ThreatModeler
SECURITY STARTS HERE

2020

ThreatModeler™: Setup and Deployment Guide

THREATMODELER SOFTWARE, INC. | 185 HUDSON STREET, SUITE 1620, JERSEY CITY, NJ 07311 | 201-266-0510

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. Please contact support via support@threatmodeler.com if you have not provided these details.
- Share the AWS Account ID where ThreatModeler will be launched with ThreatModeler Support. Please contact support via support@threatmodeler.com if have not provided an Account ID yet.
- ThreatModeler has already shared an AMI ID with the Account ID specified in the point above.
- 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.
- License files
    - These are the required files for logging into ThreatModeler initially. ThreatModeler Support will send these files to you via email.
- 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. 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.
    - If a certificate ARN is provided, please use the same domain name (for creating record sets) 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.
- If no ARN is provided, ALB is created with HTTP listener. If you are willing to install SSL certificate within the ThreatModeler (windows) server, please reach out to your SSL certificate management team.

- 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).

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

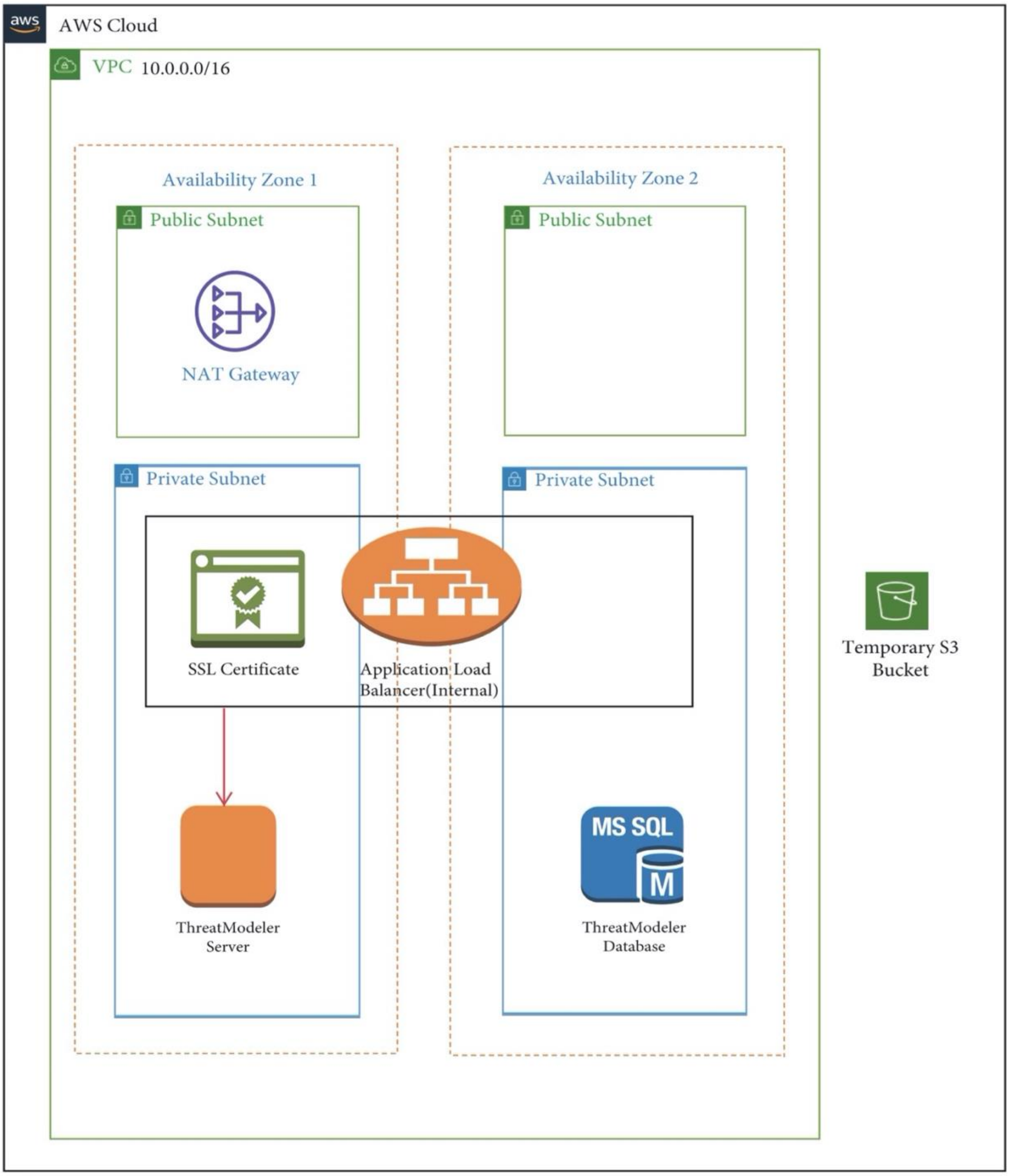
- Option 1: Deploy ThreatModeler on Microsoft Windows Server into a new VPC
- Option 2: Deploy ThreatModeler on Microsoft Windows Server into an existing VPC

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.



The 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 on Microsoft Windows Server into a new VPC).

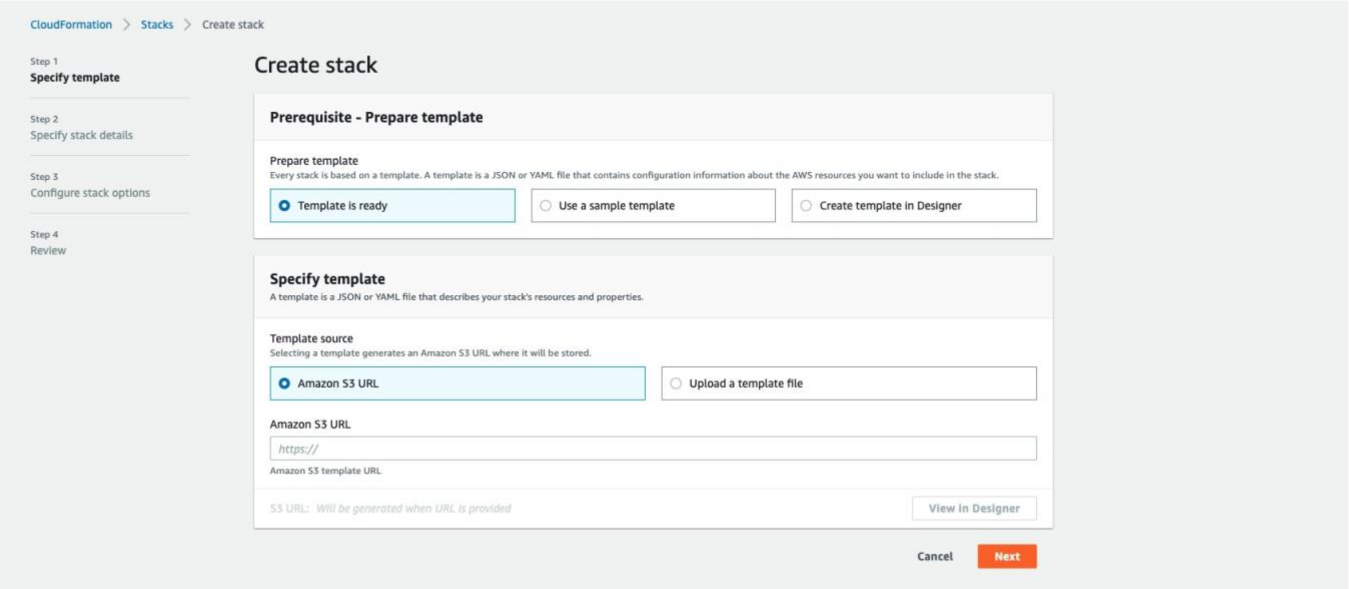
- S3 bucket – created temporarily to store the RDS database snapshot and then deleted later.
- RDS – will either be created in the same subnet as the ThreatModeler EC2 or in a secondary private subnet based on your parameter selection during CFN launch.
    1. RDS instance
        - Deployed in private subnet
        - Fixed instance type of db.t2.medium
    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 (defaults to t2.medium) EBS Root volume size of 90 GB (gp2)
        - ThreatModeler server Instance Security Group (ingress ports 3389 for RDP, 443 for HTTPs 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 (defaults to t2.medium) EBS Root volume size of 90 GB (gp2)
        - ThreatModeler server Instance Security Group (ingress ports 3389 for RDP, 443 for HTTPs respectively) IAM instance profile from the created EC2 role.

- Application Load Balancer (Internal)
    1. Deployed in Private Subnet to send traffic to EC2 Instance in Private Subnet.
    2. Deployed with HTTP for default communication (if SSL ARN is not provided while launching the CloudFormation stack) or HTTPS listener secure communication (if SSL ARN is provided while launching the CloudFormation stack).

ThreatModeler Deployment

Option 1: Deploy ThreatModeler on Microsoft Windows Server into a new VPC

1. 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.
2. Select Services → CloudFormation → Stack → Create Stack → With new resources (standard).



Create stack

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL ○ Upload a template file

Amazon S3 URL

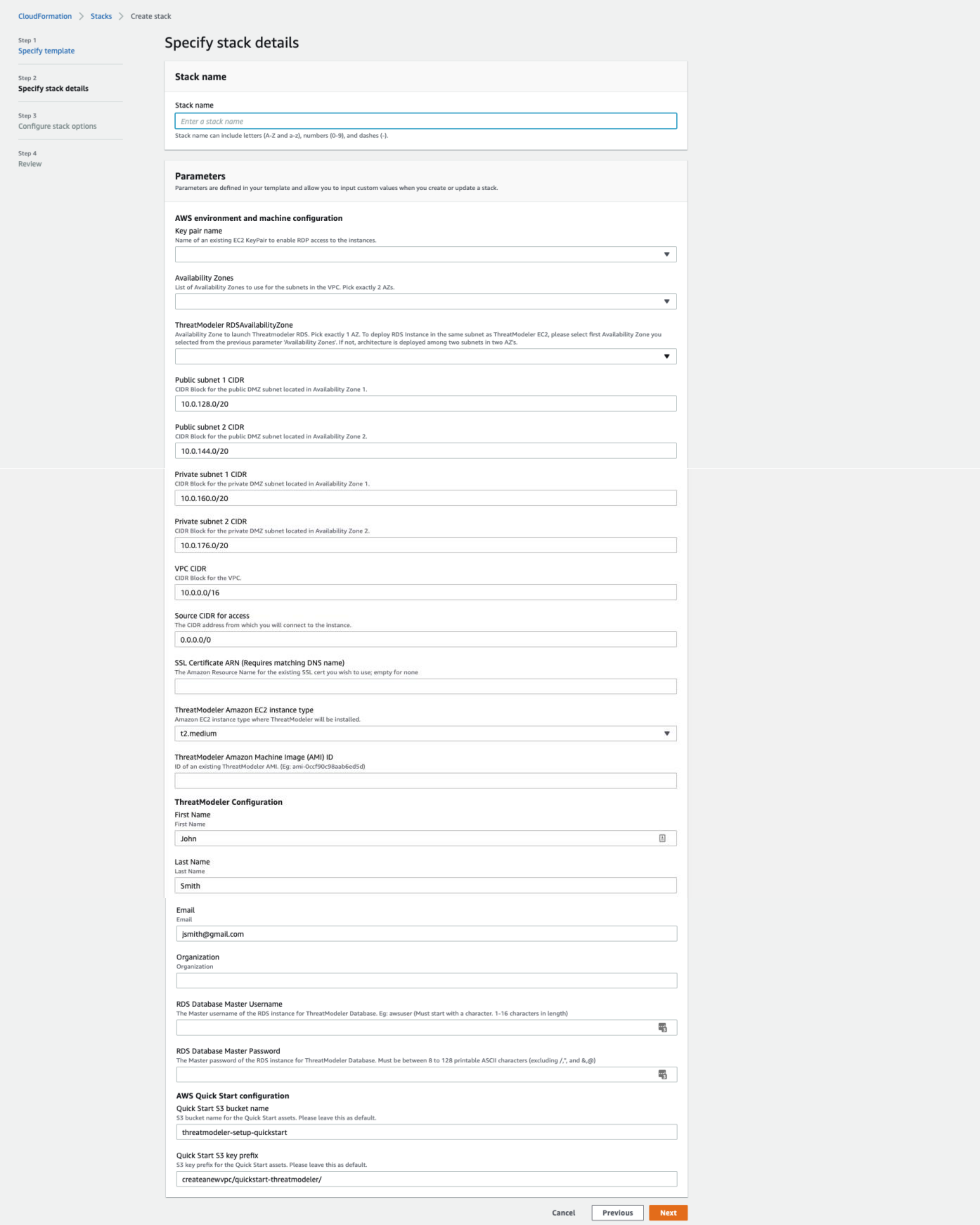
https://

Amazon S3 template URL

S3 URL: *Will be generated when URL is provided*

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

> https://threatmodeler-setup-quickstart.s3.amazonaws.com/createanewvpc/quickstart-threatmodeler/templates/threatmodeler-master.template



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.

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. Pick exactly 1 AZ. To deploy RDS Instance in the same subnet as ThreatModeler EC2, please select first Availability Zone you selected from the previous parameter 'Availability Zones'. If not, architecture is deployed among two subnets in two AZ's.

Public subnet 1 CIDR
CIDR Block for the public DMZ subnet located in Availability Zone 1.
10.0.128.0/20

Public subnet 2 CIDR
CIDR Block for the public DMZ subnet located in Availability Zone 2.
10.0.144.0/20

Private subnet 1 CIDR
CIDR Block for the private DMZ subnet located in Availability Zone 1.
10.0.160.0/20

Private subnet 2 CIDR
CIDR Block for the private DMZ subnet located in Availability Zone 2.
10.0.176.0/20

VPC CIDR
CIDR Block for the VPC.
10.0.0.0/16

Source CIDR for access
The CIDR address from which you will connect to the instance.
0.0.0.0/0

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.
t2.medium

ThreatModeler Amazon Machine Image (AMI) ID
ID of an existing ThreatModeler AMI. (Eg: ami-0ccf90c98aab6ed5d)

ThreatModeler Configuration

First Name
First Name
John

Last Name
Last Name
Smith

Email
Email
jsmith@gmail.com

Organization
Organization

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)

RDS Database Master Password
The Master password of the RDS instance for ThreatModeler Database. Must be between 8 to 128 printable ASCII characters (excluding /,", and &,@)

AWS Quick Start configuration

Quick Start S3 bucket name
S3 bucket name for the Quick Start assets. Please leave this as default.
threatmodeler-setup-quickstart

Quick Start S3 key prefix
S3 key prefix for the Quick Start assets. Please leave this as default.
createanewvpc/quickstart-threatmodeler/

5. 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	Optional	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. Defaults to t2.medium.
ThreatModeler Amazon Machine Image (AMI) ID	Requires Input	Amazon Machine ID Provided by ThreatModeler.

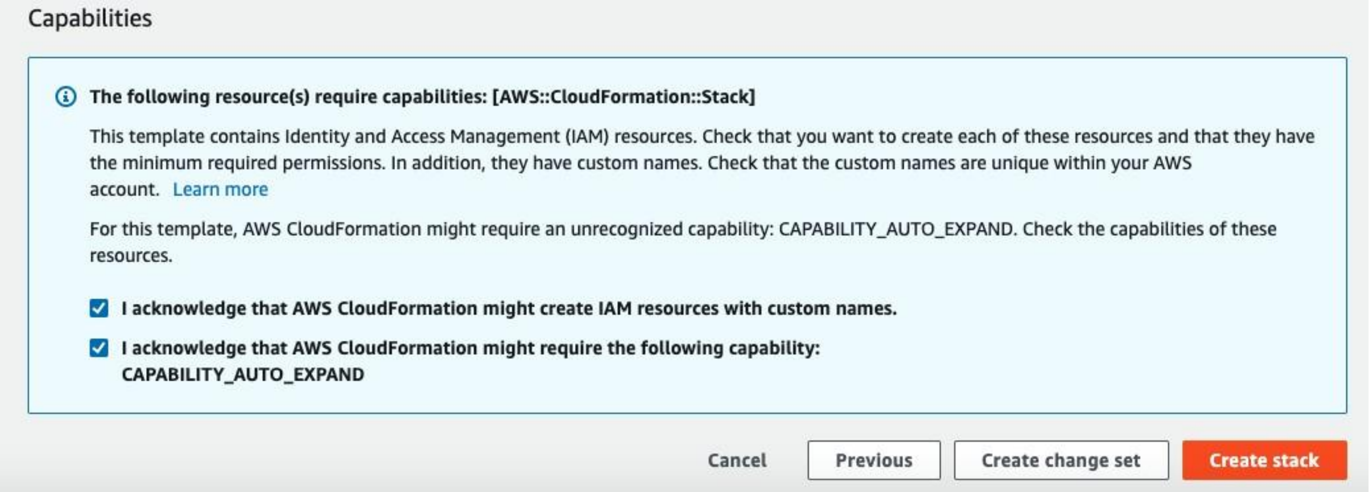
ThreatModeler Configuration

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	createanewvpc/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.

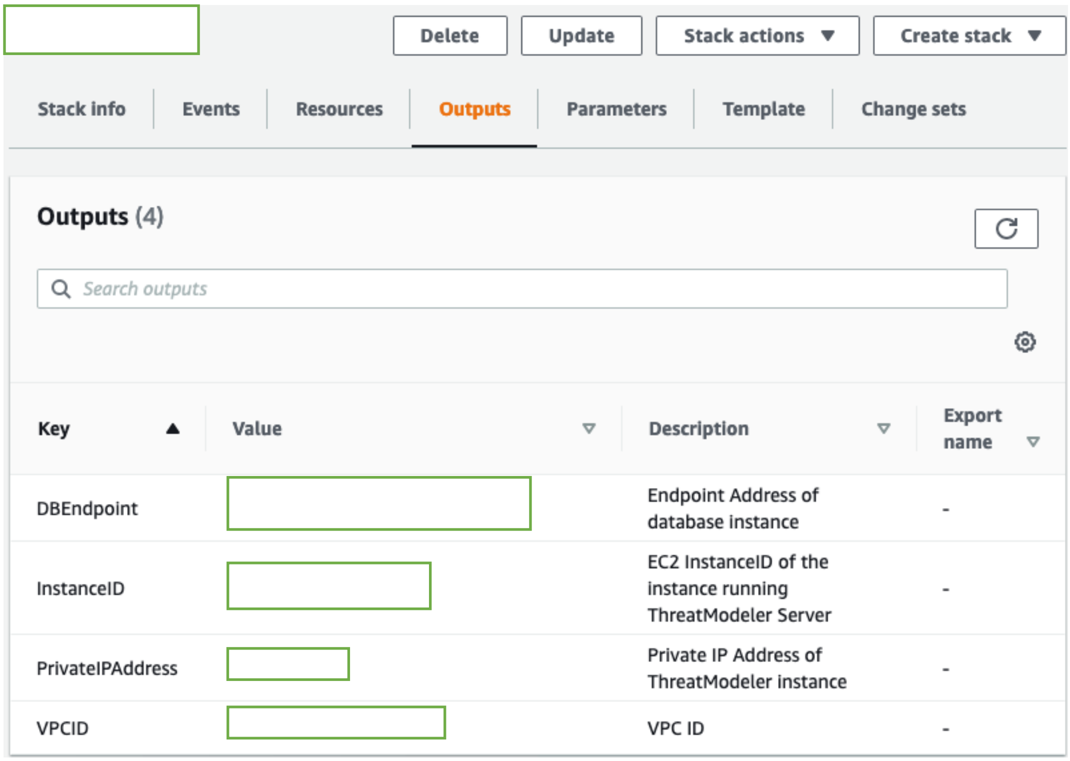
☑ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

☑ **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND**

- 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.



