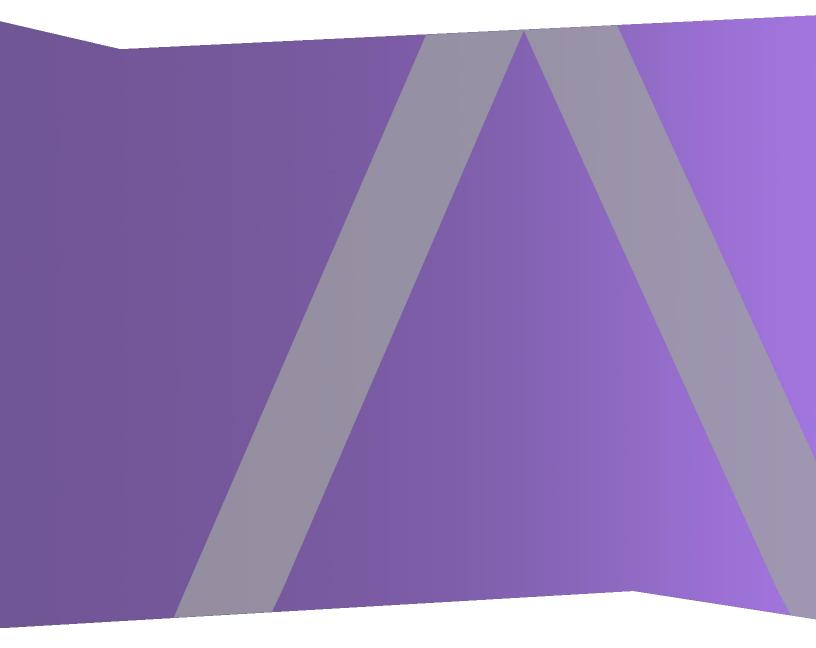


Log Parser Customization Guide

for RSA NetWitness® Platform 11.3



Copyright © 1994-2019 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.

August 2019

Contents

Log Parser Rules Tab	4
Introduction	4
Log Parsers Panel	6
Details Panel	7
Rules Panel	10
Disable log Parser Rules	11
Add or Delete a Log Parser	12
Add a Log Parser	12
Delete a Log Parser using the UI	12
Delete a Log Parser Manually	12
Add Dynamic Log Parser Parameters	13
Add or Delete a Log Parser Rule	14
About Log Parser Rules	14
Custom Log Parser Rules	14
Guidelines for Custom Rules	14
Default Log Parser and Log Parser Rules	16
Default Log Parser	16
Highlight Matching Patterns	17
Highlight Overlapping Patterns	19
Use Cases	21
Use Case 1: On Board a New Event Source	21
Use Case 2: Modify an Existing Parser	21
Extend an Existing Log Parser Example	22
Task Overview	
Notes	22
Add the Log Parser	
About Custom Rules	23
Add Rules and Deploy	23
Regex Values	
Appendix A: Select the Reference Log Decoder	27
Appendix B: Move Log Parsers to Production	28
Appendix C: Troubleshooting and Limitations	
Troubleshooting	
NwLogPlayer	
Limitations	

Log Parser Rules Tab

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.1 and later.

Introduction

This tab contains details about the rules for the default log parser, as well as any other custom rules and log parsers that have been defined.

The *default log parser* parses logs that do not match any installed log parsers. The information contained in such a log is processed against the default log parser's rules, and metadata is then extracted by those rules and is available for Enrichment, Investigation, Reporting, and Alerting. This provides immediate visibility into logs from custom or unsupported sources.

You can also add or extend a log parser. For example, you may need to parse certain fields differently than in the manner provided by the log parser for a particular event source. You can add rules that change the way meta information is extracted from the logs for the event source.

Finally, you can view and test sample log messages and rules for your log parsers, including the default log parser.

The Log Parser Rules tab displays information about log parsers that use dynamic log parser rules. This includes the following:

- The default log parser that parses logs that are not associated with a particular log parser
- Native XML-defined device parsers that have been extended with dynamic log parser rules, and
- User-created custom device parsers used to parse unsupported custom event sources

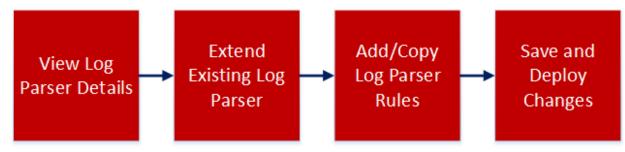
This tab contains the following information:

- You can view the rules for a particular event source type, including the default parser.
- You can view the Names, Literals, patterns, and meta for each configured log parser.
- You can add log parsers
- You can add, edit, and delete custom rules for log parsers

To access this tab, go to **CONFIGURE > Log Parser Rules**.

Workflow

This workflow shows processes available from the Log Parser Rules view.



What do you want to do?

Role	I want to	Documentation
Administrator	*View log parser rules.	Default Log Parser and Log Parser Rules
Administrator	*Add, edit or delete a log parser rule (version 11.2 and later)	Add or Delete a Log Parser Rule
Administrator	*Add or remove a log parser (version 11.2 and later)	Add or Delete a Log Parser

*You can perform this task here.

Related Topics

Default Log Parser and Log Parser Rules

Quick Look

Note: The list of log parsers is based on the first Log Decoder that is installed or registered by the Orchestration Server. If you have more than one Log Decoder, this tab only lists log parsers that have been configured on the first one.

