applications	9.75	2570	32
#2		Review Compliance Issues	2.00	8	51
#3		Fix Configuration Issues	1.00	34	34
#4		Update Operating Systems	0.25	392	3
#5		Review Suspicious Activity	0.00	6	1

Records per page: 20 1-5 of 5

The discovery results have a network icon so they can be easily recognized:

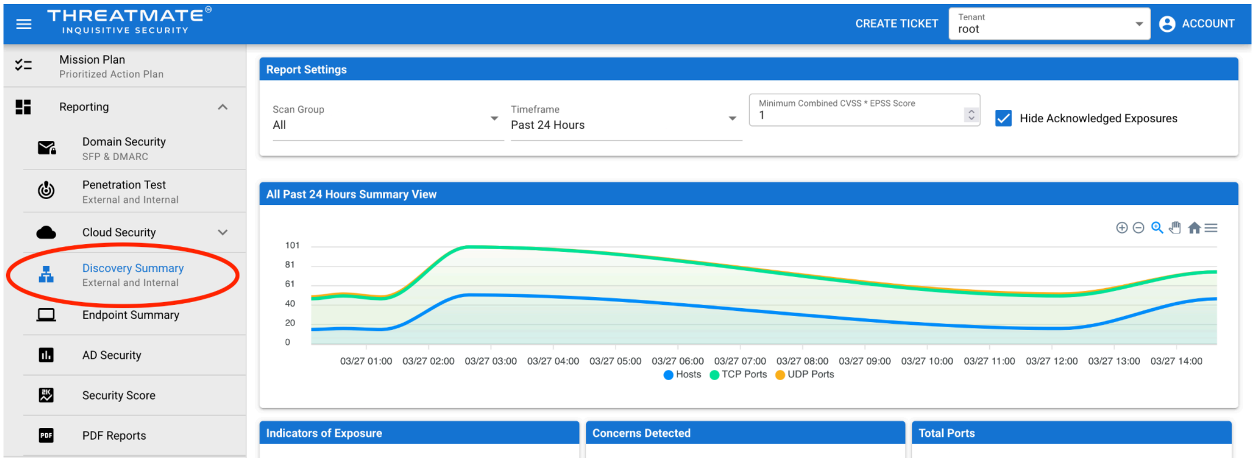


☑ Only Show Items with Score >= 0.1

Discovery and Endpoint Applications

Rank	Type	Description	Maximum Combined Score ↓	Number of Exposures	Number of Instances
#1		Update glibc	9.75	91	4
#2		Update bash	9.75	13	9
#3		Update Apache Tomcat	9.54	41	1
#4		Update Google Chrome.app	8.97	3260	1
#5		Update iCloud.app	8.40	229	1
#6		Update iTunes.app	8.40	674	1
#7		Update vsftpd	8.25	2	1

Additionally the discovery results can be viewed in **Reporting -> Discovery Summary**:



Tenant: root

Report Settings

Scan Group: All

Timeframe: Past 24 Hours

Minimum Combined CVSS * EPSS Score: 1

☑ Hide Acknowledged Exposures

All Past 24 Hours Summary View

Refer to the External Scan Results section for more information about the Discovery Summary dashboard.

The scan group dropdown will help you filter on the actual scan group results to display. By default it is set to **All** which shows the results from all scan groups combined.

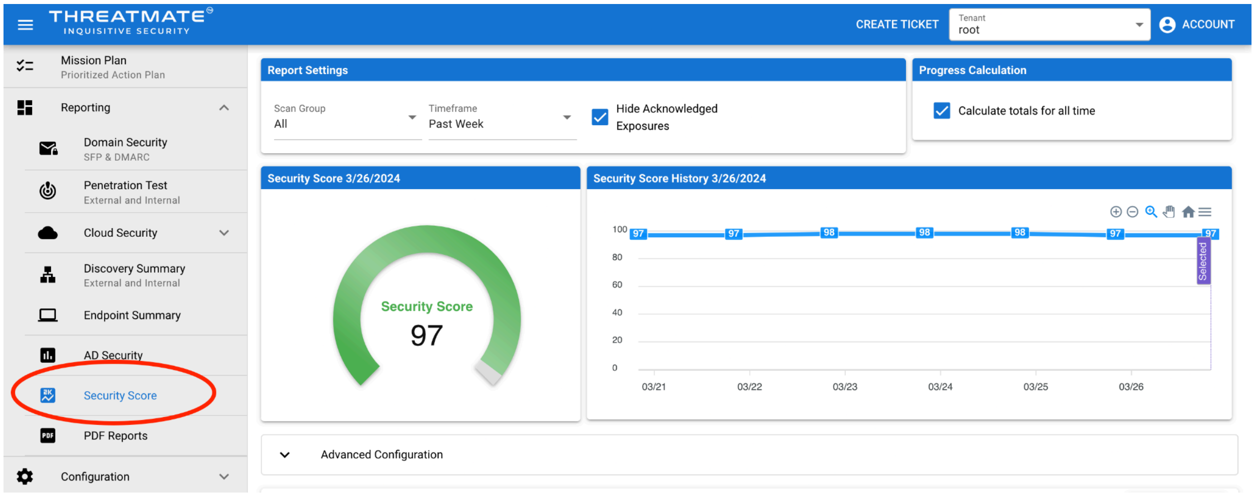
The **Timeframe** option can be used to see historical results.

The **Minimum Combined Score** selection can be used to filter exposures. By default it is set to 1 which filters all exposures with **Combined Score** less than 1. The combined score is computed by multiplying the CVSS score and the EPSS score for a vulnerability. The EPSS score is the probability of exploitation of the vulnerability in the next 30 days. The higher the EPSS score the more likely it is that the vulnerability will be exploited.

The **Hide Acknowledged Exposures** checkbox can be used to show/hide acknowledged exposures in the dashboard.

Security Score

Once you have discovery results you can also see your Security Score in the **Reporting -> Security Score** dashboard. It is computed daily and can be used to track progress and shows the top items that contribute to the security score:



Tenant: root

Scan Group: All

Timeframe: Past Week

☑ Hide Acknowledged Exposures

☑ Calculate totals for all time

Dealing with scan issues

We highly recommend deploying a discovery agent per LAN and not scanning across a router/firewall/VPN boundary. This will ensure the best scan performance with the least amount of network impact.

If a local LAN deployment is not possible and you are experiencing issues with the scans such as network congestion and devices rebooting during scans then we need to adjust the settings for the scans. We can do the following configuration changes:

- decrease the scan frequency; by default the discovery scans are performed every 12 hours with a rate limit per IP which means the scan will take about 6 hours to complete. You can slow the scan even further and make it take even longer depending on your available hardware.
- decrease the concurrent connections from 50 TCP and UDP to 10 TCP and UDP or even 5 - this can make the scan even slower than the provided scan frequency
- disable UDP scans completely - UDP scans are disabled by default, but if you have enabled them you might want to reconsider it. UDP scans are a lot less efficient than TCP scans and require more resources and are slower to complete. Disabling them will increase the performance of the scans without significant loss of data.

For devices that we know they don’t like to be scanned we can do the following:

- disable service discovery which will eliminate sending probes to the device. This will allow us to still discover the open ports on a device but we’ll lose any vulnerability information
- excluding a particular port from being scanned or excluding a port from being sent probes - if we find out that a particular port is the issue we can exclude it. For example

most printers that receive data on ports 9000 to 9012 will print the data they receive. Since our probes are binary data the printers will end up printing garbage. This is why we exclude ports 9000-9012 from being scanned.

- exclude an IP from being scanned - this will not scan an IP and we won't know any information about the device

Known scan Issues

Some devices have issues when they are scanned by the discovery agent. If you have any of them you should consider testing them first and excluding them from the scan:

- Some wireless access points - we've observed some wireless access points reboot when we scan them with the discovery agent. If this is the case for you please exclude the IPs of the access points from the scan
- Some VDI gateways - we've observed some VDI gateways disconnect connected users when scanned by the discovery agent. If this is the case you can exclude the IPs of your VDI gateways from the scan.

ThreatMate Endpoint Agent

The ThreatMate endpoint agent continuously monitors and gathers data from endpoints. The ThreatMate platform analyzes the data for security exposures. The ThreatMate endpoint agent collects data to support the following analysis:

- Asset information
- Vulnerabilities in third party applications
- Vulnerabilities in the operating system
- Compliance checks
- Threat hunting and suspicious activities

For more information check this document: ThreatMate Endpoint Agent Overview.