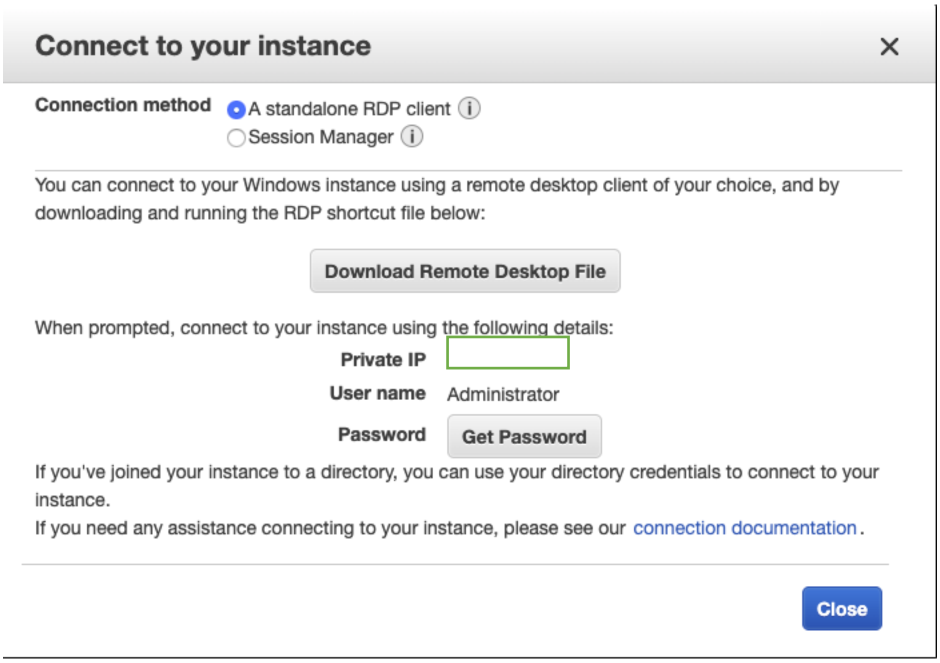
Outputs (4)

Key ▲	Value ▽	Description ▽	Export name ▽
DBEndpoint	[redacted]	Endpoint Address of database instance	-
InstanceID	[redacted]	EC2 InstanceID of the instance running ThreatModeler Server	-
PrivateIPAddress	[redacted]	Private IP Address of ThreatModeler instance	-
VPCID	[redacted]	VPC ID	-

Launching 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 Services → EC2 → Instances. Locate the instance starting with the Stack name you specified. Please copy private IP address of “****-ThreatModelerStack-****” instance we would need this information going ahead.
2. While “****-ThreatModelerStack-****” instance is selected Click on "Get Password" and then click on "Choose File."
3. Locate the KeyPair (.pem) file that you provided while launching the CloudFormation stack and upload it. Click on Decrypt Password and copy the password to your clipboard.
4. Select the “****-ThreatModelerStack -****” instance and click Connect at the top.



Connect to your instance ✕

Connection method ● A standalone RDP client ⓘ
○ Session Manager ⓘ

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

Private IP [redacted]

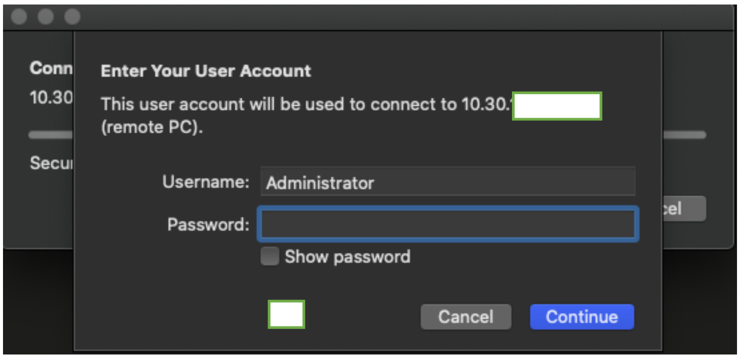
User name Administrator

Password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our connection documentation.

5. Click on "Download Remote Desktop File." This will download a file that will connect to the instance using a remote desktop client installed on your local desktop. Once downloaded, launch the Remote Desktop file and enter the password that you copied in step 3 into the client.



Enter Your User Account

This user account will be used to connect to 10.30.[redacted] (remote PC).

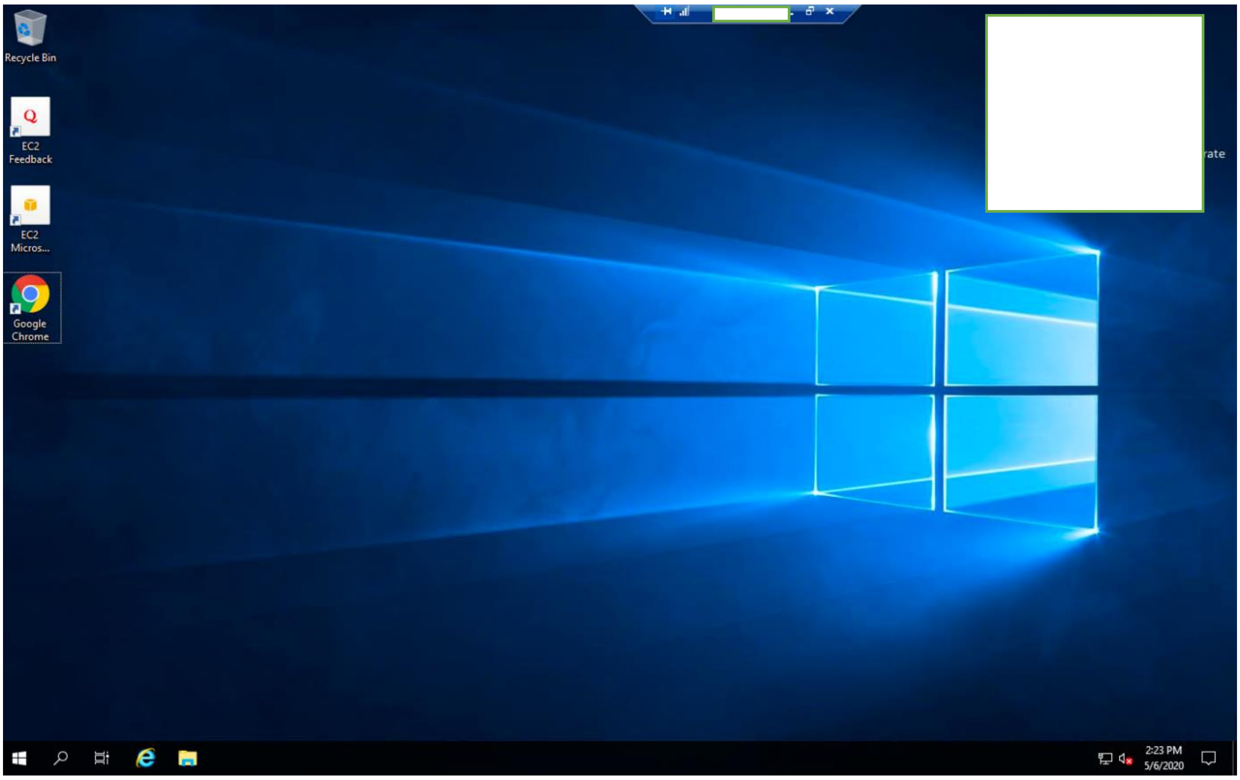
Username: Administrator

Password:

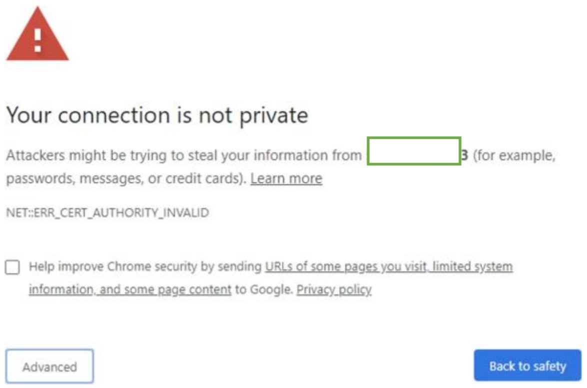
□ Show password

[redacted]

6. You should now see the Windows desktop of the instance (ThreatModeler server) to which you just connected.



7. Launch Google Chrome.
8. In the URL address bar, enter https://private-ip-address. (Copied in step 1. If you can't find it, you can also look at the Outputs section of your CloudFormation stack.)
9. You will encounter a security warning. This occurs due to not having an SSL certificate installed on the system. A self-signed SSL certificate is currently installed and this causes the error.



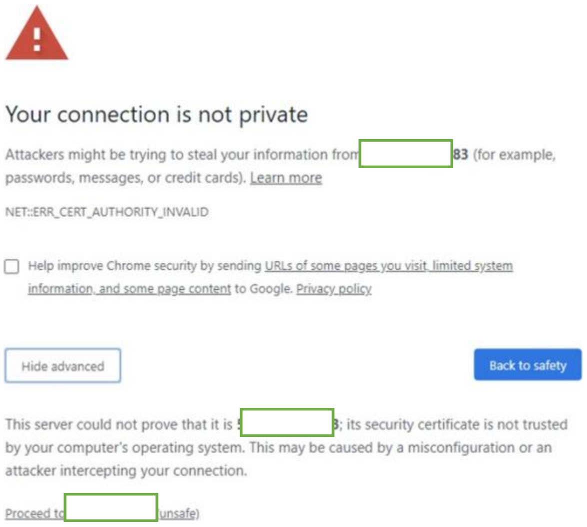
Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

10. Click on Advanced.



Your connection is not private

Attackers might be trying to steal your information from [redacted]83 (for example, passwords, messages, or credit cards). Learn more

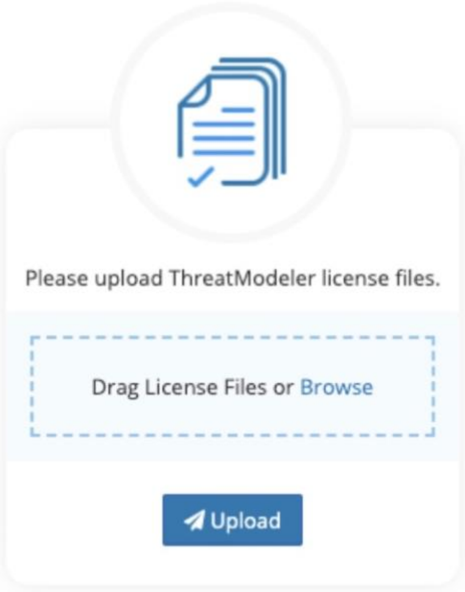
NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

This server could not prove that it is [redacted]3; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to [redacted] (unsafe)

11. Click on "Proceed to ... (unsafe)"
12. The first thing you see when you access ThreatModeler is a prompt to upload your License Files.



Please upload ThreatModeler license files.

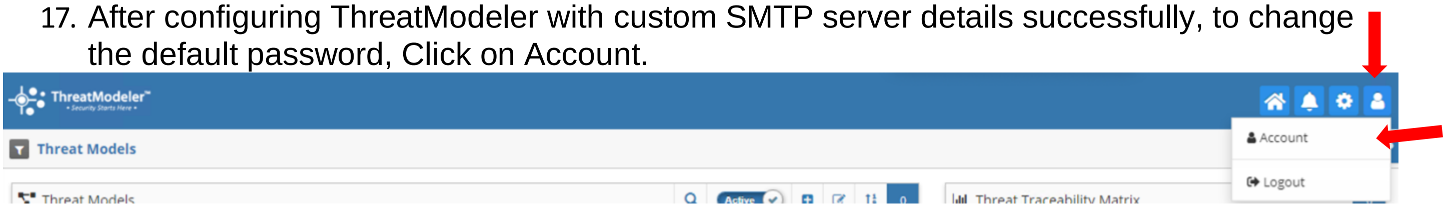
13. Logging into the ThreatModeler platform requires license files to be uploaded. Please open another tab and navigate to your Email inbox. Look for an email from ThreatModeler support (support@threatmodeler.com) with the license files.
14. We accept two types of licenses: Limited (Specific Count) and Unlimited (Site License).

- NOTE: For ThreatModeler licensing instructions please refer to section name "**ThreatModeler License Upload Instructions**"

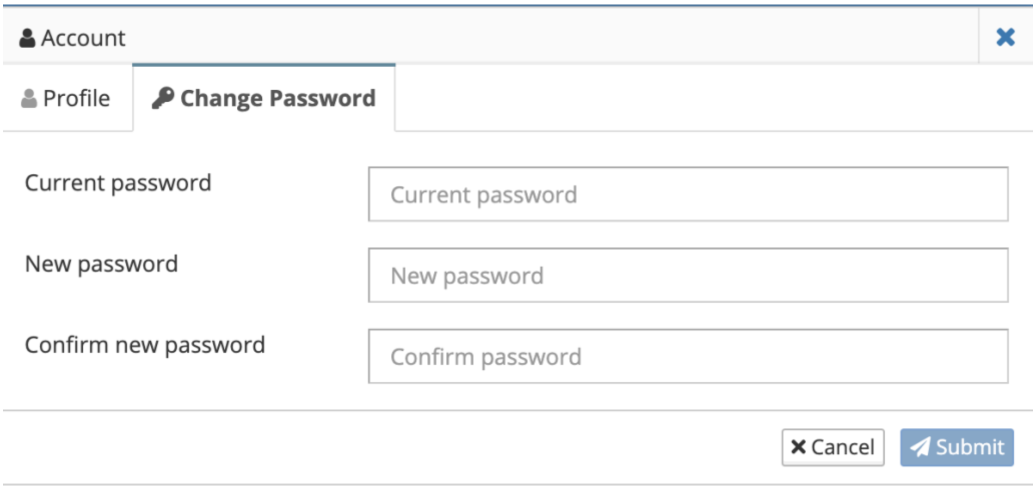
15. After successfully uploading ThreatModeler License files you should successfully logged into ThreatModeler platform.

16. As you are able to login to ThreatModeler platform, please configure ThreatModeler with your SMTP server details. For instructions please refer Setup SMTP*. This step is a must (before doing anything on ThreatModeler platform) for users to receive notifications on new user creation, reset/forgot password, licensing notifications.

17. After configuring ThreatModeler with custom SMTP server details successfully, to change the default password, Click on Account.

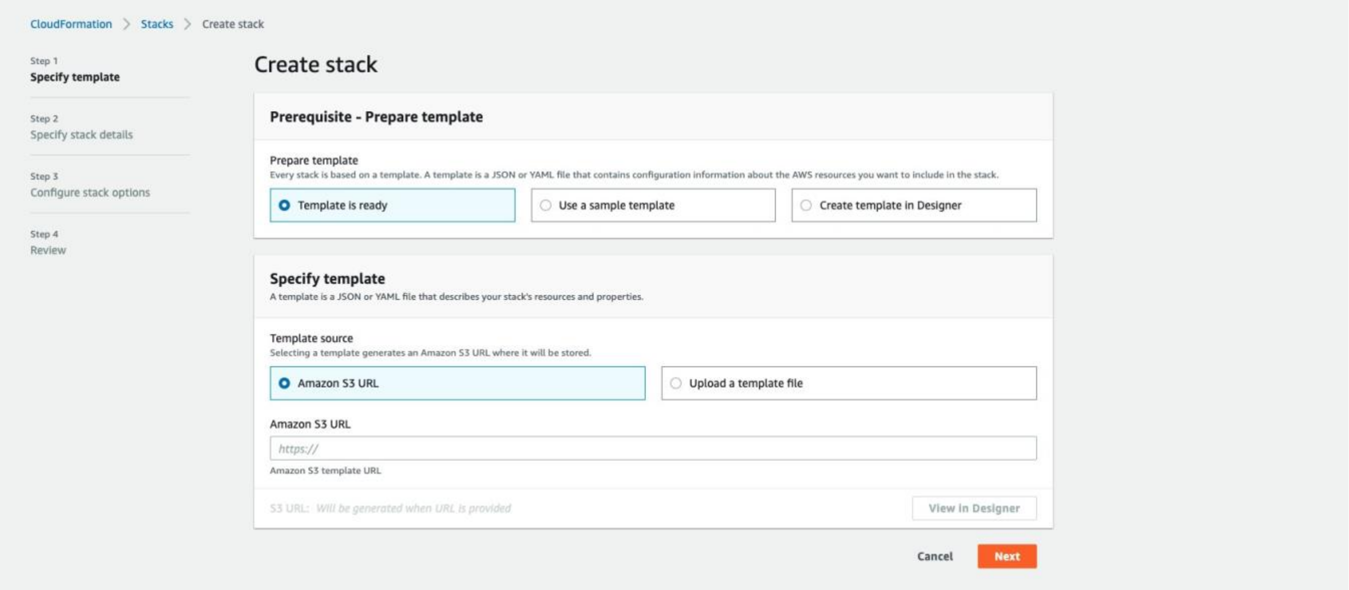


18. Click on Change Password. Enter "admin@123" (without the quotes) for current password. Enter a new password and click Submit.



Option 2: Deploy ThreatModeler on Microsoft Windows Server Into an Existing VPC

1. 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.
2. Select Services → CloudFormation → Stacks → Create Stack → With new resources (standard).



Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

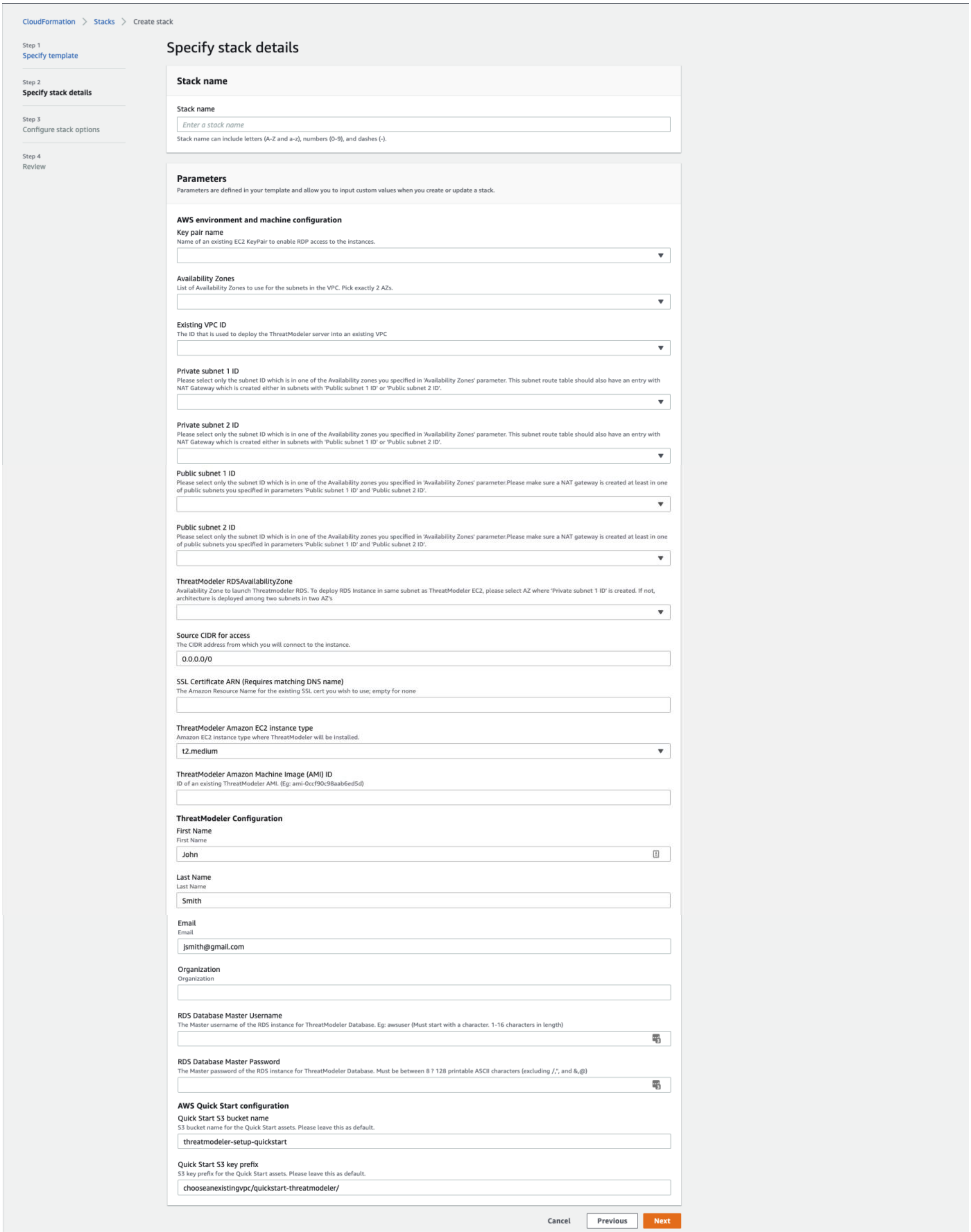
● Amazon S3 URL ○ Upload a template file

Amazon S3 URL
https://
Amazon S3 template URL

S3 URL: Will be generated when URL is provided

3. In the Specify template field, select Amazon S3 template URL to launch ThreatModeler Application in existing VPC.
4. Copy and paste the S3 template link into the field under Amazon S3 URL and click Next.