The Log Parser Rules tab organizes and displays information about the configured log parsers in your system. This tab consists of three panels: Log Parsers list, Details for the selected log parser, and Rules for the selected log parser.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE	ADMIN		(1) admin	n
Live Content Incident Rules	Respond Notifications	ESA Rules Subscriptions	Custom Feeds Log F	Parser Rules	
Log Parsers	carbonblack 👩	Deploy Save Discard Change		Rules	
Add Parser Delete	Test			Add Rule Delete	
default	TOKENS	VALUES	META	Test	Â
Cisco PIX Firewall	Please Enter New Token 🔶	REGEX PATTERN	FULL CAPTURE	Status	
O Carbon Black	'	`	port X v	Client Domain	
	IDS:	TYPE regex	FIRST CAPTURE	Destination Domain	
		MATCHING This matches Regex	None v	Source Domain	
		PATTERN	SECOND CAPTURE	Any Domain	
		\w+	None v	Client Username	
			THIRD CAPTURE	Username	
			None 🗸	Destination Port	
				Source Port	
				Any Port	
	Sample Log Messages (Test (up to 60K characters of log messages)		Destination MacAddress	
				Source MacAddress	
	date=2017-08-12 type=t	raffic subtype=violation user=ma	att status=deny src=192	Any MacAddress	
	Matr 5 2018 15 55 49 eta	nitch : %ACE-4-4000: IDS:1000 IP	Ontion Bad Ontion user	Source IP or IP:Port	
	1 May 0 2010 10100115 54		opoion bad opoion abor	Destination IP or IP:Port	
	\$IIS-4-440: 2017-08-12	13:53:34 192.170.28.192 - W4S31	url=https://test.doma	Any IP or IP:Port	
	Dec 20 13:20:20 instan	cel info mod=mail from=matt@rsa.	.com to=alex@dell.com	Source Email Address	
				Destination Email Address	
			•	· · m·	*

Log Parsers Panel

Log Parsers	•
Add Parser Delete	
default	
test	ľ
Cisco PIX Firewall	
	•
	•

he Log Parsers Panel lists the configured log parsers.

- Until you add rules to existing XML parsers on your reference Log Decoder, (or add a new, custom log parser) only the **default** parser is listed here.
- Select a specific log parser to view its details in the Details and Rules panels.
- Click Add Parser to open the Add Dynamic Log Parser dialog box.
- Click **Delete** to delete a log parser.

IMPORTANT: Once you deploy a log parser, you can no longer delete it through this interface. The **Delete** button is not available for deployed parsers. To manually delete a log parser, see <u>Delete a Log Parser Manually</u>.

The Add Dynamic Log Parser dialog box allows you to add a custom log parser.

Add Dynamic Log Parser	×
Use dynamic parser rules to create a new dynamic log parser or add to an existing log parser. SELECT LOG PARSER NEW	~
DEVICE TYPE scooterpod	
DEVICE DISPLAY NAME Scooter's iPod	
DEVICE CLASS	~
CLONE DYNAMIC PARSER RULES FROM DEFAULT ×	~
Add Parser	

When you are	adding a	log parser,	the fo	llowing pa	rameters are	available.
2	0					

Field	Details
SELECT LOG PARSER	Select NEW, or choose an existing log parser.
	By choosing an existing log parser, you can add rules to that parser, essentially extending its parsing capabilities.
	Note: If you select an existing log parser, the remaining fields are auto-filled based on the values for selected log parser.
DEVICE TYPE	Enter a string to define the device type. The name must be between 3 and 30 alphanumeric characters (including underscores), and must not match the name of any existing log parsers.
DEVICE DISPLAY NAME	Enter the display name for the log parser.
NAME	Note: The display name must be 64 characters or fewer, and must not match the name of any other device display name.
DEVICE CLASS	Select a device class.
CLONE DYNAMIC PARSER RULES FROM	Leave blank to start with no rules, or select one of the existing log parsers to clone its rules.

Details Panel

The details panel shows the three pieces for the selected rule:

- **Tokens:** one or more tokens to match in the message. For example, the Any Port rule looks for the following strings to match against: **port** , **port** , **port** , **and** others.
- Values: the value that follows the token. This is a string that is captured as meta. For example, assume a log contains the following string:

The Any Port rule has a token that matches "port". When it encounters that string, it assigns the token value, "12345" to a meta key.

• Meta: the meta keys to which the value is mapped. For example, the Any Port rule maps the port value to the **port** meta key.

Essentially, a rule says, "when you are parsing a message, if you match one of my tokens, assign the value that follows the token to the meta key that I want it stored as."

The bottom section of the Details panel contains sample log messages, and how they would be parsed for the selected log parser.

port 12345

Ciscopix Deploy Test1 2 токемs 3 Please Enter New Token + server	VALUES IPV4 ADDRES TYPE MATCHING	Discard Changes	The second secon
n@test.com from 10.100 Apr 29 2010 03:15:34 p	itch : %ACI .229.59 to vg1-ace02:	224.0.0.22 on port 12345. *ACE-3-251008: Health prod	tion Bad Option List by user admi be failed for server 218.83.175.7
0-00-00-00.			domain google.com with mac 06-0
 discarding changes. 2 Displays the name of this parser. 3 Displays the list of the determined by the type and determined by the type custom regular expression. 	This value f the select okens defin d pattern of pe of the se ession.	ed for the selected rule. E the value matching for the selected value. You can also u	lifferent parser. when you select a different rule for selected parser. The values here are use the Regex option to define a
here are determined6 Displays a sample lo	by the sele og message,	cted Rule. , and highlights strings that n	aps any matched tokens. The values natch tokens in the selected log preview how the selected parser will
Note: The sample syou paste in sample			anged or updated, as well as when

For example, consider the following scenario:

- The default parser is selected.
- The Any Domain rule is selected.
- The Tokens matching list displays all of the tokens that are matched when found in a log message: **Domain, Domain Name, domain, ADMIN_DOMAIN**, and so on.
- The Meta list displays the NetWitness meta to which the value for the token is mapped: domain.

