

ThreatModeler™: Existing and New VPC

Table of Contents

Overview.....	3
<i>Prerequisites for Deploying ThreatModeler in an AWS Account.....</i>	3
Costs	4
<i>Deployment Options</i>	4
<i>ThreatModeler Server Standalone setup.....</i>	5
Architecture	5
<i>ThreatModeler Deployment.....</i>	8
Option 1: Deploy ThreatModeler into a new VPC.	8
Accessing ThreatModeler (When Deployed into a New VPC).....	14
Option 2: Deploy ThreatModeler into an Existing VPC	23
Accessing ThreatModeler (When Deployed into an Existing VPC)	29

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.
- If 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).
 - If ThreatModeler is being launched in a new VPC, VPC peering needs to be done between the new VPC (where ThreatModeler is launched) and Corporate VPC (where VPN is deployed for accessing private resources across your enterprise).
 - If 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

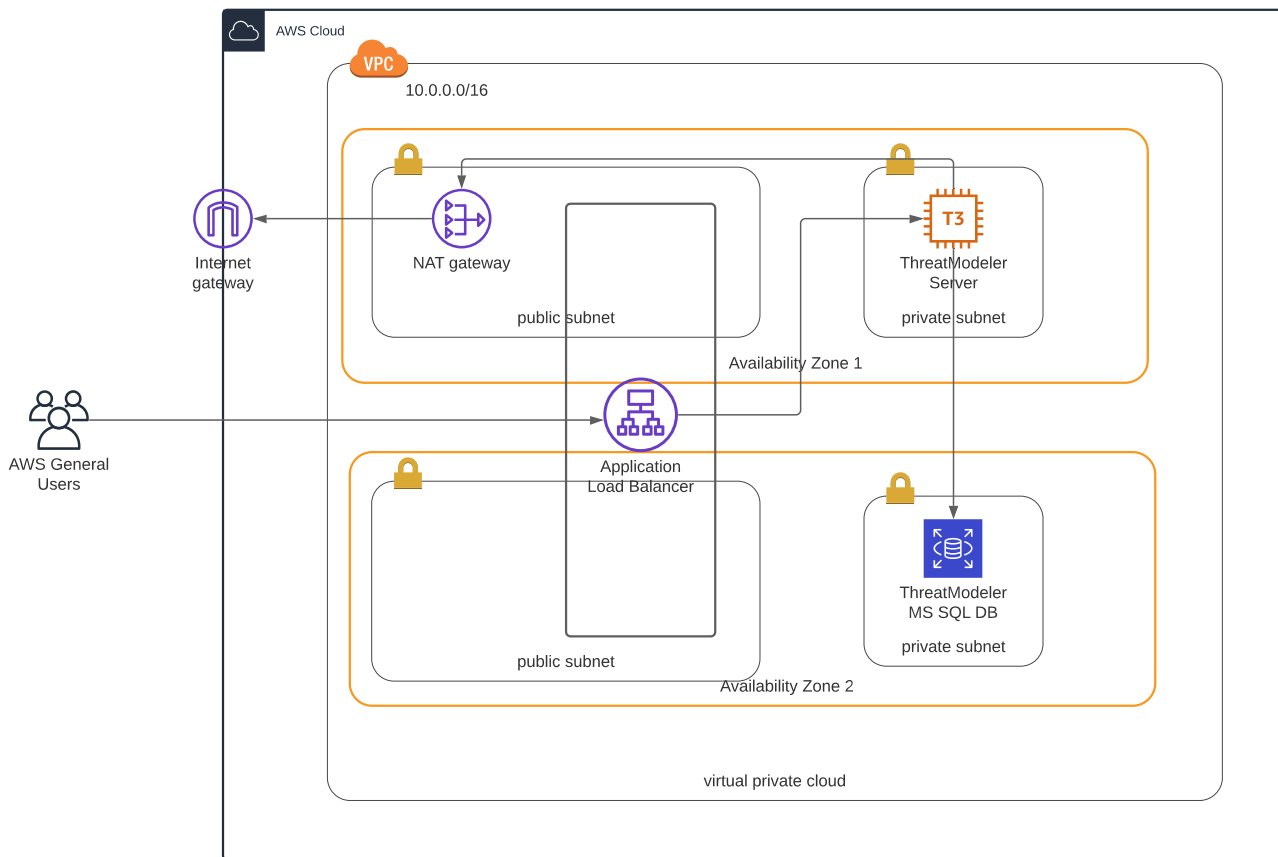
- Option 1: Deploy ThreatModeler into a new VPC.
- Option 2: Deploy ThreatModeler into an existing VPC.

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:

- VPC (the VPC deployment is based on the AWS QuickStart found [here](#)).
 1. Internet Gateway
 2. Two public and two private subnets
 3. NAT Gateway in public subnet in AZ1
 4. Elastic IP for the NAT Gateway

- Note: VPC will only be created for deployment Option 1 (Deploy ThreatModeler into a new VPC).

- 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. For Option 1 Deployment, one EC2 instance will be created in private subnet (ThreatModeler-server)
 - ThreatModeler server Deployed from the subscribed AMI
 - Instance type from CFN parameters, EBS Root volume size of 90 GB (gp2)
 - ThreatModeler server Instance Security Group (ingress ports 22 for SSH, 80 for HTTP respectively)
 -
 2. For Option 2 Deployment, 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

Option 1: Deploy ThreatModeler into a new 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.

The screenshot displays the AWS Marketplace page for ThreatModeler. The top section includes the product name, version (5.4.3.3), and a brief description: "A next generation platform that builds process flow diagram-based threat models for cloud with just one click. ThreatModeler enables you to design applications/ infrastructure securely and". A pricing box indicates a typical total price of \$1,000.05/hr. Below this is a navigation bar with tabs for Overview, Pricing, Usage (selected), Support, and Reviews.

Product Overview

What's Included

Note: Always ensure your operating system is current for your needs. This product includes both of the software packages described below:

ThreatModeler

- By: [ThreatModeler](#)

The product has all the features and functionality as our standard offering, deployed on a ThreatModeler-managed multi-tenant public cloud environment.

No Minimum Deployment Required.

AWS customers benefit from our non-NDA procurement process. Simply purchase licenses based on your needs and get started immediately. DevOps receives immediate proof of value and there is no minimum application deployment. Benefit from our leading threat modeling platform that is designed to help DevOps to meet the complex needs of Agile cloud development.

ThreatModeler enables users to build upon existing threat models through its patented Threat Chaining feature. Updates and changes made to a chained threat model will reflect across all models in which it is nested.

Alongside the highlighted features, ThreatModeler provides -

Auto Threat Mitigation - Ensure all the required security controls are implemented correctly. Based on the results of your threat model, automatically.

Highlights

- Accelerator (Patented) - With just one click, automatically build threat models for your cloud environments. ThreatModeler keeps your threat model synchronized with your cloud environment and automatically validates the security configurations.
- Onboard Architect (Patented) - Create accurate threat models with the patented Onboard Architect feature, guiding you through the process of building cloud architectures securely. Define custom rules based on your deployment needs.
- Built In Compliance Frameworks - ThreatModeler supports established regulatory standards such as NIST, GDPR & PCI which empowers teams to understand and meet compliance requirements at the beginning of your CDLC.

Fulfillment Options

ThreatModeler - Existing VPC
CloudFormation Template

One Web Server which accepts requests through an Application Load Balancer and an RDS.

- [View Template Components](#)
- [View usage Instructions](#)
- [View CloudFormation Template](#)

ThreatModeler - New VPC
CloudFormation Template

One Web Server which accepts requests through an Application Load Balancer and an RDS.

- [View Template Components](#)
- [View usage Instructions](#)
- [View CloudFormation Template](#)

End-user license agreement

By subscribing to this product you agree to terms and conditions outlined in the product [End User License Agreement \(EULA\)](#)

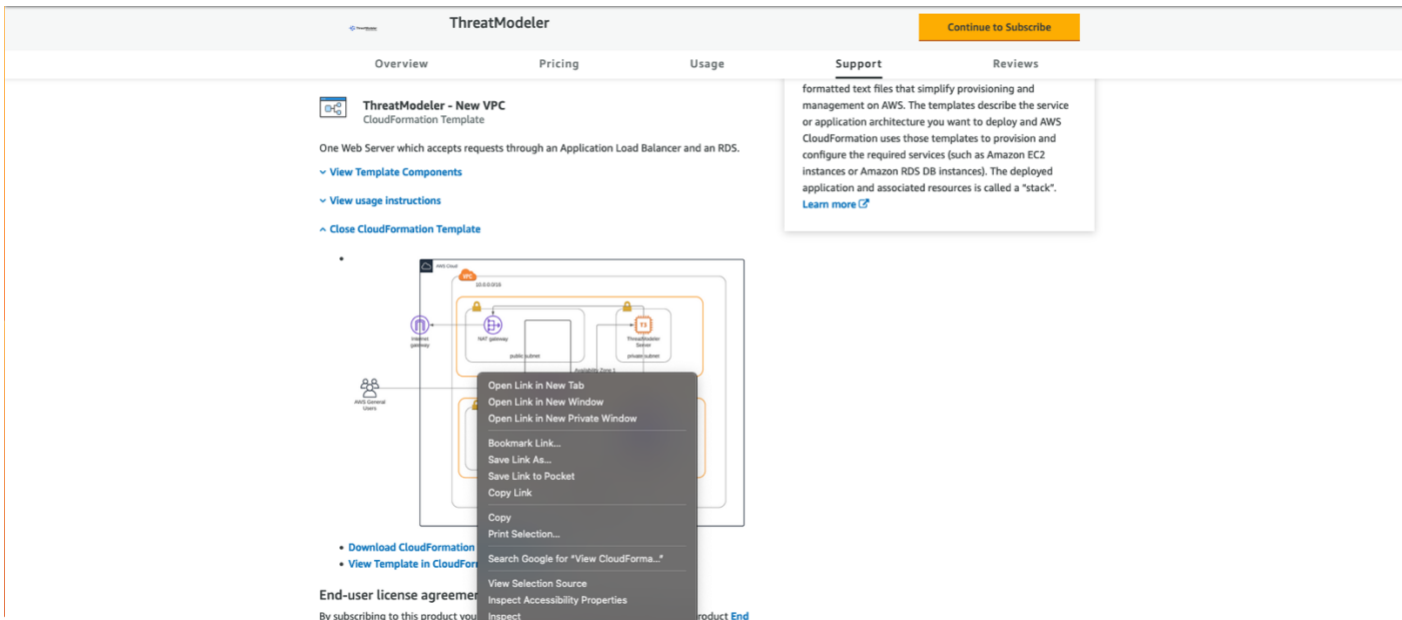
Additional Resources

- [ThreatModeler Interface Guide](#)
- [YouTube](#)
- [Technical Datasheet](#)

CloudFormation Template

AWS CloudFormation templates are JSON or YAML formatted text files that simplify provisioning and management on AWS. The templates describe the service or application architecture you want to deploy and AWS CloudFormation uses those templates to provision and configure the required services (such as Amazon EC2 instances or Amazon RDS DB instances). The deployed application and associated resources is called a "stack". [Learn more](#)

3. For New 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. Select Amazon S3 template URL in the Specify template window to launch the ThreatModeler Application in New VPC.
7. Paste the S3 template link into the field under Amazon S3 URL and click Next.

