Trend Micro
Case Diagnostic Tool 2.0
Getting Started Guide

Release Date: July 2007

Table of Contents

Introducing the Case Diagnostic Tool

The Trend Micro Case Diagnostic Tool (CDT) helps the Trend Micro Service Engineering Group, Core Team, Technical Support Team, and customers diagnose problems in Trend Micro products.

What does the Case Diagnostic Tool do?

The Case Diagnostic Tool collects debugging information from your computer for troubleshooting problems. The Case Diagnostic Tool offers the following features:

- Supports multiple product diagnostics, automatically collects relevant system information from your computer
- Allows you to enter your own description of the problem
- Automatically enables and disables your software's debugging mode and collects necessary data based on the type of problem encountered
- Monitors the status of specific processes like CPU load and memory usage
- Automatically retrieves and compresses files that are related to the problem into a ZIP file (The password for the ZIP file is "trend")

On what platforms can the Case Diagnostic Tool run?

- Red Hat Linux 7.3 ~ 9.0
- Red Hat Enterprise Linux 2.1 ~ 3
- Solaris 8 ~ 9

Using the Case Diagnostic Tool

Case Diagnostic Tool File List

- cdt
- cdt.ini
- libcdtcore.so
- libcdtcommon.so
- libstdc++-libc6.2-2.so.3 (For Linux platform use)
- ExInterface*.ini
- ExInterface*.so

Working with the Case Diagnostic Tool

Decompress the Case Diagnostic Tool zip file and execute the `cdt` file. The application then leads you through the diagnostic process.

Welcome to the Trend Micro Case Diagnostic Tool

When you run `cdt`, the Case Diagnostic Tool welcome screen opens first. When you have finished reading the introduction, press the space bar or the <Enter> key to open the next screen.

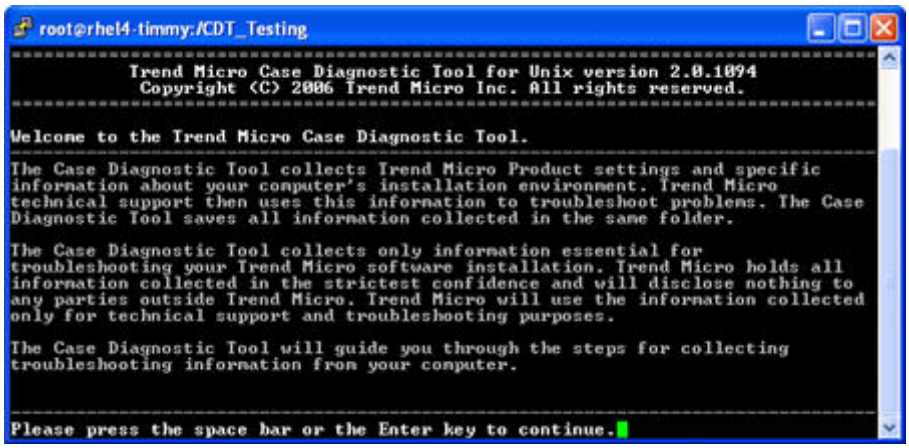

Figure 1: Welcome screen

Trend Micro License Agreement

You must accept the legal agreement to use the software. If you do not accept the legal agreement, the Case Diagnostic Tool automatically closes. Press the <Y> key to go to the next screen, or press the <N> key to exit.

