RSA NetWitness

Version 11.7

Malware Analysis Configuration Guide

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

March 2022

Contents

How Malware Analysis Works

NetWitness Malware Analysis is an automated malware analysis processor designed to analyze certain types of file objects (for example, Windows portable executable (PE), PDF, and MS Office) to assess the likelihood that a file is malicious.

Malware Analysis detects indicators of compromise using four distinct analysis methodologies:

- Network Session Analysis (network)
- Static File Analysis (static)
- Dynamic File Analysis (sandbox)
- Security Community Analysis (community)

Each of the four distinct analysis methodologies is designed to compensate for inherent weaknesses in the others. For example, Dynamic File Analysis can compensate for Zero-Day attacks that are not detected during the Security Community Analysis phase. By avoiding malware analysis that strictly focuses on one methodology, the analyst is more likely to be shielded from false negative results.

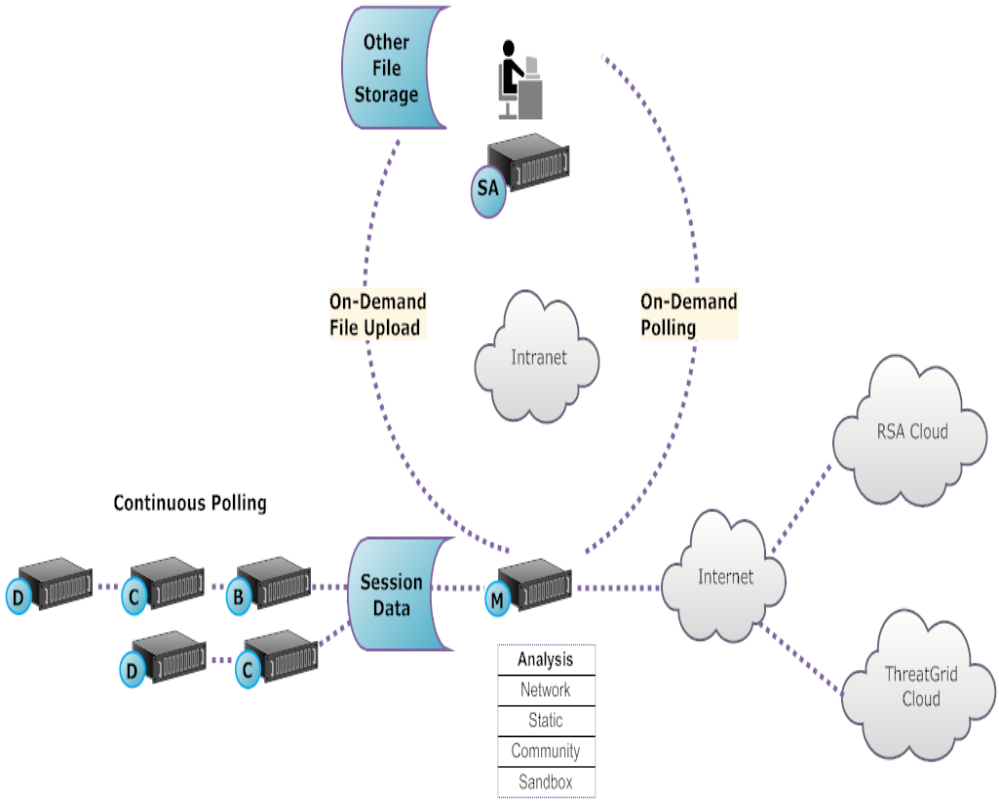
In addition to the built-in indicators of compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language, which allows malware researchers to identify and classify malware samples. This allows Indicators of Compromise (IOC) authors to add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live. These YARA-based IOCs in RSA Live will automatically be downloaded and activated on the subscribed host, to supplement the existing analysis that is performed in each analyzed file.

Malware Analysis also has features that support alerts for NetWitness Respond.

Functional Description

This figure depicts the functional relationship between the Core services (the Decoder, Concentrator, and Broker), the Malware Analysis service, and the NetWitness Server.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



The Malware Analysis service analyzes file objects using any combination of the following methods:

- **Continuous automatic polling of a Concentrator or Broker** to extract sessions identified by a parser as potentially carrying malware content.
- **On-demand polling of a Concentrator or Broker** to extract sessions identified by a malware analyst as potentially carrying malware content.
- **On-demand upload of files** from a user-specified folder.

When automatic polling of a Concentrator or Broker is enabled, the Malware Analysis service continuously extracts and prioritizes executable content, PDF documents, and Microsoft Office documents on your network, directly from data captured and analyzed by your Core service. Because the Malware Analysis service connects to a Concentrator or Broker to extract only those executable files that are flagged as possible malware, the process is both rapid and efficient. This process is continuous and does not require monitoring.

When on-demand polling of a Concentrator or Broker is chosen, the malware analyst uses Investigation to drill into captured data and choose sessions to be analyzed. The Malware Analysis service uses this information to automatically poll the Concentrator or Broker and to download the specified sessions for analysis.

On-demand upload of files provides a method for the analyst to review files captured external to the Core infrastructure. The malware chooses a folder location and identify one or more files to be uploaded and analyzed by Malware Analysis. These files are analyzed using the same methodology as files automatically extracted from network sessions.

Analysis Method

For the Network analysis, the Malware Analysis service looks for characteristics that seem to deviate from the norm, much as an analyst does. By looking at hundreds to thousands of characteristics and combining the results into a weighted scoring system, legitimate sessions that coincidentally have a few abnormal traits are dismissed, while the actual bad ones are highlighted. A user can learn patterns that indicate anomalous activity in the sessions as indicators that warrant further investigation, Indicators of Compromise.

The Malware Analysis service can perform Static analysis against suspicious objects it finds on the network and determine whether those objects contain malicious code. For Community analysis, new malware detected on the network is pushed to the RSA Cloud for checking against RSA's own malware analysis data and feeds from the SANS Internet Storm Center, SRI International, the Department of the Treasury and VeriSign. For Sandbox analysis, the services can also push data into major security, information and event management (SIEM) hosts (the ThreatGRID Cloud).

Malware Analysis has a unique method for analysis that is partnered with industry leaders and experts, so their technologies can enrich the Malware Analysis scoring system.

NetWitness Server Access to the Malware Analysis Service

The NetWitness Server is configured to connect to the Malware Analysis service and import tagged data for deeper analysis in Investigation. Access is based on three subscription levels.

- Free subscription: All NetWitness customers have a free subscription, with a free trial key for ThreatGRID analysis. The Malware Analysis service is rate-limited to 100 file samples per day. The number of samples (within the set of files from above) submitted to the ThreatGRID Cloud for sandbox analysis is limited to 5 per day. If one network session had 100 files in it, customers would hit the rate limit after processing the one network session. If 100 files were manually uploaded, that would cause the rate limit to be reached.
- Standard subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGRID Cloud for sandbox analysis is 1000 per day.
- Enterprise subscription tier: The number of submissions to the Malware Analysis service is unlimited. The number of samples submitted to the ThreatGRID Cloud for sandbox analysis is 5000 per day.

Scoring Method

By default, the Indicators of Compromise (IOC) are tuned to reflect industry best practices. During analysis, the IOCs that trigger cause the score to move upward or downward to indicate the likelihood that the sample is malicious. The tuning of IOCs is exposed in NetWitness so that the malware analyst can choose to override the assigned score or to disable an IOC from being evaluated. The analyst has the flexibility to either use the default tuning, or to completely customize the tuning to specific needs.

YARA-based IOCs are interleaved with the built-in IOCs within each built-in category and are not distinguished from native IOCs. When viewing IOCs in the Service Configuration view, administrators can select YARA from the Module selection list to see a list of YARA rules.

After a session is imported into NetWitness, all of the viewing and analysis capabilities in Investigation are available to further analyze Indicators of Compromise. When viewed in Investigation, YARA IOCs are distinguished from the built-in native IOCs by the tag `Yara rule`.

Deployment

The Malware Analysis service is deployed as a separate RSA Malware Analysis host. The dedicated Malware Analysis host has an onboard Broker which connects to the Core infrastructure (either another Broker or a Concentrator). Prior to this connection, a collection of parsers and feeds must be added to the Decoders that are connected to the Concentrators and Brokers from which the Malware Analysis service pulls data. This allows suspicious data files to be marked for extraction. These files are `malware analysis` tagged content available through the RSA Live content management system.

Scoring Modules

RSA NetWitness Malware Analysis analyzes and scores sessions and the embedded files within these sessions by scoring four categories: Network, Static Analysis, Community, and Sandbox. Each category comprises many individual rules and checks that are used to calculate a score between -100 and 100. The higher the score, the more likely the session is to be malicious and worthy of more in-depth follow-on investigation.

Malware Analysis can facilitate a historical investigation into events leading up to a network alarm or incident. If you know that a certain type of activity is taking place on your network, you can select only the reports of interest to examine the content of data collections. You can also modify behavior for each scoring category based on the scoring category or the file type (Windows PE, PDF, and Microsoft Office).

Once you become familiar with data navigation methods, you can explore the data more completely through:

- Searching for specific types of information
- Reviewing specific content in detail.

Category scores for Network, Static Analysis, Community, and Sandbox are maintained and reported independently. When events are viewed based on the independent scores, as long as one category detects malware, it is evident in the Analysis section.

Network

The first category examines each core network session to determine if the delivery of the malware candidates was suspicious. For example, benign software being downloaded from a well-known safe site, using proper ports and protocols, is considered less suspicious than downloading software known to be malicious from a known dubious download site. Sample factors used in the scoring of this criteria set may include sessions that:

- Contain threat feed information
- Connect to well-known bad sites
- Connect to high-risk domains/countries (for example, .cc domain)
- Use well-known protocols on non-standard ports
- Contain obfuscated JavaScript

Static Analysis

The second category analyzes each file in the session for signs of obfuscation in order to predict the likelihood of the file behaving maliciously if allowed to run. For example, software that links to networking libraries is more likely to perform suspicious network activity. Sample factors used in the scoring of this criteria set may include:

- Files found to be XOR encoded
- Files found embedded within non-EXE formats (for example, PE file found embedded in a GIF format)
- Files linking to higher risk import libraries
- Files highly deviating from the PE Format

Community

The third category scores the session and files based on the collective knowledge of the security community. For example, files whose fingerprint/hash is already known to be good or bad by respected anti-virus (AV) vendors is scored accordingly. Files are also scored based on knowledge that a file was delivered from a site known to be good or bad by the security community.

Community scoring also indicates whether the AV on your network flagged the files as malicious. It does not indicate that the resident AV product acted to protect your system.

