pandasecurity.com

June 2016

# Basic Troubleshooting Guide

## Adaptive Defense/Endpoint Protection products

## Table of Contents

# 1. Introduction

This troubleshooting guide aims at helping the technician provide a first line of support when dealing with customers' queries.

This document applies to the following products:

- Endpoint Protection
- Endpoint Protection Plus
- Adaptive Defense 360

The reason for having a single document for different products is that their core technologies are shared. Moreover, an improvement in a solution or shared technology of one product will be applied across the rest of the products. However, please note that some sections may be specific to certain products; mainly when referring to their own and differentiating technology.

# 2. Scope

The scope or aim of the document is not to cover 100% of the scenarios, which is not feasible, but to address the most known and usual situations that our customers may be facing. Most of the presented cases result in either a solution or in an information request to be escalated to upper support layers for further analysis and resolution.

# 3. Audience

The expected audience of this document is any technician facing customers' queries via telephone call, email, chat, etc. In other words, any technician providing Tier 1 support. The suggested tools and procedures are standard for anyone providing technical support to a corporate user.

# 4. Prerequisites and recommendations

Even if the document is intended to be a guide to be easily followed, there are some prerequisites that are highly recommended (if not mandatory) before you start using it. Among others, these would be the most relevant ones:

- Ensure you have read the product documentation as well as the online help, available from the product console.
- Complete an overview of the product via web access before and during the troubleshooting process.
- Work, whenever possible, with the latest version of the product and, in turn, recommend the customer to move to this version, as it normally includes fixes to bugs present in previous versions.

## 5. Document structure and delivery

The document is structured following the main areas a technician can identify when getting incidents/requests from our customers:

- IDP/Panda Account
- Web Console Errors
- Agent Errors
- Error Installing / Uninstalling protection
- Error Installing / Uninstalling agent
- Product not updated or upgraded
- BSOD
- Adaptive Defense issues
- Errors in the antivirus permanent protection or errors scanning
- Firewall errors, navigation or net resource lost
- Resource consumption
- Third party software
- Malware

This is a live document, so, any change will also be included so that the guide is at all times updated.

Each section includes the most useful instructions or procedures that need to be taken into account when troubleshooting the referred problems.

Additionally, an appendix has been added to detail hints on how to use the main support tools.

# 6. Troubleshooting – Common Scenarios

## IDP/Panda Account

Panda corporate Cloud products delegate credential management to an identity provider (IDP), a centralized application responsible for managing user identity. This means that with a single Panda account, the network administrator will have secure and simple access to all contracted Panda products.

Check the Getting started process flowchart to help you troubleshoot the most common scenarios.

### Key Concepts & Frequently Asked Questions

**What is the welcome email for?**

Basically, to create the Panda Account, not to activate it.
You can resend the welcome email from Salesforce.

**What is the cool user?**

The cool user is the first email address/password combination once activated. It is displayed as the "default user" and cannot be modified or removed.

**Can I use the same email address to create different Panda Accounts?**

No, once an email address is used to create an account you will NOT be able to use the same email address to create a different Panda Account.

**So, basically, to access the console, an activated email address/password combination is required?**

Correct. If the account was created but not activated, you will not be able to access the console.

**How can I activate my Panda account?**

You can activate your Panda account from the activation email that was sent automatically when you created the email account.

If you lost/deleted the email, you can force the activation email to be resent from the password reminder: https://accounts.pandasecurity.com/Web/Account/ResetPassword

**Is a Panda Account linked to the customer's product assets?**

Yes, it is.

**If I create a user from the AD360 console and this email address is not activated, what happens?**

The only way for that user to login and access his asset's services will be after activating his user from his email address.
For further information, refer to the following Support articles:

- Getting started with Adaptive Defense and Endpoint Protection
- Frequently Asked Questions regarding the Panda Account in Panda Cloud products

## Web Console Errors

Error loading the website

1- Error 404 or similar:
   - Check if you can log in from your own machine / environment / console
     - If you cannot log in, escalate the case and describe the tests you have carried out.
     - If it only occurs at the customer's environment:
       - Try to load other websites.
       - Check with other Internet browsers. If the problem persists, escalate the case.

2- Error with customer´s credentials
   - Check the credentials in your computer.
     - We can log in:
       - Check with the customer the credentials (wrong character or number).
       - Send a mail with the correct credentials.
       - Clean Internet browser cache.
       - Clean temporary Internet files.
     - We cannot log in:
       - Request customer´s information (credentials) and report the case to Support.

For the rest of the cases, and before reporting the case to Support, please check you have included the following information:

- ✓ Issue description. Screenshots of the error / visual error.
- ✓ Steps to reproduce it. Ideally, a video will be very helpful.
- ✓ Credentials of the web console.

