Table of Contents

Part I Themida 1

1 Why use Themida? ... 1

Scenarios for using Themida ... 1
Comparing Themida with other protectors/licensing systems ... 2

2 User Interface ... 3

Themida GUI overview ... 3

3 Protecting an application ... 5

Application Information ... 5
Protection Options ... 7
Protection Macros ... 10
Virtual Machine ... 13
Customized Dialogs ... 16
XBundler ... 19
Plugins ... 23
SecureEngineInitialize ... 25
SecureEngineFinalize ... 25
SecureEngineShowCustomMessage ... 25
SecureEngineGetEncryptionKey ... 27
Extra Options ... 28
Advanced Options ... 30
Protect Now ... 32
Protecting through the command line ... 32

4 SecureEngine® Macros ... 35

Using macros in your programming language ... 36
VM macro ... 39
Mutate macro ... 41
StrEncrypt macro ... 42
Unprotected macro ... 43
CheckProtection macro ... 44
CheckCodeIntegrity macro ... 46
CheckVirtualPC macro ... 49
CheckDebugger macro ... 50
Which Macros should I use? ... 52

5 FAQ ... 52

General ... 53
I want to protect several applications concurrently via the command line, because I'm creating a specific protected application for each customer. Is it possible? ... 54
I want to include relative paths in the "Input Filename" and "Output FileName" in the User Interface in Themida. How can I do that? ... 54
Is Themida compatible with Delphi 2009? ... 54
Is Themida compatible with Windows 8? ... 54
I'm using SetupBuilder to build and protect my application from the command line. The application is protected correctly but I don't see any log in the command line. ... 54
In my program I use the "JCLDebug" routines to get exception information (line, routine, etc) when an exception occurs. The problem is that once the application is protected, I get limited debug information. ... 55
What's the difference between Themida and WinLicense? If I buy WinLicense, can I use it without adding license control to my software? ... 55
Are there localized versions of your products to support other languages? ... 55
I bought a Themida license to protect my applications. My friend needs to protect his application. Can I protect his software with Themida? ... 55

I have a suggestion about a new protection feature and features for your software. Will you implement it? ... 55
What programming languages are supported by your products? ... 55
If I protect my app with the demo version and it is stable, do I have a good level of confidence that the purchased version will work also? ... 55
What is your support policy? Do you have a minimum response and/or problem-solving time? What types of support do you offer? ... 56
How compatible is your software with various win O/S? (e.g. Vista in different languages, 2003 server, 64bit etc.) ... 56
I don't use Windows Vista right now, but depending on our customers I will need Themida (and also the protected application as well) to be able to run on Windows Vista. Do you also support 64-bit operating systems such as Windows 2003 x64 and Vista x64? ... 56
I have problems protecting my installer. What can I do? ... 56

Protection Options ... 57

Can I use Themida from a computer with no internet connection or better under a VirtualBox/VMWare environment? I was wondering if internet is required for Themida to work. ... 60
Do I need to ship SecureEngine.dll with my protected application? ... 60
I use Themida with Visual Studio in the custom build steps but no output (build information) is generated at all. What's the problem? ... 60
I'm evaluating Themida DEMO to protect my Windows service, but after protecting it my service does not start at all. What should I do? ... 60
How can I avoid the command line output displayed by Themida when protecting my project via the command line protection? ... 60
My application requires administrator's privileges to run on Vista. Will my protected application run with admin's rights? ... 60
My (native) protected application fails to run after being protected. What can I do? ... 60
My .NET protected application fails to run after being protected. What can I do? ... 61
My CodeJock application looses skinning after being protected. What can I do? ... 62
My protected application is flagged as a virus. What can I do? ... 62
My MSVC application generates a crash dump file (.DMP) file when it crashes, so I can load and examine the crash dump file. When my application is protected the generated crash dump does not contain valid information ... 63
Is it possible to know from my application if the application has been unpacked? ... 63
I need to get a Vista logo. Is your protection compatible with Microsoft tests? ... 64
I want to protect my .NET application with Themida, can I use an obfuscator before protecting with Themida? ... 64
How can I omit the output displayed by WinLicense when protecting via command line? ... 64
Can you let me know which protection options affect execution speed of my application? ... 64
I'm using the CHECK_CODE_INTEGRITY macro in my Delphi application but the macro always returns that my code has been modified. Any ideas? ... 64
I see that Themida detects if my file on disk has been patched, but how can I detect if someone has patched my application in memory? ... 64
How can I insert my own splash screen using the Plugin feature? ... 65
Can you let me know about all available Advanced Options and what they are for? ... 65
Some of my users complaint regarding RegMon (Filemon) loaded in memory. How to proceed? ... 65
If I want to sacrifice a minimal amount of security to gain the maximum amount of application startup speed, what options should I disable in Themida? ... 66
Can I compress my application with UPX and then protect it with Themida? ... 66
Is there any issue to run my protected plugins on Xp 64 (32bit mode)? ... 66
My application's main function is the scientific calculation needed high performance. Is there any performace lost when I encrypt my app. with Themida? ... 66
Does Themida encrypt string constants in my code? ... 66
If I set the Anti-Patching option, can I digitally sign my application? ... 66
I would like to include the same protection options and custom dialogs in all my applications. Can I apply the same settings to all my applications? ... 67
I want to include Themida in my build system. Does Themida support command line protection? ... 67
Can I protect my Windows NT system service with Themida? ... 67
When I protect my application with Themida, the size is increased by 500Kb or more! ... 67
How many KB will my application grow in size, after being protected by Themida? ... 68
When I use macros directly around some API calls I get errors in Themida saying that one of my START or END markers is missing. What's wrong? ... 68
Please let us know how Themida influences the program performance? What would you advice us to pay attention to in order to minimize the performance losses? Will it affect the protection? ... 69

If I use the option "Entry Point Virtualization", my DLL crashes. If I uncheck that option, will it make it easier to crack? ... 69
Can I protect my .NET applications with Themida? ... 69
I'm happy with all the protection features offered by Themida, but I miss the trial/licensing features. Will they be included? ... 69
Can I get the computer Hardware ID with Themida? ... 69
Can I protect mixed managed/unmanaged DLLs? ... 70
When I enable the "Advanced API-Wrapping" option my applications runs slower ... 70
When my STR_ENCRYPT macros are processed in the last "Protection" panel, I can see "skipped" when the macro is processed. What can I do? ... 70
When I protect my application with an older version, the size of the protected application is smaller. Can I keep the same size in latest version? ... 70
When I add a JPG image in the splash option, my image is not displayed on startup ... 70

Macros ... 71

I have a function with a VM_START/END. Inside the START - END macro markers, I call an external function, called "Function2()". Is that external "Function2()" also virtualized? ... 72
I have put a VM macro in my "main()" function. Inside the VM_START/END markers I'm calling several functions. Are those called functions also virtualized? ... 72
I have a few Portuguese strings in my STR_ENCRYPT macro but some of them are not recognize when I click on the STR_ENCRYPT macro in the "Protection Macros" panel. What's wrong? ... 73
Can I use one protection macro (VM macro) inside another macro (VM macro)? ... 73
In the "custom_vms" folder I can see the name of the available virtual machines. Can I change the internal settings inside each ".vm" file? ... 74
Can I raise an exception inside a VM macro? ... 74
I have seen that insertion of VM macros in try-except clauses are a bit tricky. What about try-finally clauses? ... 74
Can Themida macros protect switch statements and try-except clauses? ... 75
If I protect the following code with a macro: VM_START InitializeCounters(i); VM_END. Will the InitializeCounters() function code also virtualized? ... 76
I have included several VM macros inside my application. I have made sure that I have not nested any macros, but when I load my application in Themida user interface, I get a nested macros message. What's wrong? ... 76
We tried to adopt Themida VM macro option. But, our particular problem was performance of the game. It was very critical issue. We hope to know how we improve performance of my game. ... 77
Can VM macros protect switch statements? We are now having an issue with VM macros crashing the application. ... 78
Where are the ENCODE/CLEAR macros that were available in version 2.x? ... 78
When I compile my Delphi application in 64-bit, the compiler says that the "asm instruction is not valid" in my VM macros ... 78
I'm using a VM macro but it fails when using it on my Delphi application. I get an exception. Can you fix it? ... 79
What does it mean that my encrypted string are not removed from the original location? ... 79
In VS2017 and VS2019 the debugger is not tracing correctly my function that uses a VM_START/END marker ... 80
When enabling optimizations, my VM_END marker is not found ... 80
I'm using the STR_ENCRYPT but sometimes, when my string contains specific German characters the string is not recognized ... 81

XBundler ... 81

Can I specify via the command line a file which contains all files that will be embedded in XBundler? ... 83
I'm trying to embed a config file in XBundler (using "Never Extract to disk"option) and I want to modify that file in runtime, is that possible? ... 83
I'm using the option “Extract to disk” for several files that I’m bundling with XBundler. The files are extracted correctly under Windows XP but it fails under Vista and Windows 7. What’s happening? ... 84
I want to bundle my OCX in XBundler but not sure if it will work as my OCX needs to be registered in the system via regsvr32.exe ... 84
I want to XBundle my files but with relative paths to parent folders, so can I move my projects and files across computers and protect them from there? ... 85
If I bundle some large graphics files and DLLs, is that going to influence the performance of my program? ... 85
I want to protect a DLL and bundle some data files using XBundler, but it does not work. ... 85
Can I copy to disk a DLL that I have embedded with the option "Never Write to disk" ... 85
In my .NET application (test.exe) I want to to embed my .exe.config file (test.exe.config) with XBundler, but when I run my protected application (without the .config file) it does not see my embedded test.exe.config file. ... 85
Can I embed several EXE files inside XBundler and run them from memory, that is, without writing them to disk? ... 86

What about performance? I'm writing a filemanager which has a lot of access to local files. 86
How are the files accessed from inside the protected application? May I call simply memo.lines.loadfromfile for example? If yes - does this mean that all accesses to files are filtered by XBundler? 86
Can XBundler be used to bundle all of the DLL's and OCX's inside a protected DLL? Does there need to be an actual executable? 86
Is it possible to use XBundler to bundle a console exe that I call run-time from my application? 86
Can I register my bundled DLLs with regsvr32.exe? 87
I tried to bundle CHM file. Command which I use to open CHM file in my application below: ShellExecute(Application.Handle,'open','help.chm',nil,nil,SW_SHOWNOR MAL); 87
We are using a couple of DLLS and OCXS in our application, and I have tried unsuccessfully to use them with the XBundler plugin I bought - whats the best way for us to move forward and maybe run some tests to see if we can get this functionality working? 87
I want to bundle my Visual Studio 2005 (or Visual Studio 2008) DLLs with XBundler but it fails to load them. Is that a known issue? 88
I have inserted about 100 files to bundle. I want to select all of them and set for all of them "Extract always". Is that possible to do it without going one file at a time? 88
I have bundled several INI files with XBundler but when I try to access to them, they cannot be found. Other bundled files are working fine 88

Sales 88

Can you tell me about how Themida subscriptions work? 89
I have paid via Shareit but you have not sent me any invoice. Can you send it, please? 89
I have paid via Fastspring but you have not sent me any invoice. Can you send it, please? 89
If we purchase your software via Bank wire transfer, will you provide our company with an invoice for our purchasing? 89
Does initial purchase include some degree of update support, or must I purchase the update subscription at the outset to get updates during the first year (or whatever period)? 90
I paid to Shareit via bank wire transfer, why I have not received your software yet? 90
As soon as the free update period (12 months initially) expires, I will need to renew Themida subscription. Do I have to pay the renewal fee before it expires or is it possible to pay somehow later (if I happen to forget)? 90
What is the difference between "Developer License" and "Company License"? 90
Suppose I will be the only one developer in our company who will use Themida, do I need to purchase Company license or will Single developer license be enough? 91

6 Support 91

Index 0

I Themida

Themida is a powerful software protection system designed for software developers who wish to protect their applications against advanced reverse engineering and software cracking. Themida uses the SecureEngine® protection system to achieve its goals, making it really difficult to break using the traditional and newest cracking tools.

Themida has been designed to completely stop novice and advanced crackers from cracking an application. That will avoid a considerable revenue loss from the distribution of cracked applications. Developers do not need any source code changes or programming experience to protect their applications with Themida.

This document explains about the advantages of using Themida and how to use it to protect your applications with the most secure techniques available against advanced cracking.

1.1 Why use Themida?

Themida has been designed with the newest and most powerful technology in software protections, SecureEngine®.

From the attacker point of view, Themida is completely different to traditional software protectors, due to its complex protection engine and its high priority code that allows supervising the whole system against possible attackers. From the software developer's point of view, Themida is quite easy to use and easily adapts its protection techniques to suit a developer's needs.

The following sections give a detailed explanation about the benefits of using Themida to protect your software.

- Scenarios for using Themida 1
- Vulnerabilities in software protectors 2

1.1.1 Scenarios for using Themida

Themida uses the SecureEngine® protection system to cover a wide range of scenarios. SecureEngine® is the ideal solution in the following situations:

- **Protecting an application against modifications and software piracy:** SecureEngine® protects the integrity of an application by encrypting and decrypting its code at runtime, using revolutionary techniques that defeats any of the traditional or newest cracking tools.

- **Protecting an application against reverse engineering:** SecureEngine® uses a wide range of techniques to prevent reverse engineering. An attacker will not be able to use cracking tools to analyze the code of a protected application.

- **Protecting an application against monitoring tools:** SecureEngine® includes the most advanced techniques to detect registry and file monitoring tools. Developers choose the desired option to finish the execution of their applications upon the detection of monitoring tools.

1.1.2 Comparing Themida with other protectors/licensing systems

Other software protectors and licensing system have important vulnerabilities, which prevent them from being a perfect solution to protect an application against reverse engineering or cracking. The following section identifies some of those vulnerabilities and shows how Themida resolves them.

Obsolete protection techniques

Most modern software protection systems use already broken techniques that are quite easy to bypass. Normally, an attacker will reuse the same proven tools that have been used over years to break protection systems. Often the attacker will release a global technique to attack every application protected by a specific protection system.

SecureEngine® uses new technology in software protection to ensure each protected application is unique thus preventing any cracking tool from being used to create a universal crack to your application.

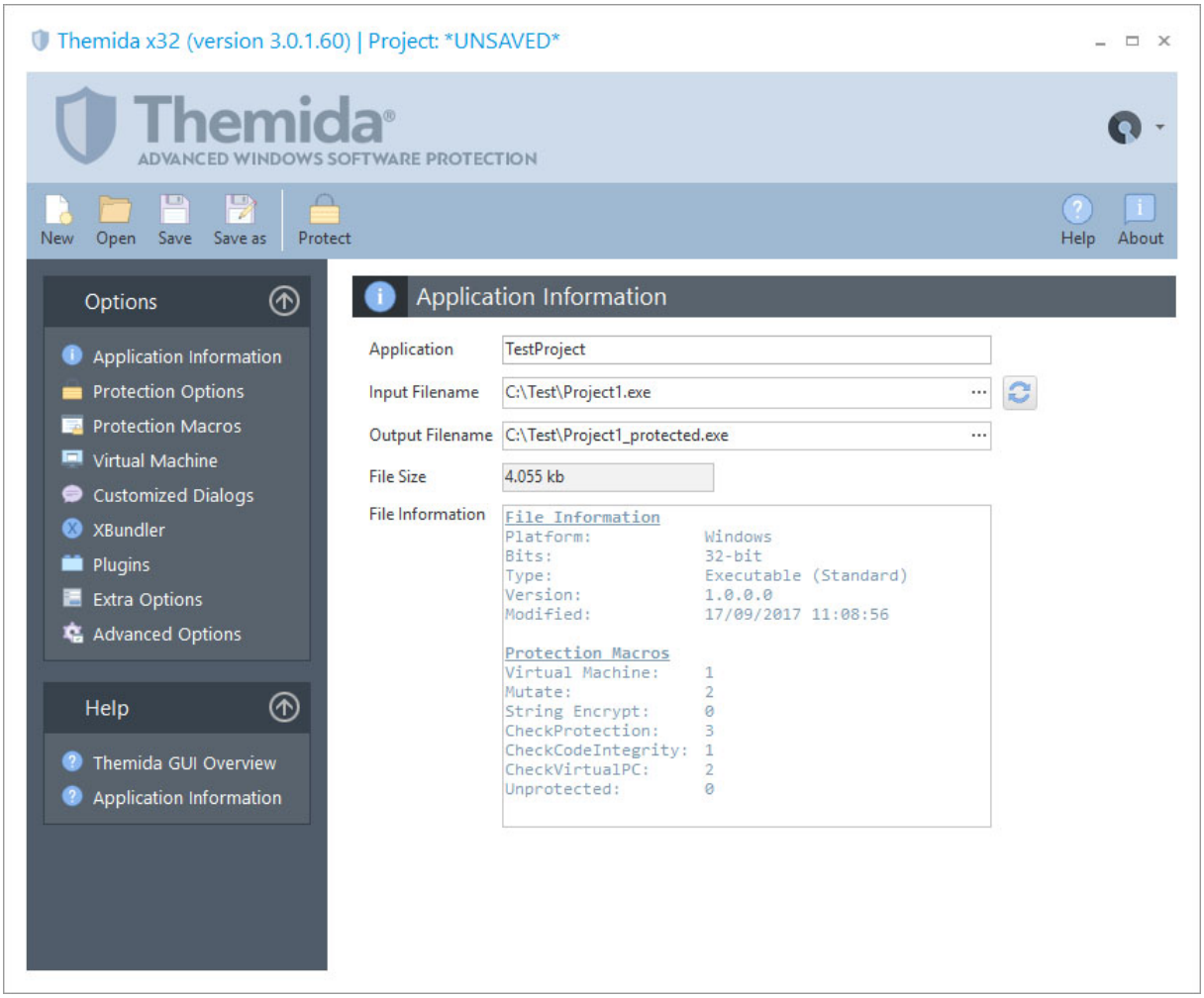
Attackers are one step ahead of the protection system

When a software protection system has been broken, their authors implement patches to avoid a specific attack from being used again on new versions. Typically attackers will inspect the new changes that have been applied in the new version and will easily bypass them again. In this common scenario, attackers are always one step ahead from the protection system because the new applied patches can easily be identified and defeated.

SecureEngine® has a different approach to avoid this. If vulnerability is found the vulnerable object is quickly changed (due to the mutable technology used in SecureEngine) instead of releasing a patch against the specific threat. The new object, joined with the rest of the SecureEngine® objects, creates a completely new protection system. The benefits of this, when compared to common software protectors, is that attackers will have to reexamine the whole protection code to bypass the new changes.

1.2 User Interface

1.2.1 Themida GUI overview



The Toolbars Menu

The toolbars menu helps you to manage your project files, protect your current application and gives you access to the main help file.

Every time that you make changes to your protection settings, you can save those changes in a project file. That project file can be loaded at a later time to restore the current protection settings and protect another application.

The Options Panel

The option panel shows the different settings that are required to protect an application and customize the different protection options that you want to include in your application.

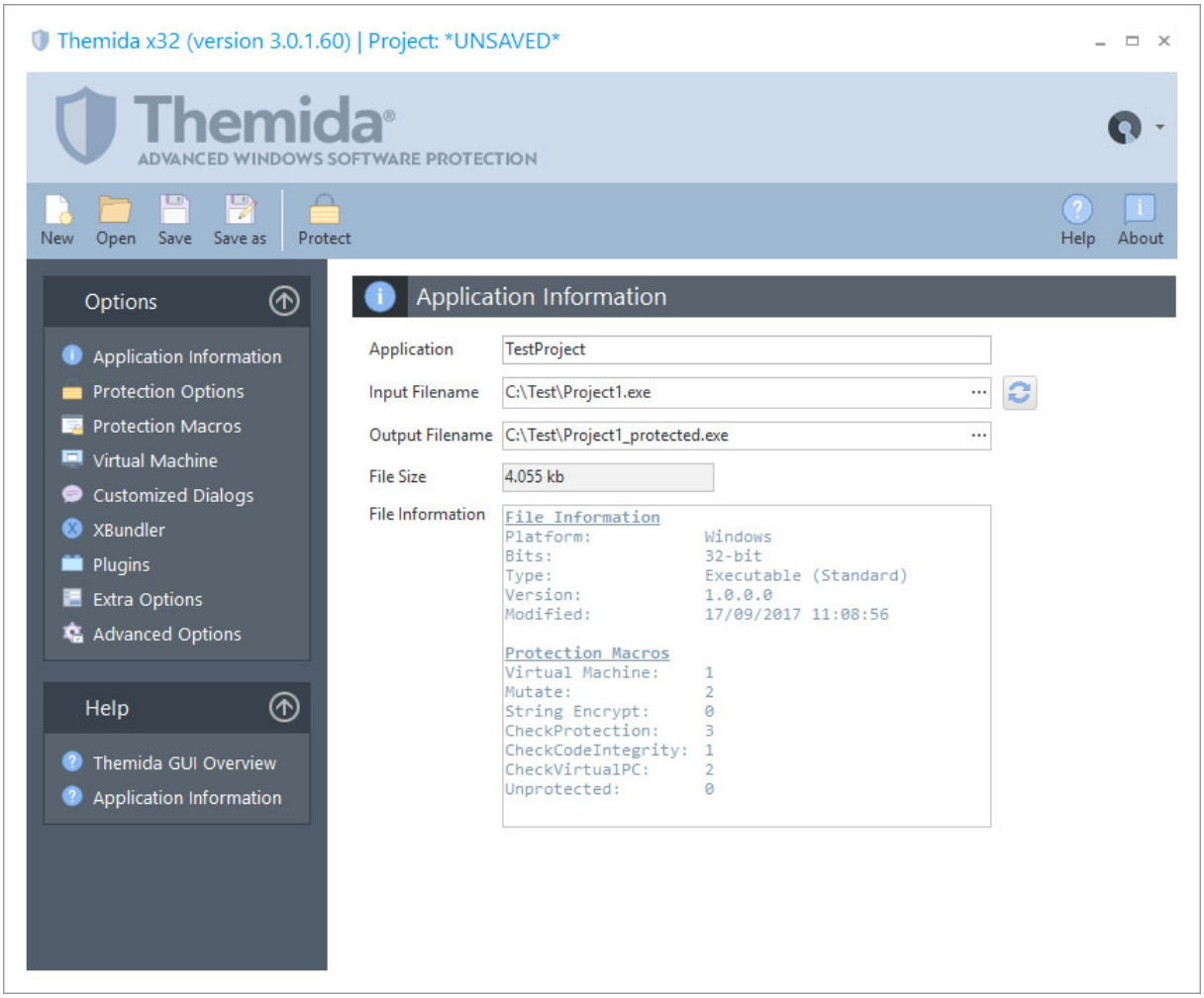
- The Application Information 5 panel allows you to set up the general information settings about the application that you are going to protect.
- The Protection Options 7 panel allows you to select the different protection options that will be included in your application.
- The Protection Macros 10 panel allows you to review and/or select the specific protection macros that have been included in your application.
- The Virtual Machine 13 panel allows you to set up all protections related with the Virtual Machine technology.
- The Customized Dialogs 16 option allows you to customize the different messages that are shown when a certain event occurs while your protected application is running.
- The XBundler 19 panel allows you to embed data files and DLLs to be embedded inside your protected application.
- The Plugins 23 panel allows you to insert custom plugins (DLLs) that will be embedded inside the protected binary.
- The Extra Options 28 panel contains specific options (not protection) related that can be added into your application.
- The Advanced Options 30 panel allows you to insert special (hidden) options related with compatibility in specific applications.

