

Guide to DeepSight Extractor 4

Copyright Notice

Copyright © 2005-2006 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and DeepSight are US registered trademarks of Symantec Corporation or its subsidiaries. DeepSight Analyzer, DeepSight Extractor, and Bugtraq are trademarks of Symantec Corporation or its subsidiaries. Other brands and products are trademarks of their respective holders.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Guide to DeepSight Extractor 4

This guide is intended as an introduction to Extractor 4.0, it includes coverage of .x revisions. It is broken into sections to provide appropriate information from your initial planning through installation and configuration:

[Extractor Overview](#)

[Running DeepSight Extractor with Windows XP SP2](#)

[Updating System Files for Windows NT4](#)

[Building Extractor 4 for Unix Systems](#)

[Extractor Installation](#)

[Extractor Configuration](#)

[Command Line Usage](#)

[Running Extractor in Daemon Mode](#)

Extractor Overview

In order to use the services of DeepSight Analyzer, an organization must upload firewall and intrusion detection system log files using Extractor 4.

Extractor does not need to run on an organization's reporting security devices. By design, any firewall or intrusion detection system, regardless of operating system, can submit data via Extractor. The only conditions are that Extractor has a parser for the specific firewall or IDS in use, and that the machine running Extractor has access to the firewall or IDS log files.

DeepSight Extractor supports the following platforms:

Platform	Version
Windows	XP Win 2000 WINNT 4.0 SP2+ Windows Server 2003
Solaris	9+
*BSD	FreeBSD 4.10 & 5.2.1 NetBSD 1.6.2 OpenBSD 3.6 Darwin
Linux	kernel 2.2+

The security systems for which log file parsers are available are listed below along with notes describing any special configuration conditions.

Supported Security Device	Versions	Rules Files	Notes & Special Conditions
BlackIce PC Protection	2.0-3.x	blackice.rules	Log file: attack-list.csv
Cisco IOS	12.x	ios.rules	In syslog
Cisco PIX	4.2-6.x	pix.rules	In syslog
Cisco Secure	2.5-3.0	secureids.rules	

IDS (Netranger)			
Enterasys Dragon	4.2.2	dragon.rules	<p>Log file: dragon.sys or dragon.log.000</p> <p>NOTE: The use of daily event logs must be disabled. When this feature is in use, Dragon event logs are renamed and Extractor is unable to find the logs. To accomplish this, two options must be set in the driders.cfg file.</p> <p>LOG_TO_EXPORTLOG=1 EXPORTLOG_ROTATION=<some high number like 99999999></p> <p>The driders.cfg file is usually in /usr/drider/driders.cfg. This path must be added to the ConfigFile.ini Profile for the system, i.e. DataSource2="/usr/drider/driders.cfg"</p> <p>The Dragon system is the only system that requires a value for DataSource2.</p>
Enterasys Dragon	5.x, 6.1.1 and higher	dragon.rules	<p>Log file: dragon.log.xxx</p> <p>NOTE: The use of daily event logs must be disabled. To accomplish this you must change one option in dragon.cfg.</p> <p>Go to the ExportLog section of dragon.cfg and add or modify the following configuration:</p> <p>Rotation=<some high number like 999></p> <p>The dragon.cfg file is usually in /usr/dragon/dragon.cfg. This path must be added to the ConfigFile.ini profile for the system, i.e. DataSource2="/usr/dragon/dragon.cfg"</p>
Firewall-1	Next Generation, NG	firewall1.rules	<p>FW-1 must be configured to export its binary log file with the command:</p> <p>fw logexport -n -f -o /home/user/fwlog.txt</p> <p>This command tells FW-1 to write the contents of the log to fwlog.txt, and to continually update fwlog.txt as new events are logged. You may wish to run this command as a background process:</p> <p>nohup fw logexport -n -f -o /home/user/fwlog.txt >/dev/null 2>&1 &</p> <p>The Extractor 4 ConfigFile.ini Profile for this Firewall-1 sensor must point to: DataSource1="/home/user/fwlog.txt" or other correct path to fwlog.txt.</p>
Firewall-1	OPSEC	opsec-fw1.rules	The firewall log is accessed via the

