# RSA® NETWITNESS®
# Logs
# Implementation Guide

## Exabeam User Behavior Analytics 3.0

Daniel R. Pintal, RSA Partner Engineering
Last Modified: May 5, 2017

RSA READY

## Solution Summary

The Exabeam User Behavior Intelligence platform provides user behavior analysis on top of existing SIEM and log management data repositories to detect compromised and rogue insiders and present a complete picture of the user session and lateral movement used in an attack chain. Exabeam uses behavior analytics and proprietary Stateful User Tracking™ to extract additional value from log data already collected and residing in the RSA Security Analytics platform.

Stateful User Tracking™ creates a full timeline of all activity for every user -- across accounts, machines, and networks -- to enable your high-value security personnel to:

- Detect advanced breaches that bypass existing technologies
- Prioritize incidents automatically, to operate efficiently
- Respond effectively, with knowledge of all impacted systems

The Exabeam solution installs easily and connects to your RSA Security Analytics without agents, network taps, or tuning.

Exabeam provides added value by scoring traditional security alerts, attributing to identities, and placing them on the timeline. All systems touched by a (potentially compromised) user credential are identified to reveal the attacker's path through the IT environment. Sessions with high risk scores can be set to trigger an alert into RSA SA workflows for further automation, correlation and centralized incident management.

In short, Exabeam provides a new layer of intelligence that detects subtle attacks that other products might miss. More importantly, the solution provides in-demand security personnel with the full picture they need to prioritize and respond effectively and efficiently, once the attack is detected.

| RSA NetWitness Features | |
|---|---|
| **Exabeam User Behavior Analytics 3.0** | |
| **Integration package name** | exabeam.envision |
| **Device display name within RSA NetWitness** | exabeampe |
| **Event source class** | analysis |
| **Collection method** | syslog |