Sandbox

The fourth category examines the behavior of the software by actually running it in a sandbox environment. By running the software to watch its behavior, a score can be calculated by identifying well-known malicious activity. For example, software that configures itself to autostart on each reboot and make IRC connections would score higher than a file with no known bad behavior.

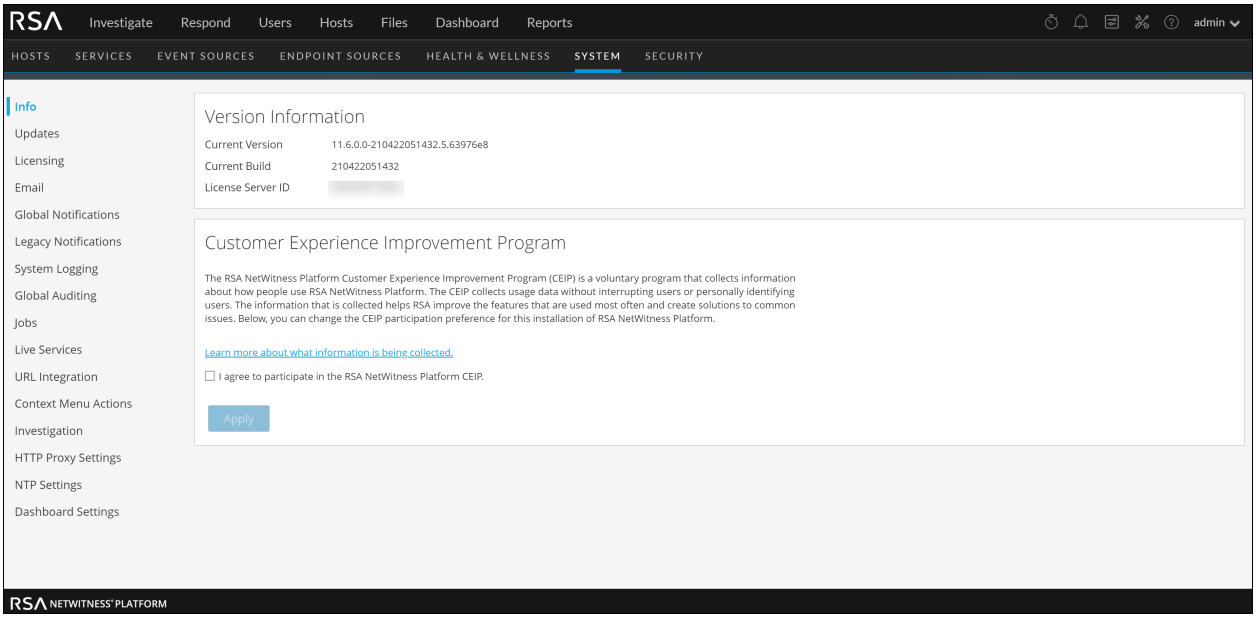
Roles and Permissions for Analysts

This topic identifies the user roles and permissions required for a user to conduct malware analysis in NetWitness. If you cannot perform an analysis task or see a view, the administrator may need to adjust the roles and permissions configured for you.

Required Roles and Permissions

RSA NetWitness manages security by providing access to views and functions using both system permissions and permissions on individual services.

On the system level, the user needs to be assigned a system role, in the (Admin) > System view, that provides access to specific views and functions.



The default `Malware_Analysts` role in NetWitness11.7 is assigned all of the permissions listed below. If necessary, an Administrator can create a custom role with some combination of the following permissions:

- Access Investigation Module (required)
- Investigation - Navigate Events
- Investigation - Navigate Values
- Access Incident Module
- View and Manage Incidents
- View Malware Events (to view events)
- File Download (to download files from the Malware Analysis service)
- Initiate Malware Scan (to initiate a one-time service scan or one-time file upload)

- Dashlet permissions for convenience: Dashlet - Investigate Top Values Dashlet, Dashlet - Investigate Service List Dashlet, Dashlet - Investigate Jobs Dashlet, Dashlet - Investage Shortcuts Dashlet.

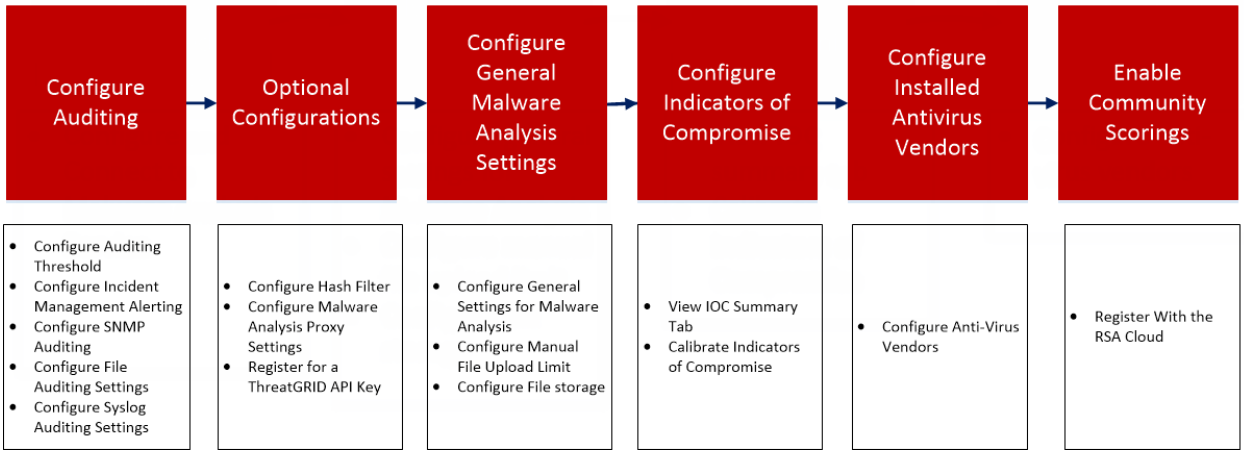
A use case for creating a custom role would be a Junior Malware Analyst role, with limited permissions that do not include the File Download permission.

On specific services, a malware analyst needs to be a member of the **Analysts** group, or to a group that has the two default permissions assigned to the Analyst group: **sdk.meta** and **sdk.content**. Users who have these permissions can use specific applications, run queries, and view content for purpose of analysis on the service.

Basic Setup

Malware Analysis can operate as a service on a Decoder or as a service on a dedicated appliance. This guide includes instructions for setting up the operating environment and then configuring the Malware Analysis service. After this configuration is complete, analysts can conduct malware analysis.

These are the configuration steps for Malware Analysis, and also for editing the configuration. Perform the steps in the section in the sequence they are given.



Basic Configuration Checklist

The following checklist provides the sequence for tasks that are required to configure Malware Analysis that has been added to NetWitness in accordance with the *Hosts and Services Guide*.

Step	High-Level Task
Step 1 - (Optional) Configure Dedicated Appliance	(Optional) Configure Dedicated Appliance This topic describes the procedures for configuring the environment to connect to the Malware Analysis service.
Step 2 - Configure General Malware Analysis Settings	Configure General Malware Analysis Settings • Enable continuous polling. • Configure manual file upload limit. • Configure the file storage repository and database. • Calibrate the Static, Network, Community, and Sandbox scoring modules.

Step	High-Level Task
Step 3 - Configure Indicators of Compromise	Configure Indicators of Compromise Calibrate Indicators of Compromise that are applied for each scoring module (Static, Network, Community, Sandbox) and for YARA-based IOCs.
Step 4 - Configure Installed Antivirus Vendors	Configure Installed Antivirus Vendors
Step 5 - Enable Community Scoring	Enable Community Analysis Register with the RSA cloud and test connections to enable Community scoring.
Step 6 - Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host Configure auditing thresholds and enable Syslog, SNMP, and file auditing.
Step 7 - Configure Hash Filter	(Optional) Configure Hash Filter Configure hash filtering to fine tune Malware Analysis event analysis based on known good or bad file hashes.
Step 8 - Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings (Optional) Configure Malware Analysis to communicate with the RSA Cloud through a web proxy instead of directly.
Step 9 - Register for a ThreatGRID API key	(Optional) Register for a ThreatGRID API Key

(Optional) Configure Dedicated Appliance

You can configure the NetWitness operating environment to connect to a NetWitness Malware Analysis service.

Malware Analysis operates as a service on a dedicated Malware Analysis appliance. If your site is using a dedicated appliance, do one of the following:

- If your site is adding a new dedicated NetWitness Malware Analysis appliance, install the physical appliance in your network and configure the operating environment.
- If your site is upgrading a dedicated Spectrum appliance to a dedicated NetWitness Malware Analysis appliance, re-image the Spectrum appliance as a Malware Analysis appliance.

Malware Analysis is dependent on the Core infrastructure to operate. The following steps are necessary before Malware Analysis can successfully analyze data.

1. Configure the onboard Broker on the Malware Analysis appliance to connect another Broker or Concentrator in the existing Core infrastructure.

   Note: If no Core infrastructure exists, only manually uploaded files can be analyzed.

2. Use NetWitness Live to find all Live resources with the `malware analysis` tag and deploy these resources to each Decoder service that will be capturing traffic for Malware Analysis to analyze. NetWitness uses this proprietary set of parsers and feeds to find events that are likely to be malware.
3. Configure communications ports. Malware Analysis requires a number of different communications ports to be open, including TCP/443 for HTTPS. These are described below in Network Connections.
4. Configure the NextGen source to which Malware Analysis will connect. This is the Broker or the Concentrator.
   Malware Analysis is now ready to begin analyzing network traffic.

Network Connections

The inbound and outbound network connections must be configured for the Malware Analysis appliance to properly communicate with services, RSA sources for software updates, and other critical information.

Your network firewall must be configured to allow the Malware Analysis access to the internet. Proxy servers may be used to facilitate these connections, if necessary.

Inbound Connections

TCP/22 - Secure Shell access to the Malware Analysis server to review log files and troubleshoot. Access can be limited to IP addresses that will be managing Malware Analysis.

- TCP/443 - HTTPS web-based connection to access the Malware Analysis user interface.
- TCP/50008 - JMX port for performance troubleshooting, using an application such as JVisualVM. This is optional and access can be limited to IP addresses that will be managing Malware Analysis.

