

Getting Started with ThreatModeler

Getting Started with ThreatModeler™ – A Step-by-Step Guide to Securing your Applications.

ThreatModeler simplifies the traditional manual process of threat modeling and automates the work to a greater degree. The major advantage of ThreatModeler™ over the traditional threat modeling process is its usability and little or no security knowledge required to create threat models. The entire process is more straightforward as compared to any other Threat Modeling tool. ThreatModeler™ allows users to capture the entire flow of the application, and define certain properties based on which it automatically generates threats and classifies them under various risk categories. ThreatModeler™ not only streamlines and automates the entire threat modeling process by reducing the manual work but it also incorporates abuse case modeling, to generate more targeted threats to individual functionality and associates mitigation steps along with it. Updating a threat model with ThreatModeler™ is a matter of minutes. ThreatModeler™ can be used by Architects, Developers, Security Professionals, QA professionals or senior executives.

ThreatModeler™ allows users to capture the entire flow of the application, and define certain properties based on which it automatically generates threats and classifies them under various risk categories. It's simple to use navigation wizard help users to enter the required information they will need to get started with their application and build a threat profile of the application. ThreatModeler™ brings a mind mapping approach to threat modeling, allowing the user to decompose the application just like they do it on the white board but at the same time provide features that a white board cannot. User can define the communication channel (protocols) between different components; assign data elements and technical controls (like Form, URL, Cookie, Session, etc) to these components.

Once a user has completed the component diagram, ThreatModeler™ with its intelligent threat engine, (ThreatSense) automatically identifies threats based on the information provided and automatically prioritizes them based on risk.

This document will guide you through the steps on using ThreatModeler™ to create a threat model and analyze threats to your application. We have also provided help on every step of the way within the tool with information to guide you through each specific screen with a help button or you could browse through the entire help file by opening it from the menu.

Getting Started with ThreatModeler

Table of Contents

Getting Started with ThreatModeler™ – A Step-by-Step Guide to Securing your Applications..	1
Prerequisites:	4
Installation:	4
Creating a New Threat Model:	6
Threat Model Details:	6
Data Elements:	7
Security Assessment Checklist:	8
Whiteboard:	8
Attack Trees:	14
Threat Management Console:.....	15
Reports:.....	16
Customization:	17
Manage Threat Library.....	18
Manage Mitigation Steps	19
Manage Question Library:.....	20
Manage Technical Controls:.....	21
Manage Data Elements:.....	23
Manage Protocols:.....	24
Manage Components:.....	25
Manage Rules:.....	27
Manage Roles:.....	28
Figure 1	4
Figure 2	5
Figure 3	6
Figure 4	7
Figure 5	8
Figure 6	9

Getting Started with ThreatModeler

Figure 7	10
Figure 8	10
Figure 9	12
Figure 10	13
Figure 11	14
Figure 12	15
Figure 13	16
Figure 14	18
Figure 15	19
Figure 16	20
Figure 17	21
Figure 18	22
Figure 19	23
Figure 20	24
Figure 21	25
Figure 22	26
Figure 23	27
Figure 24	28

Getting Started with ThreatModeler

Prerequisites:

- Microsoft Windows:
 - XP
 - Vista (32-bit and 64-bit)
 - Windows 7 (32-bit and 64-bit)
- .NET Framework 3.5 / 4.0

Installation:

After downloading the installer from www.myappsecurity.com you will receive an email containing the license key. Please check your spam folder in case you do not receive it.

After installing you will be prompted to enter the license key as seen in Figure 1.

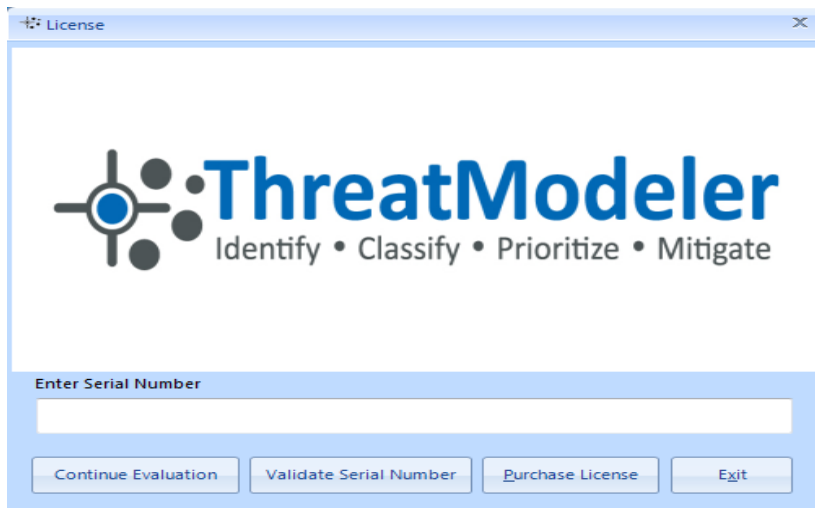


Figure 1

1. Paste in the license key you have received in the email
2. Click Validate Serial Number
3. Continue Your Evaluation

Every subsequent time you run ThreatModeler™, the license screen will pop up and you can click on 'Continue Evaluation' to continue evaluating the product. When you are ready to purchase, you can buy a license key from MyAppSecurity (sales@myappsecurity.com). After you paste in a purchased license key, the License Screen will not show up.

Getting Started with ThreatModeler

With a valid license entered, you will then reach the Threat Models window as seen in Figure 2.

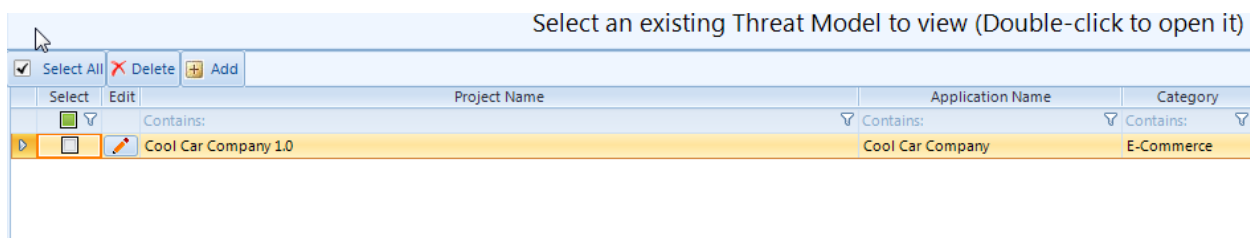


Figure 2

This page displays all the existing threat models. By default, MyAppSecurity have provided you a sample threat model of an e-commerce application 'Cool Car Company'. If you have created and saved threat models, they will appear on this page. The user can access these threat models by

- Double-clicking the Threat Model name OR
- Create a new threat model by
 - Clicking on the Add Button OR
 - File -> New Threat Model through the menu.

Getting Started with ThreatModeler

Creating a New Threat Model:

- To create a threat model, click on the Add button or through the menu File -> New Threat Model.
- This will show the 'Create Threat Model Wizard' with the following screens:
 - Threat Model Details:
 - Data Elements:
 - Security Assessment Checklist:

Threat Model Details:

At the first screen of the Wizard – Threat Model Details - the user provides general information about the threat model. These include:

- The name of the threat model.
- The application for which the threat model is created.
- Application Category - Select the category your application would be categorized under. Examples include e-commerce, healthcare, finance etc.
- Risk Classification - This is the risk classification of your application based on impact to your business. Currently the Risk Classification options are: Very High, High, Medium, Very Low and Low and are based on MITRE's CAPEC classification. This will help an organization plan their risk management and prioritize threat mitigation strategies.

The following Figure 3 is a screenshot of the Threat Model details window.

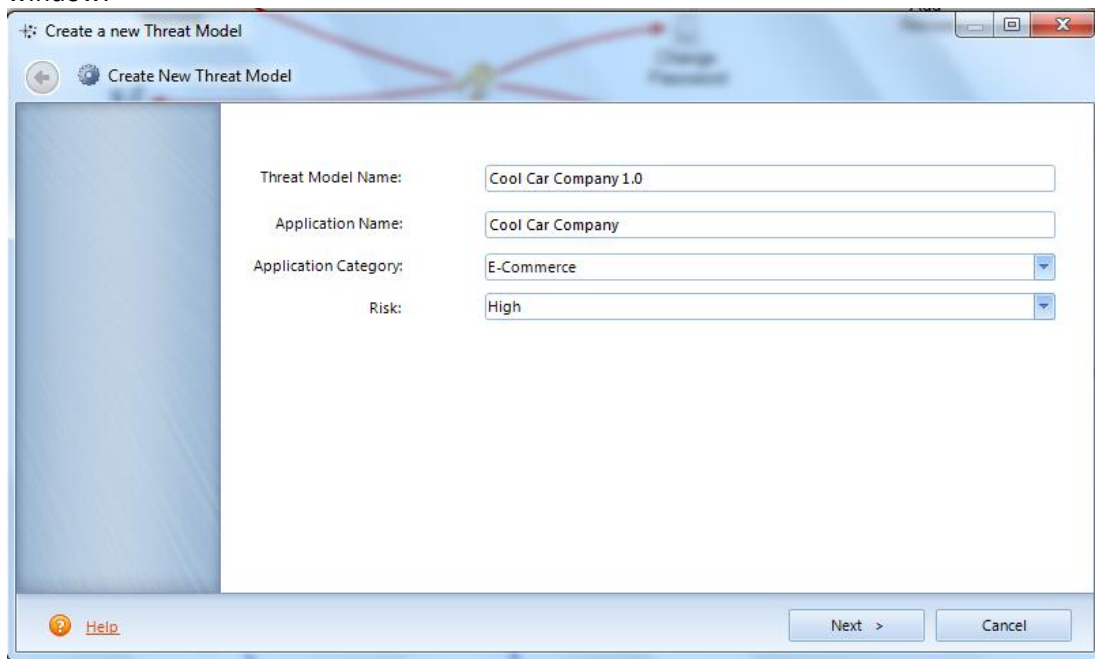


Figure 3

Getting Started with ThreatModeler

Data Elements:

The application stores and transmits various data elements through various functional components. ThreatModeler™ requires you to select the data elements to be used in the application. The data elements selected represent the data to be processed by various components and widgets of the application you are building a threat model for.

