RSA® NETWITNESS®
Logs
Implementation Guide

Digital Guardian 6.1

Daniel R. Pintal, RSA Partner Engineering
Last Modified: January 23, 2019

RSA READY

Solution Summary

Digital Guardian is a comprehensive and proven Enterprise Information Protection platform. Digital Guardian serves as the cornerstone for policy driven, data-centric security by enabling organizations to solve the information risk challenges that exist in today's highly collaborative and mobile business environment. Digital Guardian's proven architecture makes it possible to implement a datacentric security framework from which business and IT managers can:

- Utilize actionable decision support reporting to assess the risk associated with the sharing of sensitive data, enabling managers to make informed business decisions and create effective data security policies
- Implement automated policy driven information protection controls, driving accountability down to the user resulting in voluntary compliance and increased risk aware behavior
- Alert, block and record high risk behavior ultimately preventing costly and damaging data loss incidents

With the RSA integration, Digital Guardian provides a rich data stream from laptops, desktops and servers, including a forensic log of data usage events, such as the user and application which accessed the data, the data event that occurs, and the classification of the data itself. Taking this data stream into RSA allows correlation with other security event data from the network, enterprise applications and other backend systems, dramatically increasing visibility for insider threat, malware detection and containment use cases.

RSA NetWitness Features	
Digital Guardian 6.1	
Integration package name	verdasysdgmc.envision
Device display name within RSA NetWitness	verdasysdgmc
Event source class	DLP
Collection method	Syslog

RSA NetWitness Community

The RSA NetWitness Community is an online forum for customers and partners to exchange technical information and best practices with each other. The forum also contains the location to download the NetWitness Integration Package for this guide. All NetWitness customers and partners are invited to register and participate in the **RSA NetWitness Community**.

Once you have downloaded the NetWitness Integration Package, the next steps are to deploy this on all log decoders. For steps to disable or remove the NetWitness Integration Package, please refer to the **Appendix** of this Guide.

The RSA Netwitness package consists of the following files:

Filename	File Function
verdasysdgmc.envision	Netwitness package deployed to parse events from devices.
verdasysdgmcmsg.xml	A copy of the device xml contained within the NetWitness package.
table-map-custom.xml	Enables NetWitness variables disabled by default.

Release Notes

Release Date	What’s New In This Release
1/23/2019	Revised guide for NetWitness integration support.
12/02/2013	Initial SA support for Verdasys Digital Guardian.

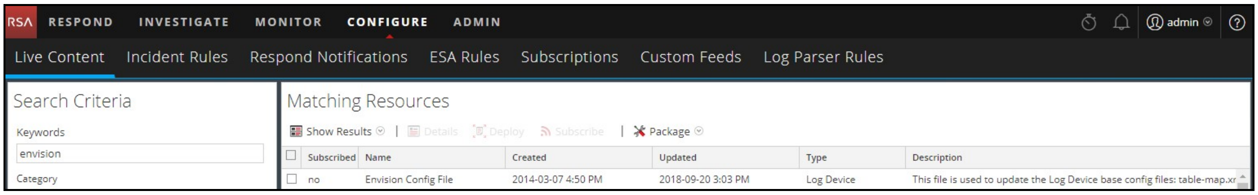
RSA NetWitness Configuration

Deploy the enVision Config File

In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **NetWitness Live** module. Log into RSA NetWitness and perform the following actions:

! Important: Using this procedure will overwrite the existing table_map.xml.

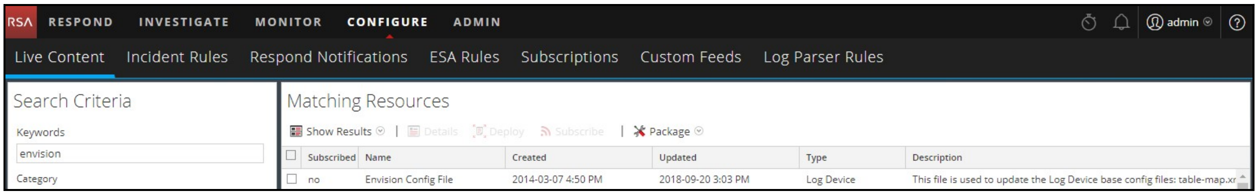
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. NetWitness will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



Keywords
envision
Category

☐	Subscribed	Name	Created	Updated	Type	Description
☐	no	Envision Config File	2014-03-07 4:50 PM	2018-09-20 3:03 PM	Log Device	This file is used to update the Log Device base config files: table-map.xr

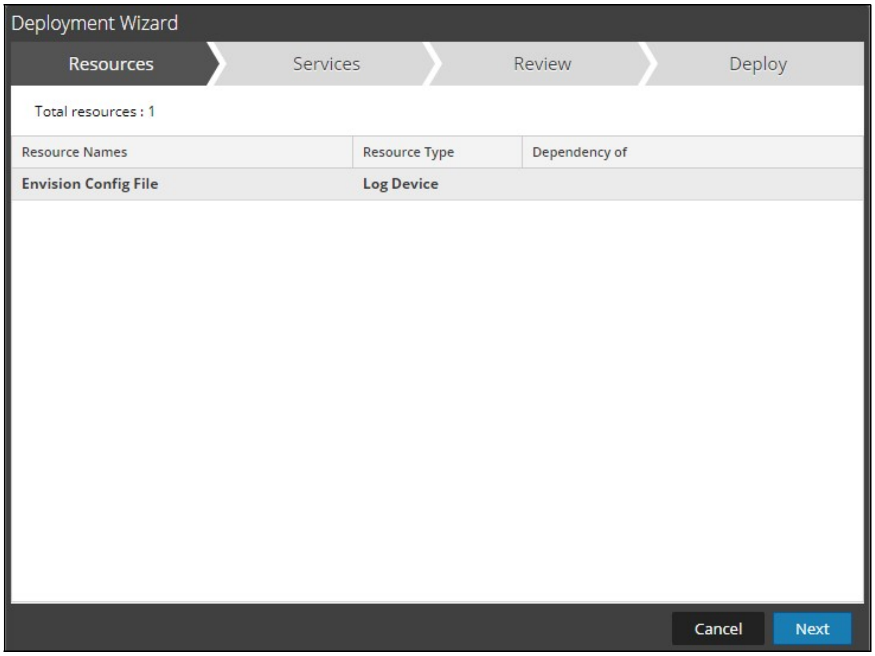
5. Click **Deploy** in the menu bar.



