

|  |  |
| --- | --- |
| Microsoft Threat Modeling Tool 2016  Getting Started Guide | |
| Microsoft Trustworthy Computing |  |

Contents

[Overview 2](#_Toc431822582)

[Installation 2](#_Toc431822583)

[For Previous Users of Threat Modeling Tool 2](#_Toc431822584)

[System Requirements 2](#_Toc431822585)

[Download Link 2](#_Toc431822586)

[Uninstall 2](#_Toc431822587)

[How to Run Threat Modeling Tool 3](#_Toc431822588)

[Starting Threat Modeling Tool 2016 3](#_Toc431822589)

[Creating a New Threat Model 3](#_Toc431822590)

[Opening an Existing Threat Model 10](#_Toc431822591)

[Converting Previous Threat Models to latest Format 11](#_Toc431822592)

[Overview of Template 13](#_Toc431822593)

[Creating a New Threat Template 13](#_Toc431822594)

[Open an Existing Template 23](#_Toc431822595)

[Upgrading an existing Threat Model to use New Template 25](#_Toc431822596)

[Analysis of Threat Modeling Tool Output 27](#_Toc431822597)

[Analysis View 27](#_Toc431822598)

[How to File Bugs on your Threat Modeling Tool Security Issues 28](#_Toc431822599)

[Support 30](#_Toc431822600)

# Overview

The Microsoft Threat Modeling Tool (TMT) 2016 is designed to guide you and your product team through the threat modeling process. TMT functionality includes:

* An easy drawing environment.
* Automatic threat generation using the STRIDE per interaction approach.
* Define your own template for threat modeling
* An option for user-defined threats to be added.

Using Microsoft Threat Modeling Tool (TMT) you can graphically identify processes and data flows that comprise an application or service.

# Installation

## For Previous Users of Threat Modeling Tool

If you have TMT 2014, it must be un-installed before installing TMT 2016. All the models created using TMT 2014 can be opened using TMT 2016.

## System Requirements

### Operating System Support

The table shows the operating systems supported by Microsoft Threat Modeling Tool 2016.

|  |  |
| --- | --- |
| **Operating System** | **Supported** |
| Windows 7 | **Yes** |
| Windows 8 | **Yes** |
| Windows 8.1 | **Yes** |
| Windows 10 | **Yes** |

Table Supported Operating Systems

## Download Link

Microsoft Threat Modeling Tool 2016 and supporting documentation can be downloaded from <http://microsoft.com/security/sdl>.

## Uninstall

1. Go to Control Panel > Programs and Features.
2. Right-click Microsoft Threat Modeling Tool and select Uninstall.

# How to Run Threat Modeling Tool

This guide will provide basic guidance on how to create a new threat template and a new threat model. This Getting Started Guide covers:

1. Creating a new threat model
2. Opening an existing threat model
3. Converting a threat model from TMT(.tm4) format to the new TMT (.tm7) format
4. Creating a new threat template
5. Opening/Modifying an existing threat template
6. Upgrade threat model to new template

For more details about TMT, see *Microsoft Threat Modeling Tool* *2016 User Guide*, available at <http://microsoft.com/security/sdl>.

## Starting Threat Modeling Tool 2016

To start TMT, click the “Microsoft Threat Modeling Tool” **desktop shortcut**.

You can also start TMT from the command line. Open a command window and execute:

**%programfiles(x86)%\Microsoft Threat Modeling Tool 2016\TMT7.exe**

## Creating a New Threat Model

This section describes the steps to create a new threat model.

1. Start TMT. From Home screen, browse a template you want to use for the threat model.
2. Click on **Create a Model** from home screen. Thisbrings up the drawing surface where you will create the data flow diagram.

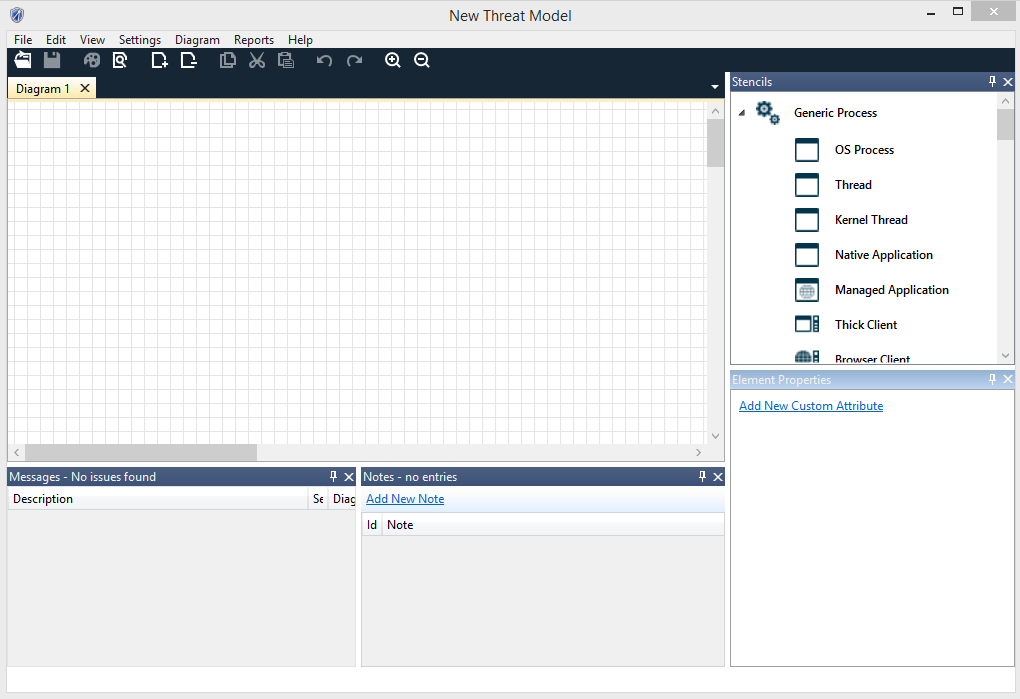


Figure Threat Modeling Tool Drawing Surface

### Drawing Your Model

Draw your data flow diagram by selecting elements from the **Stencils** pane. You can select processes, external entities, data stores, data flows, and trust boundaries.

1. To select an element to draw, click on the corresponding icon in the **Stencils** pane. You can also select an element from the **Stencils** pane and drag it across the drawing surface.
2. Right-click on the drawing surface to bring up a context menu that allows you to add a generic element from each **Stencils** category
3. To add a data flow between the two most recently selected objects, right-click the drawing surface and select **Connect** or **Bi-Directional Connect**. Alternatively, select the appropriate data flow from the **Flow** tab in the **Stencils** pane and place it on the drawing surface.

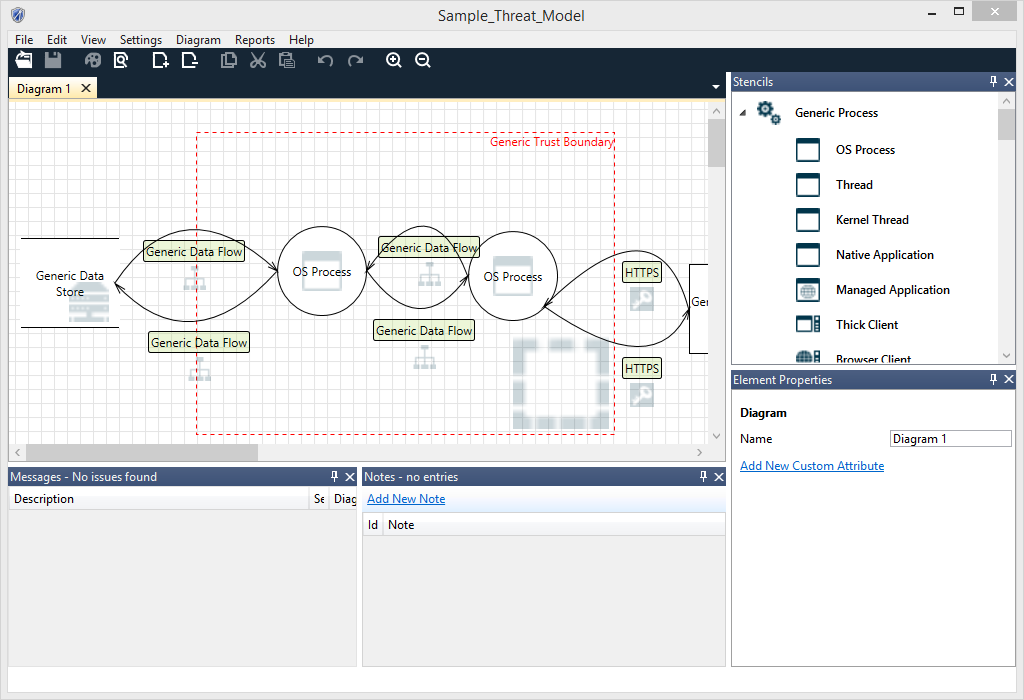


Figure Sample Threat Model Showing a Data Flow

1. To more fully describe the data flows in your system, specify attributes for the elements in your diagram. Right-clicking an element to convert it to another element type. If necessary, convert it from a generic element to a specific type of process, data flow, data store, external element, or trust boundary. For example, a generic data flow can be converted to HTTPS. Additionally, you can edit the properties of the element directly in the **Properties** pane.