ThreatModeler™ provides a predefined list of data elements along with their classification. The data classification categories are:

- Public – Publicly available data, No access restrictions and no encryption required in the database
- Restricted – Access is restricted but not sensitive enough to require encryption in the database
- Confidential – Highly sensitive data which is access restricted and requires encryption in the database.

The user should select data elements to be used in the entire application. If the user does not find a data element in the list provided, he can add a data element(s) by clicking Admin -> Manage Data Elements.

These data elements are to be associated with components in a web application and have a direct bearing on the threats generated by ThreatModeler™, so ensure that the necessary data elements have been selected.

Figure 4 is a screenshot of the data elements page.

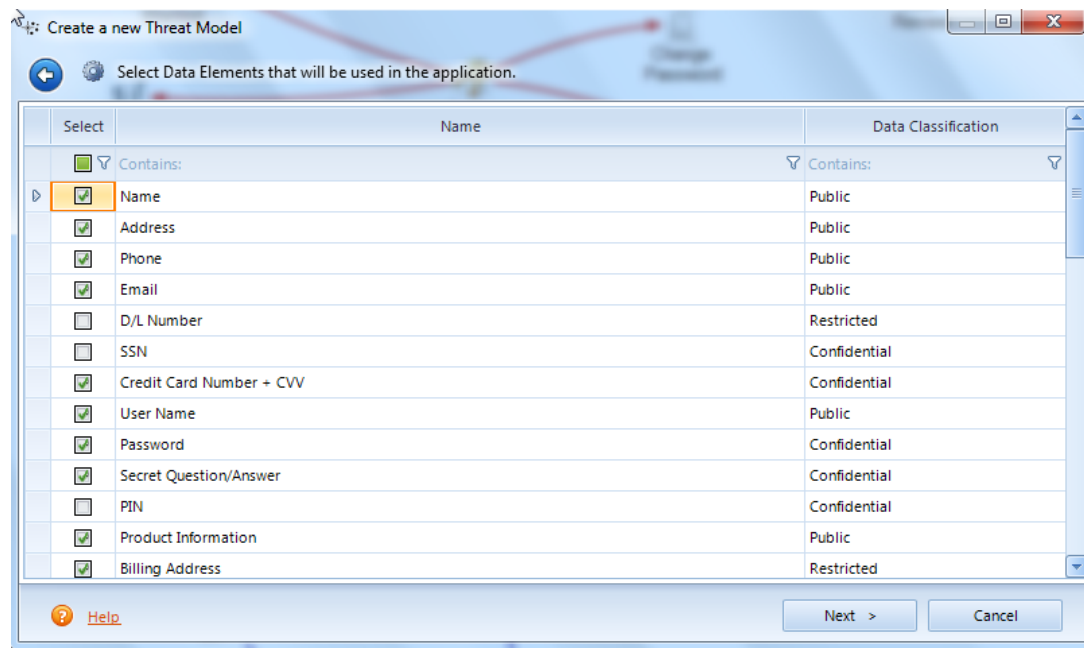


Figure 4

Getting Started with ThreatModeler

Security Assessment Checklist:

The user can assess the security controls and standards put in place using the comprehensive checklist provided by ThreatModeler™ at this stage. The checklist is comprehensive question lists to assess the strength of security control within the application.

The checklist is divided in various categories such as Authorization, Authentication, Input Validation, Database Management, Encryption, etc. to make it easier for the user to evaluate their security.

The checklist can be completely customized based on the organization standards.

If the user wants to enter a custom category or checklist according to their organization's requirements, click on Admin -> Manage Questions.

This security checklist is a reference for security professionals and auditors to verify the controls for the assessment. You can come back later to modify the answers to this checklist.

Figure 5 is a screenshot of this screen. The user will then be directed a screen which summarizes the details

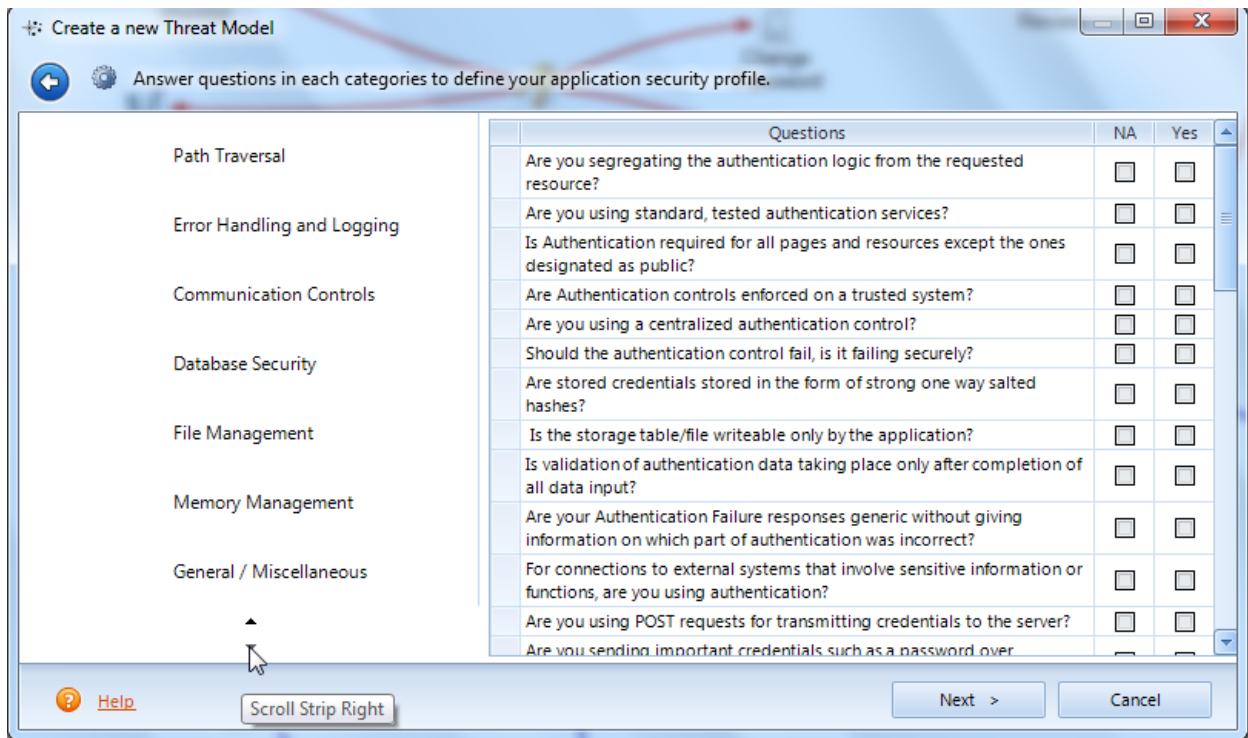


Figure 5

Whiteboard:

Getting Started with ThreatModeler

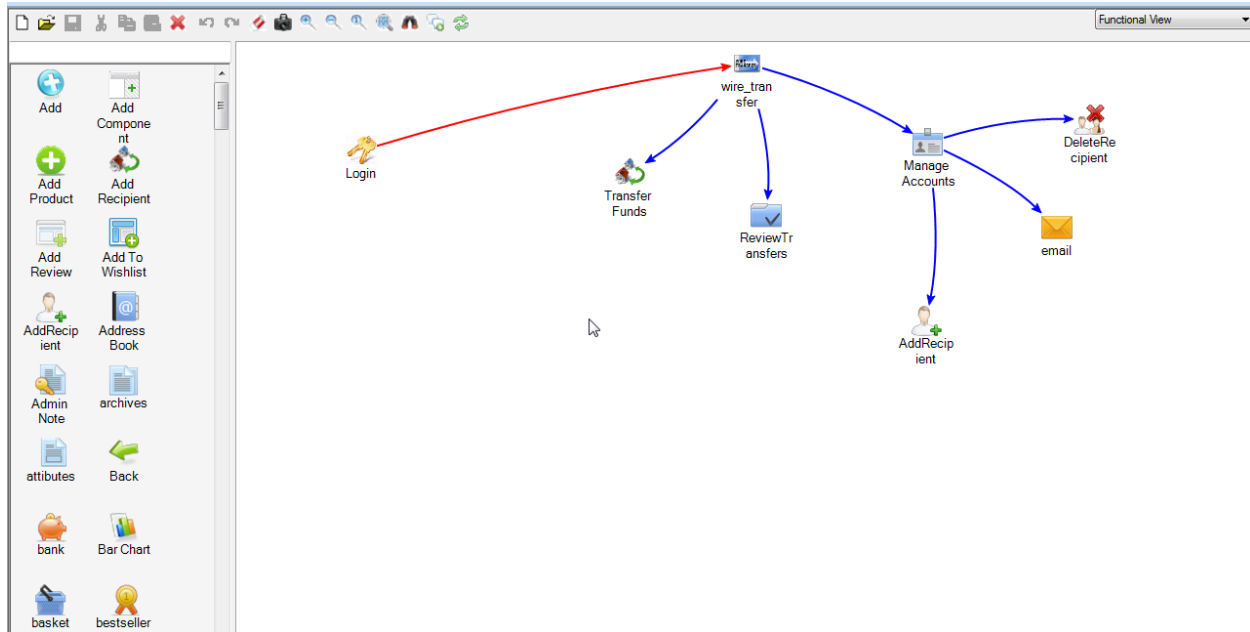


Figure 6

Figure 6 is a screenshot of the Whiteboard on which the Threat Model is designed. The Whiteboard is a simple drag-and-drop diagramming interface. The user creates a high level architecture of the application by using various components and interconnecting them by arrows which represent the communication protocol between them.