The deployment instructions depend on your operating system. The general requirements are:

- 1 CPUs
- 50MB of RAM

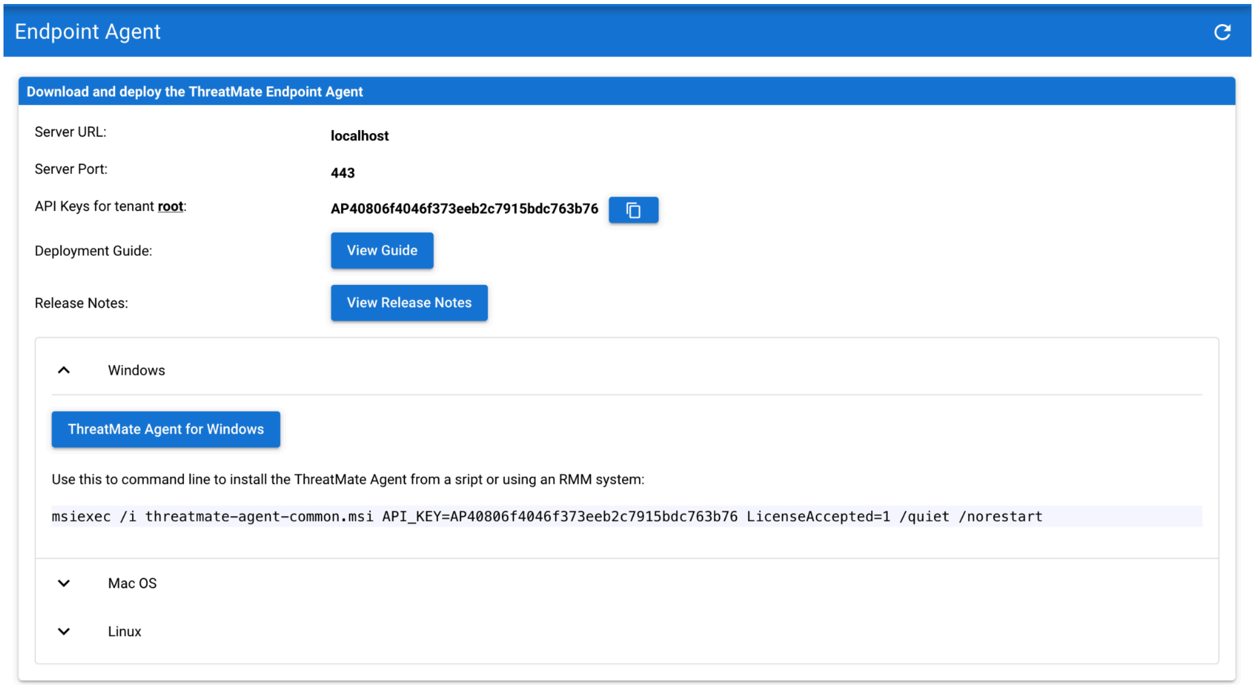
The ThreatMate Agent runs continuously and instruments the device 24x7. It gathers information on running processes, outbound connections, installed applications and more. All the data is streamed encrypted to the ThreatMate cloud infrastructure using HTTPS.

Installing the ThreatMate Agent

In order to download the agent you need to navigate to the download page on the left side menu in the web dashboard: Endpoints -> ThreatMate Agent

Windows

In order to deploy the agent on a Windows device you need to click on the Windows drop-down and then download the Windows MSI package for the agent: **threatmate-agent-common.msi**



Endpoint Agent
Download and deploy the ThreatMate Endpoint Agent

Server URL:	**localhost**
Server Port:	**443**
API Keys for tenant **root**:	**AP40806f4046f373eeb2c7915bdc763b76**
Deployment Guide:	View Guide
Release Notes:	View Release Notes

Windows
ThreatMate Agent for Windows

Use this to command line to install the ThreatMate Agent from a sript or using an RMM system:

```
msiexec /i threatmate-agent-common.msi API_KEY=AP40806f4046f373eeb2c7915bdc763b76 LicenseAccepted=1 /quiet /norestart
```

RMM Deployment

ConnectWise Automate

Microsoft Intune

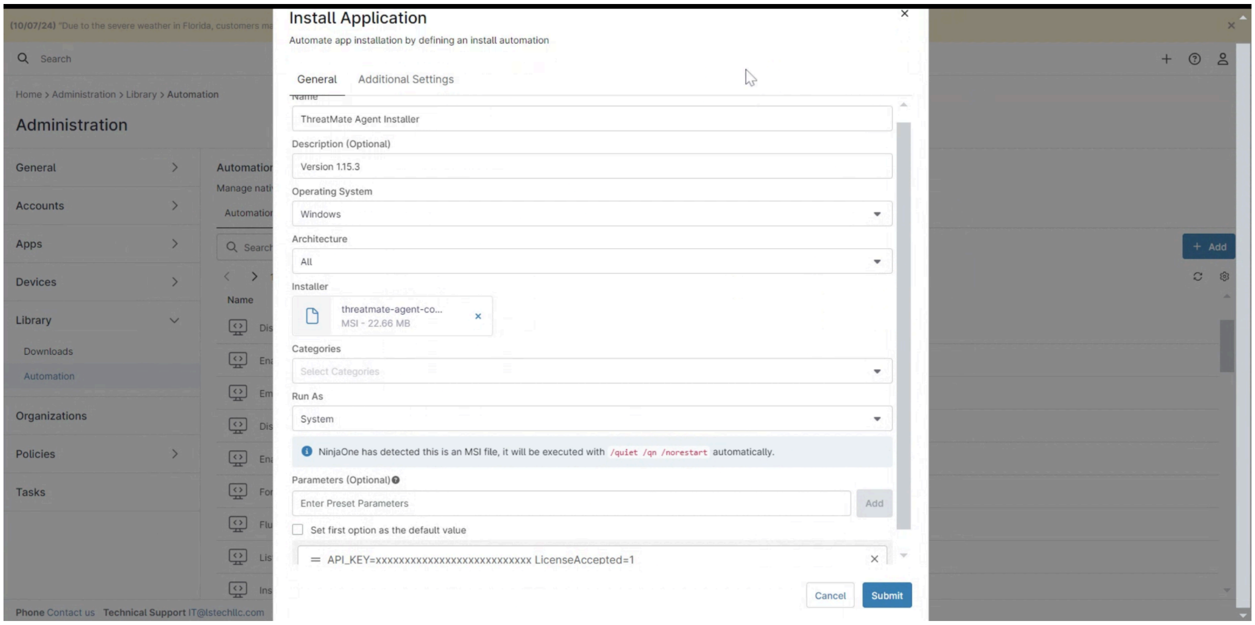
M365 Intune deployment steps:

1. Launch Intune (https://intune.microsoft.com)
2. Click into Apps
3. Select Windows

4. Click Add
5. App Type: Line-of-business app
6. Select the package file (threatmate MSI file) – Command-Line Argument is required
    1. Publisher: Threatmate
    2. Command-line Arguments: API_KEY=KEYHERE LicenseAccepted=1 /quiet /norestart
    3. Any additional information as required
7. Select Assignments
    1. Recommended: Required – Add All Users
8. Review and Create > Select Create

Deployment may take some time as devices re-check into Intune.

NinjaOne



Install Application

Automate app installation by defining an install automation

Name: ThreatMate Agent Installer

Description (Optional): Version 1.15.3

Operating System: Windows

Architecture: All

Installer: threatmate-agent-co... MSI - 22.66 MB

Categories: Select Categories

Run As: System

NinjaOne has detected this is an MSI file, it will be executed with `/quiet /qn /norestart` automatically.

Parameters (Optional): Enter Preset Parameters Add

□ Set first option as the default value

API_KEY=xxxxxxxxxxxxxxxxxxxxxxxxxxx LicenseAccepted=1

Manual Agent Configuration

If you need to tweak the agent configuration there are settings you can provide. Normally this is not needed since the agent is pre-configured for your cloud instance. The agent is installed in **C:\Program Files\threatmate-agent\**

In order to configure the agent to run you need to open the **config.env** file and edit it.

