ThreatModeler
SECURITY STARTS HERE

ThreatModeler™: Existing VPC

Table of Contents

Overview

This setup and deployment guide provide step-by-step instructions for deploying ThreatModeler and integrating it with your AWS environment.

This guide is for users who are planning to threat model their workloads – to be deployed and workloads that are deployed already.

Prerequisites for Deploying ThreatModeler in an AWS Account

The following are prerequisites for launching ThreatModeler through CloudFormation.

- ThreatModeler Support has relevant contact details (email address) of the person in-charge of setup and deployment of ThreatModeler for future references. Please contact support via support@threatmodeler.com.
- License files
  - After you complete the process of subscription to ThreatModeler on AWS Marketplace, please reach out to our support team(support@threatmodeler.com) for the getting the required license files. These are the required files for logging into ThreatModeler initially after the CloudFormation stack for launching ThreatModeler is Complete. ThreatModeler Support will send these files to you via email.
- An Amazon EC2 key pair (for logging into the ThreatModeler Instance) needs to be created prior running the CloudFormation stack.
  - To do this, in the navigation pane of the Amazon EC2 console, under Network & Security, choose Key Pairs, and then click Create Key Pair.
- This solution is being launched in an existing VPC
  - Please make sure each AZ has one public and one private subnet. ThreatModeler requires a selection of two AZ's.
    - Ex: For example, If ThreatModeler is being launched in an existing VPC in the North Virginia Region, that VPC should have a public and private subnet in us-east-1a AZ and public and private subnet in us-east-1b AZ (AZ's us-east-1a and us-east-1b are considered for example purposes).
  - NAT gateway in public subnet and the routes added to private subnet (where ThreatModeler will be launched) route table is required for content updates within the platform.
- ThreatModeler uses ALB to serve traffic with HTTPS listener. To create an HTTPS listener while ALB is being created, we require an ARN of an existing certificate in the Amazon Certificate Manager (ACM) service.
  - For the certificate ARN that is provided, please use the same domain name (for creating record sets in your DNS provider) that was used during the certificate creation for domain name resolution purposes to access ThreatModeler on custom domain name.
  - If your organization doesn't use ACM for certificate management, you could use the "**Import a Certificate**" feature in ACM to **Import** SSL/TLS certificates from third-party issuers into AWS Certificate Manager (ACM) to easily provide ARN for ALB creation with HTTPS creation.

- VPC Peering knowledge is required.
    - Since all the resources (except NAT Gateway) created during this setup are launched in private subnets for secure architecture creation (with access only to these subnets from CIDR you specify during CFN launch).
        - As ThreatModeler is being launched in an existing VPC, we assume VPN connectivity is established for that VPC (for logging and accessing private resources across the enterprise).
    - This product requires an internet connection to deploy properly as it downloads files from an ThreatModeler owned public s3 bucket.

Costs

You are responsible for the cost of AWS services used while running this deployment guide. The AWS CloudFormation templates for this deployment guide include configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

Deployment Options

- Deploy ThreatModeler into an existing VPC.

ThreatModeler Server Standalone setup

Architecture

This setup and deployment guide will help you to deploy ThreatModeler software in your AWS environment.

> • Note The following resources are not shown: associations, route tables, route table entries, security groups, IAM roles, and instance profiles.
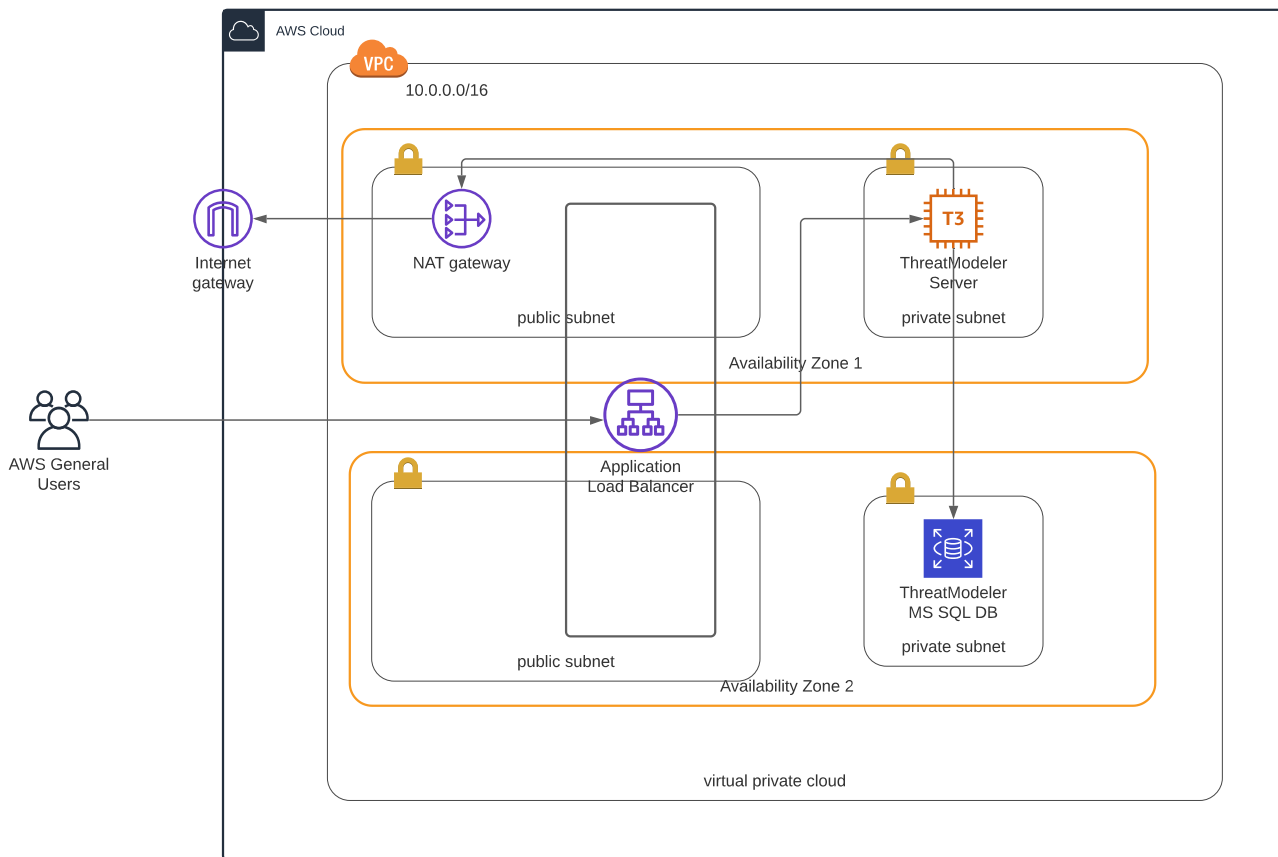
CloudFormation template deploys the following resources:

- S3 bucket – created temporarily to store the RDS database snapshot and then deleted later.
- RDS – will either be created in the same subnet as the ThreatModeler EC2 or in a secondary private subnet based on your parameter selection during CFN launch.
  1. RDS instance
     - Deployed in private subnet.
  2. RDS Option Group (SQLSERVER_BACKUP_RESTORE)
  3. DB Security Group (Port 1433 ingress for MS SQL)
- IAM
  1. EC2 Role with following policies attached:
     - AmazonSSMManagedInstanceCore Managed policy for SSM Agent
     - Read-only access to the account in which it is deployed
     - Access quick start S3 bucket resources
     - Access database snapshot bucket to delete after Restore
     - Access all accounts to assume a Read-only role
  2. RDS role to restore snapshot from S3
- EC2
  1. one EC2 instance will be created with a ThreatModeler-server instance launched in private subnet.
     - ThreatModeler server Deployed from the subscribed AMI
     - Instance type from CFN parameters, EBS Root volume size of 90 GB (gp2)
     - ThreatModeler server Instance Security (ingress ports 22 for SSH, 80 for HTTP respectively
- Application Load Balancer (Internet-Facing)
  1. Deployed in Public Subnet to send traffic to EC2 Instance in Private Subnet.
  2. Deployed with HTTPS for secure communication.

ThreatModeler Deployment

Deploy ThreatModeler into an Existing VPC

1. Before starting deployment process, you would need the S3 URL of the master CFN stack to deploy ThreatModeler.
2. On AWS Marketplace, go to the ThreatModeler listing and click on Usage as follows.

3. For Existing VPC, click on View CloudFormation Template and right click on Download CloudFormation Template -> right click and copy link to copy S3 URL of the master template.
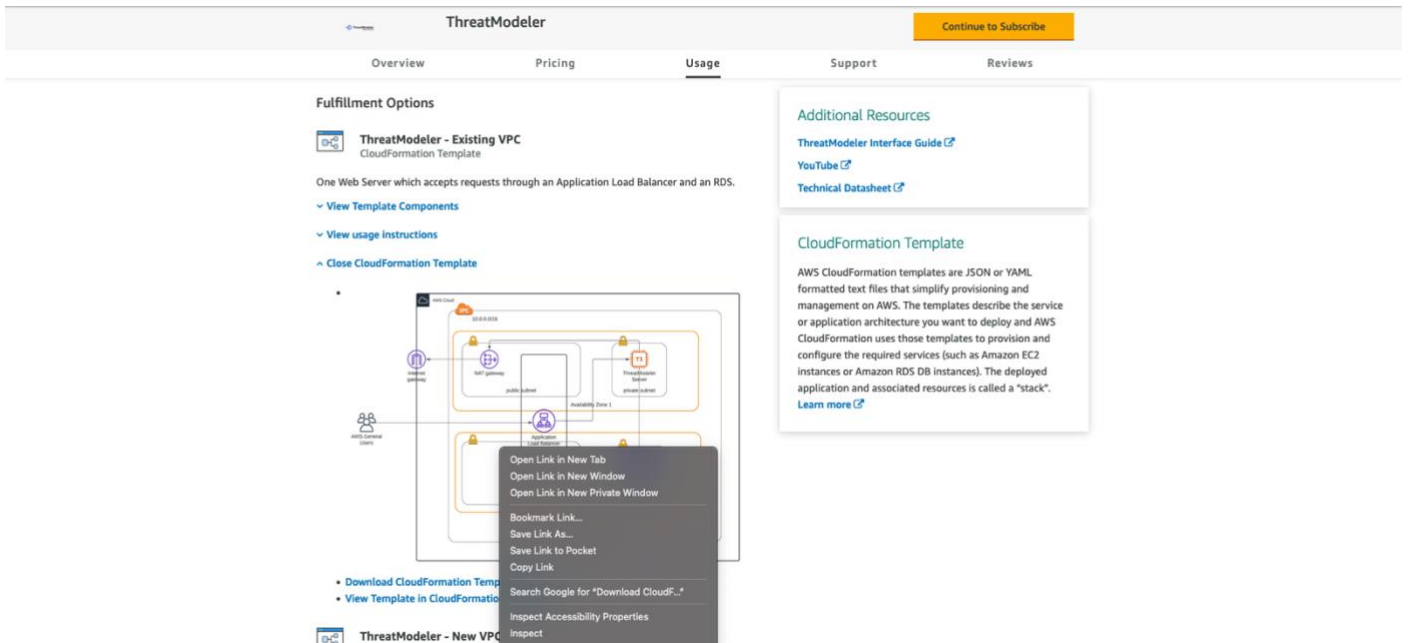
4. After you copied S3 URL, Login to the AWS Console of the AWS account where you want to deploy ThreatModeler. We recommend deploying this CloudFormation stack in Security/Audit account.
5. Select Services → CloudFormation → Stack → Create Stack → With new resources (standard).
6. Log in to the AWS Console of the AWS account where you want to deploy ThreatModeler. We recommend deploying this CloudFormation stack in Security/Audit account.
7. Select Services → CloudFormation → Stacks → Create Stack → With new resources (standard).
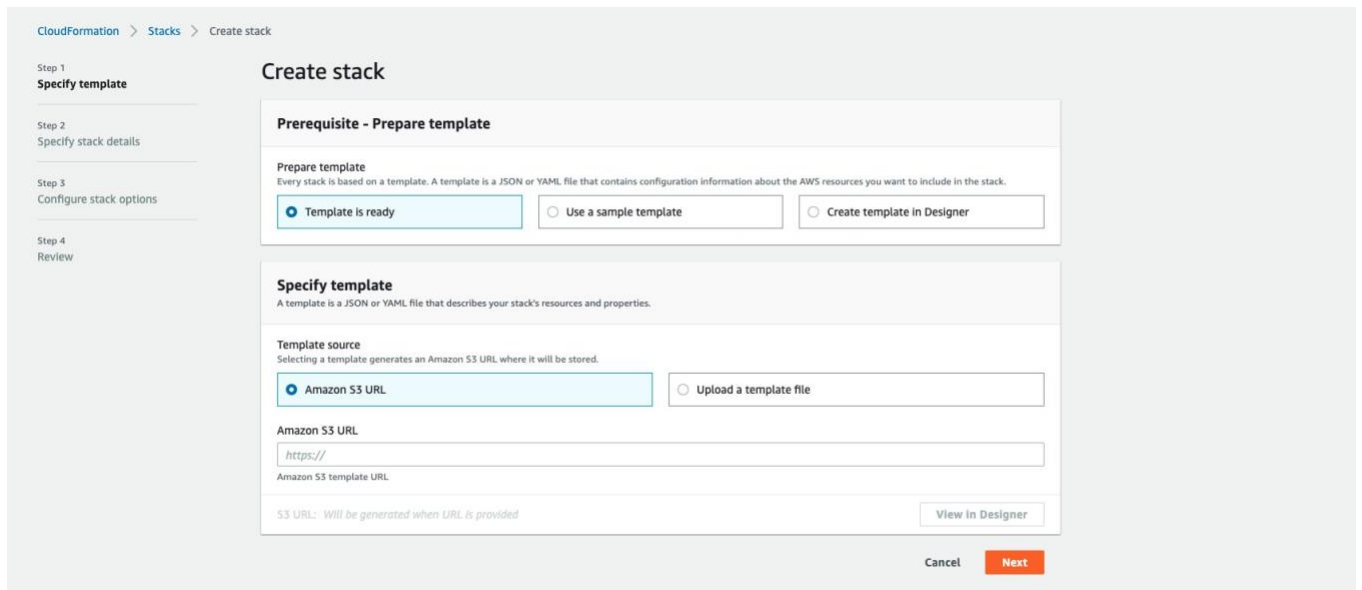
8. In the Specify template field, select Amazon S3 template URL to launch ThreatModeler Application in existing VPC.
9. Paste the S3 template link into the field copied earlier under Amazon S3 URL and click Next.

