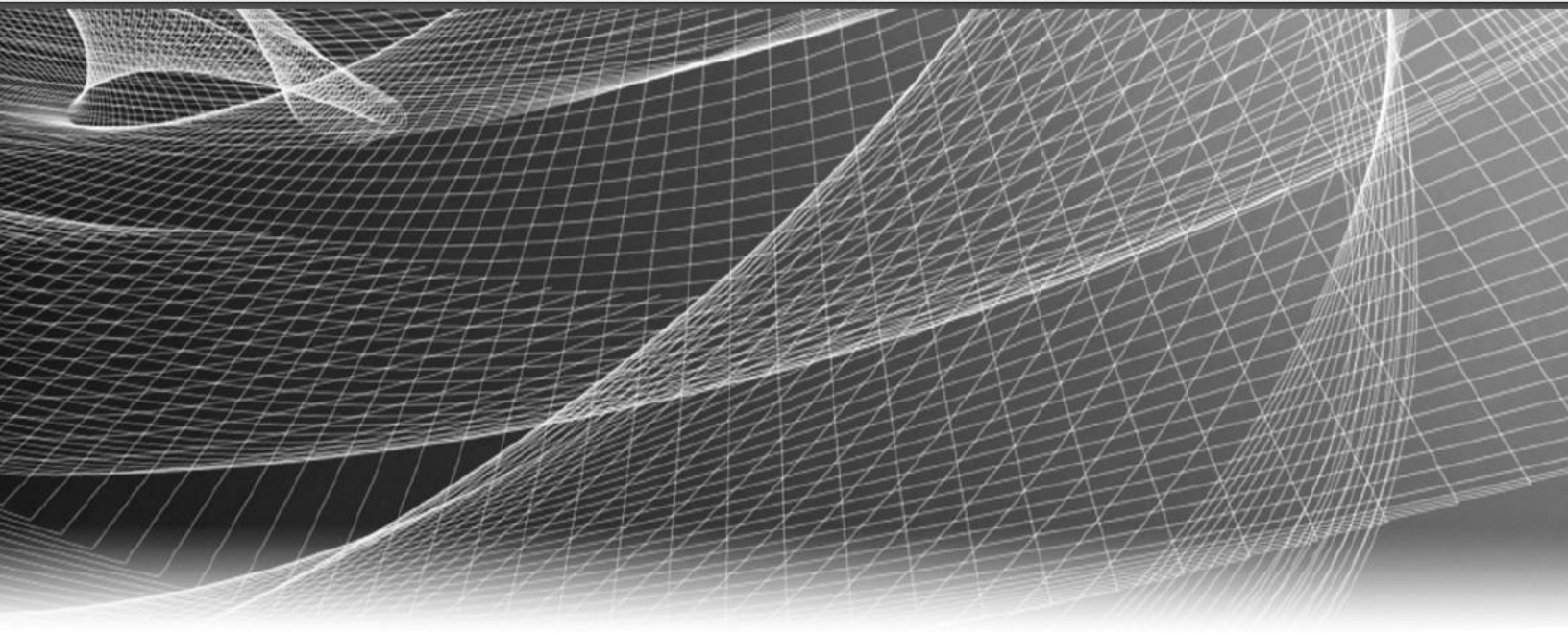


RSA | Security Analytics

FireEye – RSA NetWitness® Suite Integration

RSA

EMC²

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Contents

RSA NetWitness Native Integration with FireEye

The RSA NetWitness Native Integration solution within FireEye Web MPS enables customers to perform deeper, joint forensic analysis. Logs and packets captured in RSA NetWitness are associated with the alerts generated by the FireEye Web MPS as it detects advanced malware on the network.

This document describes the steps used to enable and configure the integration of the FireEye Web MPS appliance and the RSA NetWitness (formerly known as Security Analytics) Infrastructure, which is comprised of at least three components: Decoders, Concentrators, and Brokers.

NOTE: The FireEye/RSA NetWitness integration is supported on the FireEye Web MPS product only at this time.

Configure the Web MPS appliance to communicate with RSA NetWitness using the steps provided in the next section. In general, the **Filtered Events Detail** page in the Web MPS Web UI provides a link (URI) that accesses the associated packet capture data in the RSA NetWitness console (Web UI) for the RSA NetWitness Broker or Concentrator. The Web MPS link opens a RSA NetWitness Broker or Concentrator Investigation view that will display all packets within +/- 2 minutes of Web MPS detection. The source or destination IP in RSA NetWitness is matched with the FireEye detection alert.