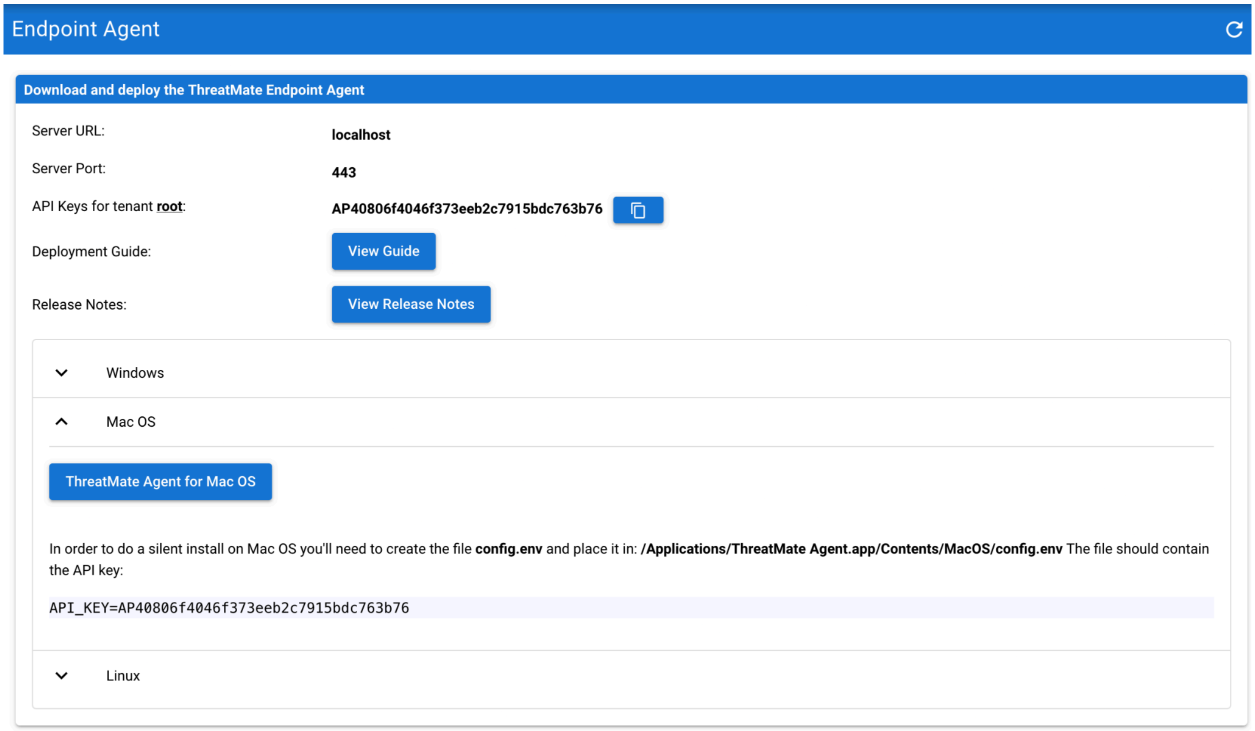
Agent Configuration Options

- `OSQUERY_SOCKET`: This specifies where to find the osquery socket. You normally don't need to change this default value.
- `API_KEY:` specify the API key for the right tenant. The API key is used to determine the destination tenant. You can get the API key from the Endpoint Agent download page in the dashboard.

After configuring the running parameters you restart the threatmate-agent from the system services.

Mac OS

In order to deploy the agent on Mac OS X you need to click on the Mac OS drop-down and then run the agent's Mac OS X package installer.



Endpoint Agent

Download and deploy the ThreatMate Endpoint Agent

Server URL: **localhost**

Server Port: **443**

API Keys for tenant **root**: **AP40806f4046f373eeb2c7915bdc763b76**

Deployment Guide: View Guide

Release Notes: View Release Notes

In order to do a silent install on Mac OS you'll need to create the file **config.env** and place it in: **/Applications/ThreatMate Agent.app/Contents/MacOS/config.env** The file should contain the API key:

```
API_KEY=AP40806f4046f373eeb2c7915bdc763b76
```

If you need to configure the agent manually, please follow the steps in [Agent Configuration Options]() for more information on the different configuration options.

After configuring the running parameters you can use launchctl to restart the com.threatmate.agent.

Silent install

In order to enable the silent install you need to create a file called **config.env** in agent installation directory which will not exist the first time you are installing the agent. So you'll need to create it:

```
mkdir -p /Applications/ThreatMate\ Agent.app/Contents/MacOS/
echo “API_KEY=ABCD1234” >> /Applications/ThreatMate\
Agent.app/Contents/MacOS/config.env
```

The contents of config.env file should just contain the API key:

```
API_KEY=1234567890
```

Then you can use this command to run the installer in silent mode:

```
sudo installer -pkg threatmate-agent-common.pkg -target /
```

The installation from the command line should look like this:

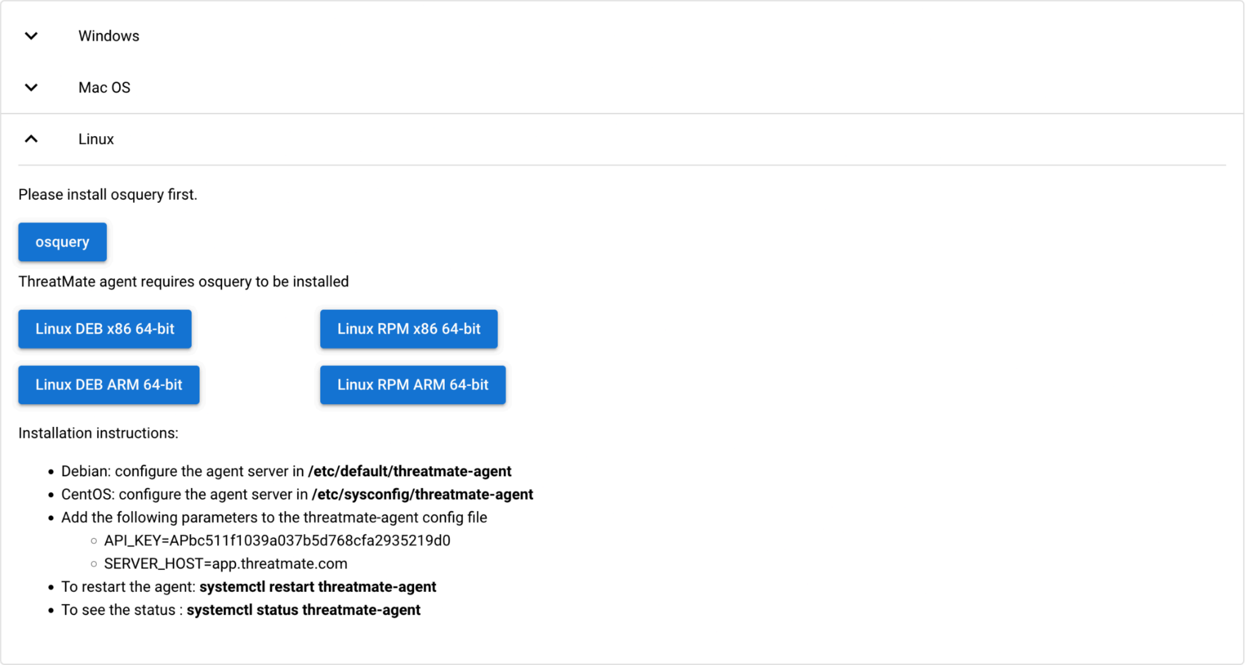
```
sudo installer -pkg threatmate-agent-common.pkg  -target /
Password:
installer: Package name is ThreatMate Agent
installer: Upgrading at base path /
installer: The upgrade was successful.
```

It should not prompt for API key. The newest version is available on the dashboard or on this URL:
https://storage.googleapis.com/agent-binaries/threatmate-agent-common.pkg

If you are using JAMF you should be able to first copy the **config.env** file and then proceed with regular pkg installation.

Linux

In order to deploy the agent on Linux you need to click on the Linux drop-down. First, you need to install osquery for your Linux distribution. You can choose between the DEB and RPM packages. The osquery download web page has other packages as well. Once you have osquery installed you can download either the DEB or RPM package of the endpoint agent.



Please install osquery first.

ThreatMate agent requires osquery to be installed

Installation instructions:

- Debian: configure the agent server in **/etc/default/threatmate-agent**
- CentOS: configure the agent server in **/etc/sysconfig/threatmate-agent**
- Add the following parameters to the threatmate-agent config file
    - API_KEY=APbc511f1039a037b5d768cfa2935219d0
    - SERVER_HOST=app.threatmate.com
- To restart the agent: **systemctl restart threatmate-agent**
- To see the status : **systemctl status threatmate-agent**

The agent deb package supports Ubuntu > 14.04. Here are the steps to deploy on Debian or Ubuntu Linux:

1. Install the agent deb package using dpkg -i https://storage.googleapis.com/agent-binaries/threatmate-agent_amd64.deb

After installation you'll need to add your Server Instance URL and API key in **/etc/default/threatmate-agent** file and restart the agent service afterwards:

```
API_KEY=XXXXXXXXXXXXXXXX
```

On CentOS the configuration file is located in **/etc/sysconfig/threatmate-agent**.