- To the left of the screen is the Component Palette. The various icons in the Palette are the components that are applicable to an application. The user can drag a component onto the whiteboard from this palette. Figure 7 is a screenshot of the palette.

Getting Started with ThreatModeler

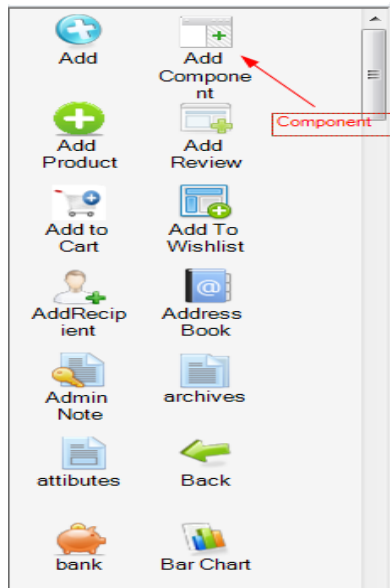


Figure 7

- A default list of components is provided but the user can add icons to represent components of their business domain by clicking Admin -> Manage Components.
- To the right of the palette is the Whiteboard which is used for your diagramming purposes.

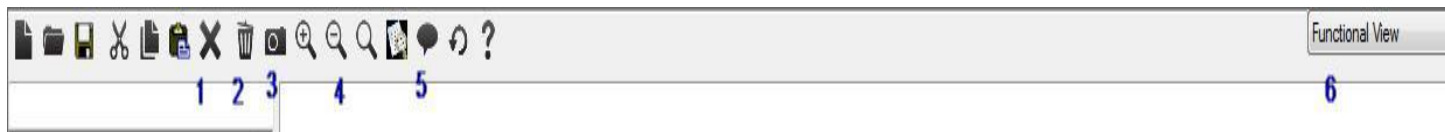


Figure 8

Figure 8 shows the various options in the taskbar. They have been numbered and their functionality has been briefly explained below.

1. Delete Selected – Select the components you want to delete
2. Clear Whiteboard – This clears the entire whiteboard
3. Save as Image – This saves your diagram as an image
4. Screen Adjustments – User can zoom in and out as well as see an overview of the entire threat model.

Getting Started with ThreatModeler

5. Add Comment – User can add comments. When you click this a comment box will pop up on the screen and this can be dragged around the Whiteboard.
 6. View Drop-down menu – User can choose to view the threat model on the basis of threats, data or in its entirety.
 - a. Data View – When you select Data View, a window will pop up with the data elements selected for the application. Select data elements from the list and the threat model will display all the components that access and process that data.
 - b. Threat View – When you select Threat View, a window will pop up with the possible threats to the entire application. Select threats from the list displayed and the threat model will show you the components vulnerable to those threats.
 - c. Functional View – This is the view of the entire threat model i.e. the way you designed it.
-
- The Edit option in the main menu bar allows the user to make changes to the Threat Model settings for Threat Model properties, data elements and answers to questions in the security checklists. The changes made here will be reflected through the entire threat model. Data elements used by a component cannot be deselected.
 - Once several components are placed on the whiteboard, **they can be linked to each other by placing the mouse over a component to get the hand pointer and generating an arrow link to the other components.**
 - The user has the option to view components based on data elements processed by the component or by threats to a particular component.
 - Right-click a component to access its properties and to view Attack Trees
 - Right-click the interconnecting arrows to change the communication protocol.

Getting Started with ThreatModeler

Component Properties:

Double-Click a component on the whiteboard. A window opens with the following tabs that define the properties of the component:

- Data Elements – These are the data elements that are accessed by the component.
- Roles – These are the different roles for the application. A role defines what type of user can access the component. User can associate roles with components. You can add a role by clicking Admin -> Manage Roles.
- Technical Controls (Widgets) – These are various data processing widgets or means by which the application accepts data and /or maintains state.
- Rules (Security requirements) – These are security requirements for a particular component which should be implemented to mitigate threats.
- Notes – One can use this feature for specific notes and this feature helps in collaboration and information sharing.

Figure 9 shows a component's properties screen.

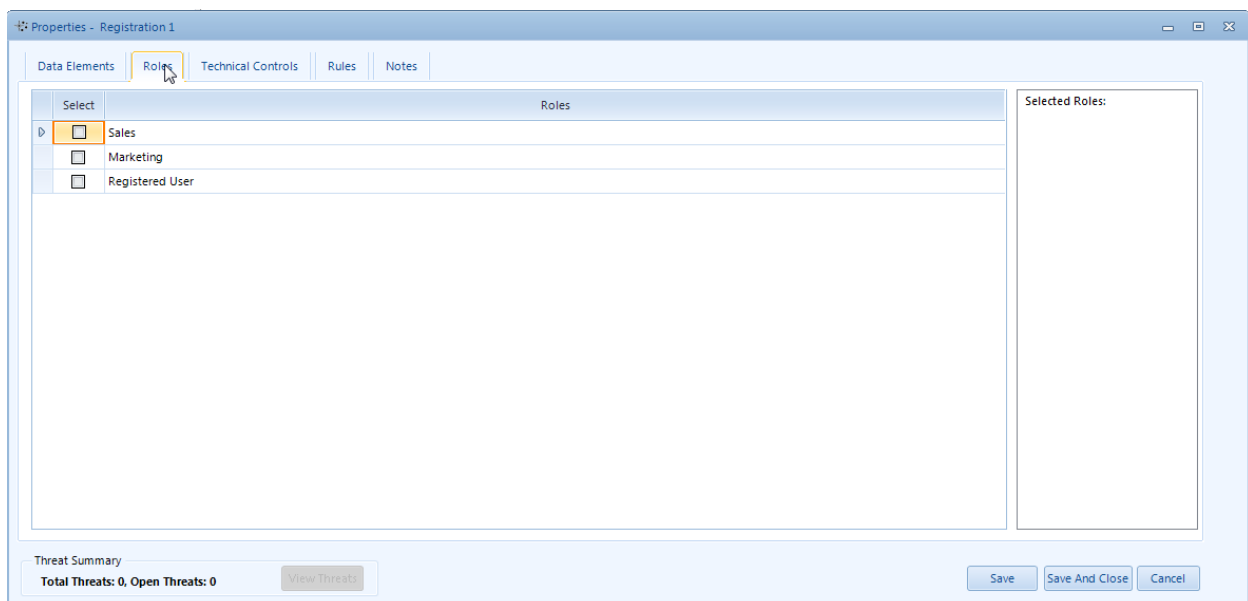


Figure 9

- Once the user clicks 'Save', the total number of threats and the open threats to the component are updated. User can view the threats by clicking the 'View Threats' button.
- The user views these by clicking the View Threats button. Figure 10 demonstrates this functionality.
- The status of the threats are:

Getting Started with ThreatModeler

- 'Open' – Threat has been identified and no security controls in place
- 'Fixed' – Secure coding guidelines and controls have been put in place and verified.
- 'Need more details' – The threat description, secure coding guidelines and controls needed might seem ambiguous or not informative enough to proceed.
- On double-clicking a threat, subsequent security guidelines and vulnerability mitigation steps will be displayed.
- Based on whether the user has implemented these secure coding steps, he can make the change to the status or if he requires more details, can change the status appropriately.