Keywords
envision
Category

☐	Subscribed	Name	Created	Updated	Type	Description
☐	no	Envision Config File	2014-03-07 4:50 PM	2018-09-20 3:03 PM	Log Device	This file is used to update the Log Device base config files: table-map.xr

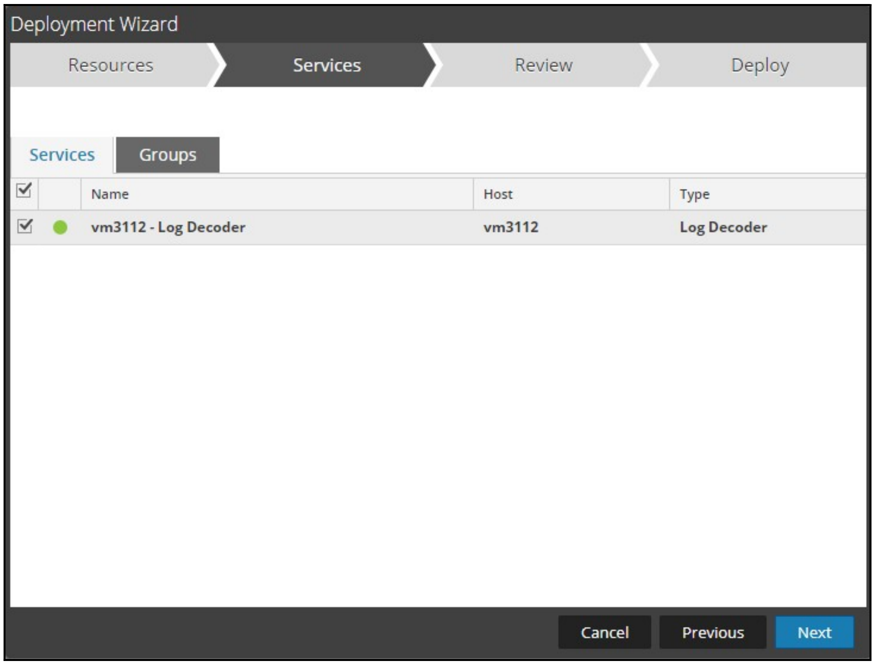
6. Select **Next**.



Total resources : 1

Resource Names	Resource Type	Dependency of
Envision Config File	Log Device	

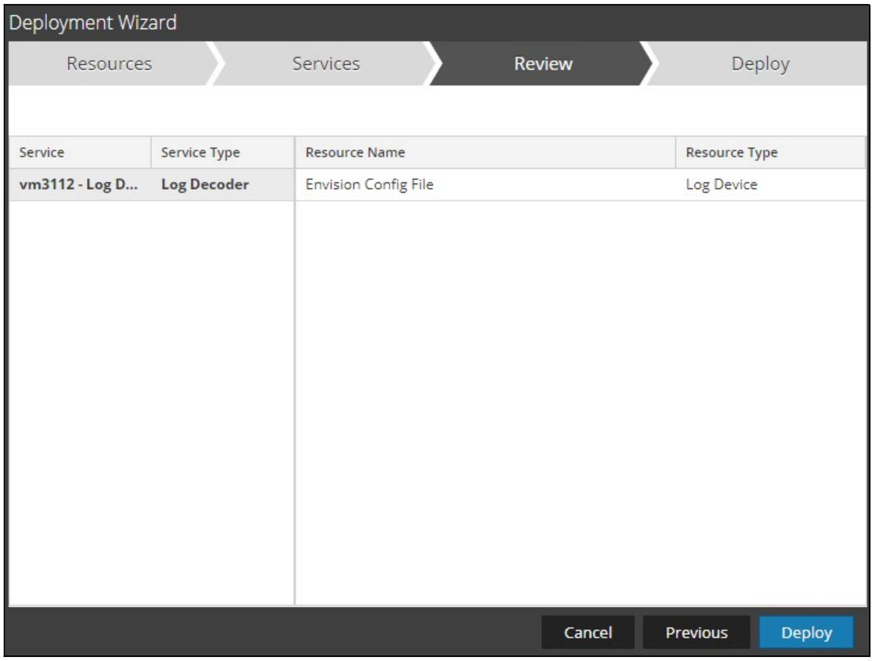
7. Select the **Log Decoder** and select **Next**.



☑		Name	Host	Type
☑	●	vm3112 - Log Decoder	vm3112	Log Decoder

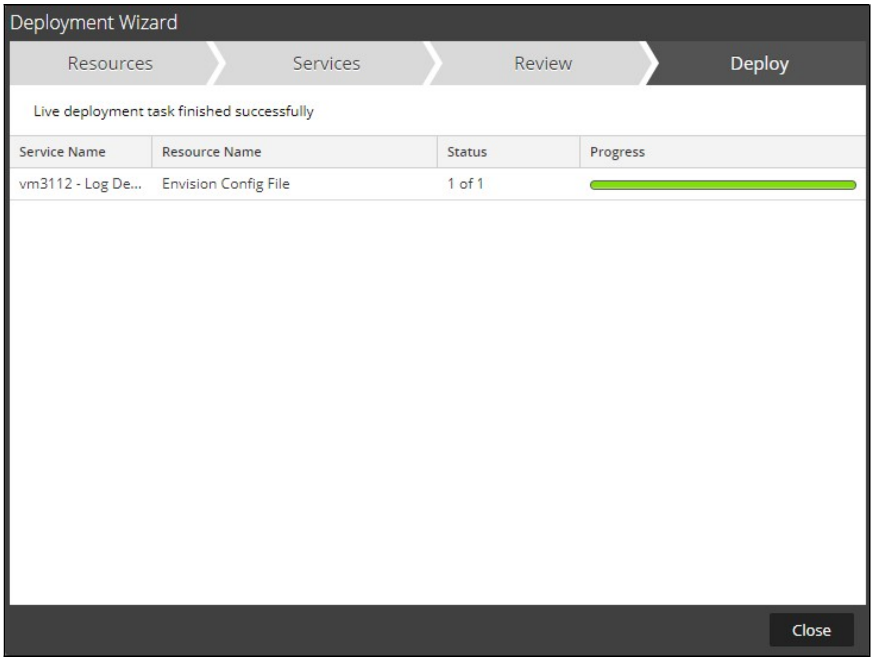
! Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.