You can copy the Server Instance URL from the dashboard. Afterwards you can restart the threatmate-agent:

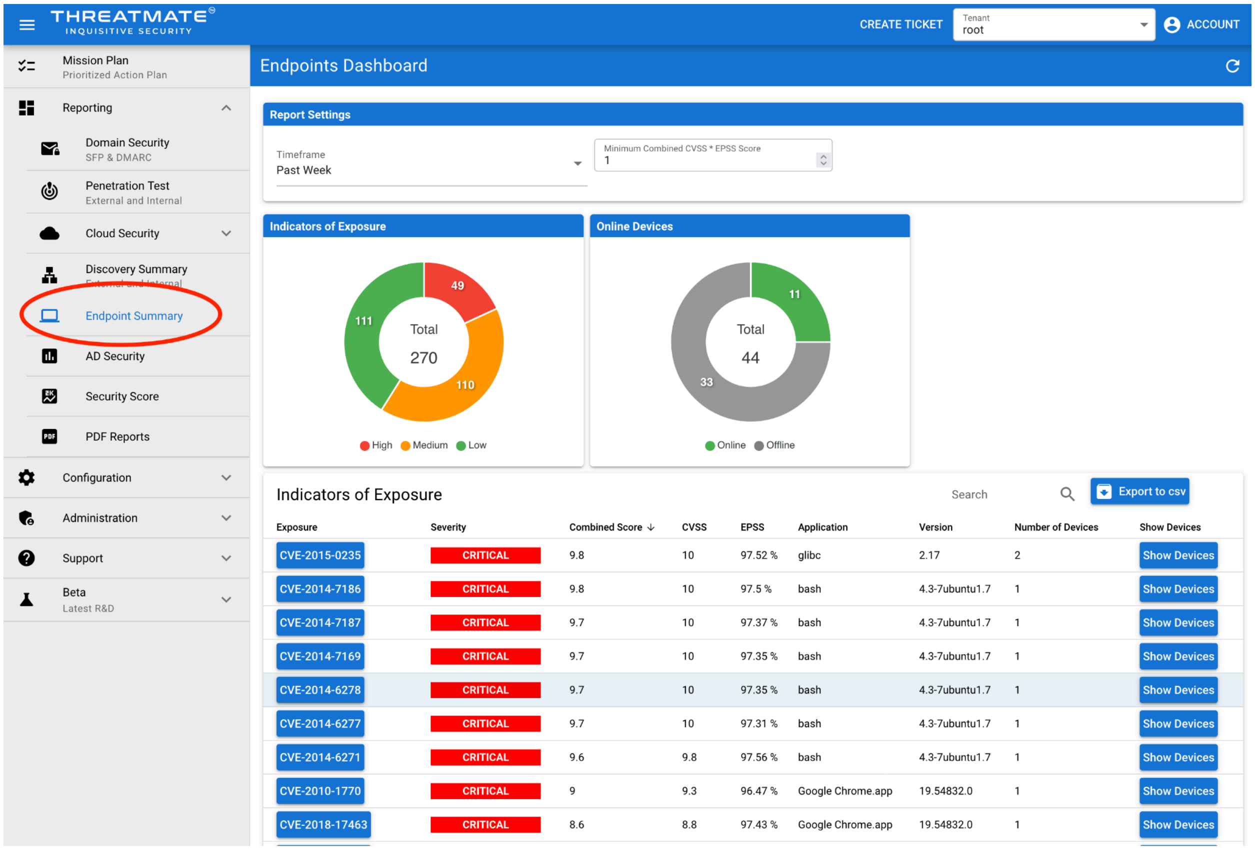
systemctl restart threatmate-agent
systemctl status threatmate-agent

The journalctl can be used to troubleshoot the agent:

journalctl -u threatmate-agent

Agent Results

To see the agent results you can navigate to **Reporting -> Endpoint Summary:**



Tenant: root

Endpoints Dashboard

Report Settings

Timeframe: Past Week

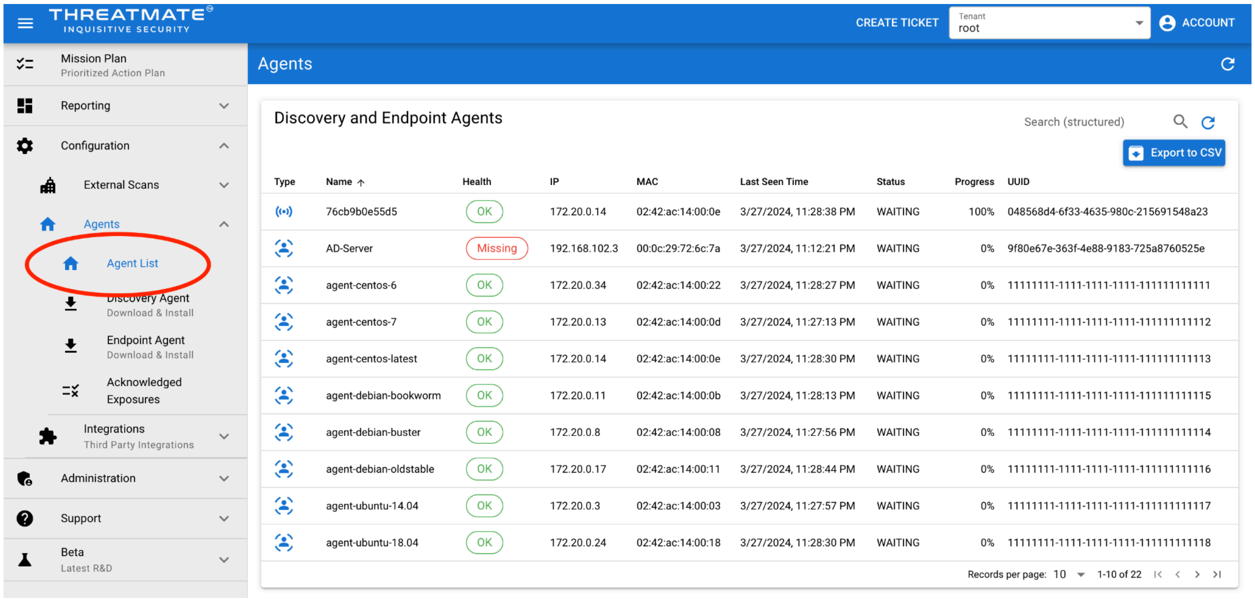
Minimum Combined CVSS * EPSS Score: 1

Indicators of Exposure

Exposure	Severity	Combined Score ↓	CVSS	EPSS	Application	Version	Number of Devices	Show Devices
CVE-2015-0235	CRITICAL	9.8	10	97.52 %	glibc	2.17	2	Show Devices
CVE-2014-7186	CRITICAL	9.8	10	97.5 %	bash	4.3-7ubuntu1.7	1	Show Devices
CVE-2014-7187	CRITICAL	9.7	10	97.37 %	bash	4.3-7ubuntu1.7	1	Show Devices
CVE-2014-7169	CRITICAL	9.7	10	97.35 %	bash	4.3-7ubuntu1.7	1	Show Devices
CVE-2014-6278	CRITICAL	9.7	10	97.35 %	bash	4.3-7ubuntu1.7	1	Show Devices
CVE-2014-6277	CRITICAL	9.7	10	97.31 %	bash	4.3-7ubuntu1.7	1	Show Devices
CVE-2014-6271	CRITICAL	9.6	9.8	97.56 %	bash	4.3-7ubuntu1.7	1	Show Devices
CVE-2010-1770	CRITICAL	9	9.3	96.47 %	Google Chrome.app	19.54832.0	1	Show Devices
CVE-2018-17463	CRITICAL	8.6	8.8	97.43 %	Google Chrome.app	19.54832.0	1	Show Devices

Agent Health

You can see both discovery and endpoint agent status in the **Configuration -> Agents -> Agent List** page.