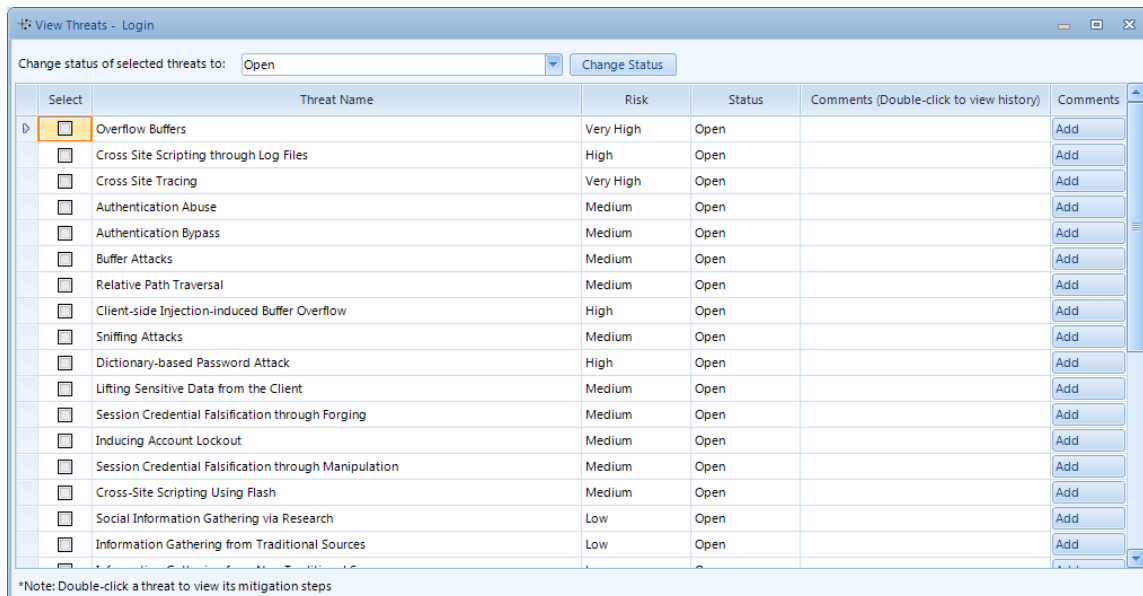


Figure 10

Getting Started with ThreatModeler

Attack Trees:

Right-click a component and choose the attack tree option. You will see an attack tree automatically created for you which will help you analyze the threats and plan mitigation steps to protect against those threats. Threat Modeler ships with attack trees for authentication module and new attack trees will be added on a periodic basis. Figure 11 depicts an Attack Tree generated for the Registration component.

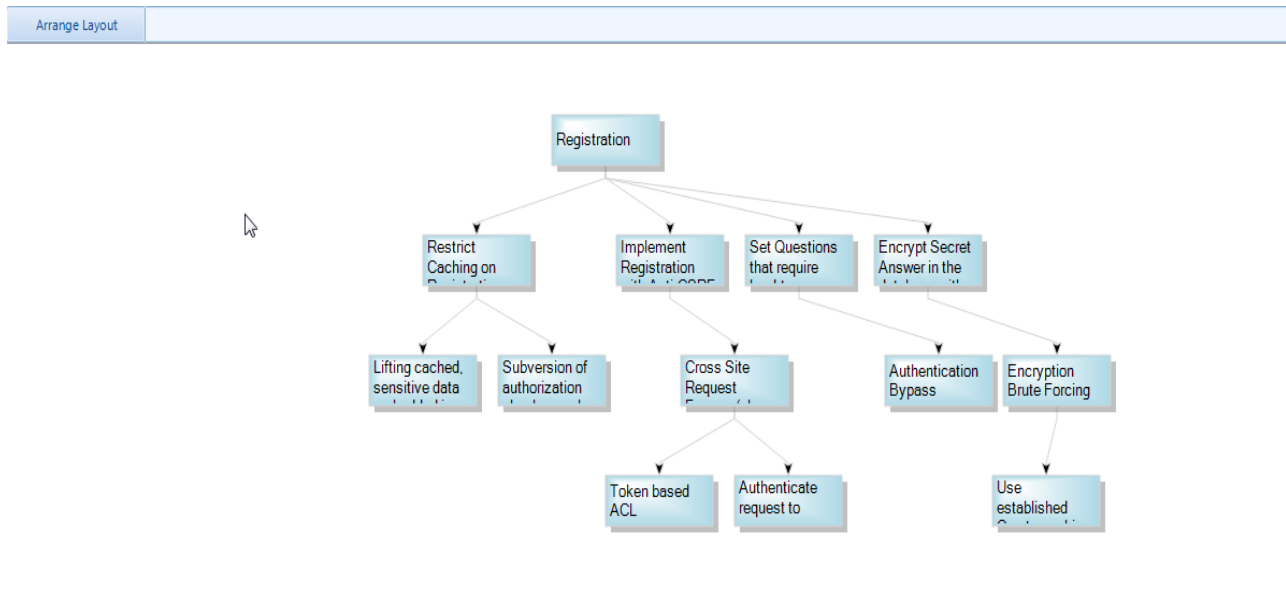


Figure 11

The attack tree is represented with the component as the root node followed by rules and security requirements at the next level. Level 3 are the threats associated with the component and finally the leaves of the attack tree are secure coding guidelines which complement the rules of level 2.

Getting Started with ThreatModeler

Threat Management Console:

As seen in Figure 12, after having created the threat model, the user can analyze threats associated with each component in the architecture. The status is indicated by:

- Open – Threat is currently open with no security controls and mitigation steps applied.
- Mitigated – Secure coding principles have been followed and security testing has validated that threat has been mitigated.
- Accepted – Threat has been identified and verified but business and technical impact are low enough to accept the risk.
- Not Applicable – This is a scenario where a specific threat might not be applicable to your business domain.

There is also provision to add in comments. With a timestamp added for each comment, it helps maintain a history of comments for archival purposes and helps in the collaborative effort among several development teams across several applications.

The user can view the threats to each component or group by the type of threat. The 'Component' view displays threats by their association to each individual component. In 'Threat' view, the threats to the application are displayed and in a drop down is a listing of all components vulnerable to those threats.

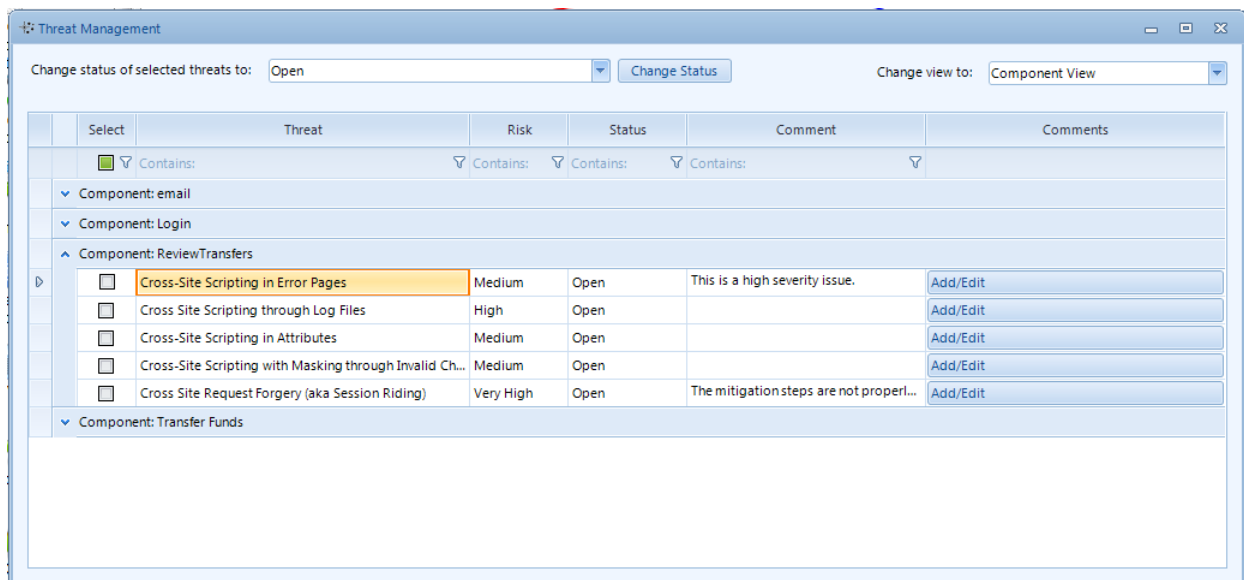


Figure 12

Getting Started with ThreatModeler

Reports:

ThreatModeler™ generates a comprehensive risk report which includes

- The Top Ten threats to your application
- Statistical details based on risk rating and threat count
- Graphical display in the form of graphs and charts.

It further

- Breaks down the data element mapping to components
- Enumerates the number of threats to each component.

Finally it

- Enumerates the threats with risk rating details and references to learn more about the threats
- Lists their current status within the application in terms of whether they are Open, Fixed, Mitigated or Not Applicable.