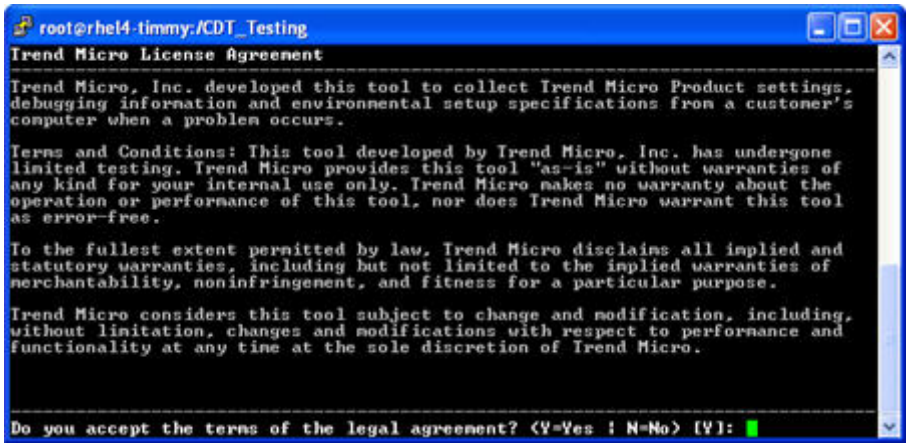

Figure 2: License Agreement screen

Choose the Product to Diagnose

The Case Diagnostic Tool checks if you have any Trend Micro software installed. If CDT finds any Trend Micro Software installed on your computer, it lists it on this screen. Select at least one item to diagnose, or press the <ESC> key to collect only basic system information.

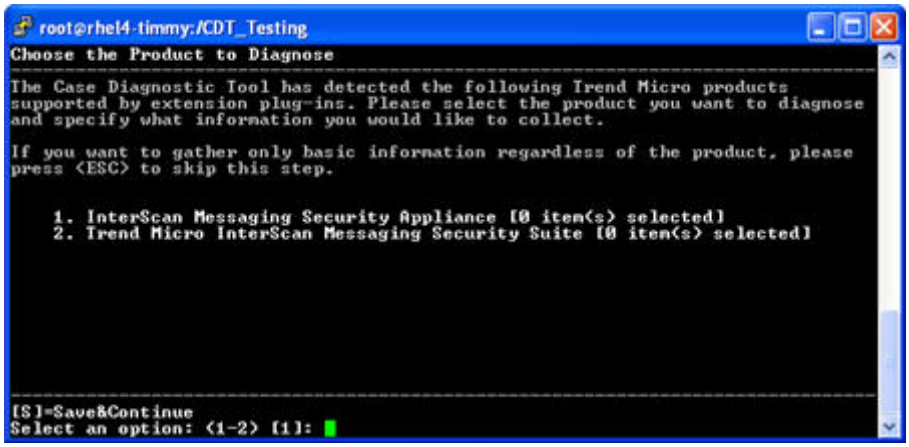

Figure 3: Choose the Product to Diagnose screen

Select the Information to Gather

Here you can see which events (problem classifications or categories) the Case Diagnostic Tool can diagnose automatically. Select the event (or events) related to the problem. If you do not know which events relate to the problem, press the <A> key to select **All Events**. You can also press the <D> key to de-select all events, the <R> key to return without making any changes, or the <S> key to save and continue to the next screen.

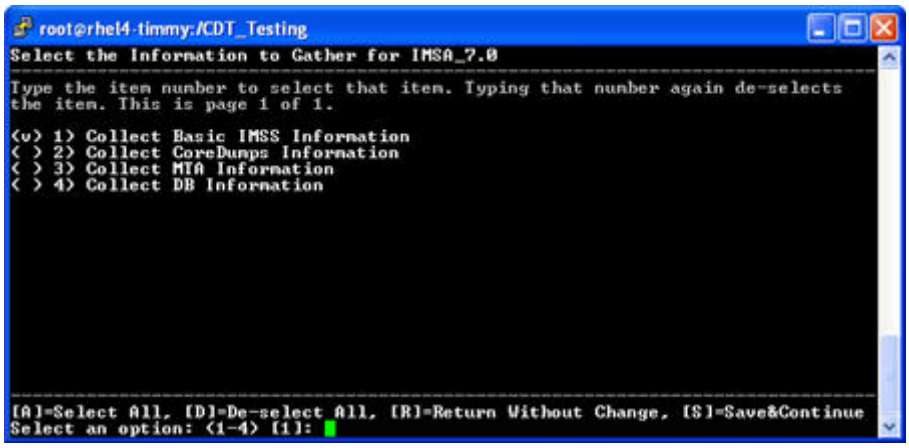

Figure 4: Select the Information to Gather

Confirm Your Selection

On this screen, the Case Diagnostic Tool summarizes the products and events selected. Press the <P> key to go back to the previous page, the <N> key to continue to the next page, the <R> key to return to the Product List screen, or the <S> key to confirm the selections.