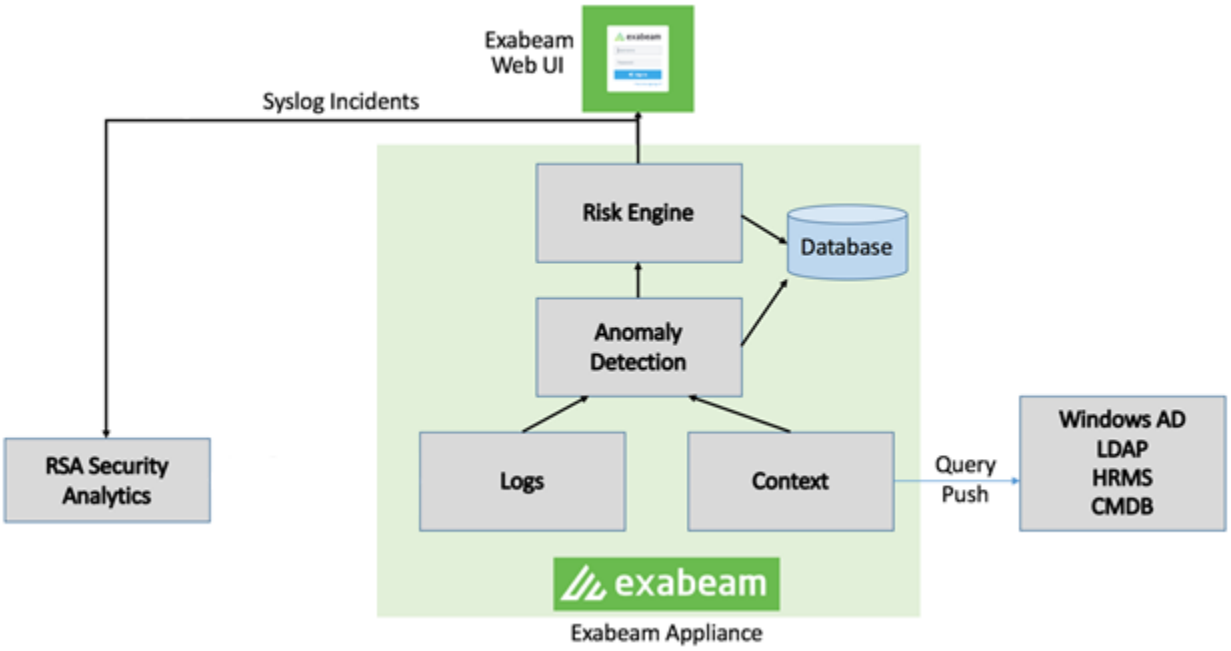



Figure 1: Exabeam Integration with RSA Security Analytics

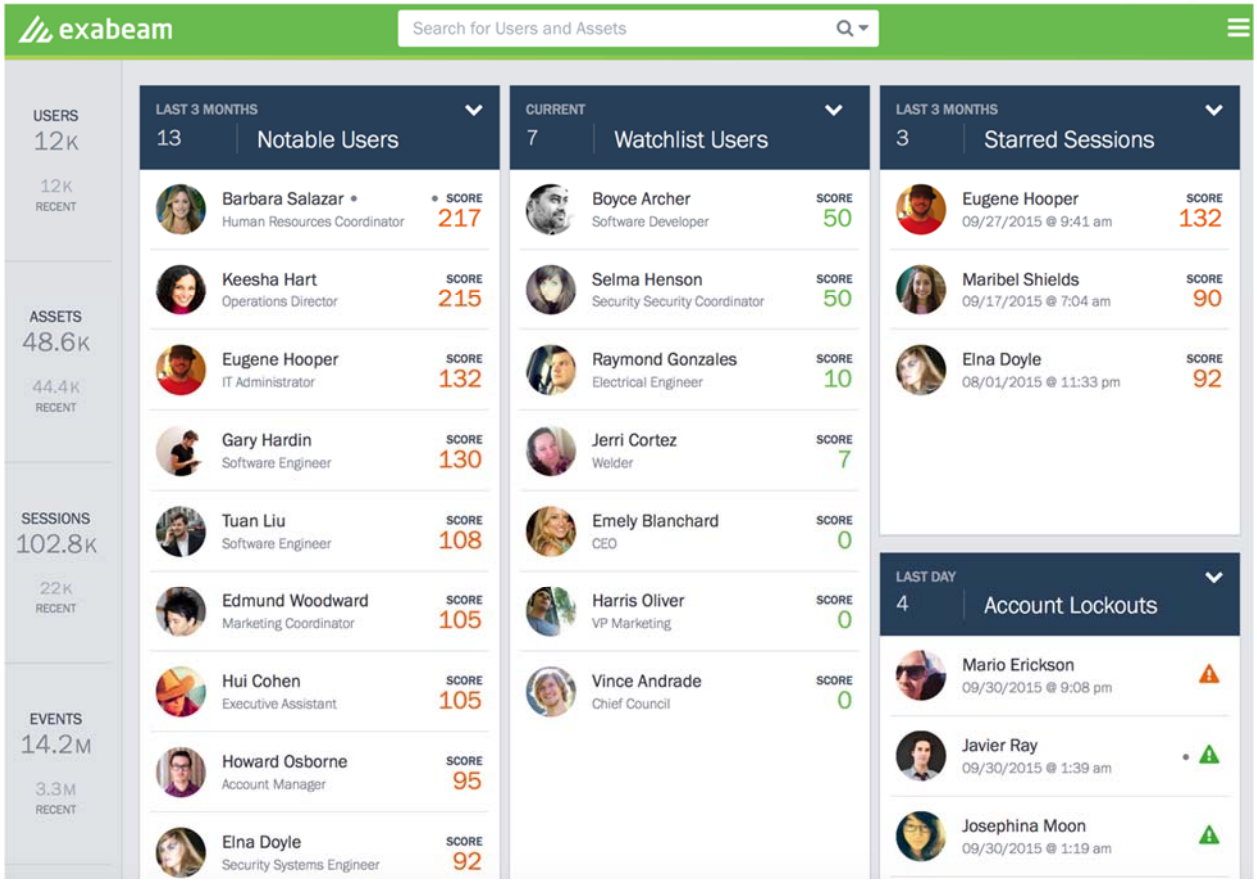



Figure 2: Exabeam User Interface

# 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 |
|---|---|
| **exabeampe.envision** | Netwitness package deployed to parse events from devices. |
| **exabeampemsg.xml** | A copy of the device xml contained within the NetWitness package. |
| **table-map-custom.xml** | Enables NetWitness keys disabled by default. |
| | |

# Release Notes

| Release Date | What's New In This Release |
|---|---|
| 11/11/2016 | Initial support for Exabeam. |
| | |

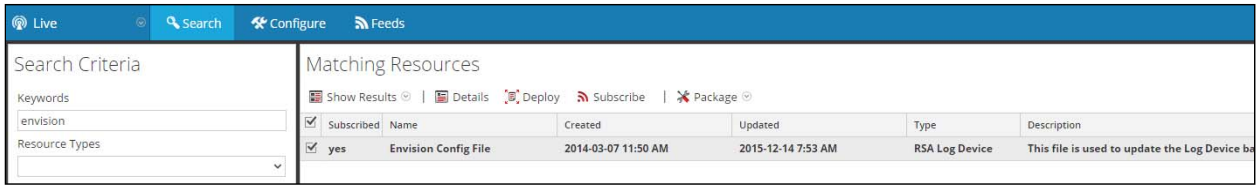
# RSA NetWitness Configuration

## *Deploy the enVision Config File*

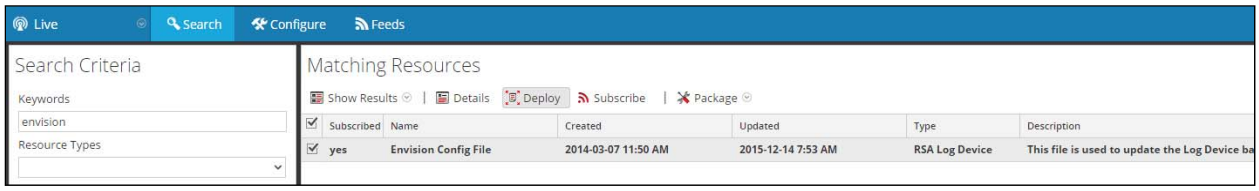
In order to use RSA Partner created content, you must first deploy the *Envision Config File* from the **NetWitness Live** module. Log into RSA NetWitness and perform the following actions:

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

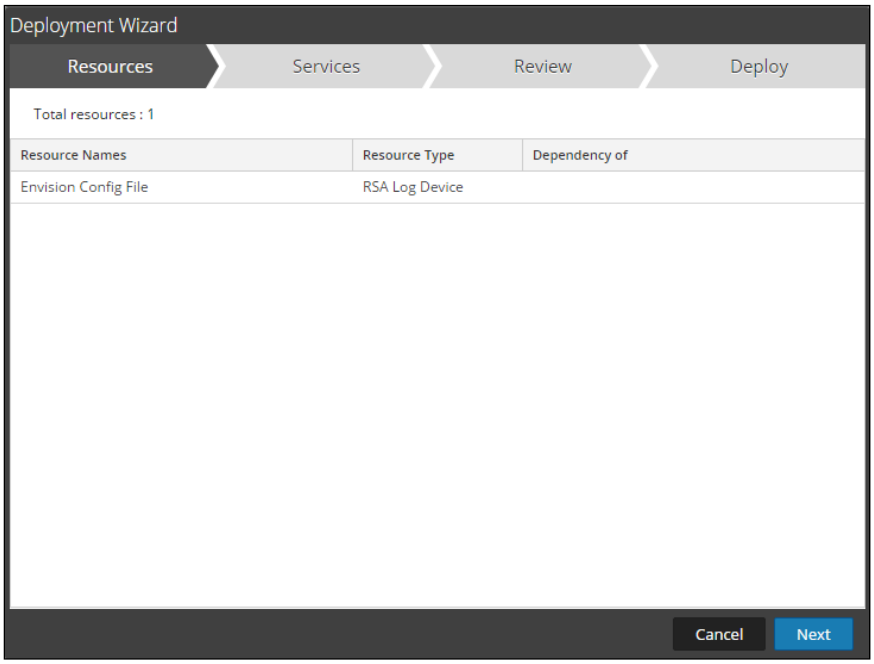
1. From the NetWitness menu, select **Live > Search**.
2. In the keywords field, enter: **Envision**.
3. NetWitness will display the **Envision Config File** in Matching Resources.
4. Select the checkbox next to **Envision Config File**.