Discovery and Endpoint Agents

Type	Name ↑	Health	IP	MAC	Last Seen Time	Status	Progress	UUID
((•))	76cb9b0e55d5	OK	172.20.0.14	02:42:ac:14:00:0e	3/27/2024, 11:28:38 PM	WAITING	100%	048568d4-6f33-4635-980c-215691548a23
👤	AD-Server	Missing	192.168.102.3	00:0c:29:72:6c:7a	3/27/2024, 11:12:21 PM	WAITING	0%	9f80e67e-363f-4e88-9183-725a8760525e
👤	agent-centos-6	OK	172.20.0.34	02:42:ac:14:00:22	3/27/2024, 11:28:27 PM	WAITING	0%	11111111-1111-1111-1111-111111111111
👤	agent-centos-7	OK	172.20.0.13	02:42:ac:14:00:0d	3/27/2024, 11:27:13 PM	WAITING	0%	11111111-1111-1111-1111-111111111112
👤	agent-centos-latest	OK	172.20.0.14	02:42:ac:14:00:0e	3/27/2024, 11:28:30 PM	WAITING	0%	11111111-1111-1111-1111-111111111113
👤	agent-debian-bookworm	OK	172.20.0.11	02:42:ac:14:00:0b	3/27/2024, 11:28:13 PM	WAITING	0%	11111111-1111-1111-1111-111111111115
👤	agent-debian-buster	OK	172.20.0.8	02:42:ac:14:00:08	3/27/2024, 11:27:56 PM	WAITING	0%	11111111-1111-1111-1111-111111111114
👤	agent-debian-oldstable	OK	172.20.0.17	02:42:ac:14:00:11	3/27/2024, 11:28:44 PM	WAITING	0%	11111111-1111-1111-1111-111111111116
👤	agent-ubuntu-14.04	OK	172.20.0.3	02:42:ac:14:00:03	3/27/2024, 11:27:57 PM	WAITING	0%	11111111-1111-1111-1111-111111111117
👤	agent-ubuntu-18.04	OK	172.20.0.24	02:42:ac:14:00:18	3/27/2024, 11:28:30 PM	WAITING	0%	11111111-1111-1111-1111-111111111118

Records per page: 10 1-10 of 22

The status is green if the agent was seeing in the past 15 minutes and red otherwise.

Troubleshooting agent problems

Agents can go missing for a variety of reasons.

Agent installation fails

If the agent installation fails with error 1603 it might be due to permission issues. Try creating the target installation directory before the installation to see if that fixes the issue:
C:\Program Files\threatmate-agent\

If the above steps don't work for you we've observed environment variables playing a role in the permissions of the installation. Try the following steps if you are receiving 1603 installation error:

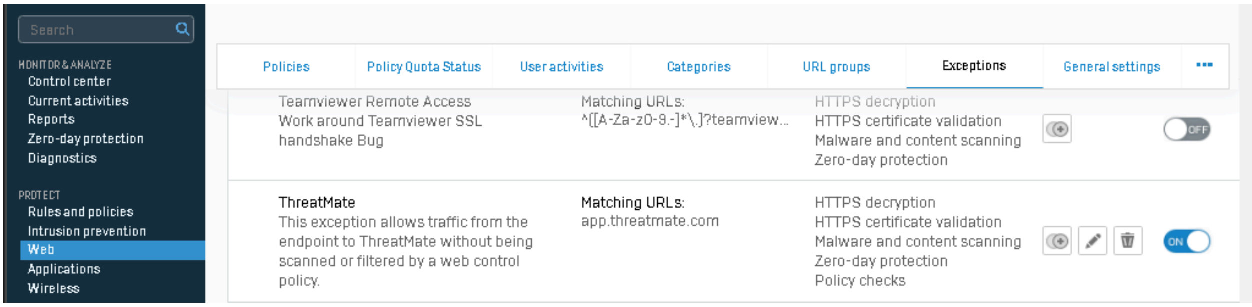
1. Open File Explorer.
2. Right-click This PC and select Properties.
3. Click Advanced system settings.
4. Click the Advanced tab.
5. Click Environment Variables.
6. On the System variables section, click Path.
7. Click Edit.
8. Click New then add this text: C:\Windows\system32
9. Using the 'Move Up' button, move this new entry to the top of the list (I am not certain this is required, but it is what I did).
10. Click OK.
11. Click OK on the next screen, then click OK again on the next screen.

12. Restart the PC. (Required)
13. Open a command prompt and try the ‘net user’ command to verify it worked.
14. Install ThreatMate.

Agent doesn't show up in the Agent List dashboard

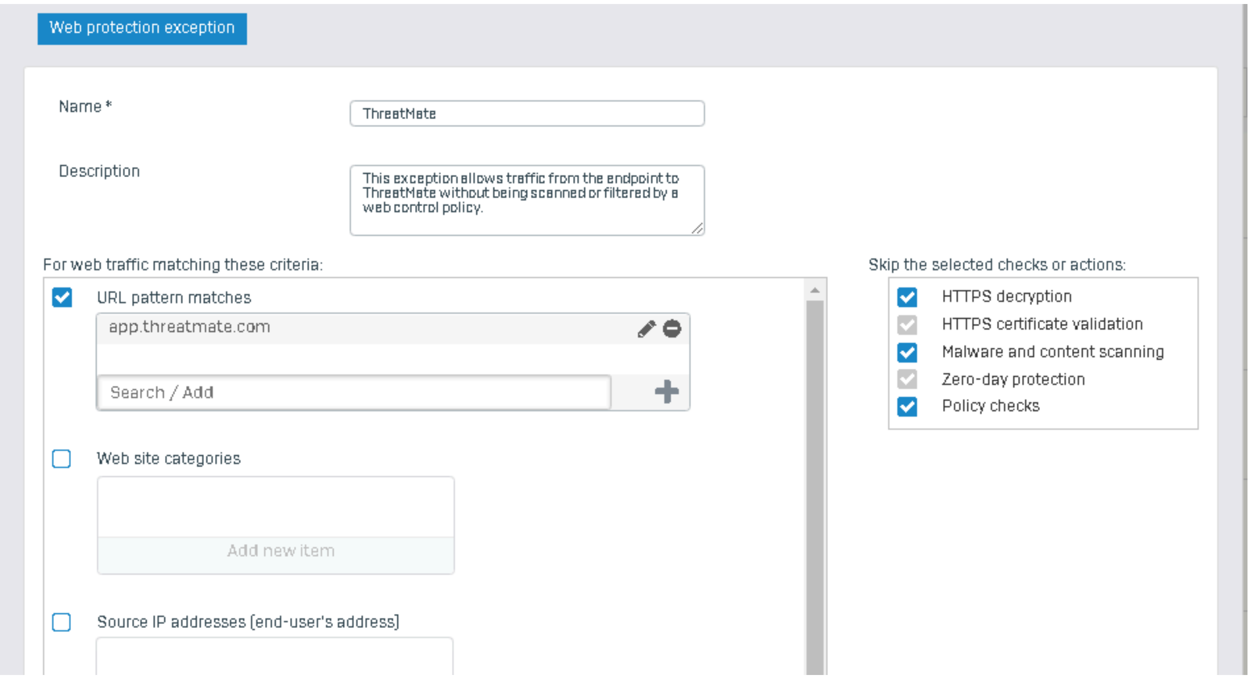
If you tried to install the agent and you’ve verified that you’re using the correct API key but the agent is missing from the Agent List the chances are the agent is being blocked somehow. We’ve observed a Sophos network firewall that does web filtering to block the agent connection to app.threatmate.com. If this is the case you need to add an exception in the firewall security rules to app.threatmate.com. The agent will refuse to connect if the traffic is modified which is an indication of man-in-the-middle attack. Our recommendation is to not block the QUIC protocol and not perform HTTPS decryption of the agent traffic to app.threatmate.com.

Here is an example for the Sophos firewall:



Teamviewer Remote Access
Work around Teamviewer SSL handshake Bug
Matching URLs:
^([A-Za-z0-9.-]*\.)?teamview...
HTTPS decryption
HTTPS certificate validation
Malware and content scanning
Zero-day protection

ThreatMate
This exception allows traffic from the endpoint to ThreatMate without being scanned or filtered by a web control policy.
Matching URLs:
app.threatmate.com
HTTPS decryption
HTTPS certificate validation
Malware and content scanning
Zero-day protection
Policy checks



Name * ThreatMate

Description This exception allows traffic from the endpoint to ThreatMate without being scanned or filtered by a web control policy.

For web traffic matching these criteria:

☑ URL pattern matches
app.threatmate.com

☐ Web site categories

☐ Source IP addresses (end-user's address)

Skip the selected checks or actions:

☑ HTTPS decryption
☑ HTTPS certificate validation
☑ Malware and content scanning
☑ Zero-day protection
☑ Policy checks

The agent goes missing after some time

We’ve observed that when the penetration test runs some anti-virus software can quarantine the agent which will stop it from running. If this is the case please add an exception for the ThreatMate agent.

Zscaler

If Zscaler is installed on the device it can interfere with the HTTPS connection that the discovery and endpoint agents perform. You’ll need to add the ThreatMate agents to the allow list of Zscaler. Otherwise the agent will refuse to connect if the connection is tampered with.