> https://threatmodeler-setup-quickstart.s3.amazonaws.com/chooseanexistingvpc/quickstart-threatmodeler/templates/threatmodeler-master.template



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.

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

The CIDR address from which you will connect to the instance.

0.0.0.0/0

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.

t2.medium

ThreatModeler Amazon Machine Image (AMI) ID

ID of an existing ThreatModeler AMI. (Eg: ami-0ccf90c98aab6ed5d)

ThreatModeler Configuration

First Name

First Name

John

Last Name

Last Name

Smith

Email

Email

jsmith@gmail.com

Organization

Organization

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)

RDS Database Master Password

The Master password of the RDS instance for ThreatModeler Database. Must be between 8 ? 128 printable ASCII characters (excluding /,", and &,@)

AWS Quick Start configuration

Quick Start S3 bucket name

S3 bucket name for the Quick Start assets. Please leave this as default.

threatmodeler-setup-quickstart

Quick Start S3 key prefix

S3 key prefix for the Quick Start assets. Please leave this as default.

chooseanexistingvpc/quickstart-threatmodeler/

5. 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	Optional	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. Defaults to t2.medium.
ThreatModeler Amazon Machine Image (AMI) ID	Requires Input	Amazon Machine ID Provided by ThreatModeler.

ThreatModeler Configuration

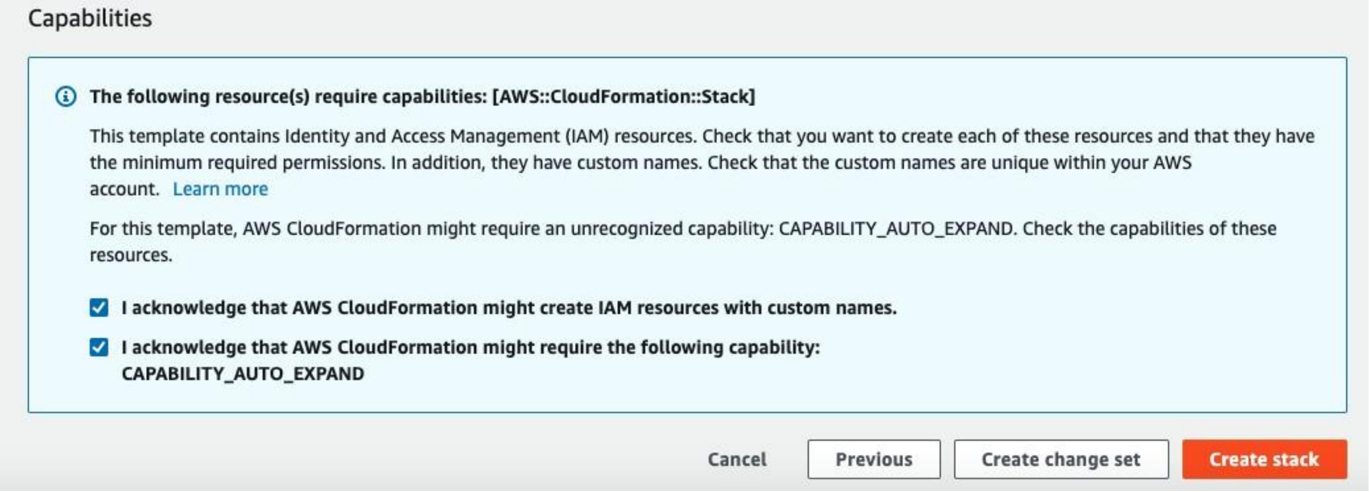
Parameter Label (Name)	Default	Description
First Name	Requires Input	First name of the customer used for creating the first user on ThreatModeler platform.
Last Name	Requires Input	Last name of the customer used for creating the first user on ThreatModeler platform.
Email	Requires Input	Valid email of 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	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.

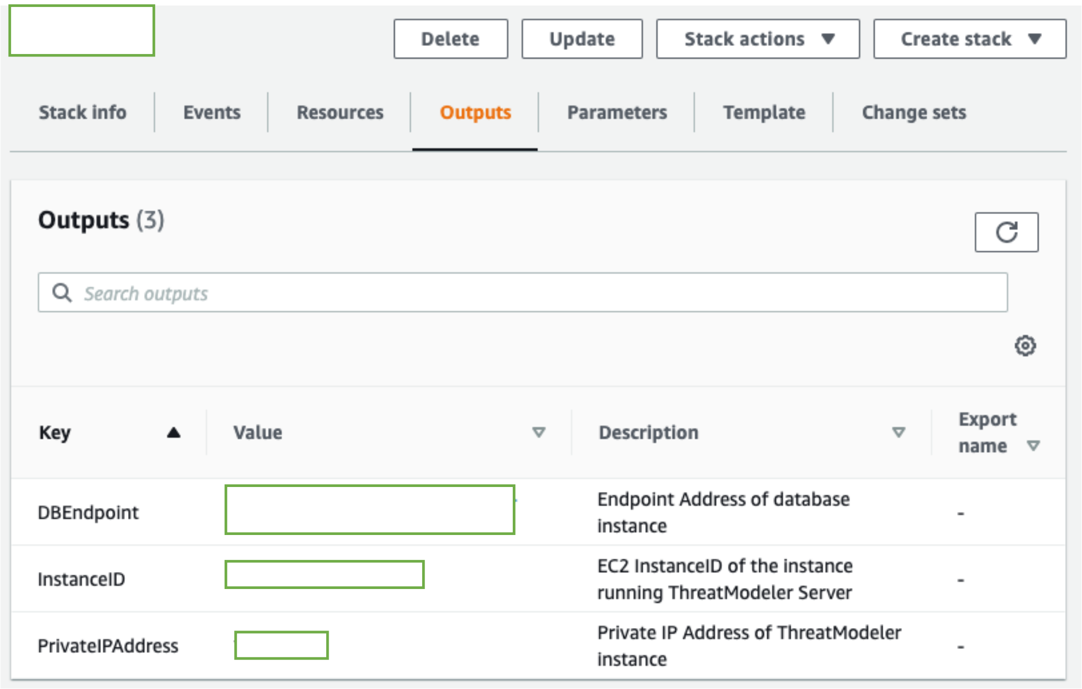
☑ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

☑ **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND**

- 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.



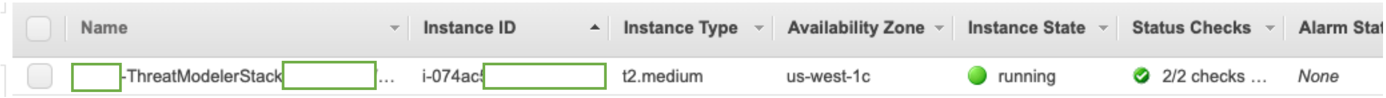
Outputs (3)

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	-

Launching ThreatModeler (When Deployed Into an Existing VPC)

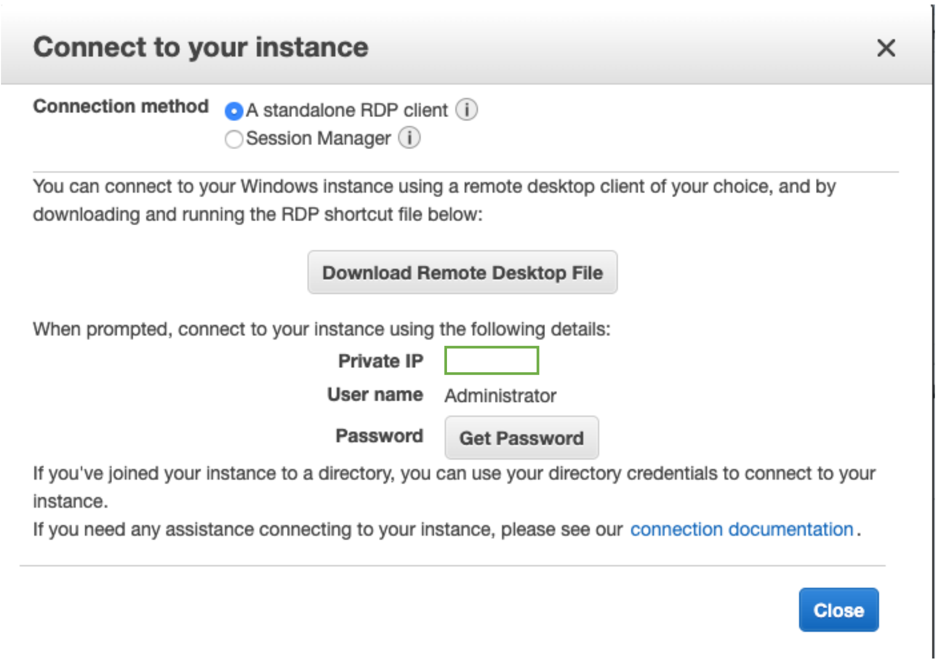
- Note: Assuming VPN connectivity is established (for connecting to instances in private subnet) for the VPC where ThreatModeler instance is created. If not, please create a Bastion-Host in public subnet to access the ThreatModeler instance created in private subnet.
- If VPN connectivity is already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

1. Go to Services → EC2 → Instances. Locate the instance starting with the Stack name you specified. Copy the private IP address of "****-ThreatModelerStack-****" instance.



□	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Stat
□	[redacted]-ThreatModelerStack[redacted]…	i-074ac[redacted]	t2.medium	us-west-1c	● running	✓ 2/2 checks …	None

2. While "****-ThreatModelerStack-****" instance is selected, click on "Get Password" and then click on "Choose File."
3. Locate the KeyPair (.pem) file that you provided while launching the CloudFormation stack and upload it.
4. Click on Decrypt Password and copy the password to your clipboard.
5. Select the "****-ThreatModelerStack-****" instance and click on Connect at the top.



Connect to your instance ✕

Connection method ● A standalone RDP client ⓘ
○ Session Manager ⓘ

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download Remote Desktop File

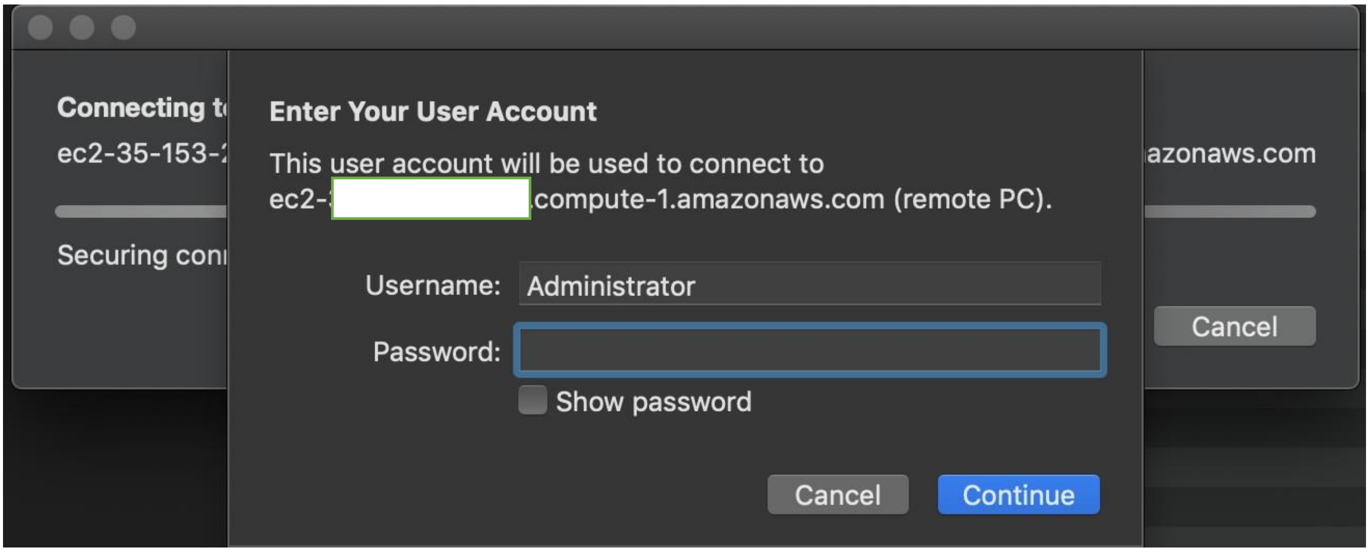
When prompted, connect to your instance using the following details:

Private IP [redacted]
User name Administrator
Password Get Password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
If you need any assistance connecting to your instance, please see our connection documentation.

Close

6. Click on "Download Remote Desktop File." This will download a file that will connect to the instance using a remote desktop client installed on your local desktop.
7. Launch the Remote Desktop File you downloaded in step 6 and enter the password that you copied in step 4 into the client.



Connecting t

ec2-35-153-

Securing con

azonaws.com

Cancel

Enter Your User Account

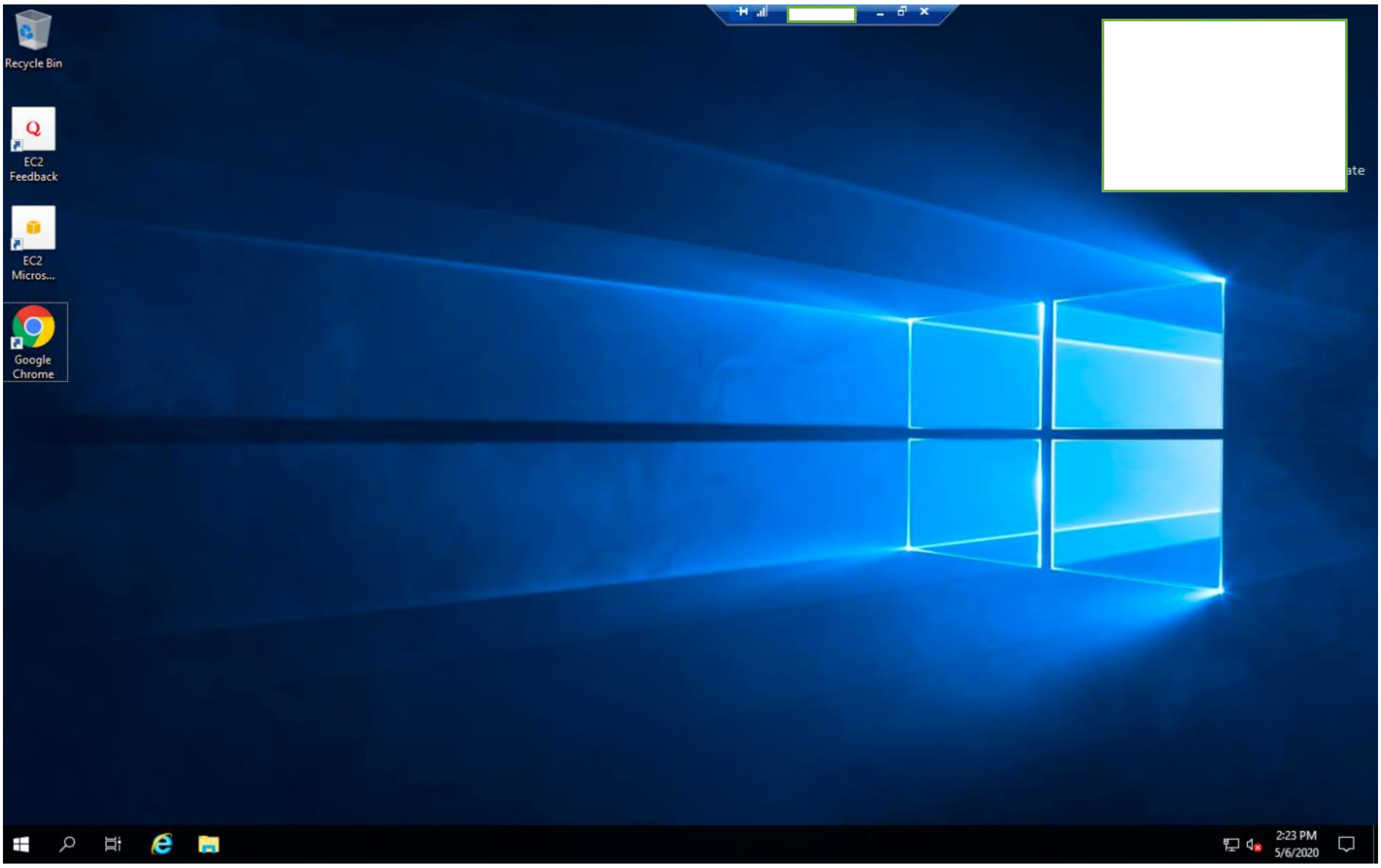
This user account will be used to connect to ec2-[redacted].compute-1.amazonaws.com (remote PC).