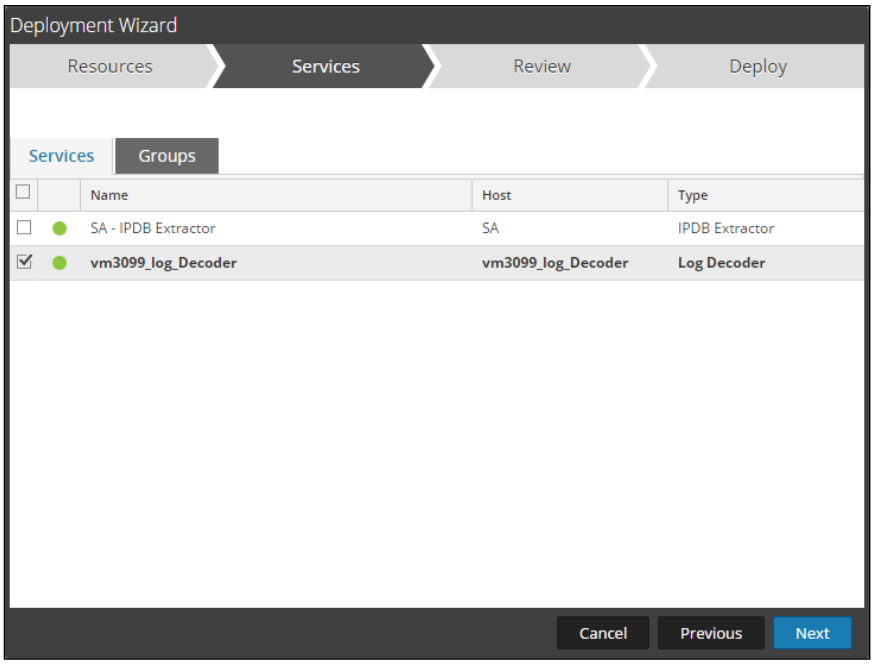

5. Click **Deploy** in the menu bar.



6. Select **Next**.

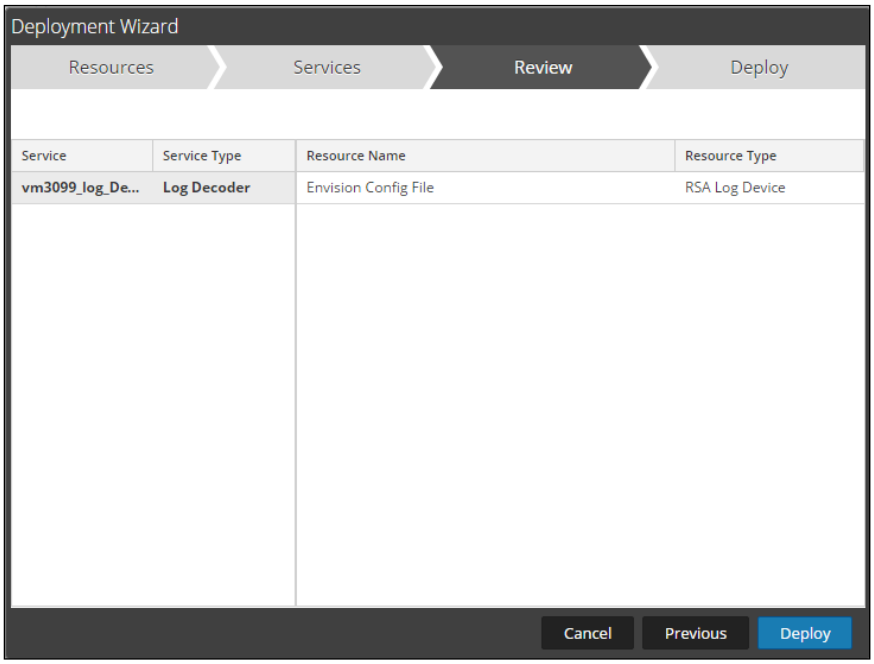



7. Select the **Log Decoder** and select **Next**.

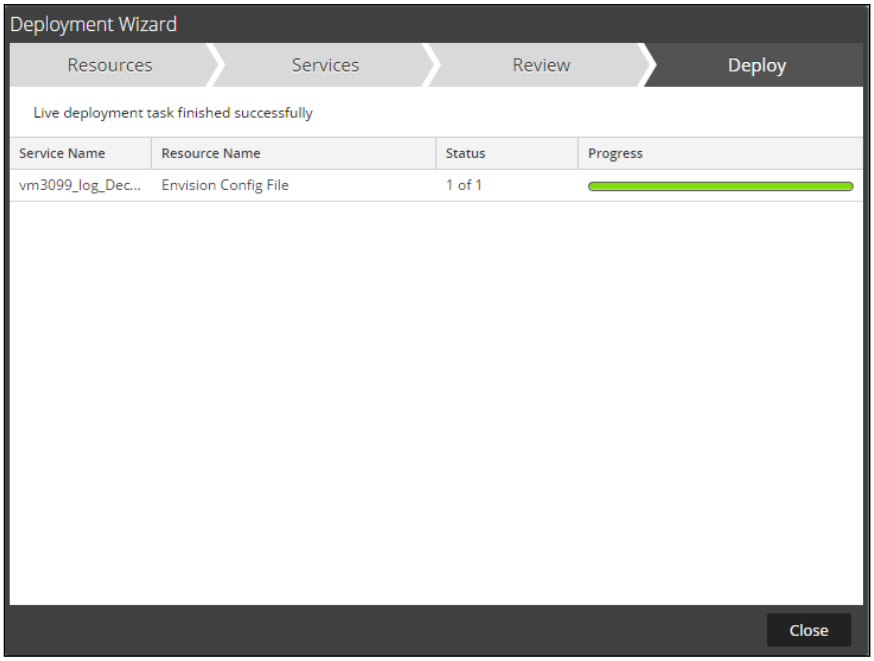



**Important: In an environment with multiple Log Decoders, deploy the Envision Config File to each Log Decoder in your network.**