Outbound Connections

- TCP/443 - HTTPS connections to SSL-based web servers. Some features include Malware Analysis sending files or documents to servers for analysis, which require a secure connection. Use of a web proxy server is supported.
- (TCP/443 - SSL connection from Malware Analysis to the RSA Cloud. Use of a SOCKS proxy server is supported. Customer infrastructure changes may be required to ensure that 443 is open to cloud.netwitness.com.)
- TCP/50103 - REST API port used to communicate with a Broker. (NetWitness 10.3.x and earlier)
- TCP/50105 - REST API port used to communicate with a Concentrator. (NetWitness 10.3.x and earlier)
- TCP/50003 TCP/56003 - Ports used to communicate with a Broker. (NetWitness 10.4 and later)
- TCP/50005 TCP/56005 - Ports used to communicate with a Concentrator. (NetWitness 10.4 and later)

- ICMP - JMS connection from NetWitness to the Malware Analysis service to verify if the hostname and ip address entered is valid for a successful test connection.

Configure General Malware Analysis Settings

You can configure several basic settings required to enable and calibrate the consumption of sessions, manual file upload, and the different scoring modules that Malware Analysis uses to analyze data.

You can also set up file sharing with the data repository. Malware Analysis has three modes of consuming sessions and files. Any combination of the three choices may be used to initiate analysis in Malware Analysis. The choices are:

- **Continuous Polling of the Core service:** You can enable and configure continuous polling of the Core service. When enabled and configured, Malware Analysis continuously polls the Core service for sessions tagged for analysis. By default, continuous polling is disabled. You can enable Denial of Service (DOS) attack prevention for use during continuous polling. You can test the connection to the Malware Analysis service that is being continuously polled using an option in the Integration tab.

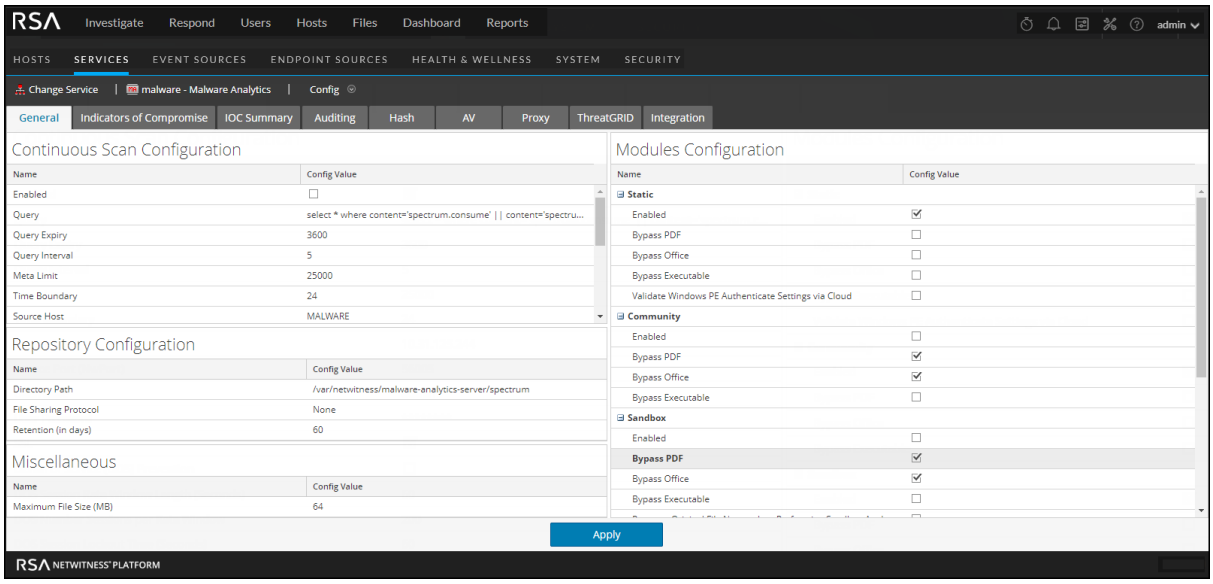
  Note: When adding a Core service as a service for continuous polling on 10.3.5 and earlier Malware Analysis, use the REST port; for example, add a Concentrator to 10.3.5 Malware Analysis with REST port (50105) instead of the native NexGen port (50005).

- **On-Demand Analysis of the Core service:** You can analyze sessions based on Investigations initiated directly in NetWitness. This method allows manually controlled consumption of Core sessions and allows tighter control over how files in those sessions are processed (for example, send to sandbox for processing). Document types can bypass the default restrictions and be sent to community or sandbox processing regardless of the configured setting.
- **Manual File Upload:** You can manually upload one or more files for analysis by navigating to a visible folder on your computer and selecting files to be uploaded. The maximum size for the uploaded files is configurable.

View the Basic Settings

To view the basic settings:

1. Go to  **(Admin) > Services**.
2. In the **Services** grid, select a Malware Analysis service and click  **> View > Config**.
   The Service Config for the service is displayed with the **General** tab open.



Configure Continuous Polling

Malware Analysis is rate limited so that 1,000 files per day may be submitted to ThreatGRID's Cloud for sandbox processing. To optimize your use of the sandbox, Malware Analysis configuration allows you to choose which of several methods of consumption Malware Analysis uses; you can enable or disable continuous polling.

An important consideration when configuring continuous polling is the Denial of Service (DOS) Prevention parameters. By default this feature is disabled because you need to carefully consider the settings for your environment before enabling the feature.

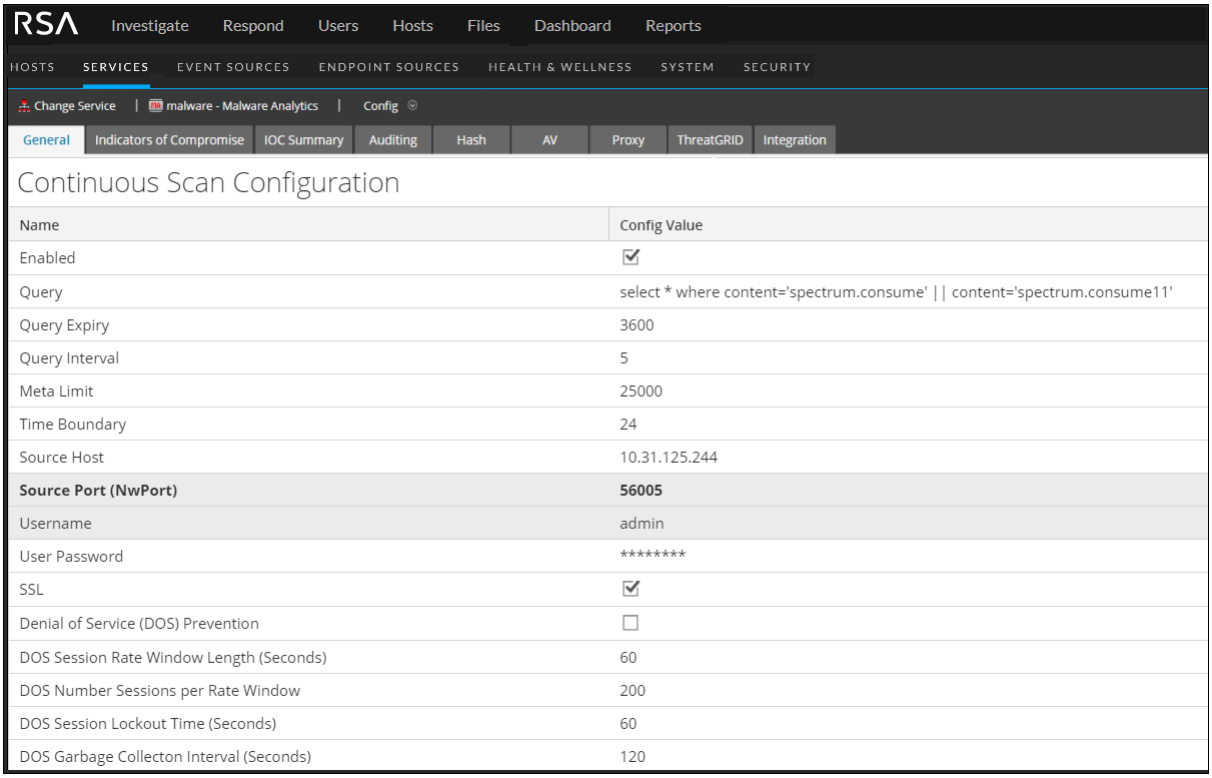
When DOS Prevention is disabled, Malware Analysis analyzes the queued sessions in first-in first-out order. A DOS attack may rapidly fill the queue so that Malware Analysis is busy handling those sessions, while a malware attack is occurring in a later session. The later session with the actual attack may not reach the beginning of the queue and undergo analysis until after the attack has begun.

When DOS Prevention is enabled, Malware Analysis treats too many sessions from a single IP address as a DOS attack. If an IP address exceeds the Number of Sessions per Rate Window, Malware Analysis begins to disregard sessions from that address until the Session Lockout time is reached. Then Malware Analysis resumes analysis of the sessions from that IP address. The disregarded sessions from the IP address are not analyzed at all, so a malware attack may slip through during the Session Lockout period.

Using the DOS Garbage Collection Interval setting, Malware Analysis clears in-memory storage of an IP source after a specified number of seconds. IP addresses with little activity during this interval are cleared from memory. If an IP address is active at intervals that exceed the DOS Garbage Collection Interval, Malware Analysis may not identify it as a DOS attack.

To configure Malware Analysis for continuous polling, in the Continuous Scan Configuration section:

1. In the **General** tab, under **Continuous Scan Configuration** you can configure continuous polling.



2. To enable continuous polling, click **Enabled**.
3. (Optional) If you want to change the default values for querying, enter new values for the **Query Expiry**, **Query Interval**, **Meta Limit**, and **Time Boundary**.
4. To configure the Malware Analysis appliance that Malware Analysis queries to retrieve data for analysis, specify the **Source Host** and **Source Port (NwPort)**.
5. (Optional) If you want to change the default logon credentials for the Malware Analysis appliance, specify the **Username** and **User Password**.
6. If you want to use SSL for communication between the Malware Analysis appliance and the Core service, enable **SSL**.
7. (Optional) If you want to configure Denial of Service (DOS) prevention:
   a. Enable the **Denial of Service (DOS) Prevention** parameter.
   b. Set up the DOS prevention session limitations:
      - Specify the number of seconds of the time window during which Malware Analysis counts sessions for a single IP address (**DOS Session Rate Window Length**). The window is called a Rate Window and a counter is set when the first session is received from that IP source. The default value is 60 seconds.
      - Specify the number of sessions allowed per Rate Window in the **DOS Number Session per Rate Window**. The default value is 200 sessions. When the number of sessions is reached within the Rate Window; Malware Analysis begins disregarding sessions from the IP address

and the disregarded sessions from that IP are not analyzed at all. Malware Analysis continues to disregard sessions until the lockout time is reached.