			OPSEC API.
IP Chains	OS Independent	ipchains.rules	Requires Linux kernel 2.2+ In syslog
ipmon (IPF)	OS Independent	ipmon.rules	Log file: ipmon log
iptables	OS Independent	iptables.rules	In syslog .
NetProwler	3.5x	netprowler.rules	NetProwler uses the Windows ODBC API to connect to the events database, as a result, the UNIX Extractor does not support NetProwler.
NetScreen	200, 100, 50, 25, 5XP	netscreen.rules	In syslog
Norton Internet Security (including Professional)	2004 - 2006	nis04.rules nis05.rules nis06.rules	Extractor runs as an NPF/NIS trusted service. NOTE: Extractor creates the file npf.log in order to upload NIS events.
Norton Personal Firewall	2004 - 2006	npf04.rules npf05.rules npf06.rules	Extractor runs as an NPF/NIS trusted service. NOTE: Extractor creates the file npf.log in order to upload NPF events.
RealSecure Workgroup Manager NOTE: DeepSight Extractor for Unix will not extract and upload from RealSecure.	3.1-5.5 6.00-6.x	realsec3.1-5.5.rules realsec6.rules	For RealSecure up to v5.5 , configure RealSecure profiles using Microsoft Access with the following steps within the Extractor Configuration Wizard: <ol style="list-style-type: none"> 1) Switch to the Machine Data Source tab. 2) Click on the New Button 3) Make the new DSN a System DSN. If a <i>User DSN is chosen, the extractor service will not have access to that DSN unless it is configured to run as that user.</i> 4) Choose the Microsoft Access Driver 5) Point it to the file in the RealSecure install directory (rsntclientlog.mdb) For RealSecure v6.0 and higher , configure RealSecure profiles using SQL Server with the following steps within the Extractor Configuration Wizard: <ol style="list-style-type: none"> 1) Go to the second screen of the profile, 2) Click 'Browse' to pick the data source 3) Switch to the Machine Data Source tab. 4) Click on the New Button 5) Make the new DSN a System DSN. If a <i>User DSN is chosen, the extractor service will not have access to that DSN unless it is configured to run as</i>

			<p><i>that user.</i></p> <p>6) Choose the SQL Server driver</p> <p>7) Enter the database details:</p> <p>a) Use SQL Server Authentication. If using Windows authentication, the extractor service will not have access to the SQL db unless configured to run as that user.</p> <p>b) Ensure the Client Configuration is set to TCP/IP. This is the default for SQL Server 2k, but not in SQL Server v6.5 and possibly 7.0</p> <p>8) Point the default database to the RealSecure database. This database is usually called ISSSED.</p>
RealSecure SiteProtector (ISS)	2.0	siteprotector2.rules	<p>Configure the ISS SiteProtector profiles using SQL Server with the following steps within the Extractor Configuration Wizard:</p> <ol style="list-style-type: none"> 1. Go to the second screen of the profile, 2. Click 'Browse' to pick the data source 3. Switch to the Machine Data Source tab. 4. Click on the New Button 5. Make the new DSN a System DSN. <i>If a User DSN is chosen, the extractor service will not have access to that DSN unless it is configured to run as that user.</i> 6. Choose the SQL Server driver 7. Enter the database details: <ol style="list-style-type: none"> a. Use SQL Server Authentication. If using Windows authentication, the extractor service will not have access to the SQL db unless configured to run as that user. b. Ensure the Client Configuration is set to TCP/IP. This is the default for SQL Server 2k, but not in SQL Server v6.5 and possibly 7.0 8. Point the default database to the