The Help Panel

The help panel gives you access to the Themida Help file to get more information about specific topics.

1.3 Protecting an application

1.3.1 Application Information



The first step to protecting an application is selecting the application that you want to protect by using **Input Filename**. After selecting the input file name you also need to set the output filename by using **Output Filename**.

The **Application** field is designed to keep track of your protected application in a project file. This field is not required to protect an application and is only used for a developer's special needs.

The **File Size** and **File Information** windows display information about the application that is going to be protected. The details include file size, type of file, the compiler used to generate the application and number of SecureEngine® macros detected.

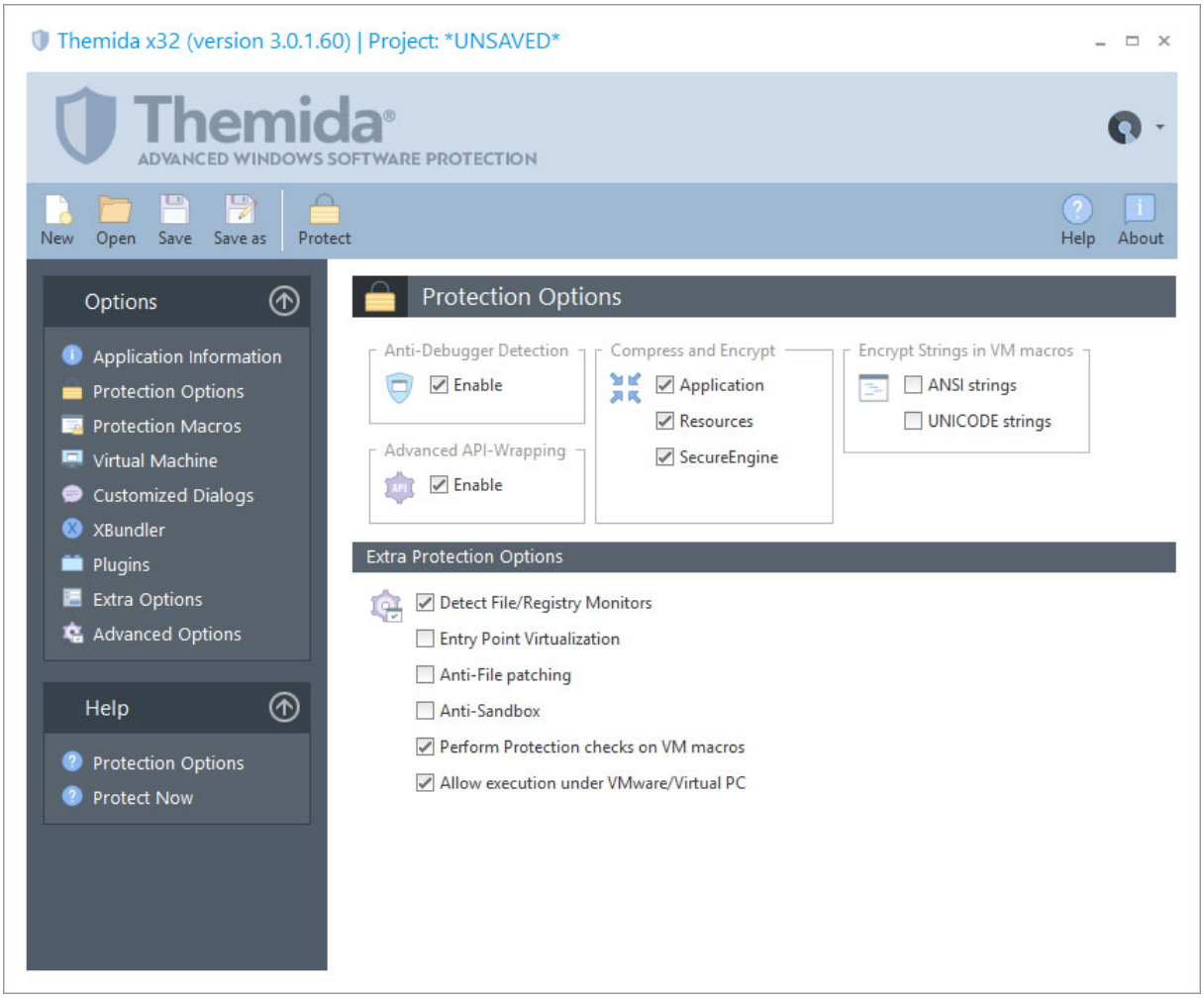
Special Constants in Input/Output file names

Sometimes you might want to work with relative or not fixed paths in the Input and Output file names, so you can easily move your project files across different PCs or when working in a cooperative environment with several developers. You can use special defined constants as part of the file paths. This constants can be used in other places in the user interface that refers to a file path (like the XBundler files, Splash file, etc.). The current available constants are the following:

- **%INPUT_FILE_FOLDER%**: Specifies the folder of the input file (the file to protect)
- **%OUTPUT_FILE_FOLDER%**: Specifies the folder of the output file (the protected file)
- **%PROJECT_FOLDER%**: Specifies the folder of the current project file
- **%THEMIDA_FOLDER%**: Specifies the folder where Themida.exe (Themida64.exe) is located
- **%CURRENT_FOLDER%**: Specifies the current folder from where Themida.exe has been launched
- ***%environment_variable%***: Specifies the folder defined in any environment variable. For example, if you want to get the path from the "temp" environment variable, you can write something like: *%temp%\MyApplication.exe*

An example of an input file to protect can be**:** *%THEMIDA_FOLDER%\MyProjects\MyApplication.exe*

1.3.2 Protection Options



In the Protection Options panel you can select the different protection options that you want to include in your application. By default all the protection options are enabled. If a specific protection option is not needed for your application it can be removed to speed up the execution of your application and make the protection code smaller.

Anti-Debugger Detection

This option will enable anti-debugger detections inside the protected application, detecting when a kernel or software debugger is debugging a protected application.

Advance API-Wrapping

This option will enable advanced API-Wrapping techniques that keep an attacker from identifying the different APIs that are used by a protected application. The API-Wrapping option has a very small penalty in the execution speed in your application in case that your application is calling a specific API massively. In any case, there are internal options that can help you to unselect specific functions from being wrapped. Please, contact us for further information.

Compress and Encrypt

You can select if your application, resources and the protection boot loader will be encrypted and compressed. There is a small penalty in the execution time before your application starts but it's recommended to keep those options enabled for further protection.

Encrypt Strings in VM macros

When you insert Virtual Machine macros in your source code (or via an external MAP file) you can encrypt all references to strings that appear inside the macro markers (START - END). The string will be removed from the original location and it will be moved inside the protection code area in an encrypted form. Once that the string is going to be referenced by your code, it will be decrypted at that specific point in order to deliver it to the required code.

If you are just using ANSI strings in your application, you should just check the "ANSI strings" options. If instead, your application is using UNICODE strings, you should just check the "UNICODE strings" option. You can go to the "Protection Macros 10" panel and select a specific macro from the list, after that click on the lower panel tabs (Ansi Strings and Unicode Strings) in order to see that strings that are found inside the selected protection macro.

This option is basically the same as putting a STR_ENCRYPT macro 42 inside each Virtual Machine Macro that you have inserted. If you are just interested in protecting specific strings that appears in specific macros that you have inserted, you should not use this option and use instead a STR_ENCRYPT macro 42 inside your Virtual Machine Macro.

Extra Protection Options

- **Detect File/Registry Monitors**: This option detects common tools that monitor access to the Windows File and Registry system by a specific application. If your application stores sensitive information in the Windows File or Registry system, you should enable this option.

- **Entry Point Obfuscation:** This option produces the equivalent result as putting a VM macro in the very first instructions that are executed in your application. This op-

tion is not compatible with all applications and you should uncheck it in case that your application does not start when protected.

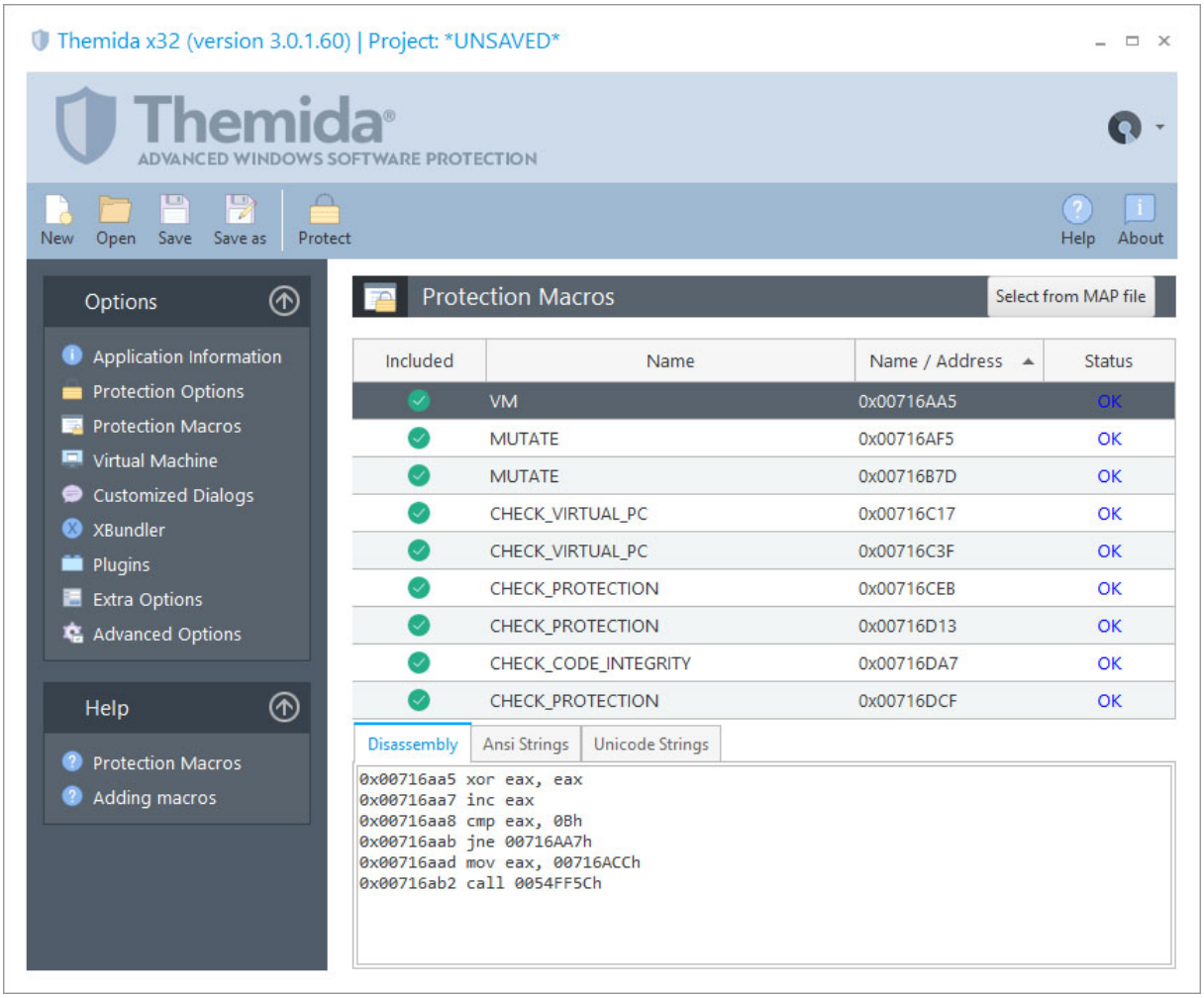
- **Anti-File Patching**: This options detects when a modification has been done to the protected application from an external source (like a virus, cracker or any other application). If you are planning to put another compressor on top of your protected application or do some external modifications to the protected file on disk, you should not check this option. If this option is set and and there is a modification in your protected application, SecureEngine will display the Customized Dialog 16 "MSG_ID_FILE_CORRUPTED". You can edit the error message or handle that specific error event from your plugin DLL.

- **Anti-Sandbox**: This option detects common sandbox applications. A sandbox application virtualizes file and registry access in order to avoid direct/real access to the file/registry system.

- **Perform Protection checks on VM macros**: When you insert a VM macro (TIGER VM, FISH VM, etc.) inside your application you can perform extra protection checks before the your protection macro is executed. This option checks if your application has been partially attacked by an attacker.

- **Allow execution under VMWare/Virtual PC**: This option allows your application to be run under common virtual environments like VMWare, Virtual PC, VirtualBox, etc. In case that you want to restrict the execution of your protected application under these virtual environments, you should uncheck this option.

1.3.3 Protection Macros



In the **Protection Macros** panel, you can see the assembly code that will be protected for each protection macro. You can also see if any ANSI or UNICODE strings are referenced inside each protection macro and decide if you want to protect those strings (see option **Encrypt Strings in VM macros** in the Protection Options 7 panel)

You can also enable or disable specific blocks from being protected. Normally, disabling macros from being protected is only required to find a problematic block in the protected application, which makes the application behave in a different way or produce an application exception. In case that you have problems protecting a specific macro, you should check that there is not a current macro restriction.

Macro Restrictions

Switch-case statements and *try-except* clauses cannot work with SecureEngine macros macros in most compilers.

Compilers generate a direct jump table in the data section which directly jumps to each "case" statement. When the code is virtualized, the jump goes into a virtualized (garbage) code and it produces exception. Switch-case and try-except clauses will be supported in a future version.

You can use a workaround to protect your switch-case statements with VM macros, like:

For switch-case:

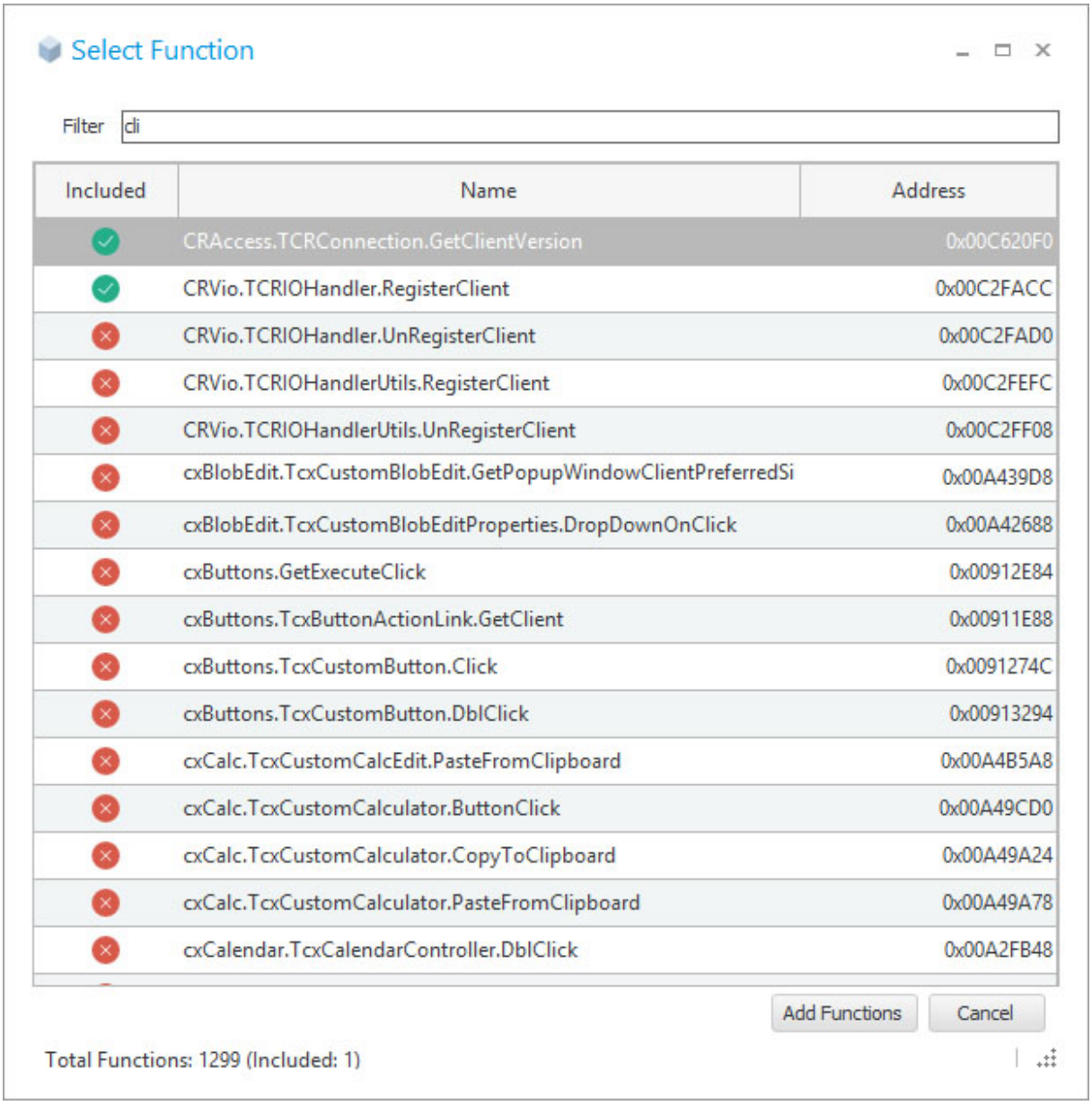
```
switch (var)
{
    case 0:

    VM_START

    // your code

    VM_END

    case 1:

    VM_START

    // your code

    VM_END

    ...
}
```

For try-except:

```
try
{
    VM_START

    // your code

    VM_END
}

except
{
    VM_START

    // your code

    VM_END
}
```

Inserting Macros from a MAP file

To insert macros from a MAP file, just click on the **Select from MAP file** button. You can insert/remove macros by clicking on the name of the function.

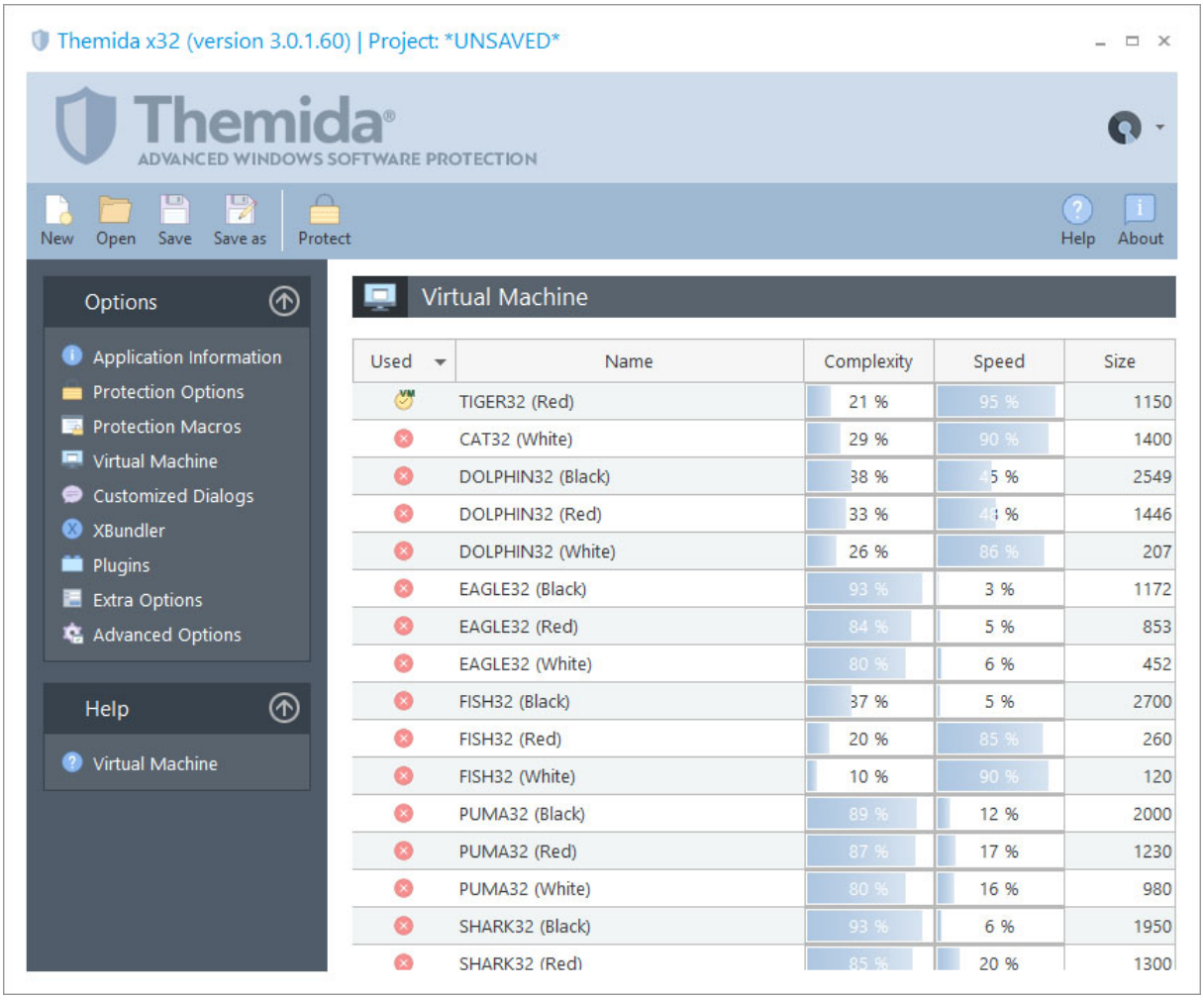


By default, the added MAP functions are handled by a "VM" macro. If you want to assign a specific virtual machine for each added MAP function, do the following steps:

- In the Protection Macros panel, select the specific MAP function

- Hold the **[SHIFT]** key and press the **[LEFT_ARROW]** or **[RIGHT_ARROW]** key to move between different machines

1.3.4 Virtual Machine



The Virtual Machine panel allows you to integrate the Virtual Machine technology into your application.

Available Virtual Machines

This panel shows all the available Virtual Machines that can be used in a protected application. Some Virtual Machines are public and others are private for specific customers. You can contact us at info@oreans.com to know more about customized Virtual Machines.

