SSL Appliance SSL Diagnostics Tool

Version 1.1.0
First Published: 9/30/15

Use the SSL Diagnostics tool to parse statistics within a diagnostic package collected by a Cisco SSL Appliance. This guide provides an overview of the SSL Diagnostics tool and its installation.

Descriptions of all the commands are provided in Using the SSL Diagnostics Tool, page 4. The tool and documentation is available on `cisco.com`.

This version of the SSL Diagnostics tool supports data export in space-delimited format, for use with Blue Coat Reporter. Use the `-r` option from the command line to output the `.csv` file in Reporter format. See the `ssldiags.pdf` documentation for syntax information.

Cisco SSL Appliance software is subject to licensing terms and conditions imposed by Cisco and third party software providers. For more information, see the following sections:

Requirements

- An x86 or x86-64 personal computer running Windows or Linux. The system must be running Python version 2.6.x or 2.7.x; Python 3.x is not supported. This is called the "host" system in this document.
- A Cisco SSL Appliance ssldiags output file you want to run the SSL Diagnostics tool on.

Cisco Systems, Inc.
www.cisco.com

Install the SSL Diagnostics Tool

The SSL Diagnostics tool is provided as a zipped package which must be installed on the host system. The package file name is `ssldiags-n.n.n.zip`, where "`n.n.n`" is a version number for the package.

Install the Package in a Linux environment

Step 1   Copy the file to the host system.

Step 2   At a command line type in the following:

```
unzip ssldiags-n.n.n.zip
cd ssldiags-n.n.n
python setup.py install
```

**Tip**   You must be logged on as a user with privileges that allow software installation.

Install the Package in a Windows Environment

On Windows systems, additional steps are required to complete the installation. You must add the directory where the script was installed to your system path. To do this, open a `Run` window (click `Start`, type `run`, and click `Enter`),

Step 1   In the `Run` window, enter

```
C:\windows\system32\rundll32.exe" sysdm.cpl,EditEnvironmentVariables
```
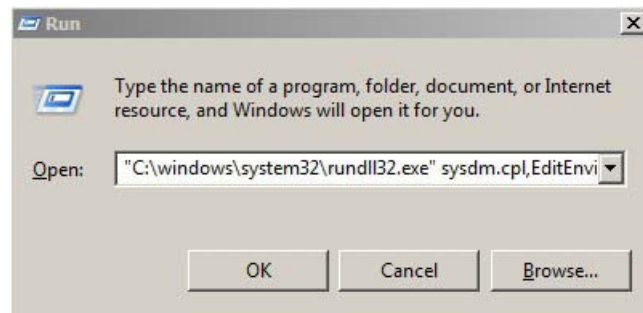
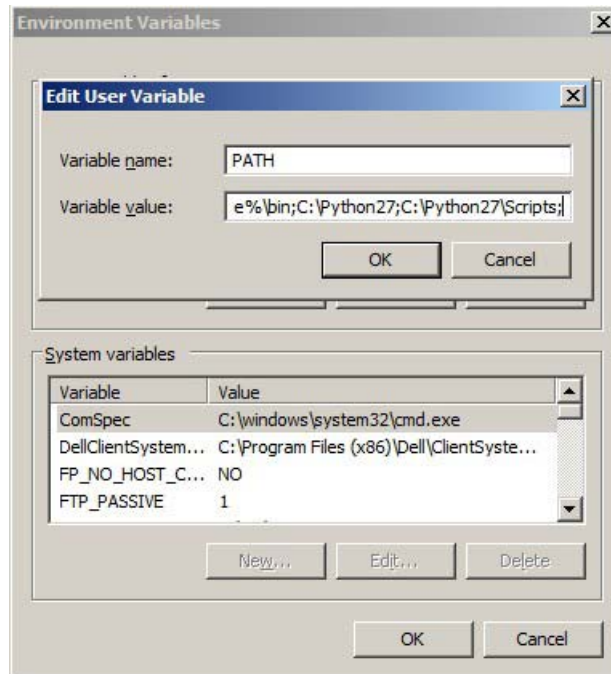**Step 2**   Click OK. The Environment Variables window displays.
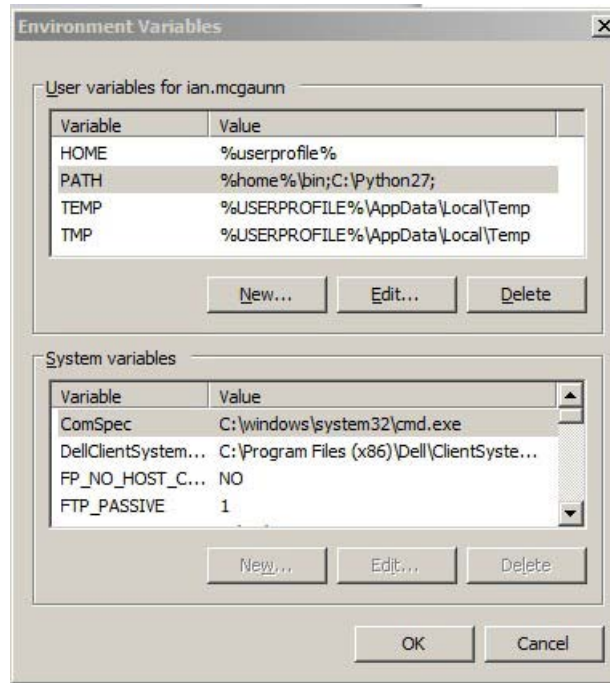
Step 3   In the top panel labeled User variables for <user name>, select the PATH entry, then click Edit. The Edit User Variable windows displays.

Step 4   Enter the path to your unzipped file in the Variable value field, followed by a semicolon. An example is shown next.

Note   The example uses Python 2.7. The SSL Diagnostics tool requires Python 2.6.x or 2.7.x (Python 3.x is not supported).

Step 5   When the entry is correct, click `OK`. Exit the `Environment Variables` window.

Verify the Installation

To verify that the SSL Diagnostics tool is installed correctly, open a command prompt and enter

```
ssldiags.py --version
```

You should see:

```
host:<path>/ssldiags/$ ssldiags.py --version
Usage: ssldiags.py -i <INPUT DIR> -c <COUNTER NAMES> -p <PREFIX PATH> [-o <OUTPUT PATH>]
Tool for parsing binary SSLV statistics files into CSV format. Version: n.n.n
```

Using the SSL Diagnostics Tool

The following options can be provided on the command-line:

Note   You must specify directory path where history files and counter names are located

Usage:

```
ssldiags.py [options]
```

Option	Result
`-h, --help`	show this help message and exit
`-i INPUT_DIRECTORY,` `--input-directory=INPUT_DIRECTORY`	Input directory with statsitsics and counter names files
`-p PREFIX, --prefix=PREFIX`	File prefix: history files are \<prefix\>.\<num\>.bin
`-c COUNTER_NAMES,` `--counter-names=COUNTER_NAMES`	Counter names file name (not path), e.g.:\<prefix\>_counter_names_\<timestamp\>.csv
`-o OUTPUT, --output=OUTPUT`	Output file. If not specified, stdout will be used
`-v, --version`	display version number and exit
`-r, --reporter`	Export Output file in Blue Coat Reporter format. (Space Delimited)

For Assistance

Cisco Support

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco SSL Appliances, see **What's New in Cisco Product Documentation** at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to **What's New in Cisco Product Documentation**, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions or require assistance with the Cisco SSL Appliance, you can also contact Cisco Support:

- Visit the Cisco Support site at http://support.cisco.com/.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.