So, let's say the sample log message area has the following text:

```
Below are sample log messages:
May 5 2010 15:55:49 switch : %ACE-4-400000: IDS:1000 IP Option Bad Option
List by user admin@test.com from 10.100.229.59 to 224.0.0.22 on port 12345.
Apr 29 2010 03:15:34 pvg1-ace02: %ACE-3-251008: Health probe failed for
server 218.83.175.75:81, connectivity error: server open timeout (no SYN ACK)
domain google.com with mac 06-00-00-00-00.
```

default 👩 Deploy Rules Add Rule Any Domain Test1 TOKENS VALUES мета Client Domain [RSA] FULL CAPTURE HOSTNAME Destination Domain [RSA] domain Source Domain (RSA) ТҮРЕ Hostname 面 Any Domain [RSA] Ü MATCHING This matches Hostname Client Username [RSA] Ü Username [RSA] Ü Destination Port [RSA] Ü Source Port [RSA] Ü Any Port [RSA] Destination MacAddress [RSA] Source MacAddress [RSA] Below are sample log messages: Any MacAddress [RSA] ource IP or IP:Port [RSA May 5 2010 15:55:49 switch : %ACE-4-400000: IDS:1000 IP Option Bad Option List by user admi to 224.0.0.22 on port n@test.com from 10 Destination IP or IP:Port [RSA] Any IP or IP:Port [RSA] Apr 29 2010 03:15:34 pvg1-ace02: %ACE-3-251008: Health probe failed for server 218.83.175.7 Source Email Address [RSA] 5:81, connectivity error: server open timeout (no SYN ACK) domain google.com with mac 06-0 0-00-00-00-00. Destination Email Address [RSA] URL [RSA]

In this case, the Sample Log Message area looks like this:

Note that some strings are highlighted, and that there are two "pairs" of highlight colors:

- Dark blue and light blue highlighting is applied to the strings that match the currently selected rule.
 - Dark Blue highlighted strings match a token in the selected rule. In this case, **domain** is the token that is matched for the **Any Domain** rule.

- Light Blue highlighted strings are the values that correspond to the tokens in dark blue. For example, **google.com** is highlighted in light blue, because it corresponds to the **domain** token.
- Orange and yellow highlighting is applied to the strings that match rules for the current parser that are *not* currently selected.
 - Orange highlighted strings match a token in a rule that is not currently selected.
 - Yellow highlighted strings are the values that correspond to the tokens in orange. For example, the **user** token matches the **Username** rule (which is not currently selected).

In this example, the **domain** meta would be assigned a value of **google.com** for this log message, if it was parsed using the default log parser.

Rules Panel

The Rules panel displays the list of rules used by the selected log parser. When you select a rule, you change the values that are displayed in both the **Tokens** and **Values** areas of the panel.

Rules
Add Rule Delete
Test1
Client Domain [RSA]
Destination Domain [RSA]
Source Domain [RSA]
Any Domain [RSA]
Client Username [RSA]
Username [RSA]
Destination Port [RSA]
Source Port [RSA]
Any Port [RSA]
Destination MacAddress [RSA]
Source MacAddress [RSA]
Any MacAddress [RSA]
Source IP or IP:Port [RSA]
Destination IP or IP:Port [RSA]
Any IP or IP:Port [RSA]
Source Email Address [RSA]
Destination Email Address [RSA]
URL [RSA]

Note the highlighted rules:

- The currently selected rule is highlighted in blue.
- Other rules that match tokens in the sample log message area are highlighted in orange.

Other notes for the Rules panel:

• RSA rules (the rules provided out-of-the-box for each log parser) are identified by **[RSA]** following the rule name.

You can copy these rules when adding a new log parser, and then change them as needed.

- The **Delete** button is only available for custom rules; for RSA rules, it is greyed out.
- Use the Add Rule button to add a custom rule.

Disable log Parser Rules

You can disable log parser rules, so that none of them are processed by the Log Decoder. You might have your log parsers working as you like, and do not want any extra processing that you do not need. You disable them from the reference Log Decoder.

- 1. Go to**ADMIN > Services**.
- In the Administration Services view, select the Decoder and Services Config.
 The Services Config view is displayed with the General tab open.
- 3. Under **Parsers Configuration**, look at the Config Value for **PARSERULESCAN**. If it is **Enabled**, log parser rules are processed. If it is **Disabled**, they are not processed.
- If the rules are Enabled, click Enabled and select Disabled to disable the log parser rules. To save the changes, click Apply.

Add or Delete a Log Parser

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.2 and later.

For version 11.2, RSA has added the ability to add log parsers through the UI. You can also delete log parsers, as long as they have never been deployed to a Decoder. You can create a new log parser definition from scratch, or extend an existing one.

You can add a log parser to extend the functionality for an existing parser. For example, if you have some unknown messages for the Cisco Pix parser, you could add rules to match your unknowns.

IMPORTANT: If you are adding a new log parser, for example when onboarding an event source, you must map the event source IP to the new log parser in order for messages to be parsed. For details, see "Acknowledging and Mapping Event Sources" in the *Event Source Management User Guide*.

Add a Log Parser

- 1. In the NetWitness Platform UI, navigate to **CONFIGURE > Log Parser Rules**.
- 2. From the Log Parsers pane, click Add Parser.

The Add Dynamic Log Parser dialog box is displayed.

- 3. Fill in details for this dialog box. For details, see Add Dynamic Log Parser Parameters below.
- 4. Click **Save** to save the new log parser.

This updates the definition file in the file system. It *does not* deploy the changes.

5. To deploy your changes to all of your Decoders, click **Deploy**.

Delete a Log Parser using the UI

You can use the UI to delete a log parser that has never been deployed.

To delete a log parser:

Note: You cannot delete a log parser through the UI, if it has ever been deployed to a Decoder.

- 1. In the NetWitness Platform UI, navigate to CONFIGURE > Log Parser Rules.
- From the Log Parsers pane, select a log parser.
 Delete Parser dialog box is displayed.
- 3. Click **Delete** to remove the log parser from the system.

Delete a Log Parser Manually

To manually delete a log parser that has been deployed at any time, you can use NwConsole.

To delete a log parser that has been deployed:

- 1. Access the RSA NetWitness Console, using the **NwConsole** command. For details, see "Access NwConsole and Help" in the *NwConsole User Guide*.
- 2. Run the following command:

```
[localhost:50002] /decoder/parsers> send . delete file=filename.xml
type=device
```

where *filename* is the name of the XML file for the log parser. For example, to delete the log parser for Oracle Access Manager, run the following command:

```
[localhost:50002] /decoder/parsers> send . delete file=oracleam.xml
type=device
```

Notes about the log parser filename:

• Log parser files are located on the Log Decoder in the following path:

/etc/netwitness/ng/envision/etc/devices

• Each log parser has its own sub-folder. For example, the Cisco ASA parser files are in the following folder:

/etc/netwitness/ng/envision/etc/devices/ciscoasa

• Some log parser file names begin with v20_, while others do not—the only way to tell is by examining the devices folders. For Cisco ASA, the log parser file name is v20_ciscoasamsg.xml. However, in the previous command, when you specify the filename, do *not* use the v20_ prefix.