Step 1
Create stack

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name

Enter a stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

AWS environment and machine configuration

Key pair name
Name of an existing EC2 KeyPair to enable RDP access to the instances.

Select AWS::EC2::KeyPair::KeyName ▼

Availability Zones
List of Availability Zones to use for the subnets in the VPC. Pick exactly 2 AZs.

Select List<AWS::EC2::AvailabilityZone::Name> ▼

Existing VPC ID
The ID that is used to deploy the ThreatModeler server into an existing VPC

Select AWS::EC2::VPC::Id ▼

Private subnet 1 ID
Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter. This subnet route table should also have an entry with NAT Gateway which is created either in subnets with 'Public subnet 1 ID' or 'Public subnet 2 ID'.

Select AWS::EC2::Subnet::Id ▼

Private subnet 2 ID
Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter. This subnet route table should also have an entry with NAT Gateway which is created either in subnets with 'Public subnet 1 ID' or 'Public subnet 2 ID'.

Select AWS::EC2::Subnet::Id ▼

Public subnet 1 ID
Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter.Please make sure a NAT gateway is created at least in one of public subnets you specified in parameters 'Public subnet 1 ID' and 'Public subnet 2 ID'.

Select AWS::EC2::Subnet::Id ▼

Public subnet 2 ID
Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter.Please make sure a NAT gateway is created at least in one of public subnets you specified in parameters 'Public subnet 1 ID' and 'Public subnet 2 ID'.

Select AWS::EC2::Subnet::Id ▼

ThreatModeler RDSAvailabilityZone
Availability Zone to launch Threatmodeler RDS. To deploy RDS instance in same subnet as ThreatModeler EC2, please select AZ where 'Private subnet 1 ID' is created. If not, architecture is deployed among two subnets in two AZ's

Select AWS::EC2::AvailabilityZone::Name ▼

Source CIDR for access
Please set CIDR to x.x.x.x/32 to allow one specific IP address access, 0.0.0.0/0 to allow all IP addresses access, or another CIDR range

Enter String

SSL Certificate ARN (Requires matching DNS name)
The Amazon Resource Name for the existing SSL cert you wish to use; empty for none

Enter String

ThreatModeler Amazon EC2 instance type
Amazon EC2 instance type where ThreatModeler will be installed.

t3.medium ▼

DNS record name
DNS name with which ThreatModeler application will be accessed

Enter String

ThreatModeler Configuration

First Name
Please enter your first name. This product collects first name for creating the first user in our database for your initial login to the ThreatModeler platform.

John

Last Name
Please enter your last name. This product collects last name for creating the first user in our database for your initial login to the ThreatModeler platform.

Smith

Email
Please enter your email address. This product collects email address for creating the first user in our database for your initial login to the ThreatModeler platform.

jsmith@gmail.com

Organization
Name of the Organization

Enter String

RDS Database Master Username
The Master username of the RDS instance for ThreatModeler Database. Eg: awsuser (Must start with a character. 1-16 characters in length)

Enter String

AWS Quick Start configuration

Quick Start S3 bucket name
S3 bucket name for the Quick Start assets. Please leave this as default and don't make any changes.

threatmodeler6-setup-quickstart

Quick Start S3 key prefix
S3 key prefix for the Quick Start assets. Please leave this as default and don't make any changes.