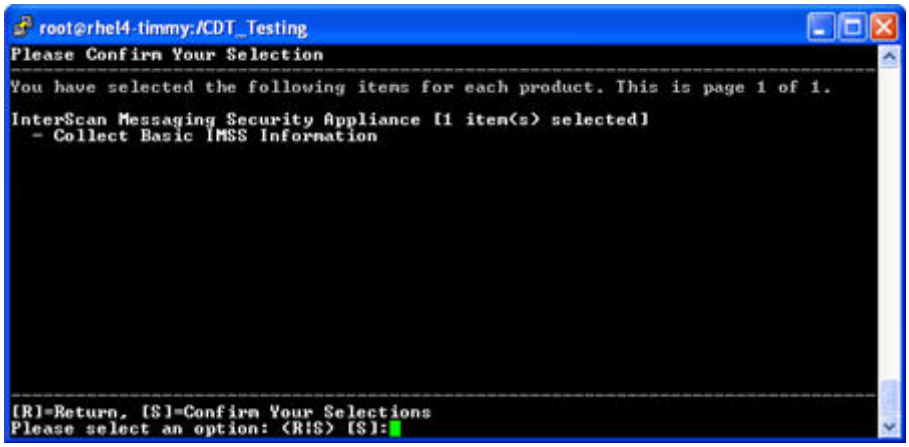

Figure 5: Confirm Your Selection screen

Describe Your Problem in Detail

On this screen, you can write a more detailed description of the problem and how frequently the problem occurs. Press the <CTRL> and <D> keys simultaneously when you have finished.

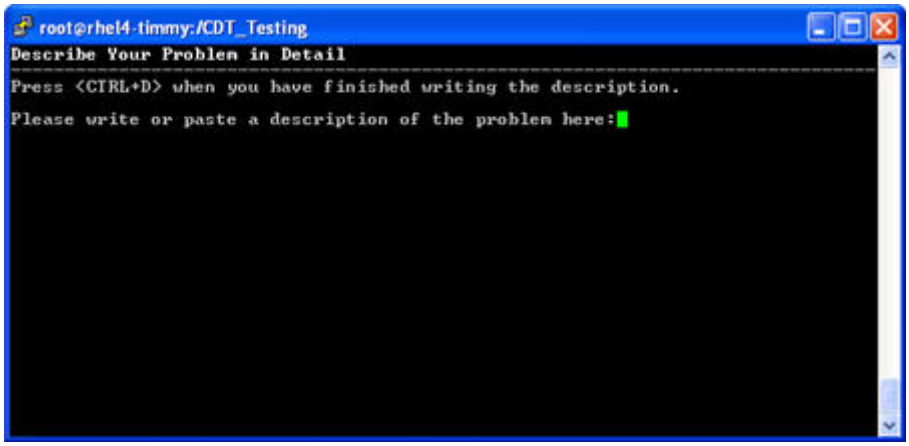

Figure 6: Describe Your Problem in Detail screen

Specify Where You Want to Save the Information Collected

On this screen, you can decide where to save the diagnostic data. Press the <Enter> key to save the information in the default directory.