ThreatLocker

The best way to allow the ThreatMate agents is to enable learning mode during the installation of the MSI so that everything can be configured for you without having to manually allow the individual files.

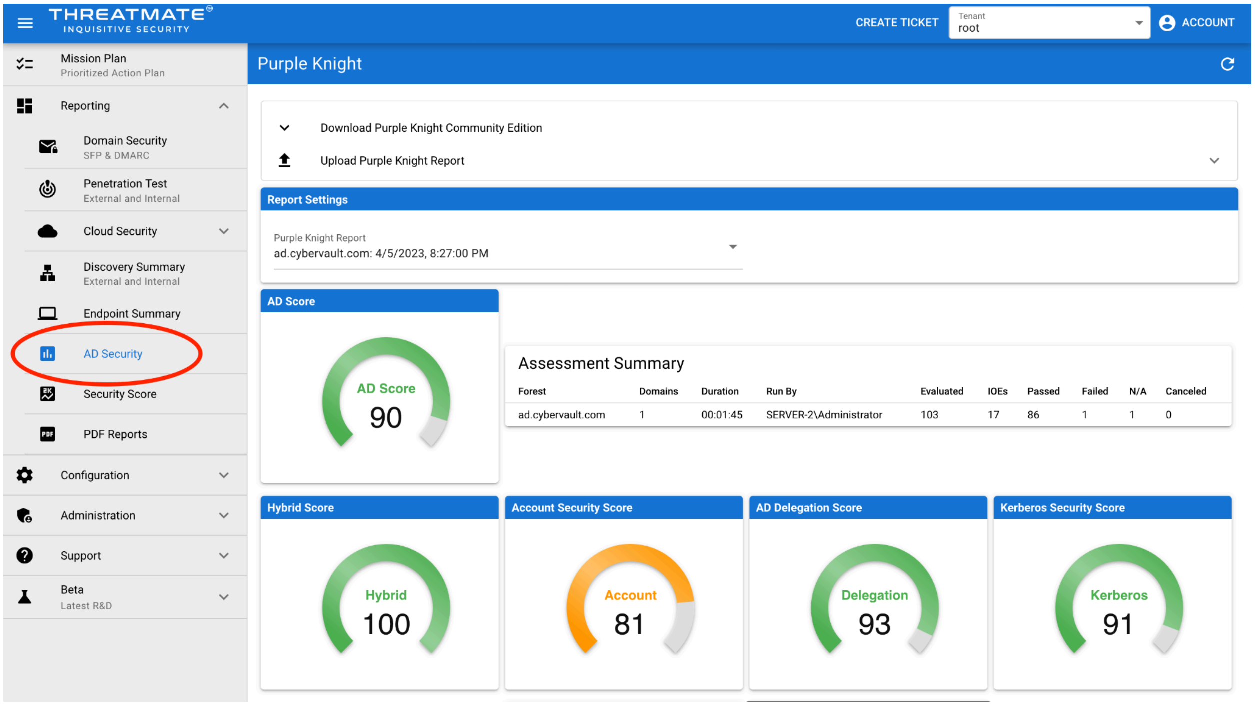
If you want to perform the steps manually you’ll need to allow the following bat scripts to run:
C:\Program Files\threatmate-discovery\run-discovery.bat
C:\Program Files\threatmate-agent\run-agent.bat

Third Party integrations

ThreatMate supports third party integrations that extend the functionality of the platform and helps you integrate it into your existing workflow.

Active Directory Assessment with PurpleKnight

PurpleKnight is a great Active Directory assessment tool. You can find the integration in **Reporting -> AD Security** page. You can download it to your Active Directory server and run the analysis. After the final report is create you can export it to CSV files, zip all the CSV files together and send them to ThreatMate for storage:



Tenant: root

Purple Knight Report: ad.cybervault.com: 4/5/2023, 8:27:00 PM

Assessment Summary

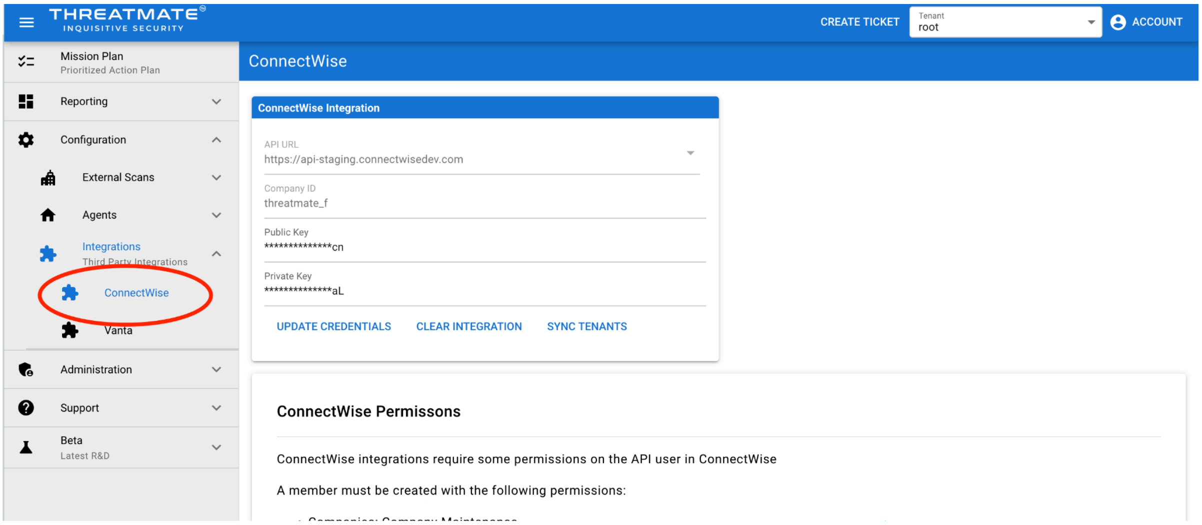
Forest	Domains	Duration	Run By	Evaluated	IOEs	Passed	Failed	N/A	Canceled
ad.cybervault.com	1	00:01:45	SERVER-2\Administrator	103	17	86	1	1	0

ConnectWise Integration

The following features are supported for the ConnectWise integration:

- Tenant synchronization - each ConnectWise company and its sites will be synchronized to ThreatMate
- Company pod integration - in Manage -> Companies there will be a ThreatMate pod that includes the current Mission Plan for the selected company

The ConnectWise integration requires a company and a public and private keys in order to be successful:



Tenant: root

API URL: https://api-staging.connectwisedev.com

Company ID: threatmate_f

Public Key: **************cn

Private Key: **************aL

ConnectWise Permissons

ConnectWise integrations require some permissions on the API user in ConnectWise

A member must be created with the following permissions:

ConnectWise Permissions

ConnectWise integrations require some permissions on the API user in ConnectWise

A member must be created with the following permissions:

- Companies: Company Maintenance
  - Inquire Level: All
    - Used to get a list of companies for syncing
  - Edit Level: All
    - Used to push API keys for authenticating requests for ConnectWise Pod integrations
- Service Desk: Service Tickets
  - Add Level: All
  - Inquire Level: All
    - These permissions are used to create tickets in ConnectWise
- System: Table Setup
  - Add Level: All
  - Edit Level: All
    - Used to create Pod in ConnectWise to show ThreatMate mission plan on company page
  - Inquire Level: All
    - Used to get company types and status for filtering
    - This permission can be customized (optional) to reduce scope to only company related tables

ConnectWise API Keys

To enable ConnectWise to communicate requests to ThreatMate, we need to be able to store API keys associated with your ThreatMate tenants in ConnectWise. For this to happen, a custom field needs to be added to company and site information in ConnectWise.