Specify stack details

Stack name

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.

Availability Zones

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

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

Public subnet 1 CIDR

CIDR Block for the public subnet located in Availability Zone 1.

Public subnet 2 CIDR

CIDR Block for the public subnet located in Availability Zone 2.

Private subnet 1 CIDR

CIDR Block for the private subnet located in Availability Zone 1.

Private subnet 2 CIDR

CIDR Block for the private subnet located in Availability Zone 2.

VPC CIDR

CIDR Block for the VPC.

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

SSL Certificate ARN (Requires matching DNS name)

The Amazon Resource Name for the existing SSL cert you wish to use; empty for none

ThreatModeler Amazon EC2 instance type

Amazon EC2 instance type where ThreatModeler will be installed.

DNS record name

DNS name with which ThreatModeler application will be accessed

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.

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.

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.

Organization

Name of the Organization

RDS Database Master Username

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

RDS Database Master Password

The Master password of the RDS instance for ThreatModeler Database. Must be between 8 to 128 printable ASCII characters (including /, and &#39;)

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.

Quick Start S3 key prefix

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

Cancel

Previous

Next

8. 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. Pick exactly 2 AZ's.
ThreatModeler RDSAvailabilityZone	Requires Input	Availability Zone to launch ThreatModeler RDS.
Public Subnet 1 CIDR	Requires Input	CIDR block for public subnet located in Availability Zone 1.
Public Subnet 2 CIDR	Requires Input	CIDR block for public subnet located in Availability Zone 2.
Private Subnet 1 CIDR	Requires Input	CIDR block for private subnet located in Availability Zone 1 to Allocate Private IP address to ThreatModeler Application Server.
Private Subnet 2 CIDR	Requires Input	CIDR block for private subnet located in Availability Zone 2 to Allocate Private IP address to ThreatModeler Database Server.
VPC CIDR	Requires Input	The CIDR range for the VPC that is to be created.
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.
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	threatmodeler-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	createnewvpc/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"

Capabilities

The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources.

☒ 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

Cancel Previous Create change set Create stack

- Click on Create Stack.
- The deployment typically takes around 30-40 minutes to complete.
- Take a note of the twelve-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 (4)
↻

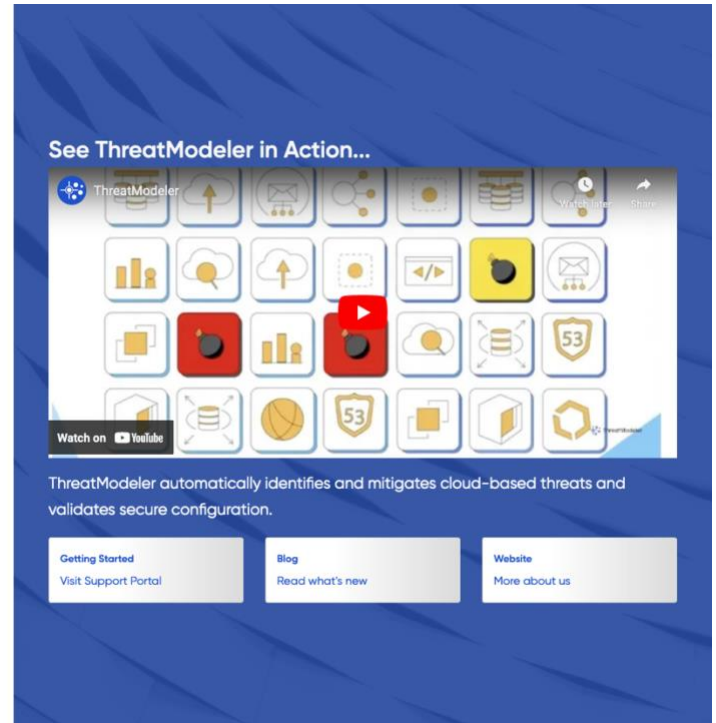
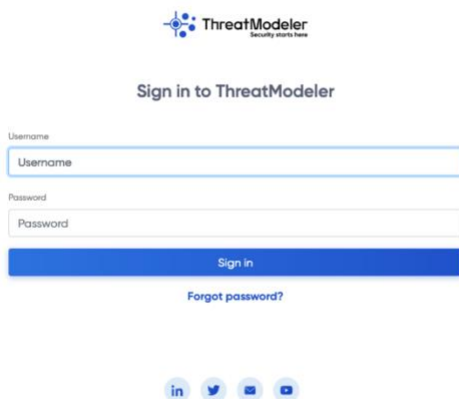
⚙

Key ▲	Value ▼	Description ▼	Export name ▼
DBEndpoint	<input type="text"/>	Endpoint Address of database instance	-
InstanceID	<input type="text"/>	EC2 InstanceID of the instance running ThreatModeler Server	-
PrivateIPAddress	<input type="text"/>	Private IP Address of ThreatModeler instance	-
VPCID	<input type="text"/>	VPC ID	-

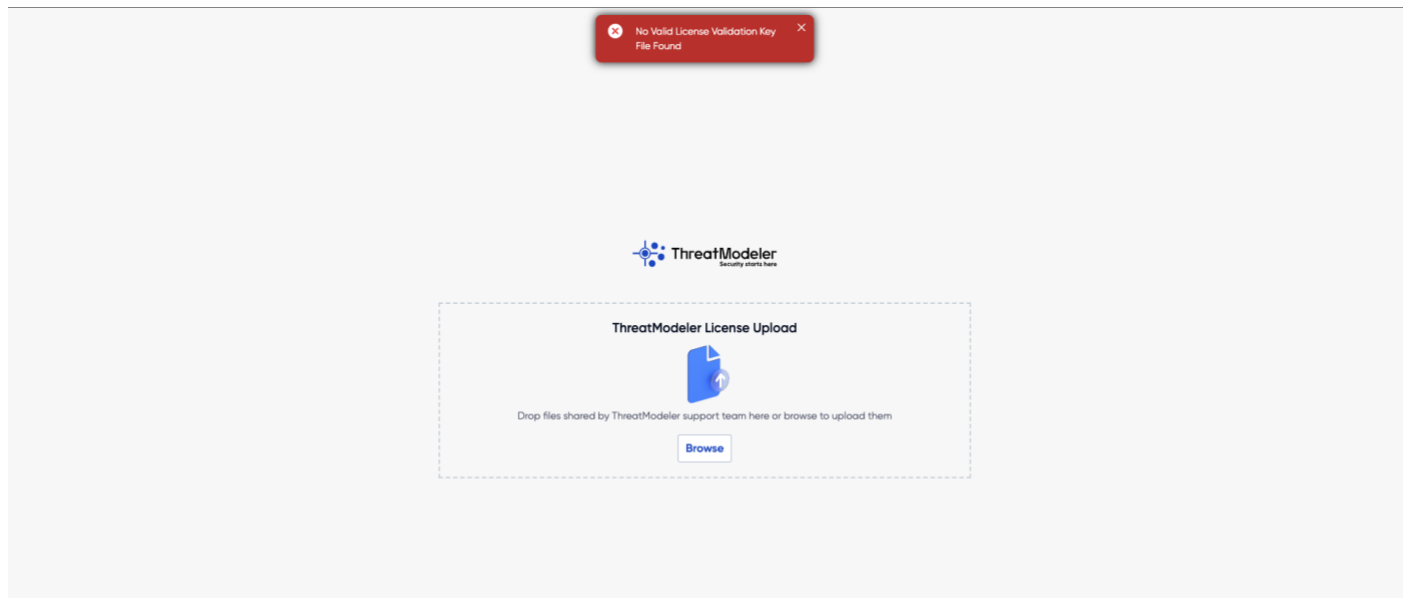
Accessing ThreatModeler (When Deployed into a New VPC)

- Assumptions:
 - VPC peering is successfully established between the new VPC (where ThreatModeler is launched) and Corporate VPC (where VPN is deployed for accessing private resources across your enterprise), so that you can RDP into ThreatModeler server.
 - After VPC peering is established, you need to be on VPN to login and access the ThreatModeler instance.