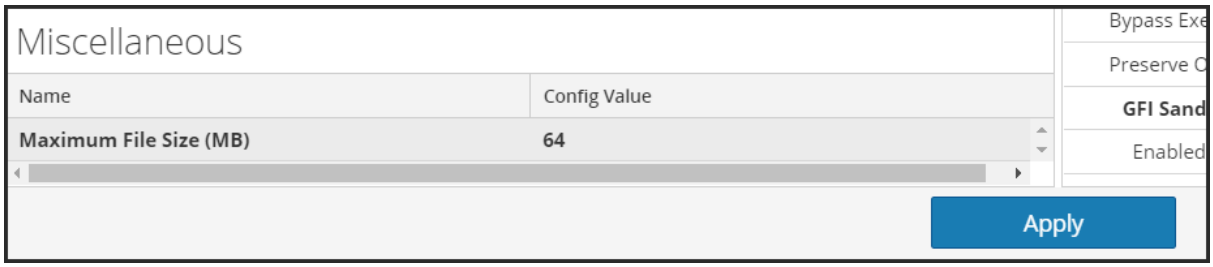
- Specify the length of lockout time (during which sessions from the IP address are disregarded and not analyzed) in the **DOS Session Lockout Time (Seconds)**. The default value is 60 seconds. When the lockout duration has elapsed, Malware Analysis resumes analysis of sessions from that IP address.
- Specify the interval of inactivity for an IP address before NetWitness removes the in-memory object for the IP source in **DOS Garbage Collection Interval (Seconds)**. The default value is 120 seconds.

8. Click **Apply** to apply the changes.
   The applied changes become immediately effective as Malware Analysis receives new packets.
9. Test the connection of the Malware Analysis service to the Core service selected in the **Integration** tab by clicking the **Test Connection** button in the **Continuous Scan Connection Test** section.

Configure Manual File Upload Settings

To configure the maximum file size for manual file upload:

1. In the Miscellaneous section, type the maximum file size in Megabytes allowed for files uploaded manually for Malware Analysis scanning.



2. Click **Apply**.
   The changes become immediately effective.

Configure the Data Repository

Malware Analysis can store a finite number of files on the appliance. The data repository configuration has a file system retention period of 60 days. This setting determines how long files are retained in the Malware Analysis appliance. When old files are deleted, they cannot be recovered. Every day, Malware Analysis deletes files that exceed the file system retention period to ensure that there is no wasted disk space.

The File System Retention Period is the only setting that governs when files are deleted. Files are not deleted based on the amount of disk space being used. If the setting needs to be changed, the administrator must configure the retention period based on the anticipated space usage during the number of retention days specified.

The visible data repository parameters in the NetWitness user interface are:

- The location of the repository is **/var/lib/netwitness/malware-analytics-server/spectrum**. Do not edit this value.
- The file sharing protocol, which allows access through one of the File Sharing Protocols to copy files from the Malware Analysis service.
- The file retention period in number of days.

To configure file sharing, in the Repository Configuration section:

1. Click on the File Sharing Protocol and select **FTP** or **SAMBA** or **None**.
2. Select the number of days that files are maintained in the repository before deletion.
3. Click **Apply.**

The changes become immediately effective.

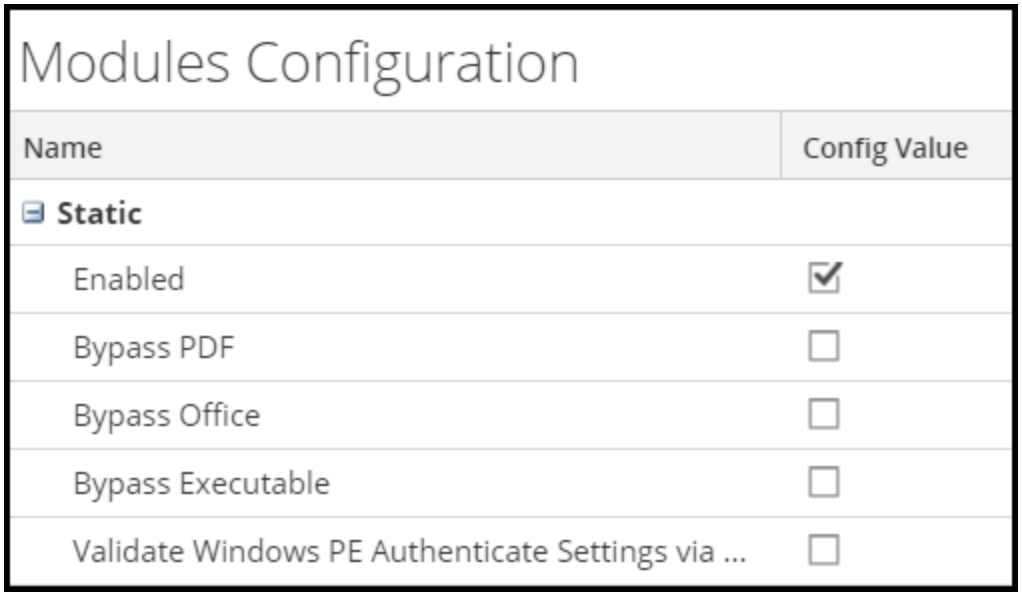
Calibrate Scoring Modules

The Modules Configuration section helps configure the following components of Malware Analysis to:

- Completely disable any or all of three scoring modules (Static, Community, and Sandbox). Before disabling or enabling any scoring module, ensure that you understand what each scoring module detects.
- Malware Analysis tags sessions containing Microsoft Office, Windows PE, and PDF files for consumption by the Malware Analysis service. You can configure Malware Analysis to ignore Windows PE, Microsoft Office, and PDF documents entirely. If this is the case, a better option is to adjust your Core settings to ignore these files so they are not tagged for Malware Analysis consumption.

A sample application for using scoring module calibration is this: when setting up rule groups or analyzing system performance, you can test various scenarios in which PDF documents are not analyzed, but Microsoft Office and Windows PE documents are. You can test the scenario in each of the three scoring modules. If you see a measurable improvement in system performance, you can apply this knowledge on a broader scale.

Configure Static Analysis Scoring



To configure Static analysis scoring, in the **Modules Configuration** section:

1. By default the Static module is enabled. To enable or disable Static analysis entirely, click the **Enabled** checkbox.
2. To configure handling of PDF, Microsoft Office, and Windows PE files in a session, select any of the checkboxes **Bypass PDF**, **Bypass Office**, and **Bypass Executable**.
3. To configure your preference for Authenticode validation of digitally signed Windows PE files, click the **Validate Windows PE Authenticate Settings via Cloud** checkbox. If you want to prevent Windows PE files that are digitally signed from being transmitted to the RSA Cloud for validation, remove the check.
   When disabled, ALL static analysis is performed locally (skipping Authenticode validation). Regardless of this setting, PDF and MS Office documents are not subject to Authenticode validation and are not transmitted over the network during static analysis.
4. Click **Apply.**The changes become immediately effective as Malware Analysis receives new packets.

Configure Community Analysis Scoring

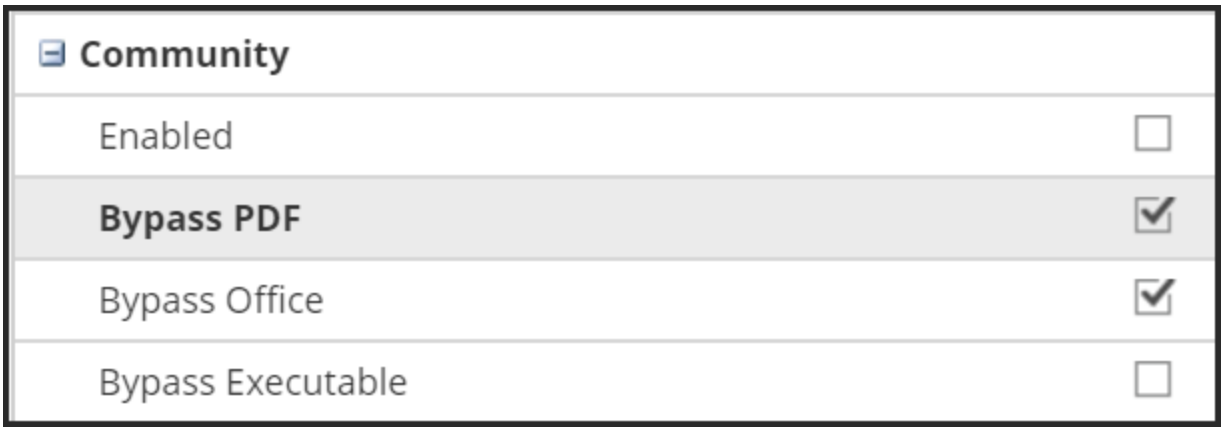
Once the Community module is enabled, the security community analyzes all documents not prevented from processing. This is achieved by sending network session and file attributes to the RSA Cloud for processing. The RSA Cloud then may make external connection to security community partners as needed to process the information.

The file content is never sent to the community for analysis. Instead, the MD5/SHA-1 hash of the file is sent for Anti-Virus detection and Blacklisting. Similarly, session Meta is harvested and analyzed as part of this process. Meta elements such as URL and Domain Name are examined and transmitted to the RSA Cloud to identify known bad URLs/Domains.

You can enable Community analysis and limit which document types are processed. There is no risk for the file content (except for a hash) being sent outside of your network.

Note: To gain access to the RSA Cloud where processing occurs, you must register your Malware Analysis service with RSA customer service. There are two methods: register the service using the options in the Integration tab or contact RSA Customer Care.

To configure Community analysis scoring, in the Modules Configuration section:



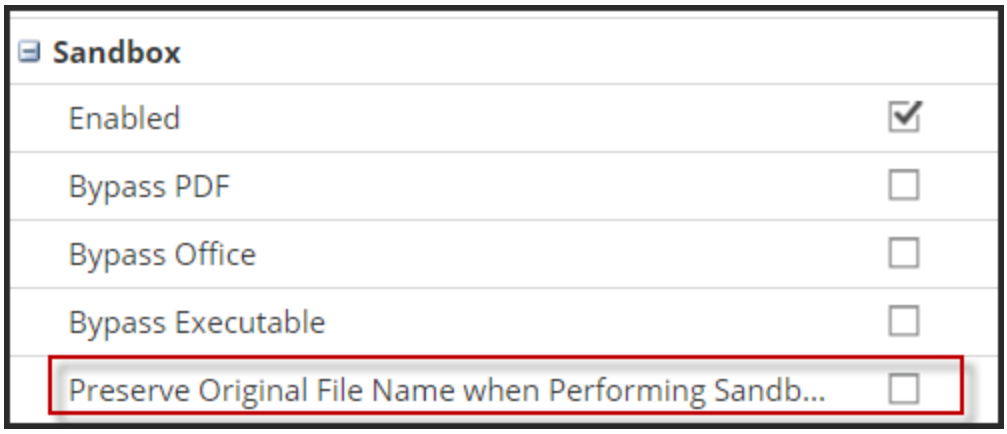
1. To enable or disable Community analysis entirely, click the **Enabled** checkbox. The default value is **Disabled**.
2. To configure handling of PDF, Microsoft Office, and Windows PE files in a session, select the specific checkboxes - **bypasspdf**, **bypass office, bypass executable.**
3. Click **Apply** to save the changes and put them into effect immediately as Malware Analysis receives new packets.