Add Dynamic Log Parser Parameters

When you are adding a log parser, the following parameters are available.

Field	Details
SELECT LOG PARSER	Select NEW, or choose an existing log parser.
	By choosing an existing log parser, you can add rules to that parser, essentially extending its parsing capabilities.
	Note: If you select an existing log parser, the remaining fields are auto-filled based on the values for selected log parser.
DEVICE TYPE	Enter a string to define the device type. The name must be between 3 and 30 alphanumeric characters (including underscores), and must not match the name of any existing log parsers.
DEVICE DISPLAY NAME	Enter the display name for the log parser.
INAIVIE	Note: The display name must be 64 characters or fewer, and must not match the name of any other device display name.
DEVICE CLASS	Select a device class.
CLONE DYNAMIC PARSER RULES FROM	Leave blank to start with no rules, or select one of the existing log parsers to clone its rules.

Add or Delete a Log Parser Rule

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.2 and later.

For version 11.2, RSA has added the ability to create custom rules for log parsers. You can create rules to change how meta values are parsed for a particular log parser. Prior to version 11.2, you could only view the out-of-the-box log parser rules.

About Log Parser Rules

Parsers are described within their XML files. Each log parser has an XML file that contains rules on how to parse messages for that parser. The out-of-the-box rules are contained within these XML files. For details, see the Log Parser Customization topic in the RSA Link space for RSA Content.

Custom Log Parser Rules

When you create a new log parser rule, it is saved to another XML definition file for the parser. These files are known as token files. This is important, since the out-of-the-box rules are overwritten if you update the parser through RSA Live, but any custom log parser rules are not overwritten, since Live does not update the token files for log parsers.

To create a custom log parser rule:

- 1. In the NetWitness Platform UI, navigate to **CONFIGURE > Log Parser Rules**.
- 2. From the Log Parsers pane, select a log parser.
- 3. From the **Rules** pane, click **Add**.

The Add Rules dialog box is displayed.

IMPORTANT: If you click outside of the Add Rule dialog box before you save your rule, your changes will be lost.

- 4. Add at least one meta key and a value to match, in order to create a valid rule.
- 5. Click Save to save your new rule.

This updates the definition file in the file system. It *does not* deploy the changes.

6. To deploy your changes to all of your Decoders, click **Deploy**.

Guidelines for Custom Rules

When you are creating a custom rule, keep in mind the following:

• For the list of tokens that match strings from the log file, very short tokens are not useful. For example, a one- or two-character string can match more items than desired.

- Remember to add the delimiter (especially if it is a space) as part of the token. For example "domain=" or "email ".
- When constructing regular expressions, the more complexity you add, the more performance overhead added to the system to compare against the rule.
- To see examples of good tokens and regular expressions, examine the rules that are provided for the default log parser.

Default Log Parser and Log Parser Rules

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.1 and later.

This tab displays information about pattern matching and rules for the parsers in your system. The features on this tab apply to all log parsers, including the Default Log Parser

Default Log Parser

The NetWitness Platform default log parser is used to parse logs coming from the Log Decoder that do not match any of the configured log parsers. This default parser parses these logs by using a default set of rules and tokens.

You can view the default log parser and its details by going to **ADMIN > Event Sources > Log Parser Rules** and selecting **default** from the Log Parsers panel.

Note: If you do not see the default log parser and its rules, you might need to go to Live and deploy the RSA Content to your log decoders. Additionally, you must have at least one Log Decoder at version 11.2 to view the default log parser.

You can view the default log parser and its details, depending on your version:

- For RSA NetWitness® Platform version 11.1, go to ADMIN > Event Sources > Log Parser Rules, then select default from the Log Parsers panel.
- For RSA NetWitness® Platform version 11.2 and later, go to **CONFIGURE > Log Parser Rules**, then select **default** from the Log Parsers panel.

Note: The list of log parsers is based on the first Log Decoder that is installed or registered by the Orchestration Server. If you have more than one Log Decoder, this tab only lists log parsers that have been configured on the first one.

This is a view of the Log Parser Rules tab, showing the **Default Log Parser** and **Any Domain** rule selected:

Live Content Incident Rules	Respond Notifications E	ESA Rules Subscriptions	Custom Feeds	Log Parser Rules	
Log Parsers	default 👩 Deploy				Rules
Add Parser Delete	Any Domain				Add Rule Delete
default	TOKENS	VALUES	мета		Test
Cisco PIX Firewall	Please Enter New Token 🛛 🕂 🚔	HOSTNAME		CAPTURE	Status URL1
Carbon Black Cisco ASA	domain 🔟	TYPE Hostname	doma	ain 🗸	mod
CISCO ASA	adom 🔟	MATCHING This matches Hostn			Client Domain [RSA]
	domain address	MATCHING This matches Hostn	ame		Destination Domain [RSA]
	domain invalid				Source Domain [RSA]
	domain_name 🏢				Any Domain [RSA]
	domainname				Client Username [RSA]
	comainname 🛄 👻				Username [RSA]
					Destination Port [RSA]
	Sample Log Messages (Test up	o to 60K characters of log messages)			Source Port [RSA]
	Sumple Log messages (rest up				Any Port [RSA]
	date=2017-08-12 type=tra	affic subtype=violation <mark> user</mark> =	<mark>matt</mark> status= <mark>deny</mark> s	src=192.168.24.49	Destination MacAddress [RSA]
	domain=google.com May 5	5 2018 15:55:49 switch : %ACE	-4-4000 TDS:1000	TP Option Bad Opti	Source MacAddress [RSA]
					Any MacAddress [RSA]
	\$IIS-4-440: 2017-08-12 1	13:53:34 192.170.28.192 - W45	31 url=https://tes	t.domain.edu/exch	Source IP or IP:Port [RSA]
	Dec 20 13:20:20 instance	el info <mark>mod=m</mark> ail from= <mark>matt@rs</mark>	a.com to=alex@dell	com	Destination IP or IP:Port [RSA]
				•	Any IP or IP:Port [RSA]

The Log Parser Rules Tab topic describes the items available for the Log Parsers tab.