Suppose that you protect the same application two times using the TIGER Virtual Machine. Each protected instance will contain a unique TIGER Virtual Machine with different registers, instruction handlers, opcode table, etc. from the previous instance. They will just share the internal skeleton of the TIGER architecture. A cracker will have to study the internal skeleton of the TIGER architecture an later try to find a way to to attack all different variations of the TIGER architecture. This scheme is the one that contains all current software protectors based on Virtual Machines (they use mutations/variations of an internal architecture model defined by them).

We wanted to go one step further, creating multiple Virtual Machine architectures with the help of our powerful Virtual Machines Generator tool. Comparing two different architecture names, like TIGER and LION, is equivalent to comparing an Intel x86 processor with an ARM processor. Each one is totally independent from each other and developed without the other in mind.

The **Complexity** and **Speed** columns display some stats about the execution speed and the complexity of a given Virtual Machine. Notice that depending on the internal Virtual Machine revision, those values might change (increasing or decreasing across versions).

The **Instances** column allows you to specify the number of copies that will be generated for a given Virtual Machine architecture. Even using the same architecture name, the generated Virtual Machine will contain different registers positions, different handlers, different opcode table, etc. When you insert several CPUs for a given Virtual Machine, some protection code and your VM macros will be virtualized with any generated CPU.

Virtual Machine selected for the Protection Boot loader

The protection boot loader (the code executed before your application takes control) uses the internal virtualization engine to protect itself from being inspected. You can select a specific Virtual Machine that will virtualize the protection boot code. To do so, just right click on the specific Virtual Machine and select "Use it in Protection Boot". We recommend you not using a very complex virtual machine (with low speed) to avoid a noticeable performance decrease while your application is being loaded.

Virtual Machine selected for standard (old) VM macros

If you have inserted the old VM_START/END macro in your source code, you can associate a specific Virtual Machine name to those macros. To do so, just right-click on the specific machine and select "Use it for old VM macros"

Guidelines to select Virtual Machines

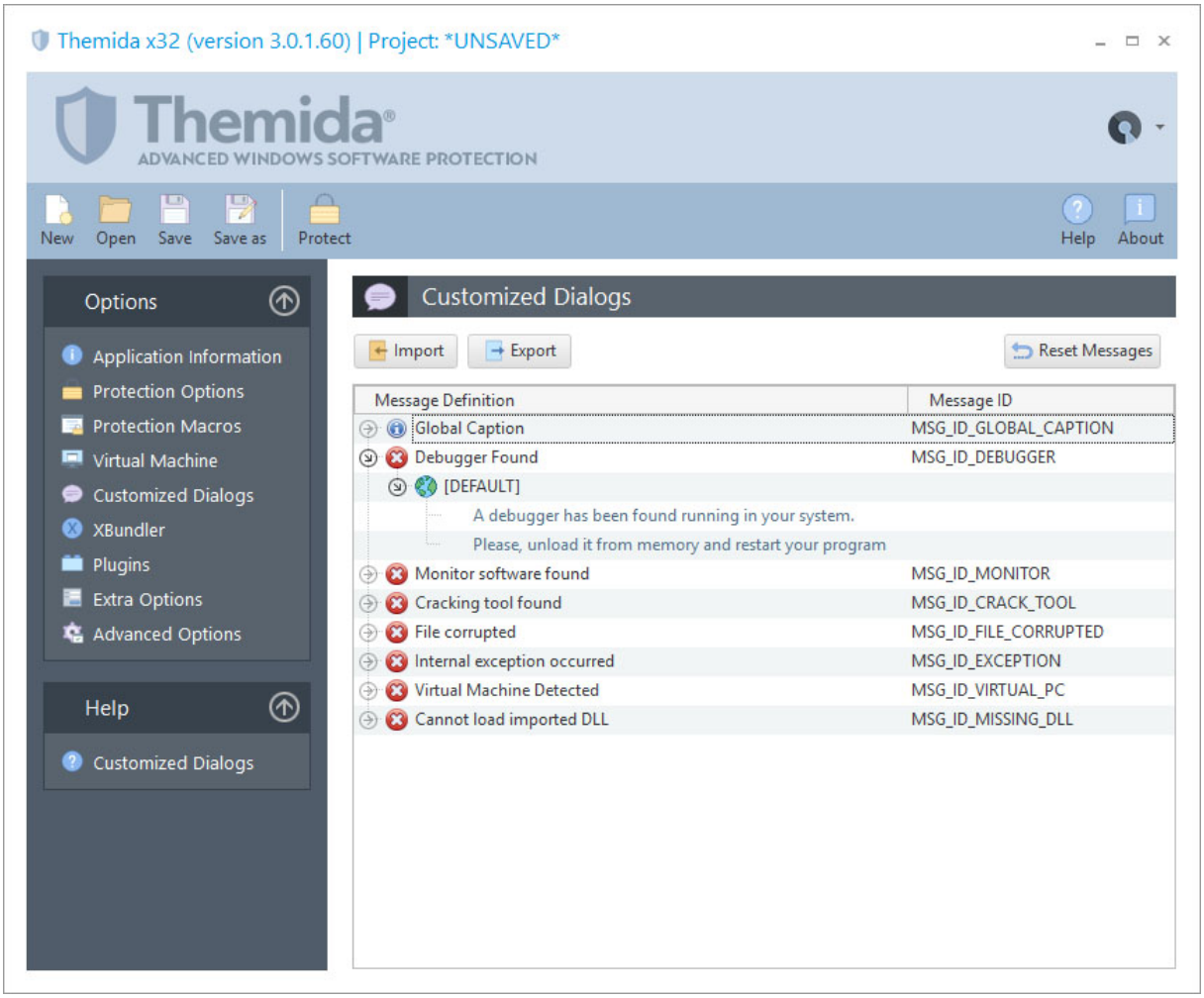
Developers might feel confused about which Virtual Machine they should select in order to get the desired security for their applications. Some developers might have the idea of adding as many Virtual Machines and CPUs as possible to highly increase the security of their applications. This might not produce the effect that they want.

1) Just insert a single Virtual Machine or a couple of them. If you insert several Virtual Machines and CPUs, it will produce a big protected application on disk and memory, as some Virtual Machines can be bigger than 1Mb. Notice that if you select several Virtual Machines and they are not selected in the lower "Virtualization" panel, SecureEngine will not insert those Virtual Machines inside your application, as they will be unused by the protection (optimizing the final size of the protected application)

2) When using the virtualization macros in your application, you should avoid using the old VM macro and specify the Virtual Machine architecture that will protect a specific macro (example: "VM_TIGER_RED_START/END"). This will allow you to use complex Virtual Machines for your most sensitive code and a lighter Virtual Machine for code that needs to be virtualized and executed at a higher speed.

3) From time to time consider updating your virtualization macros to point to a different or newer Virtual Machine architecture. If you have been using the TIGER architecture for some time, you might want to select a different architecture in new versions of your application, to fight against crackers that have been behind your application for some time.

1.3.5 Customized Dialogs



The Customized Dialog window allows changing the messages that may be shown by SecureEngine® when certain situations occur.

Languages

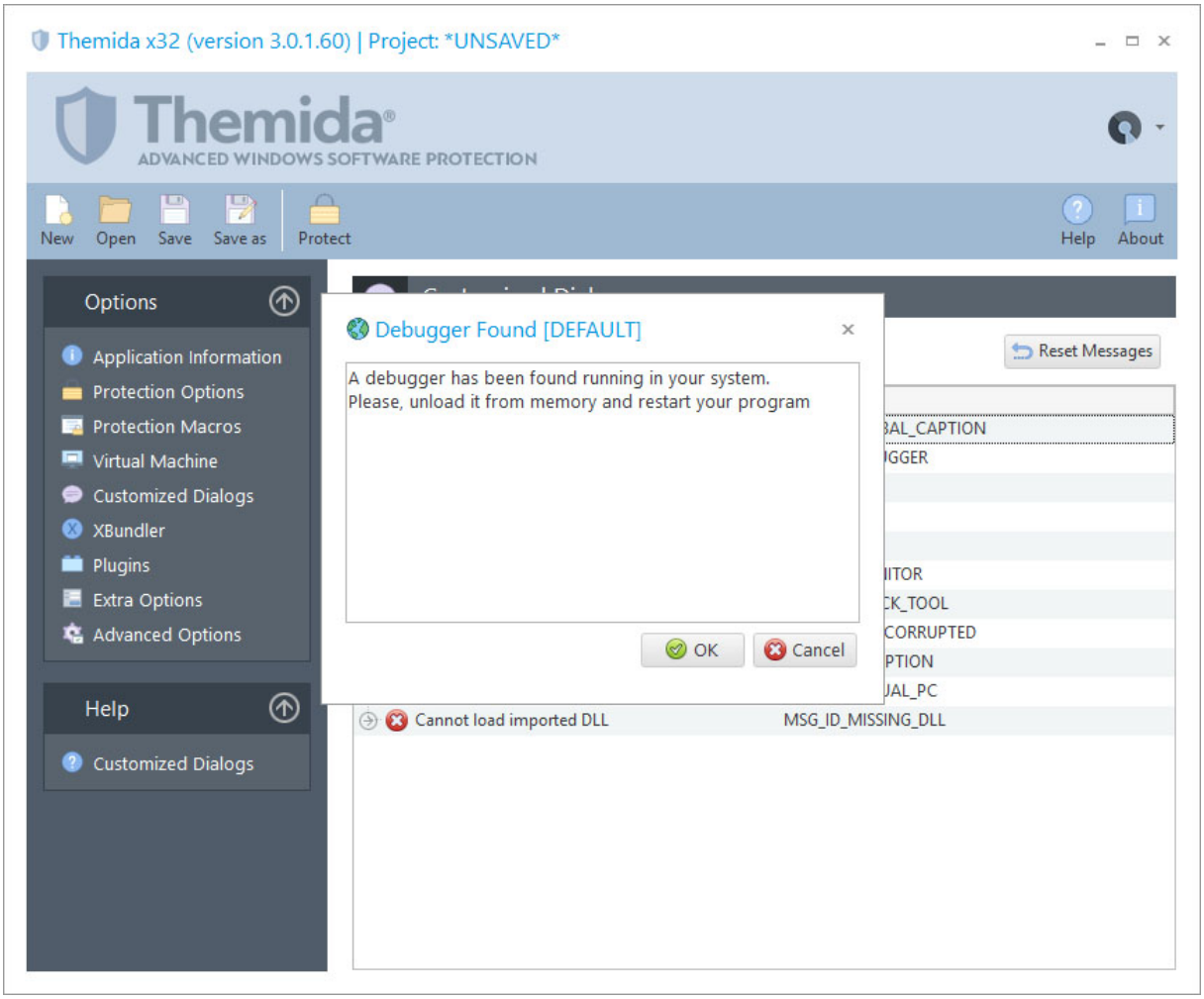
You can add several languages to each specific message, so the message will be displayed in the user's system language. In order to add a new language for a specific message, just right click on the desired message and select **Add Language**.

The **[DEFAULT]** language is the one that will be displayed in case that the current system language does not match with any of the defined languages for the current message to display. For example, you edit the MSG_ID_DEBUGGER message and define the **[DEFAULT]** and **[GERMAN]** message. If the application is running in a PC with Windows language set to Ger-

man, the message will be displayed in German (as you defined for **[GERMAN]**). If another customer is running your protected application on a PC with Windows language set to Spanish, the message will be displayed as defined in **[DEFAULT]**

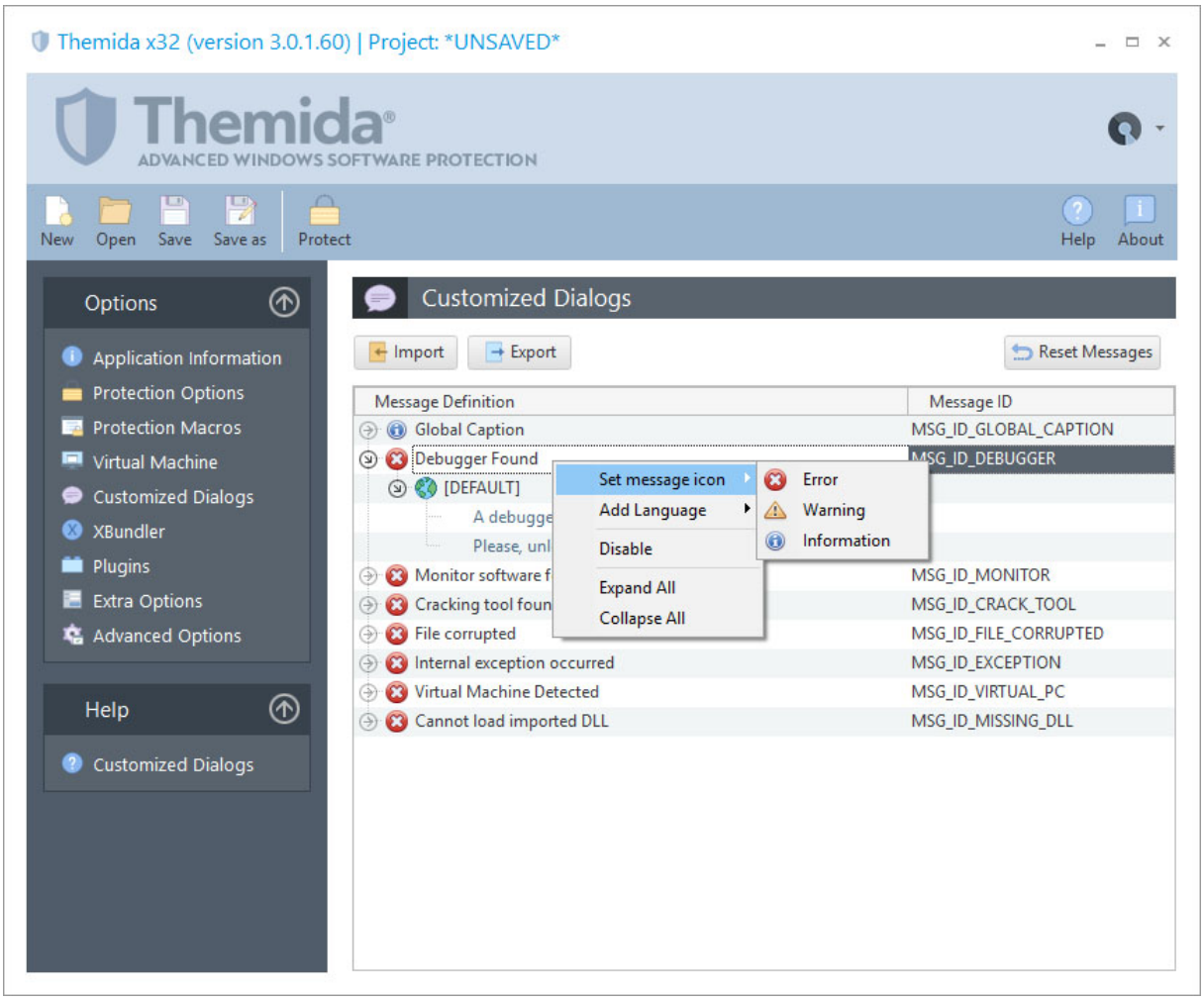
Changing a custom message

To change a custom message, double-click on a specific message to start editing.



Changing the custom message icon

Each message is displayed by default as a Windows MessageBox. You can change the MessageBox icon for each message by selecting the specific message and right-click on it, after that use the option **Set Message Icon**.



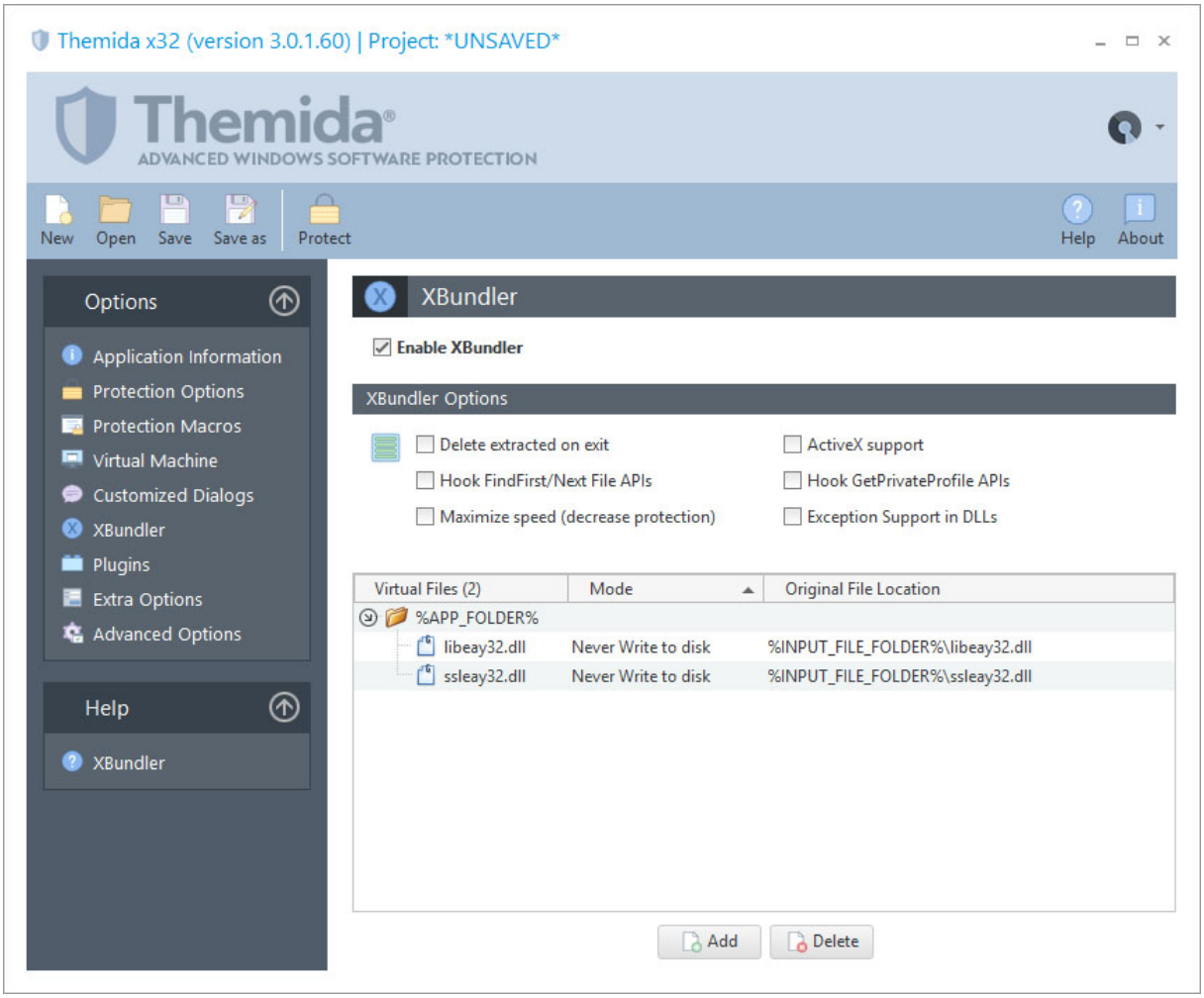
Changing the general caption for all messages

All messages are shown with a general caption that can also be customized. The general caption message is the **MSG_ID_GLOBAL_CAPTION**. This caption message can be customized in the same way as the rest of the messages, by double clicking it.

Importing and exporting your customized messages

Themida offers the possibility to export your customized messages to a single file so they can be imported in other project files without the need of retype all the messages again. To export all your messages to a file you just need to press the **Export** button and select the name of the file in which your messages will be saved. When you want to import your customized messages to the current project file, just press the **Import** button and select where the file with all your customized messages is located.

1.3.6 XBundler



XBundler allows you to embed DLLs and data files inside a protected application, simplifying the distribution of your application to your customers and avoiding your DLLs and data files being used by third party software. XBundler compresses and encrypts all of the embedded files without affecting the ability of your application to function correctly and with no additional coding.

When your application wants to access your embedded DLLs and/or data files, XBundler will not write the embedded files to disk. Instead, XBundler uses a special application hooks to detect when an application is accessing embedded DLLs and/or data files and will decrypt/encrypt the required block of data.

Scenarios for using XBundler

XBundler can be used in many scenarios. The most common ones are:

- Protect your DLLs from being reused by third party software: When you select not to write your files to disk, XBundler will keep your files totally encrypted and will access them directly in memory after decrypting the necessary blocks of data. Given that your DLLs are not written to disk, third party software cannot reuse your DLLs for their own benefits.

- Solve "DLL Hell" issues: XBundler will guarantee that your application is always using your embedded DLLs. This will avoid users and applications from modifying/deleting your DLLs hence stopping your application from working.

- Protect your DLLs against reverse engineering: XBundler encrypts your DLL and/or data files to prevent them from being extracted directly from your application. Besides, Themida/WinLicense will seat on top of XBundler supervising the system against any cracking activity, protecting your embedded DLLs and your main application with the latest technology in software protection.

- Compress your DLLs and data files: XBundler will compress all of your embedded DLLs and data files reducing their size by 35-60% and using a very fast decompression algorithm which does not decrease your applications performance.

- Protect your media files: If your application uses exclusive designs with graphics, music, video, etc. XBundler can embed all of these media files with your application to avoid other people directly viewing them, or using them for their own software.

XBundler Files Panel

To add files to be embedded inside your final protected application, you can either drag the file to the XBundler panel or select a file using the **Add** button. The file will appear in the list if it has not already been included.

- The **Virtual File** column displays the location where a specific file can be found in runtime in case that you select the option to extract the file to disk. You can create your own extraction hierarchies by creating subfolders in the Virtual File column. To do so, just right-click on the XBundler files panel and select the option "Add Folder". If you want to change the root folder for the virtual file, select the option "Add Root Folder". The current defined values are:

    - **%APP_FOLDER%**: This is the folder from where you protected application is executed

- **%WIN_FOLDER%**: Windows folder
- **%WINSYS_FOLDER%**: Windows System folder
- **%USER_DOCS%**: Current user documents folder
- **%LOCAL_APP_DATA%**: Current user local AppData folder
- **%COMMON_APP_DATA%**: Common application data for all users

- The **Mode** column allows you to select if the file will be extracted to disk in runtime or the file will never be extracted to disk. When the file is not extracted to disk, XBundler uses process hooking in order to detect file accesses and redirect them to specific locations within the process space. If you want to extract the file to disk, there are several types of extraction options to suit different developer needs.

- The **Original File Location** column specific the location of the file on disk. This is used in protection time in order to read the file to embed. If you don't want to work with full paths, you can use special constants for the file location, like **%THEMIDA_FOLDER%**, **%INPUT_FILE_FOLDER%**, **%OUTPUT_FILE_FOLDER%**, **%PROJECT_FOLDER%**. Example: *%INPUT_FILE_FOLDER%\files\my_file.dat*

XBundler Options

- **Delete extracted on exit**: In case that for any of your embedded files you have selected the option "Extract to disk", this option will delete the extracted file once that the application exits. If you are selecting the option "Never extract to disk" for all your embedded files, this option has no effect.