This integrated joint solution includes the ability to add more context to a FireEye event, such as discovering which component of the detected malware may have called in a malicious frame, or determining how much communication occurred between the malware and its CnC server.

Configuring FireEye Web MPS for RSA NetWitness Integration

Use the following procedure to configure FireEye Web MPS integration with RSA NetWitness.

Enabling/Disabling RSA NetWitness Analysis on Web MPS

Use the following CLI command to enable or disable RSA NetWitness analysis on the Web MPS appliance. A user must enable the RSA NetWitness integration in order to use it.

To enable RSA NetWitness integration:

```
wmps-7300 (config)# netwitness analysis enable
```

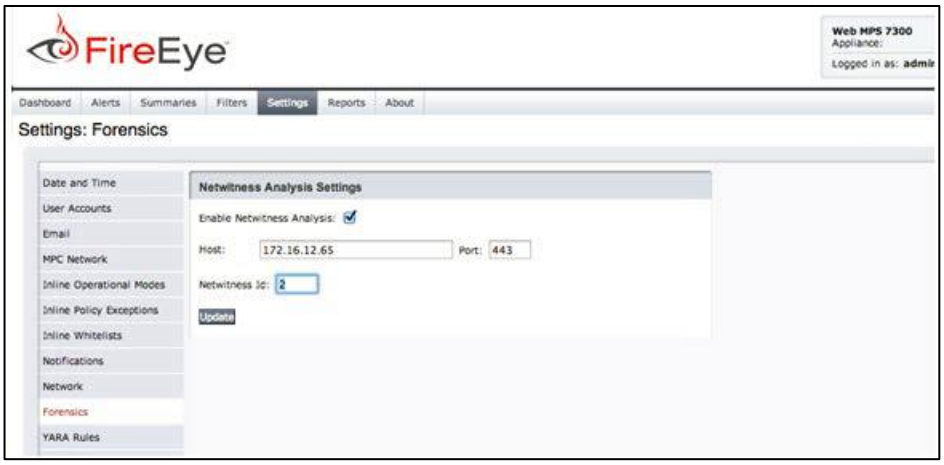
To disable RSA NetWitness integration:

```
wmps-7300 (config)# no netwitness analysis enable
```

Configuring RSA NetWitness Device Coordinates on the FireEye Web MPS

After enabling the RSA NetWitness integration feature, a configuration page becomes available in the FireEye Web MPS Web UI in which the coordinates of the RSA NetWitness appliance (Device ID) can be specified.

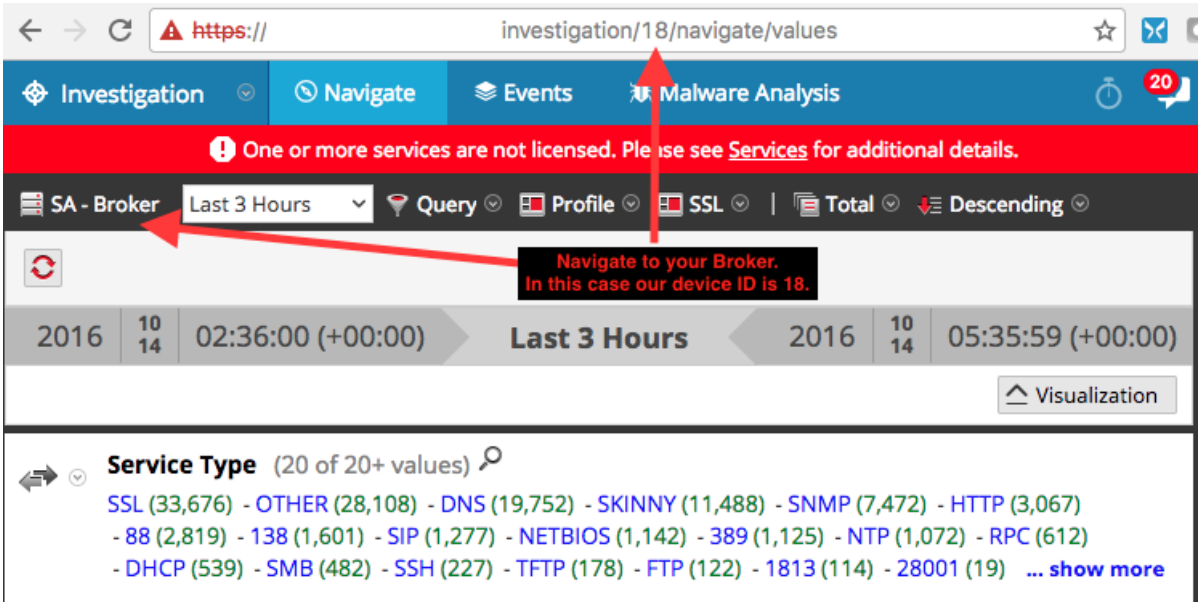
1. Navigate to the **Forensics** page from the **Settings** tab in the Web MPS Web UI.