8. Select **Deploy**.



Service	Service Type	Resource Name	Resource Type
vm3112 - Log D...	Log Decoder	Envision Config File	Log Device

9. Select **Close**, to complete the deployment of the Envision Config file.



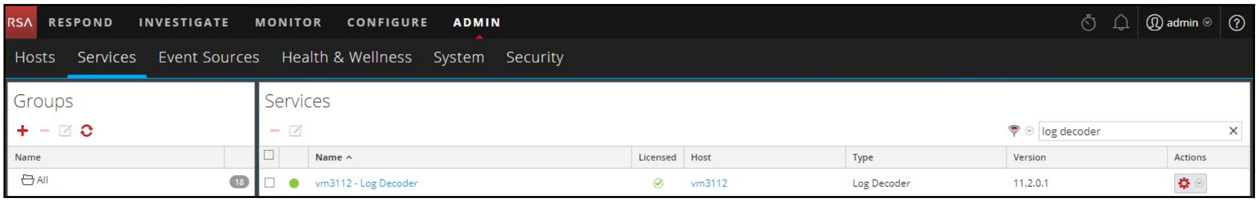
Live deployment task finished successfully

Service Name	Resource Name	Status	Progress
vm3112 - Log De...	Envision Config File	1 of 1	🟩

Deploy the RSA NetWitness Integration Package

After completing the previous section, ***Deploy the enVision Config File***, you can now deploy the NetWitness Integration Package. Download the appropriate RSA Partner Integration Package, then log into RSA NetWitness to perform the following actions:

1. From the NetWitness menu, select **Admin > Services.**

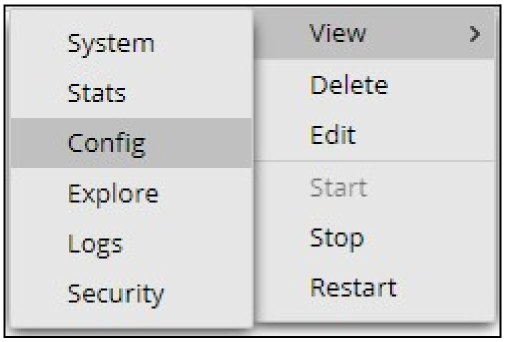


log decoder

Name	
All	18

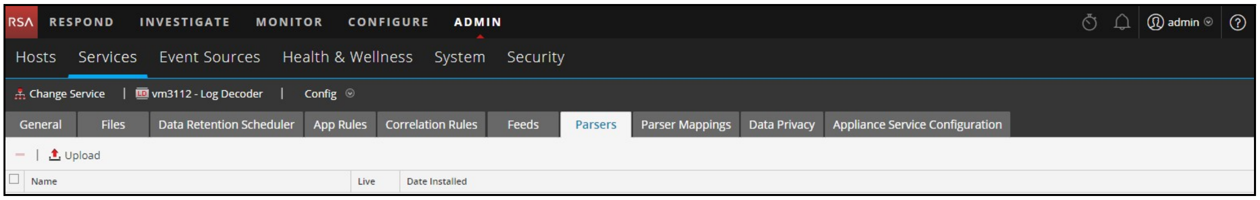
☐		Name ^	Licensed	Host	Type	Version	Actions
☐	●	vm3112 - Log Decoder	✓	vm3112	Log Decoder	11.2.0.1	

2. Select your Log Decoder from the list, select **View > Config**.



! Important: In an environment with multiple Log Decoders, repeat on the deployment of the RSA Partner Integration Package on each Log Decoder.

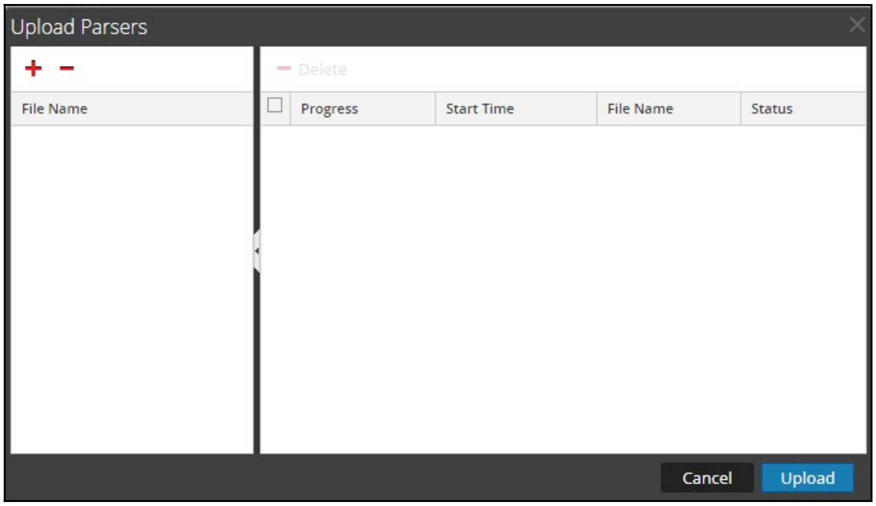
3. Select the **Parsers** tab and click the **Upload** button.