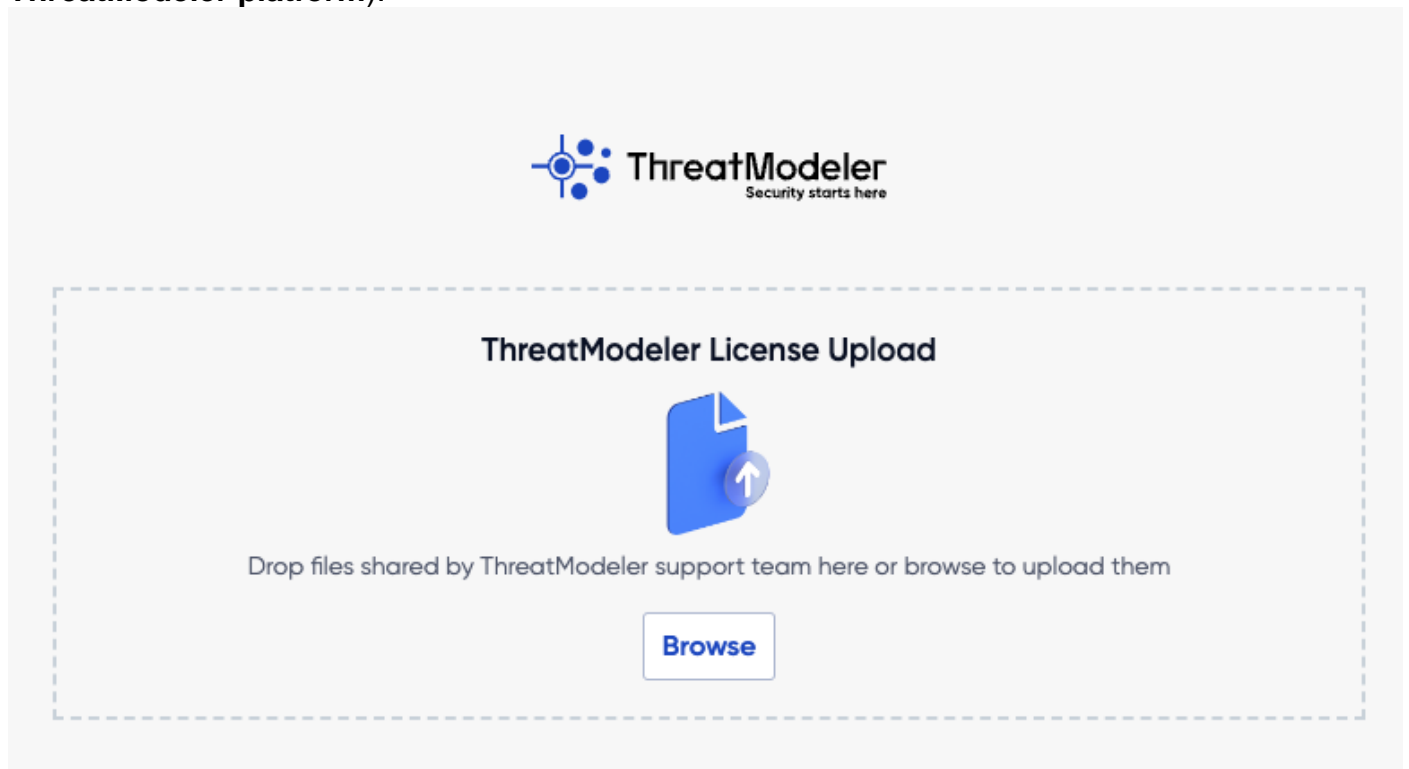
1. Go to the browser of your choice and use DNS name (parameter named DNS Record Name) provided during the CloudFormation launch and you should see the following login screen to login to the platform.



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.



License Agreement

NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT ("AGREEMENT") CAREFULLY. BY USING THE PRODUCT, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT. IF LICENSEE IS A PARTY TO A SEPARATE SIGNED CONTRACT BETWEEN LICENSEE AND THREATMODELER SOFTWARE INC. GOVERNING LICENSEE'S USE OF THE PRODUCT(S), SUCH SIGNED AGREEMENT CONTROLS THE TERMS OF SUCH PRODUCT(S).

1. Definitions.

1.1 "**Appliance**" means a hardware device, software or virtual appliance on which the Product may be or is Used pursuant to the terms herein.

1.2 "**Authorized Partner(s)**" means ThreatModeler's distributors, resellers, strategic partners, or other business partners.

1.3 "**Documentation**" means the then-current, generally available, written user manuals and online help and guides for Product.

1.4 "**Licensee**" means you as an individual or on behalf of the company, partnership, business you represent.

1.5 "**Permitted Number**" means one (1) Threat Model per license purchased unless otherwise indicated in a valid Quote.

1.6 "**Product**" means the ThreatModeler Software, Documentation, and any other software licensed hereunder.

1.7 "**Quote**" means a valid ThreatModeler or Authorized Partner quote that provides pricing for the Product that Licensee may affirmatively acknowledge, execute, or issue a purchase order against to purchase the Product.

1.8 "**Software**" means s (a) all of the software object code, portals, and contents of the files with which this Agreement is provided; or such software or content hosted by ThreatModeler or Authorized Partner(s) through electronic transmission of software as a service "SaaS" or on-premise software; (b) any Updates; and (c) any other ThreatModeler software, if any, licensed to Licensee by ThreatModeler or an Authorized Partner as part of a maintenance contract or service subscription.

1.9 "**Threat Model**" means one (1) architecture diagram for which one (1) threat model will be created by the Product. Such threat model may be deleted and refreshed at the end of every subscription year without an impact on the Permitted Number for purpose of license calculation.

1.10 "**ThreatModeler**" means ThreatModeler Software, Inc., with offices at 101 Hudson Street, Suite 2100, 21st Floor Jersey City, NJ 07302.

1.11 "**Updates**" means upgrades, updates, or any new version of Product that is made available without charge pursuant to the warranty for Product; or the Support Services for licensed Product, but does not mean a new Product.

1.12 "**Use**", "**Used**" or "**Using**" means to access or otherwise benefit from using the Product.

2. License Grant.


Subject to the payment of the applicable license fees (where applicable), and subject to the terms and conditions of this Agreement, ThreatModeler hereby grants to Licensee a non-exclusive, non-transferable license to Use the Product subject to any restrictions or usage terms specified herein including as to the Permitted Number of licenses or on the applicable Quote or Documentation. In the event Product contains or uses third party software, ThreatModeler will have no responsibility and claims no right with respect to such third party software. Your use of such third party software and other copyrighted material is governed by their respective terms. No tangible personal property is transferred. For the avoidance of doubt, Licensee may not use templates or versions to build more than the Permitted Number of a license. Licensees who use those features to circumvent this restriction are in material breach hereof.

3. Term.

This Agreement is effective for the term set forth in the Quote issued to you by ThreatModeler or an Authorized Partner and which is accepted by you (the "**Term**"). If Licensee issues a purchase order to an


Reject

Accept



Threat Models

☐ Select All

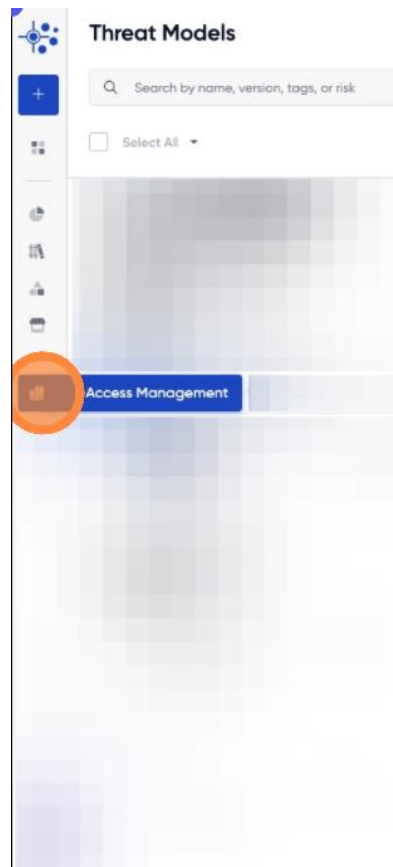


There are no Active Models

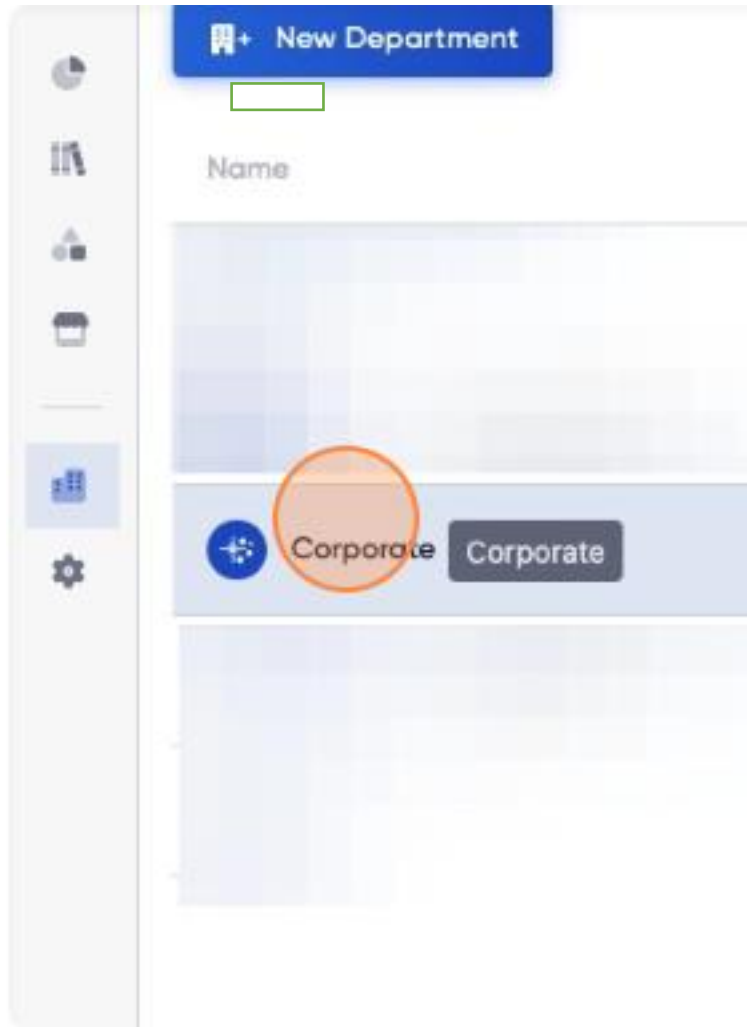
Create a new Threat Model or ask to be a Collaborator to an existing one to get access