			SiteProtector database. This database is usually called RealSecureDB.
Snort	1.6-2.x	snort.rules	Log file: alert or syslog
Snort Portscan	1.6-2.x	snort-portscan.rules	Log file: portscan.log
Snort Scan Log	1.9-2.x	snort-scan.rules	Log file: scan.log
Symantec Client Security	2.0-3.0	scs2.rules scs3.rules	NOTE: Extractor creates the file npf.log in order to upload SCS events.
Symantec Enterprise Firewall	7.0	sef.rules	<p>The remotelog tools must be used to export log files from SEF to a local file which can be parsed by Extractor.</p> <p>remotelogfile.exe <code><ipaddr_of_SEF_gateway> logfile -f > current.log</code></p> <p>This command tells SEF to write the contents of the log to current.log and the -f option continually updates the log file as new events are logged.</p> <p>The Extractor ConfigFile.ini profile for this SEF sensor must point to:</p> <p>DataSource1="<pathtofile>/current.log"</p> <p>The remotelog tools are not installed by default. They can be found on the installation CD in the directory ClientSoftware.</p>
Symantec Firewall Appliance	100/200/200R	sfa.rules	In syslog .
Symantec Gateway Security	5110, 5200, 5300	sgs.rules	<p>The remotelog tools must be used to export log files from SGS to a local file which can be parsed by Extractor.</p> <p>remotelogfile.exe <code><ipaddr_of_SGS_gateway> logfile -f > current.log</code></p> <p>This command tells SGS to write the contents of the log to current.log and the -f option continually updates the log file as new events are logged.</p> <p>The Extractor ConfigFile.ini profile for this SGS sensor must point to:</p> <p>DataSource1="<pathtofile>/current.log"</p> <p>The remotelog tools are not installed by default. They can be found on the installation CD in the directory</p>

			ClientSoftware.
Symantec Gateway Security	320	sgs.rules	In syslog .
Symantec Gateway Security 5600 Series Appliance	3.0	sgs3.rules	<p>In order to retrieve security events from Symantec Gateway Security, the remotelog tools must be used to export log files from the security gateway to a local file in the same directory as the remotelog tools. The local copy of the log can then be parsed by DeepSight Extractor.</p> <p>To do this, use the remotelogfile utility included on the CD. The command used for Windows is:</p> <p>remotelogfile <ip_address_of_SGS> lang/en logfile -i -s -f > sgs.log</p> <p>For UNIX it is:</p> <p>remotelogfile <ip_address_of_SGS> lang/en logfile -i -s -f > sgs.log</p> <p>This command tells SGS to write the contents of the log to sgs.log and the -f option continually updates the log file as new events are logged.</p> <p>NOTE: The LANG environment variable must be cleared in order to make the remotelogfile work on Linux. This can be accomplished on most Linux systems with the command: export LANG=""</p> <p>The DeepSight Extractor ConfigFile.ini profile for this Symantec Gateway Security sensor must point to:</p> <p>DataSource1=""<pathtofile>/sgs.log"</p> <p>The remotelog tools are made up of a client component and a server component. The client component must be installed onto the system that is running DeepSight Extractor. The server (SGS) needs to have a Machine Account set up through the java management interface. The client utilities can be found on the installation CD in the directory ClientSoftware.</p> <p>For more information on remotelogfile, see the Symantec Gateway Security user manual.</p>
Symantec Manhunt	3.0 – 4.0	manhunt.rules	<p>Manhunt's Event Writer should be used to output event data to a flat file.</p> <p>Extractor must be installed on the Manhunt node and the file specified by Event Writer</p>

			must be used as Extractor's log file. For more information, please review Symantec Manhunt Version 3.0 Administrative Guide – pages 148-149.
Windows Server	2003	xp.rules	Log file: pfirewall.log Usually found in: C:\Windows\pfirewall.log
Windows XP Internet Connection Firewall	Home, Professional	xp.rules	Log file: pfirewall.log Usually found in: C:\Windows\pfirewall.log
ZoneAlarm	2.6.0-4.5	zonealarm.rules	Log file: ZALog.txt

The Windows Extractor Configuration Wizard automatically selects the correct .rules file when the system type is selected; and the default log file is selected by browsing to it, the Configuration Wizard enters the correct path and file name.