Highlight Matching Patterns

You can paste logs into the Log Messages text box, and the system highlights the matching literals and patterns for the rules for the selected event source type. Use this feature to confirm that the parser is behaving as expected.

- 1. n the NetWitness Platform UI, navigate to ADMIN > Event Sources > Log Parser Rules.
- 2. In the NetWitness Platform UI, navigate as follows, depending on your version:
 - For RSA NetWitness® Platform version 11.1, go to ADMIN > Event Sources > Log Parser Rules.
 - For RSA NetWitness® Platform version 11.2 and later, go to CONFIGURE > Log Parser Rules.
- 3. From the Log Parsers pane, select a log parser.
- 4. From the **Rules** pane, select a rule.

For example, this screen shows the Any Port rule for the carbonblack log parser:

Live Content Incident Rules	Respond Notifications E	ESA Rules Subscriptions	Custom Feeds	Log Parser Rules	
Log Parsers	carbonblack 👩 📭	eploy Save Discard Cha	nges		Rules
Add Parser Delete	Any Port				Add Rule Delete
default	TOKENS	VALUES	META		Test
Cisco PIX Firewall Carbon Black	Please Enter New Token +	UNSIGNED 16-BIT INTEGER	FULL C ~ port	CAPTURE X 🗸	Status Client Domain
Carbon Black	port 🛅	TYPE Uint16		^ ``	Destination Domain
-	port:	MATCHING This matches unsi	med 16-bit int		Source Domain
	port=				Any Domain
	port-				Client Username
					Username
	port:				Destination Port
					Source Port
					Any Port
	Sample Log Messages (Test up t	to 60K characters of log messages			Destination MacAddress
					Source MacAddress
	date=2017-08-12 type=trai	affic on port 12345 subtype=	violation user=matt	status=deny src=192	Any MacAddress
	May 5 2018 15:55:49 swite	ch : %ACE-4-4000: IDS:1000	IP Option Bad Option	n user: admin@test.c	Source IP or IP:Port Destination IP or IP:Port
	\$TTS-4-440: 2017-08-12 13	.3:53:34 192.170.28.192 - W4	S31 url=https://tee	t.domain.edu/exchand	Any IP or IP:Port
					Source Email Address
	Dec 20 13:20:20 instance1	1 info mod=mail <mark> from=matt0</mark>	sa.com to=alex@dell	. com	Destination Email Address
	•			Þ	

5. Add text or paste in a sample log message.

Strings that match tokens for the selected rule are highlighted in blue. Strings that match other rules for the parser (and the rules themselves) are highlighted in orange.

RSA RESPOND INVESTIGATE M	IONITOR CONFIGURE ADMIN	
Live Content Incident Rules R	Respond Notifications ESA Rules Subscriptions Custom Feeds Log Parser Rules	
Log Parsers	default Occupient Save Discard Changes	Rules
Add Parser Delete	Source Email Address	Add Rule Delete
default	TOKENS VALUES META	mod
Cisco PIX Firewall	Please Enter New Token	Client Domain [RSA]
Carbon Black	email.src	Destination Domain [RSA]
Cisco ASA	from: EMail	Source Domain [RSA]
	sender: MATCHING This matches Email addresses	Any Domain [RSA]
	from=	Client Username [RSA]
	sender=	Username [RSA]
		Destination Port [RSA]
	sender <	Source Port [RSA]
	sender < 🔲 💌	Any Port [RSA]
		Destination MacAddress [RSA]
	Sample Log Messages (Test up to 60K characters of log messages)	Source MacAddress [RSA]
	Sample cog Messages (rest up to ook characters of log filessages)	Any MacAddress [RSA]
	date=2017-08-12 type=traffic subtype=violation user=matt status=deny src=192.168.24.49 (Source IP or IP:Port [RSA]
		Destination IP or IP:Port [RSA]
	May 5 2018 15:55:49 switch : %ACE-4-4000: IDS:1000 IP Option Bad Option user: admin@tes	
	<pre>\$IIS-4-440: 2017-08-12 13:53:34 192.170.28.192 - W4S31 url=https://test.domain.edu/exch</pre>	Any IP or IP:Port [RSA]
		Source Email Address [RSA]
	Dec 20 13:20:20 instance1 info mod=mail from=matt@rsa.com to=alex@dell.com	Destination Email Address [RSA]
	4 · · · · · · · · · · · · · · · · · · ·	URL [RSA]

For example, in the previous screen, note:

• The source email address, matching the **from** token, is highlighted in blue. The token is in dark blue, and the matching string is highlighted in light blue. This is because the **Source Email Address** is the

currently selected Rule.

• The strings highlighted in orange match tokens for rules for **Any MacAddress**, **Any Port** and **Source Port**. This is because they are in rules for the default parser that are not currently selected.

Highlight Overlapping Patterns

When you have patterns that overlap rules (that is, one pattern matches more than one rule), the behavior is as follows:

- The pattern is displayed in a single color (yellow)
- When you select one of the matching rules, the exactly-matched pattern is displayed in light and dark blue

For example, the pattern user: admin@test.com from 10.100.229.59 matches several rules.