+ Create New

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



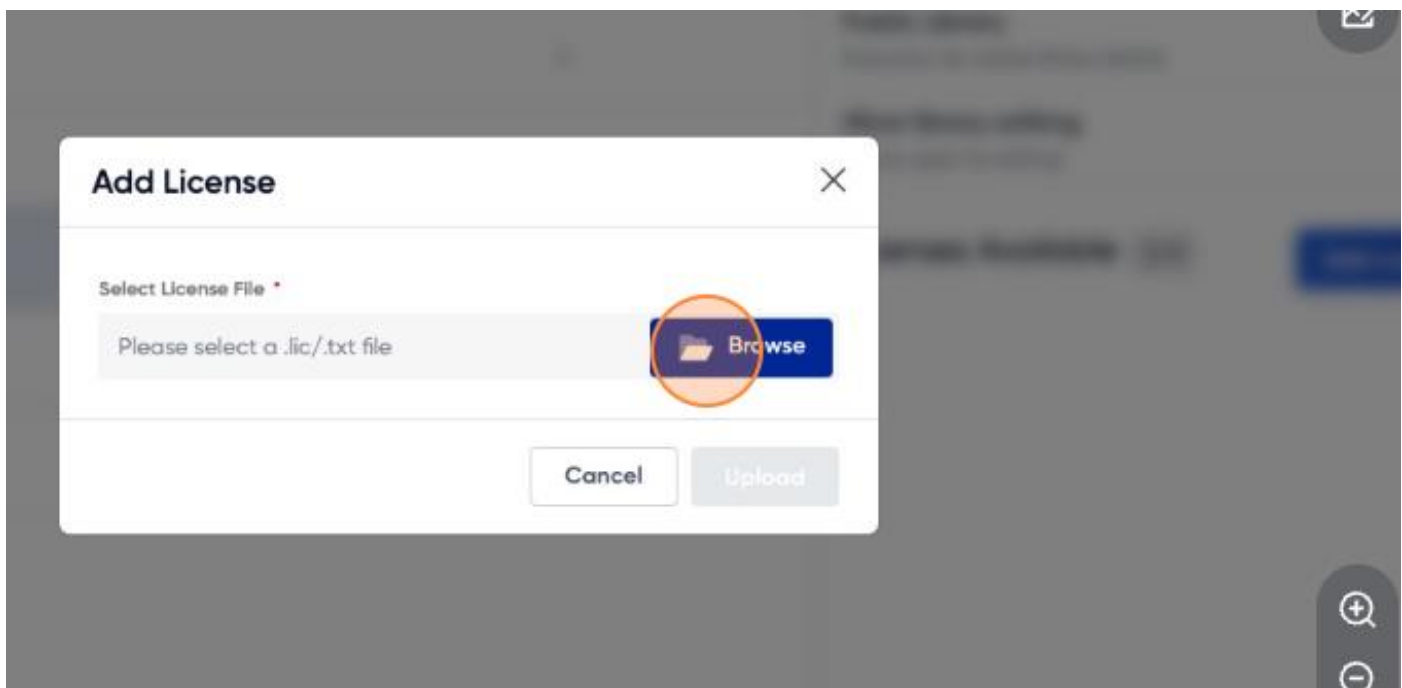
10. From the Access Management screen, click on Department you would want to add licenses to. in the Licenses section and upload tm_lic_10.txt file. After you successfully upload the license file you should see a message saying “ThreatModeler Licenses Uploaded Successfully.”



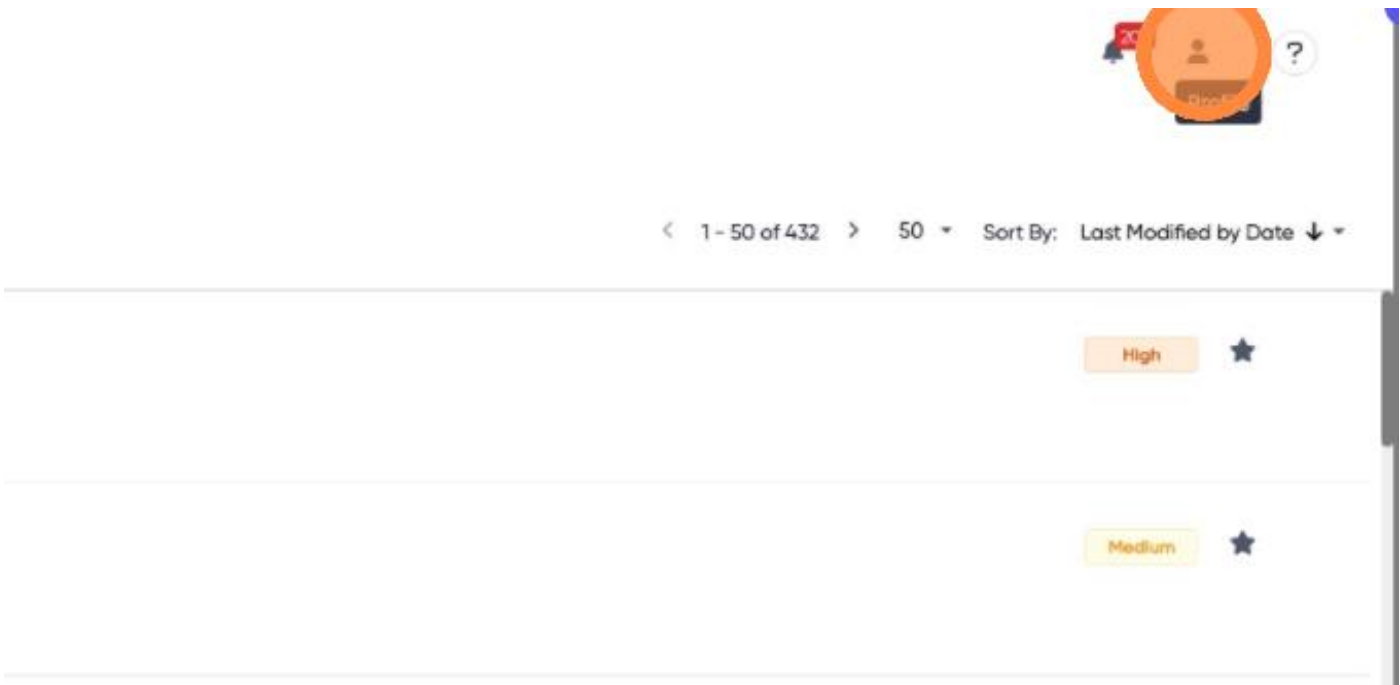
11. As you click on the desired department, on right panel you should see “Add License” to upload the tm_lic_10.txt file.



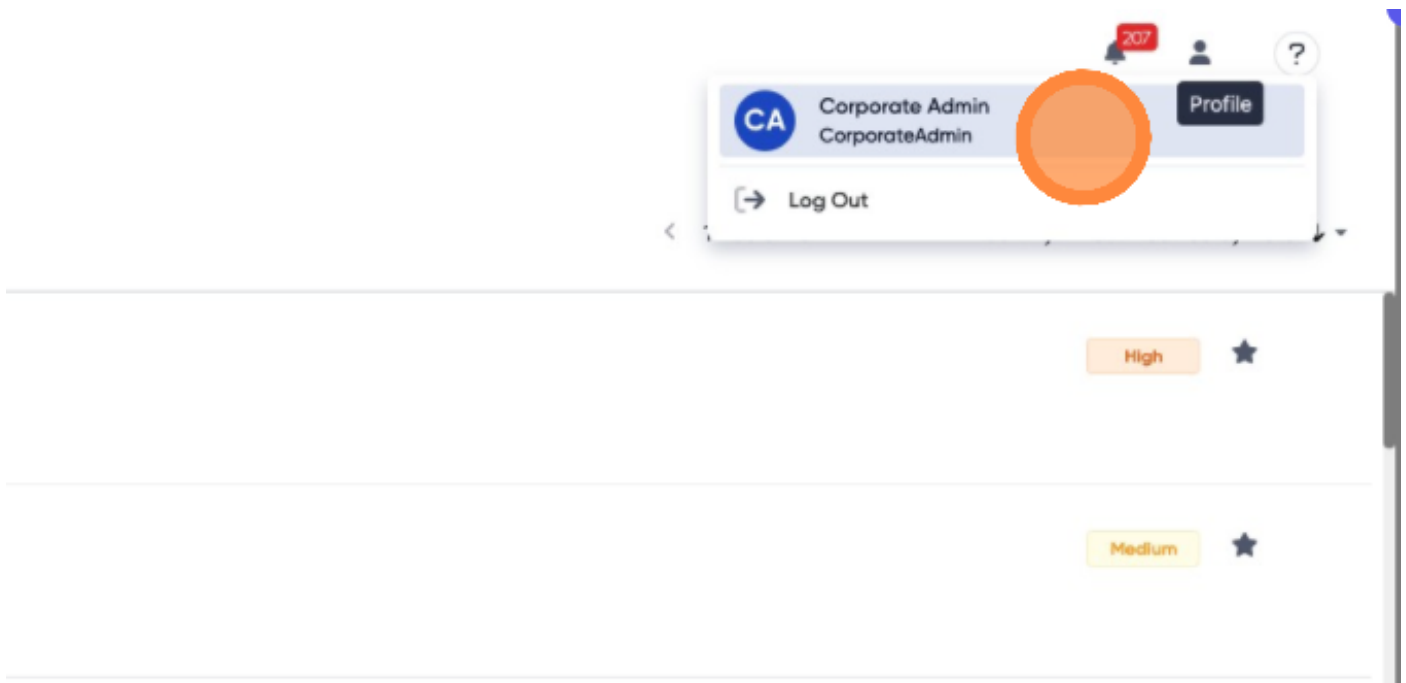
12. Click browse to select and upload the tm_lic_10.txt license file onto ThreatModeler platform.