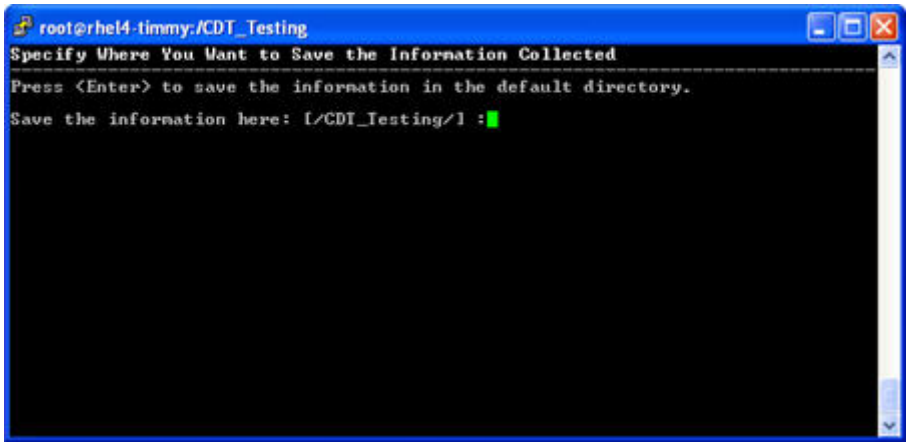

Figure 7: Specify location to save collected information screen

Choose the Debug Mode

If you did not select anything earlier on the **Choose a Product to Diagnose** screen, the Case Diagnostic Tool automatically skips this screen and proceeds to the next screen. If you selected at least one application, follow the procedure below:

1. Press the <Y> key to make the Case Diagnostic Tool automatically activate the debug mode at the proper level for the selected products and modules.
2. Switch over to the application dialog or console to reproduce the problem.
3. After reproducing the problem, press the <Enter> key to restore the original debug settings for the selected products and modules.

If you do not wish to reproduce the problem or have already activated the debug mode, reproduced the problem, and turned off debug before running the tool, press the <N> key to bypass this screen.

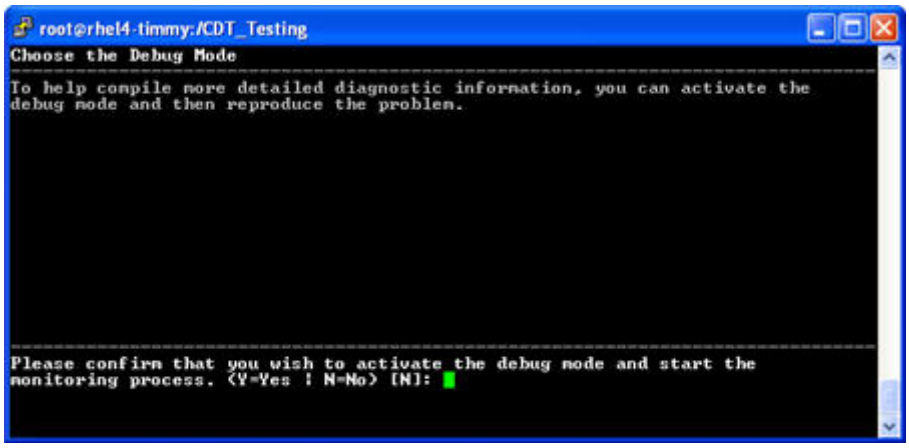

Figure 8: Choose the Debug Mode screen

Filter the Log Range

Here you can specify a time range for log files when collecting the diagnostic data. The Case Diagnostic Tool works *only* on log files with names adhering to the CommonLog log file naming convention. Press <3> to set the **From** and **To** dates yourself. Selecting <2> automatically submits the current date for the **From** and **To** fields. Press the <S> key to compile the system information and diagnostic data.

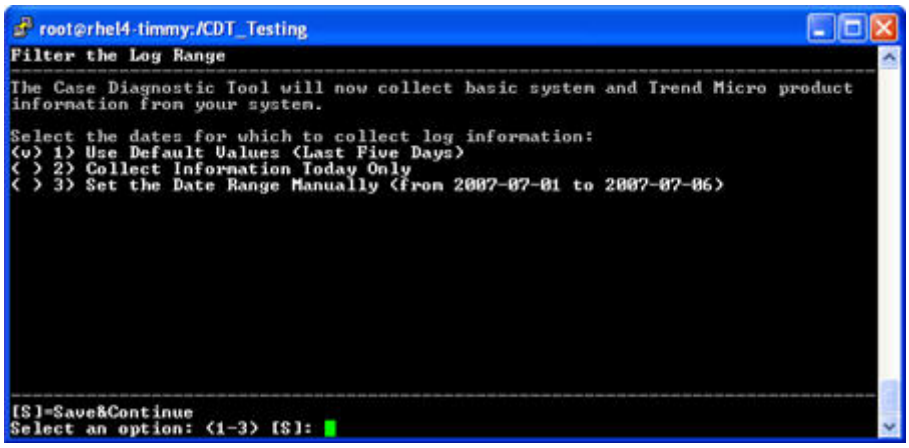

Figure 9: Filter the Log Range screen

Gathering Results

This screen summarizes the results of the diagnostic tests and shows the full path name of the diagnostic data file. Send the data collected in the listed folder to Trend Micro.