RSA RESPOND INVESTIGATE M	ONITOR CONFIGURE	DMIN				
Live Content Incident Rules Re	espond Notifications ES	A Rules	Subscr	riptions Custom Feeds	og Parser Rules	
Log Parsers	default 📀 Deploy	Save	Discard C	Thanges		Rules
Add Parser Delete	entirelog					Add Rule Delete
default	TOKENS Please Enter New Token word-	+ R4	LLUES egex Pattern PE ATCHING TTERN	regex This matches Regex	META FULL CAPTURE content FIRST CAPTURE None SECOND CAPTURE None THIRD CAPTURE	username (RSA) hostip (RSA) sourcelpport (RSA) entirelog (RSA) ip (RSA) entirelog2 (RSA) srcipport_overlap (RSA) dest_email (RSA) o user email
		atus=den 1 Bad Op	y src=192. tion <mark>user</mark>			

RSA RESPOND INVESTIGATE N	MONITOR CONFIGURE	ADMIN			(
Live Content Incident Rules F	Respond Notifications ESA	A Rules Subscr	iptions Custom Feeds Log	Parser Rules	
Log Parsers	default 🕞 Deploy	Save Discard C	hanges		Rules
Add Parser Delete	hostip				Add Rule Delete
default	TOKENS	VALUES		META	username [RSA]
		IPV4 Address			hostip (RSA)
			IPv4	alias.ip v	sourceipport [RSA] entirelog [RSA]
					ip [RSA]
		MATCHING	This matches IPV4 addresses		entirelog2 [RSA]
					srcipport_overlap [RSA]
					dest_email [RSA]
					😳 user email
	Sample Log Messages (Test up to	o 60K characters of log	messages)		
	ype=violation user=matt sta	atus=deny src=192.	.168.24.49 dst=192.56.43.56 dstdc	main=com sent=0 src_port=4135	
	-4-4000: IDS:1000 IP Option	n Bad Option <mark>user:</mark>	admin@test.com from 10.100.229.	59 port 12345.	
	.92.170.28.192 - W4S31 url=	https://test.domai	in.edu/exchange GET /exchweb/bin/	auth/owalogon.asp 440	
	(Þ	

When you select the **hostip** rule, the highlighting that matches only this rule is shown in dark and light blue.

Use Cases

This topic describes the procedures you use to either on board a new event source, or to extend the parsing capabilities for an existing log parser.

Use Case 1: On Board a New Event Source

In this case, a customer has an event source and wants to add it into the RSA NetWitness® Platform. Perform the following tasks:

- I. For your event source, get examples of the logs.
- II. In the **CONFIGURE > Log Parser Rules** view, add the Log Parser.
- III. From your sample logs, paste applicable sections into the Sample Log Messages section of the Log Parser Rules screen.
- IV. Use the sample area to understand which items are being parsed by the current parser, and note the items that are not being parsed.
- V. For anything that is not currently being parsed, add rules.
 - If the new rules apply to all parsers, you can add them to the Default parser.
 - If not, add them only to the new log parser you are creating.
- VI. Save the new rules, and deploy them to all Log Decoders.
- VII. Map the IP address for the newly added event source to the newly-created log parser. For details, see "Acknowledging and Mapping Event Sources" in the *Event Source Management User Guide*.

Use Case 2: Modify an Existing Parser

In this case, a customer wants to parse some items from the logs that are not currently being parsed by the existing log parser. Perform the following tasks:

- I. For your event source, get examples of the logs.
- II. In the **CONFIGURE > Log Parser Rules** view, add the Log Parser.
- III. From your sample logs, paste applicable sections into the Sample Log Messages section of the Log Parser Rules screen.
- IV. Use the sample area to understand which items are being parsed by the current parser, and note the items that are not being parsed.
- V. For anything that is not currently being parsed, add rules.
- VI. Save the new rules, and deploy them to all Log Decoders.

For a detailed walk through of some of the steps in these use cases, see <u>Extend an Existing Log Parser</u> <u>Example</u>.

Extend an Existing Log Parser Example

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.2 and later.

Parse Rules can be used to parse unknown logs from existing devices. If a log is identified as a particular type (**device.type** is populated), and is not already being parsed (**msg.id** is not populated), then Parse Rules can be added to pull out relevant data from these logs.

If the neither **device.type** nor **msg.id** are populated for the logs from an existing device, then you need to map the device before Parse Rules can be processed against these logs.

Note: If a log message is already being parsed (**msg.id** is populated) then Parse Rules will not be processed against that log.

Task Overview

In this example, a customer wants to parse some items from the logs that are not currently being parsed by the existing log parser. Perform the following tasks:

- I. For your event source, get examples of the logs.
- II. In the CONFIGURE > Log Parser Rules view, Add the Log Parser
- III. From your sample logs, paste applicable sections into the Sample Log Messages section of the Log Parser Rules screen.
- IV. Use the sample area to understand which items are being parsed by the current parser, and note the items that are not being parsed.
- V. For anything that is not currently being parsed, add rules as described in Add Rules and Deploy.
- VI. Save the new rules, and deploy them to all Log Decoders.

Notes

Note: All the procedures in the topic use the CONFIGURE > Log Parser Rules view.

In the Log Parser Rules tab, you may see the Refresh icon () next to an item. This indicates that the item has undeployed changes.

Add the Log Parser

The first step in the process is to add a log parser, based on an existing log parser that you want to customize.

To add a log parser

- 1. In the RSA NetWitness® Platform menu, navigate to CONFIGURE > Log Parser Rules.
- 2. In the Log Parsers panel, click Add Parser.

The Add Dynamic Log Parser dialog box is displayed.

- 3. In the **SELECT LOG PARSER** field, select the existing parser to extend. In this example, we use Cisco Pix Firewall.
- 4. You can clone the rules from any of your existing parsers, including the **default** parser. For simplicity, in this example we leave this field blank: thus, only the rules we create are added to the new parser.
- 5. Click Add Parser to create the new parser.

The new parser is listed in the Log Parsers panel. Note the Symbol next to the new parser—this indicates that your changes have not yet been saved.

RSA	RESPOND	INVESTIGATE	МО
Live	e Content	Incident Rules	Re
Lo	g Parsers		
A	dd Parser	Delete	
de	fault		
O Cis	co PIX Firewall		

About Custom Rules

When you create a new log parser rule, it is saved to an XML definition file for the parser. These files are known as token files. This is important, since the out-of-the-box rules are overwritten if you update the parser through RSA Live, but any custom log parser rules are not overwritten, since Live does not update the token files for log parsers.

Add Rules and Deploy

Once you have added the parser, the next step is to add one or more rules.

Let's say you know that your log messages have some email addresses that follow a "source_mail" string. You could add the following rule to parse these strings:

IMPORTANT: If you click on another parser in the **Log Parsers** panel, before you save your rule, your changes will be lost.