13. Before you proceed any further, please change the default password. To change the password, Click on user icon.



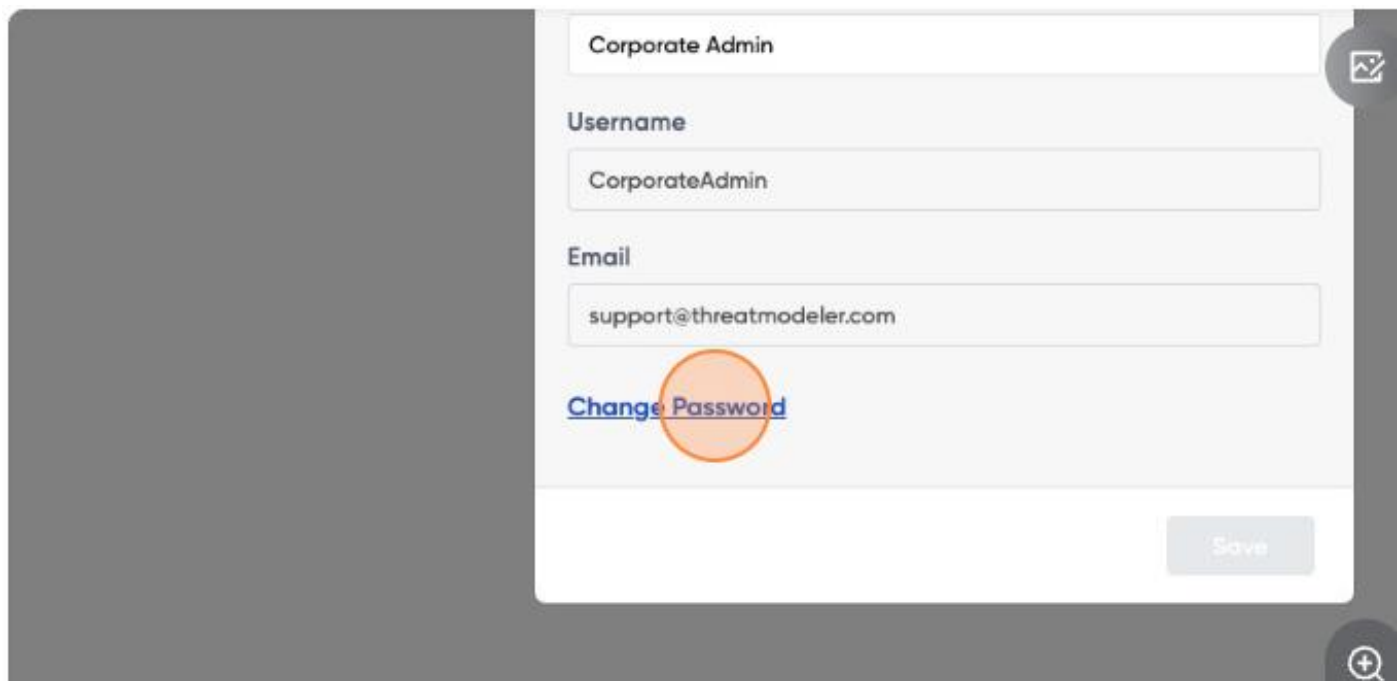
14. Click on user (Corporate admin is a test user, usually it will be your user with which you logged in).



15. Click on settings.



16. Click on change password.



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

Option 2: 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.

9.

The screenshot displays the ThreatModeler product page on AWS Marketplace. The top section includes the product name, version (5.4.3.3), and a brief description. A pricing box indicates a typical total price of \$1,000.05/hr. The main content area is divided into two tabs: 'Overview' and 'Usage'. The 'Overview' tab is currently selected, showing a 'Product Overview' section with 'What's Included' and 'Highlights'. The 'Usage' tab is also visible, showing 'Fulfillment Options' for both 'Existing VPC' and 'New VPC' scenarios, each with links to view template components, usage instructions, and the CloudFormation template. An 'End-user license agreement' section is also present. The right sidebar contains 'Additional Resources' and a 'CloudFormation Template' section with a brief explanation of AWS CloudFormation templates.

ThreatModeler
By: [ThreatModeler](#) Latest Version: 5.4.3.3
A next generation platform that builds process flow diagram-based threat models for cloud with just one click. ThreatModeler enables you to design applications/ infrastructure securely and
[Show more](#)
Windows

[Continue to Subscribe](#)
[Save to List](#)
Typical Total Price
\$1,000.05/hr
Total pricing per instance for services hosted on t3.medium in US East (N. Virginia). [View Details](#)

[Overview](#) [Pricing](#) [Usage](#) [Support](#) [Reviews](#)

Product Overview

What's Included
Note: Always ensure your operating system is current for your needs. This product includes both of the software packages described below:

ThreatModeler
• By: [ThreatModeler](#)

The product has all the features and functionality as our standard offering, deployed on a ThreatModeler-managed multi-tenant public cloud environment.

No Minimum Deployment Required.

AWS customers benefit from our non-NDA procurement process. Simply purchase licenses based on your needs and get started immediately. DevOps receives immediate proof of value and there is no minimum application deployment. Benefit from our leading threat modeling platform that is designed to help DevOps to meet the complex needs of Agile cloud development.

ThreatModeler enables users to build upon existing threat models through its patented Threat Chaining feature. Updates and changes made to a chained threat model will reflect across all models in which it is nested.

Alongside the highlighted features, ThreatModeler provides -

Auto Threat Mitigation - Ensure all the required security controls are implemented correctly. Based on the results of your threat model, automatically

Highlights

- **Accelerator (Patented)** - With just one click, automatically build threat models for your cloud environments. ThreatModeler keeps your threat model synchronized with your cloud environment and automatically validates the security configurations.
- **Onboard Architect (Patented)** - Create accurate threat models with the patented Onboard Architect feature, guiding you through the process of building cloud architectures securely. Define custom rules based on your deployment needs.
- **Built In Compliance Frameworks** - ThreatModeler supports established regulatory standards such as NIST, GDPR & PCI which empowers teams to understand and meet compliance requirements at the beginning of your CDLC.

ThreatModeler
[Continue to Subscribe](#)

[Overview](#) [Pricing](#) [Usage](#) [Support](#) [Reviews](#)

Fulfillment Options

ThreatModeler - Existing VPC
CloudFormation Template

One Web Server which accepts requests through an Application Load Balancer and an RDS.

[View Template Components](#)
[View usage instructions](#)
[View CloudFormation Template](#)

ThreatModeler - New VPC
CloudFormation Template

One Web Server which accepts requests through an Application Load Balancer and an RDS.

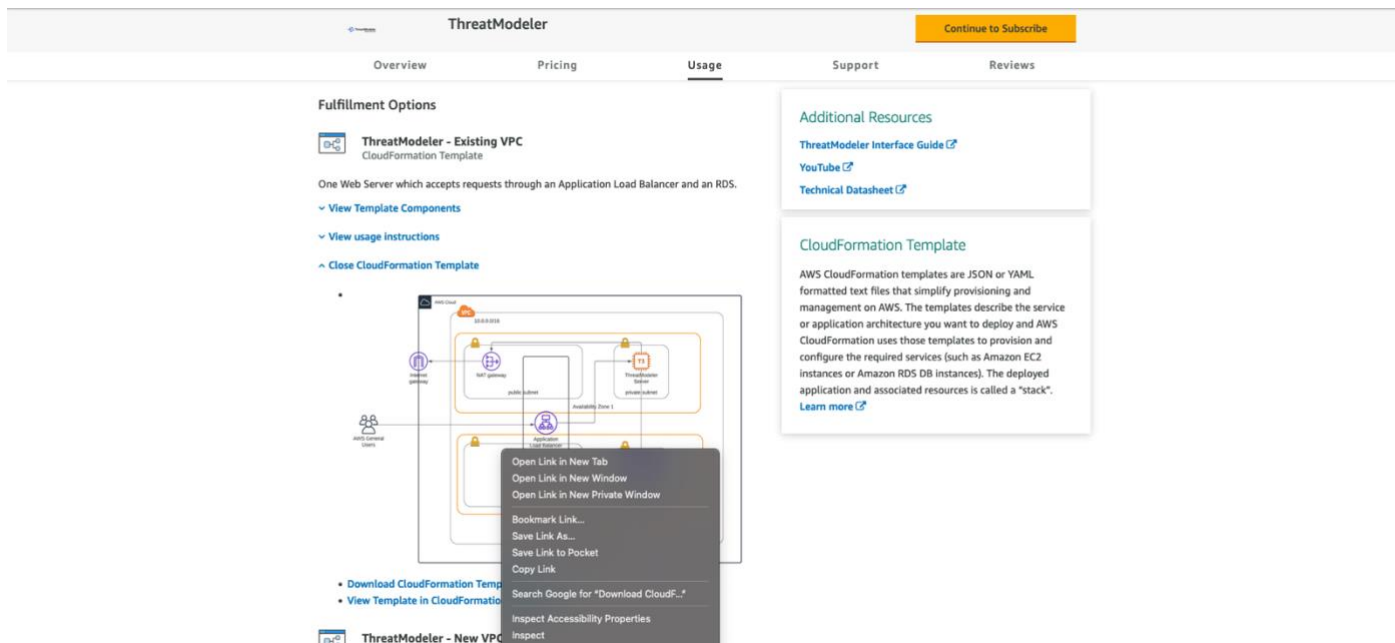
[View Template Components](#)
[View usage instructions](#)
[View CloudFormation Template](#)

End-user license agreement
By subscribing to this product you agree to terms and conditions outlined in the product [End User License Agreement \(EULA\)](#)

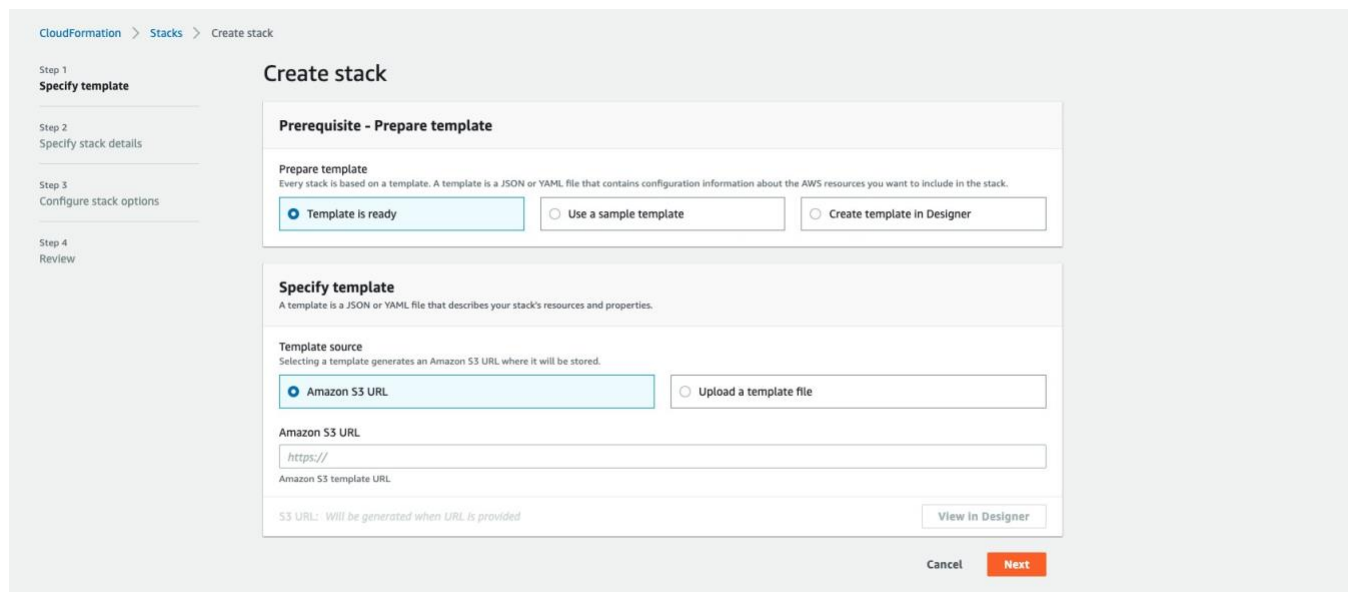
Additional Resources
[ThreatModeler Interface Guide](#)
[YouTube](#)
[Technical Datasheet](#)

CloudFormation Template
AWS CloudFormation templates are JSON or YAML formatted text files that simplify provisioning and management on AWS. The templates describe the service or application architecture you want to deploy and AWS CloudFormation uses those templates to provision and configure the required services (such as Amazon EC2 instances or Amazon RDS DB instances). The deployed application and associated resources is called a "stack".
[Learn more](#)

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.