8. Select **Deploy**.



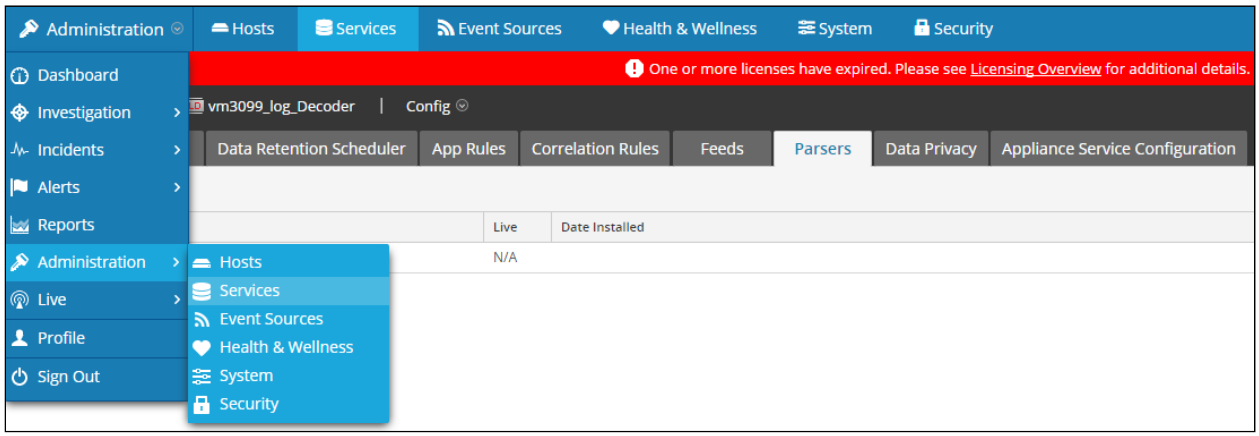

9. Select **Close**, to complete the deployment of the Envision Config file.



## *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:

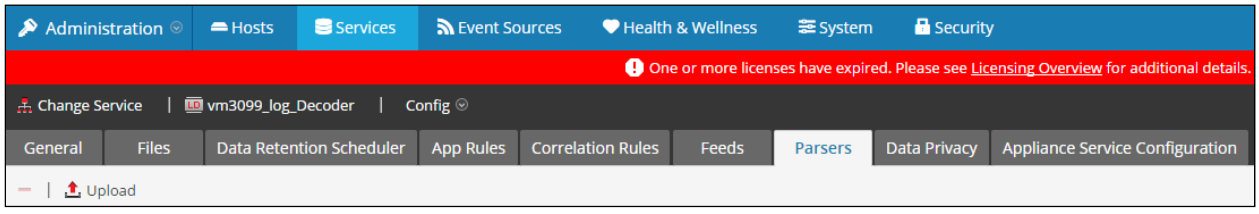
1. From the NetWitness menu, select **Administration > Services.**




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

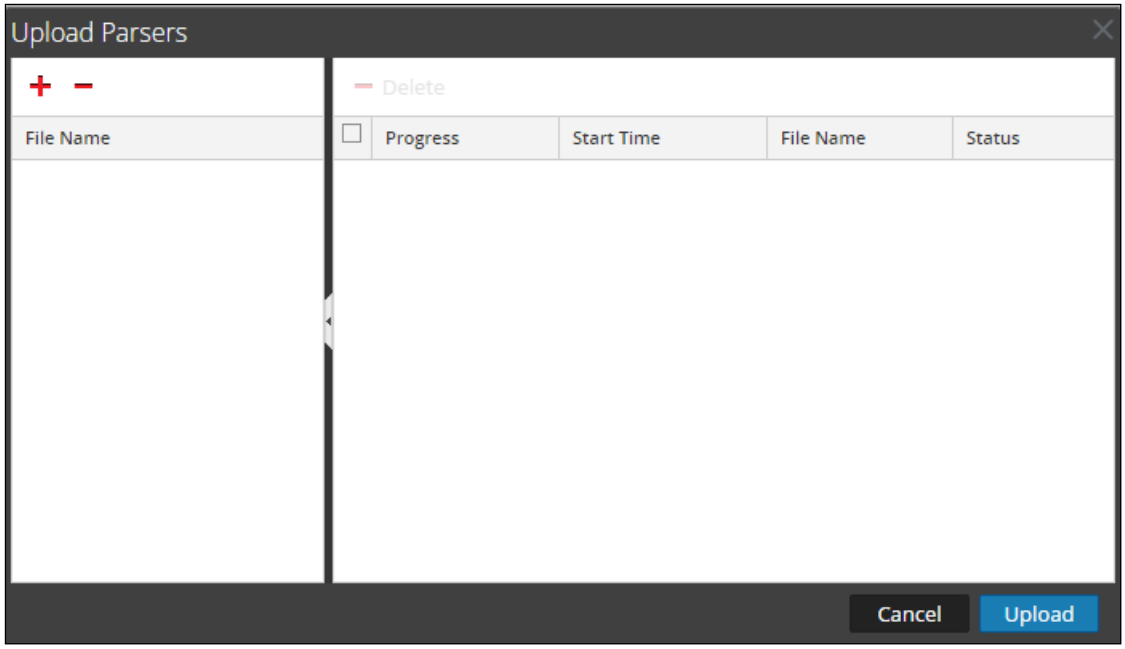

> **Important: In an environment with multiple Log Decoders, repeat on the deployment of the RSA Partner Integration Package on each Log Decoder.**