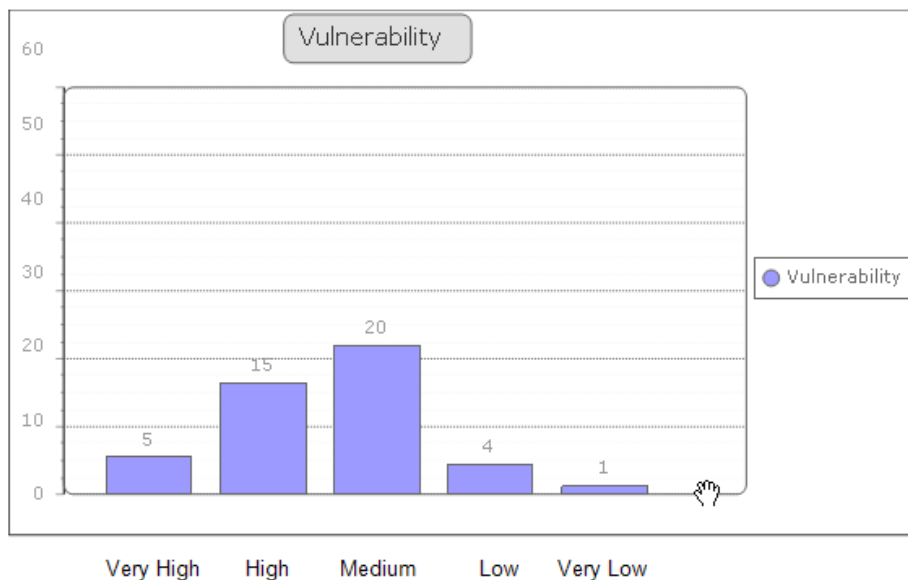


Figure 13

Getting Started with ThreatModeler

Customization:

In addition to the comprehensive threat library provided, ThreatModeler™ is a framework which can be completely customized. The user is presented with administrative features by clicking the Admin menu option. The user can perform the following tasks:

- Manage Threats
- Manage Mitigation Steps
- Manage Question Library
- Manage Technical Controls
- Manage Data Elements
- Manage Protocols
- Manage Components
- Manage Rules
- Manage Roles

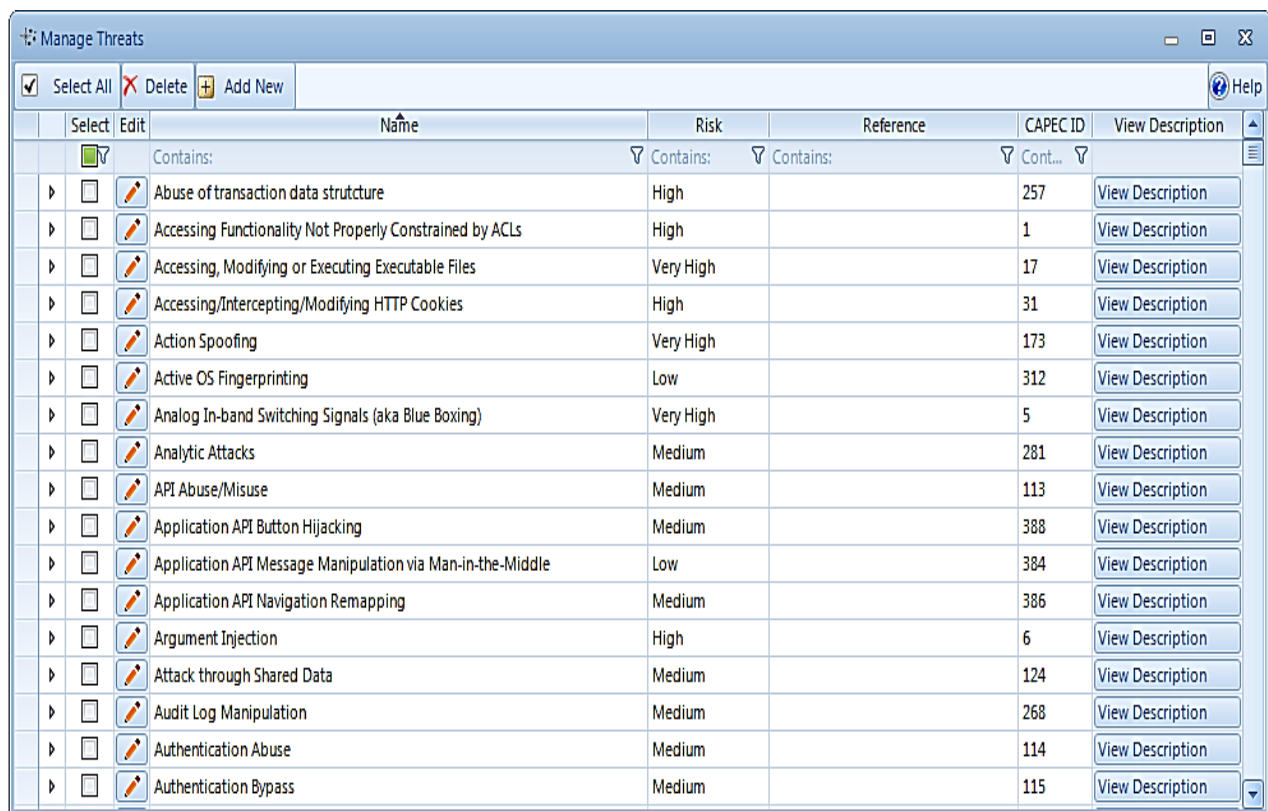
Below is a quick guide to using the Admin Features:

Getting Started with ThreatModeler

Manage Threat Library

The user can view all the threats provided by ThreatModeler™ from the MITRE's CAPEC library, WASC Threat Classification, OWASP as well as user defined threats.

You can edit a threat by double-clicking it in the grid. This will open a separate window where a user can modify threat description, CAPEC ID, and associate mitigation steps and description notes to it. The user can also make changes to the default risk classification and add URLs that link to additional resources that detail the threat. Similarly if the user chooses to add a custom threat to the library, he/she can do so by clicking the Add New button and the same screen will pop up. This screen is as in Figure 14



Select	Edit	Name	Risk	Reference	CAPEC ID	View Description
<input checked="" type="checkbox"/>		Contains:	Contains:	Contains:	Cont...	
<input type="checkbox"/>		Abuse of transaction data structure	High		257	View Description
<input type="checkbox"/>		Accessing Functionality Not Properly Constrained by ACLs	High		1	View Description
<input type="checkbox"/>		Accessing, Modifying or Executing Executable Files	Very High		17	View Description
<input type="checkbox"/>		Accessing/Intercepting/Modifying HTTP Cookies	High		31	View Description
<input type="checkbox"/>		Action Spoofing	Very High		173	View Description
<input type="checkbox"/>		Active OS Fingerprinting	Low		312	View Description
<input type="checkbox"/>		Analog In-band Switching Signals (aka Blue Boxing)	Very High		5	View Description
<input type="checkbox"/>		Analytic Attacks	Medium		281	View Description
<input type="checkbox"/>		API Abuse/Misuse	Medium		113	View Description
<input type="checkbox"/>		Application API Button Hijacking	Medium		388	View Description
<input type="checkbox"/>		Application API Message Manipulation via Man-in-the-Middle	Low		384	View Description
<input type="checkbox"/>		Application API Navigation Remapping	Medium		386	View Description
<input type="checkbox"/>		Argument Injection	High		6	View Description
<input type="checkbox"/>		Attack through Shared Data	Medium		124	View Description
<input type="checkbox"/>		Audit Log Manipulation	Medium		268	View Description
<input type="checkbox"/>		Authentication Abuse	Medium		114	View Description
<input type="checkbox"/>		Authentication Bypass	Medium		115	View Description

Figure 14

Getting Started with ThreatModeler

Manage Mitigation Steps

The user is presented with the existing list of mitigation steps. These can be edited. The user can also add new mitigation steps by a simple text box at the top of the screen. These mitigation steps help an organization promote their secure coding standards and guidelines to their development teams. The screen is as in [Figure 15](#).

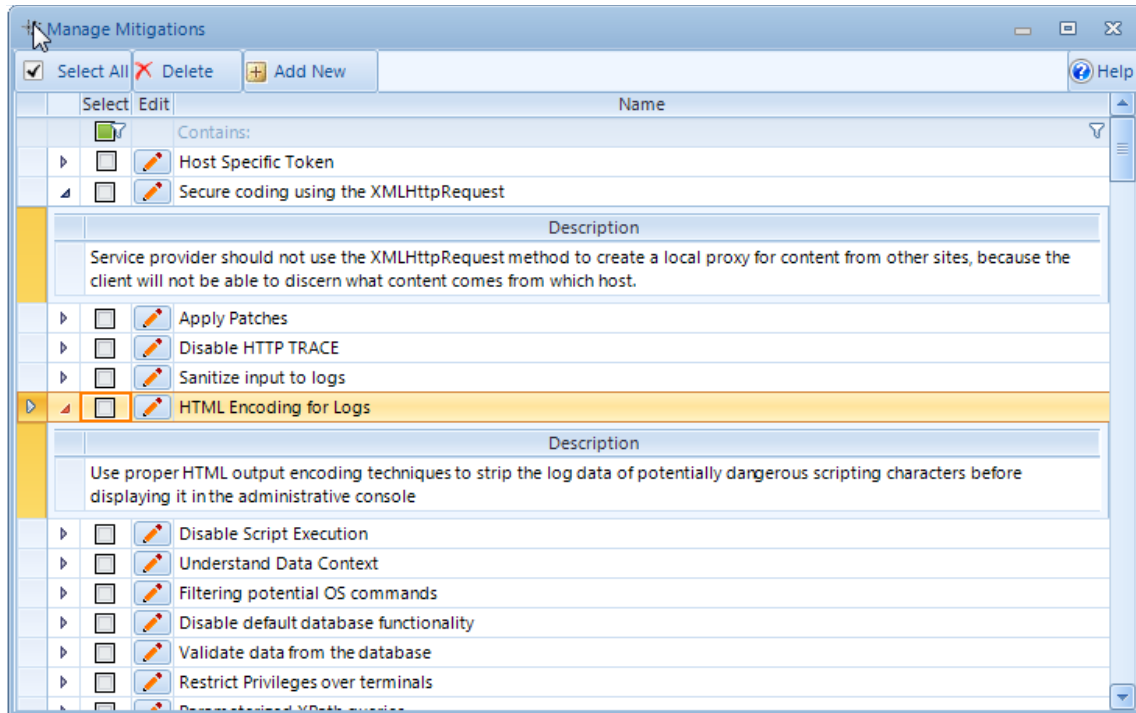


Figure 15

Getting Started with ThreatModeler

Manage Question Library:

The user can edit or add new questions to the Security Assessment Checklist section from here. The user is advised in the option of creating a new question to frame the question in such a way that by answering yes to the question, the threats will be mitigated. The categories are arranged according to various aspects of implementing security controls and best practices such as Authentication, Authorization, Encryption etc. This makes it easier to evaluate the security of the application and verify compliance to policy. The user can completely customize this checklist and add their own categories as well. The Manage Questions screen is as shown in [Figure 16](#).