chooseanexistingvpc/quickstart-threatmodeler/

Cancel   Previous   Next

10. Enter a stack name and fill out the rest of the fields. The fields and their descriptions are as follows:

AWS Environment and Machine Configuration

Parameter Label (Name)	Default	Description
Key pair name	Requires Input	Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Availability Zones	Requires Input	List of AZ's to use for the subnets in the VPC. This is based on on the region in which the stack is deployed. Pick exactly 2 AZ's where one public subnet and one private subnet is available in each AZ.
Existing VPC ID	Requires Input	Select one VPC ID where ThreatModeler to be created in.
Private Subnet 1 ID	Requires Input	Existing ID of the private subnet located in first chosen AZ. Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter.
Private Subnet 2 ID	Requires Input	Existing ID of private subnet located in second chosen AZ. Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter.
Public Subnet 1 ID	Requires Input	Existing ID of the public subnet located in first chosen AZ. Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter.
Public Subnet 2 ID	Requires Input	Existing ID of the public subnet located in second chosen AZ. Please select only the subnet ID which is in one of the Availability zones you specified in 'Availability Zones' parameter.
ThreatModeler RDSAvailabilityZone	Requires Input	Availability Zone to launch ThreatModeler RDS.
Source CIDR for access	Requires Input	The CIDR Address from which you will connect to the instance. This is typically, A range of addresses. It can be entered as a single IP address or CIDR range. Add more singular IP Addresses to the EC2 security group post-deployment If necessary.
SSL Certificate ARN	Requires Input	The Amazon Resource Name (ARN) of the existing SSL Certificate you want to use for creating HTTPS listener on ALB. If no SSL Certificate ARN is provided ALB will be created with HTTP listener.
ThreatModeler Amazon EC2 Instance Type	Requires Input	Amazon EC2 Instance type where ThreatModeler will be installed.
DNS Record Name	Requires Input	DNS name with which ThreatModeler application will be accessed.

ThreatModeler Configuration

Parameter Label (Name)	Default	Description
First Name	Requires Input	First name of the customer used for creating the first user on ThreatModeler platform.
Last Name	Requires Input	Last name of the customer used for creating the first user on ThreatModeler platform.
Email	Requires Input	Valid email of the customer which is used as the username for accessing ThreatModeler platform.
Organization	Requires Input	Organization of the customer.
RDS Database Master	Requires Input	Master username for the ThreatModeler database. Must start with Username a character 1-16 characters in length.
RDS Database Master Password	Requires Input	Master password for the ThreatModeler database. Must be between 8-128 printable ASCII characters (excluding /,", & and @)

AWS QuickStart Configuration

Parameter Label (Name)	Default	Description
Quick Start S3 bucket name	threatmodeler6-setup-quickstart	The bucket name used to store quick start assets like scripts and executables. Please leave them as default
Quick Start S3 key prefix	chooseanexistingvpc/quickstart-threatmodeler/	The folder/prefix in the bucket used to store the quick start assets. Please leave them as default.

6. (Optional) Configure stack options.
7. Review the stack details and click on the checkboxes next to the following:

- "I acknowledge that AWS CloudFormation might create IAM resources with custom names."

- "I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND"

- Click on Create Stack.

- The deployment typically takes around 30-40 minutes to complete.
- Take a note of 12-digit AWS Account ID of this account. It will be required for Multi-account setup. This can be done through the following steps:
  - Click your name located on the top right navigation pane. Select "My Account."
  - Your AWS ID is the twelve-digit number located underneath the Account Settings section.

- The deployment is completed once the CloudFormation displays a "CREATE_COMPLETE" message. At this point, click on the stack and click on the "Outputs" tab to view the deployment endpoints and identifiers.

| | Delete | Update | Stack actions ▼ | Create stack ▼ |

| Stack info | Events | Resources | **Outputs** | Parameters | Template | Change sets |

Outputs (3)

🔍 Search outputs

Key ▲	Value ▽	Description ▽	Export name ▽
DBEndpoint		Endpoint Address of database instance	-
InstanceID		EC2 InstanceID of the instance running ThreatModeler Server	-
PrivateIPAddress		Private IP Address of ThreatModeler instance	-

Accessing ThreatModeler (When Deployed into an Existing VPC)

- Note: Assuming VPN connectivity is established (for connecting to instances in private subnet) for the VPC where ThreatModeler instance is created. If not, please create a Bastion-Host in public subnet to access the ThreatModeler instance created in private subnet.
- If VPN connectivity is already established, you need to be on VPN to SSH in to ThreatModeler instance.

1. Go to the browser of your choice and use DNS name (parameter named DNS Record Name) provided during the CloudFormation launch and you should see the following login screen to login to the platform.
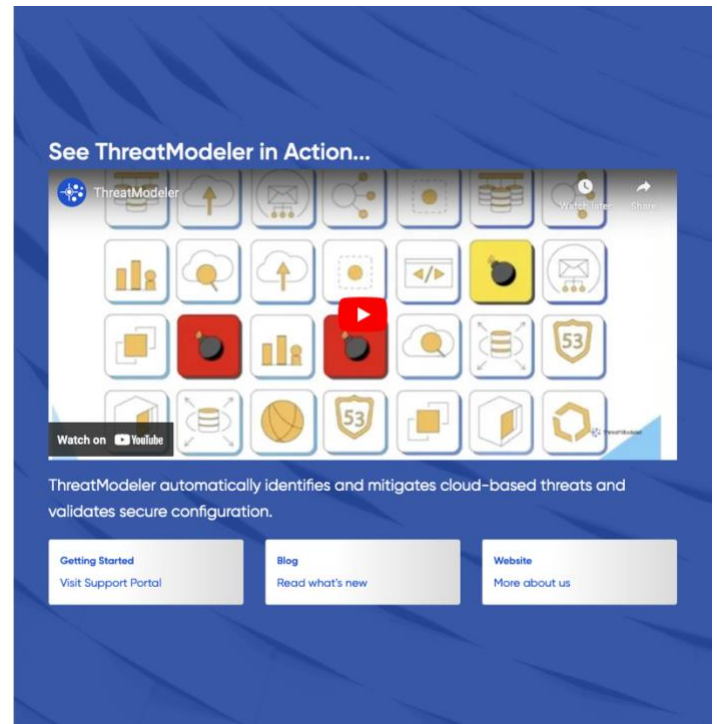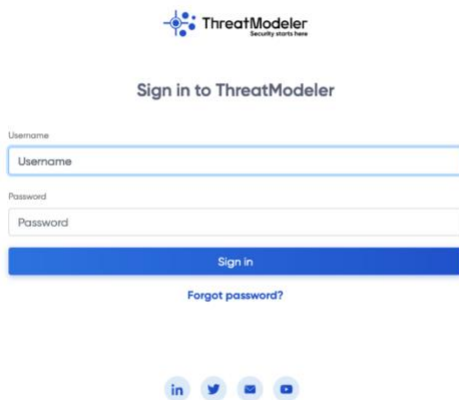
2. Use the email id (parameter named Email) provided during the CloudFormation launch as the Username and Password as "admin@123" (This password is for initial login only and you will have to change it after you login)