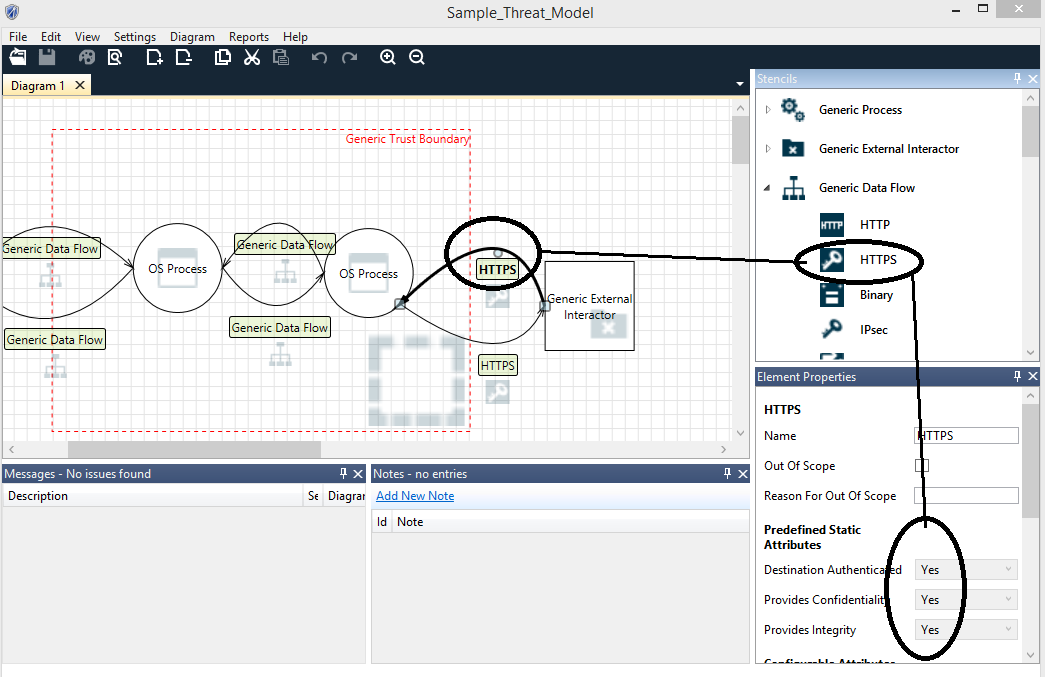
**

Figure Identifying a Data Flow as HTTPS

### Analyzing Threats

When you have completed your data flow diagram, switch to the Analysis view by using one of the following methods:

* From the View menu, select **Analysis View**.
* Click the **Analysis View** button on the toolbar.



Figure Selecting Analysis View from the Toolbar

### Entering Mitigation Information

For each of your threats, enter information about how to mitigate the threat:

1. Determine if the threat requires mitigation and categorize the mitigation by selecting one of the following options from the Threat Status dropdown list.
   1. Not Started
   2. Needs Investigation
   3. Not Applicable
   4. Mitigated

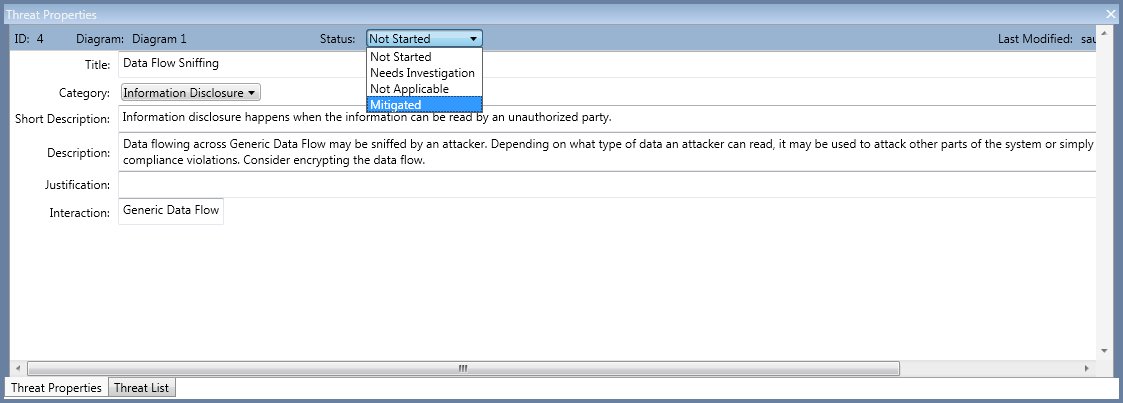
**

Figure Selecting Mitigation Information

1. Select one of the following threat priorities from the Threat Category dropdown list.
   1. High (default)
   2. Medium
   3. Low
2. Enter your mitigation information in the **Justification for threat state change** text box.

* NOTE: Justification is required for threats in the **Mitigated** or **Not Applicable** states.

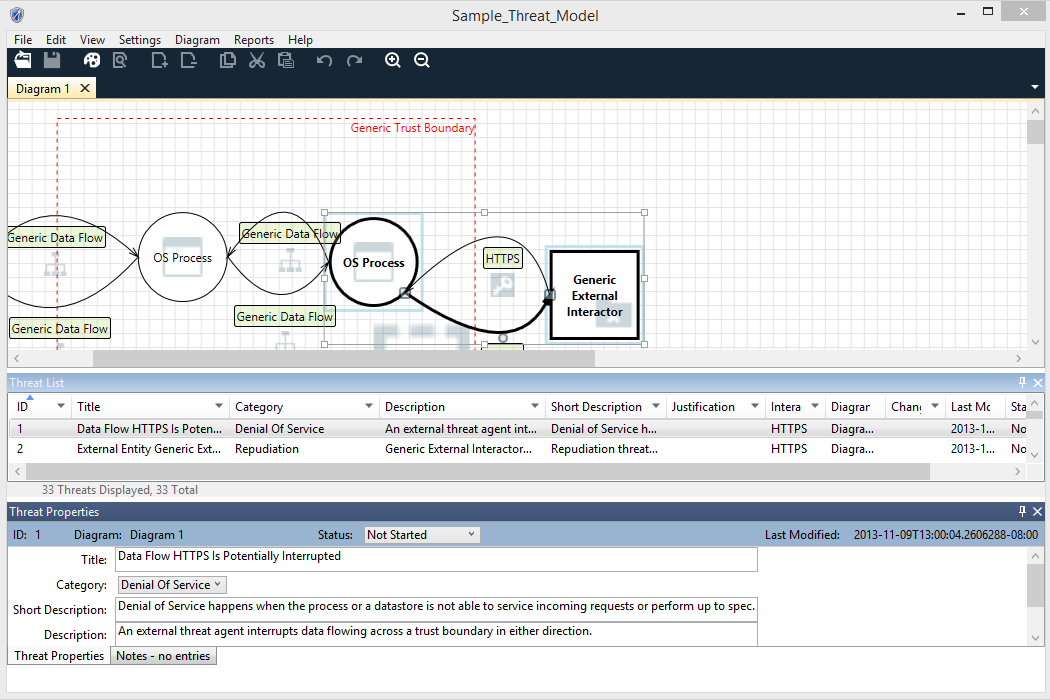
**

Figure Enter Justification for Threat State Change

### Reviewing Threats

The threat list is sortable and filterable. You can click on any column header in the threat list to sort by that column. You can click on the triangles on the column headers to filter as many columns as you like. The clear filters button at the bottom of the threat list will clear any filters. You can drag column headers to reorder them and right click column headers to hide or view them.