Configure Sandbox Analysis Scoring

By default, the sandbox module is disabled and MS Office and PDF files are prevented from being processed. The intent is to set to the most restrictive settings to force the user to specify whether or not potentially sensitive information is sent outside of the network for processing. If a document type is not prevented from being processed, the entire file (not just the hash) is sent to the destination sandbox server.

In addition, you can choose to preserve the original file name when performing sandbox analysis.

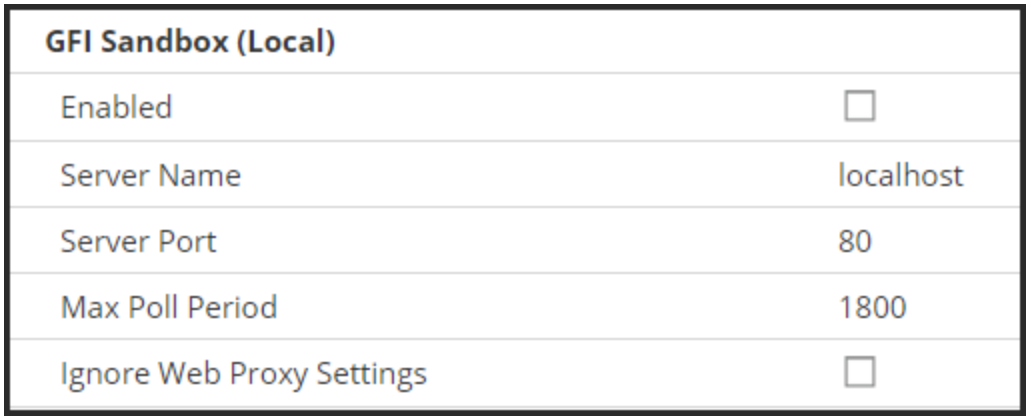
Note: If you do not specify the **Preserve Original File Name when Performing sandbox Analysis** parameter, NetWitness hashes the files.



When you enable the sandbox module, you must specify whether or not the sandbox processing is performed using a local GFI sandbox, a local ThreatGRID sandbox, or a cloud version of the ThreatGRID sandbox. The cloud version of the ThreatGRID sandbox is provided directly by ThreatGRID and requires an activation key to be obtained from ThreatGRID and configured in the ThreatGRID tab.

GFI Sandbox Settings

To use a locally installed GFI sandbox, you must enable GFI and supply the Server Name and Server Port of the GFI sandbox Server. The Max Poll Period and Polling Interval determine how long to wait for a submitted sample to finish processing and how often to check the status (in seconds). The Ignore Web Proxy Settings option allows you to indicate that you want Malware Analysis to bypass a web proxy when making this connection. If no Web Proxy has been configured in Malware Analysis, the setting is ignored.



ThreatGRID Sandbox Settings

Note: Before enabling ThreatGRID scoring, a ThreatGRID-supplied Service Key must be configured so that ThreatGRID can recognize that samples submitted from this site are legitimate. Use NetWitness to register for a ThreatGRID API key, then you can enable and configure a locally installed ThreatGRID sandbox or the ThreatGRID Cloud sandbox. Refer to the following detailed task: Register for a ThreatGRID API Key.

The Ignore Web Proxy Settings allows you to indicate that you want Malware Analysis to bypass a web proxy when making this connection. If no Web Proxy has been configured in Malware Analysis, the setting is ignored.

To configure sandbox scoring, in the Modules Configuration section:

1. To enable or disable sandbox analysis entirely, click the **Enabled** checkbox. The default value is **Disabled**.
2. To configure handling of PDF, Microsoft Office, and Windows PE files in a session, select any of the three checkboxes **Bypass PDF**, **Bypass Office, Bypass Executable.**
3. Configure the active sandbox vendor. You have three options:
   a. To use a locally installed instance of the GFI sandbox, provide the Server Name and Server Port of the GFI sandbox Server, the Max Poll Period and Polling Interval, and optionally, select the **Ignore Web Proxy** checkbox.
   b. To use a locally installed instance of ThreatGRID, enable ThreatGRID scoring, provide the ThreatGRID Service Key and optionally, select the **Ignore Web Proxy** checkbox.
   c. To use the ThreatGRID Cloud, you must first register for a ThreatGRID API key. Then enable ThreatGRID scoring, provide the ThreatGRID Service Key, enter the URL for the ThreatGRID server (https://panacea.threatgrid.com), and optionally, select the **Ignore Web Proxy** checkbox.
4. Click **Apply**.
   The changes become immediately effective.

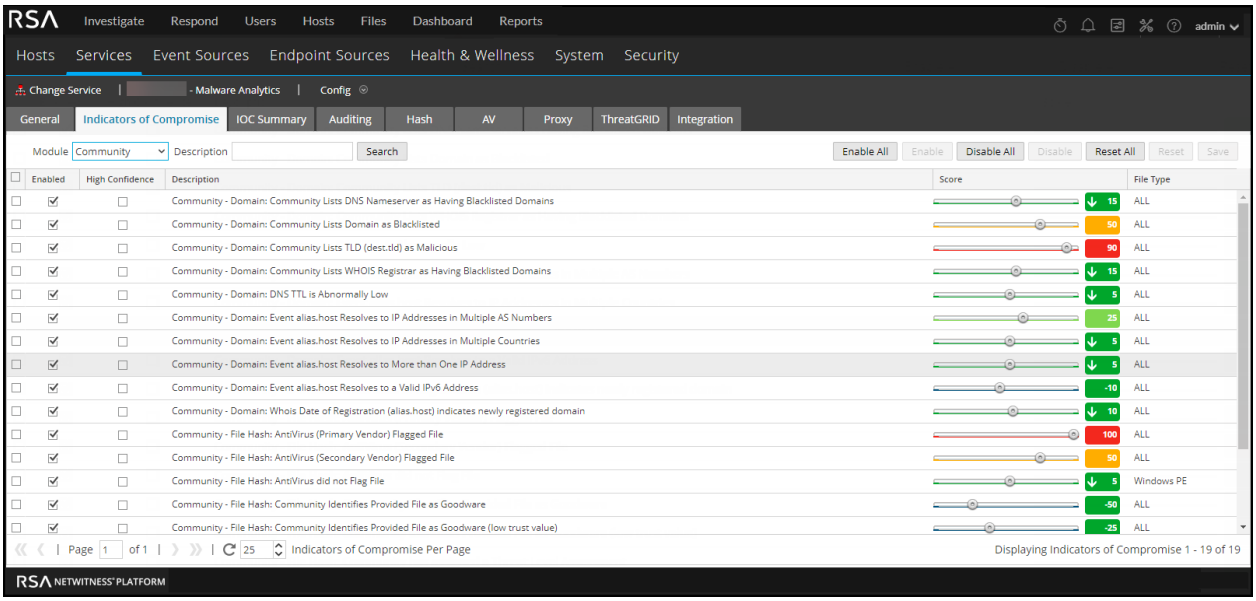
Configure Indicators of Compromise

The Indicators of Compromise (IOC) for the Malware Analysis scoring modules are configured since, each Malware Analysis scoring module -- Network, Static, Community, Sandbox, and YARA -- has a default set of Indicators of Compromise (IOCs) that it uses to evaluate the file and session data in order to assess the likelihood of malware being present.

Each IOC is assigned a numeric score weighting between -100 (good) and 100 (bad). When an IOC triggers, the numeric score weighting is factored into the total score for the session or file being analyzed. The individual score weightings for all matched IOCs are aggregated to produce the resulting score for each session or file. The aggregated score is adjusted to ensure that it does not exceed the valid score range (-100 through 100).

Note: The score weighting assigned to an IOC is not always the explicit score value that is aggregated (it is not a simple addition of score weights for each IOC that triggers). Instead, the IOC's score is a weighting or indicator of importance that is factored into calculating an overall score.

The Indicators of Compromise (IOC) configuration settings for Malware Analysis are in the Service Config view > Indicators of Compromise tab. Below is an example of the tab.



Using the **Community - File Hash: AntiVirus (Primary Vendor) Flagged File** IOC as an example, the IOC's score weighting could be set to 100. However, Malware Analysis dilutes this value based on the percentage of primary AV vendors that agree if the sample is malicious. The closer to 100% of the vendors who agree that the sample is malicious, the closer to the full 100 points are used in aggregating a score. As the percentage drops closer to 0%, the proportion of the full 100 points used in the aggregated score drops.

IOCs use logic implemented natively in Malware Analysis. You cannot adjust the logic. Instead, you can only adjust the IOC to increase or decrease its impact on scoring, to indicate a confidence setting, or to turn the IOC on or off. The typical scenario is to adjust a limited set of IOC score weighting values downward for IOCs that are inflating the final score and causing false positive analysis results. An extreme version of tuning would be to disable the IOCs entirely if they consistently contribute to false positive results. Additionally, the flexibility exists to allow you to disable all IOCs and to choose a select few to leave enabled. For example, all IOCs can be disabled with the exception of a select few IOCs that detect AntiVirus matches. Using Malware Analysis in this extremely limited configuration, you can reduce results in Malware Analysis such that only known A/V matches generate results.