3. The first thing you see when you access ThreatModeler is a prompt to upload your License Files.
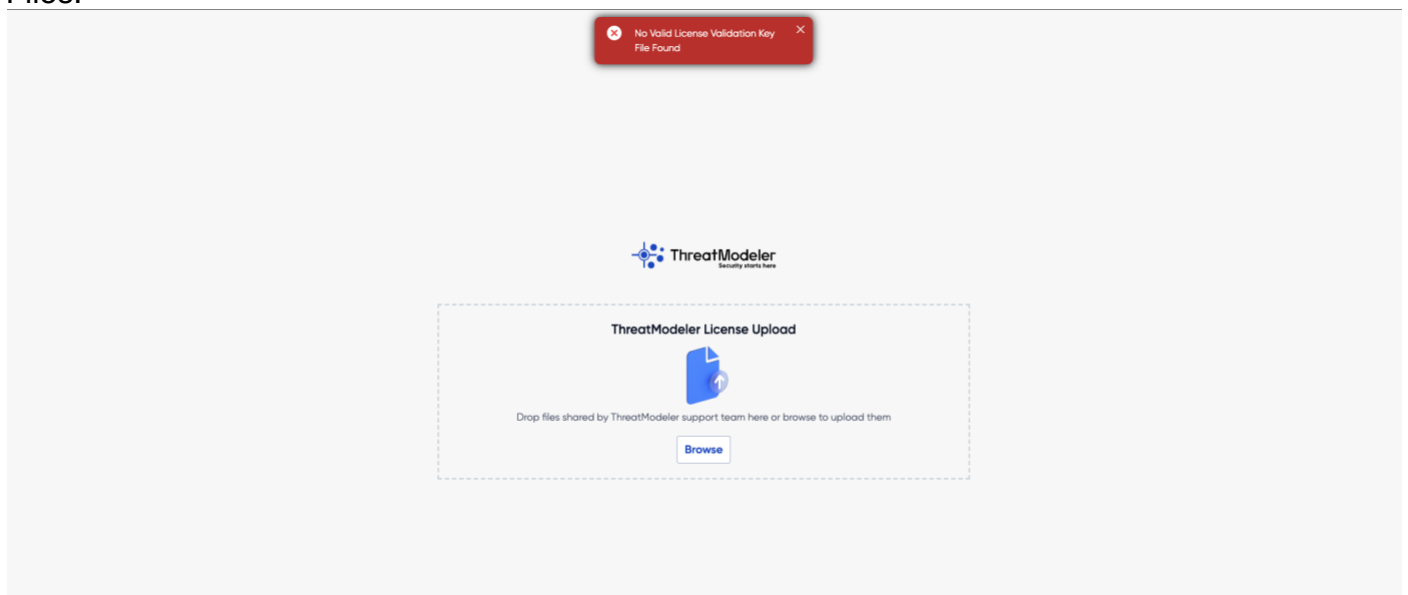
4. Logging into the ThreatModeler platform requires license files to be uploaded. Please open another tab and navigate to your Email inbox. Look for an email from ThreatModeler support (**support@threatmodeler.com**) with the license files.

5. For limited (10 Licenses) licensing model you should have four files to access ThreatModeler:
    a. tm.lic – file used by ThreatModeler
    b. validation key.txt – validates the above .lic file
    c. environmentguid.txt - file used by ThreatModeler
    d. tm_lic_10.txt – file used by ThreatModeler for licensing ThreatModels.

6. As you see the screen below, please click on upload and upload ***tm.lic, environmentguid.txt and validation key.txt*** files. (***tm_lic_10.txt file* has to be uploaded after logging into the ThreatModeler platform**).
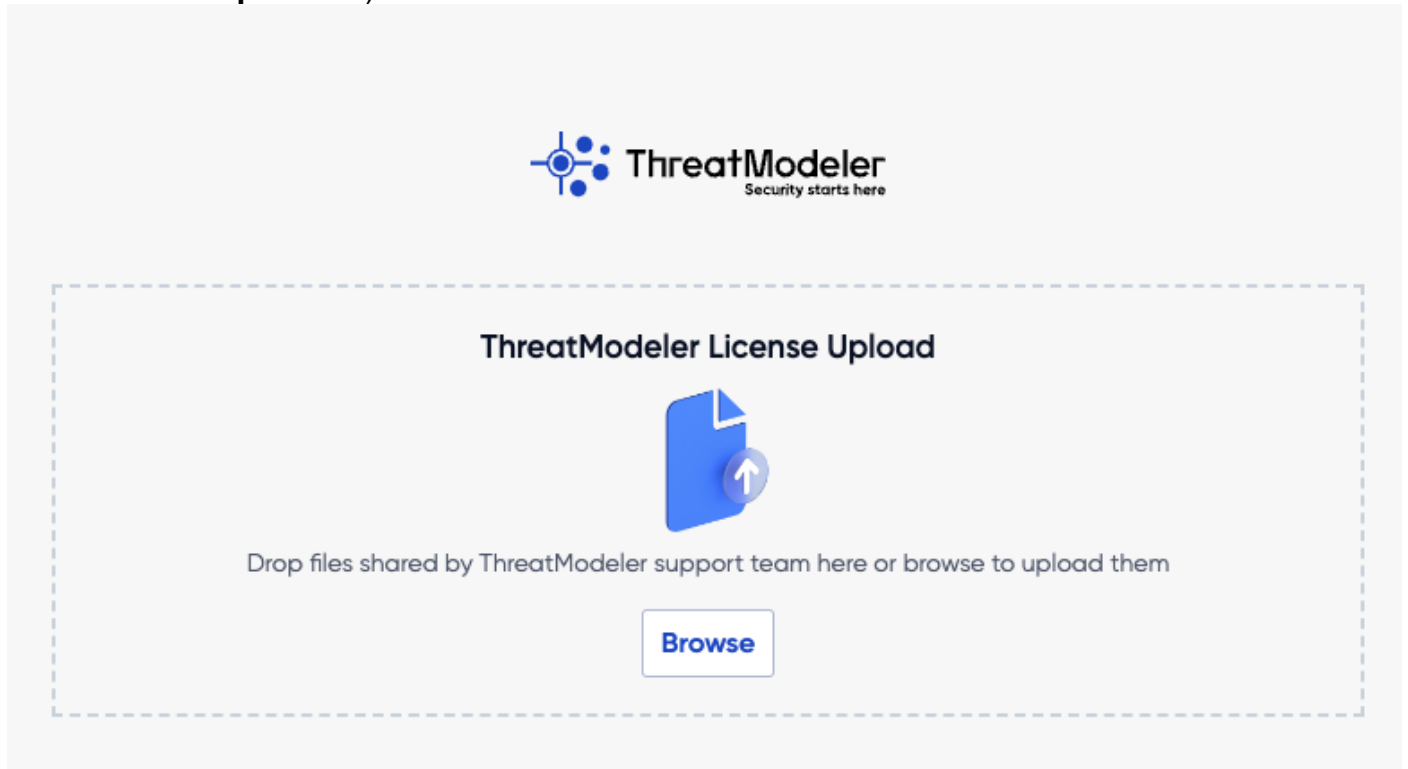
7. After successfully uploading ThreatModeler License files, you should see a success message with the page redirected to license agreement page and home page as follows.