2. Enter the IP of the SA Server, port 443 and the device ID of your primary investigation device. This will typically be the device ID of a broker in RSA NetWitness environments with multiple Concentrators. If your RSA NetWitness environment only has one Concentrator you can use your Concentrator's device ID.

To determine your RSA NetWitness device ID, login to your RSA NetWitness UI and perform an investigation on your top level Broker. This is the Broker which aggregates data from the various Concentrators. Once the investigation screen loads for your Broker look at your URL. An example is shown below. The device ID in the URL below is: 2.

Here's another screenshot of how to find your device ID:



NOTE: The Concentrators aggregate meta-data associated with the packets captured by the RSA NetWitness Decoders. This information is used in the packet capture queries sent to the RSA NetWitness device configured in the screenshot above.

Extended Forensics from the Web MPS

Once enabled, the Web MPS Web UI displays extended forensics information received from the RSA NetWitness Appliance.
To view the integrated RSA NetWitness data in the Web MPS via the **Filtered Events Detail** Web UI page:

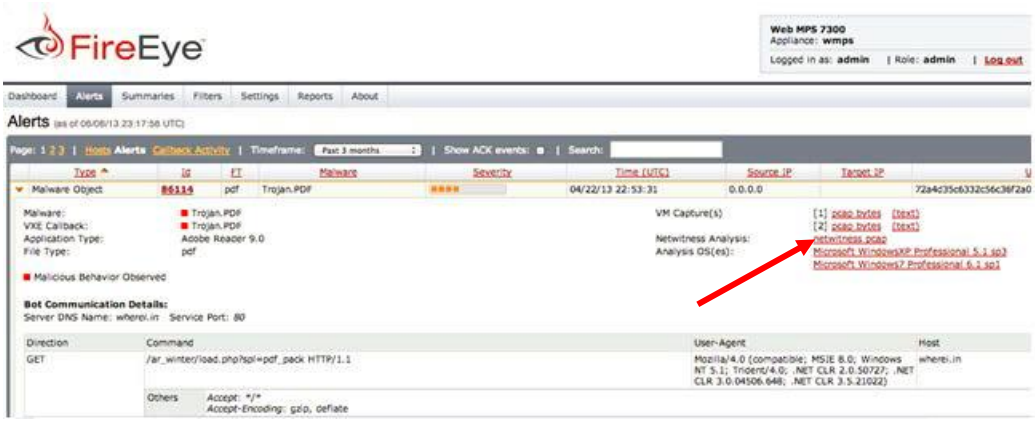
1. Navigate to the **Alerts** tab in the Web MPS Web UI.

2. Click on the **Host** sub-tab link to display the **Alerts-Host** view. This view shows all "infected Hosts" detected by Web MPS in a specified time-frame.

3. To examine a specific "Infected Host," click on the link under the **Total** column for that host; the **Filtered-Events** view displays all the alerts detected for a specific host.

4. From the **Filtered Events** view, click on the arrow icon to expand the selected alert and display alert details.

5. View the **NetWitness Analysis** sub-heading and its associated NetWitness pcap link as shown in the sample screen below.