You can configure this functionality in several ways:

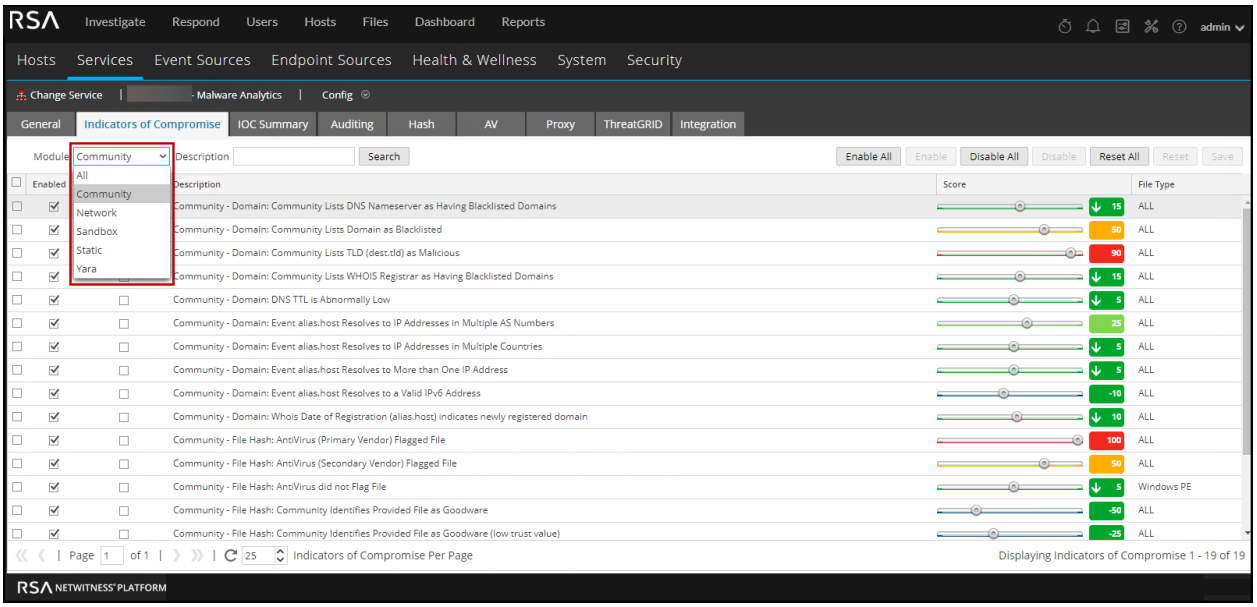
- Disable IOCs so that they are not evaluated as part of the scoring module to which they are assigned.
- Adjust the score weight for an IOC such that its impact on the aggregated score is increased or decreased.
- Mark IOCs that you expect to be strong indicators of malware and display a high-confidence (HC) flag on sessions that triggered these IOCs in the Malware Analysis results.
- Customize score and confidence settings uniquely to the file type being analyzed. Each IOC is pre-assigned a file type to which it is applied. Possible values are **ALL**, **PDF**, **MS Office**, and **Windows PE**. The IOC with the most applicable file type is used during file-based analysis. For example, if a PDF is analyzed, an IOC with a file type set to **PDF** will be chosen rather than the same IOC with a file type set to **ALL.** If no file-type specific match is found, the IOC with a file type set to **ALL** is selected.
- Search for rules to display in the grid based on a match to the rule description.

Filter Displayed IOCs by Module

You can filter the displayed IOCs by scoring module: one of the four built-in modules or YARA. YARA-based IOCs are interleaved with the native IOCs with each category. Although the YARA IOCs are not identified as such in the other views, you can select YARA from the Module selection list to see a list of YARA rules.

To view the IOCs for one or the four scoring modules or for YARA:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service.
3. In the row, select  **> View > Config**.
4. Click the **Indicators of Compromise** tab.
5. In the **Module** selection list, select **All**, **NextGen**, **Static**, **Community**, **Sandbox**, or **YARA**.
   The configured rules and settings for the module are displayed.



Filter Displayed Modules to Show Only Modified Modules

The **Indicators of Compromise** tab visually identifies IOCs that are locally modified. When an IOC has been modified, for example, the score weight has been changed, and the name is displayed in red and includes a modification indicator appended to the IOC name. The modification indicator is ++ and can be used as a filtering mechanism when searching for IOCs.
To limit the display to locally modified IOCs:

1. In the **Description** field, enter ++.
2. Click **Search**.
   The view is filtered to show only modified IOCs.

Enable and Disable IOCs for a Scoring Module

When an IOC is disabled, it no longer impacts the aggregate score for the scoring module to which it belongs. If the IOC has multiple instances (differentiated only by file type), disabling a more file-type specific IOC results in use of the more file-type agnostic version of the IOC in scoring.
For example, if the same IOC exists as file type **ALL** and file type **Windows PE**, disabling the **Windows PE** instance of the IOC causes the **ALL** version to be used in scoring. In order to disable the IOC entirely for **Windows PE**, while leaving the IOC enabled for other file types, set the score weighting of the **Windows PE** instance of the IOC to a value of zero as described below. This leaves the IOC enabled for Windows PE files (although it has a zero weighting and is suppressed from being displayed in analysis results), while not affecting the other file types. The remaining file types will continue to use the **ALL** instance of the IOC.

To enable or disable an IOC so that it no longer factors into a scoring module:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service, and in the row select  > **View > Config**.
3. Click the **Indicators of Compromise** tab.
4. In the **Module** selection list, select a scoring module: **All**, **Community**, **Network**, **Sandbox**, **Static**, or **YARA**.
   The configured rules and settings for the module are displayed.
5. Do one of the following:
   a. Click the **Enabled** checkbox in the column next to a rule that you want to enable.
   b. Select one or more rules, and click **Enable** or **Disable** in the toolbar.
   c. To toggle between Enabled and Disabled for all rules displayed on the page, click the **Enabled** checkbox in the column title.
   d. To enable or disable all rules for the scoring module, click **Enable All** or **Disable All** in the toolbar.
6. To save the changes to the page, click **Save** in the toolbar.

> **Note:** Rules that have changed settings are displayed with a red corner. If you navigate to another page of rules before saving, all changes to this page are lost.

Adjust the Score Weight for an IOC

Adjusting the score weight for an IOC increases or decreases the IOC's overall impact on the aggregate score for the module in which it is configured. To raise or lower the overall impact of the IOC, reduce the current value to a new setting.

- Values ranging from -100 to -1 indicate that the session or file being analyzed is not likely to be malware (-100 being the least likelihood).
- Values ranging from 1 to 100 indicate a likelihood that the file or session being analyzed is malware (100 being the highest likelihood).
- Setting the value to zero leaves the IOC enabled, but causes the IOC to no longer impact the aggregate score and suppresses the IOC from being displayed in analysis results. Setting the value to zero is a method of disabling a file-type specific instance of an IOC while leaving the original file-type agnostic instance of the rule intact for scoring of the remaining file types.

To adjust the score weight:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service.
3. In the row, select  **> View > Config**.
4. Click the **Indicators of Compromise** tab.
5. In the **Module** selection list, select a scoring module: **All**, **Network**, **Static**, **Community**, **Sandbox** or **YARA**.
   The configured rules and settings for the module are displayed.
6. Do one of the following:
   a. Drag the score slider left or right to decrease or increase the score weight.
   b. Click directly on the displayed score weight and enter a new score weight.
7. To save the changes to the page, click **Save** in the toolbar.

Note: Rules that have changed settings are displayed with a red corner. If you navigate to another page of rules before saving, all changes to this page are lost.

Set the High Confidence Flag for an IOC

The High Confidence setting is used as a method of flagging specific IOCs as high confidence indicators that malware is present. As an example, the **Community - File Hash: AntiVirus (Primary Vendor) Flagged File** IOC has a low probability of being a false positive, combined with a high probability of being an accurate measurement of malware being present. By flagging this IOC (and others) as High Confidence, you can use a filter in the Malware Analysis results to limit display to only those sessions that include one or more high confidence rules. By doing so, the display is limited to a smaller subset of results whose accuracy is accorded a higher degree of confidence. Displaying results not limited to high confidence IOCs still allows you to review results that are more grey in nature. This provides for results that are less prone to false negative results. Choosing to filter or to not filter results based on confidence level has a valid use case in the NetWitness workflow.
To set the High Confidence flag:

1. In the **Indicators of Compromise** tab, select a scoring module from the **Module** selection list: **All**, **Network**, **Static**, **Community**, **Sandbox**, or **YARA**.
   The configured rules and settings for the module are displayed.
2. Click the **High Confidence** checkbox in the column next to a rule that you want to flag or unflag as highly likely to indicate the presence of malware in a session when matched.
3. To save the changes to the page, click **Save** in the toolbar.

Note: Rules that have changed settings are displayed with a red corner. If you navigate to another page of rules before saving, all changes to this page are lost.

Reset IOCs to Default Settings

1. In the **Indicators of Compromise** tab, select a scoring module from the Module selection list: **All**, **Network**, **Static**, **Community**, **Sandbox**, or **YARA**.
   The configured rules and settings for the module are displayed.
2. If you want to reset all rules on the current page to their default settings, click **Reset** in the toolbar.
3. If you want to reset all rules for the selected scoring module to default settings, click **Reset All** in the

toolbar.

