



Export enVision IPDB Data

for RSA NetWitness® Platform 11.x



Copyright © 1994-2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2020

Contents

| | |
|---|----------|
| IPDB Export Utility User Guide | 4 |
| Prerequisite: Export Parsers | 4 |
| Setup Requirements | 4 |
| IPDB Export Tool Details | 5 |
| Troubleshooting | 5 |
| Using the GUI | 5 |
| Using the Command Line | 7 |
| Import Data into NetWitness Platform | 8 |
| Configure Log Decoder | 9 |
| Configure Archiver | 9 |
| Import Data to NetWitness Platform | 11 |

IPDB Export Utility User Guide

In conjunction with the release of NetWitness Platform 11.4.1, RSA is providing a tool that can export event data from an enVision IPDB, so that you can then import that data into an 11.x Archiver or Log Decoder. This allows you to retain access to this enVision data after you migrate to NetWitness Platform 11.x, and thus allows customers to comply with their audit regulations.

Depending on your needs, note the following:

- You don't need to report on any of the exported data: you may occasionally need to search through it to find some specific data. In this case, you do not need to import it into NetWitness Platform.
- You need to access the exported data and you may want to report on it. In this case, you need to import the data into a Log Decoder, then save the data to an Archiver. At this point, after the data is on the Archiver, you can remove the Log Decoder you are not using it for anything else.

Prerequisite: Export Parsers

Before you use the IPDB Export tool, you should backup existing parsers from 10.6.x LogDecoder (all, or particularly any custom parsers you have built). Then, upgrade your NetWitness Platform stack to version 11.x and copy the previously backed up parsers to a new 11.x Log Decoder.

Perform the following steps:

1. On your 10.6.x SA Node, copy the parser folders, which are located in `/etc/netwitness/ng/envision/etc/devices`, into another folder or location.

Note: You can choose to copy only your custom parsers or any of the others as well. RSA recommends you copy the information somewhere off your SA stack, to ensure the parser information is not damaged nor destroyed during the upgrade process.

2. Upgrade your stack from Security Analytics 10.6.x to NetWitness 11.x.
3. Copy the parser information onto a NetWitness Platform 11.x Log Decoder, into `/etc/netwitness/ng/envision/etc/devices`.
4. Restart the Log Decoder service and verify that the parsers you copied over are enabled.

Continue with the remaining procedures in this document, to extract the data from your IPDB database and then inject it into your NetWitness Platform.

Setup Requirements

Since the IPDB Extractor utility runs on a Windows platform, to set up the IPDB data extractor utility, you need the following:

- Any of the following physical or virtual systems:
 - Windows 2008 R2 SP1 64-Bit Server,
 - Windows 2012 Server, or

- Windows 2016 Server, or
- Windows 2019 Server
- A minimum of 20% free disk space. For example, you need at least 20 GB of free space if your system drive is 100 GB in size.

IPDB Export Tool Details

The **IPDBExportUtility.exe** file is available for download from RSA Link. You can run the tool using either a command-line interface or a graphical UI.

Note: RSA recommends using a read-only IPDB database with this tool.

- To run the tool using the GUI, double-click the executable file
- To use the command-line interface, run the tool from a command prompt. You can use the **-h** flag to list the available options.
- Expected Rate for export is approximately 30 GB per hour but can vary depending on your environment (number of CPUs, network latency, and so on).

Troubleshooting

Note that there is currently no bookmark support. So, if the data export process is going for a long period (over a day, for example), or if there is a crash or a system reboot while the extractor utility is running, then we recommend restarting the export process from beginning.

Using the GUI

After you open the GUI, you see the following window:

The following table describes the available options.

| Option | Description |
|---------------------------------|---|
| IPDB Data Folder | Specify a folder containing IPDB database. You must provide the path to a valid IPDB database. |
| Device Selection | Select a list of devices to be exported. Optional: by default, all devices under a selected folder are exported. |
| Regex Filter | Export selected events matching a regex pattern. This field is optional. |
| Exclude messages based on Regex | If selected, matched events are excluded from the export. |
| Time Filter | Export events generated within a specified date range. Optional: enter a date in YYYYMMDD format. |
| Output Folder | Specify a directory to store exported event data. |