Username: Administrator

Password:

□ Show password

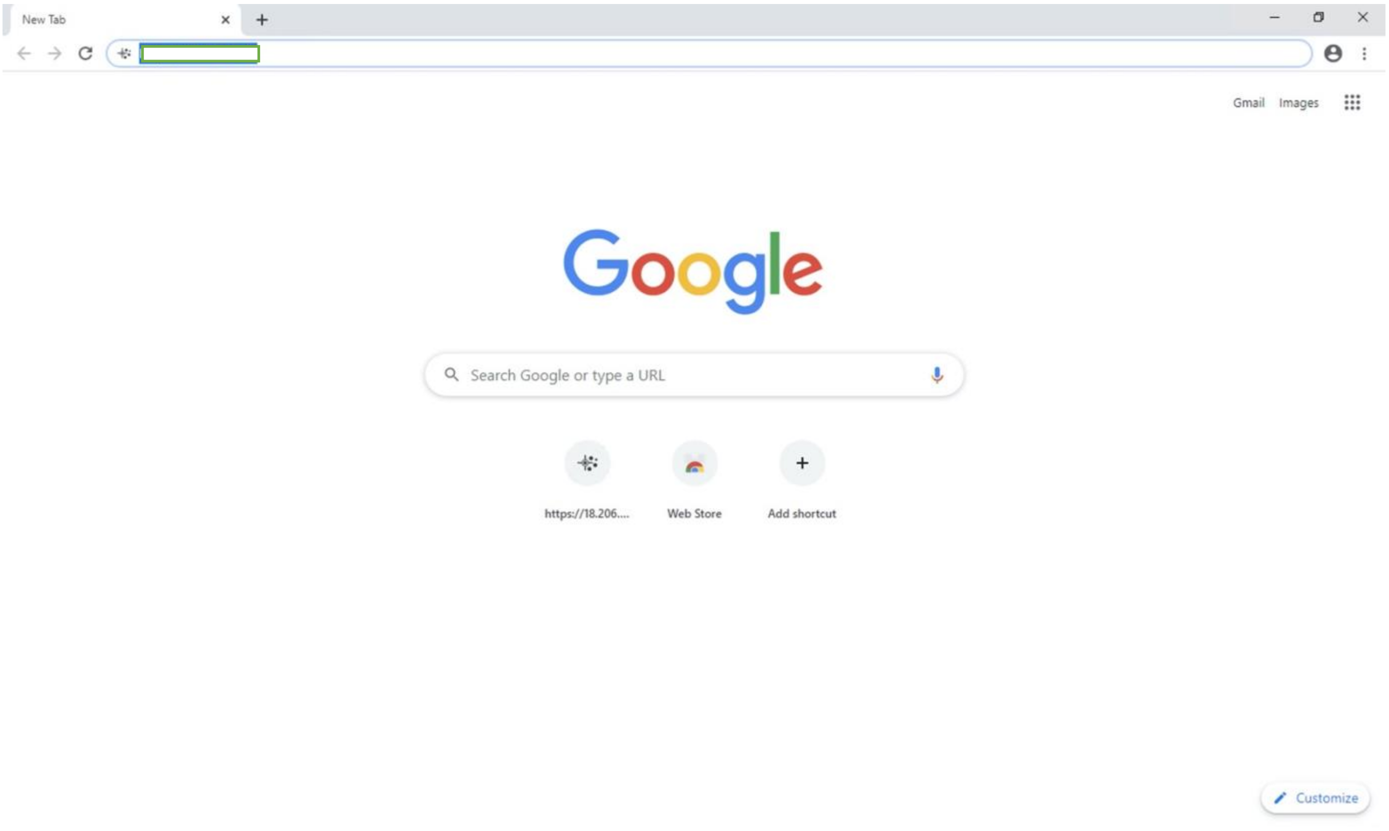
8. You should now see the Windows desktop of the instance to which you just connected.



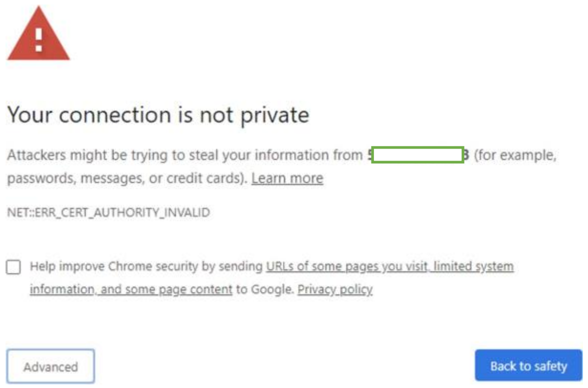
[redacted]

[redacted]

9. Launch Chrome.
10. In the URL address bar, enter https://private-ip-address. (Copied in step 1. If you can't find it, you can also look at the Outputs section of your CloudFormation stack.)



11. You will encounter a security warning. This occurs due to not having an SSL certificate installed on the system. A self-signed SSL certificate is currently installed and this causes the error.



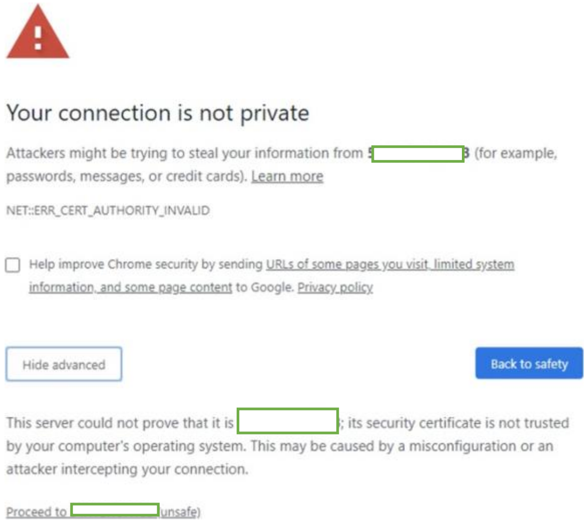
Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

12. Click on Advanced...



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

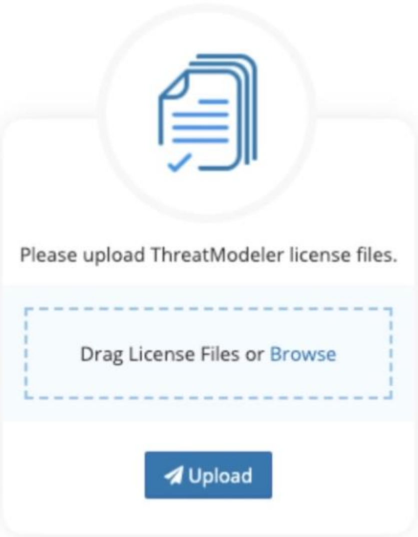
NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

This server could not prove that it is [redacted]; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to [redacted]unsafe)

13. Click on "Proceed to ... (unsafe)"
14. The first thing you see when you access ThreatModeler is a prompt to upload your License Files.



Please upload ThreatModeler license files.

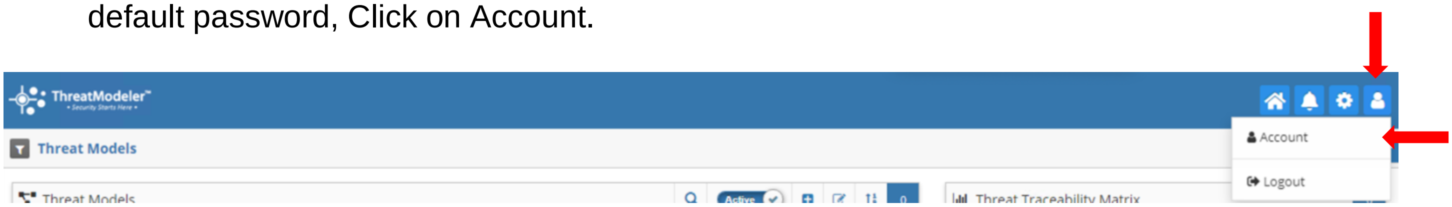
Drag License Files or Browse

15. To log into the ThreatModeler platform license files are required 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.

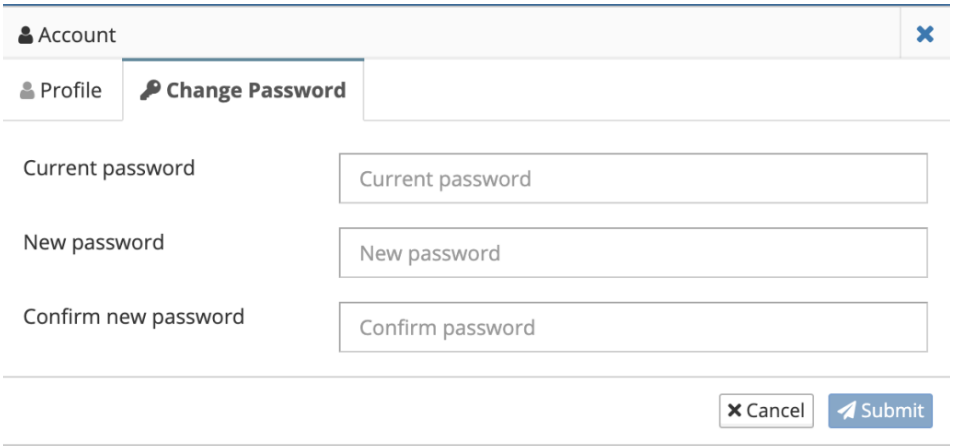
16. We accept two types of licenses: Limited (Specific Count) and Unlimited (Site License).

- NOTE: For ThreatModeler licensing instructions please refer to section name “**ThreatModeler License Upload Instructions**”

17. After successfully uploading ThreatModeler License files you should successfully logged into ThreatModeler platform.
18. As you are able to login to ThreatModeler platform, please configure ThreatModeler with your SMTP server details. For instructions please refer Setup SMTP*. This step is a must (before doing anything on ThreatModeler platform) for users to receive notifications on new user creation, reset/forgot password, licensing notifications.
19. After configuring ThreatModeler with custom SMTP server details successfully, to change the default password, Click on Account.



20. Click on Change Password. Enter "admin@123" (without the quotes) for the current password. Enter a new password and click Submit.

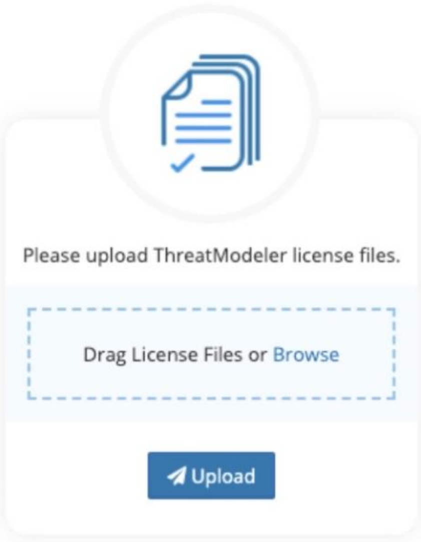


ThreatModeler License Upload Instructions

1. We accept two types of licenses: Limited (Specific Count) and Unlimited (Site License).

Limited (Specific Count): This licensing model allows you to create limited number of ThreatModels based on licenses you purchased from ThreatModeler.

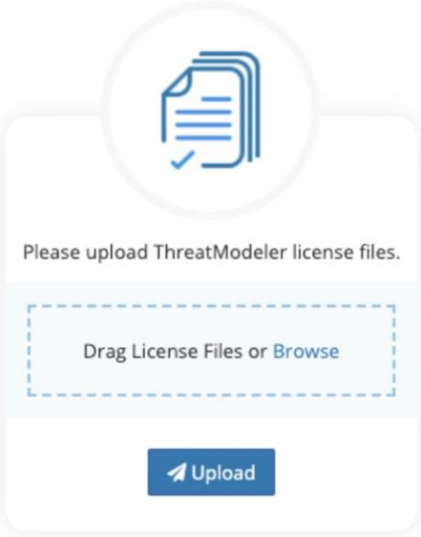
- For limited licensing model you should have three files to access ThreatModeler:
    - tm.lic – file used by ThreatModeler
    - validation key.txt – validates the above .lic file
    - tm-lic-{license-count}.txt – file used by ThreatModeler for licensing ThreatModels (This file will only exist for **ThreatModeler Limited (Specific Count) licensing model**).
        - Example: If you purchase 5 licenses this file will be named as tm-lic-5.txt
- As you see the screen below, please click on upload and upload ***tm.lic*** and ***validation key.txt*** files. (***tm-lic-{license-count}.txt file*** **will be uploaded after logging into the ThreatModeler platform, please look into steps 5,6,7**).



Please upload ThreatModeler license files.

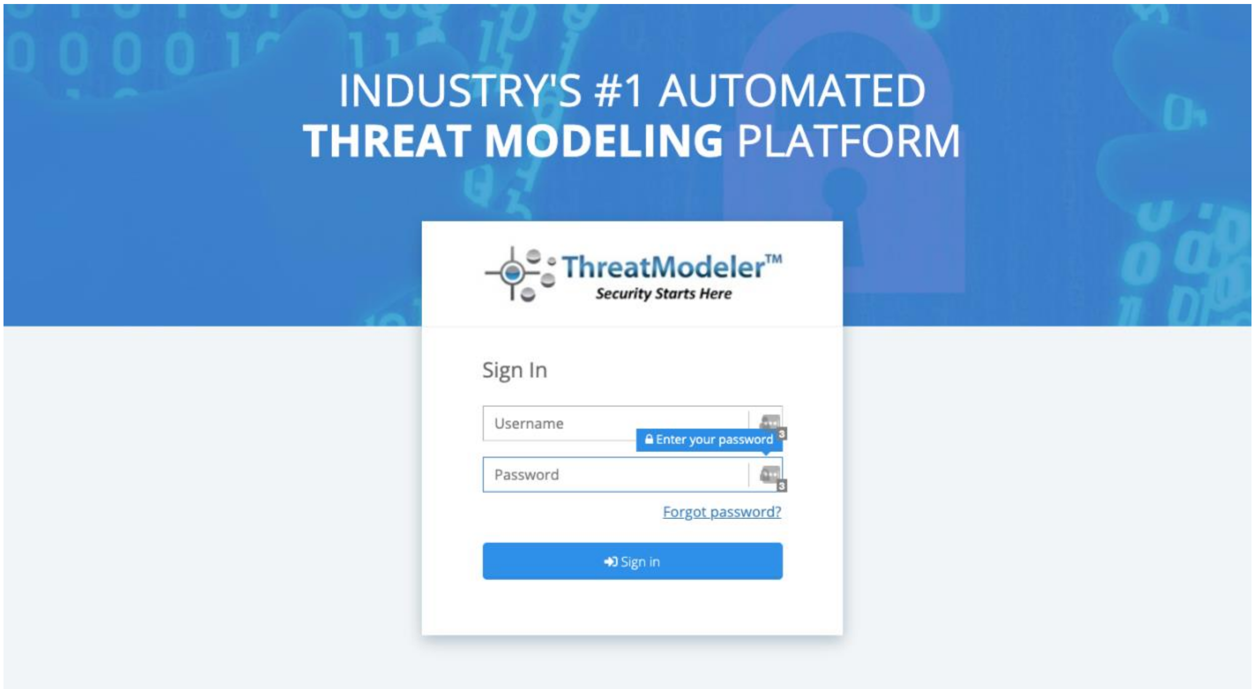
Unlimited (Site License): This licensing model allows you to create an unlimited number of ThreatModels. For this licensing model please **skip through the steps 5,6,7** mentioned below as they are applicable only for **ThreatModeler Limited (Specific Count) licensing model.**

- For the unlimited licensing model, you should have two files to access ThreatModeler:
  - tm.lic – file used by ThreatModeler
  - validation key.txt – validates the above .lic file
- As you see the screen below, please click on upload and upload the ***tm.lic*** and ***validation key.txt*** files.



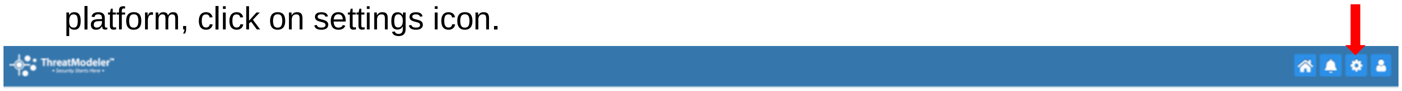
Please upload ThreatModeler license files.

2. You should see a success message with the page redirected to a login page.

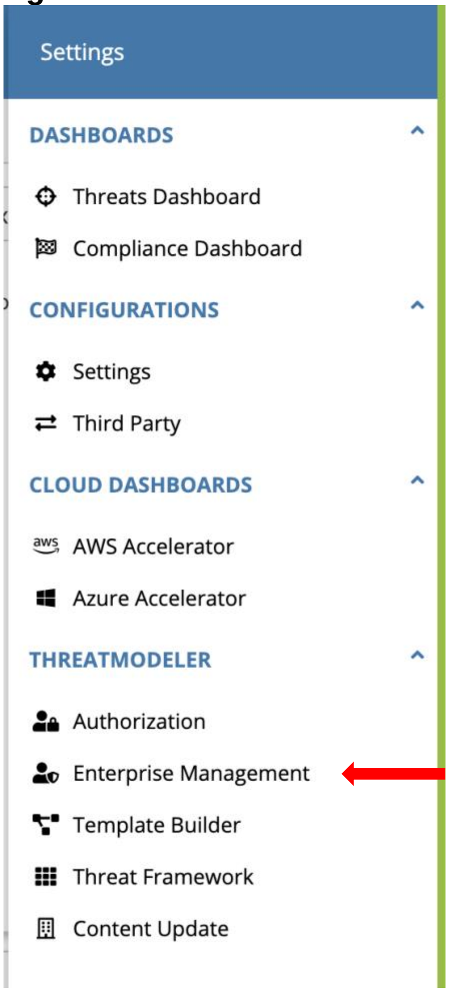


3. Use the same email-id provided while launching CloudFormation stack and the password as "admin@123" (without the quotes) to login to the platform.

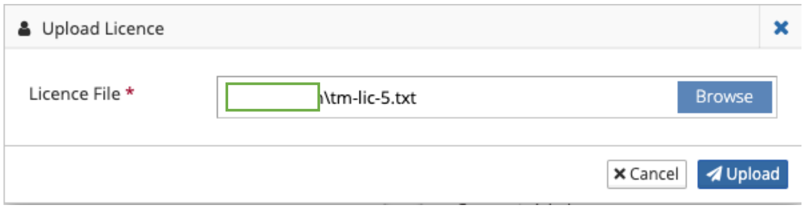
4. After logging successfully into platform, please click Accept on “**License Agreement**” page and you will be navigated to the ThreatModeler landing page.
5. For **ThreatModeler Limited (Specific Count) licensing model,** tm-lic-{license-count}.txt file needs to be uploaded within the platform as mentioned in step 1. To upload license file into the platform, click on settings icon.



6. Select “**Enterprise Management**” from the slider window.



7. From the Enterprise Management screen, click the “+” symbol in the Licenses section and upload tm-lic-{license-count}.txt file. After you successfully upload the license file you should see a message saying “ThreatModeler Licenses Uploaded Successfully.”


Upload Licence

Licence File * \tm-lic-5.txt

AWS Multi Account Deployment

Configure Multi-Account Setup

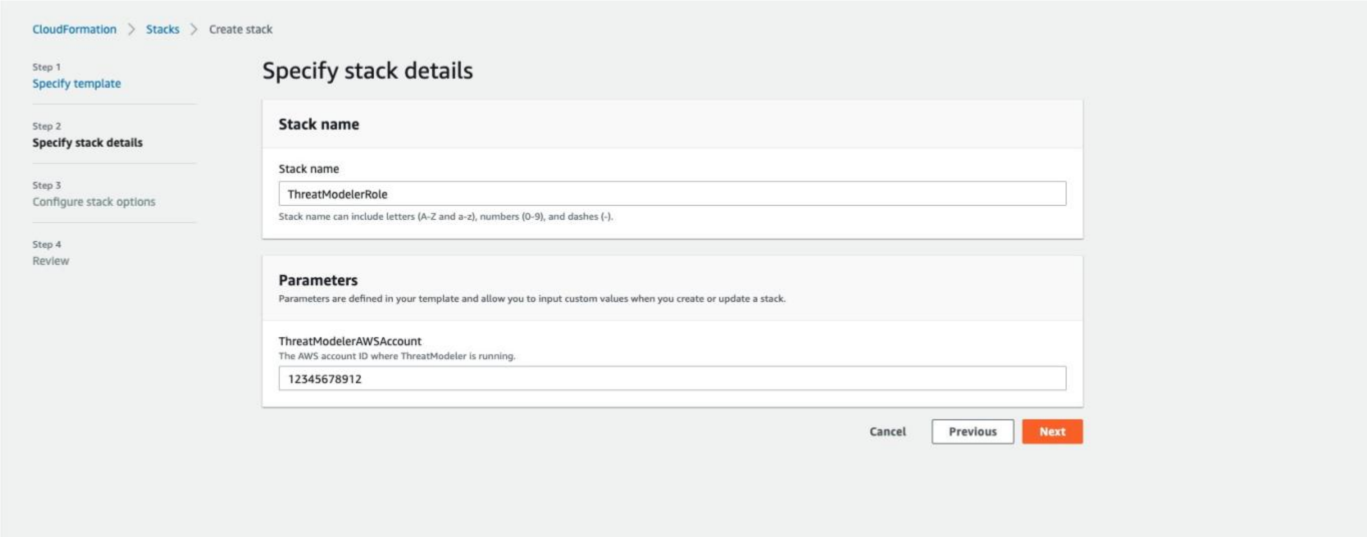
Note: For multi-account setup, your accounts need to be a part of an AWS Organization.