3. Next, select the **Parsers** tab and click the **Upload** button.

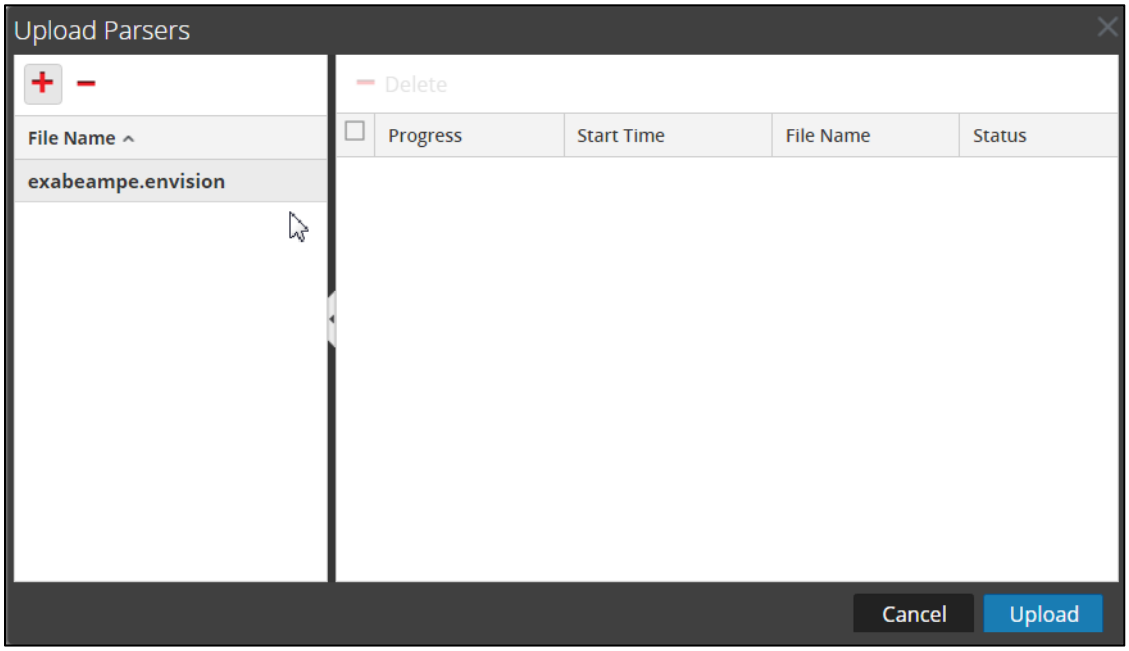


4. From the *Upload Parsers* window, click the + **Add** button and select the *.envision* file.

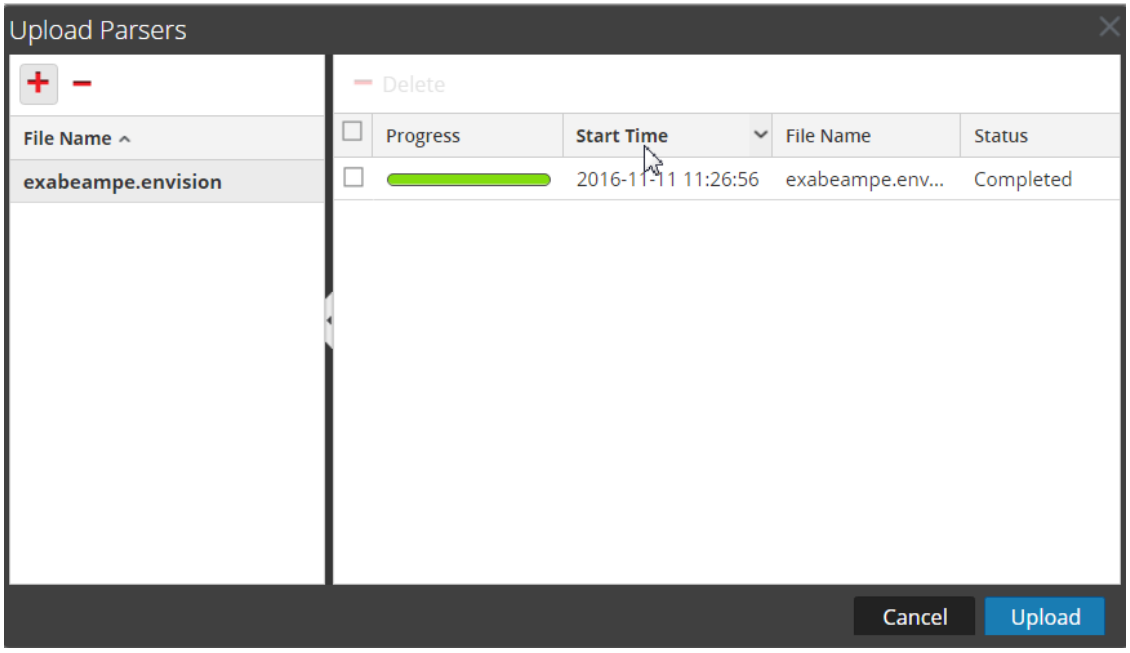
> **Important: The .envision file is contained within the .zip file downloaded from the RSA Community.**