## Agent Errors

1- Error related to **WaHost.exe** process (message window is displayed at the Desktop).
   - Upgrade the customer´s console to the latest version.

2- Error code 3369 in the Windows event viewer.
   - It is a warning. That machine has not established communication with other Endpoint agents. Check the required ports (see appendix for more details), TCP 18226 and UDP 21226

3- The local settings is different from the profile in the Web Console.
   - Do a Sync http://screencast.com/t/j5j5yUjxu97
   - Uninstall the **Endpoint Agent** from the **Control Panel – Add or Remove Programs**.
   - Uninstall **Endpoint Protection** from **Control Panel – Add or Remove Programs**.
   - Download the install package from the web console and install it again.

If the issue still persists, please include **the following information when you report the incident to Support:**

- ✓ Issue description.
- ✓ Enable log files to maximum detail level. See appendix to know how to do this.
- ✓ PSInfo. See appendix.

## Error Installing / Uninstalling protection

1- Error installing Endpoint Protection
   - Check requirements:
     - Windows
     - Linux
     - OSX
   - Check the error codes:
     - 2081, 2132 and 2133 error codes:
       - Check this article and learn how to fix 2081code. 2081fix tool will be available in the tools section of PSInfo soon.
       - For 2132, and 2133 error codes, please check the following option has been enabled: http://screencast.com/t/JLhRUfj8dqNl
     - 2093 Error code: Use the following tool included in the PSInfo.
2- Error uninstalling Endpoint Protection
   Run the generic uninstaller included tool included in the PSinfo to launch the generic uninstaller.

If the issue still persists, please include the following information when you escalate the issue to Support:

- ✓ Issue description.
- ✓ PSInfo. See appendix.

## Error Installing / Uninstalling agent

1- Error Installing Endpoint Agent
   - Check the minimum requirements:
     - Windows
     - Linux
     - OSX
   - Check the error code:
     - 1289 error code
       - Check there are free licenses in the Web Console.
       - Check the excluded computers: Delete the excluded computers to increase your licenses.
     - 5000 error code:
       Check EPP required URLs using URL Checker included in the PSInfo tool. Required URLs are detailed here.
     - 3365 error code:
       This error means that we are uploading a new catalog. You have to wait for the cloud to sync the new catalog, so we recommend to wait 20 minutes.
   - Error extracting files:
     Check **%temp%** folder permission. If not available, grant write permission to this folder.
   - The installation wizard finishes without an error:
     Execute Panda Cloud Cleaner, as in some cases, it can be an indication of a potential infection.

2- Error uninstalling Endpoint Agent:
   - Run the generic uninstaller
     1. Download
     2. Execute DG_WAGENT_7_XX.exe
     3. Reboot

If the issue still persists, please include the following information when you report it to Support:

- ✓ Issue description.
- ✓ PSInfo. See appendix.

## Product not updated or upgraded

1- Signature files not updated
   - Check if the issue is present in one or more machines:
     - Check the customer has enough number of licenses.
     - Check the customer´s network (Proxy, firewall, etc.)
     - Test our URLs and if problem persists, open PSInfo and use the internal URL tool:
       http://screencast.com/t/rfA4ibQO
       http://screencast.com/t/UU2umO7czyd
       http://screencast.com/t/Qw4lXgl1w
   - Check in the Web console if the Internet connection settings are correctly configured.
   - If the machine has not got Internet access, use URLChecker in the WaProxy/centralized server machine.
     http://screencast.com/t/Wl6KMX6avh3M
   - Check our internal communication ports are allowed ( See appendix for more details):
     - TCP port 18226
     - UDP port 21226
   - Force a Sync (http://screencast.com/t/j5j5yUjxu97)
   - Use the PSInfo tool adding the update parameter.
   - In Web console you could see in the red shield 1/1/1900
     - Uninstall Endpoint Agent.
     - Uninstall Endpoint Protection.
     - Download the install package from web console and install it again.

2- Product is not upgraded
   - Use the PSInfo tool adding the following parameter in the description box.
   - Check upgrade is enabled in the Web console
     http://screencast.com/t/GUJnhB1g
   - Check customer´s network.
     - Proxy
     - Firewall
     - Use URLChecker
   - If the machine has not got Internet access, upgrade is not possible.
   - Check our internal communication ports are allowed ( See appendix for more details):
     - TCP port 18226
     - UDP port 21226

If the issue still persists, please include the following information when you report the incident to Support:

- ✓ Describe the issue.
- ✓ Enable log files to maximum detail level. See appendix to know how to do this.
- ✓ PSInfo. See appendix.
- ✓ Describe customer´s network ( proxy, firewall, …)

### BSOD

1- Identify the problem. Is the name of the driver is displayed?
2- Is the latest product version installed on the computer?
3- Uninstall our product and check if issue is fixed.
4- Install the latest product version.
5- Check what the user was doing before checking the DMP file.
6- Check the video card has got the latest drivers installed.
7- Check the motherboard ´s chipsets are updated.