Specify stack details

Stack name

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.

Availability Zones

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

Existing VPC ID

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

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'.

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'.

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'.

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'.

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

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

SSL Certificate ARN (Requires matching DNS name)

The Amazon Resource Name for the existing SSL cert you wish to use; empty for none

ThreatModeler Amazon EC2 instance type

Amazon EC2 Instance type where ThreatModeler will be installed.

DNS record name

DNS name with which ThreatModeler application will be accessed

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.

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.

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.

Organization

Name of the Organization

RDS Database Master Username

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

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.

Quick Start S3 key prefix

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

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"

Capabilities

 **The following resource(s) require capabilities: [AWS::CloudFormation::Stack]**

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources.

☒ 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

Cancel Previous Create change set Create stack

- 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)
↻

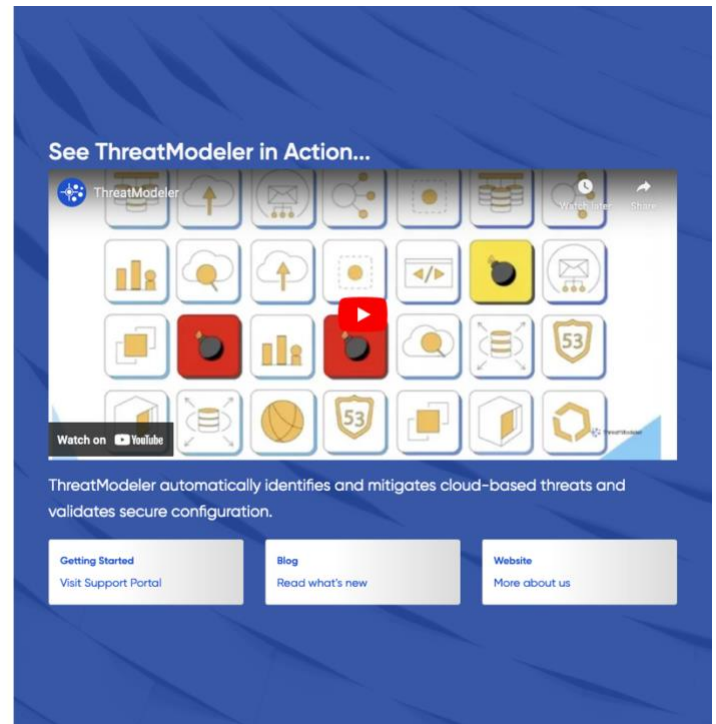
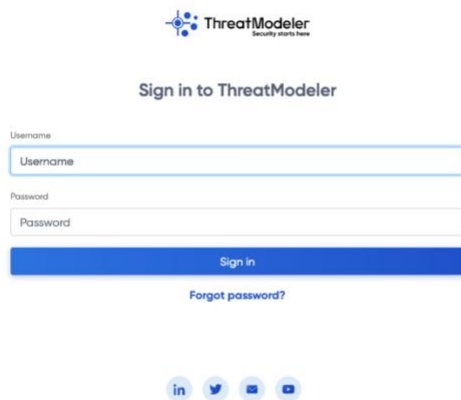
⚙

Key ▲	Value ▼	Description ▼	Export name ▼
DBEndpoint	<input type="text"/>	Endpoint Address of database Instance	-
InstanceId	<input type="text"/>	EC2 InstanceID of the instance running ThreatModeler Server	-
PrivateIPAddress	<input type="text"/>	Private IP Address of ThreatModeler instance	-

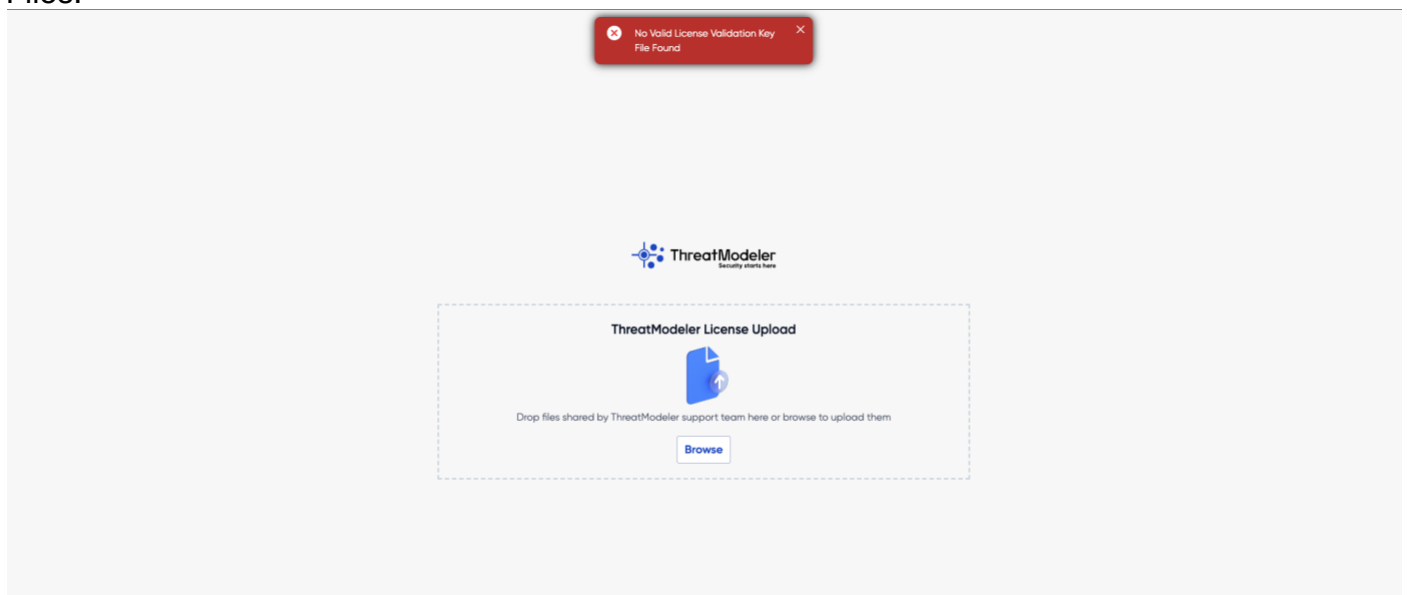
Accessing ThreatModeler (When Deployed into an Existing VPC)

- 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.

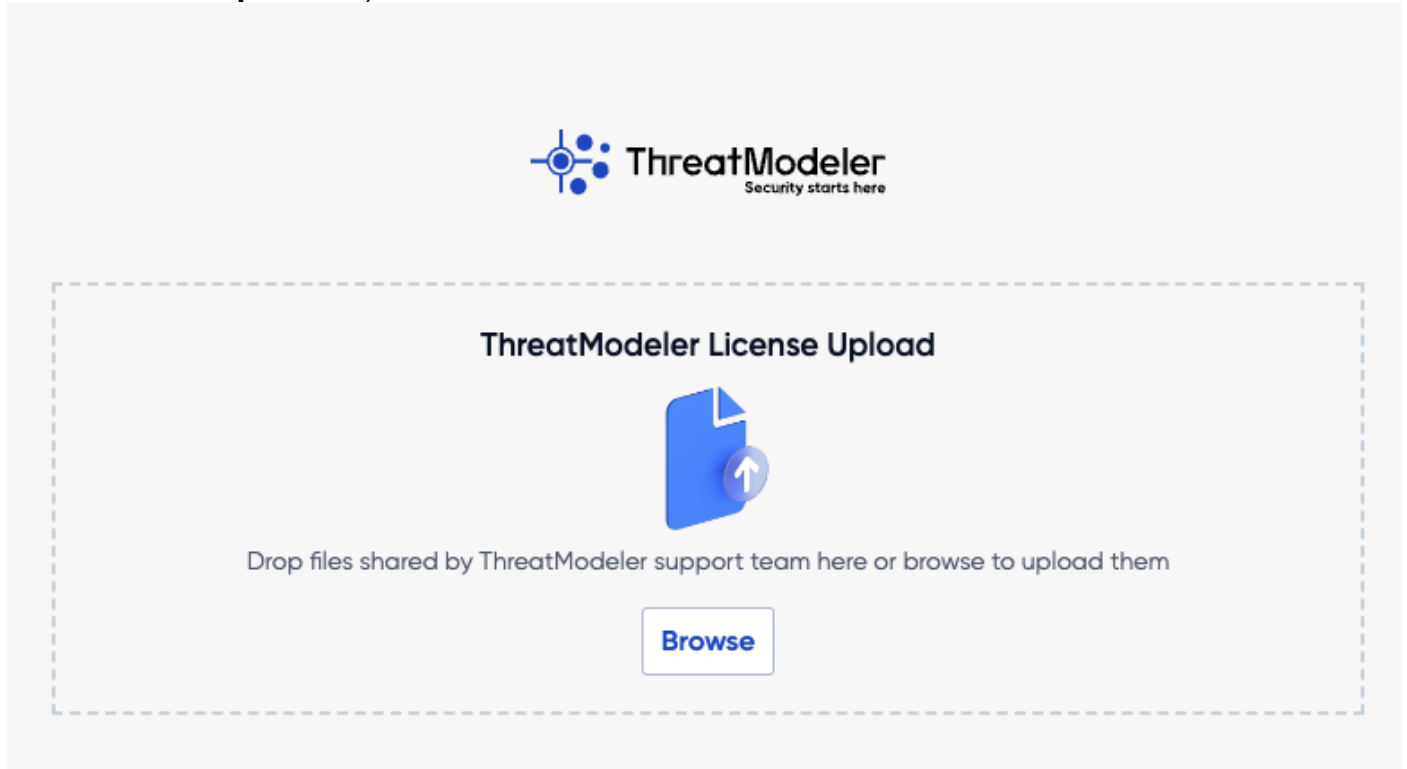
1. Go to the browser of your choice and use DNS name (parameter named DNS Record Name) provided during the CloudFormation launch and you should see the following login screen to login to the platform.