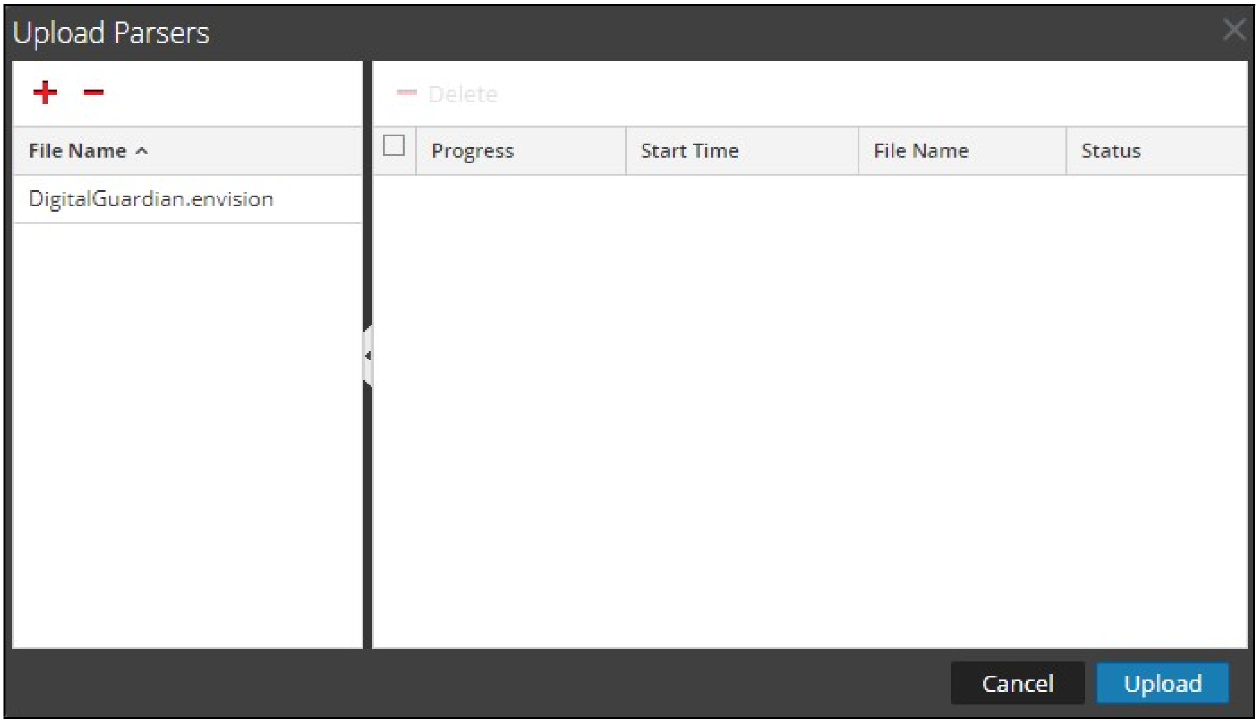
☐	Name	Live	Date Installed

4. From the *Upload Parsers* window, click the + **Add** button and select the *.envision* file.

! Important: The .envision file is contained within the .zip file downloaded from the RSA Community.