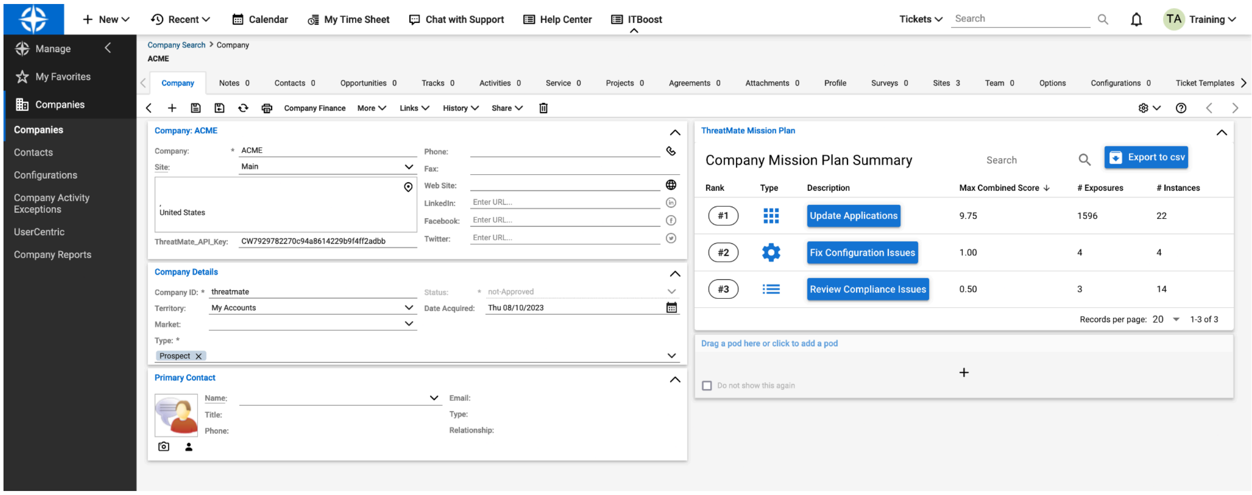
1. Log in to your ConnectWise instance
2. In the menu, navigate to System -> Setup Tables
3. In the setup tables, find or search for the entry:
   - Category: General
   - Table: Custom Fields
4. In the custom fields table, find or search for the entry:
   - Screen: Company
   - Pod Description: Company Overview
5. At the bottom, click the + button to create a new Custom Field:
   - Field Caption: ThreatMate_API_Key
   - Method of Entry: Entry Field
   - The rest of the options are not required to have values for the integration but it may be helpful to add help text
6. Go back to the custom fields tables from step 3

7. In the custom fields table, find or search for the entry:
    - Screen: Site
    - Pod Description: Site Details
8. At the bottom, click the + button to create a new Custom Field:
    - Field Caption: ThreatMate_API_Key
    - Method of Entry: Entry Field
    - The rest of the options are not required to have values for the integration but it may be helpful to add help text

Once a company has been synced, you should be able to add a Pod to the Company screen in ConnectWise to see the ThreatMate mission plan

Pod Integration

The ThreatMate's Mission Plan is visible as a pod in Manage's Companies screen:



Company: ACME

Company: * ACME

Site: Main

,
United States

ThreatMate_API_Key: CW7929782270c94a8614229b9f4ff2adbb

Phone:

Fax:

Web Site:

LinkedIn: Enter URL...

Facebook: Enter URL...

Twitter: Enter URL...

Company Details

Company ID: * threatmate

Territory: My Accounts

Market:

Type: * Prospect

Status: * not-Approved

Date Acquired: Thu 08/10/2023

Primary Contact

Name:

Title:

Phone:

Email:

Type:

Relationship:

ThreatMate Mission Plan

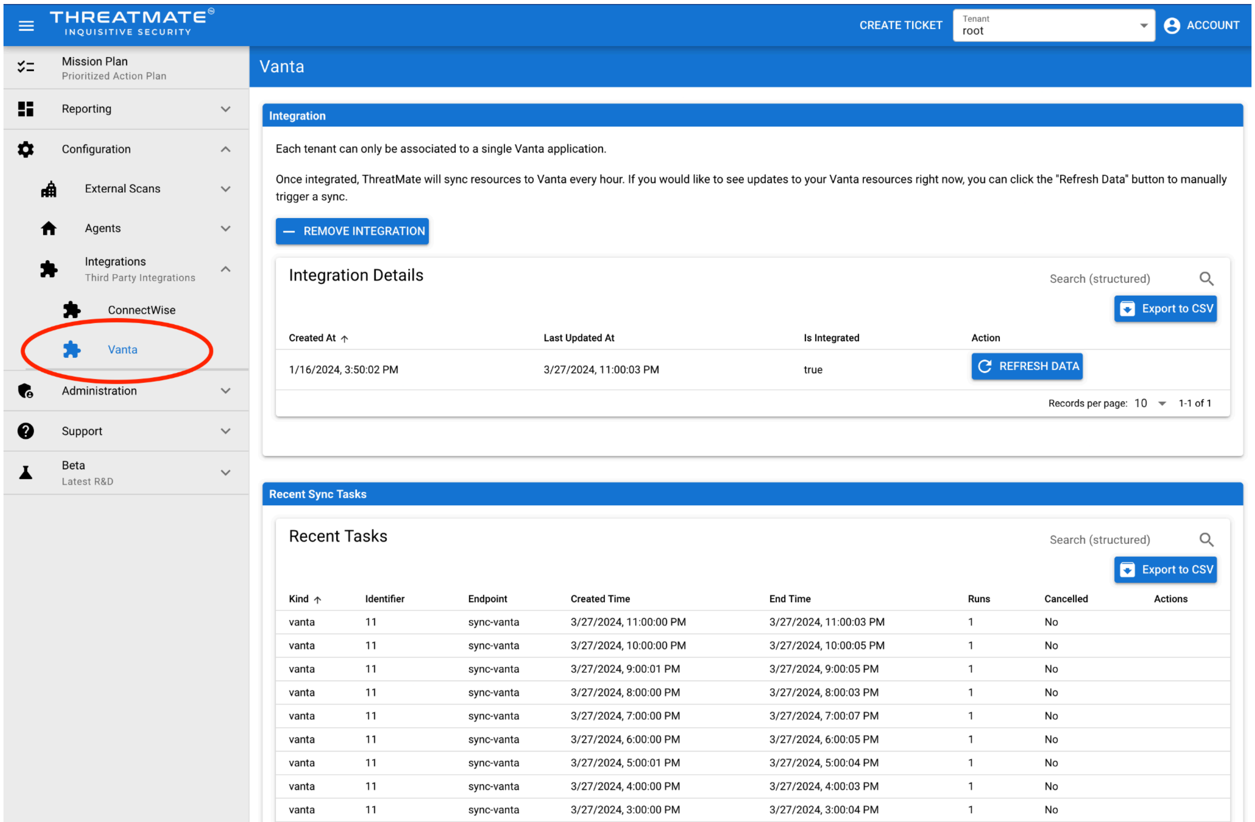
Company Mission Plan Summary

Rank	Type	Description	Max Combined Score ↓	# Exposures	# Instances
#1		Update Applications	9.75	1596	22
#2		Fix Configuration Issues	1.00	4	4
#3		Review Compliance Issues	0.50	3	14

Records per page: 20 1-3 of 3

Vanta Integration

Vanta is a continuous compliance platform. The Vanta integration allows you to send data to Vanta. You can find the integration in **Configuration -> Integrations -> Vanta**:



Vanta

Integration

Each tenant can only be associated to a single Vanta application.

Once integrated, ThreatMate will sync resources to Vanta every hour. If you would like to see updates to your Vanta resources right now, you can click the "Refresh Data" button to manually trigger a sync.

Integration Details

Created At	Last Updated At	Is Integrated	Action
1/16/2024, 3:50:02 PM	3/27/2024, 11:00:03 PM	true	REFRESH DATA