| Option | Description |
|-----------------------------------|---|
| Message Format | <p>Select the output event format from the following:</p> <ul style="list-style-type: none"> • zconnector (default): use for importing into NetWitness (for example a Log Decoder) • simple: syslog like format, used for simple viewing • syslog: RFC5424 format, used for advance viewing and to import to database (for example an Archiver). |
| Work Threads | <p>Sets the number of processing threads between 1 and 64 to use for exporting. If your hardware supports it, more threads will help get the work done faster. Default value is 8.</p> <p>Note: The work is divided by event sources. Thus, more threads do not help speed the export unless you have a large number of event sources.</p> |
| Replace Contents of Output folder | <p>If selected, running the tool removes all files in the target output directory before starting export.</p> <p>If you do not check this box, and the folder is not empty, the export could append information to existing files, and thus re-export the same data more than once.</p> <p>This option is useful if you have chosen the wrong options during a previous export, and want to wipe all previously exported data in the output directory before you change the options and try again (so you can start with a clean slate).</p> <p>In most cases, RSA recommends using an empty output folder.</p> |
| Limit Output File Sizes to 4 GB | <p>Limits output file size to 4 GB, which makes it easier to manage importing into NetWitness Platform.</p> <ul style="list-style-type: none"> • If this option is selected, the export process creates multiple files for an event source that has more than 4 GB of data, where each file is under 4 GB in size. • If this option is cleared, only a single file per event source is created, and thus may exceed the 4 GB threshold. |
| Export | Click the Export button to begin the export process. |
| Pause | If the tool is running, you can pause the current export process by clicking this button. |
| Message Preview | <p>Enables sample preview of up to 10000 events, depending on the size of the events.</p> <p>Note: The preview window size is 2,000,000 (2 million) characters.</p> <p>The relatively small result set available in the preview area means you could use this output window to see the result of a search on the data for a particular username or IP address via a regex string.</p> |

Using the Command Line

Below is a screen shot of running the tool with the **-h** (help) flag.

```
C:\Users\Administrator\Desktop>IPDBExportUtility.exe -h
C:\Users\Administrator\Desktop>

Usage : IPDBExportUtility.exe [options]

Options:      Description
-----      -
-input       Input directory location where lsnode data is located
              - Can be a subdirectory of lsnode to filter by devicetype or device

-output      Output directory location where output and logs will be written
-simple      Output will be in a simple syslog like format, used for simple viewing
-zconnector  Output will be in a zconnector format, used for importing into NetWitness (default)
-syslog      Output will be in a RFC5424 syslog format, used for advanced viewing
-threads     Number of output processing threads, range is 1-64, default is 16

-starttime   Time filter starting day in YYYYMMDD format
-endtime     Time filter ending day in YYYYMMDD format

-regex       Regular expression to match message value on
-exclude     Enable excluding messages matching the regular expression

-preview     Enables the preview window
-clean       Cleans the output directory of all data before starting
-limit       Limit output file size to 4GB
-export      Starts the export process, omit this option to populate dialog only
-exit        Enables auto exit after export is completed
-version     Version of this utility

-help        This CommandLine help. Also available with -h and -? options
```

Note: The **-input** and **-output** flags require absolute path to directories.

The following are some example commands:

- Export logs in simple format:

```
IPDBExportUtility.exe -input C:\lsnode\lsnode -output C:\Exported_CMD\1_Simple -simple -export
```

Note the absolute paths specified for the input and output folders.

- Export logs generated between a date range in YYYYMMDD date format:

```
IPDBExportUtility.exe -input lsnode\lsnode -output Exported_CMD\1_Simple -simple -starttime 20000101 -endtime 20200124 -export
```

Exports data that has timestamps between January 1, 2000 until January 24, 2020.

- Export log data in **zconnector** format:

```
IPDBExportUtility.exe -input C:\lsnode\lsnode -output C:\Exported_CMD\2_zconnector -zconnector -export
```

- Export log data in **zconnector** format, and auto exit after the export process finishes:

```
IPDBExportUtility.exe -input C:\lsnode\lsnode -output C:\Exported_CMD\2_zconnector -zconnector -export -exit
```

Import Data into NetWitness Platform

RSA recommends using either a dedicated Log Decoder or Archiver (preferable a VM) to import your IPDB event data.

Configure Log Decoder

Before you inject your IPDB data into a Log Decoder, you need to set the log collection time to the value in the TCP Connector header of the IPDB-extracted event data.

1. Connect to the Log Decoder REST API: `http://LogDecoder_IP-Address:50102`
2. Navigate to `decoder > parsers > config`.
3. Change the `lc.ctime.meta` value from **off** to **session**.
4. Click **Set** and verify that **Success** appears.


| | | |
|--|---------|-----|
| Header Prioritization Shortcut Score (header.prioritize.shortcut.score) (*) | 2900 | Set |
| Header Threshold Minimum Score (header.threshold.min.score) (*) | 1000 | Set |
| Header Threshold Percent (header.threshold.percent) (*) | 5 | Set |
| Log collection context meta generation (lc.context.meta) (*) | off | Set |
| Log Collector collection time meta generation (lc.ctime.meta) (*) | session | Set |
| Lua Debugger Auto Detach (lua.debugger.auto.detach) (*) | yes | Set |