Deploy AWS Organizations Master Read-only Role

1. Login to the Master account in AWS Organizations.
2. Select Services → CloudFormation → Stacks → Create Stack → With new resources (standard).
3. Select Specify an Amazon S3 template URL.
4. Copy and paste the following S3 template link into the page and click Next.

> https://threatmodeler-setup-quickstart.s3.amazonaws.com/createanewvpc/cross-account/master-org-readonly.template

5. Enter the AWS Account ID where the ThreatModeler Application was deployed.



Specify stack details

Stack name

Stack name: ThreatModelerRole

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.

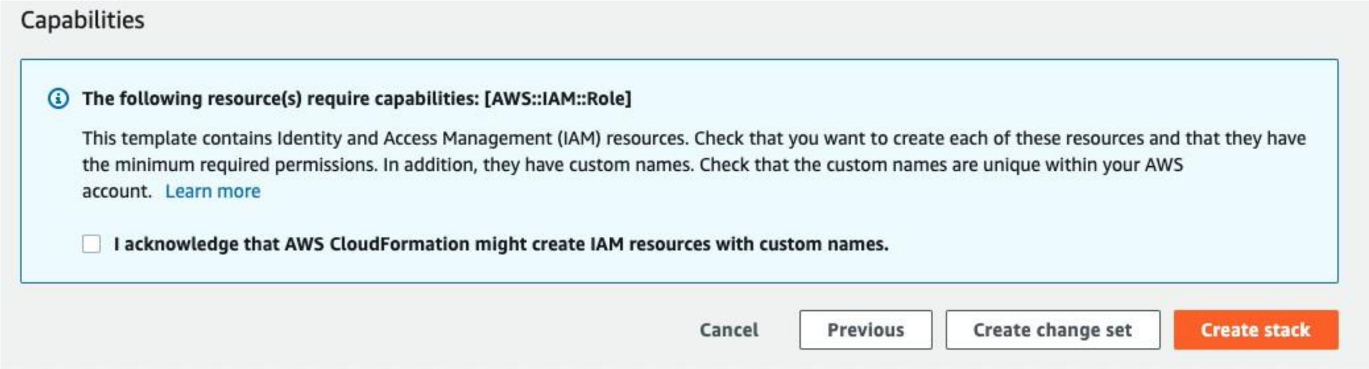
ThreatModelerAWSAccount

The AWS account ID where ThreatModeler is running.

12345678912

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."



Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

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

□ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

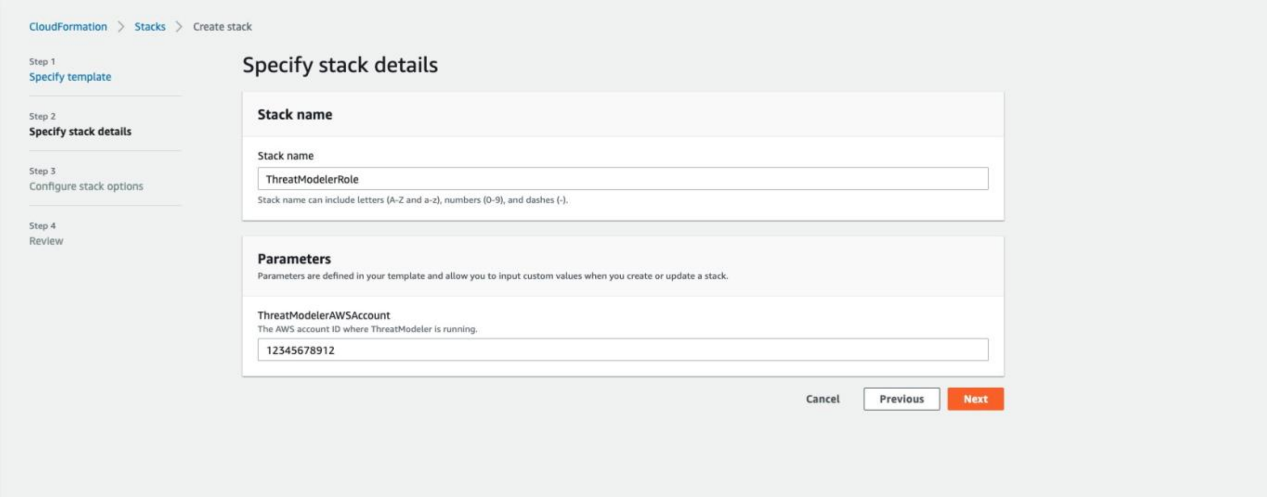
8. Click Create Stack.

Allowing Read-Only Access to Each Account for Which You Want to Build Threat Models

1. Login to the member AWS accounts that are part of your AWS Organization.
2. Select Services → CloudFormation → Stacks → Create Stack → With new resources (standard).
3. Select Specify an Amazon S3 template URL.
4. Copy and paste the following S3 template link into the page and click Next.

   > https://threatmodeler-setup-quickstart.s3.amazonaws.com/createanewvpc/cross-account/readonly-execution.template

5. Enter the AWS Account ID where the ThreatModeler Application was deployed.



Specify stack details

Stack name

Stack name: ThreatModelerRole

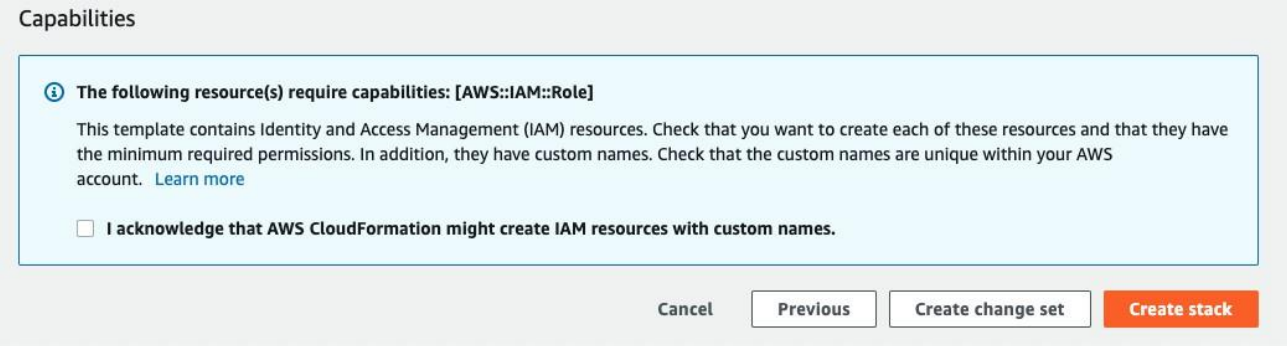
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

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

ThreatModelerAWSAccount
The AWS account ID where ThreatModeler is running.
12345678912

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."



Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

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

□ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**

8. Click Create Stack.

ThreatModeler Configuration

Note: Keys ending with * are mandatory fields.

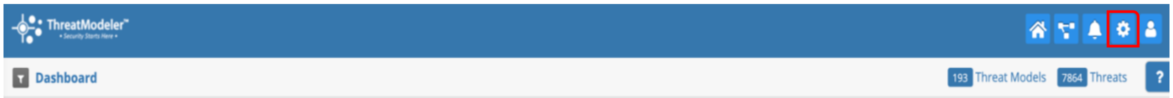
Setup SMTP*

Please setup ThreatModeler with your custom SMTP server details so that:

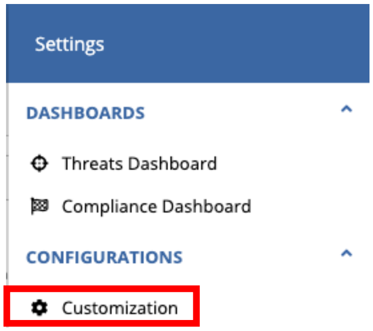
- New User creation will be successful followed by a notification sent to that user with the ThreatModeler platform information.
- Users should be able to use reset/forgot password features.
- ThreatModeler license consumption notifications will be enabled.

Set up how you handle communications within your system.

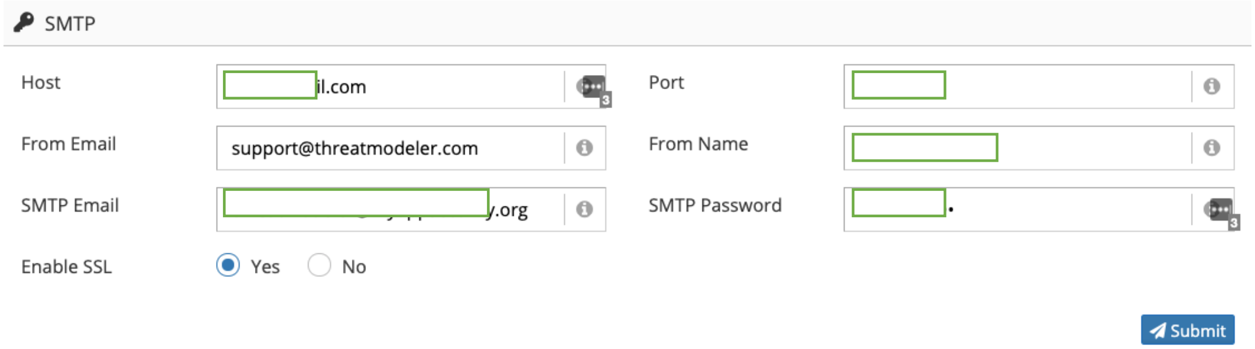
1. Click on the Settings icon in the Primary Navigation bar.



2. Click on Customization.



3. Fill in the details for SMTP setup.


SMTP

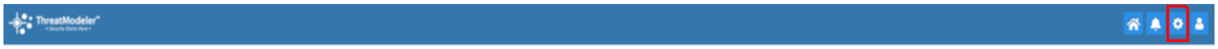
Host	[redacted]il.com	Port	[redacted]
From Email	support@threatmodeler.com	From Name	[redacted]
SMTP Email	[redacted]y.org	SMTP Password	[redacted]•
Enable SSL	● Yes ○ No		

Host – your email provider. Yahoo and Gmail, for example, are email providers. You can also have your own email provider.
From Name – the name with which you want to send an email
SMTP Email and Password – the login credentials you use to send emails on your Host account.
Enable SSL
Port – SMTP requires a port to be opened on your system for communication.

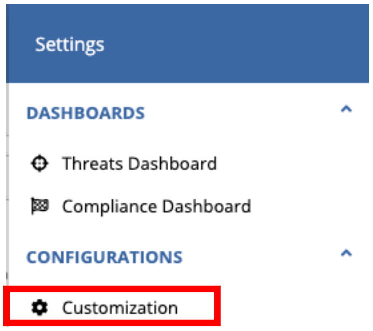
To restart IIS server please refer to Restart IIS Server section.

Setup SSO

1. Click on the Settings icon in the Primary Navigation bar.



2. Click on Customization.

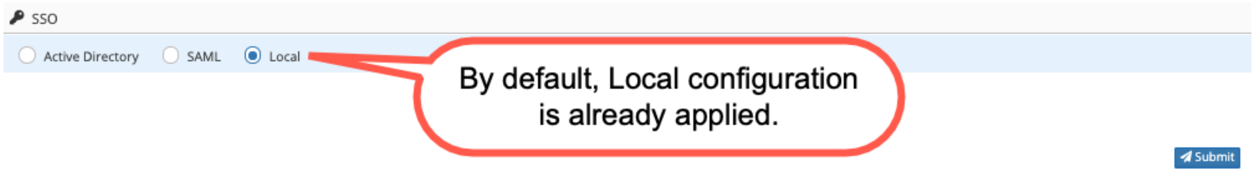


Configuration items are the most basic structural unit of a configuration management system. The login work is delegated to what types of access an individual user needs, e.g., write, read write, etc.

Federated Access and SAML-based Federation

Select the SSO method you would like to use, based on your IT infrastructure needs. There are three supported login types:

- Active directory (AD) login – an enterprise level login. ThreatModeler integrates with a user's AD Group. AD login is also used to manage access to multiple devices.
- Local login – the local database verifies the login information. By default, local configuration is applied.
- SAML – ThreatModeler integrates with Okta, which is a SAML compliant Identity Provider for single sign on.



SSO

○ Active Directory ○ SAML ● Local

By default, Local configuration is already applied.

SSO Login for Active Directory

Note: For the following details please reach out to your internal team responsible for managing your Active Directory.

In order to configure **Active Directory**, ThreatModeler will require the following information:

AD Connection String* – The connection string is made up of the LDAP server's name, and the fully qualified path of the container object where the user specified is located.

- *(LDAP://domain-controller/dc=ad,dc=local).*

AD Directory Filter By* – Allows to filter user's information in the active directory server.

- *As of now, Threat Model platform only support "**sAMAccountName"** or "**uid"** as LDAP filter.*

AD Group for Corporate Access – Name of the group inside the active directory server to which, if the current user belongs then that user should be added under the corporate group of the ThreatModeler platform.

- *User **ABC** belongs to Dept **XYZ** in Active Directory. When the user **ABC** tries to access ThreatModeler platform for the first time, If **AD** is set as default authentication and **XYZ** is set as **AD Group for corporate access** then user **ABC** will be created with corporate access inside ThreatModeler*.

- NOTE: For user to have **Corporate Access**, that user must be also part of group mentioned in **Default AD Group.** If user who is trying to logon to ThreatModeler exists only in group mentioned for Corporate Access but not existing in group mentioned for Default AD group, then user won't be able to login to platform.

AD Service Account Username/ Password – Active Directory support's service account authentication. If enabled, the incoming users will be authenticated against that service account username and password.

Is there is any service account authentication required?

If yes, please provide following information:

1. ADServiceAccountUsername
2. ADServiceAccountPassword

Default AD Group* – Name of the group to which all users belong. Only the users in this group will have access to ThreatModeler platform.

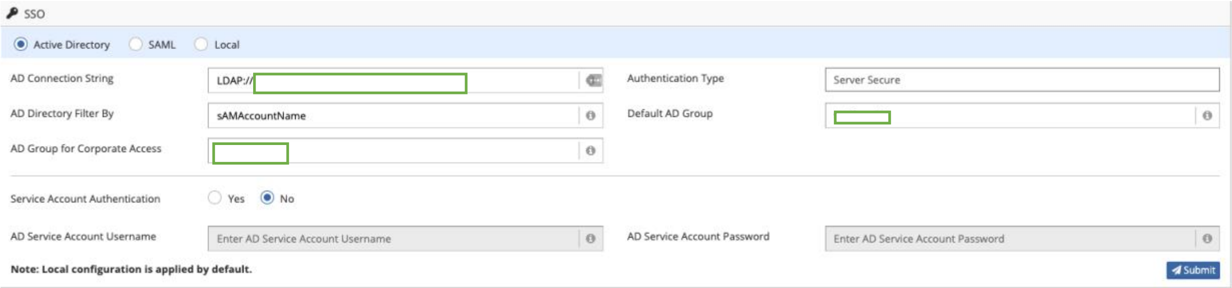
- *User **ABC** belongs to group **JKL** in Active Directory. When the user **ABC** tries to access ThreatModeler platform for the first time, If **AD** is set as default authentication and **JKL** is set as **Default AD Group**, then user **ABC** will be able to access ThreatModeler*.

- *If User **XYZ** doesn't belong to group **JKL** in Active Directory, then user **XYZ** will be denied access to ThreatModeler platform when s/he tries to log in.*

- *User **ABC** belongs to Dept **XYZ** and **JKL** in Active Directory. When the user **ABC** tries to access ThreatModeler platform for the first time, If **AD** is set as default authentication; **JKL** is set as **Default AD Group;** and **XYZ** is set as **AD Group for corporate access;** then user **ABC** will be created with corporate access inside ThreatModeler*.

Authentication Type* – Type of authentication supported by your **AD** server.

- *As of now, ThreatModeler platform only supports* ***ServerBind*** *and* ***Secure*** *as authentication Type.*



SSO

● Active Directory ○ SAML ○ Local

AD Connection String	LDAP://	Authentication Type	Server Secure
AD Directory Filter By	sAMAccountName	Default AD Group	
AD Group for Corporate Access			

Service Account Authentication ○ Yes ● No

AD Service Account Username	Enter AD Service Account Username	AD Service Account Password	Enter AD Service Account Password

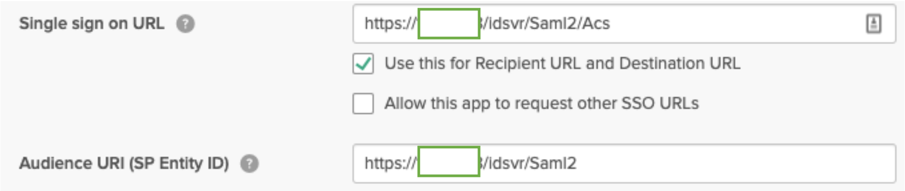
Note: Local configuration is applied by default.

To restart IIS server please refer to Restart IIS Server section.

SSO Login for SAML

Okta, a cloud user identity authentication program, is optional to use with SAML for secure login. Users input Properties to verify a user's admin. We check the user against three required properties – first name, last name and email. If any of the required information is missing, the user will be denied access and receive an Invalid login prompt.

- **Audience URI (SP Entity ID)** for ThreatModeler is: "**https://yoururl/idsvr/Saml2**"
- **Single sign on URL** for ThreatModeler is: "**https://yoururl/idsvr/Saml2/Acs**"



Single sign on URL: https:// /idsvr/Saml2/Acs

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

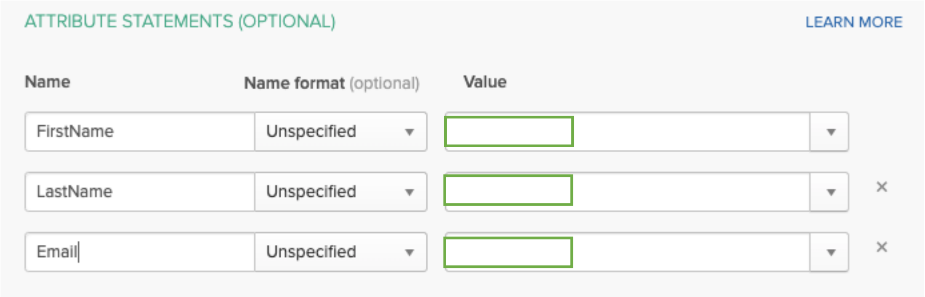
Audience URI (SP Entity ID): https:// /idsvr/Saml2

Identity ID* – Provide SAML **Identity Provider Issuer** URL.

Sample URL: *http://www.okta.com/exkh74a746KUleirN0h7*

Properties* – are the attribute statements in SAML.

ThreatModeler Requires **FirstName**, **LastName**, **Email** from the Identity provider.
(Please set the Name of the claims as **FirstName**, **LastName** & **Email**)

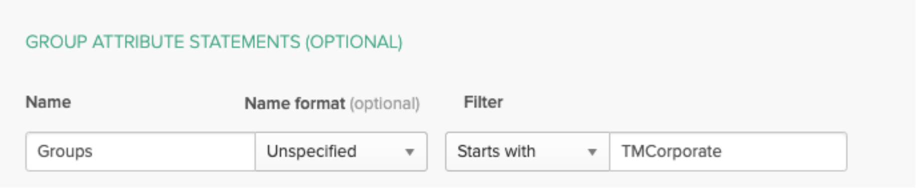


ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Value
FirstName	Unspecified	
LastName	Unspecified	
Email	Unspecified	

SAML Group property – refers to the name attribute of SAML Group Attribute Statements.