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



6. Upon completion of the upload click **Cancel**.



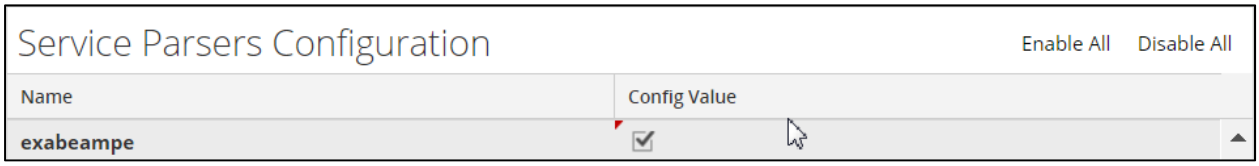

7. Connect to the Security Analytics Log Decoder Server using WinSCP. Copy the *table-map-custom.xml* file from the contents of the .zip file to the */etc/netwitness/ng/envision/etc* folder. If the *table-map-custom.xml* file already exists on the log decoder(s), enter only the contents between the *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

```
<mappings>

    <mapping envisionName="sessionid" nwName="log.session.id" flags="None"/>
    <mapping envisionName="url" nwName="url" flags="None" envisionDisplayName="URL"/>
    <mapping envisionName="trigger_val" nwName="trigger.val" flags="None"/>
    <mapping envisionName="status" nwName="status" flags="None"/>
    <mapping envisionName="user_dept" nwName="user.dept" flags="None"/>
    <mapping envisionName="info" nwName="index" flags="None"/>
    <mapping envisionName="location_desc" nwName="loc.desc" flags="None"/>
    <mapping envisionName="number" nwName="number" flags="None"/>
    <mapping envisionName="inout" nwName="inout" flags="None"/>
    <mapping envisionName="ntype" nwName="ntype" flags="None"/>
    <mapping envisionName="starttime" nwName="starttime" flags="None" format="TimeT" envisionDisplayName="StartTime"/>
    <mapping envisionName="endtime" nwName="endtime" flags="None" format="TimeT" envisionDisplayName="EndTime"/>

</mappings>
```

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

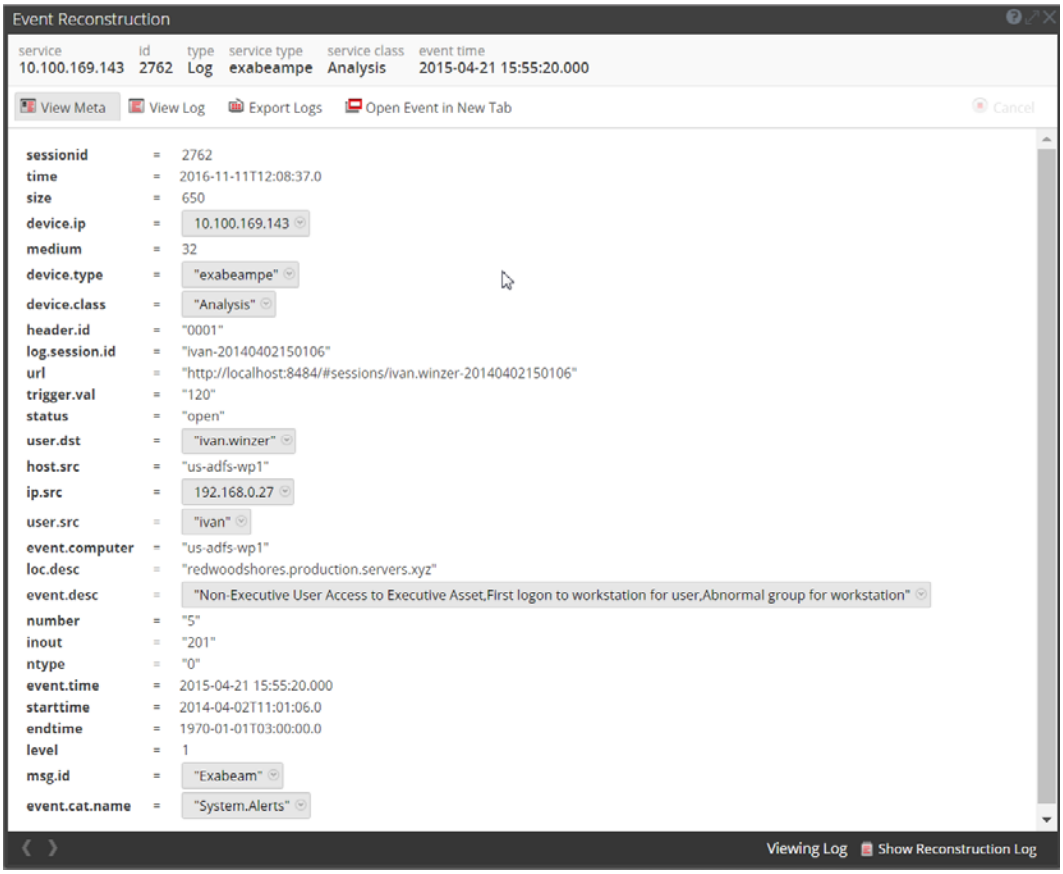

9. Navigate to **Administration > Services** and check the **Log Decoder(s)** then click **View> Config.**


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




**Important: Check the Config Value if not checked by default.**

11. The Log Decoder is now ready to parse events for this device. Below is an example of the metadata collected from a sample Exabeam logfile.