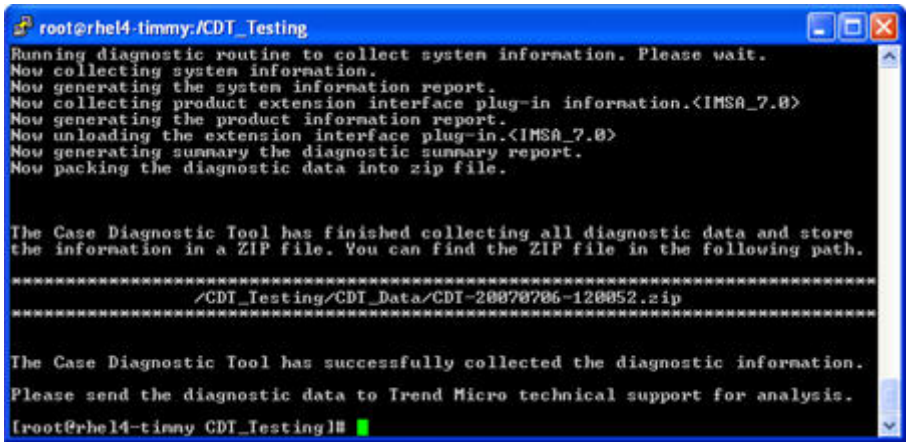

Figure 10: Case Diagnostic Tool results screen

About cdt.ini

The Case Diagnostic Tool uses `cdt.ini` as the configuration file. You must keep the `cdt.ini` file in the same folder as the `cdt` executable file. You can modify the `cdt.ini` settings for the following purposes:

1. **Adjusting the CDT Debug Log Level**
   The Case Diagnostic Tool writes debug information to `CDT_DebugLog.log` during execution according to settings defined in the `cdt.ini` file. You can change the debug log level by setting the "CDT_DebugLevel" key (under the [Setting] section) between 0 and 4, with 4 delivering the most detailed information.
2. **Enacting Silent Mode**
   Changing the "SilentMode" key (under [Setting] section) from the default value of 0 to 1 activates the silent mode and hides the user interface. In silent mode, the Case Diagnostic Tool collects diagnostic data according to settings defined in the `cdt.ini` sections below.
   - [ExInterface]
     Use the keys in the [ExInterface] section to specify from which products you need to collect data. Each supported product has a corresponding INI file in the "ExInterface" subfolder. You can define several keys ("ExInterface1," "ExInterface2," etc.) to troubleshoot multiple products. For example, defining "ExInterface1= IMSS_5" makes the Case Diagnostic Tool refer to the settings in the "ExInterface_IMSS_5.ini" INI file to collect IMSS data.
   - [EventList]
     Defining "ExInterface1=1,3" makes the Case Diagnostic Tool collect data concerning Event 1 and Event 3 for the product defined in "ExInterface1" key of the [EventList] section.
   - [BasicInfo]
     Please refer to "Describe Your Problem in Detail" of the "Working with the Case Diagnostic Tool" section in this Guide for the purpose of this value. Basically, the Case Diagnostic Tool writes a description of the problem in the [BasicInfo] section when running in silent mode.
   - [ProcessCheckList]
     Defining "CheckInterval=2" and "Process1=imssd" in the [ProcessCheckList] section makes the Case Diagnostic Tool check and record the status of the "imssd" process every two seconds.