Ex: From the picture below **SAML Group property** should be "**Groups"**



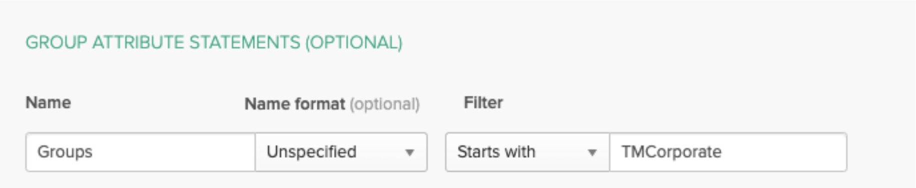
GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
Groups	Unspecified	Starts with	TMCorporate

SAML Group for Corporate Access – name of the group configured in SAML to which, if the current user belongs, then that user should be added under corporate group of ThreatModeler platform.

- *User **ABC** belongs to Dept **XYZ** in SAML. When the user **ABC** tries to access ThreatModeler platform for the first time, If **SAML** is set as default authentication; and **XYZ** is set as **SAML Group for Corporate access;** then user **ABC** will be created with corporate access inside ThreatModeler*.

Ex: From the picture below **SAML Group for Corporate Access** should be **“TMCorporate”**



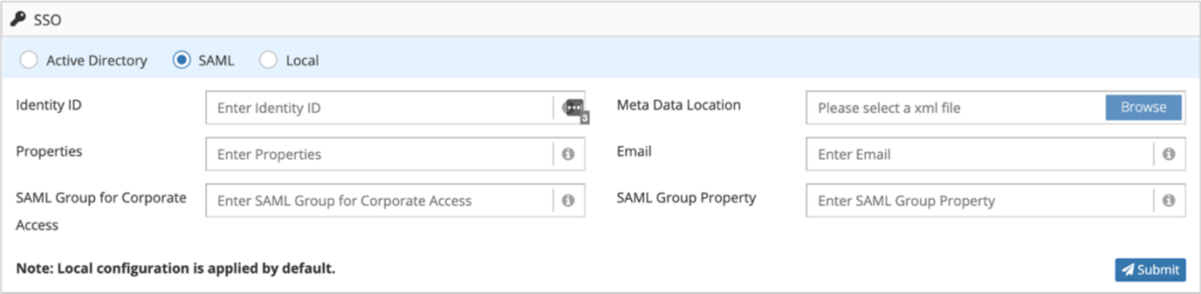
GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
Groups	Unspecified	Starts with	TMCorporate

Meta Data Location* **–** Identity provider metadata file in xml format.

Email* **–** Property that defines email.

Example – The name of the claim that defines email, it should be **Email**



SSO

○ Active Directory ● SAML ○ Local

Identity ID	Enter Identity ID	Meta Data Location	Please select a xml file [Browse]
Properties	Enter Properties	Email	Enter Email
SAML Group for Corporate Access	Enter SAML Group for Corporate Access	SAML Group Property	Enter SAML Group Property

Note: Local configuration is applied by default.

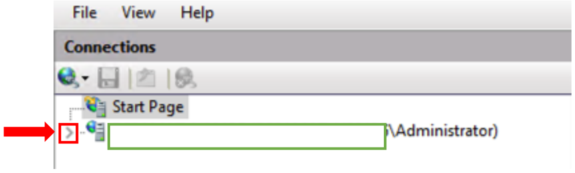
To restart IIS server please refer to Restart IIS Server section.

- **NOTE**:
    - If you are configuring ThreatModeler with SAML for logging into ThreatModeler platform you need to have following entities added in your SAML application (For accessing ThreatModeler)
        - **Audience URI (SP Entity ID)** for ThreatModeler is: ***https://yoururl/idsvr/Saml2***
            - **Audience URI when accessing ThreatModeler on Private IP address**
                - **Ex:** *https://10.0.0.132/idsvr/Saml2*
            - **Audience URI when accessing ThreatModeler on Custom Hostname**
                - **Ex:** *https://{Custom-Hostname}/idsvr/Saml2*
        - **Single sign on URL** for ThreatModeler is: ***https://yoururl/idsvr/Saml2/Acs***
            - **Single sign on URL when accessing ThreatModeler on Private IP address**
                - **Ex:** *https://10.0.0.132/idsvr/Saml2/Acs*
            - **Single sign on URL when accessing ThreatModeler on Custom Hostname**
                - **Ex:** *https://{Custom-Hostname}/idsvr/Saml2/Acs*
    - If SAML application (For accessing ThreatModeler) is configured initially with **Audience URI (SP Entity ID)** & **Single sign on URL** using **Private IP address**, before setting up Custom Hostname to access ThreatModeler application please update your SAML application **Audience URI (SP Entity ID)** & **Single sign on URL** to use **Custom Hostname** instead of **Private IP address** and re-upload the **Metadata file** in **Meta Data Location*** path with in ThreatModeler application.

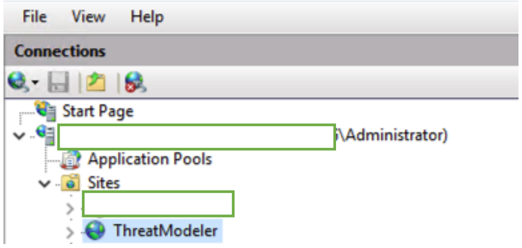
Restart IIS Server

To restart ThreatModeler IIS web server, RDP into ThreatModeler windows server.

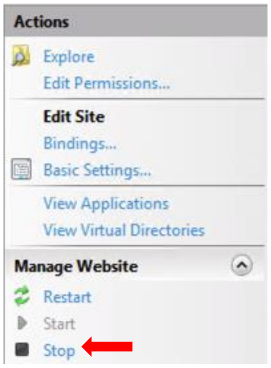
- Open **Internet Information Services (IIS) Manager**. Below Start Page you should see the hostname of the server and click on the “**>**” symbol to expand.

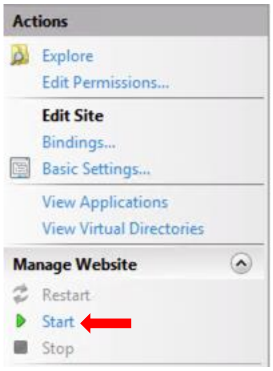


- Click on the “**>**” symbol to expand **Sites** and select **ThreatModeler.**



- With the ThreatModeler Site selected, you should see the **Actions** tab as follows and click **Stop and Start**. The ThreatModeler Application will restart.



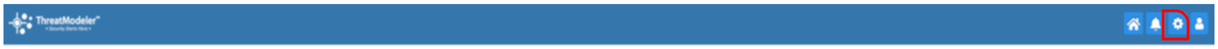


- After a successful restart, the ThreatModeler application should be accessible (within 3-5 minutes).

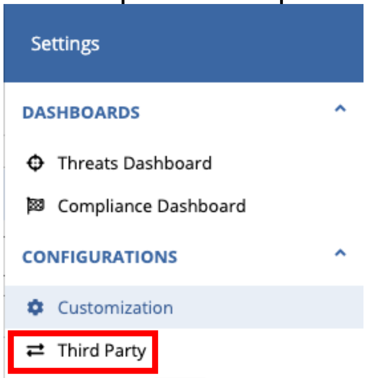
Set Up JIRA (Optional)

The Third-Party screen allows you to manage ThreatModeler integrations with several third-party platforms, including AWS, Jira, Jenkins and more.

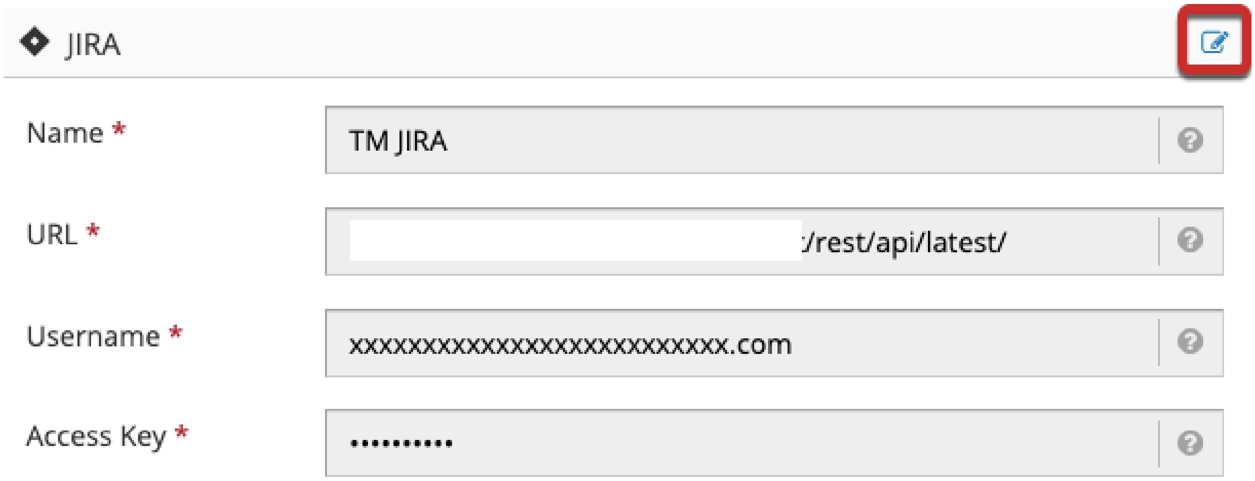
1. Click on the Settings icon in the Primary Navigation bar.



2. A slider panel will open where you can access the Third-Party screen.



3. Select the ⊞ icon in the left pane and select Jira.
4. Fill in the four fields (Name, URL of your Jira instance, and your Jira Username and Password).
5. Click on Save. If the information is entered correctly and login credentials verified, ThreatModeler will integrate with Jira.
6. Click on the ✎ icon to Edit the connection.



JIRA

Name * TM JIRA

URL * [redacted]/rest/api/latest/

Username * xxxxxxxxxxxxxxxxxxxxxxxxxx.com

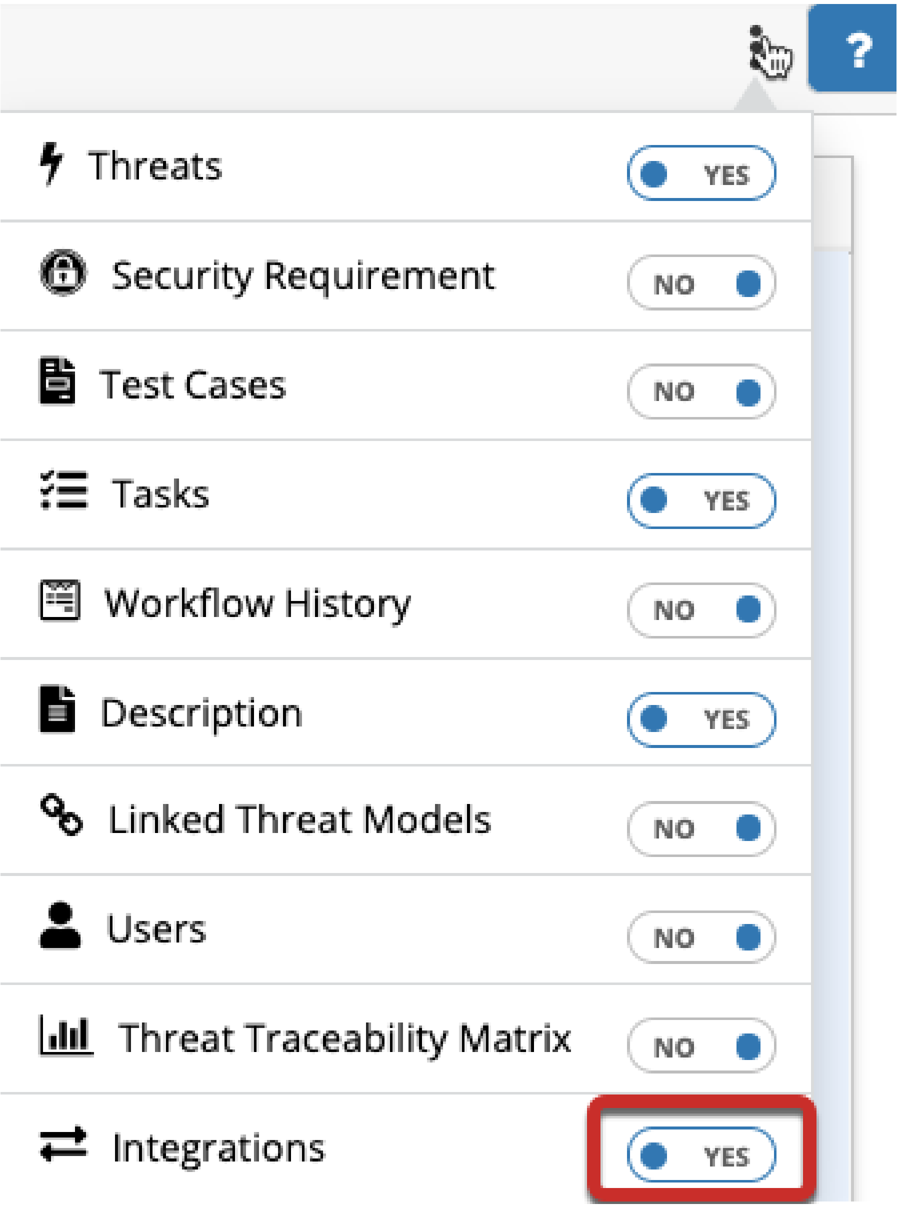
Access Key * ••••••••••

Connect Your Threat Models to Jira

Now that you have set up a bidirectional integration with Jira as a third party, you can connect some or all of your threat models. When your threat model is connected to Jira, you can push individual threats and security requirements into Jira as tickets.

1. Select the threat model you intend to connect with Jira.
2. Go to Overview.
3. Open your threat model and click on the ⋮ More icon.

4. Toggle the Integrations button to Yes.



Threats YES

Security Requirement NO

Test Cases NO

Tasks YES

Workflow History NO

Description YES

Linked Threat Models NO

Users NO

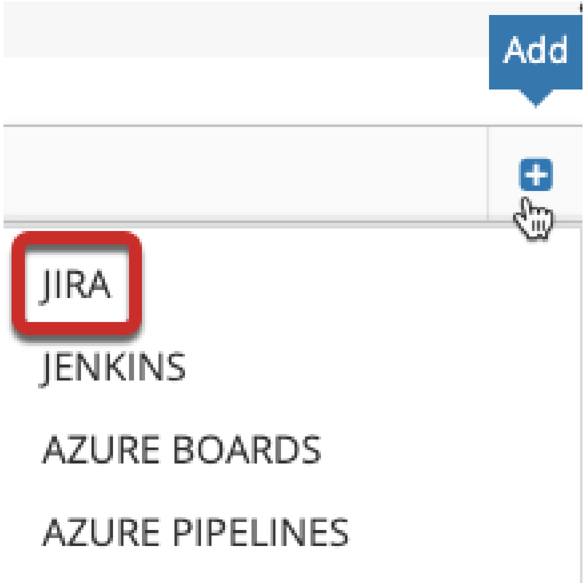
Threat Traceability Matrix NO

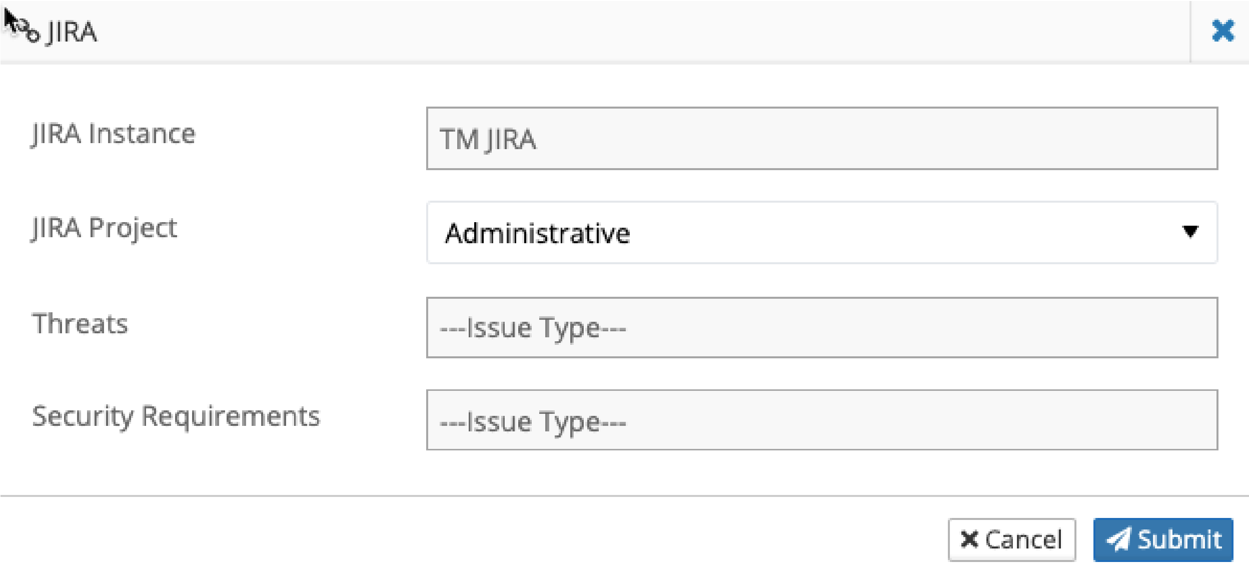
Integrations YES

5. In Overview, scroll down to the Integrations window.

6. Click the + button.

7. Click the Jira instance.




JIRA

JIRA Instance: TM JIRA

JIRA Project: Administrative

Threats: ---Issue Type---

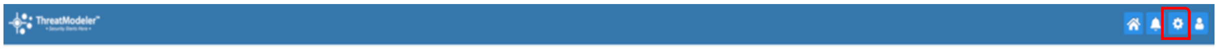
Security Requirements: ---Issue Type---

8. Select the Jira project.
9. Input the Threats and Security Requirements to determine how Jira will track identified threats and security requirements.
10. Click Submit. The threat model will be integrated with the selected Jira project.
11. When you go to the Overview screen, you will see the Jira ✓ button checked to indicate that the Jira bidirectional integration is active.
12. In the Overview screen, click on ◆ to create issues for Jira. Once created, you can search by Jira ticket ID using the Issue filter.

