RSA NETWITNESS® PLATFORM

RSA NetWitness Log Parser Tool

for Version 1.1

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase 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 www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

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. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

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.

Contents

Introduction

This document describes RSA® NetWitness Log Parser Tool, Version 1.1. RSA recommends reading this document before installing and using the NetWitness Log Parser Tool.

Product Description

The RSA NetWitness Log Parser Tool (NwLPT) enables content users to build and modify NetWitness log parsers in an offline environment without affecting NetWitness. The Log Parser Tool enables analysts to create custom parsers for critical or custom sources in their environment that are not currently parsed in NetWitness.

The NetWitness Log Parser Tool enables you to create a new log parser or customize an existing log parser with a simplified User interface.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA® NetWitness Log Parser Tool User Guide 1.1	https://community.rsa.com/docs/DOC-85016

Installation

Installation Instructions for New Users

You can install the RSA NetWitness Log Parser Tool standalone on a Microsoft Windows or MacOS computer. Download the Windows and MacOS versions of the NetWitness Log Parser Tool from the following location and running the installer locally on your computer:

https://community.rsa.com/docs/DOC-85202

If you are using an older version of the tool, uninstall the previous version and then install this version.

What's New

RSA NetWitness Log Parser Tool 1.1 includes the following new features:

Log Parser Customization

Log Parsers can be customized by adding new parser elements or modifying existing elements. On customization, you can save it as a separate custom parser file, such that the base parser can be updated independently and customizations can be applied on top of it.

VALUEMAPS are Editable

You can now edit, insert or delete VALUEMAPS.

New TAB Delimiter in TAGVALUE

A new delimiter **TAB** is introduced to enable easy parsing of event logs using the **<TAGVAL>** format. You must enter "TAB" in the **TAGVALUE** field.

Retaining Comments

The comments in the parser XML file is now retained, in case they are written by content authors to add additional coding context.

Retaining Parser Rules

The Dynamic Parsing technology introduced in 11.1 allows Parser Rules to be added to parsers. All the existing parser rules are retained by the tool.

Version 1.0 features

RSA NetWitness Log Parser Tool 1.0 includes the following features:

Periodic Saving

All parsers opened in the tool are auto-saved to a temporary location at an interval of 30 seconds. The last saved time is displayed on the top right section of the tool.

Cloning Headers and Messages

All defined Headers and Messages can now be cloned. This allows easy parser development for cases where a similar pattern is needed for a Message or Headers.

Resizing Message ID and Message Group

Message IDs and Message Groups can be of different sizes, which allows resizing them as needed.

Validation Checks for Headers and Messages

Multiple validation checks have been added to ensure the parser follows the right syntax and best practices. For example, an empty Header ID is not allowed, only 1 MessageID allowed per Header definition, creation of messages is not allowed unless the MessageID and Payload are defined.

Parser can be Exported as a Live Resource

The parser can be exported in a format that can be consumed by the Live Service in NetWitness. This allows easy deployment of parsers on multiple Log Decoders simultaneously.

Improved MessageID Concatenation Box

The MessageID concatenation box has been improved to add Literals and Meta keys easily.

Usability and User Experience Improvements

Several updates have been made to improve the overall user experience.

- Create Header/Create Message buttons are enabled based on work flow.
- Improved Event Category and Device Class selection.
- Landing Page now points to the parser and the logs directly.
- Allow changing the log file.
- Display log file name and path.

Graceful Error Handling

- Error/Exception handling added to multiple parts of the tool.
- Appropriate user readable error messages are displayed. For example, read-only files cannot be edited, you cannot open a non-compliant parser.

Redesigned Workflow to Create Headers and Messages

- Dedicated context options are added to create MessageIds, Payload, and Payload Rewinds.
- Improved the overall work flow to create Headers and Messages in a step-by-step format and direct user to the next step.

Loading Latest Table Map/Table Map Custom Through Log Parser Tool

Allow loading the latest Table Map available in Live, or uploading Custom Table Maps applicable to the customer’s environment through the Log Parser tool.

Redesigned Login Work Flow

The Login work flow now allows either creation of a new parser, or modifying an existing parser with one step to add all required fields to create or edit a parser.

Context Menu to Perform Operations on Headers and Messages

Added Context Menu with shortcuts to perform regular operations such as Reorder, Delete, and Duplicate Headers and Messages.

Removed All Obsolete enVision Functionality

Loading an existing parser now removes enVision-specific functionality arguments, such as **tableid**, **parsedef**, **level**, **summary**, **sumdata**, and so on.

Fixed Issues

This section lists issues fixed in RSA NetWitness Log Parser Tool 1.1 since the last major release.

Tracking Number	Description
SACE-8689	When you create new literals or variables and save them, they are replaced with underscores.
SACE-8712	When new parsers are created, the event category is saved in the scientific format in the parser XML file. This prevents the parser from successfully parsing the messages resulting in "unknown" messages.
SACE-8840	If you areusing an older version of Intel driver on Windows 10 and update it to version 22.20.16.4836, the File Menu is missing.

Known Issues

This section describes issues that remain unresolved in the version 1.1. Wherever a workaround or fix is available, it is noted or referenced in detail.

Description: Log Parser Tool does not launch the application after installation

Tracking Number: ASOC-46707

Workaround: You can search for the Log Parser Tool in the Start menu and run the application.

Version 1.0 Known Issues

Description: Close icon is not visible in the Parser tab on a MacOS machine.

Tracking Number: ASOC-45687

Workarounds: From the main menu, select **File > Close**.

You can use the following shortcut keys to exit from the Parser tab:

- Windows: **CTRL+W**
- MacOS: **CMD+W**

Description: In Windows 10, the header and message section cannot be moved.

Tracking Number: ASOC-45675

Workaround: None.

Description: Does not work on Windows Server 2008 VMs that do not have a video card backend.

Tracking Number: ASOC-23434

Workaround: None.

Description: Sometimes Payload Rewind rectangle periodically overlaps at the end of a header on MacOS.

Tracking Number: None.

Workaround: None.

Description: Vertical scrolling of events in the Log Data section may not be smooth when you are using the Tools scroll bar.

Tracking Number: ASOC-17707

Workaround: Use your mouse to scroll in the Log Data section.

Description: *Invalid empty Header/Message node is created when Header or Message is deleted from the Detail View*.

Tracking Number: ASOC-32031

Workaround: This is a user interface issue only. Click on a different Header/Message, then click on the invalid Header/Message to get rid of the empty Header/Message node.

Description: Log Parser Tool dialog box text may overflow if the Display is set to Medium (125%) or Larger (150%) on a Windows System".

Tracking Number: None.

Workaround: Follow the steps below.

1. Click **Start** button in Windows.
2. Select **Control Panel**.
3. Click **Appearance and Personalization**.
4. Click on **Display**.
   A page opens that displays three radio buttons: **Smaller**, **Medium**, and **Larger**.
5. Select the **Smaller** radio button to reduce the size of the text and click **Apply**.
6. Restart your computer for the change to take effect.

Contacting Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness Suite product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com/
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Community	http://www.emc.com/security/security-analytics/security-analytics.htm
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Revision History

Revision	Date	Description
1.0	December 2017	Initial Product Release
1.1.	July 2018	Final Draft