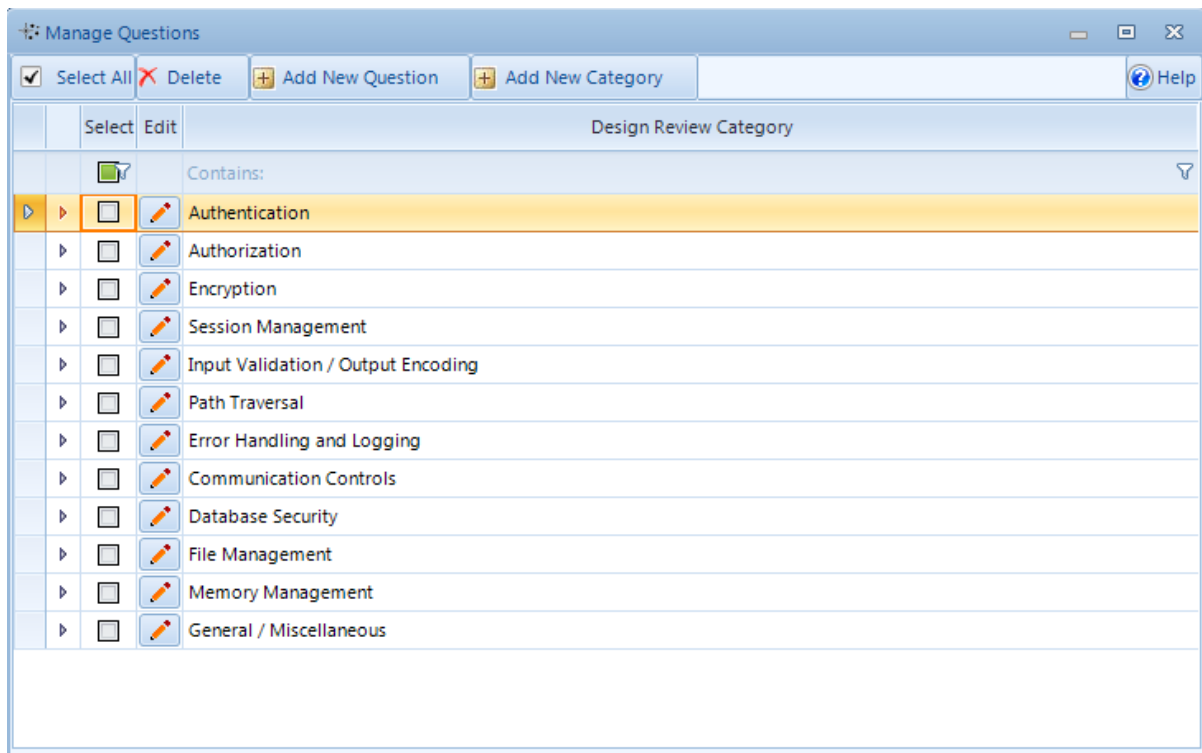


Figure 16

Getting Started with ThreatModeler

Manage Technical Controls:

Technical controls are widgets commonly used across web applications to collect or return information to the user after it is processed at the server. It also helps server keep state information of clients. In ThreatModeler™ we have provided some of the commonly used technical controls and the user can add their own as well. These Technical Controls have to further be mapped to a backend and threats. For example, a form taking user input can be mapped to a database and SQL Injection, Persistent Cross-site Scripting, and Blind SQL Injection are the corresponding threats mapped to it.

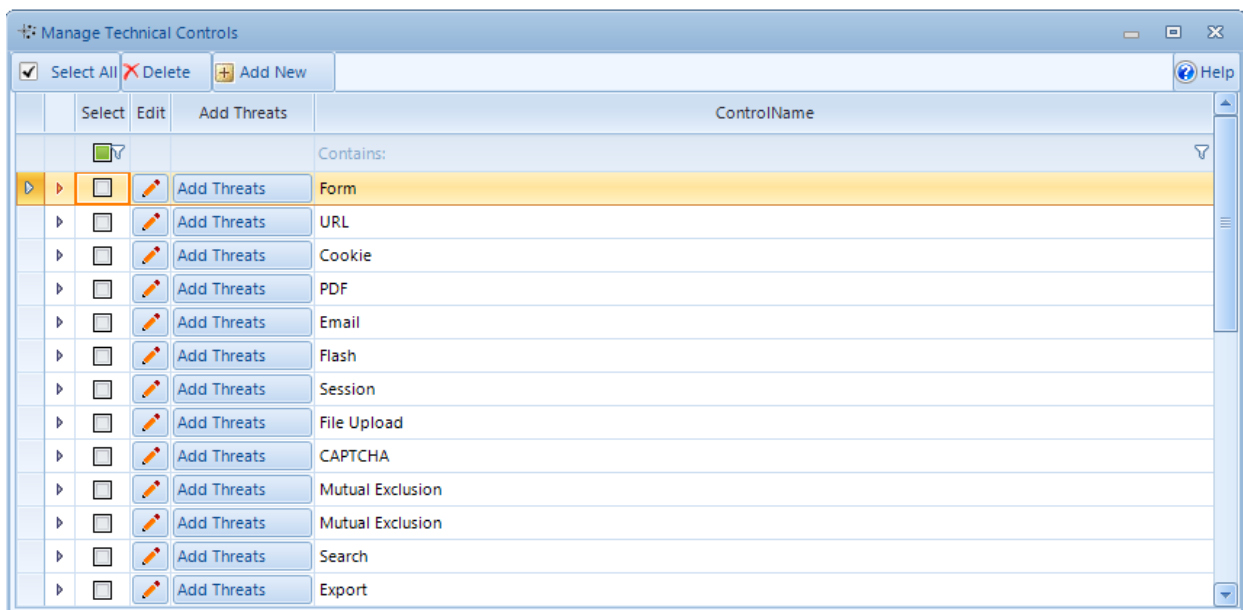


Figure 17

Getting Started with ThreatModeler

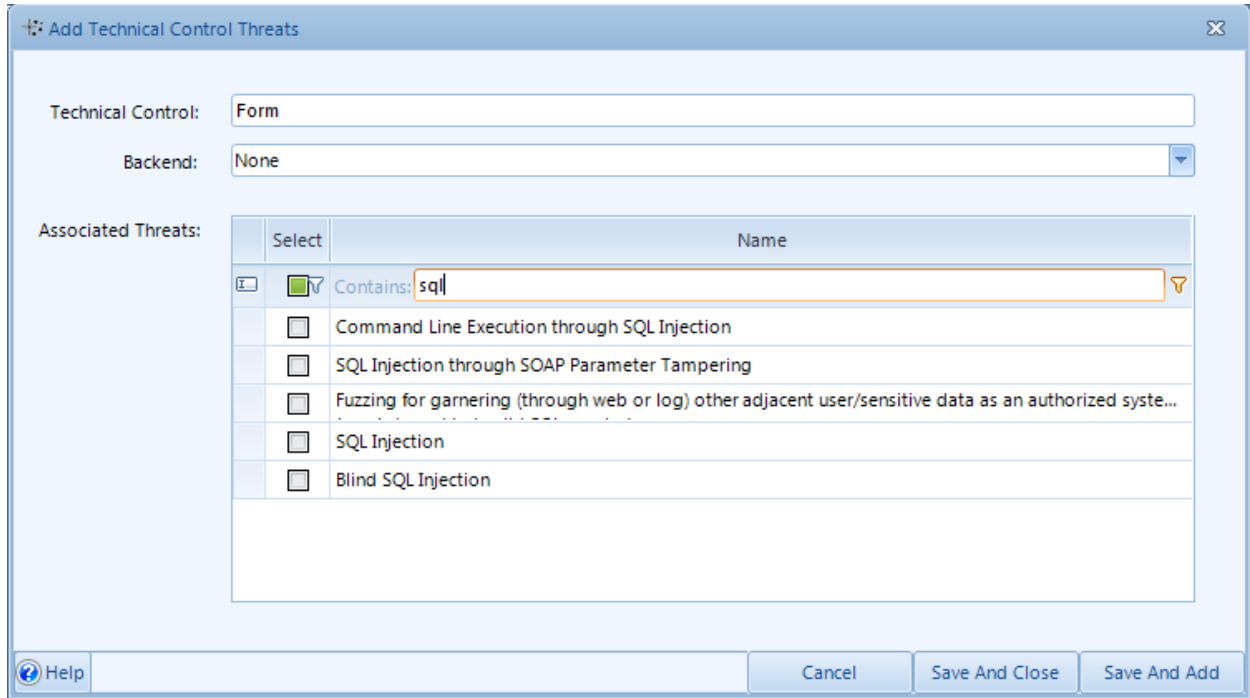


Figure 18

Getting Started with ThreatModeler

Manage Data Elements:

At this screen, the user can add data elements which will be processed by the web application. Associated with a data element is a classification category which is mapped internally to threats. This helps the user gauge the risk to data when performing a threat analysis after the threat model has been created. The user may also add custom data elements and assign a data classification category to them. A bulk upload is possible as well by adding a CSV file with two columns, the first being the name of the Data Element and the second being the classification of the data according to its sensitivity i.e Public, Restricted or Confidential. Default classification will be set to public if not specified in the CSV file.