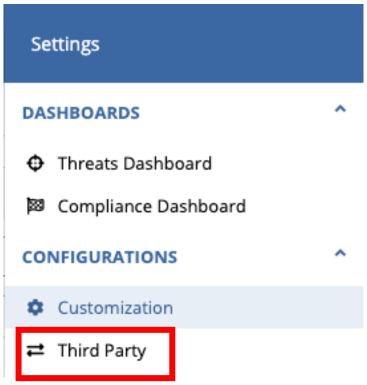
Set Up Jenkins (Optional)

ThreatModeler can help developers to automatically create secure initial builds by integrating with Jenkins. Creating the build with Jenkins requires that the threat model first be completed and approved. To connect with Jenkins:

1. Click on the Settings icon in the Primary Navigation bar.



2. A slider panel will open where you can access the Third-Party screen.



Settings

DASHBOARDS

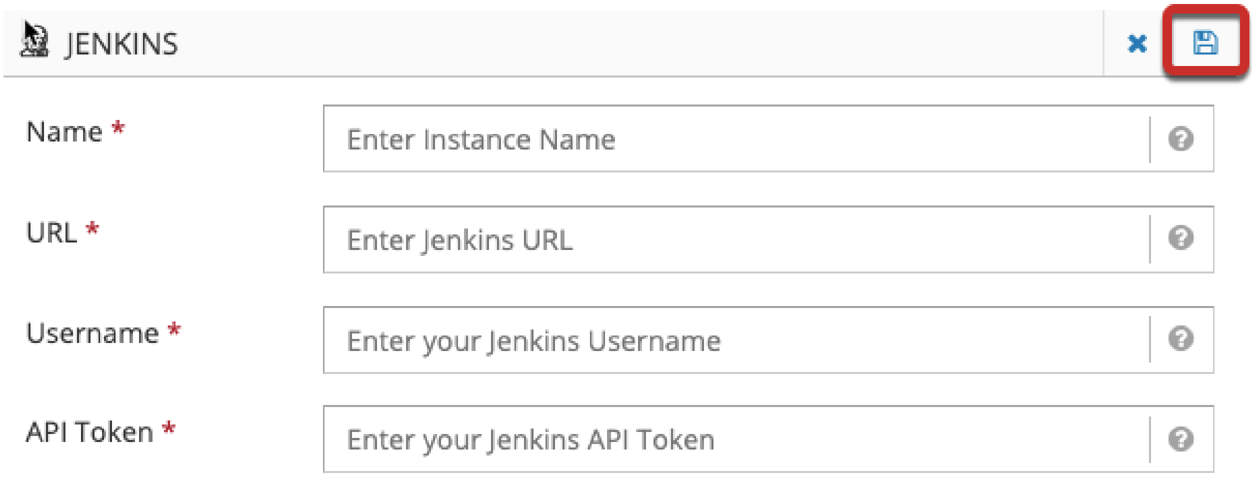
- Threats Dashboard
- Compliance Dashboard

CONFIGURATIONS

- Customization
- Third Party

The Integrations window displays a list of third-party integration connections for that threat model.

1. Click the ➕ icon.
2. Select Jenkins from the drop-down menu. The Jenkins Integrations dialog box will open.
3. Fill in the four fields (Name, the URL of your Jenkins instance, your Jenkins login credentials).
4. Click the Save icon. ThreatModeler will now be connected to Jenkins.

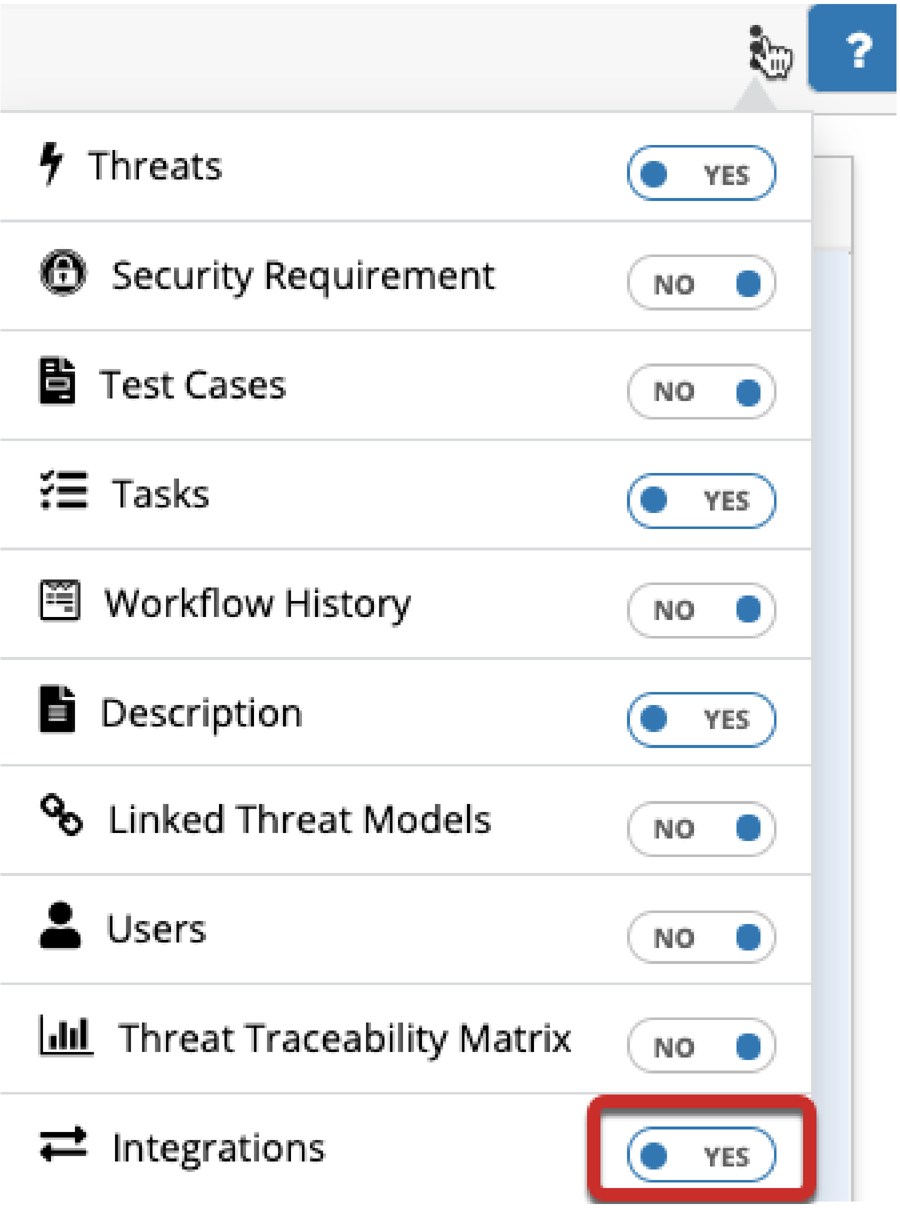


JENKINS

Name *	Enter Instance Name
URL *	Enter Jenkins URL
Username *	Enter your Jenkins Username
API Token *	Enter your Jenkins API Token

Connect Your Threat Models to Jenkins

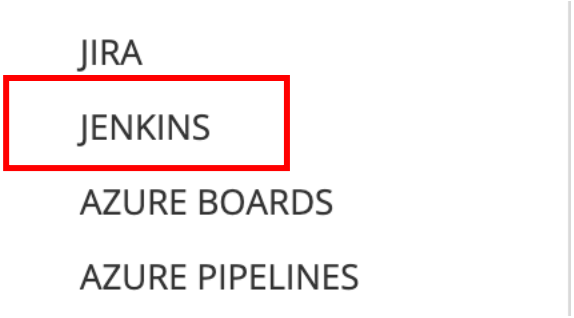
1. Select the threat model you intend to connect with Jira.
2. Go to Overview.
3. Open your threat model and click on the ⋮ More icon.
4. Toggle the Integrations button to Yes.

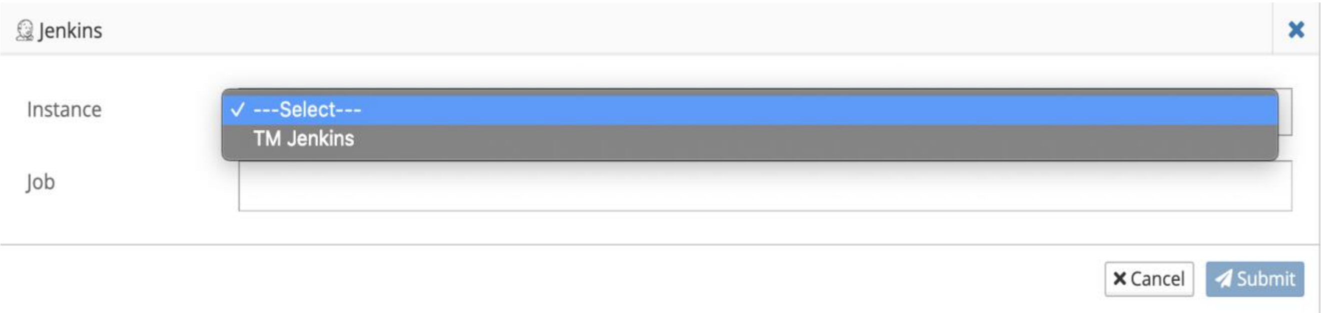


Threats	YES
Security Requirement	NO
Test Cases	NO
Tasks	YES
Workflow History	NO
Description	YES
Linked Threat Models	NO
Users	NO
Threat Traceability Matrix	NO
Integrations	YES

5. In Overview, scroll down to the Integrations window.
6. Click the + button.

7. Click the Jenkins instance.





13. Select the Jenkins job with which you want to link a threat model.
14. Click Submit. The threat model will be integrated with the selected Jenkins job.

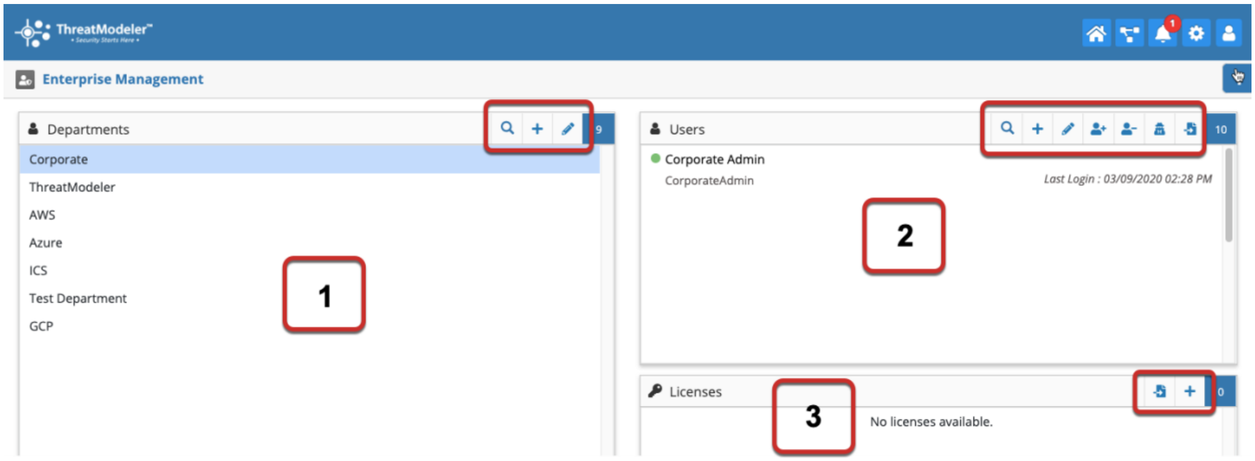
Managing the ThreatModeler Platform

Enterprise Management

The Enterprise Management screen allows users to define new departments. Once a department is created, you can associate users through the Users window on the Enterprise Management screen. The Enterprise Management screen also enables you to distribute ThreatModeler licenses amongst the various departments. For access to Enterprise Management a user needs to have at least Read Write permissions in the Administrator Group (defined in the Authorization below).

The Enterprise Management screen, accessible from the General icon in the Primary Navigation bar, has three windows:

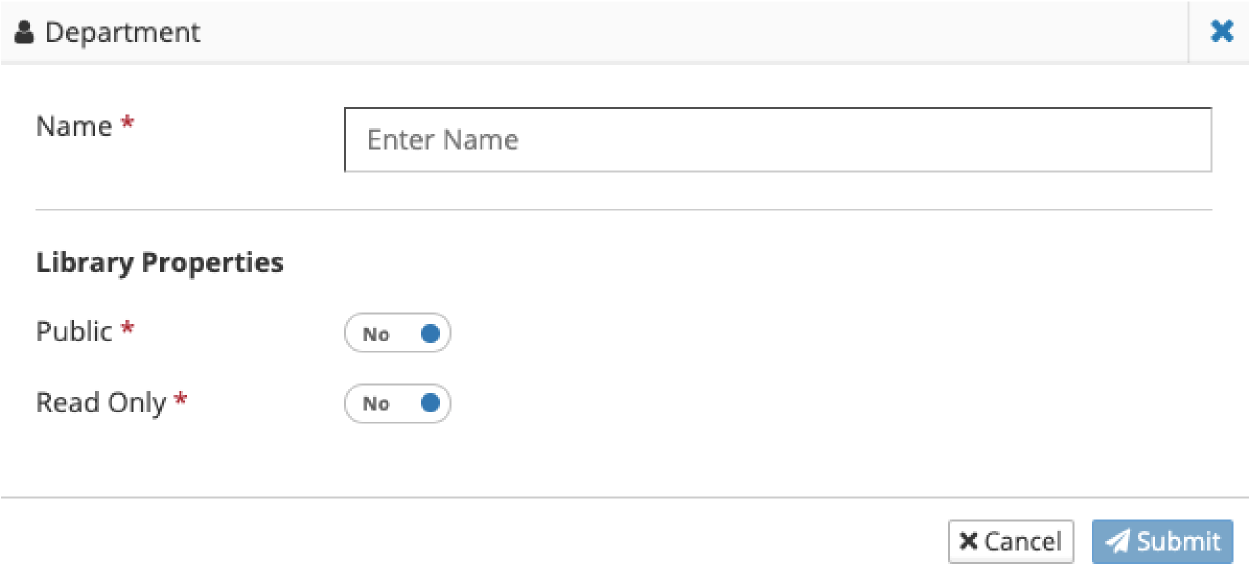
1. Departments
2. Users
3. Licenses



Department Window

The Department window lists all of your departments, which can be added to or edited using the icons at the top right-hand corner.

1. Click the + icon to add a department.
2. Add the name of the new department.
3. Identify whether you want the associated Library to be Public (Yes or No). Selecting Yes would make the Threat Framework library for the Department available to view/ edit by any other department within the organization.
4. Whether it should be Read only (Yes or No).
5. Click the ✎ icon to edit an existing department.



Name * Enter Name

Library Properties

Public * No

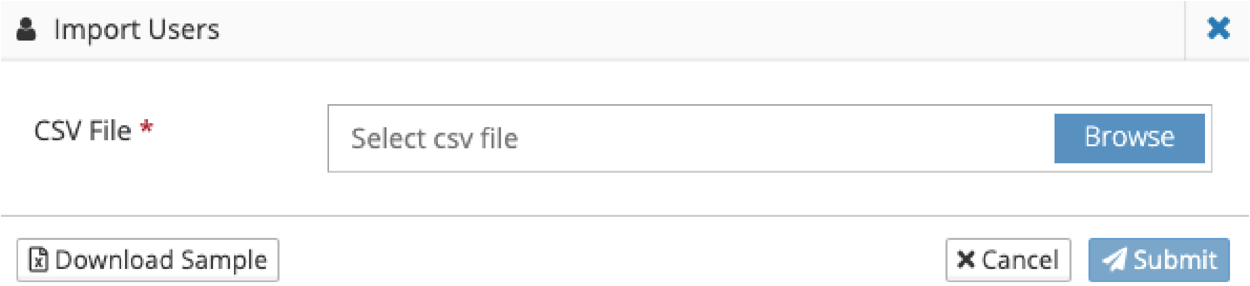
Read Only * No

Users Window

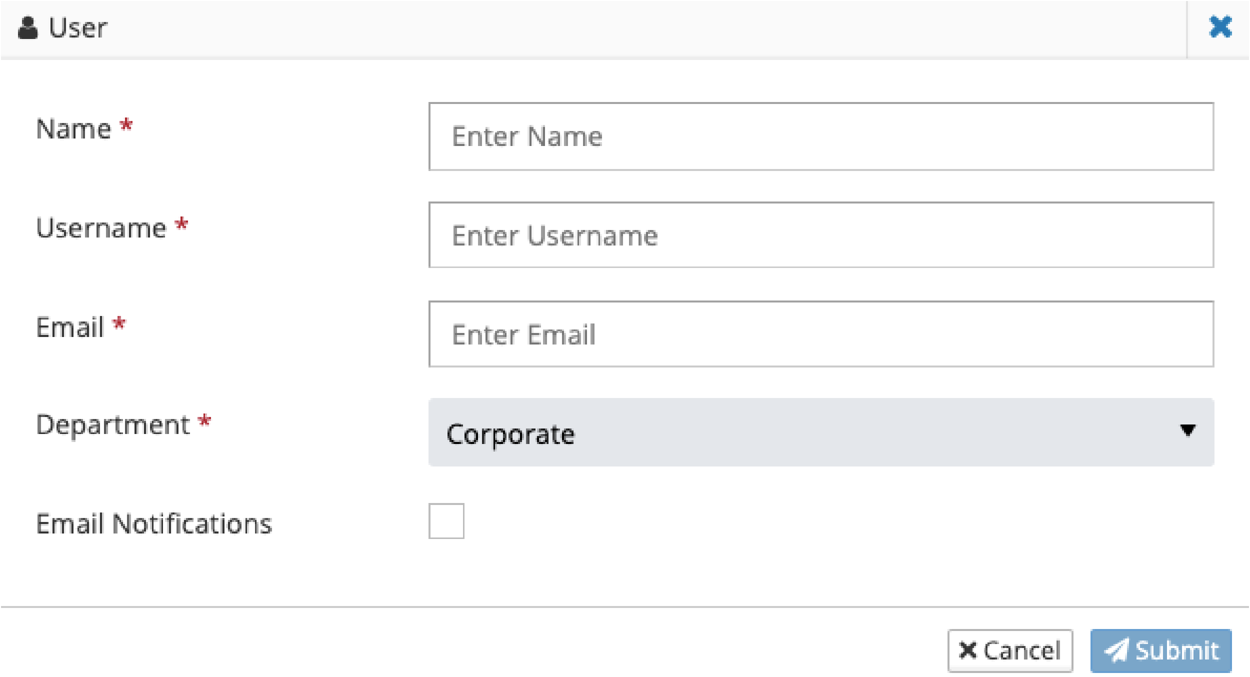
> Note: Users added via SSO will be visible for you to manage under the Users Window. The following description of Users Window allows you to add and manage new users directly from the ThreatModeler platform.

The Users Window lists all the users that belong to the selected department. There are several icons at the top right-hand corner of the Users Window to manage the users for the selected department.

1. Click the + icon to add a user to the selected department.
2. Enter the new user’s name, username, email, and role, and check the Department name, which will automatically be populated.
3. To import users from a CSV file, click, browse and select your CSV file of new users then click Submit.



CSV File * Select csv file



User

Name * Enter Name

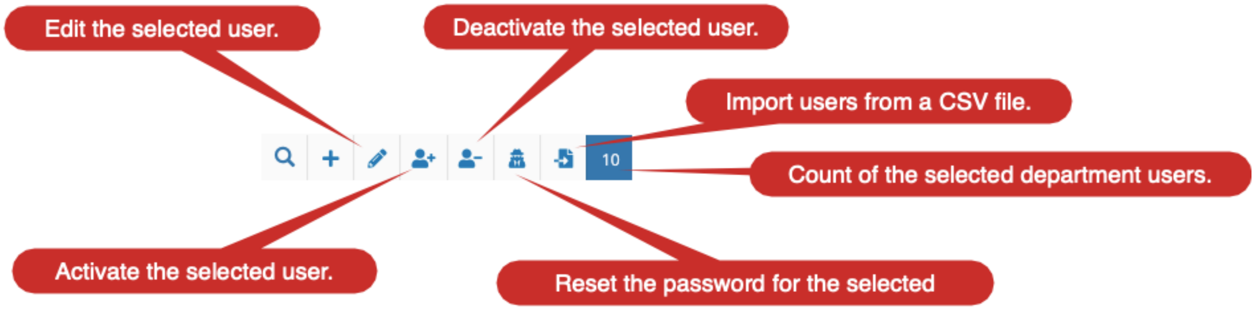
Username * Enter Username

Email * Enter Email

Department * Corporate ▼

Email Notifications □

By default, any user provisioned through the SSO integration will be created under the Corporate Department.



Edit the selected user.

Deactivate the selected user.

Import users from a CSV file.

Count of the selected department users.

Activate the selected user.