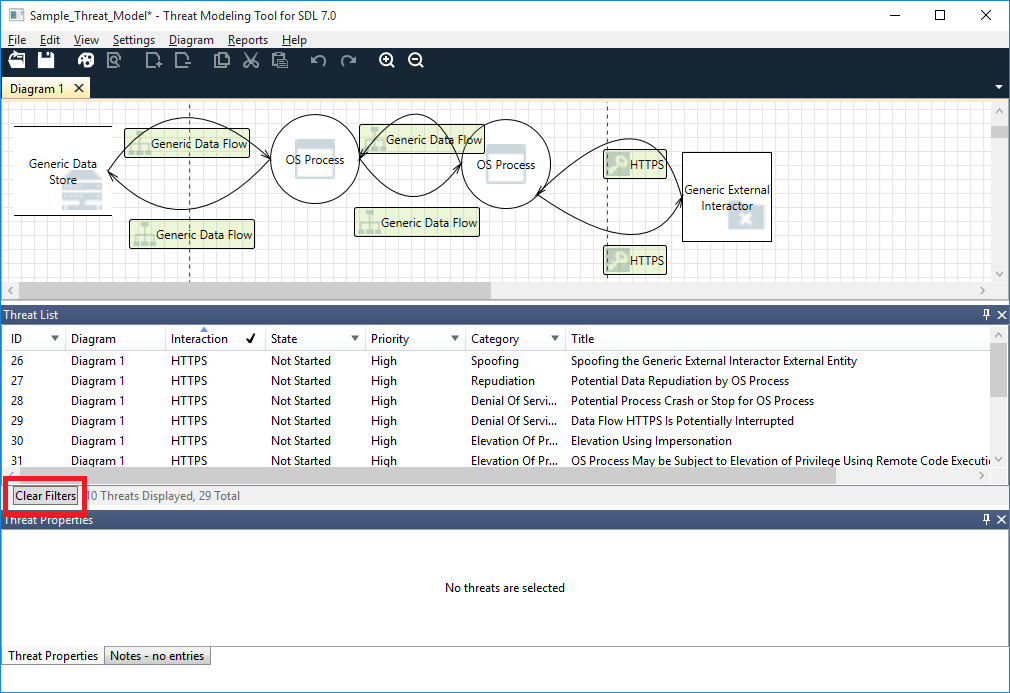


Figure Filter the Threat List

### Finish and Create a Report

After all threats have been addressed, finish your threat model:

1. If you have not done so already, enter general information about the threat model by selecting Threat **Model Information** from the main menu. This information includes:
   1. Review participants
   2. A brief description
2. To save the model, select **File >Save As.**
3. To create a report, select **Reports >Full Report.**

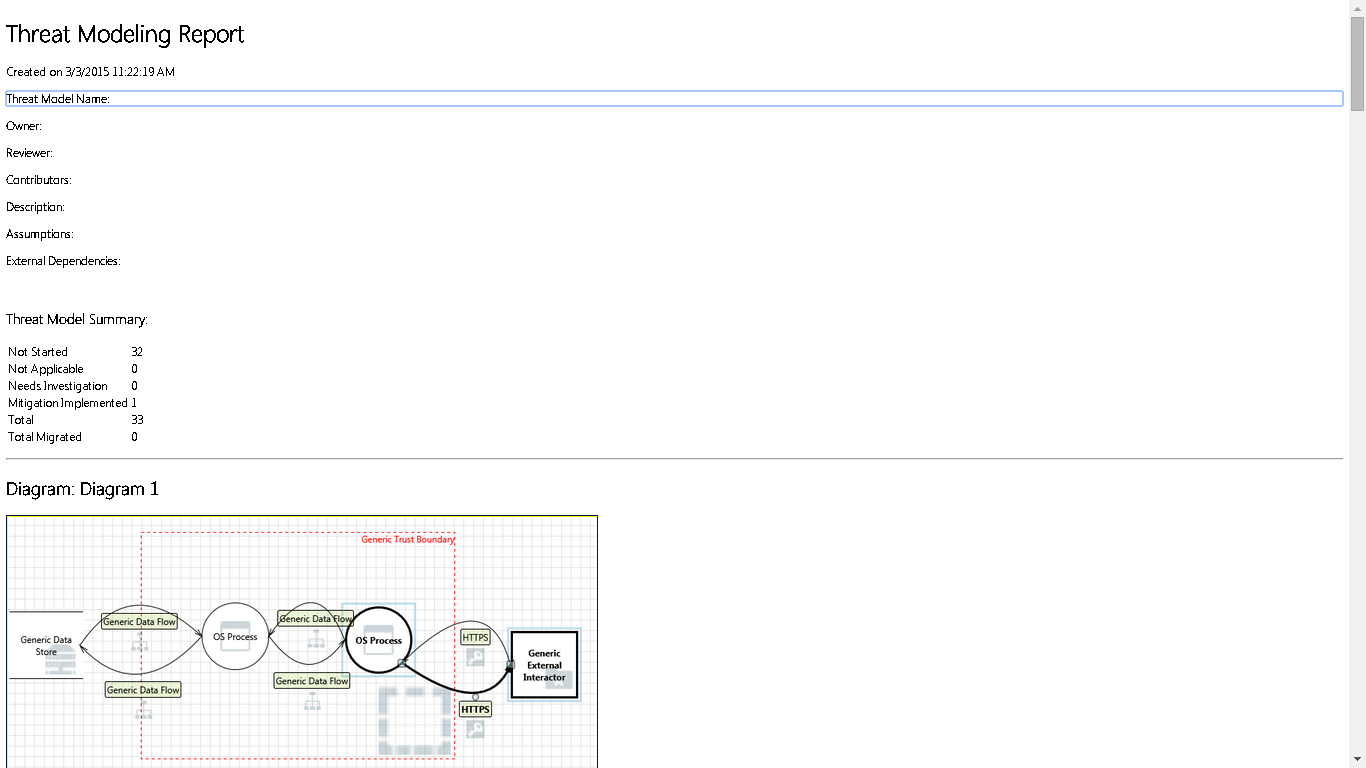


Figure Sample Threat Modeling Report

## Opening an Existing Threat Model

1. Start TMT, and from the Start screen, select the model you want under **Recently Opened Models**. If the model is not shown, select **Open A Model** and browse to the file.
2. To update the model, follow the steps described in “Creating a New Threat Model”.

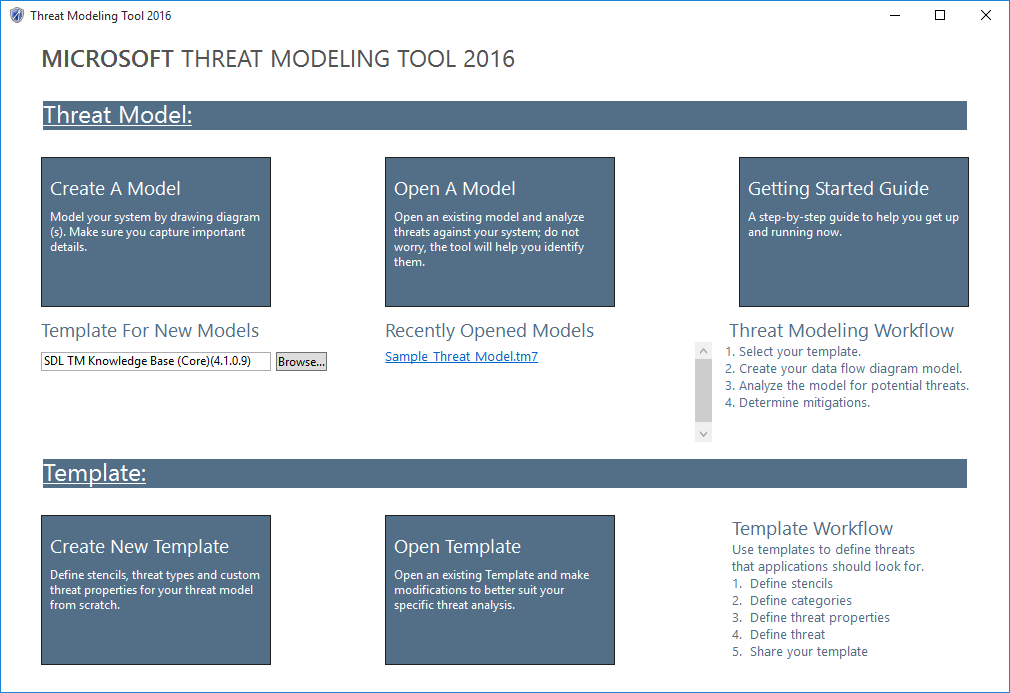


Figure Initial screen showing Recently Opened Models selected

## Converting Previous Threat Models to latest Format

You can convert your previous versions threat models to newer format.