4. To save changes to the page, click **Save** in the toolbar.

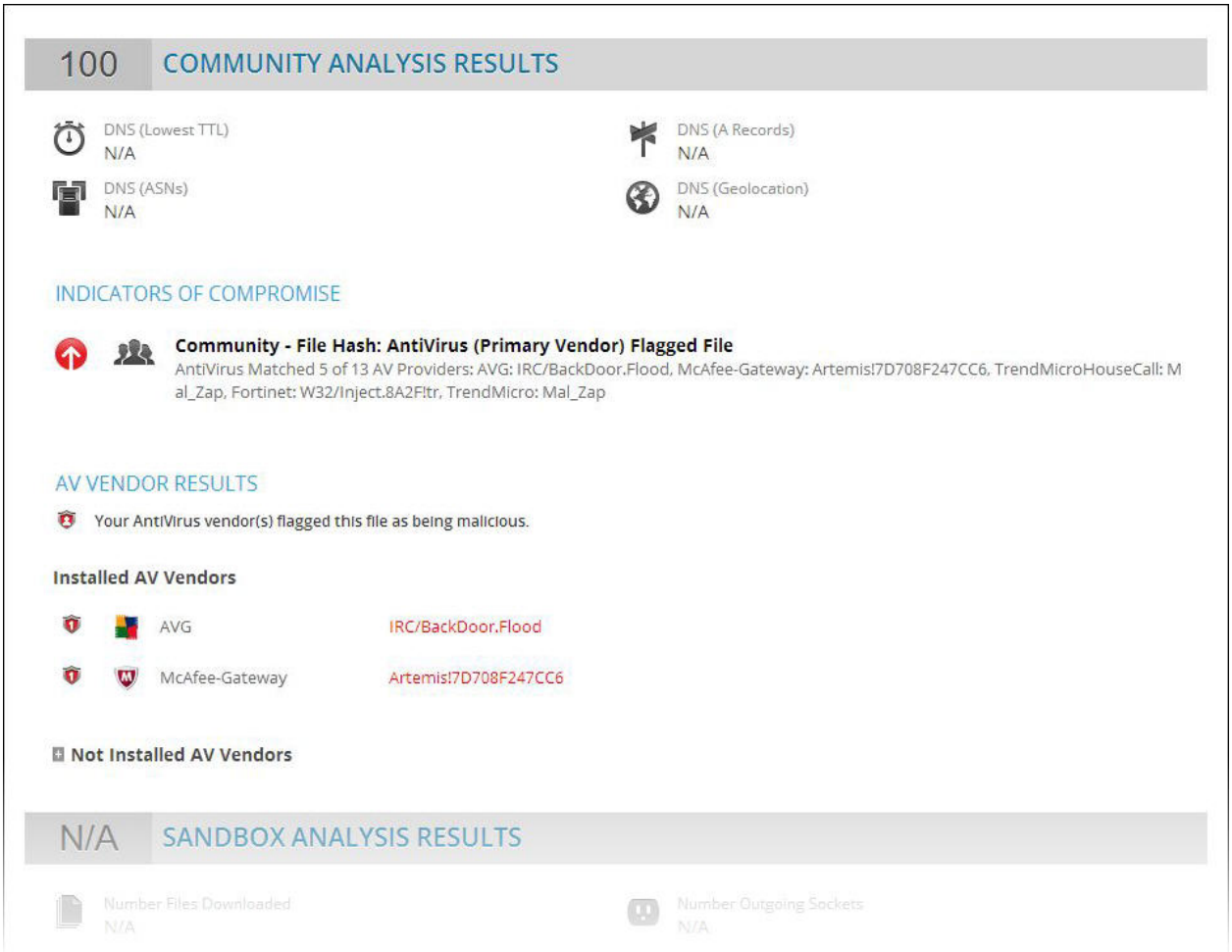
Configure Installed Antivirus Vendors

You can compare file analysis results from your installed antivirus (AV) vendors versus community results from the Malware Analysis knowledge base. While a file is being analyzed by community analysis, Malware Analysis checks an antivirus knowledge base to determine if the sample is already known to be malicious. If the file is known to be malicious, NetWitness flags the file to indicate whether a primary antivirus vendor or a secondary antivirus vendor identified the sample. NetWitness classifies vendors as primary and secondary to indicate the level of reputation the vendors have in the industry, and Indicators of Compromise factor the reputation into scoring. For example, detection made solely by secondary antivirus vendors may score less than detection by primary vendors.

Note: When choosing AV vendor software to install on your network, it is highly recommended that you include at least one from NetWitness Primary Vendors list. For more information, please see the Supported Antivirus Vendors.

You can identify the antivirus vendors installed on your network to NetWitness. NetWitness compares the antivirus results during community analysis against the results from the installed vendors selected in the AV tab. If a match is detected, the file being analyzed is flagged to indicate that your locally installed primary or secondary antivirus software detected the sample.

The example below shows the community analysis results for a file that had a score of 100. Under **Indicators of Compromise**, you can see that the file was flagged by the listed AV vendors in the Community. Under **AV Vendor Results**, NetWitness indicates whether the AV vendors installed in your environment flagged the file as malicious. If your installed AV vendors detected the virus, the name of the malware is displayed. If your installed AV vendors did not detected the virus, **--Not detected--** is displayed next the AV vendor name. Under **Not Installed Vendors**, you can click + to expand the section and see if other vendors not installed on your system detected the virus.



Identify Installed AV Software

To identify Antivirus software installed on your network:

1. Go to **(Admin) > Services.**
2. Select a Malware Analysis service, and in the row select **> View > Config**.
3. In the **Service Config View**, select the **AV** tab.
4. Select the checkbox next to each antivirus vendor (primary and other) whose software is installed on your network.
5. To save the changes, click **Apply**.
   The Community Analysis results will indicate whether your software flagged an event.
6. (Optional) If you want to reset the list of installed AV software to the default value (none), click **Reset**.
   All selections are removed.
7. To save changes, click **Apply**.

Enable Community Analysis

An Administrator can enable community analysis. For Community analysis, new malware detected on the network is pushed to the RSA Cloud for checking against RSA's own malware analysis data and feeds from the SANS Internet Storm Center, SRI International, the Department of the Treasury and VeriSign. To enable Community analysis, you must register with the RSA cloud and test connection to the cloud, then to test the connection between the RSA cloud and the service you have configured for continuous scanning.

A complete description of analysis methods is provided in How Malware Analysis Works.

1. Go to  **(Admin) > Services.**
2. Select a Malware Analysis service, and in the row select  **> View > Config**.
3. In the **Service Config View**, select the **Integration** tab.
4. Scroll down to **RSA Cloud Connection Test and Registration**.

   NetWitness tests communications with the site at `https://cloud.netwitness.com`. If your company uses a proxy for outbound traffic, please check your Proxy settings. A valid connection is required in order to register with the RSA Community Service.
5. Enter your company name and contact email. Click **Register**.

   If all required fields are complete, your registration is completed. The label on the button used to register changes to Update.
6. To verify that the Malware Analysis Service can connect to the Core service selected for continuous scanning, click **Test Connection**.

   NetWitness initiates a check based on the Source Host, Source Port, Username, and User Password specified in the General tab. When the test executes successfully, analysts are able to see Community Scoring in Malware Analysis.

(Optional) Configure Auditing on Malware Analysis Host

This topic introduces the configurable features of the Malware Analysis auditing log and the procedures for configuring the features. Malware Analysis is capable of generating auditing alerts based on configured score module thresholds. Once the analysis score for a file in an analysis session meets or exceeds the configured threshold(s), an auditing alert is generated. Thresholding allows sessions and files that score high enough to be likely malware candidates to automatically generate an alert.

Alerts can be configured to be formatted as SNMP, Syslog or File entries. Supporting various audit formats provides a method for external systems to ingest auditing events based on their capability of parsing the supported formats.

In addition to auditing analysis sessions, the following events will trigger an audit alert:

- User login successes and failures
- Changes to system configuration settings

- Server restart
- Server version upgrade and install

The Auditing configuration settings for Malware Analysis are in the Service Config view > Auditing tab.

Configure the Auditing Threshold

The sole purpose of the thresholds is to specify the criteria that must be reached prior to an alert being generated for an analyzed session/file. If auditing is enabled, each scored file/session is examined to determine if the score in each score module meets or exceeds the configured auditing threshold. If so, an alert is generated using the configured audit alert format (e.g., SNMP, Syslog or File). For example, by configuring SNMP and setting the Community Threshold to 90, all sessions/files that score 90 or higher in the Community Score module generate an SNMP trap. If all of the thresholds are set to 90, then an alert is not generated unless a session or file scores 90 or higher in the Network, Static, Community and sandbox score modules.

To configure the auditing threshold:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service, and select  **> View > Config**.
3. In the **Services Config** view, click the **Auditing** tab.
4. In the **Auditing Thresholds** section:
   a. Set the threshold for the **Community**, **Static**, **Network**, and **Sandbox** by doing one of the following for each scoring module:
      - In the slider, click and drag the handle in either direction.
      - In the value field, type a number between 0 and 100, inclusive.
   b. (Optional for 10.3 SP2) Select one or more triggers to record a message and deliver it through all enabled auditing methods.
   c. Click **Apply**.
      - The threshold setting becomes effective immediately for all enabled auditing methods: SNMP, File, and Syslog.
      - The recorded messages are sent through all enabled auditing methods: SNMP, File, and Syslog.

Configure Incident Management Alerting

When enabled, Malware Analysis alerts feed into the NetWitness Respond workflow.

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service, and select select  **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.

4. In the **Respond Alerting** section, select the **Enabled** checkbox and click **Apply**.
   Alerting becomes effective immediately.

Configure SNMP Auditing

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing services on IP networks. When SNMP auditing is enabled, Malware Analysis can send an audit event as an SNMP trap to a configured SNMP trap host. In addition to the score and event ID, the alert includes all session meta as well as generated meta data. This is useful for users who want to feed event data to third-party systems.

To configure SNMP auditing:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service, and select  **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.
4. In the **SNMP Auditing** section, click the checkbox to enable SNMP auditing.
5. Configure the SNMP server name and port.
6. Configure the SNMP version and trap OID for sending traps.
7. Configure the Malware Analysis community, and retry and timeout parameters when sending traps.
8. Click **Apply**.
   The SNMP auditing settings become effective immediately.

Configure File Auditing Settings

When file auditing is enabled, the audit log file is kept in the Malware Analysis Home Directory. The default location for this log file is:

`/var/lib/netwitness/malware-analytics-server/spectrum/logs/audit/audit.log`.

As each log reaches the maximum file size, it is archived and a new log is created. The size of these audit logs and their number are both configurable.

Caution: Avoid setting the max file size and archive file count too high, because it may have an adverse effect on the available disk space on the Malware Analysis appliance.

To configure the file auditing settings:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service, and select  **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.
4. In the **File Auditing** section, click the checkbox to enable file auditing.
5. (Optional) Set the Archive File Count and Max File Size.
6. Click **Apply**.
   The file auditing settings become effective immediately.

Configure Syslog Auditing Settings

When enabled, Syslog provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

In addition to the score and event ID, the syslog includes all session meta as well as generated meta data. This is useful for users who want to feed event data to third-party systems.

To configure the syslog auditing settings:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service, and select  **> View > Config**.
3. In the **Services Config** view, select the **Auditing** tab.
4. In the **Syslog Auditing** section, click the checkbox to enable syslog auditing.
5. Configure the host where the target syslog process is running and the port on the host where the syslog process is listening.
6. Configure the facility, encoding, format, max length, and timestamp for outgoing syslog messages.

   Note: (Optional) Configure Identity String to prepend to syslog alerts.
   For CEF format, please refer to Create Custom Alert in CEF Format for additional considerations.

7. Click **Apply**.

   The syslog auditing settings become effective immediately.

(Optional) Configure Hash Filter

This topic introduces hash filters as a method of marking files in Malware Analysis that are known to be good or known to be bad. Hash filtering allows you to maintain a list of known good or known bad file hashes. In the Hash tab, you can fine tune Malware Analysis event analysis based on file hashes. When a file hash is marked as Good, Malware Analysis does not analyze the file the next time it is seen. When a file hash is marked as Bad, Malware Analysis automatically raises the file's community score by a large number of points. Malware Analysis still analyzes the file, just in case new information becomes available.

Note: If an event contains a single file and that file's hash is marked as Good, Malware Analysis filters the entire event and you do not see it in Malware Analysis results.

To add hash filters to the hash list, you can use either of these manual methods:

1. Context menu add in the Event Detail view: Right-click on a file, and a context menu allows marking of the hash for the selected file as Good (Normal) or Bad (Malicious).
2. Hash tab toolbar: Click **Add** in the Hash tab to add a file hash, file size, and optionally, mark the hash as trusted.