8. To upload *tm_lic_10.txt* file into the platform, click on settings icon.
9. Select "**Access Management**" from the left panel.

Threat Models

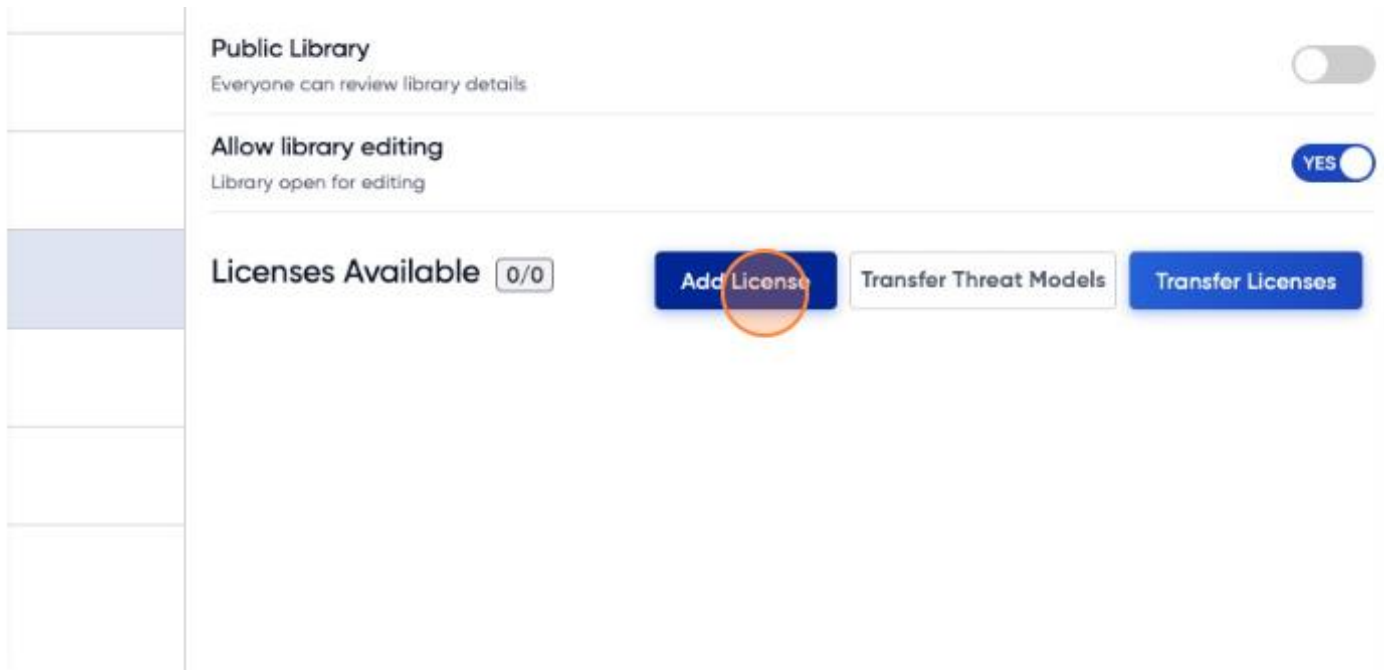Search by name, version, tags, or risk

Select All ▾
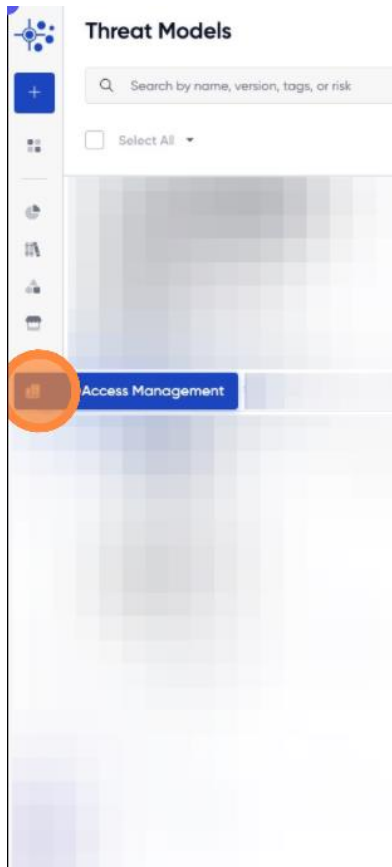
Access Management

10. From the Access Management screen, click on Department you would want to add licenses to. in the Licenses section and upload tm_lic_10.txt file. After you successfully upload the license file you should see a message saying "ThreatModeler Licenses Uploaded Successfully."
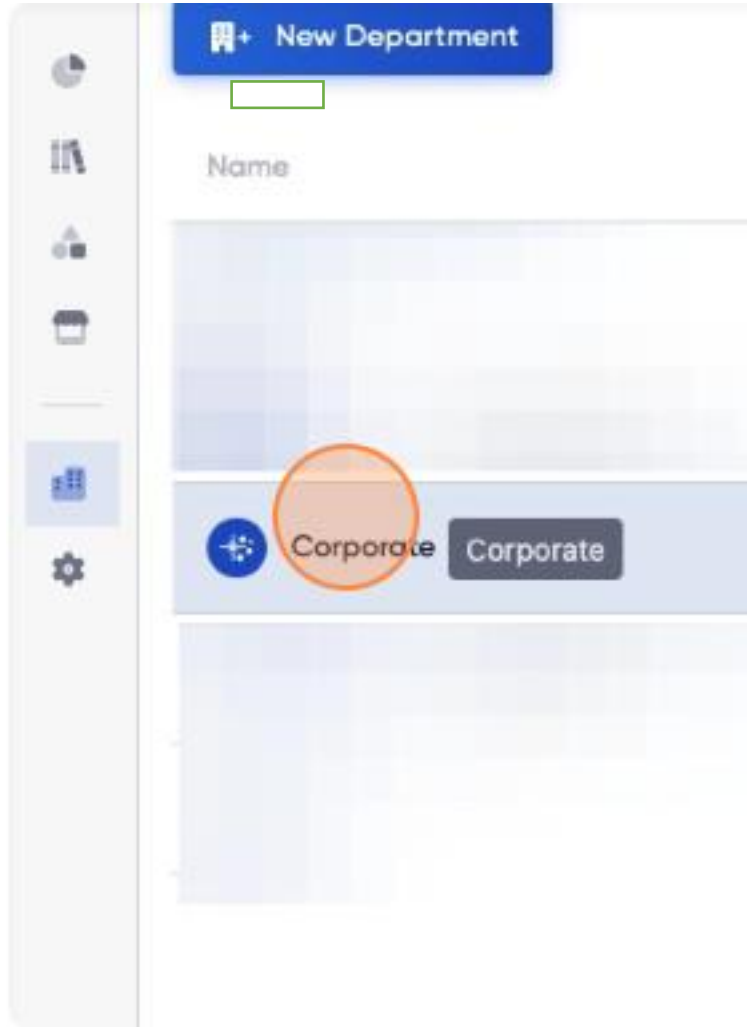

11. As you click on the desired department, on right panel you should see "Add License" to upload the tm_lic_10.txt file.

Public Library
Everyone can review library details

Allow library editing
Library open for editing

Licenses Available 0/0   Add License   Transfer Threat Models   Transfer Licenses