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.

License Agreement


NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT ("AGREEMENT") CAREFULLY. BY USING THE PRODUCT, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT. IF LICENSEE IS A PARTY TO A SEPARATE SIGNED CONTRACT BETWEEN LICENSEE AND THREATMODELER SOFTWARE INC. GOVERNING LICENSEE'S USE OF THE PRODUCT(S), SUCH SIGNED AGREEMENT CONTROLS THE TERMS OF SUCH PRODUCT(S).

1. Definitions.









- 1.1 "**Appliance**" means a hardware device, software or virtual appliance on which the Product may be or is Used pursuant to the terms herein.
- 1.2 "**Authorized Partner(s)**" means ThreatModeler's distributors, resellers, strategic partners, or other business partners.
- 1.3 "**Documentation**" means the then-current, generally available, written user manuals and online help and guides for Product.
- 1.4 "**Licensee**" means you as an individual or on behalf of the company, partnership, business you represent.
- 1.5 "**Permitted Number**" means one (1) Threat Model per license purchased unless otherwise indicated in a valid Quote.
- 1.6 "**Product**" means the ThreatModeler Software, Documentation, and any other software licensed hereunder.
- 1.7 "**Quote**" means a valid ThreatModeler or Authorized Partner quote that provides pricing for the Product that Licensee may affirmatively acknowledge, execute, or issue a purchase order against to purchase the Product.
- 1.8 "**Software**" means s (a) all of the software object code, portals, and contents of the files with which this Agreement is provided; or such software or content hosted by ThreatModeler or Authorized Partner(s) through electronic transmission of software as a service "SaaS" or on-premise software; (b) any Updates; and (c) any other ThreatModeler software, if any, licensed to Licensee by ThreatModeler or an Authorized Partner as part of a maintenance contract or service subscription.
- 1.9 "**Threat Model**" means one (1) architecture diagram for which one (1) threat model will be created by the Product. Such threat model may be deleted and refreshed at the end of every subscription year without an impact on the Permitted Number for purpose of license calculation.
- 1.10 "**ThreatModeler**" means ThreatModeler Software, Inc., with offices at 101 Hudson Street, Suite 2100, 21st Floor Jersey City, NJ 07302.
- 1.11 "**Updates**" means upgrades, updates, or any new version of Product that is made available without charge pursuant to the warranty for Product; or the Support Services for licensed Product, but does not mean a new Product.
- 1.12 "**Use**", "**Used**" or "**Using**" means to access or otherwise benefit from using the Product.


2. License Grant. Subject to the payment of the applicable license fees (where applicable), and subject to the terms and conditions of this Agreement, ThreatModeler hereby grants to Licensee a non-exclusive, non-transferable license to Use the Product subject to any restrictions or usage terms specified herein including as to the Permitted Number of licenses or on the applicable Quote or Documentation. In the event Product contains or uses third party software, ThreatModeler will have no responsibility and claims no right with respect to such third party software. Your use of such third party software and other copyrighted material is governed by their respective terms. No tangible personal property is transferred. For the avoidance of doubt, Licensee may not use templates or versions to build more than the Permitted Number of a license. Licensees who use those features to circumvent this restriction are in material breach hereof.

3. Term. This Agreement is effective for the term set forth in the Quote issued to you by ThreatModeler or an Authorized Partner and which is accepted by you (the "**Term**"). If Licensee issues a purchase order to an


Threat Models

☐ Select All

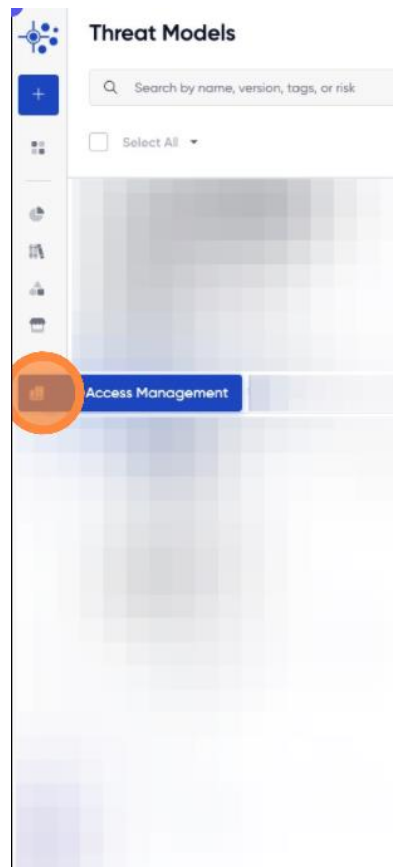











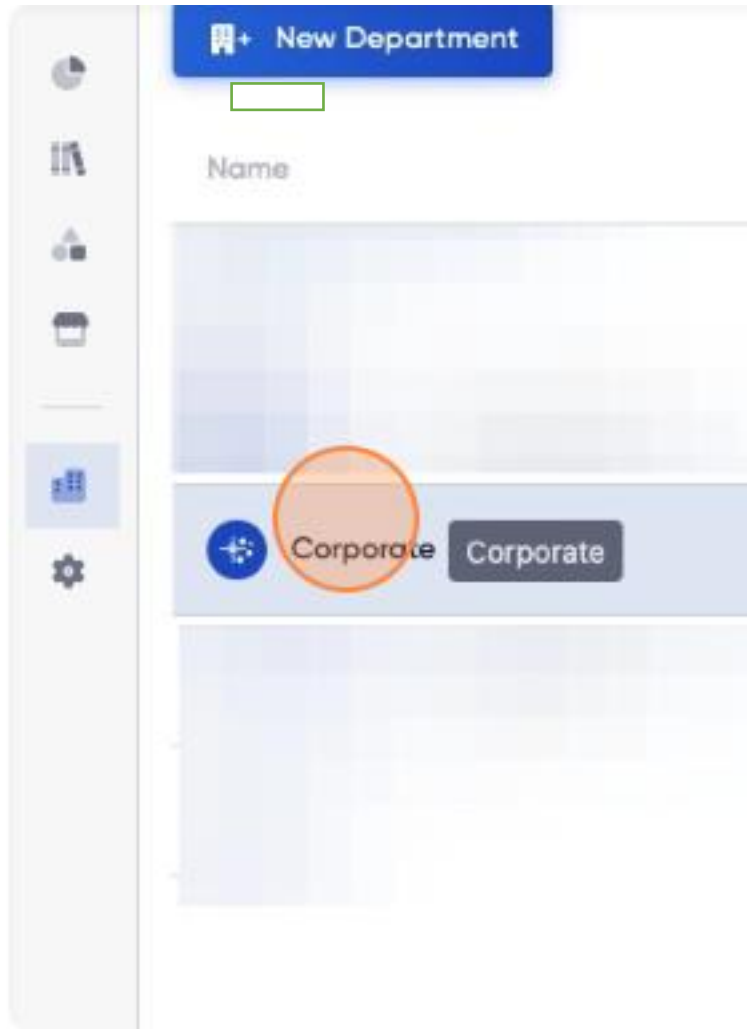
There are no Active Models

Create a new Threat Model or ask to be a Collaborator to an existing one to get access

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



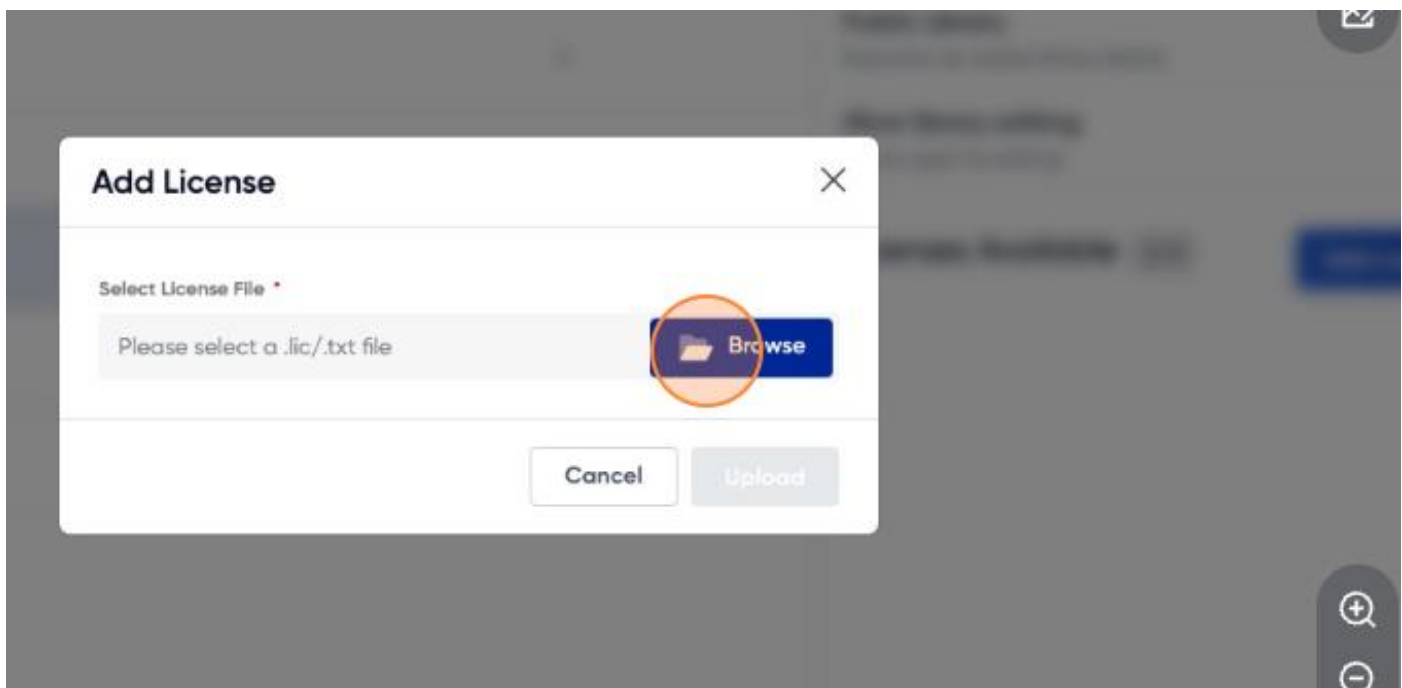
10. From the Access Management screen, click on Department you would want to add licenses to. in the Licenses section and upload tm_lic_10.txt file. After you successfully upload the license file you should see a message saying “ThreatModeler Licenses Uploaded Successfully.”