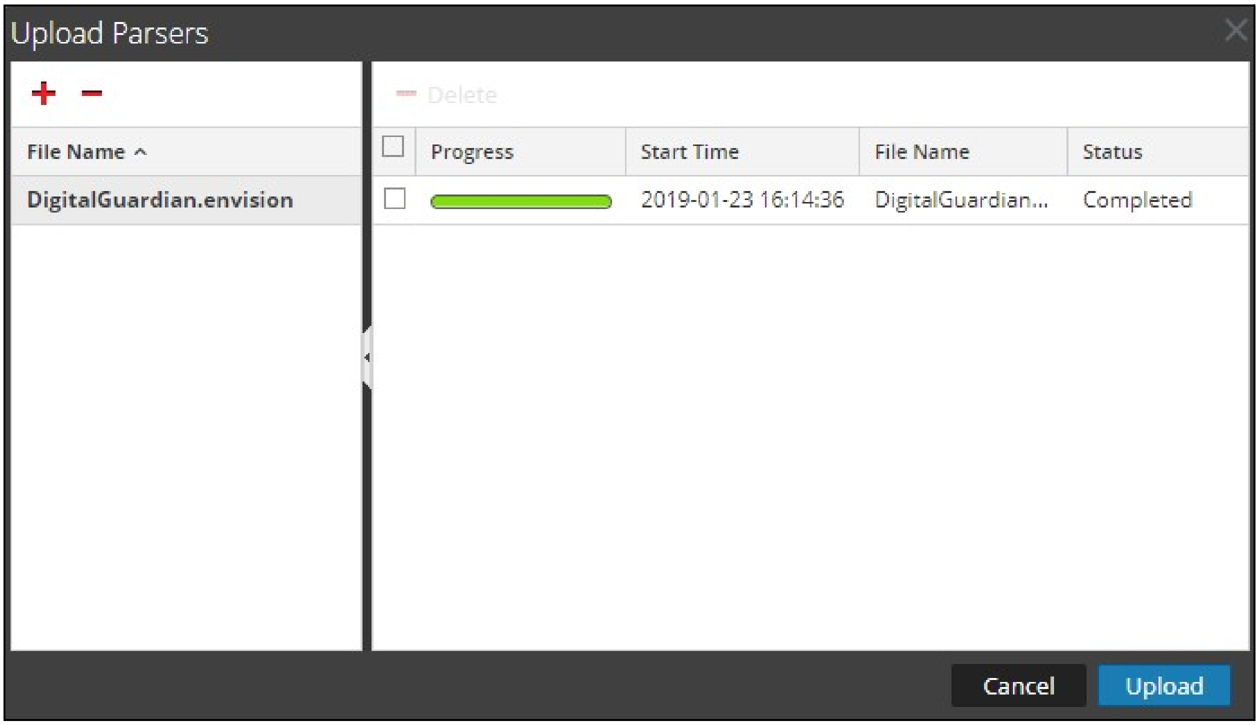


5. Under the file name column, select the integration package name and click **Upload**.



DigitalGuardian.envision

6. Select **Cancel** to complete.



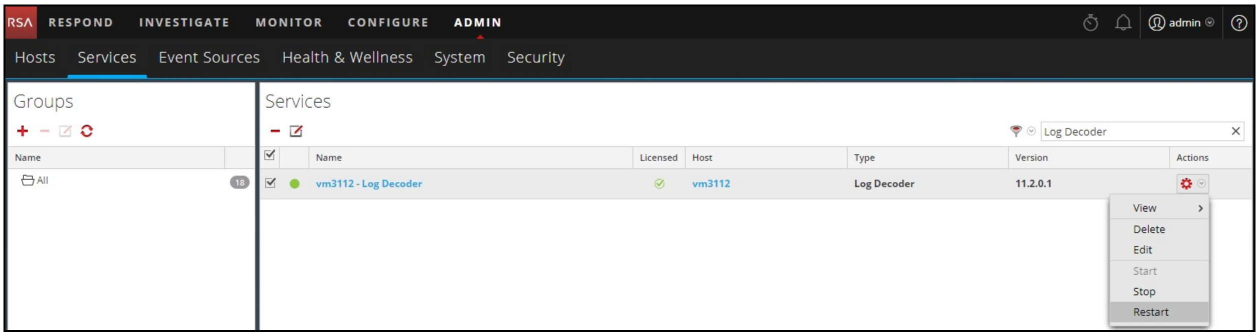
File Name ^
DigitalGuardian.envision

□	Progress	Start Time	File Name	Status
□	🟩	2019-01-23 16:14:36	DigitalGuardian...	Completed

7. Connect to the RSA NetWitness Log Decoder Server using WinSCP. Copy the table-map-custom.xml file from the contents of the .zip file to the /etc/netwitness/ng/envision/etc folder. If the table-map-custom.xml file already exists on the Log Decoder(s), copy only the contents between the <mappings>…</mappings> to the table-map-custom.xml file located on the Log Decoder.

! Important: Failure to utilize the contents of the table-map-custom.xml will result in keys not being displayed within Investigator.

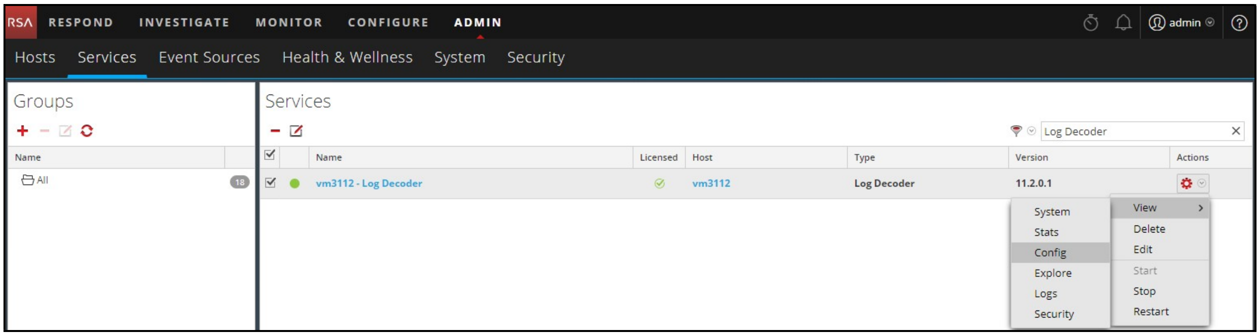
8. Navigate to **Admin > Services** and check the **Log Decoder(s)** then click **Restart.**



Name	
All	18

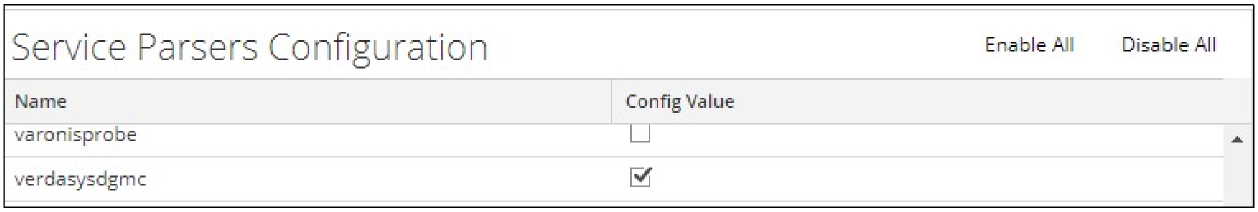
☑		Name	Licensed	Host	Type	Version	Actions
☑	●	vm3112 - Log Decoder	✓	vm3112	Log Decoder	11.2.0.1	⚙

9. Navigate to **Admin > Services** and check the **Log Decoder(s)** then click **View> Config.**



☑	Name	Licensed	Host	Type	Version	Actions
☑	● vm3112 - Log Decoder	✓	vm3112	Log Decoder	11.2.0.1	

10. The new device is listed under the Log Decoder(s) General Tab within the Service Parsers Configuration.


Service Parsers Configuration

Name	Config Value
varonisprobe	□
verdasysdgmc	☑

11. The Log Decoder is now ready to parse events for this device.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Digital Guardian with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

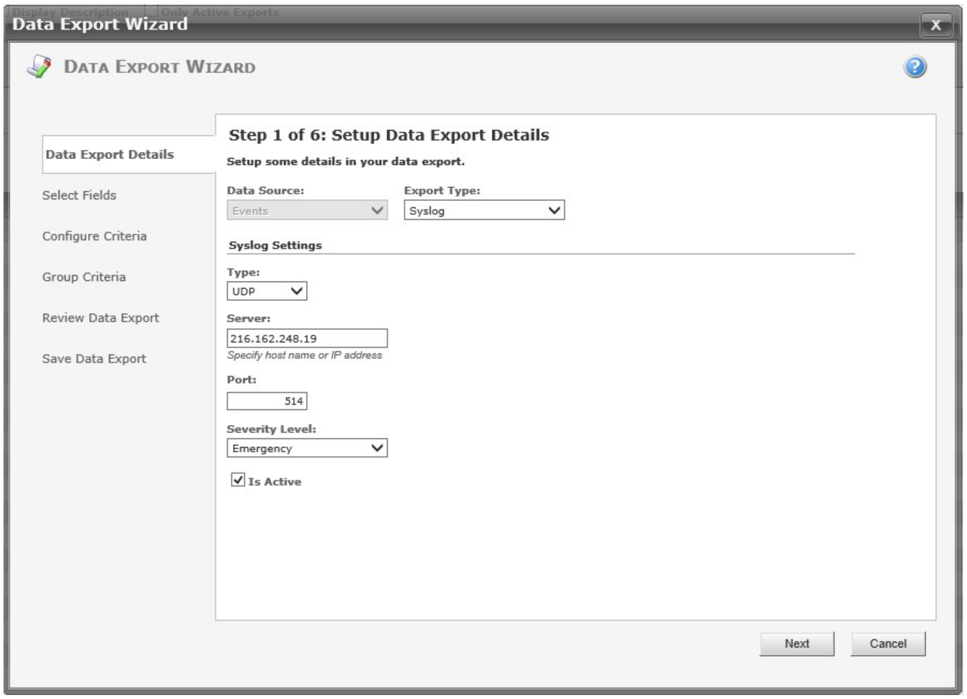
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Digital Guardian components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Digital Guardian is properly configured and secured before deploying to a production environment. For more information, please refer to the Digital Guardian documentation or website.