1. Make sure the Cisco Pix Firewall parser is selected.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE ADMIN
Live Content Incident Rules	Respond Notifications ESA Rules Subscriptions Custom Feeds Log Parser Rules
Log Parsers	CISCOPIX _ Deploy Save Discard Changes
Add Parser Delete	
default	
O Cisco PIX Firewall	

2. In the Rules panel, click Add Rule.

The Add New Rule dialog box is displayed.

3. Enter a name for the rule, and click Add New Rule.

The center panel is updated to reflect that you are working on a new rule.

RSA RESPOND INVESTIGATE M	ONITOR CONFIG	URE ADMIN		(1) admin
Live Content Incident Rules Re	espond Notificatio	ns ESA Rules Subscriptions	Custom Feeds Log Pa	arser Rules
Log Parsers	ciscopix 👩	Deploy Save Discard Changes		Rules
Add Parser Delete	Source email			Add Rule Delete
default	TOKENS	VALUES	META	
Clisco PIX Firewall	At least one token required. <u>Please Enter Nev</u> +	REGEX PATTERN	At least one meta capture selection is required. FULL CAPTURE None	
		PATTERN	None V	
			SECOND CAPTURE	
			None 🗸	
			THIRD CAPTURE	
		Invalid regular expression.	None 🗸	
	Below are sample log	messages:		
	date=2017-08-12	type=traffic subtype=violation user=m	natt status=deny src=19	
	May 5 2018 15:55	:49 switch : %ACE-4-4000: IDS:1000 IP	9 Option Bad Option use	
	\$IIS-4-440: 2017-	-08-12 13:53:34 192.170.28.192 - ₩453	31 url=https://test.dom	

4. In the TOKENS section, enter a string for the token that you want to match, then click +. In this example, we entered **email**. **Note:** Make sure to include a delimiter for your token. For example, in this case, the token consists of 6 characters: the string "email," and then a space. Some tokens might use a colon, semicolon, or some other character as the delimiter, but it can be easy to forget to add the space character when that is the delimiter.

You can enter more tokens, or continue to add values.

5. In the VALUES section, choose the value for the rule. If you choose to match a Regex Pattern, you need to enter the pattern in the PATTERN field. Other values do not require any options.

In this example, we selected **Email**.

- 6. In the META section, click 🗹 to select a meta key to which the rule stores its information. Some notes:
 - Enter characters to filter the list of available meta keys.
 - For Regex values, you can select "pieces" of the value, and store each piece to its own meta key.

Note: If any new meta keys are added to the Log Decoder, they do not appear in the list of Meta immediately. They appear automatically after 24 hours, or you can restart the **content server** service to view them.

In this example, we selected the **email.src** meta key.

The following image shows an example rule:

espond Notifications E		ubscriptions	Custom Feeds	Log Parser Rules	
espond Notifications E	SA Rules S	ubscriptions	Custom Feeds	Log Parser Rules	
ciscopix 💽 Deploy	Save	Discard Changes			Rules
Source email					Add Rule Delete
TOKENS	VALUES			META	Source email
Please Enter New Token +	EMAIL ADDR	RESS	~	FULL CAPTURE - email.src X 🗸	
email	ТҮРЕ	EMail		. <u></u>	
	MATCHING	This matches E	mail addresses		

- 7. Click Save to save the rule. Repeat this procedure to continue adding rules.
- 8. Once you have added all of your rules, click **Deploy** to deploy the new parser to your Log Decoders. Some notes about deploying rules:
 - You deploy an entire set of rules for a parser. That is, you can continue adding rules for a specific parser until you have all of your rules, and then you can deploy them all at once.
 - Once you deploy a custom parser, you can no longer delete it. You can only delete parsers that you have not yet deployed.

Note: In this example, we extended an existing log parser. However, if you are creating a new log parser for a new event source, make sure to map the new log parser to the IP address of the event source, as described in "Acknowledging and Mapping Event Sources" in the *Event Source Management User Guide*.

Regex Values

Custom Log Parser Rules can match regular expression patterns. If you select a Regex pattern for your Value, you can capture the entire matched token, or sections of it:

- Full capture: the entire matched string is stored to your selected meta key.
- First capture: the first portion of the string, up to the period character, is stored to the meta key.
- Second capture: the second portion of the string, starting after the first period character, is stored to the meta key.
- Third capture: the third portion of the string, starting after the second period character, is stored to the meta key.

You can choose any or all four of these captures, depending on the token you are matching.

For example, we examine the **Source IP or IP:Port** RSA rule:

- Regex Pattern: $s*((b(?:[0-9]{1,3}).){3}[0-9]{1,3})):?((d*))$
- Full capture: none
- First capture: ip.src
- Second capture: port.src
- Third capture: none
- Assume example string of "src=192.168.24.4:8080", where **src** is one of the tokens defined for this rule:
 - 192.168.24.4 is saved to the ip.src meta key.
 - 8080 is saved to the **port.src** meta key.

For more details, see any online reference that describes PERL regular expressions. There are many tutorials available online.

IMPORTANT: Be careful when constructing regular expressions in your custom rules. Badly constructed regular expressions could impact your performance.

Appendix A: Select the Reference Log Decoder

For version 11.2, RSA has added the ability to add log parsers and log parsing rules through the UI, using the Log Parsers view. The Log Parsers tab is populated based on your reference Log Decoder. If you have more than one Log Decoder, you can select which acts as the reference one for populating the tab in the UI. This topic describes the procedure to do so.

To change the reference log decoder:

- 1. In the NetWitness Platform UI, navigate to **ADMIN > Services**.
- 2. For the **Content Server**, select **View > Explore**.
- 3. From the left navigation panel, expand **content > parser**.
- 4. To set the reference log decoder, enter a value for preferred-log-decoder-name-for-sync.

Enter the name listed in the **Name** column on the **ADMIN** > **Services** screen for your preferred log decoder.