If previous threat model is based on TMT 2014 (.tm4)

1. Click on **Open A Model** on Home Page screen
2. Select your .tm4 file after expanding file type drop down on file selection dialog box

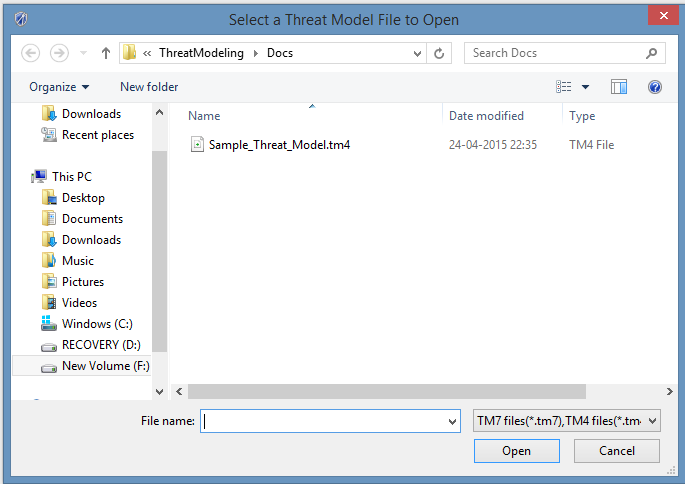


Figure Select .tm4 file

1. TMT will automatically convert .tm4 file to .tm7 file.
2. Save the file from **File->Save (Save As)** menu items.

**Note**: Your converted diagram may not look exactly the same as the original diagram, but all the elements should be present and connected correctly. Automatic threat generation is disabled for converted threat models. However, you can enable automatic threat generation through the **Settings** menu.

# Overview of Template

The Template specifies the set of elements, attributes, and threat definitions used by the Threat Modeling Tool to create threat models. Most of the time default template shipped with TMT is sufficient to analyze threats for your products however sometime depending upon your product requirements e.g. online services often also need to consider the business impact and privacy implications of the data managed by the service. In this case default template is not sufficient and new template is needed. Open template can be used to edit an existing template and new template can be used to create an altogether new template. In order to create threat models which are based on template created by you, use Browse button from home page to select required template.

## Creating a New Threat Template

This section describes the steps to create a new template.

1. Start the Threat Modeling Tool and from the Home screen click **Create New Template.**
2. **Template Information** dialog box pops up. Fill Title which you need for template and also version number for your template in Title and Version fields respectively.

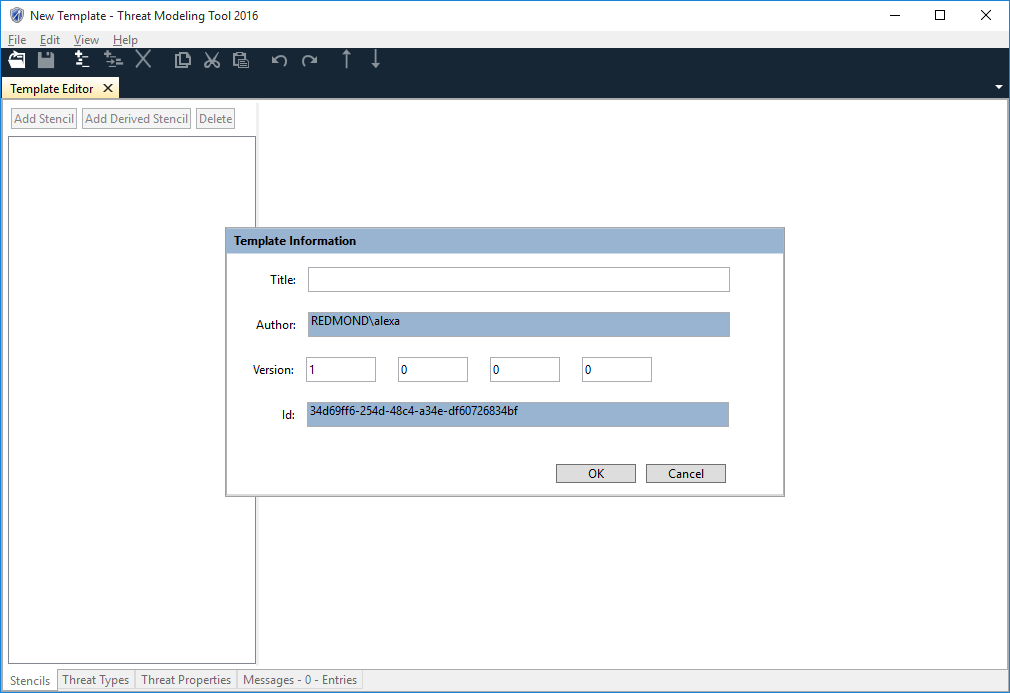


Figure Template Information

1. Click Ok on **Template Information** dialog box. This brings up **Template Editor** which you can use to create **Stencils**, **Threat Properties**, **Threat Categories** and **Threat Types**. During the template creation process, if some error occurs, message for the same will appear in Message tab.

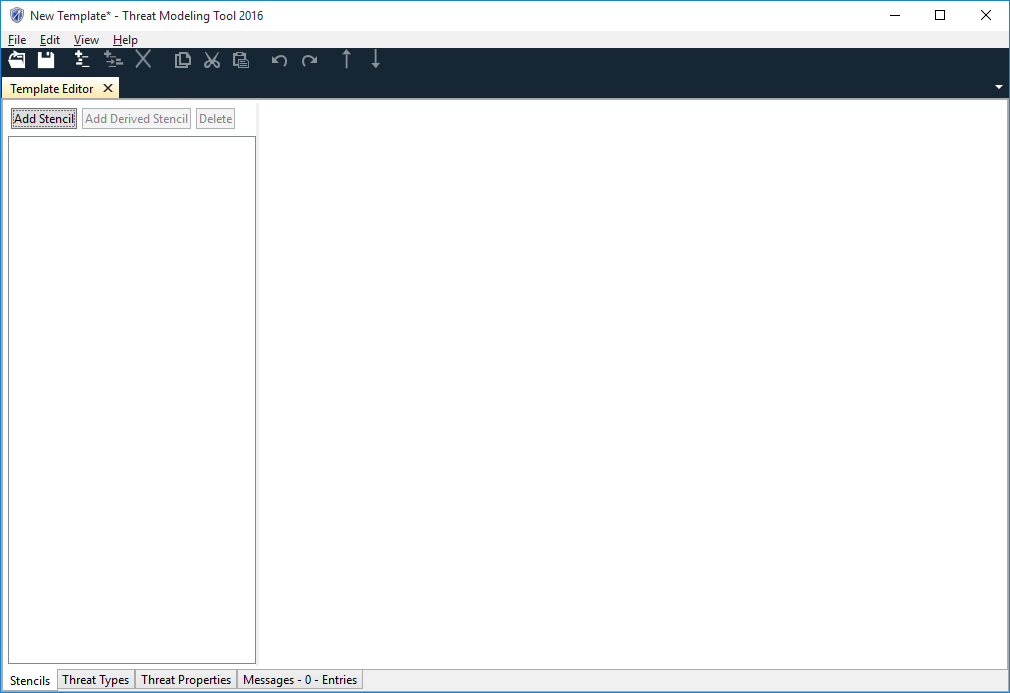


Figure Template Editor

### Creating a Stencil

Stencils are the basic building blocks for creating threat models. **Stencils** tab can be used to create two types of stencils namely Stencils and Derived Stencils. These stencils will show up in the stencil pane of threat model window while creating threat model.

1. Click the **Add Stencil** button at the top of the **Stencils** tab to create a **Stencil**. A new stencil gets created with a default name **New Stencil**. Modify the name as per your requirements.