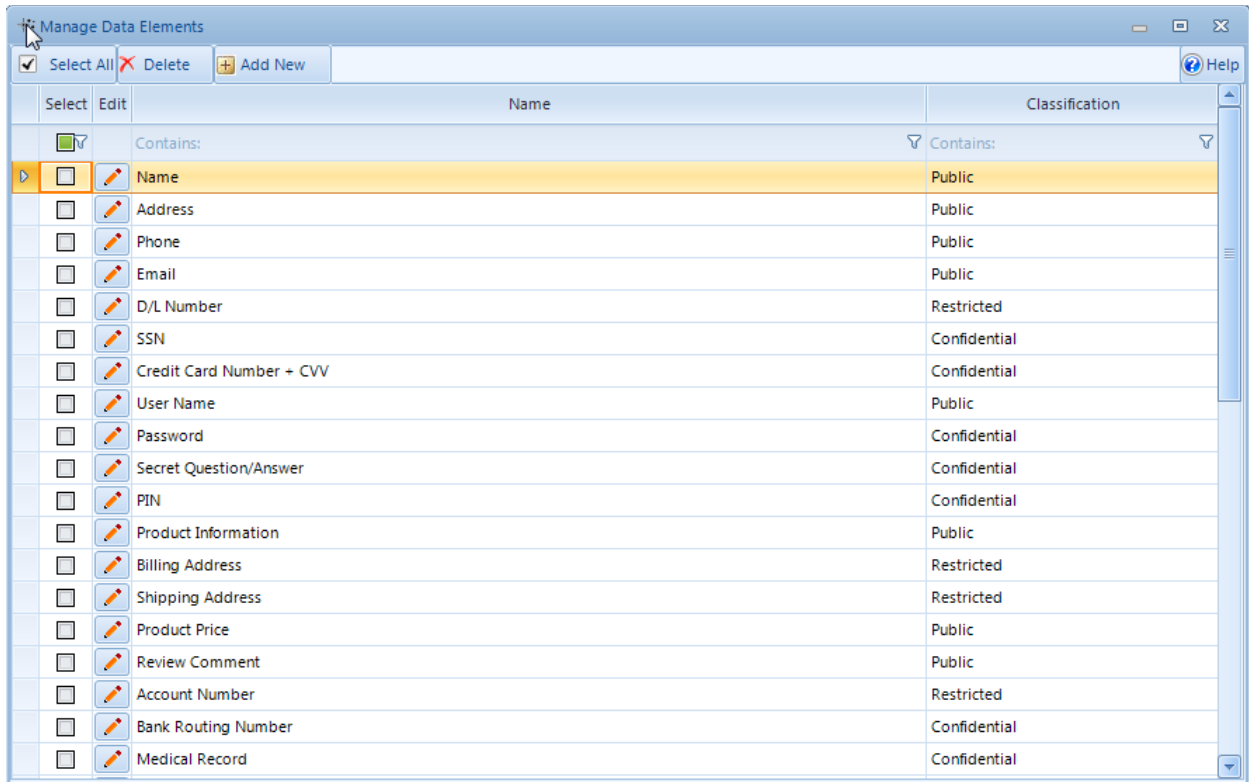


Figure 19

Getting Started with ThreatModeler

Manage Protocols:

The user can add communication protocols which are to be used in the Threat Modeling whiteboard and associate a color with it. The protocol is represented as an arrow linking one component to another and represents the logical process flow. This is useful in evaluating the security of communication between components especially when sensitive data is being transmitted. The screenshot is as in [Figure 20](#)

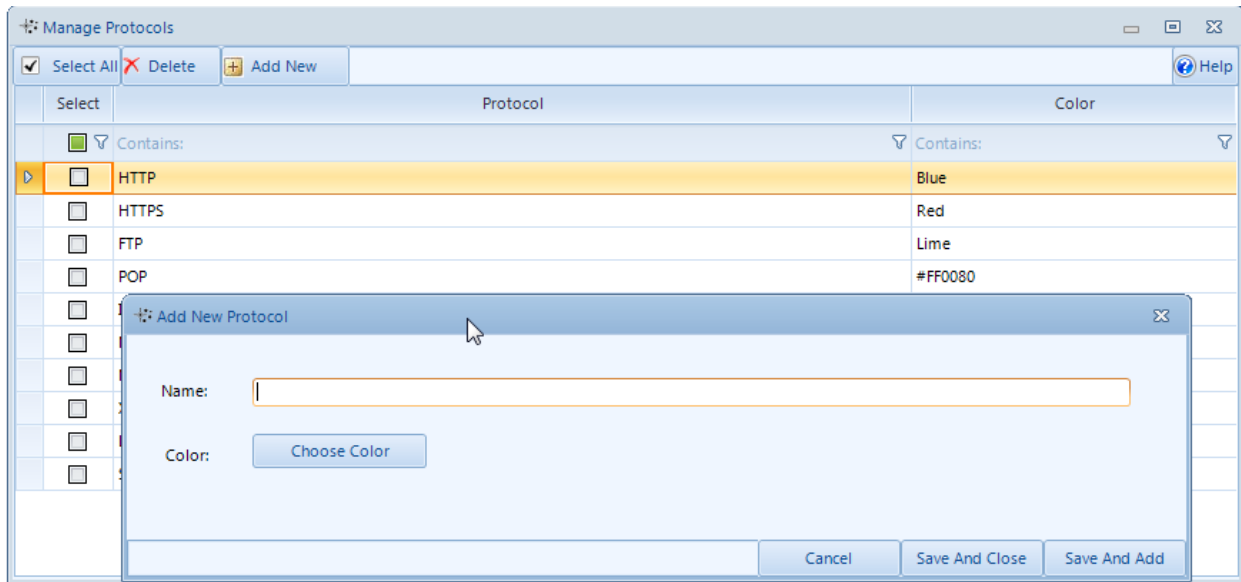


Figure 20

Getting Started with ThreatModeler

Manage Components:

Components are denoted by icons (with an ideal resolution of 32x32 px). The Admin has to add components by selecting images and assigning Rules to these. This in turn automatically generates an Attack Tree. The layout of this Attack Tree can be edited from the Manage Components screen. [Figure 21](#) shows the Manage Component screen. [Figure 22](#) is a screenshot of the Add / Edit screen for a component and the block to assign rules to it. The user can upload multiple components at a time via the Bulk Upload button as seen in [Figure 22](#). Mapping these components to rules and security requirements is a feature which helps you scale across all your applications. For example if you have multiple applications that require a 'Login' component, by mapping your component with your company, regulatory compliance and industry standard requirements for authentication, you have ensured that these requirements are promoted through all your applications by this feature. For a visual approach, click Edit under the Threat Patterns column, right-click the component name and click 'Add Rules'. In this way you can create attack trees making it easy for an architect with little or no security knowledge to ensure maximum coverage of company security requirements.