RSA RESPOND INVESTIGATE	MONITOR CONFIGURE ADMIN	
Hosts Services Event Sour	ces Health & Wellness System Security	
🚠 Change Service 🕴 SAUII - Content Ser	ver Explore	
■ SAUII - Content Server <	/rsa/content/parser	SAUII - Content Server
	cache-duration	24 HOURS
SAUII - Content Server (CONTENT_SERVER)	database-initialization-enabled	true
admin/security/settings	log-decoder-sync-interval	12 HOURS
C configuration	max-try-counter-for-ld-sync-failure	3
Content	Content preferred-log-decoder-name-for-sync	
🗋 parser	previously-synced-log-decoder-id	74d327e6-239c-45e7-9d02-e1821424635e
data/control	remove-previous-sync-parsers-for-new-log-decoder	false
🖬 🗋 filesystem	retrieval-timeout	30 SECONDS
formats sleep-interval-after-notification		60 SECONDS
🗋 health	sync-from-log-decoder-enabled	true
Iogging		
metrics		

- 5. The change takes effect during the next system sync, based on the log-decoder-sync-interval. To sync sooner, you can do either of the following:
 - To sync immediately, restart the Content Sever: in the ADMIN > Services view, from the Actions menu for the Content Server, select > Restart.
 - Change the log-decoder-sync-interval parameter from its default of 12 hours to your preferred interval. Note that the minimum value for this parameter is 1 HOUR.

Appendix B: Move Log Parsers to Production

You may have a development or test environment where you work on new and updated log parsers and log parser rules. In this case, at some point you need to move your new and updated log parsers into your production environment. This topic describes how to do this.

To move custom log parsers and log parser rules from development to production environment:

- 1. On the development system, do the following:
 - a. SSH to the NetWitness Server
 - b. Export the log parser information by running the following command:

```
mongodump --host localhost --port 27017 --db "content-server" --username
"deploy admin" --password "netwitness" --authenticationDatabase admin
```

- c. Copy the "dump" folder to your production NetWitness Server.
- 2. On the production system, do the following:
 - a. SSH to the NetWitness Server
 - b. Drop the content-server table from Mongo by running below commands in the order listed:

```
mongo --username deploy_admin --password netwitness --
authenticationDatabase admin
use content-server
db.logDeviceParser.drop()
db.patternFormatType.drop()
exit
```

c. Run the following restore command:

```
mongorestore --host localhost --port 27017 --db "content-server" --
username "deploy_admin" --password "netwitness" --authenticationDatabase
admin PATH_TO_DUMP_FOLDER
```

Make sure to replace *PATH_TO_DUMP_FOLDER* with the actual path to the "dump" folder.

d. Restart the content-server by running the following command:

systemctl restart rsa-nw-content-server

Appendix C: Troubleshooting and Limitations

This section describes some common issues that can occur when you customize log parsers and log parser rules.

Troubleshooting

You do not see any log	You may have forgotten to map the new parser. To map a parser, go to
parsing against a	Admin > Event Sources > Discovery tab. See the "Discovery Tab" topic in
newly created parser.	the <i>Event Source Management Guide</i> for details.
Deployment fails	If you click Deploy to deploy a new or updated log parser, and it fails, you should check the log for your reference log decoder. You access this log in the following location on the NetWitness Server: /var/log/netwitness/content-server/content-server.log

NwLogPlayer

NwLogPlayer is a troubleshooting tool that simulates syslog traffic. NwLogPlayer.exe is a command line utility located on the Log Decoder host in /usr/bin.

At the command line, type nwlogplayer.exe -h to list the available options, as reproduced here:

Option	Description
priority arg	set log priority level
-h [help]	show this message
-f [file] arg (=stdin)	input message; defaults to stdin
-d [dir] arg	input directory
-s [server] arg (=localhost)	remote server; defaults to localhost
-p [port] arg (=514)	remote port; defaults to 514
-r [raw] arg (=0)	Determines raw mode.
	• 0 = add priority mark (default)
	• 1= File contents will be copied line by line to the server.
	• 3 = auto detect
	• 4 = enVision stream
	• 5 = binary object
-m [memory] arg	Speed test mode. Read up to 1 Megabyte of messages from the file content and replays.

Option	Description
rate arg	Number of events per second. This argument has no effect if $rate > eps$ that the program can achieve in continuous mode.
maxcnt arg	maximum number of messages to be sent
-c [multiconn]	multiple connection
-t [time] arg	simulate time stamp time; format is yyyy-m-d-hh:mm:ss
-v [verbose]	If true , output is verbose
ip arg	simulate an IP tag
ssl	use SSL to connect
certdir arg	OpenSSL certificate authority directory
clientcert arg	use this PEM-encoded SSL client certificate
udp	send in UDP

Limitations

Please note the following limitations when using the Log Parser Rules tab:

- Log Decoder must be at version 11.2: For the functionality in the Log Parser Rules tab to work, your installation must have at least one Log Decoder running NetWitness version 11.2.
- **Mixed Mode:** If any Log Decoders are at version 11.2, and the NetWitness Server is at version 11.2, the Log Decoders will have parseall rules enabled by default, and thus will begin to parse logs accordingly. However, the 11.2 NetWitness Server does not support Log Decoders with versions less than 11.2, so the Log Parser Rules tab in the UI stays blank.
- Meta key fields list refresh: If any new meta keys are added to the Log Decoder, they do not appear in the list of Meta in the Log Parser Rules tab immediately. They appear automatically after 24 hours, or you can restart the **content server** service to view them.
- Field Restrictions: Note the following field restrictions:
 - Rule name must be 64 characters or fewer.
 - **Parser Name** must be between 3 and 30 alphanumeric characters (including underscores), and must not match the name of any existing log parsers.
 - **Parser Display Name** must be 64 characters or fewer, and cannot match any other parser display name.
 - Regex Expression must be 1-255 characters, and a valid regex (closed capture list allowed).
 - Tags cannot be duplicates.
- **Deploy only to 11.2 Log Decoders:** The Deploy operation only deploys log parsers to version 11.2 Log Decoders.
- Cannot Remove Deployed Parsers: Once deployed, you cannot delete a log parser using the UI.

• See log for errors: Refer to content-server logs for more details on deploy failure details and log decoder names.