If issue still persists, please include the following information:

- ✓ Issue description.
- ✓ PSInfo. See appendix.
- ✓ **Full DMP File**. Please check the appendix in order to know how to obtain a full dump file.

## Advanced protection issues (only for Adaptive Defense 360)

The following step applies to the following situations:

- Resource consumption or machine slowdown.
- Error in the advanced protection.
- Third party software incompatibility or binary is being blocked.

Open the advanced protection local configurator tool to enable or disable this feature.

- After disabling this feature the issue no longer exists.
  - Enable the setting again with the tool and reproduce the issue taking traces with PSErrortrace.
  - Take a PSInfo.
  - Provide, if possible, a copy of the software with the steps for reproduction.
- After disabling this feature the issue is still present.
  - Take a PSInfo enabling the agent logs and forcing a sync.
  - Provide, if possible, a copy of the software with the steps for reproduction.

For third party items being blocked by the advanced protection, open the web console and check if the items are present in the Currently blocked items being classified dashboard. If you need the blocked item for your daily activity, bear in mind that you can choose the Do not block again button in order to make an exclusion until the item is classified.

## Errors in the antivirus permanent protection or error scanning

1- Error in the product antivirus tray icon.
   - If a third party security software is present, please, uninstall it.
   - If other Panda Products are installed, then, execute Panda generic uninstaller.
   - Wrong installation or upgrade
     - Uninstall Endpoint Agent.
     - Uninstall Endpoint Protection.
     - Download the install package from web console and install it again.
   - Discard a possible malware infection and execute Panda Cloud Cleaner.
   - Make sure the operating system is updated. Consider carrying out a Windows update.

2- Protection error icon in the Web Console
   - Ask the customer to force a communication between the agent and the Web console, following this procedure:
     - Use the PSInfo tool adding the following parameter in the description box.
     - Right click on the task icon and sync http://screencast.com/t/j5j5yUjxu97
   - Uninstall the Endpoint Agent and install it again.

3- Error scanning
   - Check if you can see an error code and take a screenshot of the error.
   - Check if the issue is random or not.
   - Check if it always crashes in the same file / folder. If it is a temporary file, delete it.
   - Check if it happens with the latest product version.
   - If it is a random issue:
     - Run a **disk defrag.**
     - Run **chkdsk.**
     - Run **scandisk.**
     - Check the machine is updated (**Windows update**).

Report the case with the following:

- ✓ Issue description
- ✓ PSInfo
- ✓ PSErrortrace. See appendix.

## Firewall errors, navigation or net resource lost

1- Error in the firewall protection of the endpoint
   - Error in the local interface (error or a red cross when you open the local interface).
     - Check Windows firewall and disable it.
     - Check other firewall software and disable it.
     - Check the Endpoint Protection and install the latest version if necessary.
   - Error in the Web console.
     - Force a Sync.
     - Check the Web console again and if the last connection does not change http://screencast.com/t/vDXO6kM5Ac, and reinstall the Endpoint Agent.

2- Lost Internet connection or shared folder access
   - Lost network access.
     - Check that you have the latest Endpoint Protection version installed.
     - Uncheck **Network Activity Hook Server Driver.**
       http://screencast.com/t/HldoPlu3Ba
       If the issue is fixed, the problem is related to our Endpoint Firewall Technology. In this case, report the case to Support with the requested information.
     - Windows key + R and write **cmd.**
       - Execute this command: **netsh winsock reset**

3- Lost connection with third party software
   - Check how the firewall protection may be managed:
     - From the web Console
       - Add a new rule for that software.
       - Sync locally to apply the new rule.
     - From the local host
       - Check firewall settings.
         http://screencast.com/t/EklBy4cSA
       - Restore the rules
         http://screencast.com/t/SJSVFx6wj

If issue still persists, please include **the following information:**

- ✓ Issue description
- ✓ PSInfo. See appendix.
- ✓ NNSDiag. See appendix.
- ✓ Describe the network topology.