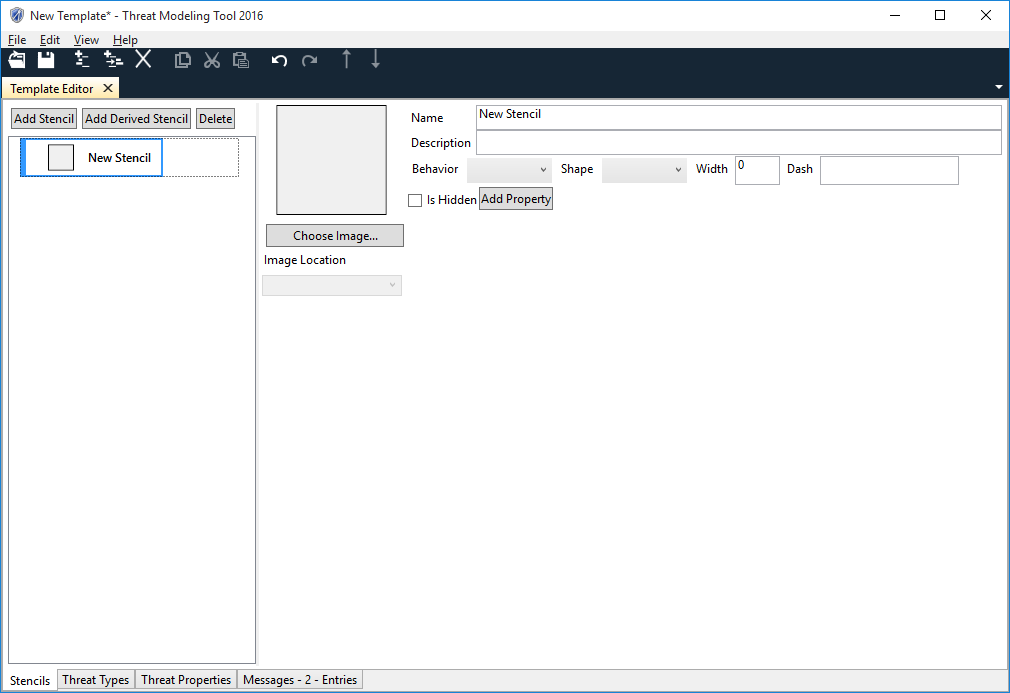


Figure Stencils Tab

1. Choose **Image** for the stencil.
2. Choose **Image Location** for Image. This location will be used to display image while creating threat model.
3. Assign **Behavior** and **Shape** for the stencil.
4. Define **Width** and **Dash** attributes of Stencil.
5. Define **Properties** and **Values** for each property for stencil by clicking **Add Property** button below the name of the stencil.
6. Optionally you can create **Derived Stencils**. Click on a **Stencil** and click the **Add Derived Stencil** button at the top of the **Stencils** tab.
7. The derived stencils inherit properties of the parent. Additionally Standard Stencils can define their own properties.

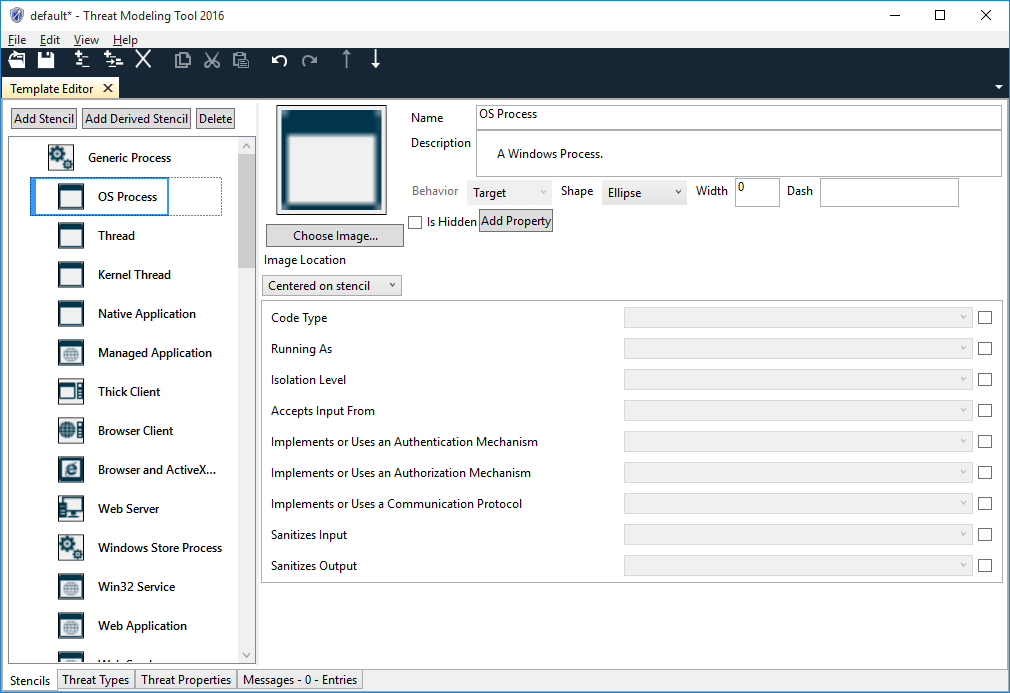


Figure Standard Elements

1. You can reorder properties and properties values.

### Creating Custom Columns

By default Threats have Description, Short Description, Justification, Interaction and Priority columns. If you click on **Threat Properties tab**, these rows are shown greyed out except Priority column since these cannot be modified. These properties will appear as columns in the threat list and threat properties panes in the analysis view of the threat model unless you have marked them as hidden.

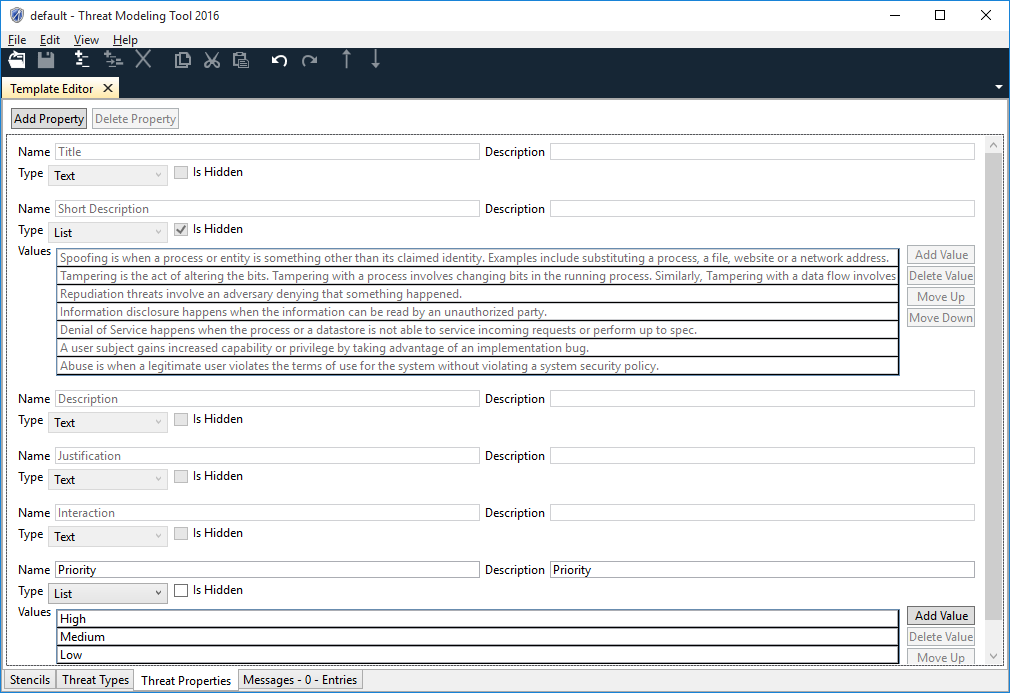


Figure Threat Properties

1. You can add custom threat properties by clicking on **Add Property** button on the Threat Properties page. The system creates a new custom threat property with the name **New Threat Property**.
2. You can modify the name by clicking on the Name field and modifying it. Name is compulsory and can’t be empty.
3. There are two types of threat properties. One is Text and the other is List. The Text type is used when the property takes just one value. The List type is used when the property can take any one of the multiple values present in the list.
4. The **Type** is by default set to **Text**. If you select **Text** then value field gets disabled. This is because the actual value will be given when the property will be used while defining a new threat type.
5. If you don’t want to show this threat property as column in Threat List in threat model, choose **Is Hidden** as selected.
6. When the type is set to List, the user can add property values by clicking the **Add Value** button. By clicking the **Delete Value** button, one is able to delete property values.

### Defining Threat Category and Threat Types

Go to **Threat Types** tab to create **New Threat category** and **New Threat type.** TMT compares the stencils on the DFD in the threat modeling design view against the threat types to determine which threats to create in analysis view.