The Unix Extractor requires manual configuration of the **ConfigFile.ini** file **Profile** values. The .rules file is specified with the IDSRules="" value and the log file with the DataSource1="" value. Here is an example of the relevant portion of a Snort profile:

```
[profile="snort"]
IDSRules="/root/Extractor/rules/snort.rules"
DataSource1="/var/log/snort/alert"
DataSource2=""
```

In both cases the complete path to the log file must be specified.

NOTE: The first upload of a new Extractor profile may be CPU intensive because Extractor must parse the entire log file. The duration of this CPU load is dependent on the size of the log file to parse. Subsequent uploads are incremental, this minimizes the CPU load when Extractor is parsing.

Extractor 4 – Parsing syslog for multiple security devices

This special condition involves IDS and firewall systems that allow data to be logged to a single file, typically, syslog. The systems capable of reporting to a syslog are listed below:

Cisco IOS
Cisco PIX
IP Chains
iptables
NetScreen
Snort
Symantec Firewall Appliance
Symantec Gateway Security 320

Extractor can correctly parse syslog and upload events to DeepSight Analyzer so that each security device is properly identified. The proper Profile configuration is critical.

NOTE: Configuring Extractor with the Kiwi Syslog Daemon for Windows is conceptually identical to using Extractor with other syslog. It is, however, important to use the **Log to File** option with the **BSD Unix syslog format**.

For instance, a single syslog may contain entries from Cisco PIX, IP Chains, and Snort security devices. In this example, Extractor requires three profiles that could be named: *syslog-PIX*, *syslog-chains*, and *syslog-snort*. Remember each Extractor profile in both WIN32 and Unix identifies the type of security device with the **IDSRules=** configuration parameter, the location of the log file, in this case, syslog, is specified with the **DataSource1=** configuration line (The WIN32 Configuration Wizard makes these entries based on the specified device type and identified log location). So to upload data from each of those devices, Extractor accesses the syslog 3 times, parsing the file for the correct data type identified by the **.rules** file in the **IDSRules=** parameter. However, each profile may represent multiple security devices of the same type. Extractor parses each system by reading the syslog; the devices need not be named within the configuration file.

After the Extractor upload, the Analyzer user must identify the location of each device during the next DeepSight Analyzer login. For example, the *syslog-PIX* profile may have 2 PIX firewalls reporting, PIX-1 and PIX-2. There are 3 possible cases for this example:

1. Both devices report data;
2. One of the devices reports data;
3. None of the devices reports data.

When both devices report data on the initial upload, the Analyzer user is asked to specify the location of each PIX firewall. Subsequent uploads proceed normally.

When only one device has data on the initial upload, the Analyzer user is asked to specify the location of the uploading PIX firewall. Subsequent uploads proceed normally. When the second PIX reports in with data, the Analyzer user is again asked to specify the location of that firewall.

Finally, when neither of the devices has data in the syslog for the initial upload, the profile name, *syslog-PIX*, appears on the Events-log tab showing empty logs. From then on, whenever empty logs are reported by PIX-1 or PIX-2, the empty logs are recorded under the profile name.

Running DeepSight Extractor with Windows XP SP2

When you install Windows XP Service Pack 2, the Windows Firewall is installed and activated by default. It does this even if another firewall is already installed. This may prevent DeepSight Extractor from working with your originally installed firewall, either by blocking Extractor from uploading your events to DeepSight; or by blocking all traffic to your original firewall so that it looks like your original firewall is not working, in which case, Extractor will have no new events to upload.

If you decide to use the Windows Firewall, you must reconfigure DeepSight Extractor and add a profile for Windows XP firewall. In addition to changing your Extractor configuration, you will also be asked to confirm the location of your new firewall on your first login to the DeepSight Analyzer site.