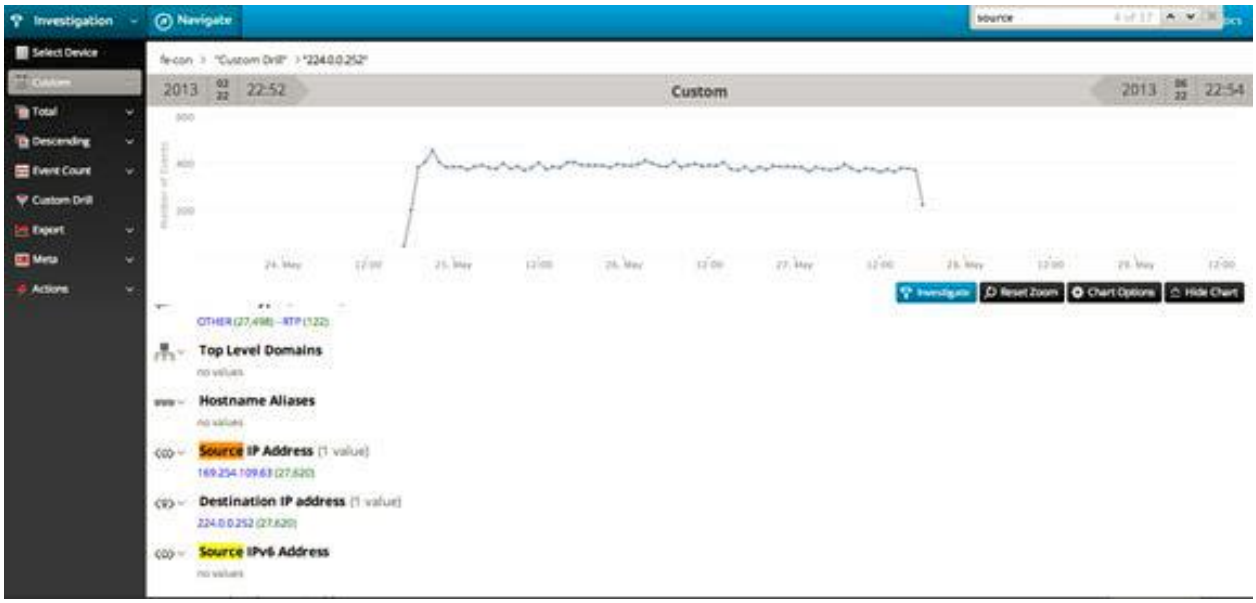


6. The "NetWitness pcap" link provides direct access to the collection of network traffic associated with the infected host (as either the source or the destination). The pcap output contains 2 minutes of relevant traffic information before and after the time-stamp of the alert.

7. The forensics links you into RSA NetWitness (an example is shown below) and provides direct access to the query Web UI in the NetWitness Broker.

Viewing Forensics Information in RSA Netwitness

The Forensics link shown in the section above will take you to the appropriate screen in the RSA NetWitness Web UI where it will look similar to the screenshot below depending on what version of RSA NetWitness you're using.



Critical Start Threat Analytics Google Chrome Extension

RSA NetWitness has the ability to conduct investigations via a web interface. Many other security tools (SIEM, IPS, threat feeds, etc.) also use a web interface. Critical Start released their Threat Analytics Search extension for Chrome that allows integration of 3rd party (web GUI) security tools with RSA NetWitness.

If you aren't familiar with the extension, it can be summarized as a:
Tool for security analysts, malware hunters, and incident responders that allows the use the of right-click menu in Chrome to conduct single or group searches for selected text such as file hash, IP address, or domain. The extension reduces time analysts spend visiting the same websites repeatedly to gather information about IP addresses, websites, file hashes, and domains.
source: https://community.fireeye.com/people/criticalstart1/blog/2014/03/31/fireeye-integration-with-rsa-netwitnesssecurity-analytics

Configuring the Critical Start extension is very simple. A detailed instructional video is located here: https://community.rsa.com/videos/21070. There is also a configuration guide on RSA Link that focuses entirely on configuring the plugin located here: https://community.rsa.com/docs/DOC-63056.

This extension allows a user to right click and drill into virtually any piece of metadata in RSA NetWitness while in virtually any one of your existing security tools.

Contact Customer Care

RSA SecureCare Online:	https://knowledge.rsasecurity.com/ or https://community.rsa.com/community/rsa-customer-support
Phone:	1-800-995-5095, option 3
International Contacts:	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email:	support@rsa.com
Community:	https://community.rsa.com/community/products/netwitness
Basic Support:	Technical Support for your technical issues is available during 8am to 5pm your local time, Monday through Friday.
Enhanced Support:	Technical Support is available by phone 24 x 7 x 365 days of the year for Severity 1 and Severity 2 issues only.

Preparing to Contact Customer Care

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

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