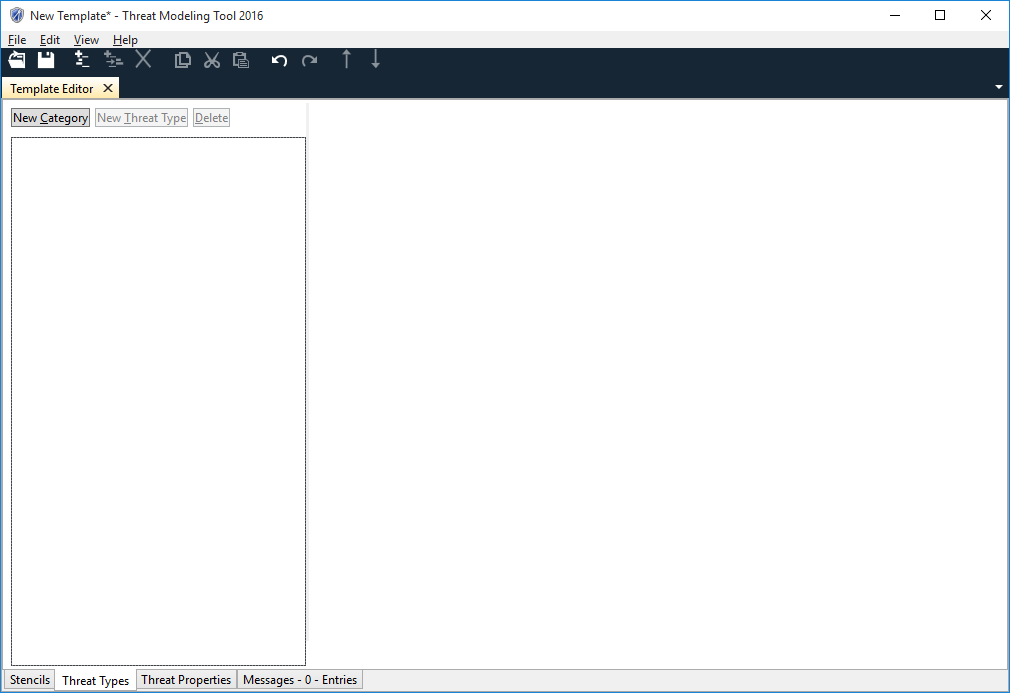


Figure Threat Category

1. Click on **New Category** buttonon **Threat Types** tab to create new threat category
2. Click on **New Threat Type** button to create a Threat Type under a Threat Category

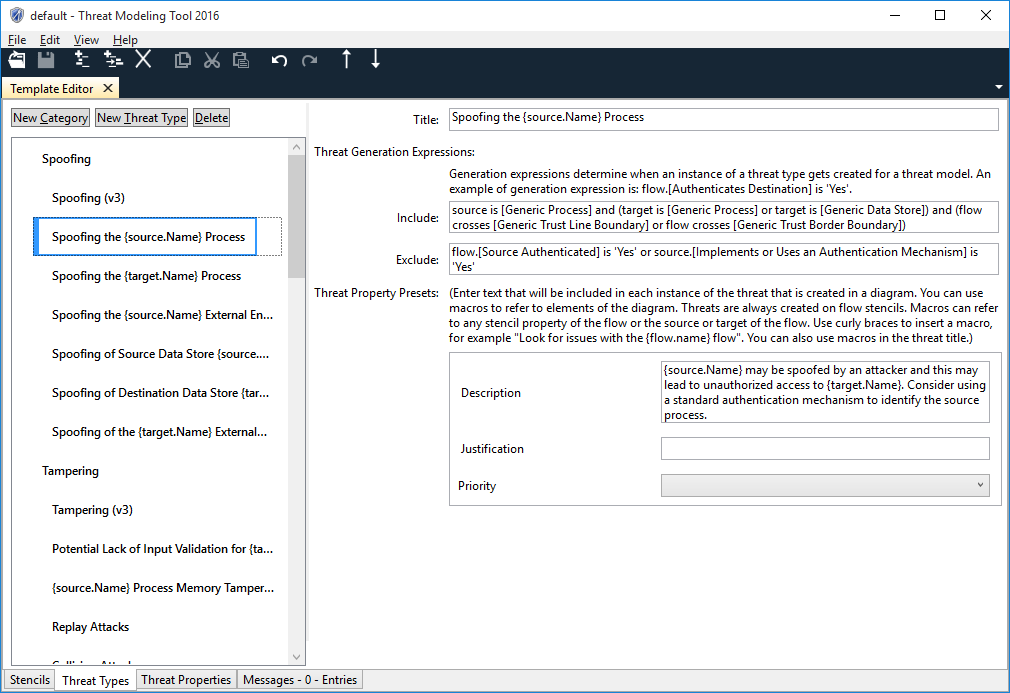


Figure Threat Types

1. Define **Title** of Threat Type by clicking Title text box on the UI
2. Define **Include** and **Exclude** expressions for Threat Type. Expressions reference objects in the design view to determine when to create a threat in the analysis view. Grammar for expressions is as follows:

The grammar for creating the Threat Expression is given below.

<rule> ::= <expression> { <op><expression> }

<expression> ::= <object>[.<property>] IS <value>  |  Flow crosses <entity\_id> | [ NOT ]( <expression> )

<object> ::= Source | Target | Flow

<property> ::= [Stencil Property Name]

<value> ::= ‘Stencil Property Value’

<entity\_id> ::= [Stencil Name]

<op> ::= AND | OR

1. Define values for other columns for the threat like **Description**, **Justification**, **Priority** and any other custom column you might have defined in **Custom Column** screen. The values in the fields can be plain text describing information about the fields corresponding to threats. You can add presets. Presets helps in creating dynamic text for the field. E.g. if you want to define text for the Description field which contains information about the flow for the threat you can define text for the field like “Description of threat for {flow.Name}”. In the analysis view when the threat is generated, the preset expands to get name of the flow the threat applies to.

### Error Reporting

The fourth tab present in the template editor is the Error Messages tab. This tab is not used for your configuration but is a notification window that indicates errors or warnings that have occurred in the system based on some user configuration. E.g. while creating a stencil there are 2 mandatory fields which need to be configured. If either of these 2 is not set by the user then an error message is logged in this window indicating to the user that there is an error.

The Error message window is a dock able window. This means that the error message window can appear as a dock able window upon double-clicking any error message in the Messages Tab will cause the tab to turn into a dock able window and attach itself to one of the 3 tabs i.e. Stencil, Threat Types or the Threat Properties.

The user can then use the arrow keys or the mouse to select the error notification from the list and look at the control which is causing the error. The control in question is highlighted using a red colored border and the parent object (Stencil, Threat Type) is highlighted using a red colored box.

The **Messages** window allows the tool to identify any errors, warnings or inconsistencies in the Template. In order to use the template in Threat Model creation, all the issues appearing in Message tab must be fixed.

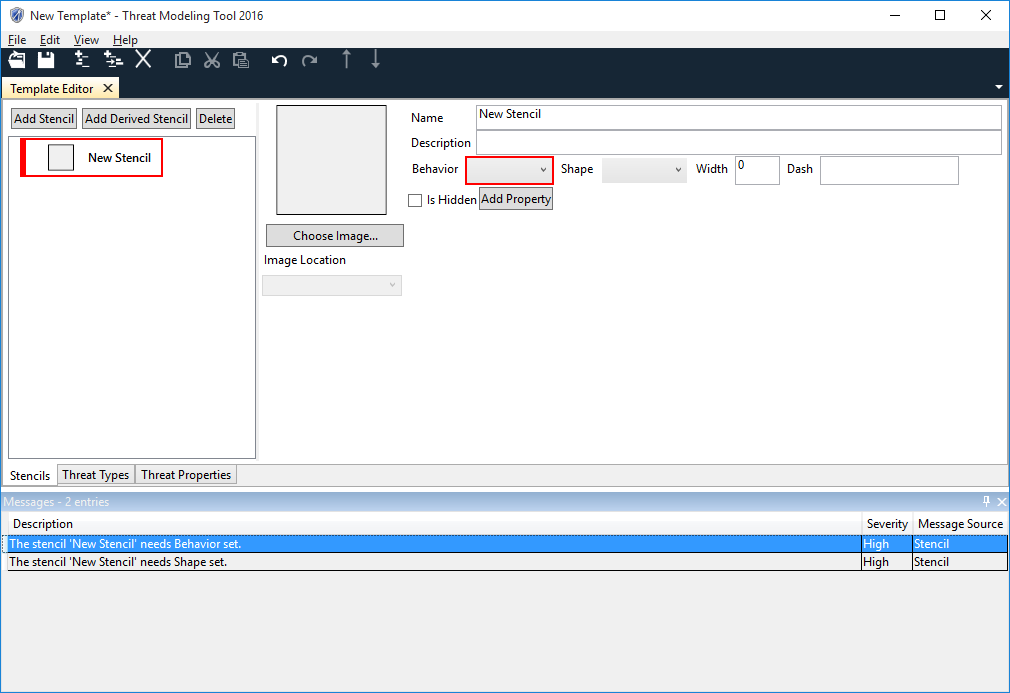


Figure Error Reporting

### Save Template

1. Click on the *menu button*, and then click **Save** Page. The ***Save As*** dialog window will open.
2. In the dialog window, type in a name for the page you want to save and choose a location. In the *Save as type* drop-down, choose the type of file that you want to save the page as: *TB7 files(\*.tb7)*