- [LogFilter]
  Defining “LogFileRange=0” in the [LogFilter] section makes the Case Diagnostic Tool collect all logs. Defining “LogFileRange=1” and “LogFile_JustToday=1” makes the Case Diagnostic Tool collect only today’s logs. You can set a date range by defining the “LogFile_Begin” and “LogFile_End” keys with date values (for example, “LogFile_Begin=20041130” and “LogFile_End=20041201”).

Cdt.ini Contents

```
[Setting]
;Define whether running in silent mode.
SilentMode=0

;Define the default path to store necessary log files when running in
silent mode.
SilentFolder=/tmp/CDT_Data
;Range 0 - 4
CDT_DebugLevel=4

;Define the time period in minutes to reproduce the problem in silent
mode, 0 means timeless
SilentDebugTime=60

;Don’t Run Reproduce Item on Silent mode
SkipSilentReproduce=0

[ProcessCheckList]
; CheckInterval can be 2 to 60 seconds
CheckInterval=2
;Please change those ProcessX pair according to your request.
;Process1=init
;Process2=klogd

;All below sections are used for the silent mode
[BasicInfo]
;Please write description about the problem
```

```
<Problem_Desc_Begin>
<Problem_Desc_End>

;ExInterface plug-ins will be selected in silent mode.
[ExInterface]
;DebugLevel can be 0 to 9
DebugLevel=4
ExInterface1=IMSS_5

;Event related to ExInterface plug-ins will be selected in silent mode.
[EventList]
ExInterface1=1,3

[LogFilter]
;if LogFileRange is 1, LogFile_JustToday, LogFile_Begin and LogFile_End
will be use, otherwise they will be ignored.
LogFileRange=0
;if LogFile_JustToday is 1, LogFile_Begin and LogFile_End will be
ignored.
LogFile_JustToday=1
;LogFile_Begin and LogFile_End, their format must be YYYYMMDD
LogFile_Begin=20041130
LogFile_End=20041201
```

Diagnostic Data Package

After collecting system information and retrieving log files, the Case Diagnostic Tool saves all of the collected diagnostic data files in a single folder for compression into a zip file. Assuming you selected the `CDT_Data` folder (such as `/CDT_Data`), the Case Diagnostic Tool creates a timestamp folder under `CDT_Data, YYYYMMDD-hhmmss`, such as `20041229-113001`. Refer to the following table to identify the files in the timestamp folder:

Table 1: Contents of Diagnostic Data package

Item	Description
`ReadmeFirst.txt`	Summary of the diagnostic process results
`SystemInfo.Report.txt`	System information report
`cdt.ini`	Case Diagnostic Tool configuration file
`CDT_DebugLog.log`	Case Diagnostic Tool debugging log file

The timestamp folder also contains folders named after each product name and version in this format: <`product name_version`>.

In the folder `IMSS_5`, for example, you will find `ProductInfo.Report.txt`, which contains a basic information report. That `IMSS_5` folder also contains two more folders: the `LogFile` folder stores retrieved log files, while the `ConfigFile` folder stores configuration files and registry dump files. The Case Diagnostic Tool separates these retrieved files by EventID and saves them in a specific event folder, such as `Event1, Event2`, and so on. Under each event folder, you can find a `__FILELIST__.LOG` file, which contains list comparing the original filename with the saved filename.

The Case Diagnostic Tool compresses all of the subfolders and files under the timestamp folder into a ZIP file. The ZIP file is saved under the `CDT_Data` folder in this format: `CDT-<TIMESTAMP>.zip` (for example, `CDT-20041229-113001.zip`).

Sample Folder for Reference

```
//--------------------------------------------------------------------
[CDT_DataFolder]                                          <DIR>
  20050822-172312                                         <DIR>
      IMSS_5                                              <DIR>
          LogFile                                         <DIR>
              Event1                                      <DIR>
                  __FILELIST__.LOG
              eMan_db.xml
          ConfigFile                                      <DIR>
          ProductInfo.Report.txt
  ReadmeFirst.txt
  SystemInfo.Report.txt
  cdt.ini
      CDT_DebugLog.log
  CDT- 20050822-172312.zip
//--------------------------------------------------------------------
```