Success

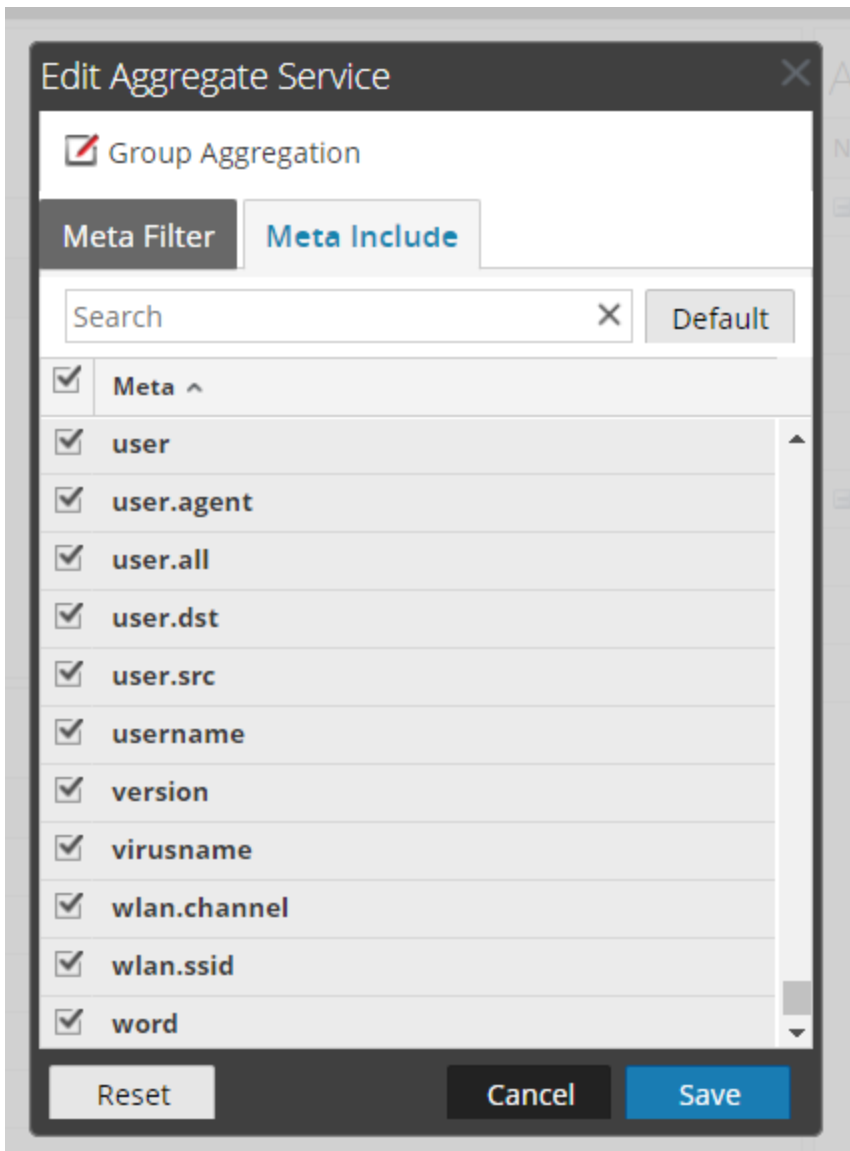
Configure Archiver

Before you inject your IPDB data into an Archiver to use in reporting, you need to set up the correct meta key information.

To add meta keys to Log Decoder on Archiver:


1. Go to **Admin > Services**.
2. Find an Archiver service and select  > **View > Config**.

- For the Log Decoder that is aggregating, edit the service to include the meta keys by selecting all keys.



- Click **Save**.
- Make sure that the included meta keys are seen after you click **Save** and **Apply**.

Next, you need to copy the information from `index-concentrator.xml` file on the Concentrator.

- Go to **Admin > Services**.
- In the **Services** view, select a Concentrator, and select  > **View > Config**.
- Click the **Files** tab and select the `index-concentrator.xml` file from the drop-down menu.
- SSH onto the Archiver, go to `/etc/netwitness/ng`, and modify the `index-archiver.xml` file so that its contents are identical to the contents in the `index-concentrator.xml` file.
- Restart the Archiver service.

6. Ensure the following:
 - Your Reporting Engine has the Archiver as a data source.
 - Your Log Decoder capture is on.
7. Use Log Player to inject the IPDB data onto the Log Decoder.

Now, you can go to **Monitor > Reports** to report on your IPDB data.

Import Data to NetWitness Platform

To import your data, use the **NwLogPlayer** utility. The following is an example command:

```
NwLogPlayer -s LD-IP -r 3 -f filenameExportedData
```

where:

- *LD-IP* is the IP address of your NetWitness Platform Log Decoder.
- *filenameExportedData* is the path and name of the file to which you exported your IPDB data.