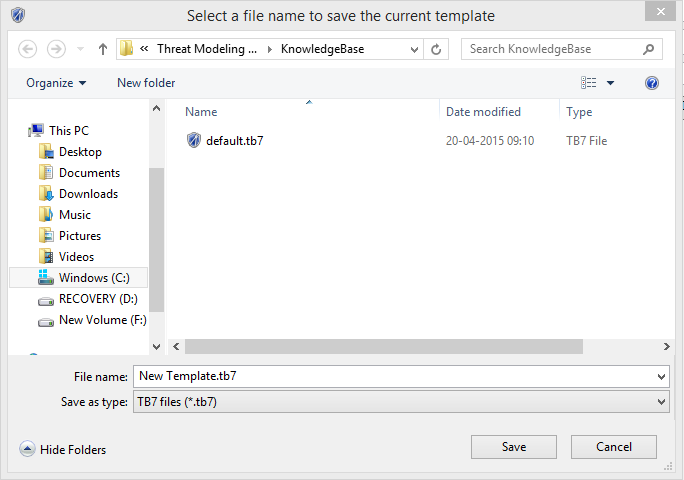


Figure Save Template

1. Click **Save**. A copy of the page will be saved as the type you specified in the location you chose.

## Open an Existing Template

You can open an existing Template to view/edit the template.

1. Click on the ***Open Template*** *on Home Page*. The ***Open***dialog window will open.

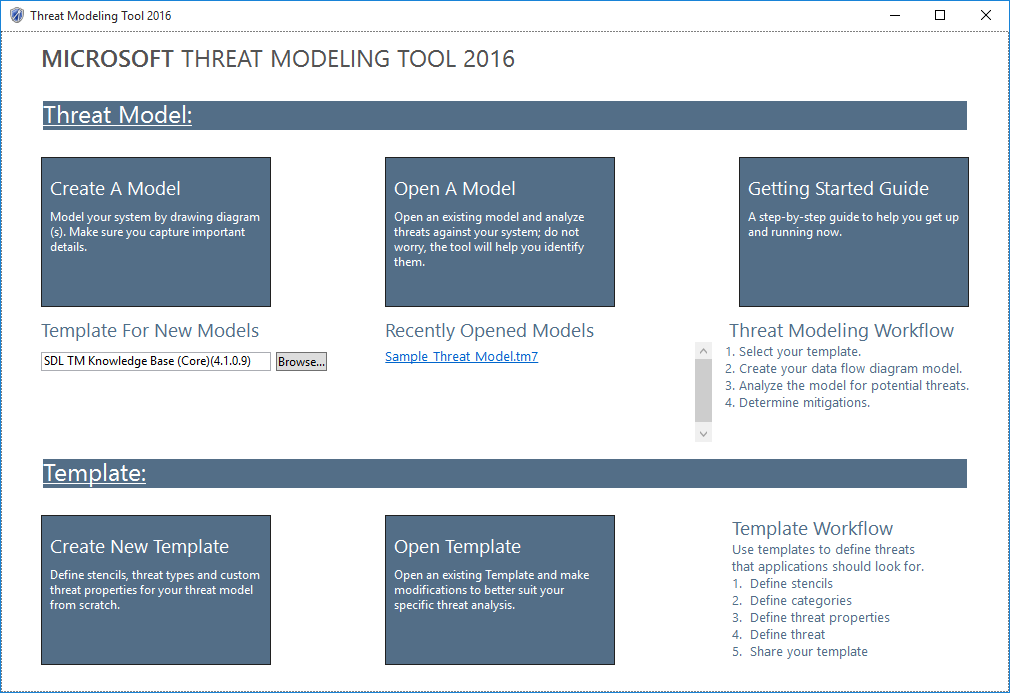


Figure Home Page

1. In the dialog window, type in a name for the template you want to open or you can select template file from given list. In the *File name* drop-down, choose the tb7file that you want to open the page as: *TB7 files(\*.tb7)*

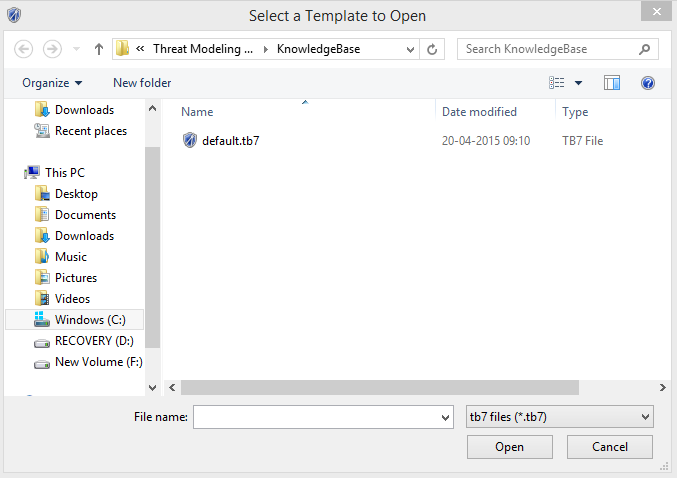


Figure File Open

1. Click***Open***. A tb7 file will be opened as the type you specified in the location you chose.
2. To update the template, follow the steps described in “Creating a New Threat Template”.
3. Alternately you can double click on template file and it will open template in template editor if TMT is installed on the machine.

## Upgrading an existing Threat Model to use New Template

You will be encountering scenarios where a threat model was created using some version of template. Later on a security team/PM or other teams in the group may create a refined template which covers more security cases. You might want to upgrade your previous threat models to this new template so that if there are more security issues, you can identify them. The apply template feature applies a new template to an existing threat model.

1. Click on Open A Model on home page
2. Go to **File -> Apply Template**

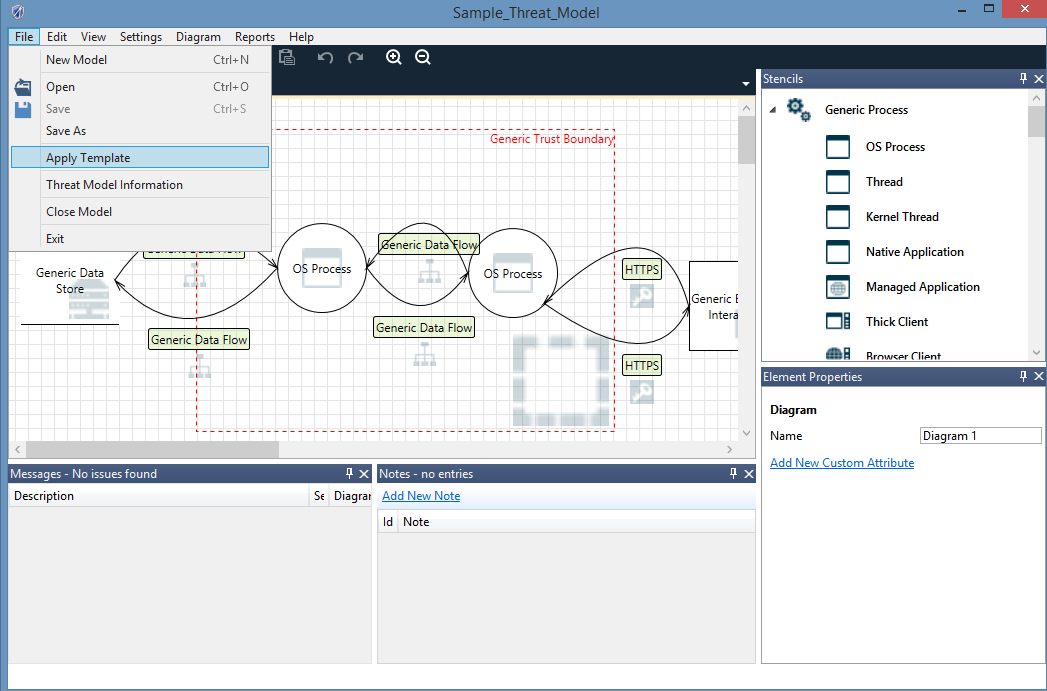


Figure Apply Template

1. Select the template which you want to apply to upgrade threat model to
2. Select **Yes** on the Confirmation Dialog box and also make a choice to delete the stale threats or keep them

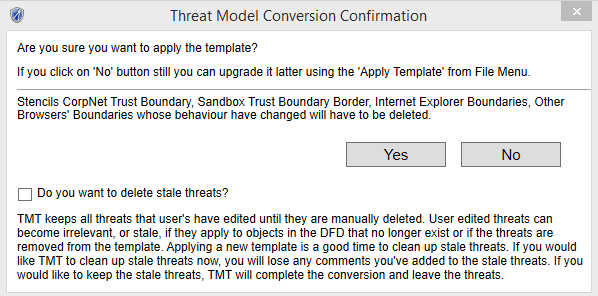


Figure Confirmation Dialog for Upgrade

1. Save upgraded Threat Model using **File -> Save/Save As or Ctrl + S**

# Analysis of Threat Modeling Tool Output

## Analysis View

The **Analysis** view allows you to analyze the threats generated for your diagram, identify which threats are not applicable, require investigation, require mitigation, or have been mitigated and verified. For models that have multiple diagrams, the threat list displayed is global and includes threat entries for all diagrams.