Digital Guardian Configuration

1. Log in to the Digital Guardian Management Console.
2. Use the **workspace > data** export tab use the **Hostname/IP address** of the RSA Security Analytics server. Use the data export type **Syslog**.



Step 1 of 6: Setup Data Export Details

Setup some details in your data export.

Data Source: Events

Export Type: Syslog

Syslog Settings

Type: UDP

Server: 216.162.248.19

Specify host name or IP address

Port: 514

Severity Level: Emergency

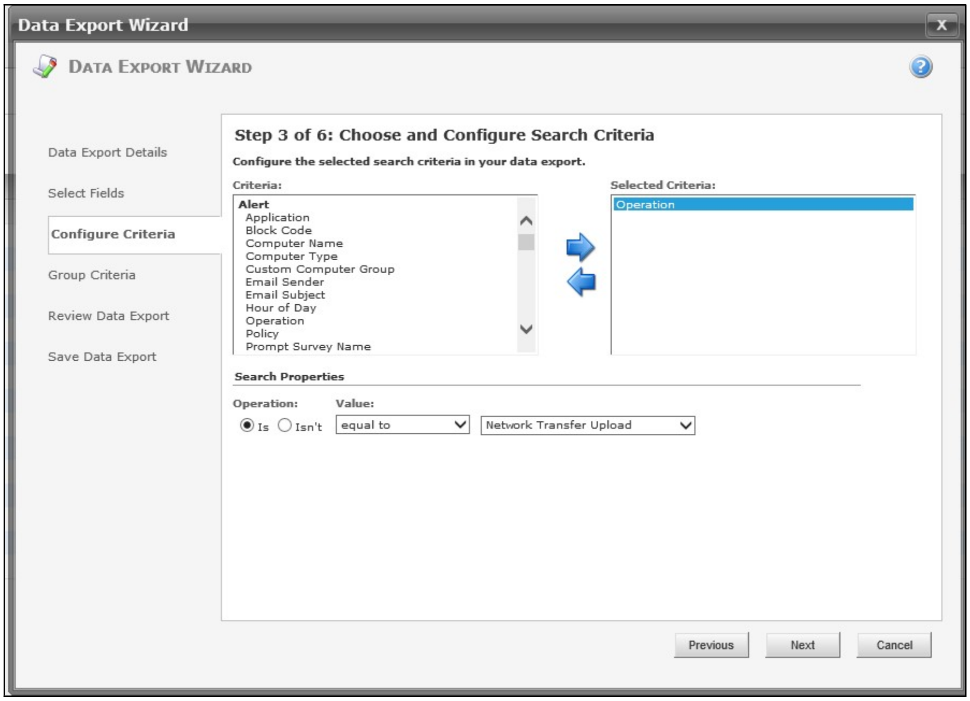
☑ Is Active

3. Select only the following 63 fields to export. All fields must be selected. The alert severity field will be mapped to the magnitude field in Security Analytics. If the there is no severity, then the Syslog severity will be mapped.

! Important: All 63 Fields must be selected alphabetically as shown above or log messages will not parse correctly within NetWitness.

Agent Local Date
Agent Local Time
Agent UTC Date
Agent UTC Time
Application
Computer Name
Computer Type
Email Sender
Email Subject
Operation
Policy Rule
Severity
Destination Directory
Destination File
Detail File Size DNS Hostname
Email Recipient
Email Recipient Type
IP Address
Local Port
Printer
Printer Jobname
Protocol
Remote Port
Source Directory
Source DNS Hostname
Source File
Source IP Address
URL Path
Was Destination Classified
Was Destination Removable
Was Screen Captured
Was Source Classified
Was Source File Captured
Was Wireless
Source Drive Type
Source Device Custom ID
Source Device Class
Source Device ID
Source Device Friendly Name
Source Device Product ID
Source Device Product Name
Source Device Removal Policy
Source Device Serial Number
Source Device Storage Bus Type
Source Device Supports Predict Failure
Source Device Vendor
Source Device Vendor ID
Destination Drive Type
Destination Device Custom ID
Destination Device Class Destination Device ID
Destination Device Friendly Name
Destination Device Product ID
Destination Device Product Name
Destination Device Removal Policy
Destination Device Serial Number
Destination Device Storage Bus Type
Destination Device Supports Predict Failure
Destination Device Vendor
Destination Device Vendor ID
User ID

4. Choose and configure the search criteria. By default, the Criteria field is blank. Selecting the criteria limits the amount of data exported. If no criterion is selected Digital Guardian will export all data (not recommended).



Step 3 of 6: Choose and Configure Search Criteria

Configure the selected search criteria in your data export.