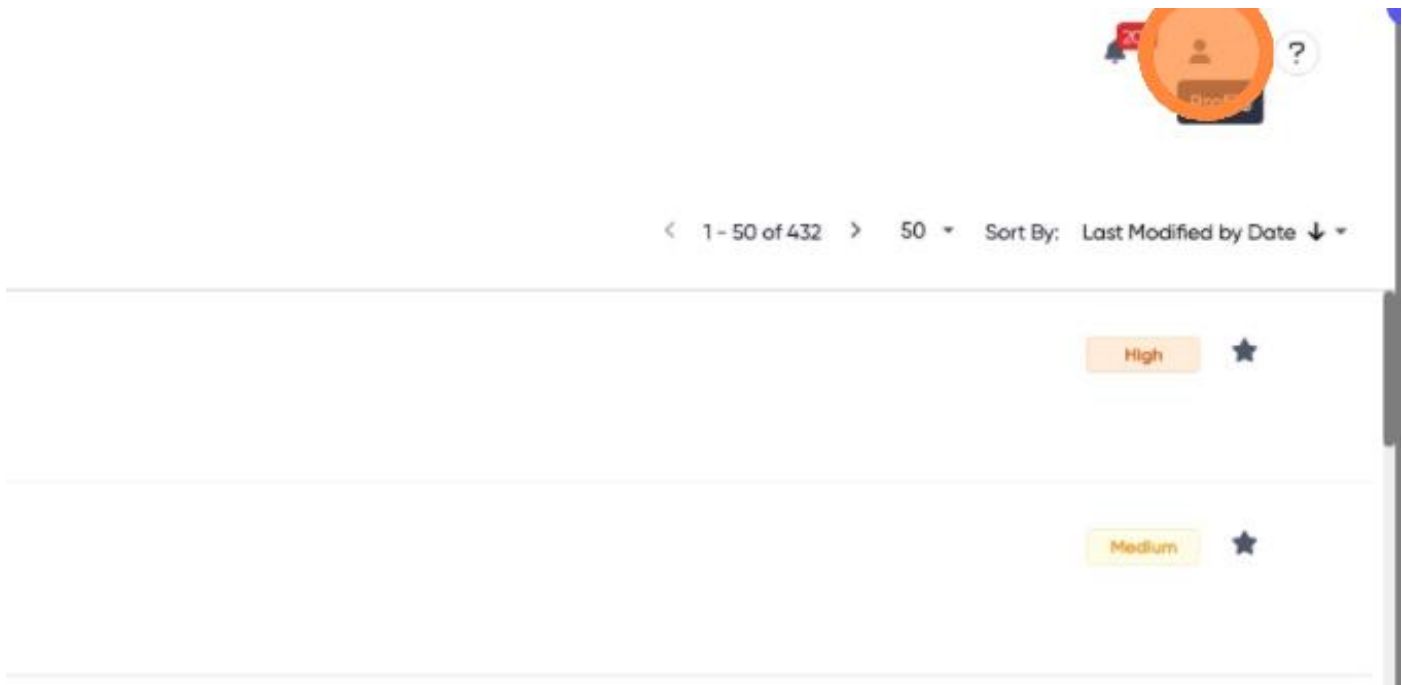
11. As you click on the desired department, on right panel you should see “Add License” to upload the tm_lic_10.txt file.



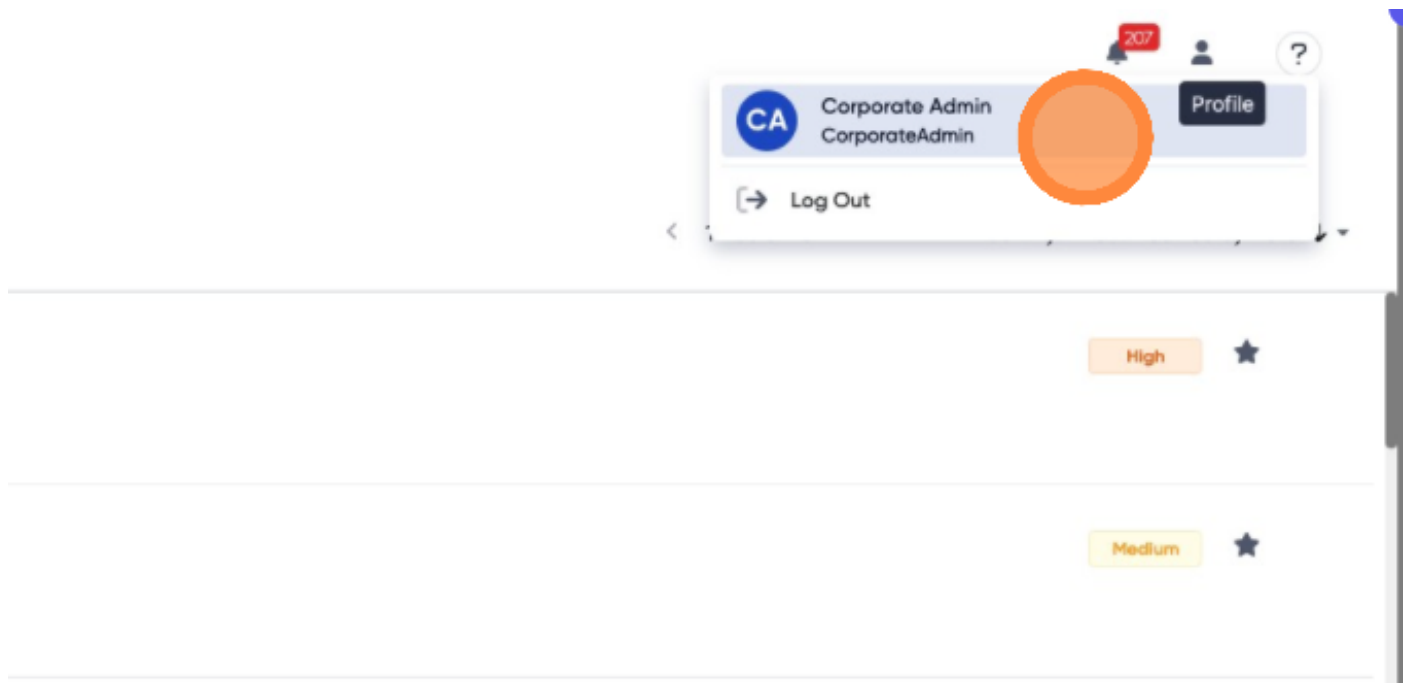
12. Click browse to select and upload the tm_lic_10.txt license file onto ThreatModeler platform.



13. Before you proceed any further, please change the default password. To change the password, Click on user icon.



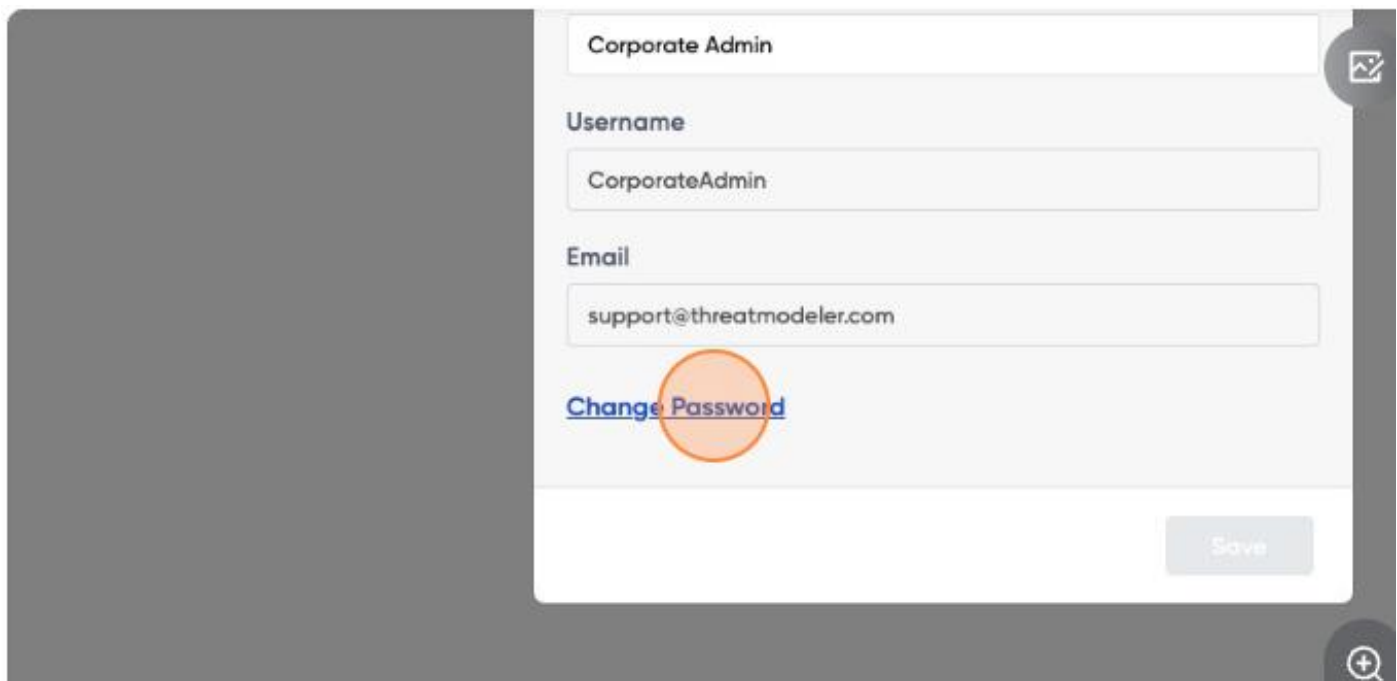
14. Click on user (Corporate admin is a test user, usually it will be your user with which you logged in).



15. Click on settings.



16. Click on change password.



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