- **Hook FindFirst/FindNext File APIs**: This option hooks the FindFirst/FindNext Windows API. These APIs are normally used by Windows when files are going to be listed in a Windows Shell Dialog. If you want to make your embedded files visible to Windows Shell Dialogs or you want to enumerate your embedded files from inside your application (using FindFirstFile, FindNextFile, etc.) you have to select this option. Note that even if you see your embedded files from inside your application when you select this option, your embedded files will NOT be visible to users and other applications.

- **Maximize speed (decrease protection)**: This option will decrease the encryption/virtualization of the XBundler protection code to avoid a performance decrease in case that you access to your embedded files quite frequently.

- **ActiveX support**: This option allows you to register your embedded DLLs/OCXs before your application starts. It has the same effect as if "regsvr32" is performed before your application starts. Notice that in order to register your embedded DLLs/OCXs, your application needs to be running with administrator's rights. If the application is running with restricted user rights, the embedded DLLs won't be register in the system. You have to make sure that the protected application runs with administrator's rights the first time that is executed in the system to allow registration of embedded DLLs.

- **Hook GetPrivateProfile APIs**: This options hooks the Win32 GetPrivateProfile APIs in case that your application use those functions to access to the files that are going to be bundled (and never written to disk). This option should be checked in your are bundling .INI files with the option "Never write to disk".

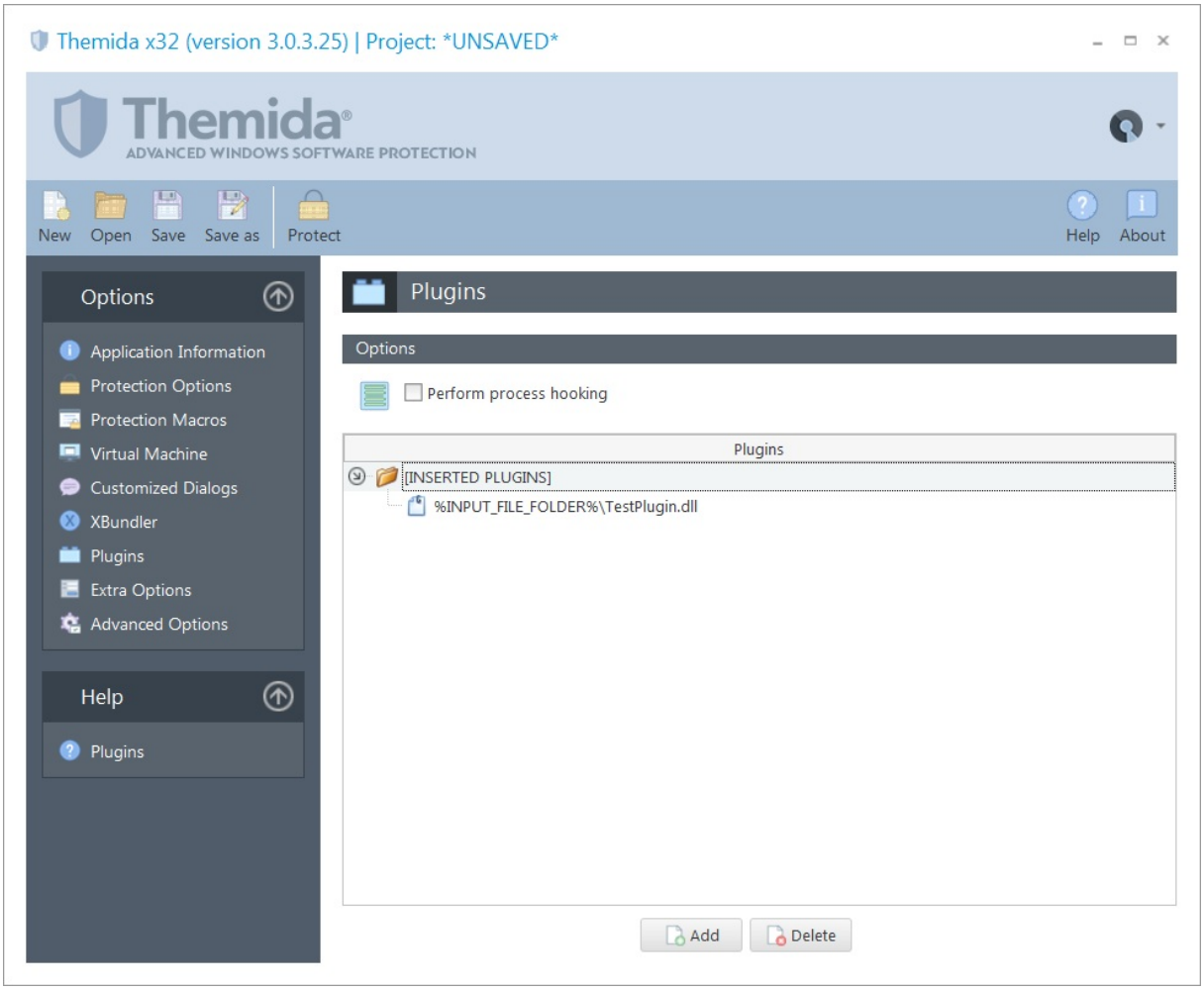
- **Exception support in DLLs**: Some DLLs generates exceptions (handled) on start and that interacts with the exception handling in the protection code. If any of your embedded DLLs produce handled exceptions on start, you have to check this option

Changing the Extraction Mode for all selected files

If you want to change the extraction type for several files at the same time, just select all wanted files and press:

- CTRL + 0 = "Never Write to disk"
- CTRL + 1 = "Extract always"
- CTRL + 2 = "Extract if not exists"
- CTRL + 3 = "Extract if older exists"
- CTRL + 4 = "Extract if different exists"

1.3.7 Plugins



Themida allows you to insert custom plugins (DLLs) that will be embedded inside the protected binary. The embedded plugin can implement specific defined callbacks that will be called when a specific protection event occurs, so you can have more control on the protection, add your own custom protections, etc.

A plugin is basically a compiled native DLL (.NET DLLs are not supported), that exports specific functions names that matches a specific name pattern. For example, the callback "***SecureEngineInitialize***" (notice the *wildcard*) means that you can define any function (to export) that will contain the "SecureEngineInitialize" string within your function name. For example, the function name *MyPlugin_SecureEngineInitialize* will match the "***SecureEngineInitialize***" callback.

Options

- **Perform process hooking**: This option will fully emulate the loading of your DLL in memory. This option is only required for specific plugins. Most plugins will work fine without this option. The preferred is to have this option unchecked, because it won't perform any hooking on the current process.

Testing your plugins

It's a good idea to test your plugins after your modify them, just to make sure that the calling convention (***stdcall***) and parameters are defined as expected. To test your plugin, you can just right-click on it and select "**Test Plugin**". Your defined callbacks will be called with default/dummy parameters to test your callbacks. If a callback fails (produces exception, etc) it will be reported on the User Interface.

Supported Compilers

There are no restrictions about the compiler used to create a plugin. The only requirement is that the plugin cannot be a .NET (or mixed managed) DLL. Only native DLLs are supported.

In case that you are using Visual Studio to create your plugin, you should avoid the explicit linking with the Microsoft Runtime Libraries (such as MSVCR100, etc.). You should compile your DLL with the /MT compiler switch.

Plugin Callbacks

The plugin system will be extended in future versions with new callbacks. The current defined callbacks (name patterns) are:

- SecureEngineInitialize 25
- SecureEngineFinalize 25
- SecureEngineShowCustomMessage 25
- SecureEngineGetEncryptionKey 27

1.3.7.1 SecureEngineInitialize

This function is called when the protection starts, before your application has been processed (decrypted, decompressed, etc) to be executed in memory. This can be a good place if you want to add your own protection checks, etc.

Show C/C++ function definition

```
STDCALL bool SecureEngineInitialize(void);
```

Show Delphi function definition

```
function SecureEngineInitialize():Boolean; stdcall;
```

Return Values

If your callback returns FALSE, the application will be terminated. If it returns TRUE, the protection will continue execution.

1.3.7.2 SecureEngineFinalize

This function is called when the protection boot loader has been executed, your application is ready to have control of the CPU.

Show C/C++ function definition

```
STDCALL bool SecureEngineFinalize(void);
```

Show Delphi function definition

```
function SecureEngineFinalize():Boolean; stdcall;
```

Return Values

If your callback returns FALSE, the application will be terminated. If it returns TRUE, the protection will continue execution.

1.3.7.3 SecureEngineShowCustomMessage

This function is called when a Customized Dialog 16 is going to be displayed by the protection. This function receives the message that is going to be displayed by the protection in ANSI format (SecureEngineShowMessageA) or UNICODE format (SecureEngineShowMessageW)

Show C/C++ function definition

```
STDCALL bool SecureEngineShowCustomMessageA(
    int      CustomMessageId,
    char*    CustomMessageString
);

STDCALL bool SecureEngineShowCustomMessageW(
    int      CustomMessageId,
    wchar_t* CustomMessageString
);
```

Show Delphi function definition

```
function SecureEngineShowCustomMessageA(
    CustomMessageId:Integer;
    CustomMessageString:PAnsiChar
):Boolean; stdcall;

function SecureEngineShowCustomMessageW(
    CustomMessageId:Integer;
    CustomMessageString:PWideChar
):Boolean; stdcall;
```

Parameters

CustomMessageId

[in] Identifier for the message that is going to be displayed. Please, refer to the *CustomMessagesConstantsDefinitions.h* (for C/C++) or *CustomMessagesConstantsDefinitions.inc* (for Delphi)

CustomMessageString

[in] Pointer to a null-terminated string with the message that is going to be displayed.

Return Values

If the function handles the message, you should return TRUE, that means that the protection will not display the message.

If the function does not handle the message or you want that the protection proceeds displaying the message, you should return FALSE.

1.3.7.4 SecureEngineGetEncryptionKey

This function allows you to specify an encryption key to encrypt/decrypt specific areas in your application. At the moment, only the encryption/decryption of the different sections in the PE file is supported (parameter "ZoneId = 0")

This function is called in protection time to get the encryption key from your plugin. The retrieved encryption key will be used to encrypt your application (apart from other encryption layers applied to encrypt your application).

In runtime, the protection will call your embedded plugin to retrieve the encryption key to decrypt your application. Once that the key has been used, the buffer with the retrieved key will be destroyed.

Show C/C++ function definition

```
STDCALL bool SecureEngineGetEncryptionKey(
    int      ZoneId,
    char*    OutputEncryptionString
);
```

Show Delphi function definition

```
function SecureEngineGetEncryptionKey(
    ZoneId:Integer;
    OutputEncryptionString:PAnsiChar
):Boolean; stdcall;
```

Parameters

ZoneId

[in] Identifies the zone for where the encryption key is required. At the moment only 0 (zone 0) is supported, meaning the encryption key to encrypt the application code/data.

OutputEncryptionString

[out] Pointer to an allocated buffer where the encryption key will be copied.

Return Values

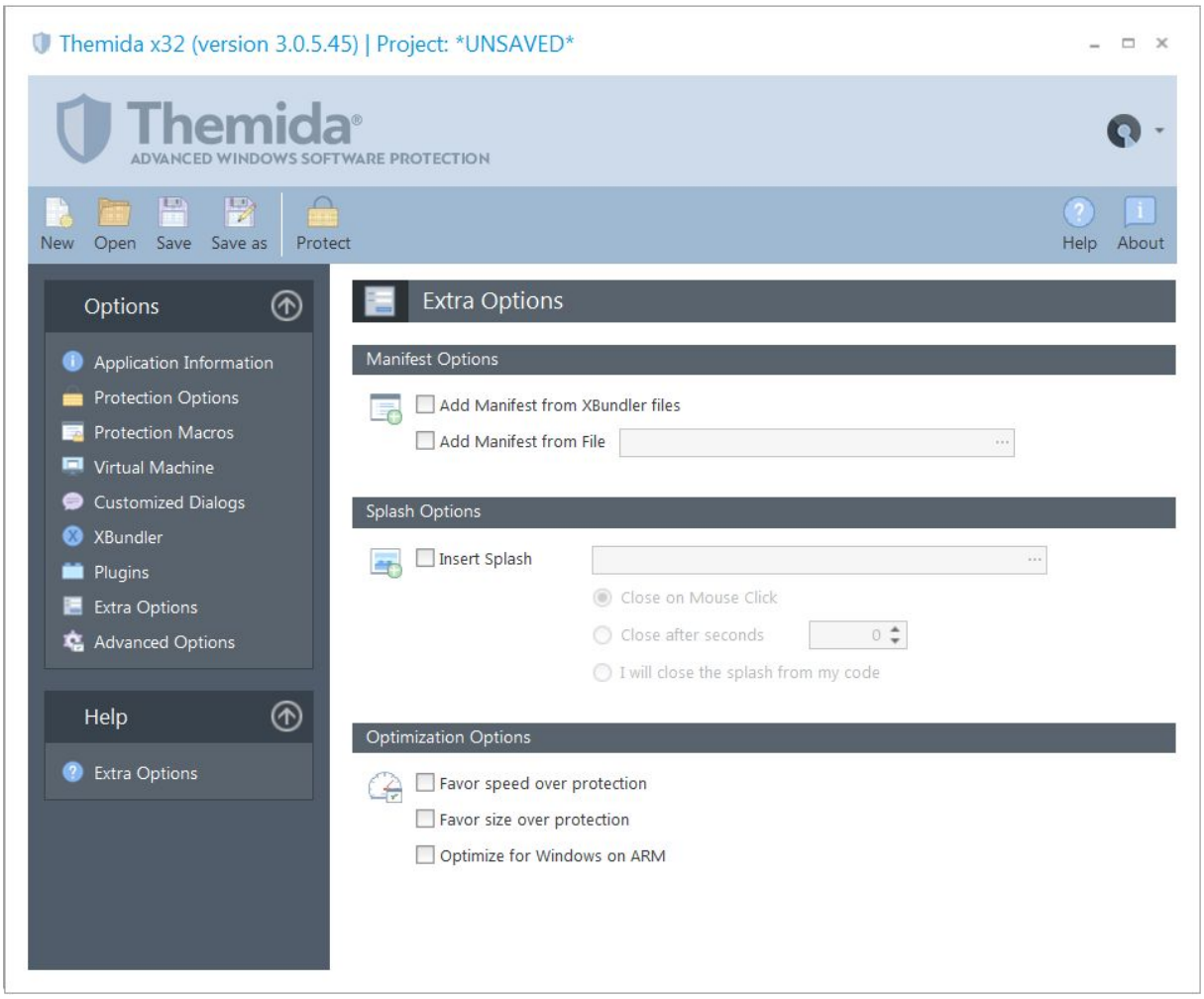
If the function returns the encryption key for the specified zone, you should return TRUE. Otherwise, return FALSE.

Remarks

At the moment, this function is only supported in 32-bit applications.

The returned encryption key must be a NULL terminated ANSI string. The size must be less than 256.

1.3.8 Extra Options



Manifest Options

You can explicitly add a custom manifest resource to your protected application in case that it's not present in your unprotected application.

- **Add Manifest from XBundler files**: Sometimes a bundled DLL (not extracted to disk) requires a manifest to operate correctly (for example, it requires admin's rights). If the DLL is bundled, that manifest is not seem by the operating system, so it cannot apply it before the application starts. This option extracts the manifest of the bundled files and apply them to the protected application.

- **Add Manifest from File**: You can add any manifest information into your protected application from an external text file. If you require to extract the manifest from an external binary (EXE/DLL) you can use any PE file editor that can read/display the resources section and you can grab the manifest (in text format) from there. After that, just create a text file with that information and pass the path to that file into the "Add Manifest From File" option. This is an example of the content of a possible external manifest file to require admin's rights in the protected application:

```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" mani-
festVersion="1.0">
  <assemblyIdentity version="1.0.0.0"
       processorArchitecture="X86"
       name="AliasDatabaseServer"
       type="win32" />
  <description>AlaiasDatabaseServer manifest</description>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level="requireAdministrator"
/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

Splash Options

You can insert a splash image (JPG image) that will be displayed before your application starts (while the protection boot code is running). If you use a heavy virtual machine for the boot protection in the Virtual Machine 13 panel, a splash screen is ideal to let your customers know that your application is booting up.

When the splash is displayed, there are several ways to close the splash screen, like **Close on Mouse Click**, **Close after** a number of **seconds** or close it from your code.

To close the splash from your own application, you can read the splash window from the environment variable ***SecureEngineSplashWnd***. Once you get the splash window you can just send a **WM_DESTROY** message to that window. This is an example in Delphi:

```
procedure CloseSplash;
var
  WndStr: String;
begin
  WndStr := GetEnvVarValue('SecureEngineSplashWnd');
  SendMessage(StrToInt(WndStr), WM_DESTROY, 0, 0);
end;
```

Optimization Options

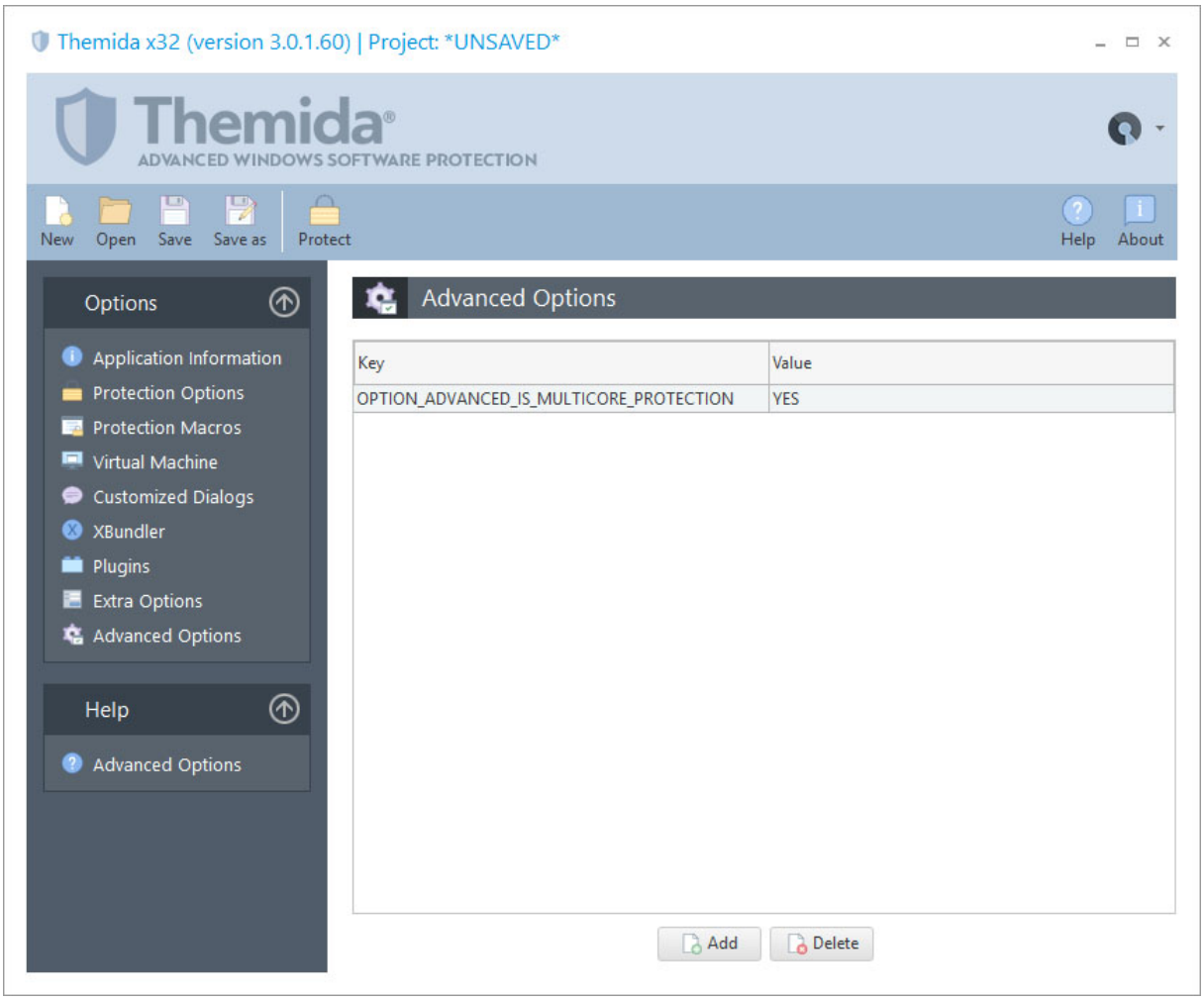
In some cases or for specific applications, you can sacrifice some complexity in the protection ir order to gain extra speed or a smaller size of your protected binary. The following options help on that:

- **Favor speed over protection**: This option reduces the complexity of the protection boot loader to increase the boot time in the protected application
- **Favor size over protection**: This option reduces in minor degree the protection and uses a different compression algorithm in order to achieve a better compression
- **Optimize for Windows on ARM**: The Windows on ARM emulation produces some penalties when emulating specific code or data accesses. This option produces a protection code that is emulated faster on Windows on ARM with just a small reduction in complexity in the protection code.

1.3.9 Advanced Options

SecureEngine contains lots of internal options mostly related to compatibility issues with specific applications. These options are not public available as they will confuse developers if we display all current available options, which are not related to security and hardly used by most applications. Developers will feel confuse (and unsecure) if they see lots of options and he is not using them in their applications.

When there is a special compatibility issue in a specific application when applying our protection, we send the required special option to the customer so he can use it for that application. In order to add a new advanced option, just **right-click** on the Advanced Options panel and select **Add**.

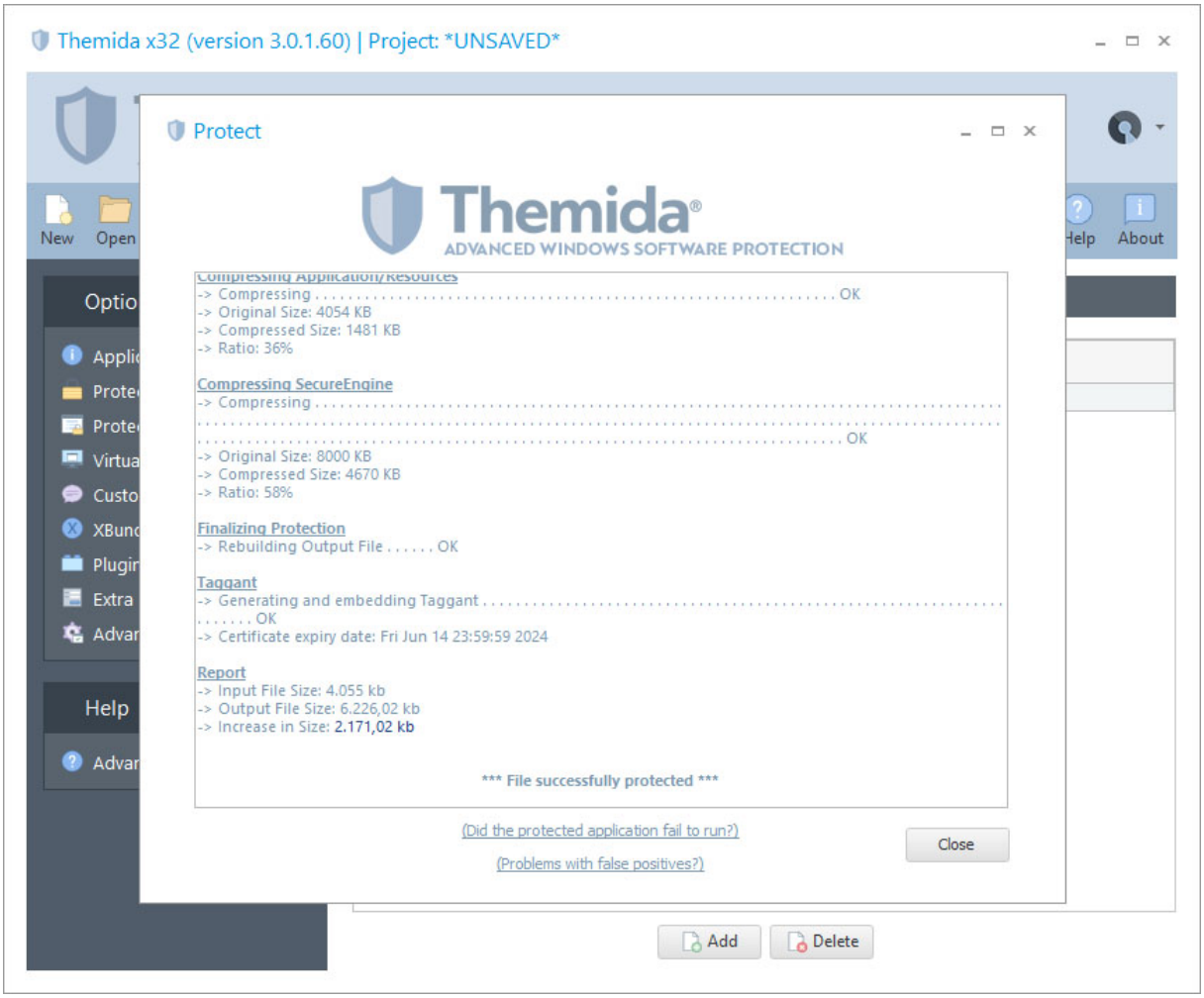


Here we have a small list of advanced options that you can use if you consider:

- **OPTION_ADVANCED_IS_MULTICORE_PROTECTION**: You can set this option to **NO** in case that you want to use a single core to protect your application.
- **OPTION_ADVANCED_SECTION_NAME:** You can set the section name (PE header) that will be appended to your protected application
- **OPTION_ADVANCED_KEEP_DEBUG_INFO**: You can set this option to **YES** to keep the debug information in your protected application. This option is recommended if you want to debug crash dumps (.dmp)

1.3.10 Protect Now

When you are done setting your protection options all you need to do is press the **Protect** button in the main toolbar to start the protection phase. A new window will appear to show you the current progress of the protection phase.



1.3.11 Protecting through the command line

Themida can be used to protect your files through the command line in order to include the protection of your application on all of your build systems.

First you need to create a Themida project file (.tmd). To create this project file, you need to start the Themida user interface and set up the protection options that you want to include in your application. After that you can invoke the following command in the command line to protect your application:

```
Themida /protect YourProjectFile.tmd
```

One of the following codes will be returned:

0 Protection was successful.

1 Project file does not exist or invalid.

2 File to protect cannot be opened.

3 File already protected.

4 Error in inserted SecureEngine macros.

5 Fatal error while protecting file.

6 Cannot write protected file to disk.

7 Error while opening or reading the inserted Splash file.

8 Taggant certificate cannot be applied.

Note: When command line protection is invoked under Windows XP, you will be able to see information about each protection stage in the current console.

Load a project file from the command line

Themida also allows you to load a project file into the user interface through the command line. To do this you have to invoke Themida in the following way:

```
Themida YourProjectFile.tmd
```

After this, Themida user interface will appear with all the information contained in your project file and is ready to protect your applications.

Protecting a different application from the one in a project file

You can specify a different input and output application from the one that is stored in your project file when protecting via command line. Example:

```
Themida /protect YourProjectFile.tmd /inputfile YourInputApplication.exe /out-
putfile YourProtectedApplication.exe
```

Protecting a different software from the one in a project file

You can specify a different software from the one that is stored in your project file when protecting via command line. Example:

```
Themida /protect YourProjectFile /software YourSoftware
```

Redirecting output to a file

To redirect the console output to a file, you have to use an extra parameter to avoid that Themida attaches itself to the current console and after that, you can use the common output redirection. The parameter to use is **/shareconsole**. This is also required when you are calling Themida from within Visual Studio and you want to display the information in the Output Window in Visual Studio. Example:

```
Themida.exe /protect YourProjectFile /shareconsole > output.txt
```

Protecting an application with a text project file

When you protect from the command line, Themida reads the internal database to retrieve the project information, software to protect, etc. That is, Themida depends on it's database (MySQL) in order to perform protection. The problem with this approach is that the embedded MySQL database can only be accessed by one instance at a time, so you cannot protect multiple applications concurrently (at least that you move Themida.exe and its database to different folders). To avoid this problem, you can export your Themida project file as a text (INI) file and use that text project file to perform protection.

To generate a text project file, you can go to the Project Manager in Themida (click on Open Project) and select the desired project and click on **Export** button.

To protect your application from a text project file, you just need to invoke Themida as follows (suppose that your text project file is called *my_project.tm*)

```
Themida /protect my_project.tm
```

Of course, you can also specify the above extra parameters (/inputfile and/or /outputfile) if you want to use different input/output file from the one in your project file.

Example of command line processing in a BAT file

The following example shows a BAT file that can be included in your build system to protect your applications through the command line:

```
@echo off

start /w Themida /protect YourProjectFile.tmd

if errorlevel 3 goto 3
if errorlevel 2 goto 2
if errorlevel 1 goto 1
if errorlevel 0 goto 0
goto done

:0
echo Application protected successfully
goto done

:1
echo ERROR: File already protected
goto done

:2
echo ERROR: File to protect cannot be opened
goto done

:3
echo ERROR: An internal error occurred while protecting

:done
```

1.4 SecureEngine® Macros

The SecureEngine® Macros allow you to interact with your application using SecureEngine®, making your application and SecureEngine® run as a single unit.

To include SecureEngine® Macros into your application, you need to specify these macros in your application source code. When SecureEngine® is going to protect your application, it will find these macros inside your application and apply the required action to each specific macro.

The different macros that SecureEngine® offers to software developers are the following:

- Using macros in your programming language 36
- VM macro 39
- Mutate macro 41
- StrEncrypt macro 42
- Unprotected macro 43
- CheckProtection macro 44

- CheckCodeIntegrity macro 46
- CheckVirtualPC macro 49
- CheckDebugger macro 50
- Which Macros should I use? 52

1.4.1 Using macros in your programming language

The current version of SecureEngine supports macros for native applications (developed with C/C++, Delphi, Visual Basic, etc.). Please note that these macros are not available for .NET languages or Visual Basic compiled in PCode mode.

To apply a macro to a specific block of code, you have to mark the beginning of the block with the "*MacroName*_**START**" marker and the end of the block using the "*MacroName*_**END**" marker.

Restrictions

A few conditions need to be satisfied in order to successfully insert SecureEngine® macros into your application. If any of these conditions are not fulfilled, Themida will show an error message when opening the file to be protected. The conditions are the following:

- Macros cannot be nested, that is, a macro cannot be inserted inside another macro. The following is an example of nesting macros:

```
void MyFunction(void)
{
    VM_START

      // your code

      VM_START     <--- nested!!!

          // your code

      VM_END

      // your code

    VM_END
}
```

- Each macro needs to have each corresponding "*MacroName*_**END**" delimiter.
- The code inside the macro must be at least 5 bytes in size.

Usage for specific programming languages

Specific information for Delphi developers

For Delphi, SecureEngine® macros can be inserted as a "assembly language" include file or linking with the SecureEngineSDK.pas file.

- **Macros as "include files":** In this case, macro markers appears as an external include file that will inserted with a parameter directive, *{$I filename}*. The included file will insert a special sequence of assembly code right after the *{$I filename}* directive. That sequence of assembly code will be detected and replaced by SecureEngine® in the protection phase. Notice that for 64-bit applications, Embarcadero RAD Studio for Delphi does not allow inline assembly to be inserted directly into your application. In this case, you have to insert the protection macros via function names.

- **Macros as "function names**": You can use the defined macros function names in the SecureEngineSDK.pas file in order to insert the different macro markers in your application. With this approach you are linking with the SecureEngineSDK.dll **only** in unprotected state, that is, your unprotected application will require the SecureEngineSDK.dll in order to run. Once that your application is protected, the linking with the SecureEngineSDK.dll is removed, so your protected application does not require the SecureEngineSDK.dll to run.

In the following we present a real example of how to use SecureEngine® macros in your Delphi application.

```
function TfmMain.GetCRC32(FileName: string): string;

begin

  {$I VM_Start.inc}             // the following block of code is protected with
an "VM" macro

  BuildCRCTable;
  CRC := $FFFFFFFF;

  AssignFile(F, FileName);
  FileMode := 0;
  Reset(F);

  {$I VM_End.inc}               // end of "VM" macro

  GetMem(Buffer, SizeOf(B));

  {$I Registered_Start.inc}        // the following block of code is protected
with a "Registered" macro

  repeat
    FillChar(b, SizeOf(b), 0);
```

```
    BlockRead(F, b, SizeOf(b), e);
    for i := 0 to (e-1) do
     CRC := RecountCRC(b[i], CRC);
  until (e < 255) or (IOresult <> 0);

  {$I Registered_End.inc}          // end of "Registered" macro

  {$I Mutate_Start.inc}             // the following block of code is protected
with an "Mutate" macro

  FreeMem(Buffer, SizeOf(B));
  CloseFile(F);
  CRC := Not CRC;
  Result := '$' + HextL(CRC);

  {$I Mutate_End.inc}               // end of "Mutate" macro

end;
```

Specific information for C/C++ developers

For the C/C++ language you have to include the "*ThemidaSDK.h*" in your application source code, so you can put the different macro markers inside your source code. By default, the ThemidaSDK.h file emits inline assembly for your C/C++ 32-bit applications and function names (from within the SecureEngineSDK.dll) for your C/C++ 64-bit applications. This means that your 64-bit applications require the SecureEngineSDK.dll when you run your application **unprotected**. Once that you protect your application, the linking with the SecureEngineSDK.dll is removed, so your protected application does not require that DLL.

Following will demonstrate a real example of how to use SecureEngine® macros in your C/C++ application. .

```
LRESULT CALLBACK MainHandler(HWND hDlg, UINT message, WPARAM wParam, LPARAM
lParam)
{
    switch (message)
    {
    case WM_INITDIALOG:

        VM_START                        // the following block of code is protec-
ted with a "CodeReplace" macro

        if (WLRegGetStatus(NULL) == 1)
        {
            WLRegGetLicenseInfo(Name, Company, ExtraData);
            SetDlgItemText(hDlg, IDC_NAMEEDIT, Name);
            SetDlgItemText(hDlg, IDC_COMPANYNAME, Company);
            SetDlgItemText(hDlg, IDC_EXTRAEDIT, ExtraData);
        }

        VM_END                          // end of "VM" macro

        return TRUE;

    case WM_COMMAND:
```

```
            if (LOWORD(wParam) == IDCANCEL)
            {
                MUTATE_START                        // the following block of code is
    protected with an "Encode" macro

                EndDialog(hDlg, LOWORD(wParam));

                MUTATE_END                          // end of "Mutate" macro

                return TRUE;
            }
            break;
        }
        return FALSE;
    }
```

Specific information for Visual Basic developers

For Visual Basic these macros appear as a special Visual Basic instruction that will be detected by SecureEngine® during the protection phase.

In the following we present a real example of how to use SecureEngine® macros in your Visual Basic application. .

```
    Private Sub CheckStatusButton_Click()

           If AppStatus <> 1 Then

                    Call VarPtr("VMStart")

                    TrialDaysLeftLabel.Caption = WLTrialDaysLeft
                    TrialExecLeftLabel.Caption = WLTrialExecutionsLeft
                    MinutesLabel.Caption = WLTrialGlobalTimeLeft
                    RuntimeLabel.Caption = WLTrialRuntimeLeft

                    Call VarPtr("VMEnd")

           End If

    End Sub
```

1.4.2 VM macro

The **VM** macro allows you to mark regions of code that will be executed inside the SecureEngine® Virtual Machine. When the CPU is going to execute the code inside your VM macro, SecureEngine® will take control and will emulate the original code inside the macro with virtual opcodes that only the SecureEngine® Virtual machine can understand.

The VM macro is the original name used in older versions of our protection. In newer versions of our protection we recommend that you specify the name of the Virtual Machine that will be used to virtualize the code inside the START - END markers. For example, instead of using "VM_START/END" for a block of code, you should select which Virtual Machine (from

the Virtual Machine panel 13) will be used to virtualize that code (example "VM_TIGER_WHITE_START/END")

We strongly recommend the use of this macro whenever possible, due to its flexibility and continuous improvement in the internal protection of these macros.

NOTE: The current version of SecureEgine® does not support this macro for .NET languages or Visual Basic compiled in PCode mode.

Show Delphi Macro Usage

```
{$I VM_TIGER_BLACK_START.inc}

// your code goes here

{$I VM_TIGER_BLACK_END.inc}
```

Show C/C++ Macro Usage

```
VM_TIGER_BLACK_START

// your code goes here

VM_TIGER_BLACK_END
```

Show Visual Basic Macro Usage

```
Call VarPtr("VM_START")

' your code goes here

Call VarPtr("VM_END")
```

Remarks

To make sure that you have inserted a VM macro in a right place in your application, you should be aware of the following details:

- To avoid a performance decrease, you should avoid tight loops (*FOR, WHILE, DO*...) with a big number of iterations inside the VM macro. If a specif code is called many times per second you should avoid putting a VM macro or select a lighter virtual machine macro like VM_TIGER_WHITE
- Switch/Case statements inside the macro might not work properly in some compiled applications. Notice that Switch statements are named in a different way in different programming languages ("*Case*" --> Delphi, "*Select Case*" --> VB, etc).

- Exception handling inside the macro will not work properly. You should avoid putting VM macros around *try-except* clauses. For Visual Basic, "try-except" clauses corresponds to "On Error" statements.

1.4.3 Mutate macro

The **MUTATE** macro allows you to mark regions of code that will be mutated. The original x86 machine code will be converted into equivalent but complex x86 machine code. The execution of the MUTATE macro is quite fast compared to VM macros but the level of security is quite low compared with VM macros.

The MUTATE macro is suitable for those code areas that you want to apply some obfuscation and want to keep a high performance in the execution of the mutated code.

NOTE: The current version of SecureEgine® does not support this macro for .NET languages or Visual Basic compiled in PCode mode.

Show Delphi Macro Usage

```
{$I Mutate_Start.inc}
// your code goes here
{$I Mutate_End.inc}
```

Show C/C++ Macro Usage

```
MUTATE_START
// your code goes here
MUTATE_END
```

Show Visual Basic Macro Usage

```
Call VarPtr("MUTATE_START")
' your code goes here
Call VarPtr("MUTATE_END")
```

Remarks

To make sure that you have inserted a MUTATE macro in a right place in your application, you should be aware of the following details:

- Switch statements inside the macro might not work properly in some compiled applications. Notice that Switch statements are named in a different way in different programming languages ("*Case*" --> Delphi, "*Select Case*" --> VB, etc).

- Exception handling inside the macro might not work properly. You should avoid putting MUTATE macros around *try-except* clauses. For Visual Basic, "try-except" clauses corresponds to "On Error" statements.

1.4.4 StrEncrypt macro

The **STR_ENCRYPT/STR_ENCRYPTW** macro allows you to mark regions of code where all referenced strings inside the region will be encrypted in protection time and decrypted in runtime when required by the target application. The decryption is performed inside the SecureEngine Virtual Machine and the location of the decrypted string is different from the original one in the unprotected application. The original location of the string is destroyed and never used again in the protected application.

If you are using Unicode strings in your application, you have to use the macro **STR_ENCRYPTW** which can process Unicode strings.

NOTE: The current version of SecureEgine® does not support this macro for .NET languages or Visual Basic compiled in PCode mode.

Show Delphi Macro Usage

```
{$I StrEncrypt_Start.inc}
// your code goes here
{$I StrEncrypt_End.inc}
```

Show C/C++ Macro Usage

```
STR_ENCRYPT_START
// your code goes here
STR_ENCRYPT_END
```

Show Visual Basic Macro Usage

```
Call VarPtr("STR_ENCRYPT_START")
' your code goes here
Call VarPtr("STR_ENCRYPT_END")
```

Remarks

For further protection you can put a VM macro around the "STR_ENCRYPT" macro, so all your code area where your strings are used is also virtualized. Example:

```
VM_START
  STR_ENCRYPT_START
  ' your code goes here
 STR_ENCRYPT_END
VM_END
```

There are some internal options that can be added to increase the protection of the STR_ENCRYPT macro. You can add the following entries in the Advanced Options 30 panel:

- **OPTION_MACROS_ENCRYPT_STRINGS_DECRYPT_ON_HEAP=YES**

  The string will be decrypted on an allocated block in the heap

- **OPTION_MACROS_ENCRYPT_STRINGS_REENCRYPT=YES**

  The decrypted string on the heap will be destroyed when the STR_ENCRYPT_END marker is executed

1.4.5 Unprotected macro

The **UNPROTECTED** macro allows you to mark regions of code that will be ONLY executed when your application is not yet protected. Once your application is protected, the code inside the macro will not be executed, basically the code inside the macro markers is destroyed and jumped to avoid execution. This macro is only necessary to avoid releasing unprotected applications by mistake.

NOTE:The current version of SecureEgine® does not support this function to be called for .NET languages or Visual Basic applications.

Show Delphi Macro Usage

```
{$I Unprotected_Start.inc}

// your code goes here

{$I Unprotected_End.inc}
```

Show C/C++ Macro Usage

```
UNPROTECTED_START

// your code goes here

UNPROTECTED_END
```

1.4.6 CheckProtection macro

The **CHECK_PROTECTION** macro allows you to check if your application has been partially unpacked or some protection engines have been attacked by a cracker. This macro offers communication between the protected application and the SecureEngine protection.

NOTE: The current version of SecureEgine® does not support this macro for .NET languages or Visual Basic applications.

The CHECK_PROTECTION macro can be called from inside other macros. In fact, it's highly recommend to call the CHECK_PROTECTION macro from inside VM 39 macros.

The CHECK_PROTECTION macro has a special syntax:

CHECK_PROTECTION (user_variable, user_value)

Where "*user_variable*" is any **local** or **global** variable in the application and "*user_value*" is any **immediate value (constant value)**. The way that it works is the following:

- The CHECK_PROTECTION macro is called.
- SecureEngine takes control of the processor and make special checks to know if the application has been tampered.
- If the application is not tampered, SecureEngine sets "user_variable" equal to "user_value".
- If the application is tampered, SecureEngine does not set "user_variable". You should take care of initializing "user_variable" to something else from "user_value".

- SecureEngine returns control to the protected application. The protected application should check the value of "user_variable" and execute the desired action if the application has been tampered.

If you detect that your application has been tampered, please, consider the following practices:

- Avoid taking an immediate action, like displaying a message or crashing the application. If you take an immediate action, the cracker will know where the problematic code is located and will focus all his attention at that point, trying to figure out the root of the problem in that code.
- Avoid displaying messages saying that the application has been tampered. Instead, make a "late" crash (see below) or display a strange error message at a later point in your application.
- Produce a "late crash" or malfunction. That is, if you detect that your application has been tampered, you mark special variables (or similar action) in your code. At a later point in your application, you crash your application or initialize further structures in a wrong way, so, your application won't work as expected. For example, suppose that you are protecting a CD burning application. When your application is initializing, you call "CHECK_PROTECTION" macro to determine if the application is tampered or not. If it's tampered, you won't take any action yet, but instead, you will wait for the CD recording process to burn random or incorrect data into the CD.
- Use VM 39 macros in all those places where you call CHECK_PROTECTION and where you check if the application was tampered. Also, if you decide to produce a "late" crash or malfunction, that code which produces the crash or malfunction should go inside VM or CodeReplace macros.

Show C/C++ Macro Usage

```
int MyCheckVar;

VM_START

   // your code goes here

   CHECK_PROTECTION(MyCheckVar, 0x12345678)

   // your code goes here

   if (MyCheckVar != 0x12345678)
     printf("We are tampered!");

VM_END
```

Show Delphi Macro Usage

```
var
  MyCheckVar: Integer;

begin

{$I VM_Start.inc}

   // your code goes here

   {$I CheckProtection_Prolog.inc}
   asm
     push 11111111                    // 11111111 is our special constant
     pop  MyCheckVar                  // SecureEngine will set "MyCheckVar" to
   11111111 if protection is OK
   end;
   {$I CheckProtection_Epilog.inc}

   // your code goes here

   if MyCheckVar <> 11111111 then
     ShowMessage("We are tampered!");

{$I VM_End.inc}
```

Advises about how to use this macro

- Put the CHECK_PROTECTION macro inside VM or CodeReplace macros.
- Think always that the first attack from a cracker is just directly jump over your VM / CodeReplace macro (that is, the code inside the macro is not executed), so you should make sure that inside the macro you put code that is necessary for your application to run correctly.
- You don't have to call the CHECK_PROTECTION macro periodically, just make sure that it's executed at any time in your application.
- You can put as many CHECK_PROTECTION macros as desired, but we recommend you just putting a few of them (about 5 of them) in different routines in your application.

1.4.7 CheckCodeIntegrity macro

The **CHECK_CODE_INTEGRITY** macro allows you to check if the code section of your protected application has been patched in runtime (using for example an memory patcher). This macro offers communication between the protected application and the SecureEngine protection.

NOTE: The current version of SecureEgine® does not support this macro for .NET languages or Visual Basic applications.

The CHECK_CODE_INTEGRITY macro can be called from inside other macros. In fact, it's highly recommend to call the CHECK_CODE_INTEGRITY macro from inside VM 39 macros.

The CHECK_CODE_INTEGRITY macro has a special syntax:

CHECK_CODE_INTEGRITY (user_variable, user_value)

Where "*user_variable*" is any **local** or **global** variable in the application and "*user_value*" is any **immediate value (constant value)**. The way that it works is the following:

- The CHECK_CODE_INTEGRITY macro is called.
- SecureEngine takes control of the processor and make special checks to know if the code section of your application has been patched.
- If the code section of the application is not patched, SecureEngine sets "user_variable" equal to "user_value".
- If the application is patched, SecureEngine does not set "user_variable". You should take care of initializing "user_variable" to something else from "user_value".
- SecureEngine returns control to the protected application. The protected application should check the value of "user_variable" and execute the desired action if the code section of the application has been patched.

If you detect that the code section of your application has been tampered, please, consider the following practices:

- Avoid taking an immediate action, like displaying a message or crashing the application. If you take an immediate action, the cracker will know where the problematic code is located and will focus all his attention at that point, trying to figure out the root of the problem in that code.
- Avoid displaying messages saying that the application has been tampered. Instead, make a "late" crash (see below) or display a strange error message at a later point in your application.
- Produce a "late crash" or malfunction. That is, if you detect that your application has been tampered, you mark special variables (or similar action) in your code. At a later point in your application, you crash your application or initialize further structures in a wrong way, so, your application won't work as expected. For example, suppose that you are protecting a CD burning application. When your application is initializing, you

call "CHECK_CODE_INTEGRITY" macro to determine if the application code is patched or not. If it's patched, you won't take any action yet, but instead, you will wait for the CD recording process to burn random or incorrect data into the CD.

- Use VM 39 or macros in all those places where you call CHECK_CODE_INTEGRITY and where you check if the application code was patched. Also, if you decide to produce a "late" crash or malfunction, that code which produces the crash or malfunction should go inside VM or CodeReplace macros.

Show C/C++ Macro Usage