12. Click browse to select and upload the tm_lic_10.txt license file onto ThreatModeler platform.

Add License   ✕

Select License File *

Please select a .lic/.txt file   📁 Browse

Cancel   Upload
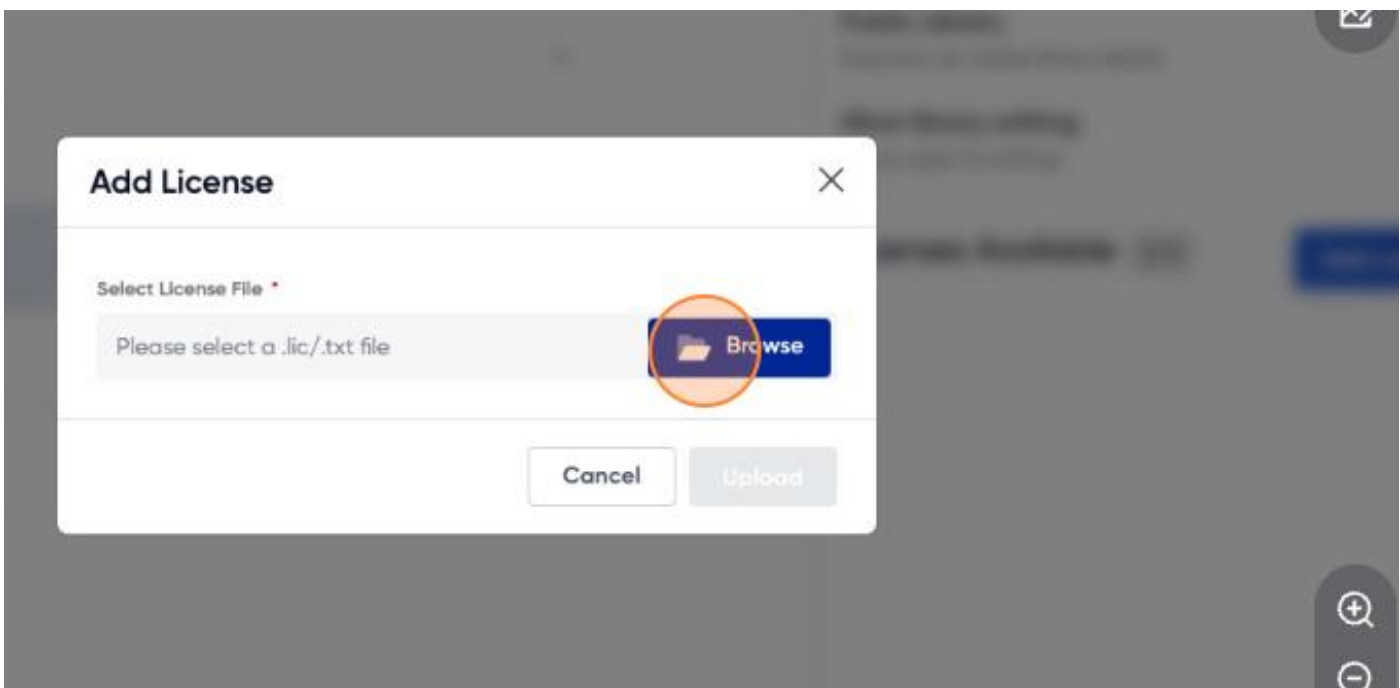
13. Before you proceed any further, please change the default password. To change the password, Click on user icon.
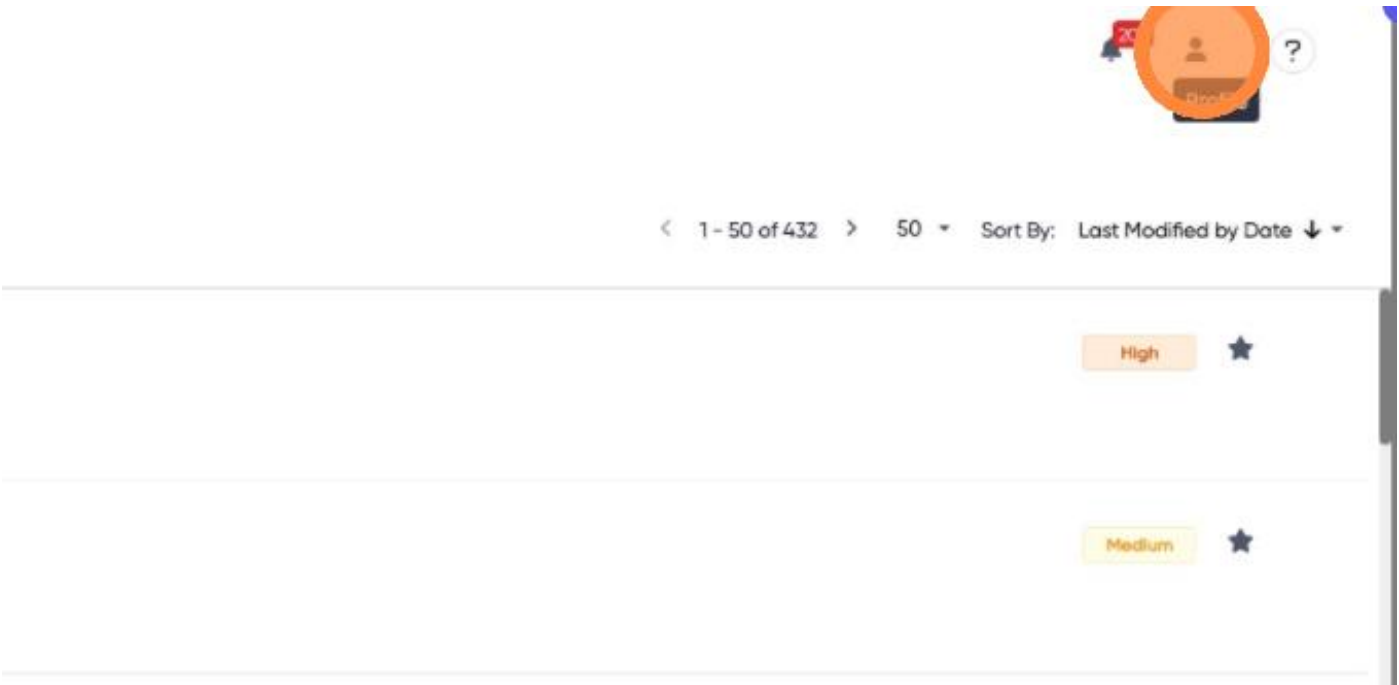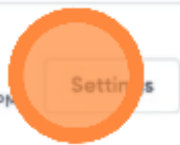
14. Click on user (Corporate admin is a test user, usually it will be your user with which you logged in).
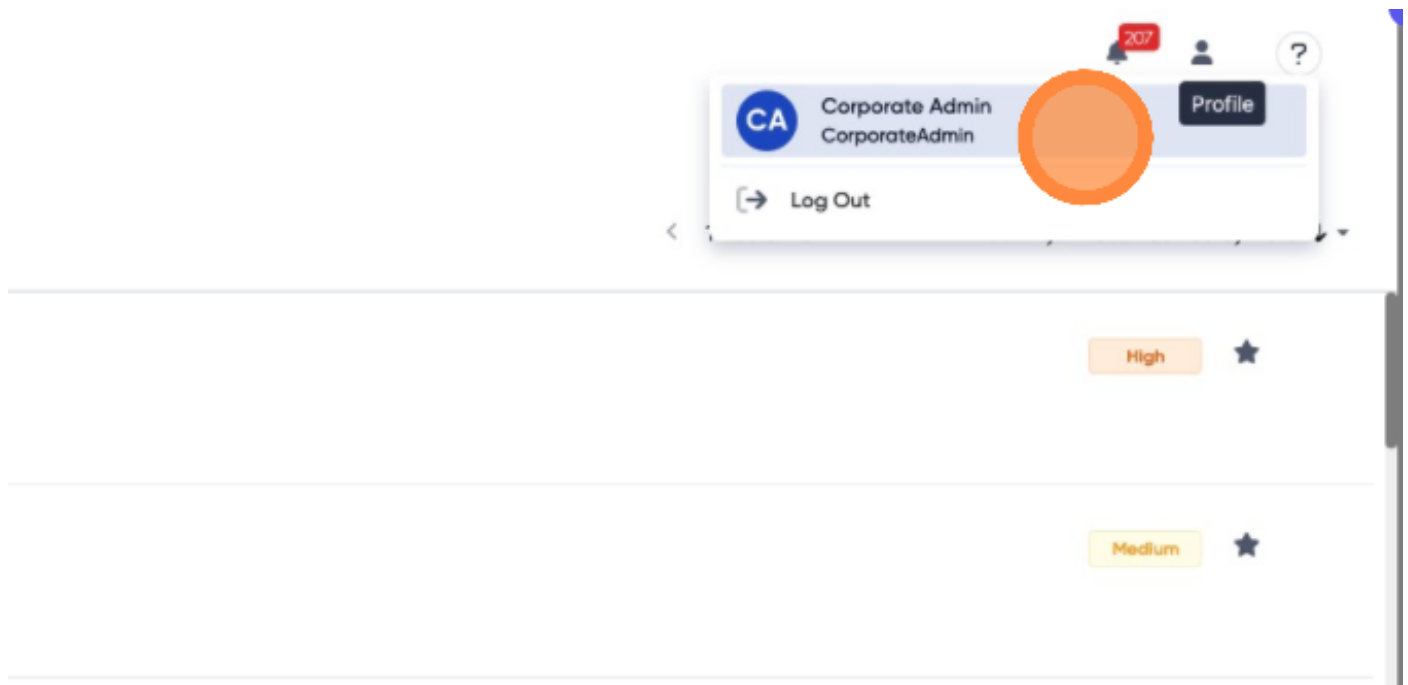
15. Click on settings.

Last login:
Sep 15, 2023 at 12:56 PM

Settings

Admin

16. Click on change password.

Corporate Admin

Username

CorporateAdmin

Email

support@threatmodeler.com

Change Password

Save

17. Enter the password of your choice and click change.

Change Password

×

Old password *

Enter old password

New Password *

Enter new password

Required atleast 1 special (non-alphanumeric) character

Minimum Length must be 8 characters long

Required atleast 1 lowercase character (no s)

Required atleast 1 uppercase character (no s)

Required atleast 1 Number

Re-enter Password *

Enter password again

Cancel Change