To continue using your original firewall, you need to turn off the Windows Firewall:

1. Click **Start->Settings->Control Panel** double click on **Windows Firewall**.

2. From the **General** tab, select the **Off (not recommended)** radio button.
3. Click **OK**.

NOTE: For some systems it may be necessary to reboot to turn on the originally installed firewall system.

WARNING: You should only turn off the XP firewall if you are certain your original firewall is installed and configured correctly to protect your system.

Updating System Files for Windows NT4

To run DeepSight Extractor on Windows NT 4.0 (Server and Workstation) the system files must be updated. The system file update is necessary if you receive the installation error:

The ordinal 6880 could not be located in the Dynamic Link Library MFC42.DLL

To update the system files, follow the steps outlined below:

1. Uninstall DeepSight Extractor.
2. Download the required update from the Microsoft website:

<http://activex.microsoft.com/controls/vc/mfc42.cab>

3. Use Winzip or another application which will allow you to extract files from a CAB file to extract the file mfc42.exe from the CAB file.
4. Execute mfc42.exe to update the system file. The update might require you to reboot your computer.
5. Proceed to install DeepSight Extractor.

Building Extractor 4 for Unix Systems

Installation Requirements:

cURL 7.9 – 7.9.8 and 7.11-7.15.0 - We do not support cURL 7.10 at this time.
(cURL requires OpenSSL)

The latest version of curl can be obtained at the time of this document's creation from:

cURL 7.15 source: <http://curl.haxx.se/download/curl-7.15.0.tar.gz>
Other formats and versions: <http://curl.haxx.se/download/>

GNU make 3.79

Is available from gnu.org: <http://www.gnu.org/software/make/make.html>

To test for the correct version of cURL and GNU Make, and to ensure you have OpenSSL installed correctly, enter the following commands at the prompt:

curl -V

Example:

```
bash-2.05a$ curl -V
curl 7.15.0 (i386-unknown-freebsd4.5) libcurl/7.15.0 (OpenSSL 0.9.6a) (ipv6
enabled)
```

openssl version

Example:

```
bash-2.05a$ openssl version
OpenSSL 0.9.6a 5 Apr 2001
```

make -v (or gmake -v)

Example:

```
bash-2.05a$ gmake -v
GNU Make version 3.79.1, by Richard Stallman and Roland McGrath.
Built for i386--freebsd4.5
Copyright (C) 1988, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 2000
Free Software Foundation, Inc.
This is free software; see the source for copying conditions.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
```

Once the system requirements are met, download the appropriate version of Extractor for UNIX from: <http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=159> or <https://analyzer.securityfocus.com/download.aspx>

You can now make the binary file Extractor.

```
cd /wherever/downloaded/extractor.tar.gz  
Move to the location of the download.
```

```
gzip -dc extractor-filename |tar xvf -
```

```
cd Extractor
```

```
make
```

This command builds the Extractor binary. OpenBSD, Free BSD and some other platforms may require the use of **gmake**. The Extractor install requires GNU make 3.79.

In the event you get linker errors because the compiler cannot find the OpenSSL libraries, try this:

```
make SSLDIR=/usr/local/ssl/lib
```

Extractor Installation

Login with root or equivalent privileges.

Symantec strongly recommends that users remove all previous versions of Extractor.

cd to location of old Extractor binary

Old versions of Extractor are installed in `/usr/local/bin` for Linux; the `/usr/bin` directory; or another user specified location

rm extractor

Remove the old Extractor binary

rm -rf /home/user-directory/.extractor/ConfigFile.ini (OPTIONAL)

This file removes your old Extractor configuration settings

cd Extractor

make install

This command will copy Extractor binary files from the source directory to `/usr/local/extractor` creating the following directory structure:

```
/usr/local/extractor/bin/extractor  
  rules/      } rules files  
  bin/       } extractor binary and parser .so files
```

A symbolic link is created from `/usr/local/extractor/bin` to `/usr/local/bin/extractor`

NOTE: OpenBSD, Free BSD and some other platforms may require the use of gmake. The Extractor install requires GNU make 3.79.