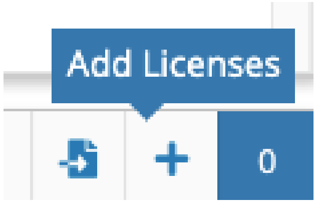
Reset the password for the selected

Working with Licenses

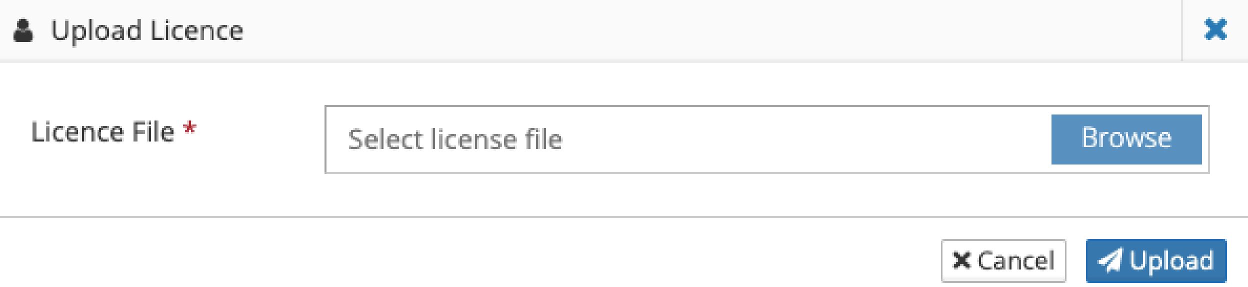
Users can add or transfer available licenses using the License window Toolbar. The Enterprise Management keeps track of the license usage per department. ThreatModeler also displays a color bar under the department name indicating the number of available licenses consumed.

Adding a License

1. Click on the + icon.



2. Browse your network or device and select the license file.
3. Click Upload.

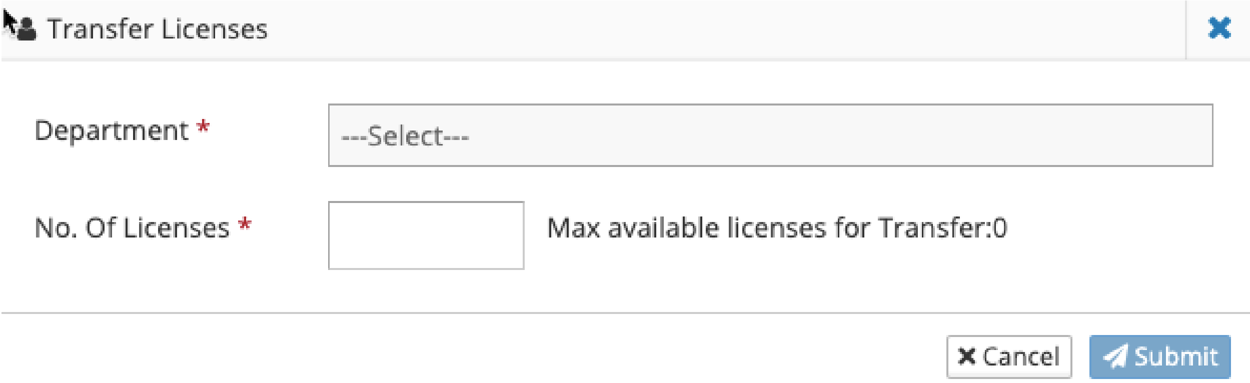


Upload Licence

Licence File * Select license file

Transferring a License

1. If there are Licenses available, click the ⇥ icon to transfer a license from another department. A dialog popup box will open.
2. Select the Department from which to transfer the license.



Transfer Licenses

Department * ---Select---

No. Of Licenses * Max available licenses for Transfer:0

3. Enter the number of licenses to be transferred. The counter on the top right corner shows the maximum available licenses that can be transferred from the department you have selected.
4. Click Submit to transfer the licenses.

Authorization

You can use permissions to control the type of access each user has from the Authorization screen.

To navigate to the Authorization screen, click on the Settings ⚙ icon on the Primary Navigation bar, then choose Authorization from the drop-down menu.

User Permissions

You can define one of the following three permissions to a user. Each of these is further explained under System Defined Groups:

1. Read Only
2. Read Write
3. Admin

System Defined Groups

The authorization screen allows you to control which users have access to which models; and control what kind of access they have within a Department (as created in Enterprise Management). The following Platform management groups perform administrative and backend functions for the ThreatModeler platform. As such, they do not provide group members with access to threat models or threat model output. User authorization is specific to the Department to which the user is assigned.

1. **Common Projects for a Department** – Adding users into this entity would allow them to have visibility into the threat model projects within that department. A user can be provided with any of the following three permission levels:

    - **Read Only** – access pre-existing threat models, but cannot edit or delete it. Can create a new threat model with edit/ delete permissions.
    - **Read Write** – access and edit threat models, but cannot delete it.
    - **Admin** – can access, edit and delete ThreatModeler content.

    For the user to be able to use features outside of access to threat model projects, the following permissions may be required.

2. **Administrator** – has access to Third-Party Integrations and Enterprise Management; also provides Authorization to the platform users.
    - **Read Only** – access to view Enterprise Management, Authorization and Third Party. Cannot edit/ delete.
    - **Read Write** – Access to view and edit Enterprise Management, Authorization and Third Party. Cannot delete.
    - **Admin** – Access to view, edit and delete Enterprise Management, Authorization and Third Party.

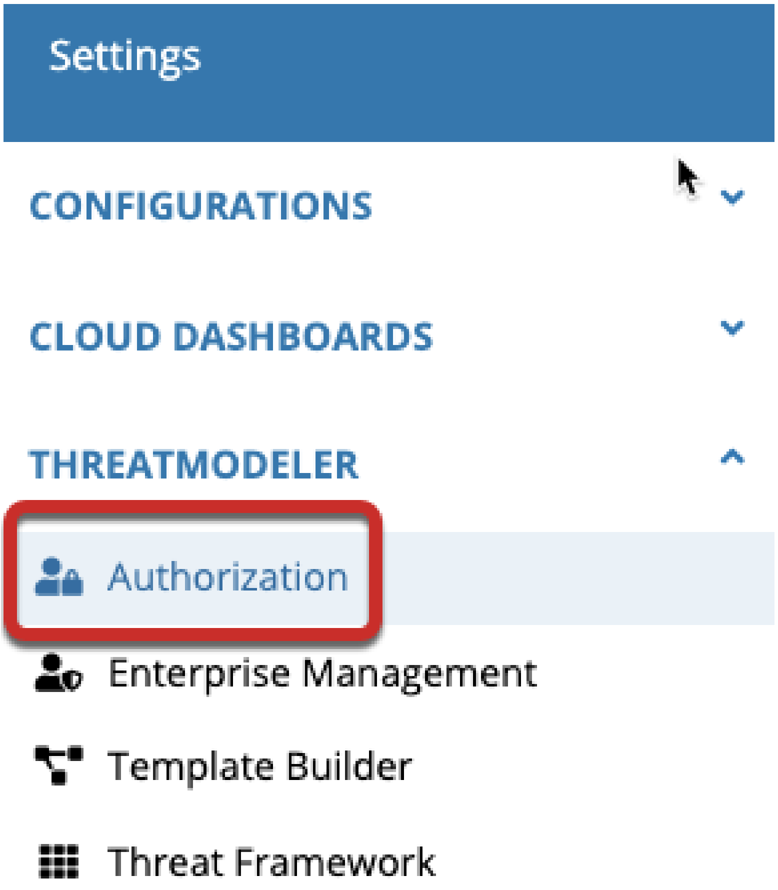
3. **Content Management** – provides access to the platform's Threat Framework.
    - **Read Only** – access to view Threat Framework. Cannot edit/ delete pre-existing content. Cannot add new content.
    - **Read Write** – Create new content in Threat Framework. Access to view and edit existing content. Cannot delete pre-existing content.
    - **Admin** – Access to view, edit and delete content within Threat Framework.

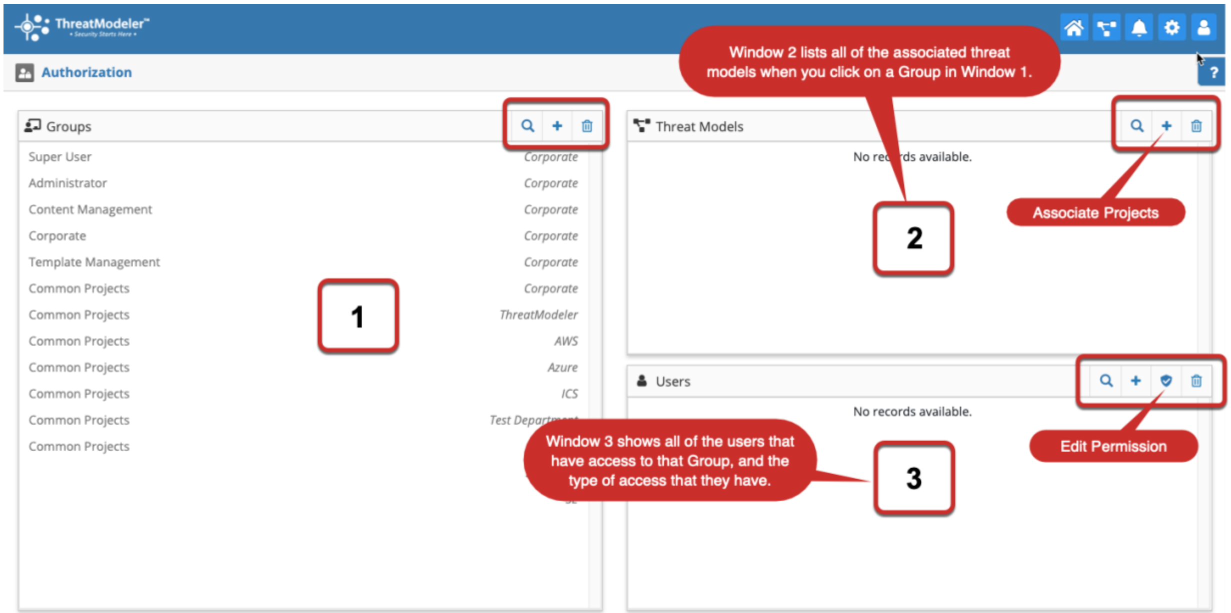
4. **Template Management** – provides access to the Template Builder.
    i) **Read Only** – access to view Template Builder and create new templates. Cannot edit/ delete pre-existing templates.
    ii) **Read Write** – Create new Templates in Template Management. Access to view and edit existing templates in Template Management. Cannot delete pre-existing templates.
    iii) **Admin** – Access to view, edit and delete content within Template Management.

The **Corporate Group** is the primary group for access to threat models. The Corporate Group is divided into departments. Organizations can create as many departments as needed. Users can create departments in Enterprise Management. The Super User Group has access to all administrative functions and threat models. Therefore, Super Users are not associated with any particular threat model. They have access to all threat models.

Working with Authorization

1. Click on the Settings ⚙ icon in the Primary Navigation bar.
2. Click on Authorization. You will be navigated to the Authorization window.





Groups	
Super User	Corporate
Administrator	Corporate
Content Management	Corporate
Corporate	Corporate
Template Management	Corporate
Common Projects	Corporate
Common Projects	ThreatModeler
Common Projects	AWS
Common Projects	Azure
Common Projects	ICS
Common Projects	Test Department
Common Projects	

Threat Models: No records available.

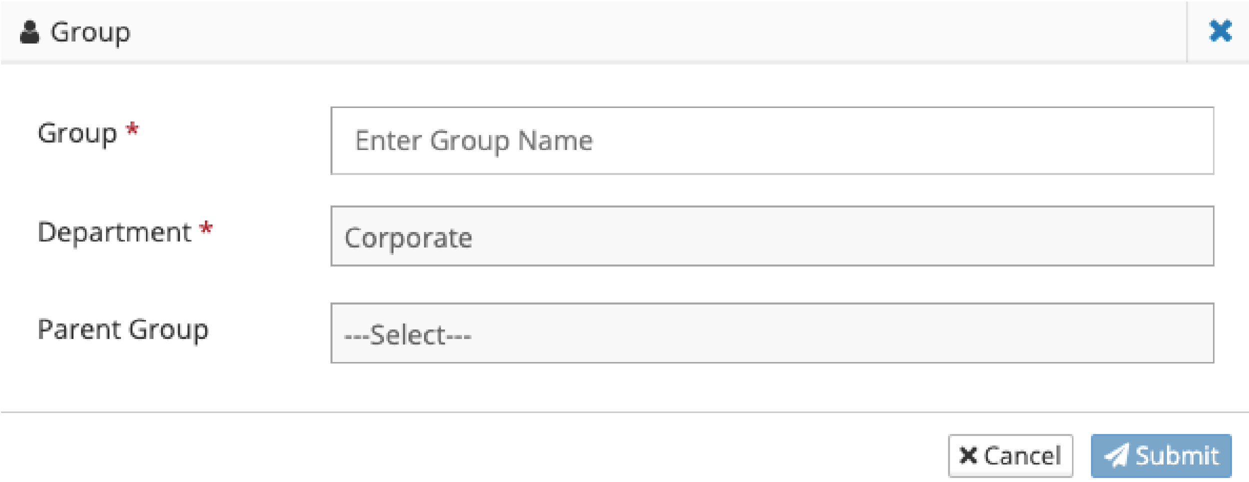
Users: No records available.

Window 2 lists all of the associated threat models when you click on a Group in Window 1.

Window 3 shows all of the users that have access to that Group, and the type of access that they have.

Adding a Group – In addition to the System Defined Groups, a user with Admin/ Read Write permissions to Administrator Group can create new groups within department to isolate threat models created within Common Projects for the Department. For example, there are 2 groups (Group A and Group B) under Common Projects for Department 1. Any user provisioned with permission to Group A will not be able to view/ edit threat models created by users of Group B and vice-versa. Further, any member in the parent group (in this case Common Projects for Department 1) will be able to manage threat models created by Group A and Group B members.

1. Click the + icon to add a Group.



Group ✖

Group * Enter Group Name

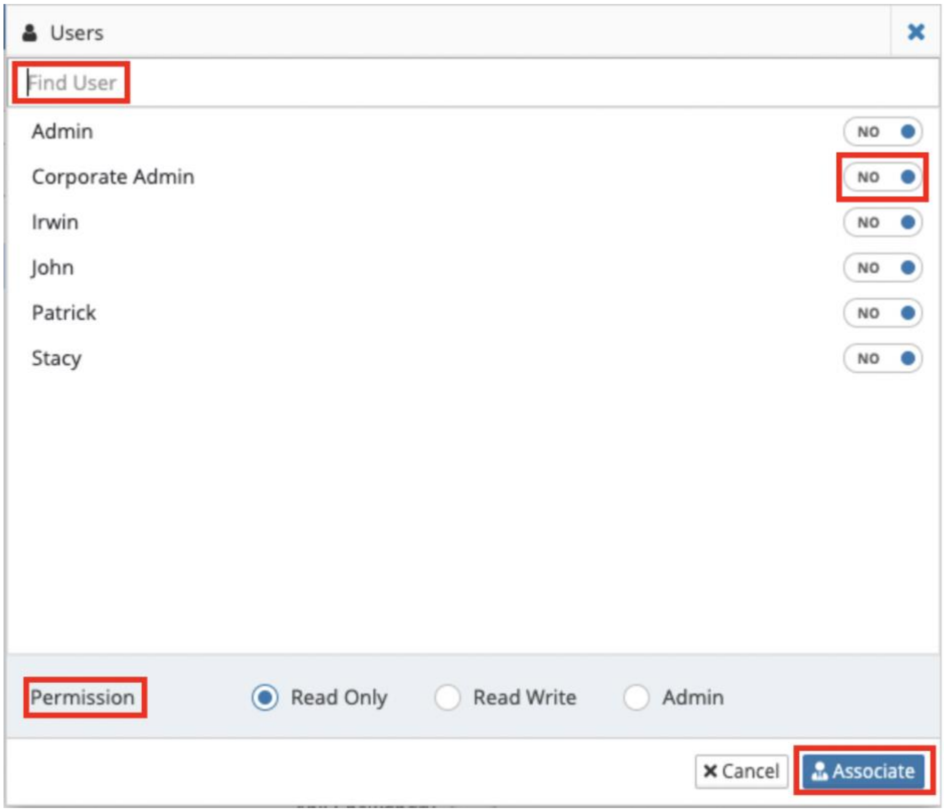
Department * Corporate

Parent Group ---Select---

2. Fill in the Group name (required).
3. Fill in the Department (required).
4. Select the Parent Group (when appropriate).
5. Click Submit.
6. Click the ✏ item to edit a selected Group and click the 🗑 icon to delete a Group.

Associate Threat Models to a Group

1. Click the + icon at the top right-hand corner of the Associated Threat Models Window.
2. Find and select the user to which you'd like to associate additional threat models. For longer lists, use the free text search field.
3. Set the Permission level.
4. Click on Associate.
5. Use the 🗑 icon to remove the association with a threat model.



Users ✕

Find User

Admin	NO
Corporate Admin	NO
Irwin	NO
John	NO
Patrick	NO
Stacy	NO

Permission ● Read Only ○ Read Write ○ Admin

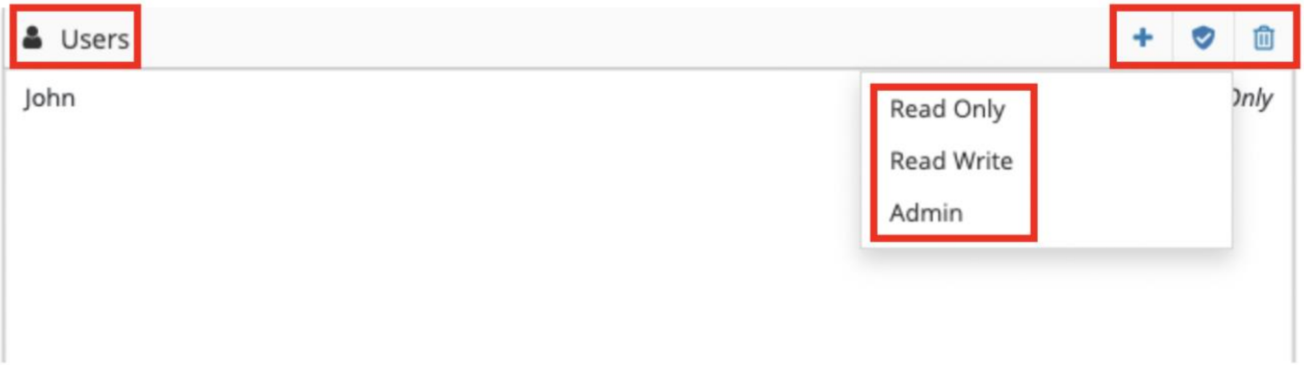
✕ Cancel | Associate

Editing User Permissions

1. Click the ✚ icon at the top right-hand corner of the Users Window to add users to that Group.

2. Click the 🛡 icon in the User Window to edit the permissions for a user in the selected Group. Users with the following permissions can Read Only, Read Write and Admin.

3. Click the 🗑 icon in the Users Window to remove a user from that Group.



Users ✚ 🛡 🗑

John

Read Only
Read Write
Admin

Next Steps

Once your setup is complete you can get started with your threat modeling exercise. Please access the guides below to gain insight into various threat modeling scenarios and how to accomplish them with ThreatModeler:

ThreatModeler Interface Guide: This guide provides in-depth guidance with regards to navigating through the ThreatModeler platform

Threat modeling scenarios for AWS: This guide covers common scenarios with detailed steps of accomplishing the same in ThreatModeler.

ThreatModeler Hostname Resolution: This document helps you to set up domain name resolution to access the ThreatModeler application on a custom domain name.