```
int MyCheckVar;

VM_START

   // your code goes here

   CHECK_CODE_INTEGRITY(MyCheckVar, 0x12345678)

   // your code goes here

   if (MyCheckVar != 0x12345678)
     printf("Application code is patched!");

VM_END
```

Show Delphi Macro Usage

```
var
  MyCheckVar: Integer;

begin

{$I VM_Start.inc}

   // your code goes here

   {$I CheckCodeIntegrity_Prolog.inc}
   asm
     push 11111111                    // 11111111 is our special constant
     pop  MyCheckVar                  // SecureEngine will set "MyCheckVar" to
   11111111 if protection is OK
   end;
   {$I CheckCodeIntegrity_Epilog.inc}

   // your code goes here

   if MyCheckVar <> 11111111 then
     ShowMessage("We are tampered!");

{$I VM_End.inc}
```

Advises about how to use this macro

- Put the CHECK_CODE_INTEGRITY macro inside VM macros.
- You should call the CHECK_CODE_INTEGRITY at specific points in your application code. You could also call it from a thread which calls that macro periodically (once each 30-60 seconds).
- For applications with a big code section, this macro might take some time to be executed. If you want to increase the speed when calling this macro, you can insert the following option in the Advanced Options 30 panel:

```
OPTION_MACROS_FAST_CHECK_CODE_INTEGRITY=YES
```

1.4.8 CheckVirtualPC macro

The **CHECK_VIRTUAL_PC** macro allows you to check if your application is running under VMWare/VirtualPC.

NOTE: The current version of SecureEgine® does not support this macro for .NET languages or Visual Basic applications.

The CHECK_VIRTUAL_PC macro can be called from inside other macros.

The CHECK_VIRTUAL_PC macro has a special syntax:

CHECK_VIRTUAL_PC (user_variable, user_value)

Where "*user_variable*" is any **local** or **global** variable in the application and "*user_value*" is any **immediate value (constant value)**. The way that it works is the following:

- The CHECK_VIRTUAL_PC macro is called.
- SecureEngine takes control of the processor and make special checks to know if your application is running under VMWare/VirtualPC.
- If your application is **not** running under VMWare/VirtualPC, SecureEngine sets "user_variable" equal to "user_value".
- If the application is running under VMWare/VirtualPC, SecureEngine does not set "user_variable". You should take care of initializing "user_variable" to something else from "user_value".

- SecureEngine returns control to the protected application. The protected application should check the value of "user_variable" and execute the desired action if the application is running under VMWare/VirtualPC.

Show C/C++ Macro Usage

```
int MyCheckVar;

VM_START

   // your code goes here

   CHECK_VIRTUAL_PC(MyCheckVar, 0x12345678)

   // your code goes here

   if (MyCheckVar != 0x12345678)
     printf("Application is running under VMWare/VirtualPC");

VM_END
```

Show Delphi Macro Usage

```
var
  MyCheckVar: Integer;

begin

{$I VM_Start.inc}

   // your code goes here

   {$I CheckVirtualPC_Prolog.inc}
   asm
     push 11111111                    // 11111111 is our special constant
     pop  MyCheckVar                  // SecureEngine will set "MyCheckVar" to
   11111111 if VMWare not present
   end;
   {$I CheckVirtualPC_Epilog.inc}

   // your code goes here

   if MyCheckVar <> 11111111 then
     ShowMessage("Application is running under VMWare/VirtualPC!");

{$I VM_End.inc}
```

1.4.9 CheckDebugger macro

The **CHECK_DEBUGGER** macro checks if your application is running under a debugger.

NOTE: The current version of SecureEgine® does not support this macro for .NET languages or Visual Basic applications.

The CHECK_DEBUGGER macro can be called from inside other macros.

The CHECK_DEBUGGER macro has a special syntax:

CHECK_DEBUGGER (user_variable, user_value)

Where "*user_variable*" is any **local** or **global** variable in the application and "*user_value*" is any **immediate value (constant value)**. The way that it works is the following:

- The CHECK_DEBUGGER macro is called.
- SecureEngine takes control of the processor and make special checks to know if your application is running under a debugger.
- If your application is **not** running under a debugger, SecureEngine sets "user_variable" equal to "user_value".
- If the application is running under a debugger, SecureEngine does not set "user_variable". You should take care of initializing "user_variable" to something else from "user_value".
- SecureEngine returns control to the protected application. The protected application should check the value of "user_variable" and execute the desired action if the application is running under a debugger.

Show C/C++ Macro Usage

```
int MyCheckVar;

VM_START

   // your code goes here

   CHECK_DEBUGGER(MyCheckVar, 0x12345678)

   // your code goes here

   if (MyCheckVar != 0x12345678)
     printf("Application is running under a debugger!");

VM_END
```

Show Delphi Macro Usage

```
var
  MyCheckVar: Integer;

begin
```

```
{$I VM_Start.inc}

   // your code goes here

   {$I CheckDebugger_Prolog.inc}
   asm
     push 11111111                    // 11111111 is our special constant
     pop  MyCheckVar                  // SecureEngine will set "MyCheckVar" to
   11111111 if VMWare not present
   end;
   {$I CheckDebugger_Epilog.inc}

   // your code goes here

   if MyCheckVar <> 11111111 then
     ShowMessage("Application is running under a debugger!");

{$I VM_End.inc}
```

1.4.10 Which Macros should I use?

It is normal that a programmer feel lost when deciding which macros he/she should use. We recommend mostly using our virtualization macros (VM, TIGER_VM, FISH_VM, etc) as they offer the biggest protection in latest versions of our protection.

It's not a good idea to insert multiple (different) protection virtual machines as the final size of your application will growth noticeably. A good approach is to use a lighter VM (like FISH/TIGER) for your code that needs to be quite protected but also executed fast and use a heavier VM (like FISH_BLACK, PUMA, SHARK, ...) for your code that needs to be highly protected and you can afford that extra time that it takes to execute the virtualized code under the heavier VM.

1.5 FAQ

Here there is a list with the most frequently asked questions:

- General 53
- Protection Options 57
- Macros 71
- XBundler 81
- Sales 88

1.5.1 General

- I want to protect several applications concurrently via the command line, because I'm creating a specific protected application for each customer. Is it possible? 54
- I want to include relative paths in the "Input Filename" and "Output FileName" in the User Interface in Themida. How can I do that? 54
- Is Themida compatible with Delphi 2009? 54
- Is Themida compatible with Windows 8? 54
- I'm using SetupBuilder to build and protect my application from the command line. The application is protected correctly but I don't see any log in the command line. 54
- In my program I use the "JCLDebug" routines to get exception information (line, routine, etc) when an exception occurs. The problem is that once the application is protected, I get limited debug information. 55
- What's the difference between Themida and WinLicense? If I buy WinLicense, can I use it without adding license control to my software? 55
- Are there localized versions of your products to support other languages? 55
- I bought a Themida license to protect my applications. My friend needs to protect his application. Can I protect his software with Themida? 55
- I have a suggestion about a new protection feature and features for your software. Will you implement it? 55
- What programming languages are supported by Themida? 55
- If I protect my app with the demo version and it is stable, do I have a good level of confidence that the purchased version will work also? 55
- What is your support policy? Do you have a minimum response and/or problem-solving time? What types of support do you offer? 56
- How compatible is your software with various win O/S? (e.g. Vista in different languages, 2003 server, 64bit etc.) 56
- I don't use Windows Vista right now, but depending on our customers I will need Themida (and also the protected application as well) to be able to run on Windows

Vista. Do you also support 64-bit operating systems such as Windows 2003 x64 and Vista x64? 56

- I have problems protecting my installer. What can I do? 56

1.5.1.1 I want to protect several applications concurrently via the command line, because I'm creating a specific protected application for each customer. Is it possible?

Yes, you can do it with the specific command line that you use for Themida. In latest versions we have removed all intermediate files during protection, so there are no collisions when invoking Themida concurrently. Example:

```
Themida.exe /protect MyProject1.tmd
Themida.exe /protect MyProject2.tmd
...
```

1.5.1.2 I want to include relative paths in the "Input Filename" and "Output FileName" in the User Interface in Themida. How can I do that?

You can use special constants in your input/output file names, so you don't have to rely on full paths.

Please, refer to the Special Constants in Input/Output file names 5 section.

1.5.1.3 Is Themida compatible with Delphi 2009?

Yes, Themida is compatible with old and new Delphi versions. Please, notice that Delphi 2009 works with UNICODE strings by default, so you might want to use the UNICODE functions of the SDK.

1.5.1.4 Is Themida compatible with Windows 8?

Yes, latest versions of our products are compatible with latest Windows versions. In case that a new version of Windows appears and current Themida is not compatible with it, we will fix it as soon as possible as that's one of our main priorities.

1.5.1.5 I'm using SetupBuilder to build and protect my application from the command line. The application is protected correctly but I don't see any log in the command line.

Themida will display a log with all the protection steps when you protect under Windows XP or higher.

If you want to display the log from SetupBuilder, you can write a batch file to call Themida and issue a "#run themida.bat". This will open the command window and the log will be seen.

The Themida.bat file will contain:

Themida.exe /protect YouProjectName

1.5.1.6 In my program I use the "JCLDebug" routines to get exception information (line, routine, etc) when an exception occurs. The problem is that once the application is protected, I get limited debug information.

For JCL exceptions, please, add the following line in the Advanced Options panel:

```
OPTION_ADVANCED_ADD_IMPORTS=[kernel32.dll,RaiseException]
```

1.5.1.7 What's the difference between Themida and WinLicense? If I buy WinLicense, can I use it without adding license control to my software?

WinLicense is in fact Themida, plus Trial/Licensing options. Every protection option included in Themida, is included in WinLicense.

You can use WinLicense without adding license control to your software. So, if you purchase WinLicense, you don't need to buy Themida.

1.5.1.8 Are there localized versions of your products to support other languages?

Unfortunately, in version 3.0 we removed the user interface localization. We might add it in a future.

1.5.1.9 I bought a Themida license to protect my applications. My friend needs to protect his application. Can I protect his software with Themida?

No, each license is private for the company/user that acquires it. You can use your Themida license to protect applications that are developed by you or that you own the full copyrights.

Each protected application is watermarked with the license key information to help us track about possible misuse in Themida license keys. In case that we find a borrowed/stolen key, we will invalidate that license key for future updates.

1.5.1.10 I have a suggestion about a new protection feature and features for your software. Will you implement it?

We are happy to receive suggestions about possible protection features that you think should included in our products. We will try to implement your suggestions as soon as possible. Please, contact us at info@oreans.com and let us know your requests.

1.5.1.11 What programming languages are supported by your products?

Themida supports most programming languages, like C/C++, C#, Delphi, Visual Basic, PowerBasic, PureBasic, Assembly, .NET languages, etc.

1.5.1.12 If I protect my app with the demo version and it is stable, do I have a good level of confidence that the purchased version will work also?

Some protection features are disabled (or reduced) in the DEMO version, but you can make sure that if it works in the DEMO version, it will work in the Registered version.

Anyway, in case that you find an incompatibility we can help you out and let you know what the problem is (or fix it in case that there is a bug)

1.5.1.13 What is your support policy? Do you have a minimum response and/or problem-solving time? What types of support do you offer?

We know how important is support for our customers. In this type of software (software protection) we know that support is highly important for our customers, because if we fail in supporting our customers, they will fail supporting their customers!

We try to fix any reported problem the same day as reported (of course, this cannot be always done when we cannot reproduce the problem here and we require external tests to be done in the problematic client's PC). As soon as the problem is fixed, we release a new private version with the fix for the customer who reported the problem. The fix will be available for any of our customers who require the new private version or face the same problem.

1.5.1.14 How compatible is your software with various win O/S? (e.g. Vista in different languages, 2003 server, 64bit etc.)

Our software has been tested against all Windows versions. Notice that version 3.x does not support Windows 95/98.

1.5.1.15 I don't use Windows Vista right now, but depending on our customers I will need Themida (and also the protected application as well) to be able to run on Windows Vista. Do you also support 64-bit operating systems such as Windows 2003 x64 and Vista x64?

It's very important for us (and for our customers!) to keep their applications fully compatible under new operating systems (like Vista, and new x64 systems). Our products support from Windows XP to latest versions of Windows (in both 32 and 64 bits).

1.5.1.16 I have problems protecting my installer. What can I do?

Installers are very special applications. Basically an installer compress all files and create a single file (like a ZIP file). When the installer is launched, it decompress all files in runtime (like a ZIP decompressor). Before the files are decompressed, the installer normally checks for the integrity (CRC) of the whole file, to know if it has been manipulated and it will fail to run if the file has been modified.

When an installer file is protected, the protection modifies the original installer application, so it will fail on the CRC check performed by the installer runtime code.

It does not make much sense to protect an installer, as the cracker will focus on the main extracted (installed) application to crack/attack it, not the installer itself. Also, as the main file is already compressed inside the installer file, the protection does not have the chance to apply protection on your main (installed) application.

The normal procedure would be the following:

1) Compile your application

2) Protect it with our protection

3) Create the final installer (including the protected application and all required files for the installer)

1.5.2 Protection Options

- Can I use Themida from a computer with no internet connection or better under a VirtualBox/VMWare environment? I was wondering if internet is required for Themida to work. 60
- Do I need to ship SecureEngine.dll with my protected application? 60
- I use Themida with Visual Studio in the custom build steps but no output (build information) is generated at all. What's the problem? 60
- I'm evaluating Themida DEMO to protect my Windows service, but after protecting it my service does not start at all. What should I do? 60
- How can I avoid the command line output displayed by Themida when protecting my project via the command line protection? 60
- My application requires administrator's privileges to run on Vista. Will my protected application run with admin's rights? 60
- My (native) protected application fails to run after being protected. What can I do? 60
- My .NET protected application fails to run after being protected. What can I do? 61
- My CodeJock application looses skinning after being protected. What can I do? 62
- My protected application is flagged as a virus. What can I do? 62
- My MSVC application generates a crash dump file (.DMP) file when it crashes, so I can load and examine the crash dump file. When my application is protected the generated crash dump does not contain valid information. 63
- Is it possible to know from my application if the application has been unpacked? 63

- I need to get a Vista logo. Is your protection compatible with Microsoft tests? 64
- I want to protect my .NET application with Themida, can I use an obfuscator before protecting with Themida? 64
- How can I omit the output displayed by WinLicense when protecting via command line? 64
- Can you let me know which protection options affect execution speed of my application? 64
- I'm using the CHECK_CODE_INTEGRITY macro in my Delphi application but the macro always returns that my code has been modified. Any ideas? 64
- I see that Themida detects if my file on disk has been patched, but how can I detect if someone has patched my application in memory? 64
- How can I insert my own splash screen using the Plugin feature? 65
- Can you let me know about all available Advanced Options and what they are for? 65
- Some of my users complaint regarding RegMon (Filemon) loaded in memory. How to proceed? 65
- If I want to sacrifice a minimal amount of security to gain the maximum amount of application startup speed, what options should I disable in Themida? 66
- Can I compress my application with UPX and then protect it with Themida? 66
- Is there any issue to run my protected plugins on Xp 64 (32bit mode)? 66
- My application's main function is the scientific calculation needed high performance. Is there any performace lost when I encrypt my app. with Themida? 66
- Does Themida encrypt string constants in my code? 66
- If I set the Anti-Patching option, can I digitally sign my application? 66
- I would like to include the same protection options and custom dialogs in all my applications. Can I apply the same settings to all my applications? 67

- I want to include Themida in my build system. Does Themida support command line protection? 67
- Can I protect my Windows NT system service with Themida? 67
- When I protect my application with Themida, the size is increased by 500Kb or more! 67
- How many KB will my application grow in size, after being protected by Themida? 68
- When I use macros directly around some API calls I get errors in Themida saying that one of my START or END markers is missing. What's wrong? 68
- Please let us know how Themida influences the program performance? What would you advice us to pay attention to in order to minimize the performance losses? Will it affect the protection? 69
- If I use the option "Entry Point Virtualization", my DLL crashes. If I uncheck that option, will it make it easier to crack? 69
- Can I protect my .NET applications with Themida? 69
- I'm happy with all the protection features offered by Themida, but I miss the trial/licensing features. Will they be included? 69
- Can I get the computer Hardware ID with Themida? 69
- Can I protect mixed managed/unmanaged DLLs? 70
- When I enable the "Advanced API-Wrapping" option my applications runs slower 70
- When my STR_ENCRYPT macros are processed in the last "Protection" panel, I can see "skipped" when the macro is processed. What can I do? 70
- When I protect my application with an older version, the size of the protected application is smaller. Can I keep the same size in latest version? 70
- When I add a JPG image in the splash option, my image is not displayed on startup 70

1.5.2.1 Can I use Themida from a computer with no internet connection or better under a VirtualBox/VMWare environment? I was wondering if internet is required for Themida to work.

Themida does not require internet access for the protection process. You can use it on a PC with no internet connection or under VirtualBox/VMWare.

1.5.2.2 Do I need to ship SecureEngine.dll with my protected application?

The linking with SecureEngineSDK DLL is removed at protection stage. Your protected application does not require that DLL to run, so you don't need to ship it with your application.

1.5.2.3 I use Themida with Visual Studio in the custom build steps but no output (build information) is generated at all. What's the problem?

Please, pass the /shareconsole parameter when you call Themida via the command line. Example:

```
Themida.exe /protect YourProject.tmd /shareconsole
```

1.5.2.4 I'm evaluating Themida DEMO to protect my Windows service, but after protecting it my service does not start at all. What should I do?

Please, notice that the DEMO version displays a splash screen before the protected application starts. For Windows services, that splash screen cannot be displayed, so the protected service cannot start. You can send us your unprotected windows service and we are happy to protect it for your with our latest version, so you can check it in your computers.

1.5.2.5 How can I avoid the command line output displayed by Themida when protecting my project via the command line protection?

You just need to add the "/q" parameter when you call Themida from the command line. Example:

Themida.exe /protect MyProject /q

1.5.2.6 My application requires administrator's privileges to run on Vista. Will my protected application run with admin's rights?

Protected applications will run with the same privilege level as your unprotected application. If you want to raise to admin's rights your protected application, please, refer to the section "Add Manifest" in the Extra Options 28 panel.

1.5.2.7 My (native) protected application fails to run after being protected. What can I do?

If you are having problems with your protected native EXE/DLL, please, perform the following steps:

1) Uncheck the option "**Entry Point Virtualization**" and protect again. This option is not compatible with all applications and this option might not be suitable for your application

If the application still fails, go to step 2)

2) If you are using protection macros (like VM macros, etc), uncheck the option "**Encrypt Strings in VM macros**" (ANSI strings and UNICODE strings). If your application only works in UNICODE, do not set the ANSI string option. The same applies if your application is implemented with ANSI strings (do not check the UNICODE strings option). In any case, it's better to use the STR_ENCRYPT macro around those sensitive strings that you want to protect.

If the application still fails without the option "Encrypt Strings in VM macros", go to step 3)

3) Uncheck the option "Advanced API-Wrapping". If the problem is coming from here, let us know please, so we can add support for it.

4) If you are using XBundler, please, temporally uncheck the XBundler option, just to know if the problem is coming from there. In case that this option is the culprit of the problem, let us know please, so we can add support for it.

5) If you are using different protection macros, maybe the problem is coming from a "bad" inserted macros. First, you can uncheck all macros to know if the problem is coming from there. To do so, please, ***temporally*** add the following line in the Advanced Options panel:

```
OPTION_MACROS_DISABLE_ALL_MACROS=YES
```

If the problem is coming from your inserted macros, please, check that you have not inserted one of the known macros restrictions. Please, check them here 75. Please, do not forget to remove the option "`OPTION_MACROS_DISABLE_ALL_MACROS`"

6) If the problem still persist, please, send us your unprotected application (or any other test compiled application) to reproduce the problem here and fix it for you. Of course, any files that you send us will be treated with total confidentiality.

1.5.2.8 My .NET protected application fails to run after being protected. What can I do?

If you are having problems with your protected .NET EXE, please, perform the following steps:

1) Go to the Advanced Options 30 panel and add the following line:

```
OPTION_ADVANCED_DONT_HOOK_ALL_MODULES=YES
```

If the problem persists, go to step 2)

2) If you are using XBundler, temporally uncheck it and see if the problem is coming from there. If it does, try removing some of your inserted files to see the one that is causing the

problem. You can also send us any compiled test application and the problematic file to bundle to check it here and fix it.

3) If the problem persists, go to the Advanced Options panel and add the following line:

```
OPTION_ADVANCED_DOT_NET_RELOCATE=YES
```

4) If the problem persists, please, send us any compiled test application to reproduce your problem here. Of course, any files that you send us will be treated with total confidentiality.

1.5.2.9 My CodeJock application looses skinning after being protected. What can I do?

Please, go to the Advanced Options panel and add the following line:

```
OPTION_ADVANCED_CODEJOCK_SUPPORT=YES
```

1.5.2.10 My protected application is flagged as a virus. What can I do?

We have been fighting with false positives since the beginning of our protection. Virus/malware writers usually use a software protector to protect their code and make it "invisible" to antivirus. Due to this, antivirus companies are more strict on packed files.

Also, some (not widely known) antivirus, have a very bad heuristic and they even report as virus any application with a slightly different PE header. They don't even look at the code inside the application. They also ignore any file that is digitally signed and report it as virus.

If you can afford to digitally sign your protected application, that should be the best solution to fight against false positives. Most (widely used) antivirus trust digitally signed files and they are not reported as false positive.

In any case, if your protected application is flagged as virus, please, try the following steps:

1) Include version information in your application before compiling it (company name, version, etc) as some antivirus do not like compressed applications without version information on it

2) Change the icon of your application in case that you are using a default compiler icon, as some antivirus shows false positive detections if you leave a standard icon.
We have seen some cases where just changing a single pixel in the application icon removes a false positive.

3) Add an internal "pre-loader" to your protected application. These "pre-loaders" are available for our registered customers. Add the following option in the Advanced Options panel:

```
OPTION_ADVANCED_HEURISTIC_PRELOADER=PATH_TO_YOUR_PRELOADER_DLL
```

Protect your application. If you still have problems with false positives or want to try to decrease the number of false positives, go to step 4)

4) Add the following option in the Advanced Options panel:

```
OPTION_ADVANCED_HEURISTIC_PRETTY_NAMES=YES
OPTION_ADVANCED_HEURISTIC_FAKE_RESOURCES=YES
```

Protect your application. If you still have problems with false positives or want to try to decrease the number of false positives, go to step 5)

5) Add the following option in the Advanced Options panel:

```
OPTION_ADVANCED_HEURISTIC_ENTRY_FIRST_SECTION=YES
```

Unfortunately, there are not a specific set of options that works better for all applications. Some applications report less false positives when protecting using just one of the above options and if more options are added, more false positives are reported. Other applications require to set *all* the above options to have less false positives.

1.5.2.11 My MSVC application generates a crash dump file (.DMP) file when it crashes, so I can load and examine the crash dump file. When my application is protected the generated crash dump does not contain valid information

You have two options to match the debug information in the protected application.

- The easiest solution (but not general for all applications) is to add the following line in the Advanced Options panel:

  OPTION_ADVANCED_KEEP_DEBUG_INFO=YES

- The second solution is to use our application **minidump_patcher** to patch the DMP file and match it for the protected application. Please, contact us for more information

1.5.2.12 Is it possible to know from my application if the application has been unpacked?

Themida uses its own detections to know if your application has been partially unpacked. You can also use the macro CHECK_PROTECTION to know if your application has been unpacked.

1.5.2.13 I need to get a Vista logo. Is your protection compatible with Microsoft tests?

All our products have been tested against Application Verifier (AppVerifier.exe) with all options enabled and they are fully compatible with it.

1.5.2.14 I want to protect my .NET application with Themida, can I use an obfuscator before protecting with Themida?

Yes, you can (and it's recommended) to use a .NET obfuscator before protecting with Themida, so your assemblies will be obfuscated and protected.

1.5.2.15 How can I omit the output displayed by WinLicense when protecting via command line?

You just need to specify the "/q" command line parameter. Example:

Themida.exe /q /protect MyProject

1.5.2.16 Can you let me know which protection options affect execution speed of my application?

Default protection options should not cause an impact in the execution of your application. If your application have a very big import table (this normally happens in applications with dozens of MBs) you might notice a delay before your application is launched. Notice that the Virtual Machine settings will affect the loader speed, so your application will take more or less time to boot up. All of this is related to speed in booting up.

When your application has taken control of the CPU, it should run almost as fast as the original one (with all defaults options enabled). If you are inserting protection macros (we strongly recommend the use of VM macros) in specific functions in your application, you might notice a performance decrease if the code inside the macro is called many times per second or you have tight loops inside the VM/CodeReplace macros. If you are carefully enough and put protection macros in non critical places in your application, your protected application will have an equivalent performance as the original one.

1.5.2.17 I'm using the CHECK_CODE_INTEGRITY macro in my Delphi application but the macro always returns that my code has been modified. Any ideas?

Please, notice that some components used in Delphi/BCB, like MadExcept, makes memory patching in your code in order to hook some APIs. That patch is detected by CHECK_CODE_INTEGRITY macro, so you have to avoid using the CHECK_CODE_INTEGRITY macro if you are using one of those components that patch the code section of your application in runtime.

1.5.2.18 I see that Themida detects if my file on disk has been patched, but how can I detect if someone has patched my application in memory?

The macro CHECK_CODE_INTEGRITY checks the integrity of your application in memory (code section). You can use this macro and call it on specific places in your application.

Notice that there is a penalty in execution when calling this macro, you should avoid calling it multiple times or in places that requires a fast processing.

You can find here 46 how to use this function.

1.5.2.19 How can I insert my own splash screen using the Plugin feature?

In the Themida subfolder /ThemidaSDK/ExamplesSDK/Plugins/Examples, you can find a basic example to create a plugin.

Basically, in your `SecureEngineInitialize()` function, you display your own splash screen. When `SecureEngineFinalize()` is called, you could hide your splash screen.

1.5.2.20 Can you let me know about all available Advanced Options and what they are for?

The Advanced Options panel allows you to add very specific options that are mostly related with compatibility in specific applications.

When a customer has a compatibility problem with Themida in his application, we let him know the option that he has to include in the Advanced Options panel to fix the compatibility issue.

Please, notice that the advanced options don't offer more protection to your application, but compatibility.

We try to hide those options to our customers, because the common behavior is trying to use as many options as possible to feel more secure (when basically they will add more in-compatibilities to their applications)

If you are interested in a list of the available advanced options, please, contact us.

1.5.2.21 Some of my users complaint regarding RegMon (Filemon) loaded in memory. How to proceed?

If you enable the option "Detect File/Regstry Monitors" (in the Protection Options panel), Themida will detect common registry/file monitor tools loaded in memory. The problem with Regmon, FileMon and Process Monitor is that the driver is loaded all the time in memory even if you close the User Interface for Regmon, Filemon, etc. So, the File system and Registry are still hooked by the monitor driver until you restart the computer. Looks that the developers of those monitor tools are not unloading the driver to avoid system crashes in case that a packet request is in the middle of processing while unloading the driver. Summing up, you customer needs to restart the PC if they have launched Regmon, Filemon, etc. before launching your protected application.

1.5.2.22 If I want to sacrifice a minimal amount of security to gain the maximum amount of application startup speed, what options should I disable in Themida?

You should select a fast VM in the Virtual Machine panel, that will produce a noticeable startup speed.

1.5.2.23 Can I compress my application with UPX and then protect it with Themida?

Please, notice that Themida might not be compatible with already compressed/packed applications. Some compressors/packers make their own checksums to know if the file has been modified, in that case the application cannot be protected by Themida (or any other compressor/protector)

Another important thing to notice is that from the protection point of view, Themida works much better with unprotected (not packed) files, because it has access to the original application code/data in order to perform the protection.

Another alternative is to protect with Themida and put a compressor on top.

1.5.2.24 Is there any issue to run my protected plugins on Xp 64 (32bit mode)?

There should not be any issues under XP 64-bit. The protected DLL should be as compatible as the unprotected DLL.

1.5.2.25 My application's main function is the scientific calculation needed high performance. Is there any performace lost when I encrypt my app. with Themida?

Your protected application should run almost at the same speed as the original one. As you might know, Themida offers the chance to include protection macros (like VM, MUTATE, etc) in your application to fully virtualize the code inside the macro, where the code is emulated and never decrypted back.

You have to avoid putting those macros in critical places in your application (like code that is executed many times per second) because the execution of virtualized code is much slower than the original code. A good place to put those macros is in serial/password checking, license checks, etc.

1.5.2.26 Does Themida encrypt string constants in my code?

Themida will encrypt them but will be decrypted when your application takes control.

If you want to specifically keep encrypted some strings, you can use the macro STR_ENCRYPT 42.

1.5.2.27 If I set the Anti-Patching option, can I digitally sign my application?

Yes, the Anti-File patching option is compatible with digital certificates. After protecting your application, you can use Signtool.exe to digitally sign your protected application.

1.5.2.28 I would like to include the same protection options and custom dialogs in all my applications. Can I apply the same settings to all my applications?

Yes, to do so just save a project file with all the protection options and your customized messages. After that you just load your project file and change the name of the file to protect.

Another alternative is that you have a common project file and use it to protect different applications from the command line. Example:

```
Themida.exe /protect MyGlobalProjectFile.tmd /inputfile Applica-
tion1.exe /outputfile Application1_protected.exe
Themida.exe /protect MyGlobalProjectFile.tmd /inputfile Applica-
tion2.exe /outputfile Application2_protected.exe
```

1.5.2.29 I want to include Themida in my build system. Does Themida support command line protection?

Yes, Themida supports command line protection.

Please, refer to the section Protecting through the command line 32.

1.5.2.30 Can I protect my Windows NT system service with Themida?

Yes, Themida can detect which applications are Windows NT system services, so you can protect them just like normal applications. We have found few NT services that need to have resources not encrypted and not compressed. If you have problems protecting your NT service, please, uncheck the option "Compress and Encrypt --> Resources" (in the Protection Options panel) and protect again.

1.5.2.31 When I protect my application with Themida, the size is increased by 500Kb or more!

Themida adds protection code to keep your application fully protected against cracking. The protection code that is embedded into your application has about 500 Kb in size (depending on the protection options that you select). So, if you have a 50Kb application and our compression engine decrease it to 10Kb, the final protected application will be 10Kb + 500Kb in size. That's the reason why you see your final application with bigger size.

Suppose that you have a 4000 Kb application and the compression module compress it to 2000 Kb, the final protected application will be 2000 Kb + 500 Kb = 2500 Kb, so you can see here a decrease in the final size of your protected application.

Please, go to the "Virtual Machine" panel and select a lighter Virtual Machine (like FISH (White)) to make your protected application smaller. Depending on the selected Virtual Machine the final application size will be affected considerably. In the "Virtual Machine" panel you have some statics about the size/speed/complexity of each specific Virtual Machine.

1.5.2.32 How many KB will my application grow in size, after being protected by Themida?

It depends on the protection options that you include. The most noticeable options are in the Virtual Machine panel. You can see different types of Virtual Machines and an approximate size for each one.

1.5.2.33 When I use macros directly around some API calls I get errors in Themida saying that one of my START or END markers is missing. What's wrong?

Please, notice that macros are in fact "dummy" code that does nothing (it's just recognized by Themida). If you put the VM_END at the end of a procedure, the compiler might remove the VM_END code when optimizations are enabled. If you compile with optimizations disabled, you should not have any problems.

The following code might generate a "missing" macro pair:

```
YourFunction()
{
    VM_START
    // your code goes here
    return;
    VM_END
}
```

The compiler knows that after the "return" statement, no code is executed, so it won't generate code for the VM_END marker. To avoid the above problem, just put it like:

```
YourFunction()
{
    VM_START
    // your code goes here
    VM_END
    return;
}
```

Also, you might want to disable optimizations in those places where macros are used, to make sure that compiler optimizations won't remove any macro markers. For C/C++ language you can use the following directive:

```
#pragma optimize("", off)
YourFunction()
{
    VM_START
    // your code goes here
    return;
    VM_END
}
#pragma optimize("", on)
```

You should be able to use the same approach for other programming languages.

1.5.2.34 Please let us know how Themida influences the program performance? What would you advice us to pay attention to in order to minimize the performance losses? Will it affect the protection?

As you might know, you can use macros (like VM, MUTATE...) to protect more the sensitive code in your application. Those macros are executed much slower than the real code (but they are highly recommended to put much protection in your application). So, you have to make sure that you don't put those macros in critical code in your application (that is executed many times per second). A good place to put those macros is in code that checks for serial, passwords or other routines that are not executed constantly.

1.5.2.35 If I use the option "Entry Point Virtualization", my DLL crashes. If I uncheck that option, will it make it easier to crack?

Please, notice that Entry Point Virtualization is not compatible with some applications (specially with some compilers). When you virtualize your Entry Point, it will be destroyed and emulated somewhere else in the protection memory. Some compilers, jump at a later point in the middle of the Entry Point code, so as it's virtualized it will execute invalid opcodes and will produce a crash in the protected application. In that case, you have to protect your application unchecking the option "Entry Point Virtualization".

Notice that Entry Point Virtualization has the same effect as putting a VM macro in the beginning of your main function. So, you can just use VM macros in several parts of your application and you will keep a high level of protection inside your application.

1.5.2.36 Can I protect my .NET applications with Themida?

Yes, .NET applications (EXE) can be protected with Themida. Please, notice that our .NET protection is not as strong as the native protection, due to the nature of the .NET interpreted language and also our protection macros (VM, MUTATE, etc.) are not available for .NET

Notice that .NET DLLs cannot be protected with Themida.

1.5.2.37 I'm happy with all the protection features offered by Themida, but I miss the trial/licensing features. Will they be included?

Themida is just a software protector and will not include Trial/Licensing features. If you need Trial/Licensing features in conjunction with a really strong software protection, we have developed a specific product for that.

Please refer to https://www.oreans.com/WinLicense.php to get more information about WinLicense.

1.5.2.38 Can I get the computer Hardware ID with Themida?

Unfortunately, that functionality is out of scope for Themida. Our product WinLicense allows you to get the computer Hardware ID and create hardware locked licenses.

Basically, WinLicense is the same as Themida plus Trial/Registration functions.

1.5.2.39 Can I protect mixed managed/unmanaged DLLs?

We have done several tests on mixed managed/unmanaged DLLs and they can be protected. If you have problems with your mixed managed/unmanaged DLL, let us know so we can work on it.

1.5.2.40 When I enable the "Advanced API-Wrapping" option my applications runs slower

The Advanced API-Wrapping options has a very small penalty in execution, but it should not be noticeable in most applications. For your case, it seems that a specific API is called massively per second and you might notice a performance decrease. We have a special tool to detect which API is called massively so you can continue using the "Advanced API-Wrapping" option and just skip that specific API from wrapping (using the Advanced Options 30 panel). Please, contact us for more information at support@oreans.com

1.5.2.41 When my STR_ENCRYPT macros are processed in the last "Protection" panel, I can see "skipped" when the macro is processed. What can I do?

When the STR_ENCRYPT is "skipped" it is because there are not strings found inside the STR_ENCRYPT macro markers (START - END). If you are sure that there are strings inside the macro markers, you might be using UNICODE strings in your source code but you are using the ANSI macro "STR_ENCRYPT" instead of the UNICODE version of the macro "STR_ENCRYPTW".

You can go to the "Virtual Machine" panel and click on your STR_ENCRYPT/W macros and you will see in the lower panel the strings found inside the STR_ENCRYPT macro markers, so you can make sure that your strings are recognized by the protection.

1.5.2.42 When I protect my application with an older version, the size of the protected application is smaller. Can I keep the same size in latest version?

We try to change our protection from version to version and sometimes we add more complexity to the current internal protection, making the protected application bigger.

You can go to the "Virtual Machine" panel and select a lighter/smaller VM, like VM_FISH_WHITE. You can also change the internal compressor engine to use one with better compression ratio. Please, contact us at support@oreans.com to know how to change the internal compression engine.

1.5.2.43 When I add a JPG image in the splash option, my image is not displayed on startup

Make sure that your JPG image uses the RGB color mode. JPG images with CMYK color mode are not supported yet.

1.5.3 Macros

- I have a function with a VM_START/END. Inside the START - END macro markers, I call an external function, called "Function2()". Is that external "Function2()" also virtualized? 72
- I have put a VM macro in my "main()" function. Inside the VM_START/END markers I'm calling several functions. Are those called functions also virtualized? 72
- I have a few Portuguese strings in my STR_ENCRYPT macro but some of them are not recognize when I click on the STR_ENCRYPT macro in the "Protection Macros" panel. What's wrong? 73
- Can I use one protection macro (VM macro) inside another macro (VM macro)? 73
- In the "custom_vms" folder I can see the name of the available virtual machines. Can I change the internal settings inside each ".vm" file? 74
- Can I raise an exception inside a VM macro? 74
- I have seen that insertion of VM macros in try-except clauses are a bit tricky. What about try-finally clauses? 74
- Can Themida macros protect switch statements and try-except clauses? 75
- If I protect the following code with a macro: VM_START InitializeCounters(i); VM_END. Will the InitializeCounters() function code also virtualized? 76
- I have included several VM macros inside my application. I have made sure that I have not nested any macros, but when I load my application in Themida user interface, I get a nested macros message. What's wrong? 76
- We tried to adopt Themida VM macro option. But, our particular problem was performance of the game. It was very critical issue. We hope to know how we improve performance of my game. 77
- Can VM macros protect switch statements? We are now having an issue with VM macros crashing the application. 78
- Where are the ENCODE/CLEAR macros that were available in version 2.x? 78
- When I compile my Delphi application in 64-bit, the compiler says that the "asm instruction is not valid" in my VM macros 78

- I'm using a VM macro but it fails when using it on my Delphi application. I get an exception. Can you fix it? 79
- What does it mean that my encrypted string are not removed from the original location? 79
- In VS2017 and VS2019 the debugger is not tracing correctly my function that uses a VM_START/END marker 80
- When enabling optimizations, my VM_END marker is not found 80
- I'm using the STR_ENCRYPT but sometimes, when my string contains specific German characters the string is not recognized 81

1.5.3.1 I have a function with a VM_START/END. Inside the START - END macro markers, I call an external function, called "Function2()". Is that external "Function2()" also virtualized?

No. In that case, you will virtualize the calling convention for Function2() but not the code inside Function2(). Example:

```
void MyMainFunction()
{
   VM_START
      // some code
      Function2(1, 2, 3)
      // some code
   VM_END
}
```

In the above example, all the code inside the START - END markers is virtualized. The calling convention (passing parameters) for Function2() is also virtualized, but not the code inside "Function2()". If you also want to virtualize the code inside Function2(), you will have to put *another* macro inside Function2(). Example:

```
void Function2(param1, param2, param3)
{
    VM_START
    // some code
    VM_END
}
```

1.5.3.2 I have put a VM macro in my "main()" function. Inside the VM_START/END markers I'm calling several functions. Are those called functions also virtualized?

Suppose the following example:

```
int main(void)
{
    VM_START
```

```
    MyFunction1();
    MyFunction2();

    return 0;

    VM_END
}
```

?
In the above example you are protecting the code inside the "main()" function but not the code inside "Function1()" and "Function2()".

If you want to protect/virtualize also the code inside "Function1()" and "Function2()" you need to put another VM macros inside "Function1()" and another VM macro inside "Function2()"

1.5.3.3 I have a few Portuguese strings in my STR_ENCRYPT macro but some of them are not recognize when I click on the STR_ENCRYPT macro in the "Protection Macros" panel. What's wrong?

Themida searches for printable chars to be able to determine if a pointer to "something" is a string or not. As your string might contain special Portuguese characters the internal function to determine if a specific char is printable might fail.

You can change the current locale, so Themida will be able to find your Portuguese string.

1) Edit your Themida.ini file and add under the **[General]** section add the following entry:

StrEncryptLocale = Portuguese

2) Restart Themida and go to the "Protection Macros" panel and click on your STR_ENCRYPT macro and make sure that your Portuguese strings can now be recognized

You can change the "StrEncryptLocale" entry for a different language, like "Russian", "Spanish", etc.

1.5.3.4 Can I use one protection macro (VM macro) inside another macro (VM macro)?

You cannot nest VM macros. The following is incorrect:

```
void MyFunction()
{
   VM_START

    // your code

    VM_START    // <-- NESTED!!!!

      // your code
```

```
    VM_END

  VM_END
}
```

There is an exception for nested macros inside VM macros. You can put STR_ENCRYPT_START/END macros inside VM macros and you can also include "single marker" macros inside VM macros (like CHECK_CODE_INTEGRITY, CHECK_PROTECTION, ...)

1.5.3.5 In the "custom_vms" folder I can see the name of the available virtual machines. Can I change the internal settings inside each ".vm" file?

We have inserted an internal CRC to avoid people changing the settings inside the .vm files. We normally deliver 3 files for each specific VM architecture. For example, the TIGER architecture contains: "Tiger white", "Tiger red" and "Tiger Black".

The "white" edition decreases the protection but increases the speed in execution.

The "red" edition is balanced between protection and speed.

The "black" edition offers more security but decreases the speed in execution.

Basically, you don't need to edit the .vm files because you normally have those files ready (for better speed or protection) in the "white, red and black" editions. If you change those settings by yourself, you could create a VM with very low protection, which is not recommended, or a VM highly complex but with very low performance (and really big in size)

Anyway, if for a special reason you need to change the VM internal settings we can let you know how to proceed.

1.5.3.6 Can I raise an exception inside a VM macro?

Yes, raising an exception is possible from VM macros.

1.5.3.7 I have seen that insertion of VM macros in try-except clauses are a bit tricky. What about try-finally clauses?

You have to insert VM macros in try-finally clauses in the same was as you do for try-except. Example:

```
try
{

    VM_START

    // your code

    VM_END
```

```
}

finally

{

    VM_START

    // your code

    VM_END

}
```

1.5.3.8 Can Themida macros protect switch statements and try-except clauses?

Switch-Case statements and try-except clauses cannot work with Themida macros in most compilers.

Compilers generate a direct jump table in the data section which directly jumps to each "case" statement. When the code is virtualized, the jump goes into a virtualized (garbage) code and it produces exception. You can use a workaround to protect your switch-case statements with Themida macros, like:

```
switch (var)
{

    case 0:

    VM_START

    // your code

    VM_END

    case 1:

    VM_START

    // your code

    VM_END

    ...