## Resource consumption

1- Check the customer has got the latest Endpoint version installed.
2- Ensure that the issue is caused by our product.
   - **Start** – **Run** (Windows key + R) and write **services.msc**
   - Stop our services:
     - Panda Cloud Office Protection Service
     - Panda Endpoint Administration Agent
     - Panda Product Service
   - If the issue is reproduced with our services stopped, uninstall the product to make sure the issue is not related to our product.
3- After stopping Panda Cloud Office Protection Service, the issue is fixed. Then:
   - Go to web console and select the profile used in the machine with the issue.
     - Uncheck this option http://screencast.com/t/vuDpCiWh
     - Uncheck compressed files http://screencast.com/t/DM7BXEyXMc
   - Add exclusions http://screencast.com/t/InYyqbLi
     - extension
     - folder
     - files
4- Use the PCOP_protectionerror tool to know what technology is causing the issue:
   - File protection. Stop each driver to find the one causing the issue.
   - Firewall. Stop each drivers to find the one causing the issue.
5- Problem only occurs in one machine.
   - Uninstall Endpoint Agent.
   - Uninstall Endpoint Protection.
   - Download the install package from the web console and install it again.
6- Uncheck settings. See appendix to know more about this step.

If the issue still persists, please include **the following information:**

- ✓ Issue description.
- ✓ PSInfo. See appendix.
- ✓ PSErrortrace if the issue is related to Panda Cloud Office Protection Service. See appendix.
- ✓ NNSDiag if the issue is related to our Firewall Technology. See appendix.

## Third party software

If the issue is caused by a third party software being blocked by the advanced protection of Adaptive Defense 360, refer to section explaining how to deal with blocked items.

1- Error executing software from shared folder.
   a. In the workstation.
      i. Go to the appendix and use the Advanced Protection Local Configurator tool.
      ii. Disable the Adaptive Defense module. If the issue is solved escalate the case. If not, continue with the next step.
      iii. Uncheck the Panda Firewall Hook (http://screencast.com/t/HldoPlu3Ba). If the issue is solved escalate the case.
   b. On the third party server side:
      i. Go to the appendix and use Advanced Protection Local Configurator tool.
      ii. Disable the Adaptive Defense module. If the issue is solved, report the case to Support. Otherwise, continue with the next step.
      iii. Uncheck the Panda Firewall Hook.

We need the following data in order to analyze this type of issues:

- ✓ Third party software.
- ✓ Steps to reproduce the issue.
- ✓ Screenshoots of the error.
- ✓ PSInfo.
- ✓ PSErrortrace if issue is related to Panda Cloud Office Protection Service.
- ✓ NNSDiag if issue is related to the Panda Firewall Technology.

## Malware

Now, we will explain how to deal with malware issues in:

- Adaptive Defense/Adaptive Defense 360
- Endpoint Protection/Endpoint Protection Plus

The procedures below detail what to verify, which data to collect and how to report to Support malware issues.

### How to deal with malware issues with Adaptive Defense/Adaptive Defense 360

When an Adaptive Defense/Adaptive Defense 360 reports a malware issue, you are likely to come across either of these two scenarios:

- Scenario 1: Computer infected
- Scenario 2: Incorrect detection or block

Check either one to know the steps to follow.

**Scenario 1 - Computer infected**

Information collection

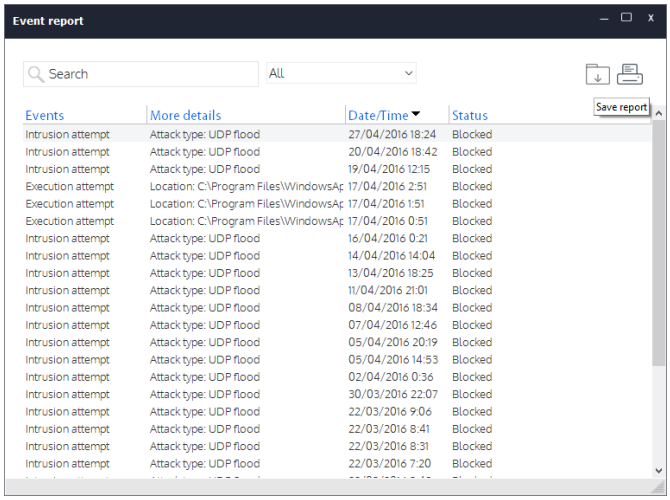
To report malware infections at the endpoint to Support, please collect the following information from the customer:

- Customer Account number and name
- Computer name
- Estimated date of infection
- Source of the infection:
    - SPAM with malicious attachment. If so, please attach suspicious email.
    - On accessing a website
    - Source unknown; the customer only noticed his files were infected.
- PSInfo

**Scenario 2 – Incorrect detection**

Information collection

- Customer Account number and name
- Computer name
- Export of the report from the endpoint antivirus.