Criteria:
Alert
Application
Block Code
Computer Name
Computer Type
Custom Computer Group
Email Sender
Email Subject
Hour of Day
Operation
Policy
Prompt Survey Name

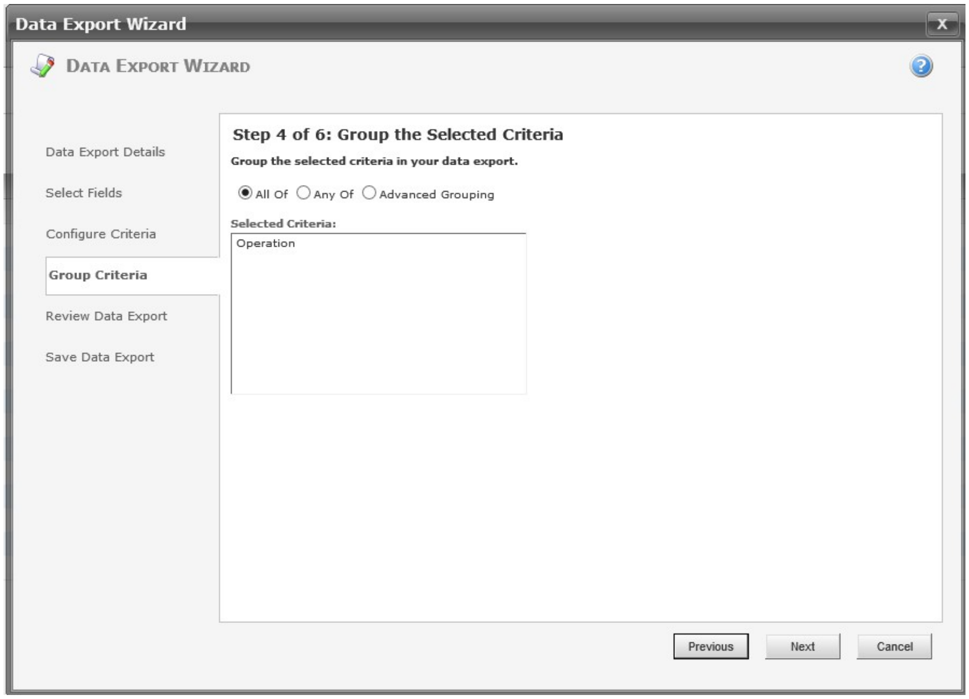
Selected Criteria:
Operation

Search Properties

Operation: ● Is ○ Isn't

Value: equal to | Network Transfer Upload

5. Group the selected criteria (optional). By default, the Criteria field is blank.



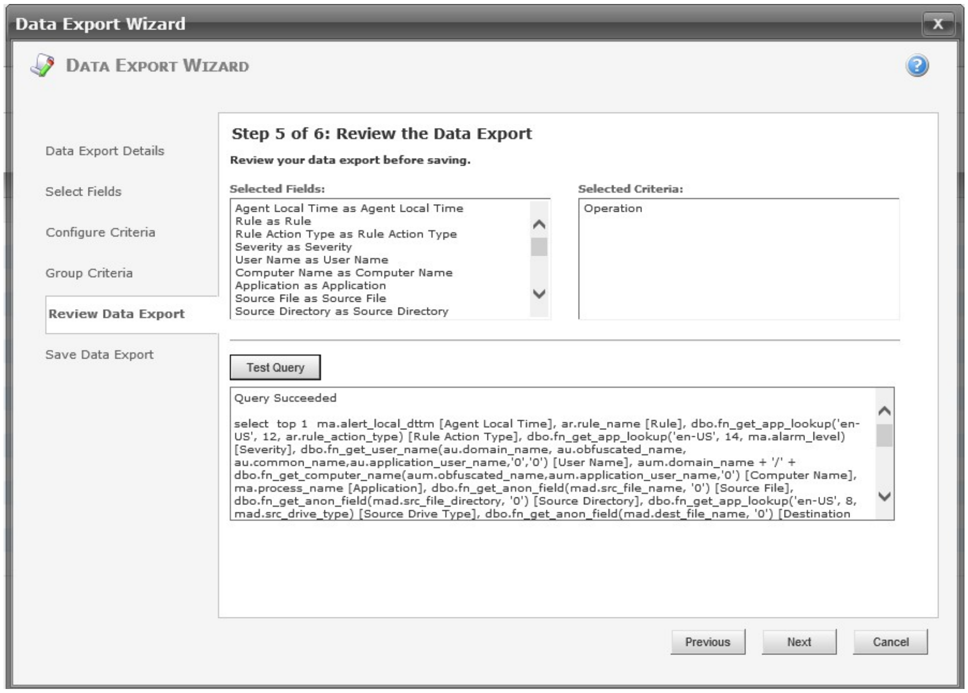
Step 4 of 6: Group the Selected Criteria

Group the selected criteria in your data export.

● All Of ○ Any Of ○ Advanced Grouping

Selected Criteria:
Operation

6. Review the data export. A **Test Query** ensures the database runs properly.



Step 5 of 6: Review the Data Export

Review your data export before saving.

Selected Fields:

Agent Local Time as Agent Local Time
Rule as Rule
Rule Action Type as Rule Action Type
Severity as Severity
User Name as User Name
Computer Name as Computer Name
Application as Application
Source File as Source File
Source Directory as Source Directory

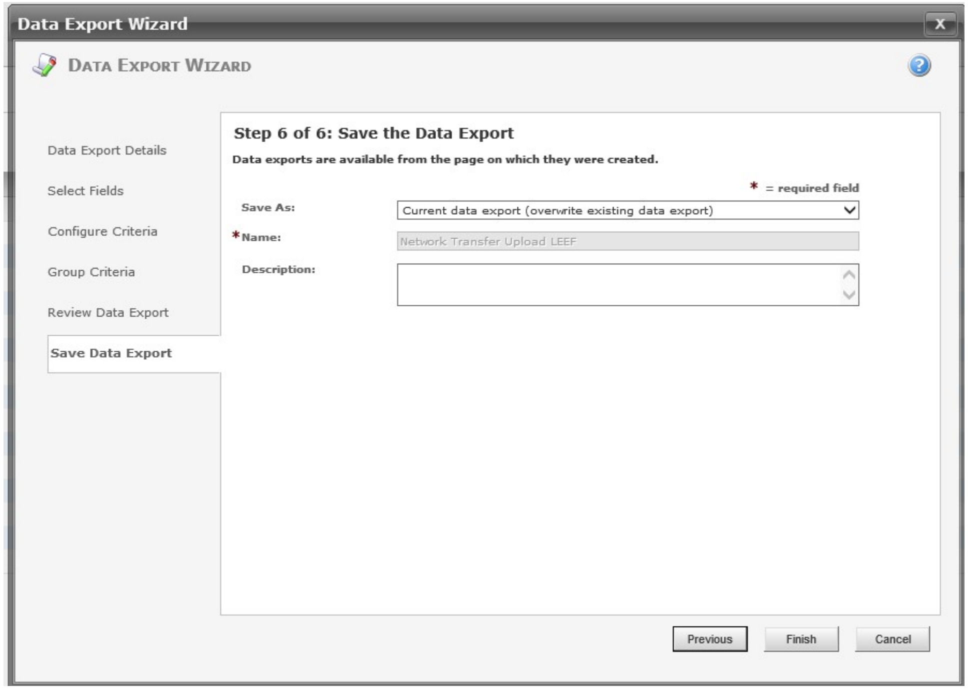
Selected Criteria:

Operation

```
Query Succeeded

select  top 1  ma.alert_local_dttm [Agent Local Time], ar.rule_name [Rule], dbo.fn_get_app_lookup('en-
US', 12, ar.rule_action_type) [Rule Action Type], dbo.fn_get_app_lookup('en-US', 14, ma.alarm_level)
[Severity], dbo.fn_get_user_name(au.domain_name, au.obfuscated_name,
au.common_name,au.application_user_name,'0','0') [User Name], aum.domain_name + '/' +
dbo.fn_get_computer_name(aum.obfuscated_name,aum.application_user_name,'0') [Computer Name],
ma.process_name [Application], dbo.fn_get_anon_field(mad.src_file_name, '0') [Source File],
dbo.fn_get_anon_field(mad.src_file_directory, '0') [Source Directory], dbo.fn_get_app_lookup('en-US', 8,
mad.src_drive_type) [Source Drive Type], dbo.fn_get_anon_field(mad.dest_file_name, '0') [Destination
```

7. Save the data export. Click **Finish**.



Step 6 of 6: Save the Data Export

Data exports are available from the page on which they were created.

* = required field

Save As: Current data export (overwrite existing data export)

*Name: Network Transfer Upload LEEF

Description:

Certification Checklist for RSA NetWitness

Date Tested: December 2, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.2	Virtual Appliance
Digital Guardian	6.1	Microsoft Windows 2003

NetWitness Test Case	Result
Device Administration	
Partner's device name appears in Device Parsers Configuration	✓
Device can be enabled from Device Parsers Configuration	✓
Device can be disabled from Device Parsers Configuration	✓
Device can be removed from Device Parsers Configuration	✓
Investigation	
Device name displays properly from Device Type	✓
Displays Meta Data properly within Investigator	✓

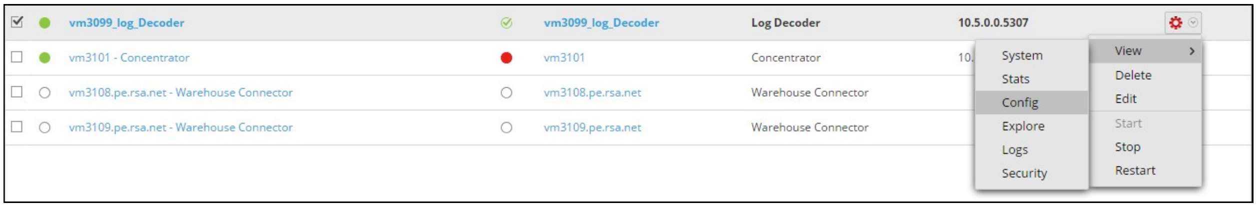
✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

NetWitness Disable Device Parser

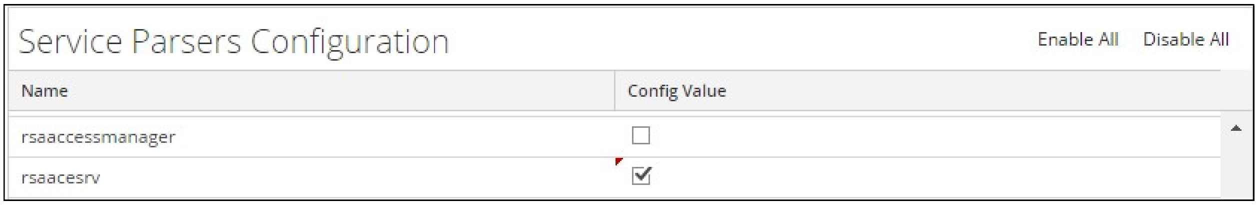
To disable the NetWitness Integration Package but not delete the XML from the system, perform the following:

1. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View> Config.**



☑	●	vm3099_log_Decoder	✓	vm3099_log_Decoder	Log Decoder	10.5.0.0.5307
☐	●	vm3101 - Concentrator	●	vm3101	Concentrator	10.
☐	○	vm3108.pe.rsa.net - Warehouse Connector	○	vm3108.pe.rsa.net	Warehouse Connector	
☐	○	vm3109.pe.rsa.net - Warehouse Connector	○	vm3109.pe.rsa.net	Warehouse Connector	

2. From the **Service Parses Configuration** window, scroll down to the device you wish to disable and uncheck the Config Value checkbox.



Service Parsers Configuration

Name	Config Value
rsaaccessmanager	☐
rsaacesrv	☑

3. Click **Apply** to save settings.

NetWitness Remove Device Parser

To remove the NetWitness Integration Package files from the environment, perform the following:

1. Connect to the NetWitness Log Decoder/Collector Server using SSH and open the **/etc/netwitness/ng/envision/etc/devices** folder.
2. Search for the device you are targeting for removal and delete the folder containing the device xml.
3. Returning the system to its original state will require either modifying or removing the **table-map-custom.xml** based on your systems configuration. The table-map-custom.xml file is located in the **/etc/netwitness/ng/envision/etc** folder of the NetWitness Log Decoder(s).