### Threat Information

After a model is drawn, you will be presented with a list of threats. You’ll find the list of threats organized in a grid that shows for each threat:

* Threat Title
* Threat (STRIDE) Category
* Justification
* Interaction
* Diagram
* Last modified
* Threat State
* Threat Priority

Each threat will have a **Description** field**,** which will have content for every auto-generated threat and a **Justification** field in which mitigation information can be entered by the user.

For newly generated threat models, the setting for auto-generation threat mode is enabled by default. For migrated threat models created with Threat Modeling Tool 3.1.8, the auto-generation threat mode is set to off. To turn it on go to **Settings** and select **Enable Threat Generation**. Each threat will have options that enable you to manage the identified threats. By default, the state of all newly generated threats is **Not Started**.

|  |  |
| --- | --- |
| Default state for newly generated threat    Mitigation implemented and verified | Mark threat as needs mitigation    Mark threat as not applicable |

Threats are generated using STRIDE per interaction. An interaction is defined by two elements connected by a data flow, and may include a boundary. If an element is marked **Out of Scope** threats will still be auto-generated for that interaction but the element itself will have visual feedback that is marked **Out of Scope**. You can also add a user-defined or custom threat by right-clicking on the desired data flow in the interaction and selecting **Add User-defined Threat**. When you do so you’ll find your custom threat at the end of the existing threat list.   
  
Threat priority is by default set to **High.** As applicable, it can be changed to **Medium** or **Low**.

### Threat List Filter

**Threat List Filters** are available on selected columns. All the columns where threat filter is possible, filter icon  is displayed. Clicking on this filter button will show available options for threat filtering e.g. clicking on filter button against Category button displays options as shown in below screen

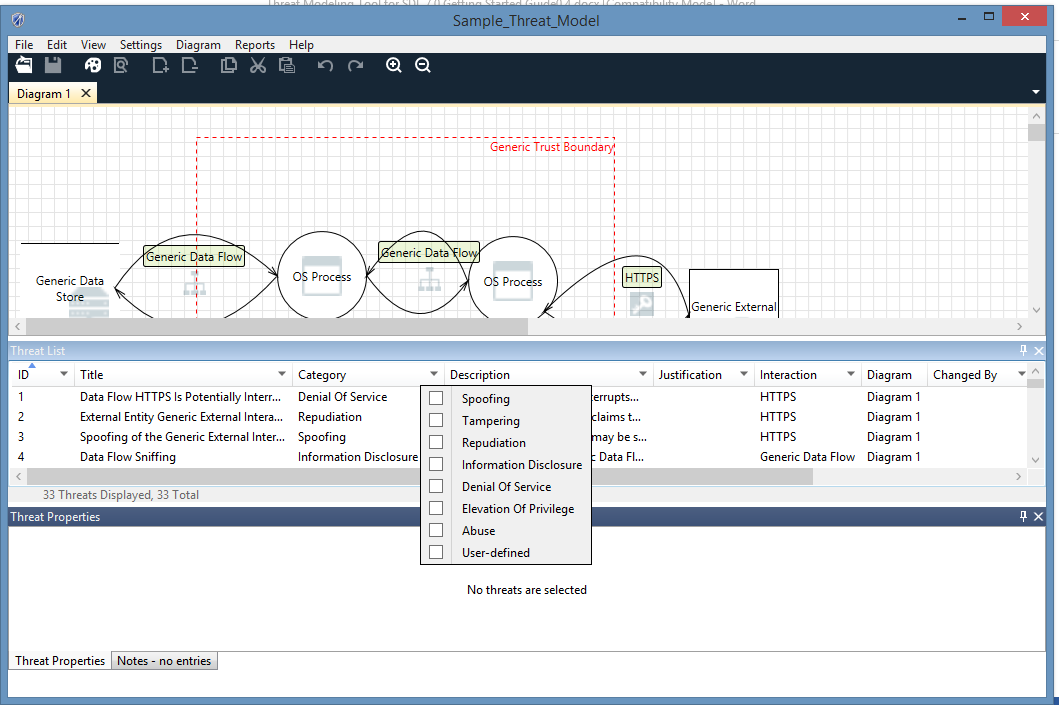


Figure Threat List Filter

# How to File Bugs on your Threat Modeling Tool Security Issues

You may want to track the security issues found by Threat Modeling Tool in your team’s work item tracking tool (i.e. TFS or VSOnline).

To create a bug from **Analysis** view:

1. Select a threat to create a bug for.
2. Right-click the threat and select **Copy threat(s)**.

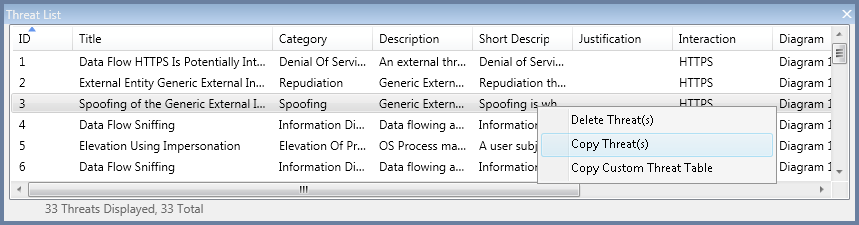


Figure Copying a Threat

Your threat information is copied to the clipboard in the following format:

* THREAT: Spoofing of Destination Data Store Generic Data Store
* CATEGORY: Spoofing
* DIAGRAM: Diagram 1
* INTERACTION: Generic Data Flow
* PRIORITY: High
* STATE: Not Started
* DESCRIPTION: Generic Data Store may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Generic Data Store. Consider using a standard authentication mechanism to identify the destination data store.
* JUSTIFICATION: <none provided>

You can now paste the copied information in a bug tracking system of your choice.

**NOTE**: You can select all threats in your list to be copied to the clipboard by pressing CTRL+A then and right-clicking **Copy Threat(s).**

Select **Copy Custom Threat Table** to use the clipboard content to paste into Microsoft Excel and then bulk-import into a bug tracking system of your choice. You can do so for a single threat or all of them by selecting all entries using CTRL+A.

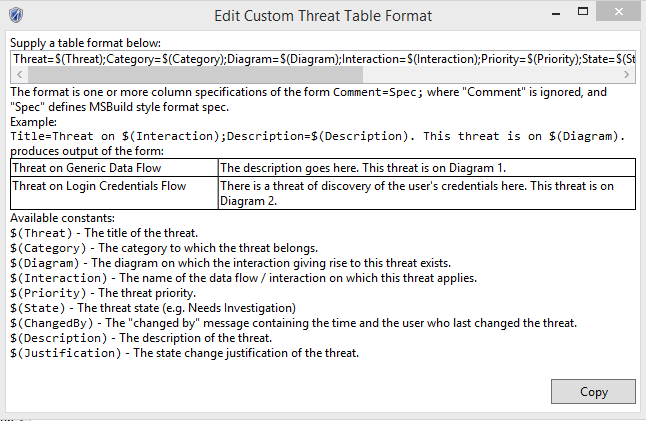


Figure Edit Custom Threat Table Format

# Support

For support, please visit the following links:

* [Microsoft Security Development Lifecycle](http://www.microsoft.com/security/sdl/default.aspx)
* [Microsoft Trustworthy Computing Blog](http://blogs.technet.com/b/trustworthycomputing)
* [MSDN Forums for SDL](http://social.msdn.microsoft.com/Forums/en-US/home?forum=sdlprocess)

Copyright © 2015 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.