- PSInfo

## How to deal with malware detection issues with Endpoint Protection/Endpoint Protection Plus

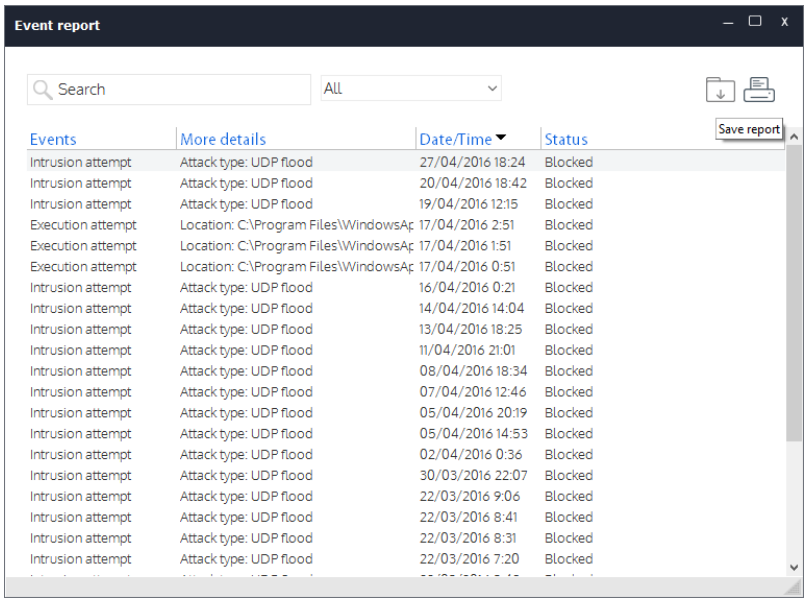
Scenario 1: Endpoint computer infected
To deal with the most usual malware infection cases, please refer to the guide: How to deal with malware issues according to their type.

If you infection persists, as a general rule, please do as follows:

- Run Panda Cloud Cleaner

If the infection persists, collect the following information and report the case to Support:

- Panda Cloud Cleaner log files. From the Panda Cloud Cleaner installation path, by default, **%ProgramFiles\PandaSecurity\PandaCloudCleaner**, locate and create a copy of **Ramdom_Name.pad** file.
  NOTE: Please bear in mind that for 64-bits operating systems, the folder is **%ProgramFiles(x86)\PandaSecurity\PandaCloudCleaner**
- Customer Account number and name
- Computer name
- Export of the report from the endpoint antivirus.

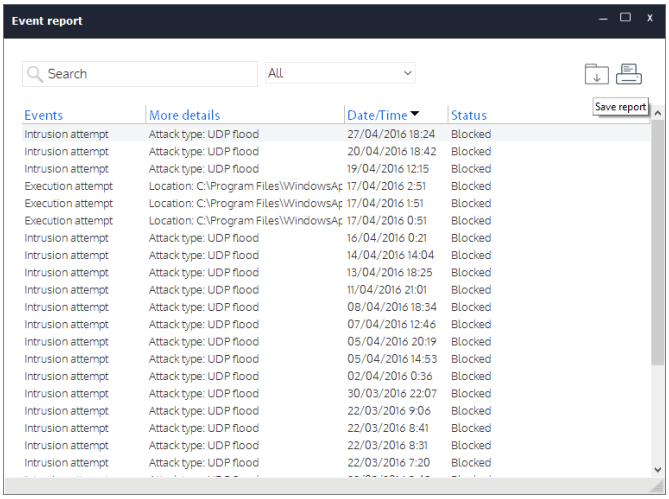



- PSinfo

**Scenario 2 – Incorrect detection**

Information collection

- Customer Account number and name
- Computer name
- Export of the report from the endpoint antivirus.