Complete the installation by issuing this command:

```
/usr/local/bin/extractor -c (if /usr/local/bin is not in your PATH)  
extractor -c
```

This command creates the hidden sub-directory `.extractor` in the user's home directory and then creates the blank configuration file: **ConfigFile.ini** You must configure this file for Extractor to function.

You must now configure Extractor profiles for each sensor.

Extractor Configuration

Change to the hidden Extractor sub-directory `.extractor`

cd /home/user-directory/.extractor

Use your favorite text editor to open and modify the **ConfigFile.ini** file

The **ConfigFile.ini** configuration file is divided into 2 sections: **globals** and **profiles**. Each component is described in more detail below, but the **[globals]** section configures Extractor itself and the **[profile]** section details individual sensor configurations. To add and configure additional sensors, duplicate a properly configured **[profile]** section then modify the copied **[profile]** section.

[globals] Configuration Parameters

EnableStatusLogging="0"

Set to "1" to turn on Extractor status logging. If you activate status logging you must specify a location for the Extractor status log using the **StatusLogFile** parameter.

The next group of parameters defines how Extractor connects to the upload server through a proxy.

EnableProxy="0"

Set to "1" to connect through a proxy.

ProxyHost=""

Enter the DNS name or IP address of the proxy, i.e., "fwall.yourdomain.com" or 192.168.0.1

ProxyPort=""

Specify the connection port to the proxy. Port 3128 is a common proxy connection port value.

ProxyEnableAuth="0"

Set to "1" when the proxy requires authentication.

ProxyUser=""

Enter the authorized proxy users' name "jchosely"

ProxyPassword=""

Enter the authorized proxy users' password "password"

The next parameters specify the Analyzer upload account information.

AnalyzerUsername="analyzer-user"

The Analyzer user account for the upload.

AnalyzerPassword="analyzer-password"

The user account password.

StatusLogFile="/home/user-directory/.extractor/logfile"

Specify the location for the extractor status log when **EnableStatusLogging** is set to "1"

UploadEnableEventLimit="0"

Set to "1" to limit the number of events in one upload.

UploadEventLimit="10000"

Limit the number of events Extractor will upload at one time by entering a whole number. 10000 is a reasonable starting point.
UploadEnableEventLimit must be set to "1" to use this parameter.

UploadReportErrors="1"

When set to "1," Extractor will log a connection failure to another Symantec server. The log entry specifies the time of the failure and your Analyzer username to assist technical support in troubleshooting the connection issues. No entry is logged for connection issues on your local network.

UploadEnableRetry="1"

Set to "0" to disable retries.

UploadRetries="10"

Set the number of retries after a connection failure.

UploadEnableCompression="1"

Set to "0" to turn off log file compression.

UploadSSL="1"

Set to "0" to upload log files without SSL. Login authentication still requires SSL, but the log is sent in the clear.

The "**AlternateHost**" parameters should be used only at the direction of Symantec technical support.

UploadEnableAlternateHost="0"

Set to "1" to upload to a special location.

UploadAlternateHostName=""

Enter the "hostname" provided by Symantec.

ScheduleFreq="5"

Specify the number of minutes between Extractor uploads.

NOTE: The maximum value for **ScheduleFreq** is 1440 minutes which limits uploads to once a day.

SOPath="/usr/local/extractor/bin"

This provides the path to the shared object files for parsers. By default, this is the path where Extractor is installed.

[profile=] Configuration Parameters

The profile section defines differences in firewalls and Intrusion Detection Systems acting as Analyzer sensors. To add a new sensor, copy and modify an existing sensor profile using your favorite text editor.

[profile="ids-sensor1"]

Enter a profile name for the sensor. Unique profile names are required.