Records per page: 10 1-1 of 1

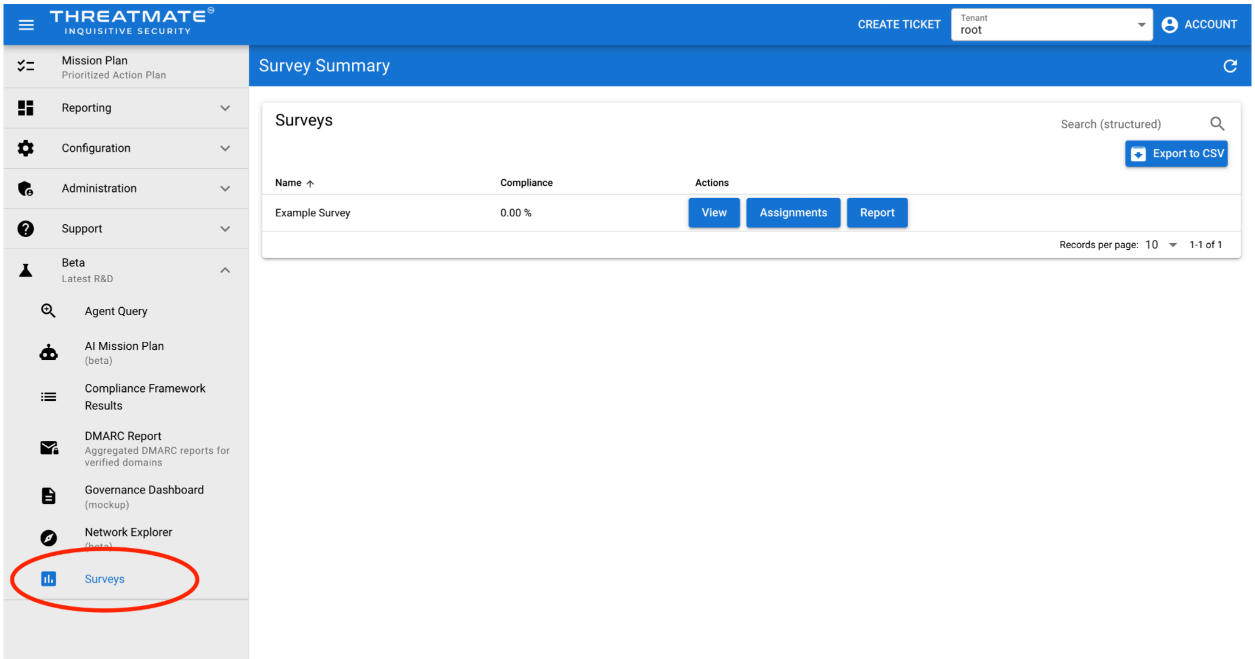
Recent Sync Tasks

Recent Tasks

Kind	Identifier	Endpoint	Created Time	End Time	Runs	Cancelled	Actions
vanta	11	sync-vanta	3/27/2024, 11:00:00 PM	3/27/2024, 11:00:03 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 10:00:00 PM	3/27/2024, 10:00:05 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 9:00:01 PM	3/27/2024, 9:00:05 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 8:00:00 PM	3/27/2024, 8:00:03 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 7:00:00 PM	3/27/2024, 7:00:07 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 6:00:00 PM	3/27/2024, 6:00:05 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 5:00:01 PM	3/27/2024, 5:00:04 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 4:00:00 PM	3/27/2024, 4:00:03 PM	1	No	
vanta	11	sync-vanta	3/27/2024, 3:00:00 PM	3/27/2024, 3:00:04 PM	1	No	

Surveys

Surveys is a new feature which allows you to assign surveys to users in different tenants and see the survey results. This way you can gather and store data across all tenants and then analyze the survey statistics across tenants. The survey feature is currently in Beta and can be found in **Beta -> Surveys**:



Tenant: root

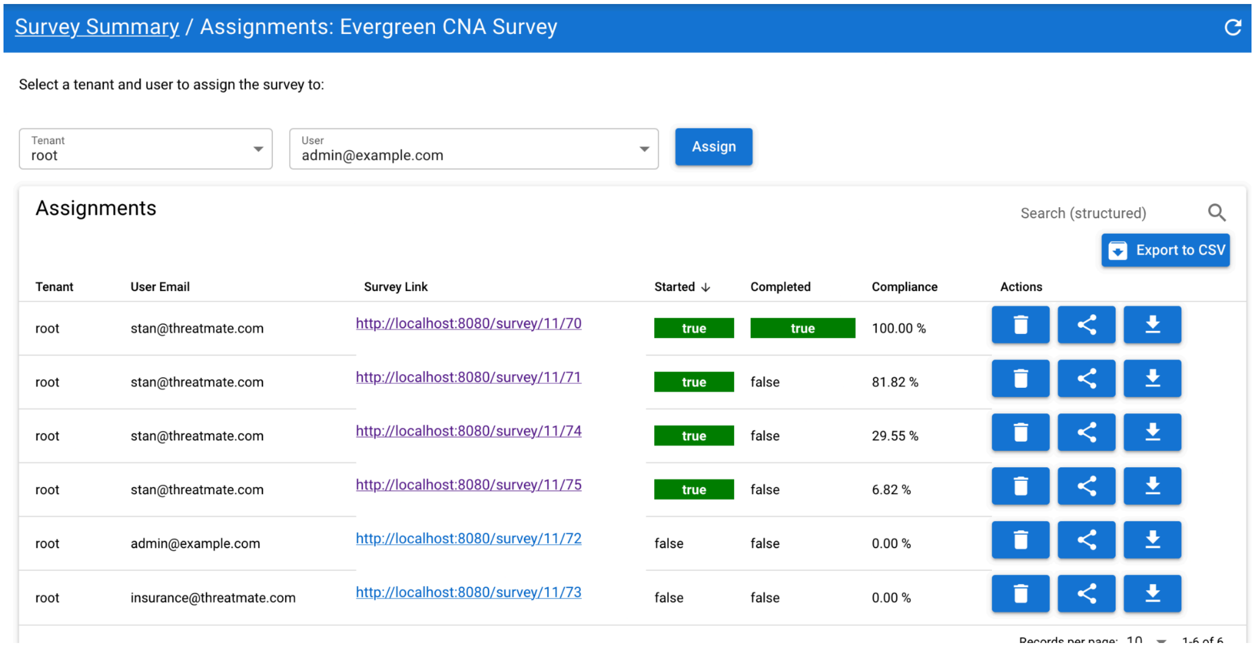
Survey Summary

Surveys

Name	Compliance	Actions
Example Survey	0.00 %	View Assignments Report

Records per page: 10 1-1 of 1

A survey can be assigned if you click on Assignments:



Survey Summary / Assignments: Evergreen CNA Survey

Select a tenant and user to assign the survey to:

Tenant: root

User: admin@example.com

Assign

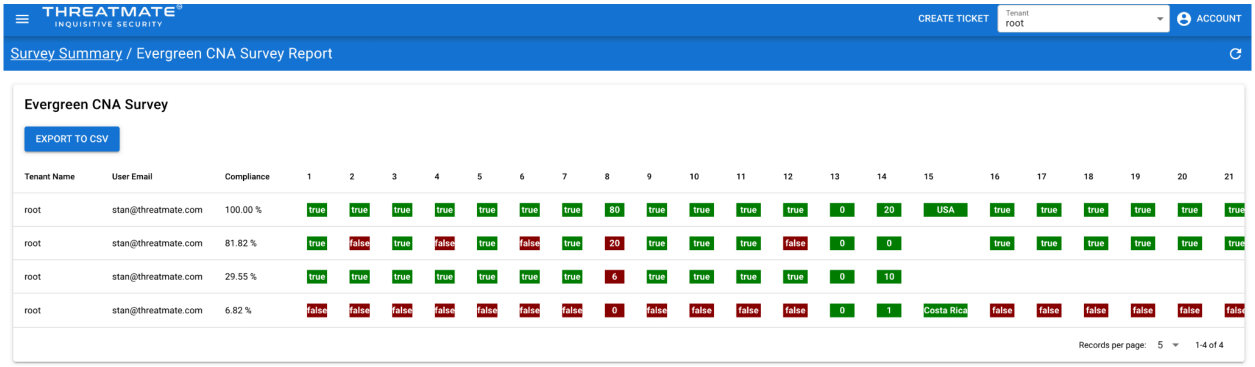
Assignments

Tenant	User Email	Survey Link	Started	Completed	Compliance	Actions
root	stan@threatmate.com	http://localhost:8080/survey/11/70	true	true	100.00 %	
root	stan@threatmate.com	http://localhost:8080/survey/11/71	true	false	81.82 %	
root	stan@threatmate.com	http://localhost:8080/survey/11/74	true	false	29.55 %	
root	stan@threatmate.com	http://localhost:8080/survey/11/75	true	false	6.82 %	
root	admin@example.com	http://localhost:8080/survey/11/72	false	false	0.00 %	
root	insurance@threatmate.com	http://localhost:8080/survey/11/73	false	false	0.00 %	

Records per page: 10 1-6 of 6

On the assignments page you can see who has started the survey, who has completed it and what is the compliance level.

The survey report allows you to see the results across tenants in one view:



Survey Summary / Evergreen CNA Survey Report

Evergreen CNA Survey

EXPORT TO CSV

Tenant Name	User Email	Compliance	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
root	stan@threatmate.com	100.00 %	true	true	true	true	true	true	true	80	true	true	true	true	0	20	USA	true	true	true	true	true	true
root	stan@threatmate.com	81.82 %	true	false	true	false	true	false	true	20	true	true	true	false	0	0		true	true	true	true	true	true
root	stan@threatmate.com	29.55 %	true	true	true	true	true	true	true	6	true	true	true	true	0	10							
root	stan@threatmate.com	6.82 %	false	false	false	false	false	false	false	0	false	false	false	false	0	1	Costa Rica	false	false	false	false	false	false

Records per page: 5 ▾ 1-4 of 4