- Sample of the file erroneously detect as malware.
- PSinfo

# 7. Appendix

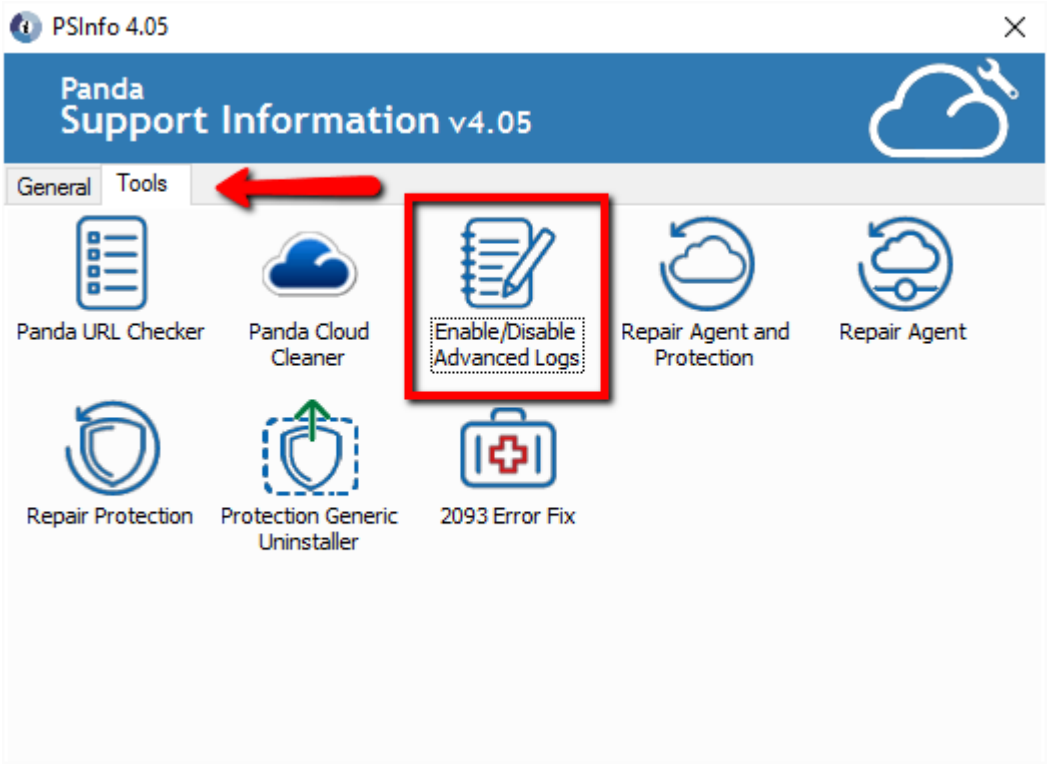
This appendix includes the tools and procedures to use them that could assist in the troubleshooting process.

## URLs

Refer to the Support article Which URLs are necessary for the product to work correctly?

## Enable Agent Logs

How to enable log files to maximum detail level. Use the PSInfo tool Enable/Disable Advanced Logs option.




## PSInfo

Link

## Check ports

Our product uses TCP port 18226 and UDP port 21226. Those ports are used to establish communication with other Endpoint Agents. If you need to check if the communication is fine, please do this:

- Windows key + R
- Write **cmd** and press the **Enter** key
- **telnet destinationmachinename 18226**
- **telnet destinationmachineipaddress 18226**

With this, you can check if the port is denied or allowed.

## PSErrorTrace

PSErrorTrace tool gathers useful information to diagnose and study Endpoint Protection issues related to the installation, scan or compatibility with third-party software.
Follow the steps below:

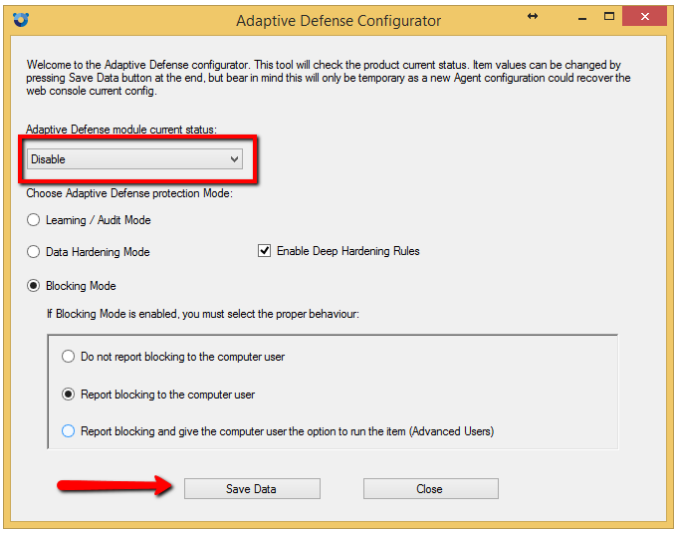
1. Download PsErrorTrace.exe and run the file with elevated privileges.
2. Click the **Start** button.
3. Choose the type of operation you were doing when you encountered the problem (installing, activating, opening a program, scanning, etc.) and click **Continue**.
4. Fill in your email address and description of the problem and click **Continue**.
5. Now, you will be asked to replicate the issue you had encountered (scan stuck, failed installation, etc.). When you are ready to do so, click **Start**.
6. Once you are able to replicate the problem and when the button is no longer greyed out, click **Finish**.
7. Choose **Exit** and click **Yes** to save the report **PsErrorTrace.PSInfo** to your computer.
8. Finally, send the **PsErrorTrace.PSInfo** file to Support.

## Advanced Protection Local Configurator

The panda_adaptivedefense360.exe tool checks the product configuration and allows to carry out changes in the advanced protection locally. This allows to determine if the issue is being caused by the advanced protection (Minerva) or narrow down with which configuration the issue is occurring.

The tool verifies the correct product is installed and checks the service is running.

Choose disable option and save the changes.




## NNSDiag

NNSDiag gathers useful information to diagnose issues related to the Endpoint Firewall technologies.