# Partner Product Configuration

## *Before You Begin*

This section provides instructions for configuring Exabeam 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.

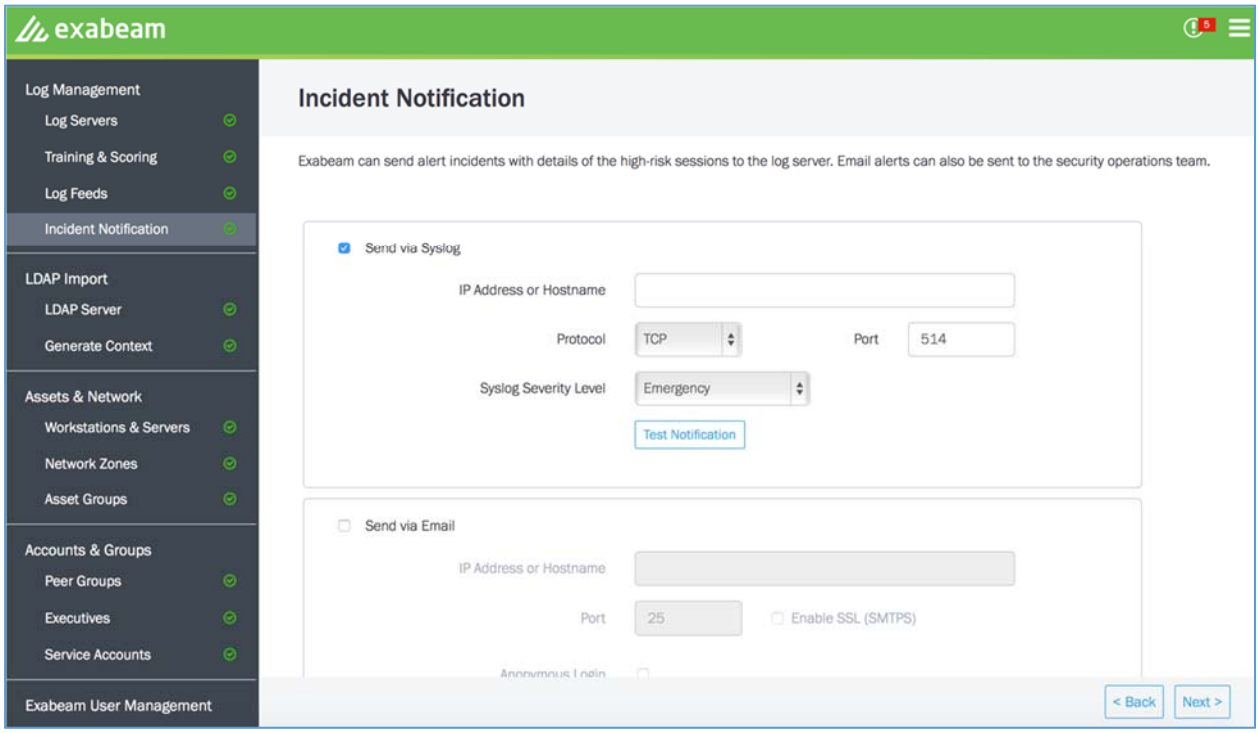
All Exabeam components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

**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 Exabeam User Behavior Analytics is properly configured and secured before deploying to a production environment. For more information, please refer to the Exabeam User Behavior Analytics documentation or website.**

## *Exabeam User Behavior Analytics Configuration*

Follow the instructions specified in the **Exabeam Administration Guide (login required)** to learn how to perform administrative tasks through the Exabeam UI and from the command line. We will explain the architecture behind Exabeam, the ways in which Exabeam interfaces and uses your log and contextual information, guide you through the deployment of the Exabeam Appliance and the setup process, and teach you how to operationalize, manage, and monitor the Exabeam solution.

Incident alerts, with details of any high-risk sessions, can be sent to RSA Security Analytics for reporting and incident investigations. They can also be sent via Syslog to another SIEM or by email directly to the analysts.



# Certification Checklist for RSA NetWitness

Date Tested: November 11, 2016

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| RSA NetWitness | 10.6 | Virtual Appliance |
| Exabeam User Behavior Analytics | 3.0 | Virtual or Physical Appliance |
| | | |

| Security Analytics 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

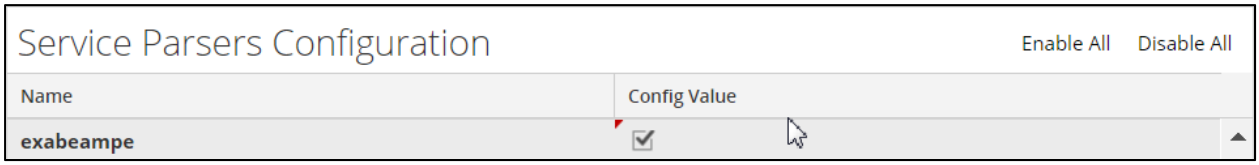
# Appendix

## Security Analytics 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.**


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




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).