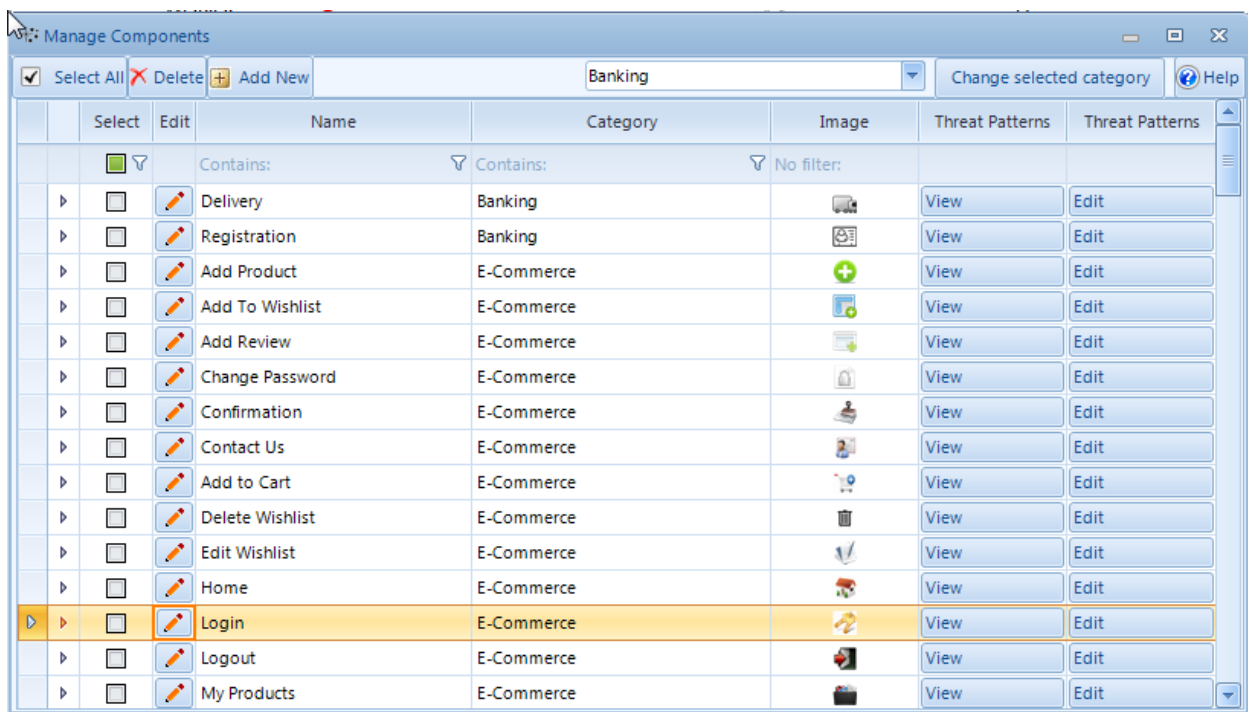



Figure 21

Getting Started with ThreatModeler

Add New Component

Name:

Classification: Banking

Upload an image:  (*Max file size is 1MB)

Assign Rules:

Select	Rules
<input checked="" type="checkbox"/>	Contains: <input type="button" value="Filter"/>
<input checked="" type="checkbox"/>	Amount should be less than the maximum limit and greater than 0. bank account has to be greater than 0.
<input type="checkbox"/>	Use out of band communication to prevent Man in the middle attacks
<input type="checkbox"/>	Implement Captcha or a challenge question
<input type="checkbox"/>	Implement Token or captcha
<input type="checkbox"/>	Account Lockout has to be 3 unsuccessful attempts

Figure 22

Getting Started with ThreatModeler

Manage Rules:

Rules are the various Security Requirements that should be implemented in the web application's architecture as part of security best practices to minimize known threats and to alleviate damages that can be caused by script kiddies and automated scripts. Failure to implement these rules as part of development or deployment can lead to several gaping vulnerabilities which can be exploited. These threats are displayed in the Threat Management console where the user decides on mitigating them.

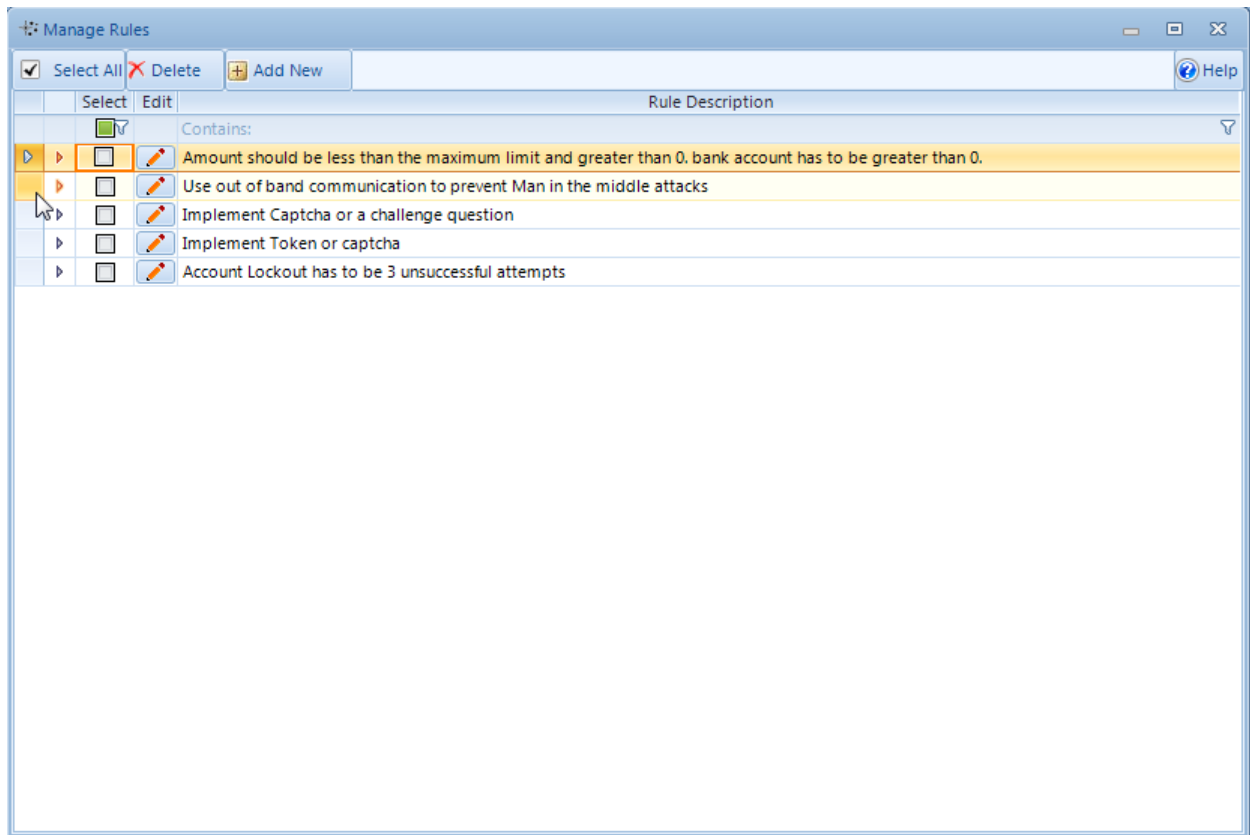


Figure 23

Getting Started with ThreatModeler

Manage Roles:

These are roles that are defined by the Organization's hierarchy. If a Role-Based Access Control policy is being implemented, this feature makes it simple for the developer to implement various policy requirements within the code.

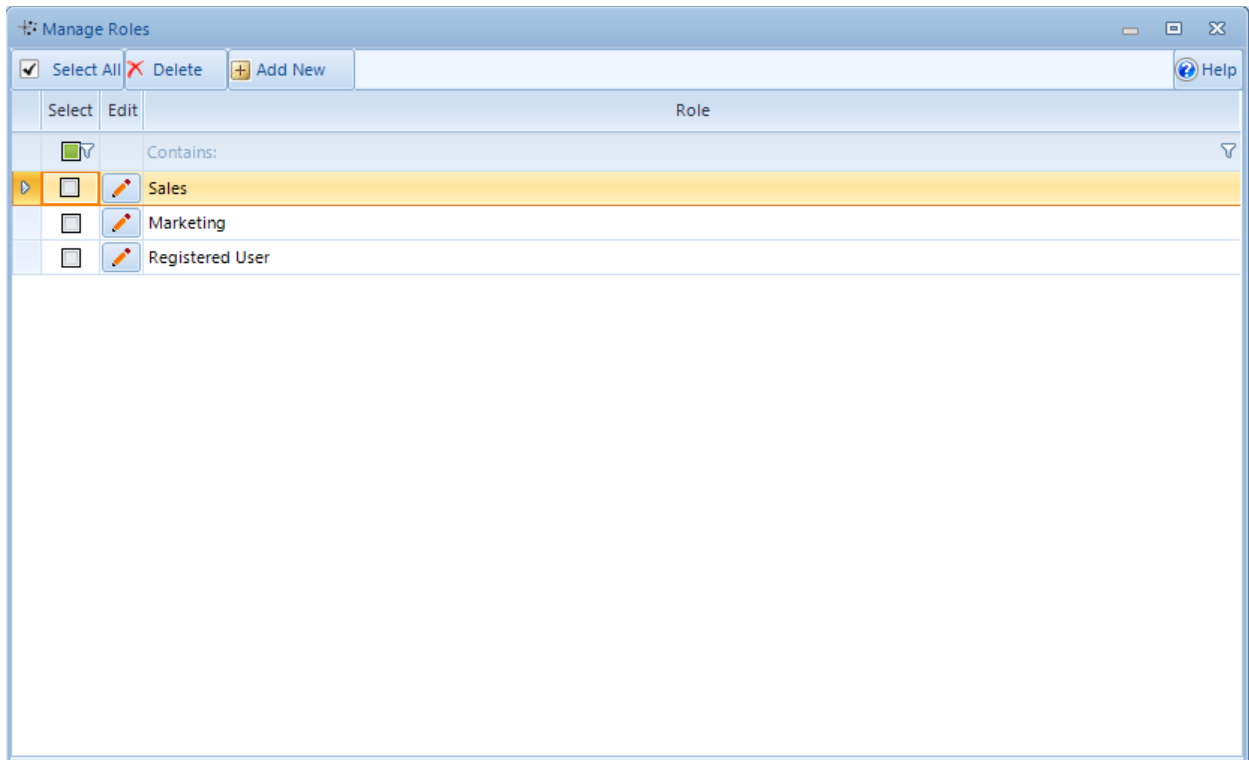


Figure 24