}
```

For try-except clauses:

```
try
{
    VM_START

     // your code

     VM_END

}

except
{

     VM_START

     // your code

     VM_END

}
```

1.5.3.9 If I protect the following code with a macro: VM_START InitializeCounters(i); VM_END. Will the InitializeCounters() function code also virtualized?

No, in your example, you are just virtualizing the code which puts the parameters in the stack and call your function. But the function "InitializeCounters" itself is not virtualized. You have to put a new VM macro inside the function "InitializeCounters" if you want to virtualize it.

1.5.3.10 I have included several VM macros inside my application. I have made sure that I have not nested any macros, but when I load my application in Themida user interface, I get a nested macros message. What's wrong?

If you have not inserted nested macros and you get that message, you might be facing a compiler optimizations issue. Some compilers remove the VM_END marker when they are at the end of a procedure (or after a "return" statement) because the VM markers are in fact dummy code that might be affected by compiler optimizations.

Please, make sure that you avoid putting the VM_END marker after a "return" statement or as the last instruction in a function/procedure.

You can also disable local optimizations. In C/C++, you can disable local optimizations. Example:

```
#pragma optimize("", off)

void MyFunction(void)
{
    VM_START

    // your code
```

```
    VM_END
}

#pragma optimize("", on)
```

1.5.3.11 We tried to adopt Themida VM macro option. But, our particular problem was performance of the game. It was very critical issue. We hope to know how we improve performance of my game.

Please, notice that when you protect an area of code in a function with a VM or CodeReplace macro, the code is converted into a highly complex and unique opcodes. Those macros are executed under a specific VM (which is included inside your protected application) that is able to understand the virtualized code. Execution of code inside the Virtual Machine is much slower than the original code.

Summing up, you have to avoid putting macros in the following cases:

1) Functions which are called many times per second

2) Functions which has tight loops ("for", "while", "do-while") which iterate multiple times

3) Critical code in your application. That is, code that must be executed as soon as possible

A real example could be the case that you want to protect a function, but it has a tight loop, so, you just have to put the loop outside of the macro.

Example:

```
void MyFunction( )
{
    VM_START

    // your code goes here

    VM_END

    for(i = 0; i < 0x100000; i++)
    {
        // your code
    }

    VM_START

    // your code goes here

    VM_END
}
```

1.5.3.12 Can VM macros protect switch statements? We are now having an issue with VM macros crashing the application.

Switch-Case statements cannot work with VM macros in most compilers.

Compilers generate a direct jump table in the data section which directly jumps to each "case" statement. When the code is virtualized, the jump goes into a virtualized (garbage) code and it produces exception. You can use a workaround to protect your switch-case statements with VM macros, like:

```
switch (var)
{
    case 0:

    VM_START

    // your code

    VM_END

    case 1:

    VM_START

    // your code

    VM_END

    ...
}
```

1.5.3.13 Where are the ENCODE/CLEAR macros that were available in version 2.x?

We removed the ENCODE/CLEAR macros as they were not strong enough compared to our virtualization macros. The ENCODE/CLEAR macros got their strength in older versions when our protection was using Ring-0 code. We later removed the Ring-0 protection and added our protection virtual machines, so our most powerful protection macros are the VM macros (VM_TIGER_WHITE, VM_FISH_RED, etc.). We encourage our customers to change their ENCODE/CLEAR macros with our newest VM macros to keep a good level of protection.

1.5.3.14 When I compile my Delphi application in 64-bit, the compiler says that the "asm instruction is not valid" in my VM macros

In order to use the protection macros (like VM macros) when compiling a 64-bit Delphi application, you have to insert the macros via "Function names" instead of "inline assembly". Please, refer to the example in the subfolder in the "`ThemidaSDK/ExamplesSDK\Macros\Delphi\Via Functions`"

1.5.3.15 I'm using a VM macro but it fails when using it on my Delphi application. I get an exception. Can you fix it?

You can try the following which might fix your issue:

1) Go to the Advanced Options 30 panel and add the following option:

```
OPTION_MACROS_SEH_SUPPORT=YES
```

2) Protect again

If you still have problems, please, check that you have not inserted any of the current macro restrictions. Please, check the following KB entry 75.

1.5.3.16 What does it mean that my encrypted string are not removed from the original location?

When a string is referenced from inside a STR_ENCRYPT macro or from a VM macro (when using the option Encrypt Strings in VM macros 7), the protection redirects the pointer to the string to a location inside the protection code and copy the string in that location (in an encrypted form). As the original location of the string is not referenced after being protected, the original string is patched with zero values.

In some cases, the same string is also used in a different location in your application code and due to compiler optimizations, the string is only stored once.

Show Example

```
LRESULT CALLBACK MainHandler(HWND hDlg, UINT message, WPARAM wParam, LPARAM
lParam)
{
   switch (message)
   {
   case WM_INITDIALOG:

      STR_ENCRYPT_START

      printf("Hello World");    // "Hello World" string found and redirected the
pointer inside "printf"

      return TRUE;

      STR_ENCRYPT_END

      break;

    case WM_COMMAND:

      printf("Hello World");   // The "Hello World" string is referenced here
again, from outside a STR_ENCRYPT marker

      break;
   }
```

```
    return FALSE;
}
```

In the above example, as the "Hello World" string is also referenced from another location (outside of a STR_ENCRYPT marker) the protection cannot remove the original string "Hello World" from its original location, as it will be later referenced by a different code. In this case, there is an encrypted "Hello World" string that is referenced by the code inside the STR_ENCRYPT marker and an unencrypted "Hello World" that is used in a different code location.

In some cases, you only use a specific string one time inside the STR_ENCRYPT marker, but the string is not removed. The reasons could be:

- Your compiler is creating a pointer to the string in a different location in your application. Probably the linker is using a table of symbols that contains the pointer to all your strings
- There is a special code or data sequence in your application code that matches exactly an offset to the original string. In this case, this is not a real access to the string, it was just a coincidence that a specific code sequence matched the pointer to the string

If you are sure that there are no more access to the specific string (or to overcome the two above situations), you can go to the Advanced Options 30 panel and add the following option:

OPTION_MACROS_ENCRYPT_STRINGS_FORCE_DESTROY=YES

1.5.3.17 In VS2017 and VS2019 the debugger is not tracing correctly my function that uses a VM_START/END marker

We have contacted Microsoft about this and there is a bug on Visual Studio where the debugger incorrectly traces over a code with "inline code" (like our START - END macro markers). The bug is not present on Visual Studio 2015 and it should be fixed in a new release of Visual Studio.

Meanwhile, you can also use other type of insertion for the protection macros, you could try using the ASM module method, as described in the subfolder "\Examples\C\VC (via ASM module)"

1.5.3.18 When enabling optimizations, my VM_END marker is not found

This can be an issue with Tail Call Optimization.

To avoid the issue with the "missing END" marker due to Tail Call Optimization, please, just put an intrinsic __nop() after the END macro marker. You could also edit the definition of the

END marker (or create your own wrapper for it) where you add at the end the "__nop();" instruction. Example:

```
VM_START;

MessageBoxW(0, L"Hello world!", 0, 0);

VM_END;

__nop();   // prevent TCO in this function
```

1.5.3.19 I'm using the STR_ENCRYPT but sometimes, when my string contains specific German characters the string is not recognized

We use the C function "isprint()" to determine if a char is valid. We have an external option to change the locale, so "isprint()" behaves differently (using "_wsetlocale()").

Please, edit the Themida.ini file and add the following line under the "[General]" tab:

```
StrEncryptLocale=de-DE
```

You can use different srtings admitted by _wsetlocale for other specific languages

1.5.4 XBundler

- Can I specify via the command line a file which contains all files that will be embedded in XBundler? 83
- I'm trying to embed a config file in XBundler (using "Never Extract to disk"option) and I want to modify that file in runtime, is that possible? 83
- I'm using the option "Extract to disk" for several files that I'm bundling with XBundler. The files are extracted correctly under Windows XP but it fails under Vista and Windows 7. What's happening? 84
- I want to bundle my OCX in XBundler but not sure if it will work as my OCX needs to be registered in the system via regsvr32.exe 84
- I want to XBundle my files but with relative paths to parent folders, so can I move my projects and files across computers and protect them from there? 85
- If I bundle some large graphics files and DLLs, is that going to influence the performance of my program? 85

- I want to protect a DLL and bundle some data files using XBundler, but it does not work. 85
- Can I copy to disk a DLL that I have embedded with the option "Never Write to disk" 85
- In my .NET application (test.exe) I want to to embed my .exe.config file (test.exe.config) with XBundler, but when I run my protected application (without the .config file) it does not see my embedded test.exe.config file. 85
- Can I embed several EXE files inside XBundler and run them from memory, that is, without writing them to disk? 86
- What about performance? I'm writing a filemanager which has a lot of access to local files. 86
- How are the files accessed from inside the protected application? May I call simply memo.lines.loadfromfile for example? If yes - does this mean that all accesses to files are filtered by XBundler? 86
- Can XBundler be used to bundle all of the DLL's and OCX's inside a protected DLL? Does there need to be an actual executable? 86
- Is it possible to use XBundler to bundle a console exe that I call run-time from my application? 86
- Can I register my bundled DLLs with regsvr32.exe? 87
- I tried to bundle CHM file. Command which I use to open CHM file in my application below: ShellExecute(Application.Handle,'open','help.chm',nil,nil,SW_SHOWNORMAL); 87
- We are using a couple of DLLS and OCXS in our application, and I have tried unsuccessfully to use them with the XBundler plugin I bought - whats the best way for us to move forward and maybe run some tests to see if we can get this functionality working? 87
- I want to bundle my Visual Studio 2005 (or Visual Studio 2008) DLLs with XBundler but it fails to load them. Is that a known issue? 88
- I have inserted about 100 files to bundle. I want to select all of them and set for all of them "Extract always". Is that possible to do it without going one file at a time? 88

- I have bundled several INI files with XBundler but when I try to access to them, they cannot be found. Other bundled files are working fine 88

1.5.4.1 Can I specify via the command line a file which contains all files that will be embedded in XBundler?

The XBundler files are specified in your themida project file. You can directly modify the project file to set your files to bundle.

Another option is to specify a separate file in the "Advanced Options" panel that will contain the list of files to bundle. For example, you can add the following line in the "Advanced Options" panel if you want to have a separate options file (let's call it "ExternalOptions.txt"):

```
OPTION_ADVANCED_EXTERNAL_PROJECT_OPTIONS=%THEMIDA_FOLDER%\ExternalOp-
tions.txt
```

In your external options file, you specify the list of files to bundle.

```
OPTION_XBUNDLER_NUMBER_FILES=2

OPTION_XBUNDLER_FILE_NAME_AT_0=%INPUT_FILE_FOLDER%\MyFile.txt
OPTION_XBUNDLER_FILE_TYPE_AT_0=EXTRACT_NEVER
OPTION_XBUNDLER_FILE_VIRTUAL_PATH_AT_0=%APP_FOLDER%\MyFile.txt

OPTION_XBUNDLER_FILE_NAME_AT_1=%INPUT_FILE_FOLDER%\MyDll.dll
OPTION_XBUNDLER_FILE_TYPE_AT_1=EXTRACT_NEVER
OPTION_XBUNDLER_FILE_VIRTUAL_PATH_AT_1=%APP_FOLDER%\MyDll.dll
```

You can use any of the predefined constants to specify the path where the file to bundled is located, instead of using full paths, so you can easily move your project files and bundled files across different computers. You can refer to Special Constants in Input/Output file names 5.

1.5.4.2 I'm trying to embed a config file in XBundler (using "Never Extract to disk"option) and I want to modify that file in runtime, is that possible?

Please, notice that all embedded files in XBundler (with option "Never Extract to disk") are handled as read-only files, so you cannot modify them in runtime. If you want to modify a file that you are bundling, you have to select an extraction option for that file (instead of "Never Extract to disk"). For your specific scenario, where you want to write to an embedded file, you should set the option "Write if file not present" in the XBundler panel for that config file.

1.5.4.3 I'm using the option "Extract to disk" for several files that I'm bundling with XBundler. The files are extracted correctly under Windows XP but it fails under Vista and Windows 7. What's happening?

It seems that the problem is that the file cannot be created under Vista/Windows 7 due to UAC restrictions, which might be denying file creation if your application is not launched with an administrator manifest.

You have two options:

1) In the Extra Options panel 28, "Add a manifest from File" to run as administrator. This will force your application to be launched with admin's rights.

2) Go to the XBundler panel and right click on the XBundler files panel. Select the option "Add Root Folder --> USER_DOCS" (or any other special folder from the list). After that you can create a subfolder inside the added root folder. Example:

```
--> %USER_DOCS%
  |--> My Folder
     |--> File1.txt
     |--> File2.txt
```

The defined "Root Folders" are:

- APP_FOLDER: Folder where the protected application is located
- WIN_FOLDER: Windows folder (i.e: C:\Windows)
- WINSYS_FOLDER: Windows system folder (i.e: C:\Windows\System32)
- USER_DOCS: Current user documents folder
- LOCAL_APP_DATA: Local application data for the current user
- COMMON_APP_DATA: Common application data for all users
- TEMP_FOLDER: User temporal folder

1.5.4.4 I want to bundle my OCX in XBundler but not sure if it will work as my OCX needs to be registered in the system via regsvr32.exe

Latest versions of Themida supports ActiveX support in XBundler. You just need to go to the XBundler panel, add your desired OCX/DLLs, select the option "ActiveX Support" and protect your application

1.5.4.5 I want to XBundle my files but with relative paths to parent folders, so can I move my projects and files across computers and protect them from there?

In the XBundler panel, you can use specific constants to specify the location of the files to bundle. Please, refer to the "Original File Location" help section.

1.5.4.6 If I bundle some large graphics files and DLLs, is that going to influence the performance of my program?

Notice that everything that you embed with XBundler is encrypted all the time till it's required by your application. That is, if you load/unload your DLL or you open/close your graphic files, it will be decrypted and encrypted back. So, you could see some performance decrease if they are large files/DLLs and if they are opened and closed many times.

If you want to speed the above process, you can select the option "Maximize speed" in the XBundler panel.

1.5.4.7 I want to protect a DLL and bundle some data files using XBundler, but it does not work.

If you are having problems with embedded DLL, you can check the option "Exception Support in DLLs" in the XBundler panel.

1.5.4.8 Can I copy to disk a DLL that I have embedded with the option "Never Write to disk"

You can treat an embedded file exactly like if it were present on disk. If you want to extract a bundled file at any time, you can use for example the Windows API "CopyFile" and the embedded file will be copied to disk.

1.5.4.9 In my .NET application (test.exe) I want to to embed my .exe.config file (test.exe.config) with XBundler, but when I run my protected application (without the .config file) it does not see my embedded test.exe.config file.

Embedding .exe.config files in .NET applications is a bit tricky for some applications. You have to embed your original "test.exe.config" file with XBundler (option "Never extract to disk") but you have to ship your protected application with a "fake" or dummy "test.exe.config" file. This is because Windows checks the presence of a .config file before your application is launched. When your application reads information from the .config file, it will read it from the embedded one and not from the fake/dummy .config file. An example of a dummy .config file could be:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>

</configuration>
```

1.5.4.10 Can I embed several EXE files inside XBundler and run them from memory, that is, without writing them to disk?

Sorry but execution from memory (without writing to disk) only works with DLLs and data files. Injection of application can only be done if you mark the option "extract to disk" for the .EXE file in the XBundler panel.

1.5.4.11 What about performance? I'm writing a filemanager which has a lot of access to local files.

All embedded files are encrypted inside the protected executable. When the file handle is closed, the file is encrypted again. Please, notice that opening and closing a file multiple times will make the whole process slower due to decryption/encryption.

In that case, we recommend that you protect checking the option "Maximize Speed" in the XBundler panel 19.

1.5.4.12 How are the files accessed from inside the protected application? May I call simply memo.lines.loadfromfile for example? If yes - does this mean that all accesses to files are filtered by XBundler?

Notice that accessing to bundled files should be TOTALLY transparent for you. XBundler must know how to handle all different ways to access to a file (even like "memo.lines.loadfromfile"). In case that you have compatibility problems with XBundler and your application, we are happy to work on it to fix your problem.

1.5.4.13 Can XBundler be used to bundle all of the DLL's and OCX's inside a protected DLL? Does there need to be an actual executable?

XBundler is mainly designed to operate from a protected EXE. So, you bundle all your DLLs to your EXE applications. Anyway, we added support to embed DLLs inside a protected DLL (like your scenario) but it could fail in some situations as reported from a customer (depending on the target application that use your DLL). For other customers, it works fine embedding DLLs inside a main DLL.

The best thing is that you try our DEMO version of Themida and see how XBundler goes with your scenario. For ActiveX protected DLLs, you might need to disable the option "Compress resources and encrypt resources" as Windows cannot register some DLLs when the resource section is compressed.

Anyway, if it does not work for you, it would be great if you can send us the test DLLs to re-produce the problem here, so we could add support for it.

1.5.4.14 Is it possible to use XBundler to bundle a console exe that I call run-time from my application?

Sorry but XBundler only works with DLLs and data files.

You can embed the console application inside XBundler and mark the option “extract to disk”, but you might not want that as the console application will be written to disk and viewable by your customers.

Data files and DLL can be embedded inside the protected application and can be used without writing them to disk.

1.5.4.15 Can I register my bundled DLLs with regsvr32.exe?

Sorry but bundled DLLs cannot be registered via "regsvr32.exe". Bundled DLLs are only visible for the protected application. As you can see, "regsvr32.exe" is an external process and won't be able to see the bundled DLLs.

Please, go to the XBundler panel 19, check the option "ActiveX support" and protect again. Your embedded DLLs will be correctly registered from the protected application. Notice that your application must be running with admin's rights the first time that is executed, so the registration of the bundled DLLs can be performed. You can add an admin manifest from the Extra Options panel 28.

1.5.4.16 I tried to bundle CHM file. Command which I use to open CHM file in my application below: ShellExecute(Application.Handle,'open','help.chm',nil,nil,SW_SHOWNOR MAL);

Sorry, but ShellExecute calls are not supported by XBundler. ShellExecute creates an external process and the embedded files in XBundler are only visible by the protected application, so the called process from ShellExecute cannot see the help file.

You need to call the Help file directly from your application (no using ShellExecute). Most programming languages have facilities to do that.

Please, notice that some programming languages open the Help file via FindFirstFile API, so, you need to enable the option "Hook FindFirst/Next File APIs" in the XBundler panel 19.

1.5.4.17 We are using a couple of DLLS and OCXS in our application, and I have tried unsuccessfully to use them with the XBundler plugin I bought - whats the best way for us to move forward and maybe run some tests to see if we can get this functionality working?

If your DLL links with the Microsoft runtime libraries (MSVCRxx.dll), you could make a static linking with those libraries using the linking switch /MT (More information can be found at: http://msdn2.microsoft.com/en-us/library/abx4dbyh(VS.80).aspx) After that, compile again and it should work correctly with XBundler. Another solution is to check the option "Add Manifest from XBundler files" in the Extra Options 28 panel.

If the problem persists, it will be great if you send us your application and the DLLs that you plan to bundle which cause the problem, so we can reproduce the problem here. If you cannot send the unprotected application, it will be great also if you send us any test application that we can use to reproduce your problem.

1.5.4.18 I want to bundle my Visual Studio 2005 (or Visual Studio 2008) DLLs with XBundler but it fails to load them. Is that a known issue?

If your DLL is linking with the MSVC runtime libraries (MSVCR80 or MSVCR90), please go to the Extra Options 28 panel and check the option "Add Manifest from XBundler files".

1.5.4.19 I have inserted about 100 files to bundle. I want to select all of them and set for all of them "Extract always". Is that possible to do it without going one file at a time?

Yes, you can change the Extraction Mode for all selected files:

1) Select all the wanted files

2) Press:

- CTRL + 0 = "Never Write to disk"
- CTRL + 1 = "Extract always"
- CTRL + 2 = "Extract if not exists"
- CTRL + 3 = "Extract if older exists"
- CTRL + 4 = "Extract if different exists"

1.5.4.20 I have bundled several INI files with XBundler but when I try to access to them, they cannot be found. Other bundled files are working fine

If you are bundling INI files with the option "Never write to disk" you should check the option "Hook GetPrivateProfile APIs" and protect again.

1.5.5 Sales

- Can you tell me about how Themida subscriptions work? 89
- I have paid via Shareit but you have not sent me any invoice. Can you send it, please? 89
- I have paid via Fastspring but you have not sent me any invoice. Can you send it, please? 89
- If we purchase your software via Bank wire transfer, will you provide our company with an invoice for our purchasing? 89

- Does initial purchase include some degree of update support, or must I purchase the update subscription at the outset to get updates during the first year (or whatever period)? 90
- I paid to Shareit via bank wire transfer, why I have not received your software yet? 90
- As soon as the free update period (12 months initially) expires, I will need to renew Themida subscription. Do I have to pay the renewal fee before it expires or is it possible to pay somehow later (if I happen to forget)? 90
- What is the difference between "Developer License" and "Company License"? 90
- Suppose I will be the only one developer in our company who will use Themida, do I need to purchase Company license or will Single developer license be enough? 91

1.5.5.1 Can you tell me about how Themida subscriptions work?

When you purchase Themida, you will have 12 months of free upgrades and technical support. In order to keep our projects alive and up dated we require a small amount of capital to keep producing the updated versions. When your original subscription expires all you have to do is purchase a new subscription.

We have 2 types of subscriptions: 12 months subscription or 6 months subscription. Please, check Prices and subscriptions for more details (http://www.oreans.com/order.php)

1.5.5.2 I have paid via Shareit but you have not sent me any invoice. Can you send it, please?

Please, notice that Shareit changed the way that orders are processed. When you purchase a product from us, Shareit is the one that purchases the product from us and sells it to you (that is, you are purchasing the product to Shareit and not to us) So, Shareit is the one that emits a valid invoice for you.

1.5.5.3 I have paid via Fastspring but you have not sent me any invoice. Can you send it, please?

Please, notice that when you purchase a product from us, FastSpring is the one that purchases the product from us and sells it to you (that is, you are purchasing the product to FastSpring and not to us) So, FastSpring is the one that emits a valid invoice for you.

1.5.5.4 If we purchase your software via Bank wire transfer, will you provide our company with an invoice for our purchasing?

Sure, just let us know your company details that you want to appear in the invoice and VAT ID for European Union countries and we will send you a valid invoice for your purchasing (in PDF format)

1.5.5.5 Does initial purchase include some degree of update support, or must I purchase the update subscription at the outset to get updates during the first year (or whatever period)?

When you purchase any of our products, you have 12 months of free updates and technical support. After that period, you need to get a subscription plan to keep receiving updates and technical support. Of course, you can continue using our products even if your subscription period expires (though you won't be able to receive new updates of our software until you purchase a new subscription plan)

1.5.5.6 I paid to Shareit via bank wire transfer, why I have not received your software yet?

You have paid via bank wire transfer to Shareit. In that case, Shareit is the one that collects the money and send us the notification when everything is processed. So, you will receive your license as soon as we get the Shareit notification email.

This take about 4-5 business days to process by Shareit. You might want to contact Shareit for detailed information about the status of your transfer.

If after 5 days you have not receive any news from us, that means that Shareit has not made any notification to us about your payment. Please, let us know your Shareit order number and we will contact Shareit directly for further information about your oder.

1.5.5.7 As soon as the free update period (12 months initially) expires, I will need to renew Themida subscription. Do I have to pay the renewal fee before it expires or is it possible to pay somehow later (if I happen to forget)?

You can renew it at any time, even if your free update period expired for several months. When you purchase the subscription plan, it will start again the day that you purchase the subscription plan.

1.5.5.8 What is the difference between "Developer License" and "Company License"?

Company licenses are for companies with more than one software developer. All developers in the company can use the license to protect all the software developed within the company.

The single **Developer License** is intended to be used for single developers or companies with **just one software developer**. If there is more that one software developer, then you need to purchase a company license.

If you purchase the "Developer License", you can protect all your projects with your license. Notice that **you cannot protect projects which are not developed by you**.

The same is applied to "Company Licenses". That is, the company license can be used by any employee inside the company, but they can **only** protect software developed **inside** the company where the license belongs.

The company license is suitable for a company inside a region (country), but not for overseas offices.

1.5.5.9 Suppose I will be the only one developer in our company who will use Themida, do I need to purchase Company license or will Single developer license be enough?

Company licenses are for companies with more than one software developer. If you are the only developer in your company or registered as one-man company, you just need to get the "Single Developer" license.

1.6 Support

If you have any technical problems using Themida or need a special feature to be included in a next release, please feel free to contact us at support@oreans.com.