In order to narrow down the problem and offer a solution, we need to collect and study certain data. Please follow the steps below:

1. Download and extract the **nnsdiag.zip** and run **nnsdiag.exe**.
2. Follow the steps indicated in the wizard.
3. It is important NOT TO restart your computer during these tests.
4. Once the process finishes, the tool save the data collected. Provide TechSupport the resulting **NNSDiagResults.zip** file.

## Uncheck Settings

In the local interface, we can temporarily allow a local administration panel to help us find where the problem is. To enable this local administration panel, follow the steps below:

1. Go to the Web console and choose the profile affected by the issue.
2. Go to the **Windows and Linux** option and click on **Advanced settings**

   tab http://screencast.com/t/sicv22Z9Do7
3. Access the **Administration password** option and enable it.

   http://screencast.com/t/2qoAXdoEf
4. Then, go to the local machine and do a SYNC.

   http://screencast.com/t/INGyWghvvOa
5. Open the local interface and click on **Administrator Panel.**

   http://screencast.com/t/SQNX4AVs4
6. Write the password set and click on log in. There you could enable or disable the modules in order to find which is causing the issue.

   http://screencast.com/t/7FcZYIP8
7. When you log out, you could set how long to keep the changes.

   http://screencast.com/t/E929b3IX

## How to generate a post-mortem memory dump (BSODs)

Follow the steps below to automatically generate a post-mortem memory dump that records information about errors.

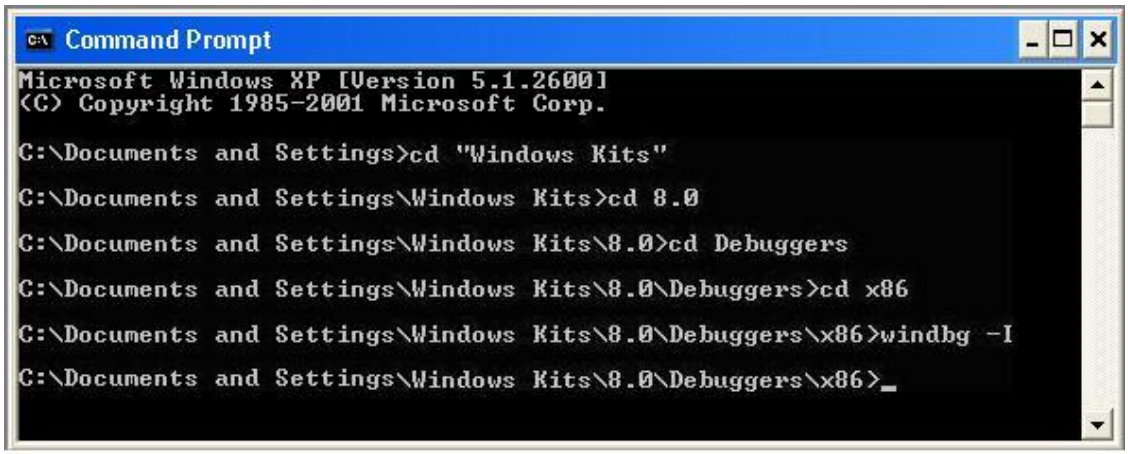
1. Download and install the Microsoft Debugging Tools for Windows:

   http://msdn.microsoft.com/windows/hardware/hh852363
2. Follow the steps below to establish **WinDBg** as the default debugger:
   1. Open the MS-DOS Prompt window. To do this, go to **Start** -> **Run**, type **cmd** and click **OK**.
   2. Go to the **WinDBg** installation directory.

To do this, type the commands below and press **Enter** after every command:

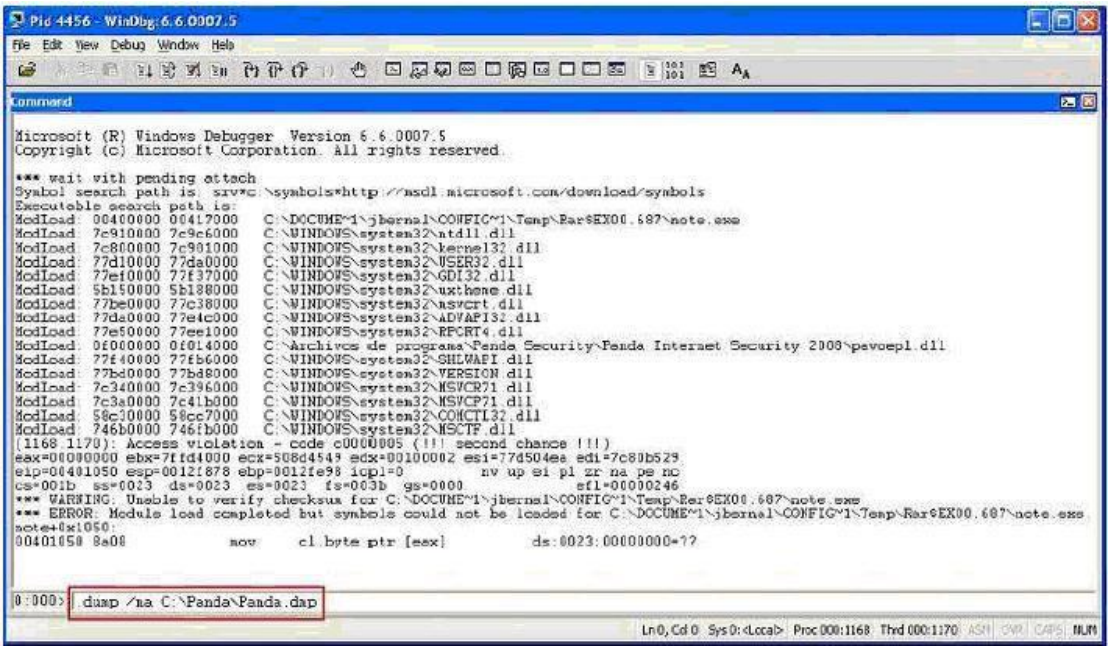
cd\
cd "Program Files"
cd Windows Kits
cd 8.0
cd Debuggers
cd x86 (if you have 32-bit OS) or cd x64 (if you have 64-bit OS)
Windbg –I

WinDbg -I
Note: 'I' is capital 'i'.




3. Create a folder called Panda in the **C:** drive to store the dump file (**C:\Panda**).

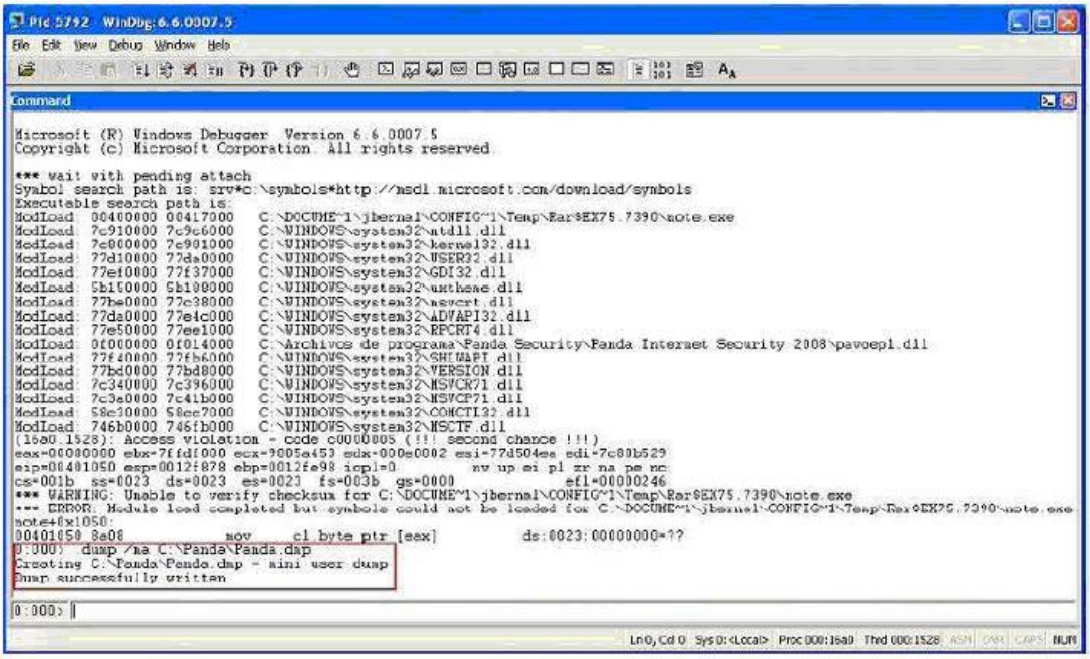
   From now onwards, whenever an error message is displayed, the **WinDBg** window below will be displayed:




4. At the bottom of the window, where 0: 000> is indicated, enter the following command:

   **.dump /ma C:\Panda\Panda.dmp**

   If the dump is correctly generated, the message **'Dump successfully written'** will be displayed at the bottom of the screen.



Once these steps are completed, a file called **Panda.dmp** will automatically be generated in the C:\Panda directory.

5. Compress the **dmp** result and send us to analyze it.

## List of generic errors

The following webpages include the list of the most common errors you could find when working with Endpoint Point Protection and Adaptive Defense products:

List of the most common errors in Endpoint Protection