IDSRules="/usr/local/extractor/rules/snort.rules"

Specify the complete path and the .rules file that defines the sensor device. These device definitions are in the /usr/local/extractor/rules directory.

DataSource1="/var/log/snort/alert"

Enter the complete path to the sensor log files.

DataSource2=""

The secondary DataSource is provided for NetProwler and Dragon systems as well as for future use.

DataSourceUsername=""

Enter the username required to access the sensors' log files; this is usually not required.

DataSourcePasswd=""

Enter the password required to access the sensor log files. This is necessary only if a **DataSourceUsername** value was required.

StripList=""

Anonymize a network or device by entering an address in CIDR notation or just an IP address. Multiple addresses may be specified using a "," or ";" as a delimiter between the addresses.

EnableSchedule="1"

Set to "0" to require manual uploads of sensor data. The frequency of the Extractor uploads is specified in the [globals] section.

Time="gmt"

Valid values are: "local", "GMT", or "TZ" If "TZ" is specified, an offset must be specified for the **GMTOffset** parameter. For details on using the "TZ" parameter, see the "extractor-tz-offset" file.

GMTOffset=""

Enter your GMT offset.

Extractor Command Line Usage

extractor

Show the command line options available (help text).

extractor <options> <command-switch> <-u [Analyzer-username] -p [password]>

This is the basic command line format. The username and password may be supplied by the **ConfigFile.ini**.

extractor <options> -U [profile-name] <-u [Analyzer-username] -p [password]>

Upload log data from a specific sensor.

extractor <options> -L [xml file] <-u [Analyzer-username] -p [password]>

Upload an xml file.

extractor <options> -X [profile] -o [output_file.xml]

Save the log data of a specific sensor to an xml file.

extractor <options> -D

Run Extractor in Daemon mode using the configured schedule.

extractor -c

Write a blank configuration file to: /home/user-directory/.extractor/ConfigFile.ini

<options>

-a <config file> Specify a path to an alternate configuration file when you do not want to use the default.

-q Quiet operation prints only error messages to the screen

-f Ignore saved sensor timestamps for this profile and start reading from the beginning of the log file. (used with **-X** or **-U**)

-n Do not update sensor timestamps for this profile (used with **-U**)

-d Write all status log messages to the syslog; verbose logging. The default behavior is to write only important messages and errors. (used with **-D**)

-o Allows specification of an output file name. (used with **-X**)

-t <timestamps file> Specify path to the saved timestamps file. This option is used in conjunction with **-D**, **-X** and **-U**

-w <pid file> Write the process ID to a file

Running Extractor in Daemon Mode

When started, Extractor uploads all profiles you have selected for scheduling with the profile configuration option **EnableSchedule="1"**. Extractor continues these uploads based on the profile configuration option **ScheduleFreq**.

During operation, Extractor logs to your syslog user log. The log entries include Extractor's pid [Process ID]. While in daemon mode, Extractor handles the following signals:

- **HUP** [Hangup Signal]

Send a HUP to the Extractor process when:

- Any of the logfiles your profiles point to are rolled or renamed.
- You change your configuration file.

When sent a HUP, Extractor will finish the current round of profile uploads; close all log files; reload your configuration; and then restart the upload cycle.

- **TERM** [Terminate signal] or QUIT [Console quit signal]

Send a TERM to the Extractor process when you want it to exit cleanly. To send this signal to the Extractor process:

BSD/Linux:

```
killall -HUP extractor    (to send a HUP)
killall extractor        (to send a TERM)
```

Solaris:

```
pkill -HUP extractor     (to send a HUP)
pkill extractor          (to send a TERM)
```

NOTE: It may be necessary to use the assigned process ID to terminate the Extractor process when using pkill.

HELP WITH DEEPSIGHT EXTRACTOR

If you have any comments or questions regarding Symantec DeepSight Extractor, please email extractor@symantec.com.