There is also an automated method to add hash filters to Malware Analysis by importing a hash list in bulk from the watched folder. Hashes imported through the watched folder do not appear in the hash list. With bulk importing and the watched directory (/var/netwitness/malware-analytics-server/spectrum/hashWatch) on the Malware Analysis server set up, copy a hash list into the watched folder to be automatically imported into the system. Hashes imported using the bulk import method overwrite hashes that were previously imported through the watched folder.

View the Hash List

To view the Hash List:

1. Go to  **(Admin) > Services**.
2. In the Services view, select a Malware Analysis service, and select  **> View > Config**.
3. Select the **Hash** tab.

   The hash list is displayed in the Hash tab. Only file hashes that have been added using one of the methods are displayed.

Add a File Hash to the Hash Filter

To add a file hash to the hash filter:

1. In the **Hash** tab, in the toolbar, click **Add**.

   The Add Hash dialog is displayed.
2. If the hash is trusted, select **Trusted**.
3. Enter the MD5 hash and the file size in bytes.
4. Click **Save**.

   The file hash is added to the hashes and used to perform hash filtering in Malware Analysis.

Mark a Hash as Trusted or Untrusted

To mark a file hash as trusted or untrusted:

1. In the **Hash** tab, to toggle between trusted and untrusted, click in the **Trusted** column for the hash.
2. In the toolbar, click **Save Edit**.

Delete a Hash from the Hash Filter

To delete a hash from the hash filter:

1. In the **Hash** tab, select one or more hashes that you want to remove from the hash filter.
2. In the toolbar, click **Delete**.

   A dialog requests confirmation and offers an opportunity to cancel.
3. To confirm the deletion, click **Yes**.

The file hash is deleted from the grid and no longer used to perform hash filtering in Malware Analysis.

Search for a File Hash

In the Hash tab, you can search for a file hash that is displayed in the grid. In the MD5 field, type the file hash for which you are searching, and click **Search**. The list of files that contain the hash is displayed in the grid.

Import a Hash List Using the Watched Folder

To import a hash list from the watched directory, the hash list must be in the specified format and must be sorted on md5. You can drop a file formatted as described below into a folder (/var/netwitness/malware-analytics-server/spectrum/hashWatch) on the Malware Analysis appliance, and it is automatically imported into the local hash database. This is the only way to import file hashes into. An additional use case is to allow a system administrator to expose the watched directory to some process that would push a file to this directory. This is a bulk import method designed to handle a high volume of hash imports.

This is a csv-formatted file with no spaces between the data in each row. The assumption with the data in the hash list is that there are no duplicates. Duplicates are ignored during processing. If duplicate hashes are encountered, the log file will display the following message to indicate the number of duplicate hashes contained in the file:

2013-08-09 09:46:00,674 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processing - /var/lib/rsa>malware/hashWatch/test.csv
2013-08-09 09:47:56,619 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.services.file.hash.HashServiceImpl - Skipped 21 Duplicate Hashes Already on File
2013-08-09 09:48:06,638 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processed - /var/lib/rsa>malware/hashWatch/test.csv

Below is an example of a hash list in the default file format.

```
[BeginFileExample]
392126E756571EBF112CB1C1cdEDF926,98865,True
0E53C14A3E48D94FF596A2824307B492,2226,True
176308F27DD52890F013A3FD80F92E51,42748,False
9B3702B0E788C6D62996392FE3C9786A,32768,False
937ADE76A75712B7FF339403B4FCB5A6,4821,False
B47139415F735A98069ACE824A114399,1723,False
E6CAF205E602CFA9A65663DB1A087874,704,False
680CA0BCE1FC7BC4136ADF4E210869C5,2075,False
[EndFileExample]
```

A NetWitness configuration file (**/var/netwitness/malware-analytics-server/spectrum/conf/hashFileWatchConfig.xml**) specifies the format and options in the hash list import process. Below is a listing of the configuration file.

```
<config>
 <enabled>true</enabled>
 <distributedCacheEnabled>true</distributedCacheEnabled>
 <watchDirectory>//var/lib/rsamalware/hashWatch</watchDirectory>

<processedDirectory>/
var/lib/rsamalware/hashWatch/processed</processedDirectory>

<erroredDirectory>/
var/lib/rsamalware/hashWatch/error</erroredDirectory>
 <md5Col>0</md5Col>
 <fileSizeCol>-1</fileSizeCol>
 <isTrustedCol>1</isTrustedCol>
 <isTrust>false</isTrust>
 <ignoreFirstLine>false</ignoreFirstLine>
 <frequencyInMinutes>1</frequencyInMinutes>
 <isGzipCompressed>false</isGzipCompressed>
 </config>
```

Line	Description
<md5Col>0</md5Col>	The location of the md5 hash in each entry. The default value is position **0**, or the first position.
<fileSizeCol>1</fileSizeCol>	The location of the hash size in each entry. The default value is position **1**, or the second position. If the hash size is not included in the csv file, the value must be **-1**.
<isTrustedCol>2</isTrustedCol>	The location of the Trusted Column in each entry. The default value is position **2**. If the Trusted parameter is not included in the csv file, the value must be **-1**.
<isTrust>false</isTrust>	The default assumption for **Trusted** in each entry is **false**.
<ignoreFirstLine>false</ignoreFirstLine>	The presence or absence of a header in the hash. The default value is **false**. If the hash has a header, the value must be set to **true**.
<frequencyInMinutes>1</frequencyInMinutes>	The interval between checks by NetWitness in the watched directory. The default value is **1** minute.
<isGzipCompressed>false</isGzipCompressed>	The hash is compressed using Gzip. The default value is **false**. If the hash is Gzip compressed, the value must be set to **true** here.

When the hash list has been imported, the system log has entries similar to this:

```
2013-04-11 03:22:00,597 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing - /var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 2013-04-11 03:22:00,600 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processed
- /var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

If there is a problem loading the file, the system log has entries similar to this:

```
2013-04-11 03:17:00,597 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing - /var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 ... Verbose log
 2013-04-11 03:17:00,632 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Error
Processing - /var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

To import a hash list using the watched folder method:

1. Copy the hash lists that you want to import into the **/var/netwitness/malware-analytics-sever/spectrum/hashWatch** directory.
   Malware Analysis automatically watches this folder and processes files placed there.
   Malware Analysis adds every hash found in the hash lists to the hash filter.
   If there are processing errors, they are logged in **/var/netwitness/malware-analytics-sever/spectrum/hashWatch/error**
   Processed files are cataloged in **/var/netwitness/malware-analytics-sever/spectrum/hashWatch/processed**
   Processed files are not removed from the hashWatch directory.
2. After importing hashes in bulk, the System Administrator can use a cronjob to clean up old processed files.

(Optional) Configure Malware Analysis Proxy Settings

This topic describes the configuration of a web proxy for communicating with the RSA Cloud service and local ThreatGRID or GFI service. The settings in the Service Configuration view > Proxy tab set up communication by web proxy, which Malware Analysis can use to communicate with RSA Cloud for community analysis and sandbox analysis. Once the proxy is configured:

- Malware Analysis communicates via web proxy with the RSA Cloud for community analysis.
- Malware Analysis communicates via web proxy with the configured ThreatGRID or GFI sandbox service. Using a web proxy may negatively affect performance. ThreatGRID and GFI configuration sections in the General tab have an option to ignore the web proxy and communicate directly with the sandbox to improve performance.

Configure the Web Proxy

To configure the web proxy for Malware Analysis:

1. Go to  **(Admin) > Services** view.
2. Select a Malware Analysis service, and select  **> View > Config**.
3. In the **Services Config** view, select the **Proxy** tab.
4. To enable the proxy, select the **Enabled** checkbox.
5. (Optional) To automatically detect proxy settings for the NetWitness Server, select the checkbox.
   The proxy host and proxy port fields are autofilled.

6. If you want to use a different proxy, enter the **Proxy Host** and **Proxy Port**.
7. Enter the username and password used to log on to the proxy host.
8. (Optional) Select **SSL**, if the proxy host communicates over SSL.
9. Click **Apply**.
10. Restart the Malware service.

Note: Malware Analysis does not support NTML web proxy authentication.

(Optional) Register for a ThreatGRID API Key

This topic provides the procedure for obtaining a trial ThreatGRID API key for use in the ThreatGRID Cloud sandbox. Before enabling ThreatGRID as the sandbox service in the sandbox module, a ThreatGRID-supplied Service Key must be configured so that ThreatGRID can recognize that samples submitted from this site are legitimate.

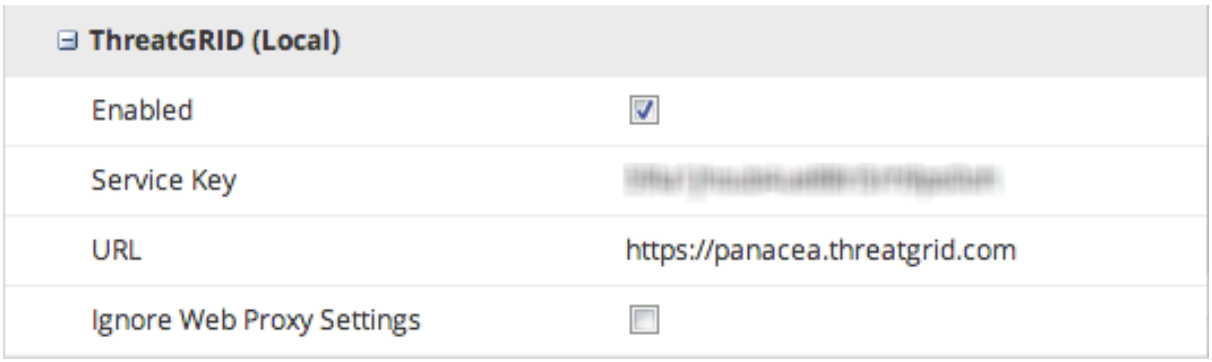
If you do not have a ThreatGRID-supplied Service Key, you can obtain a key using this tab. The key is provided on a trial basis.

When you fill in your user information and click **Register**, a key is displayed in this tab, and automatically added to the ThreatGRID configuration in the **General** tab. In a few minutes, you will receive an email from ThreatGRID containing a link to their page where you can log on. After you agree to the license terms on the ThreatGRID page, you can submit files for analysis, and ThreatGRID will recognize files that Malware Analysis submits for sandbox analysis.

To obtain a Trial ThreatGRID API key:

1. Go to  **(Admin) > Services**.
2. Select a Malware Analysis service, and select  **> View > Config**.
3. In the **Services Config** view, select the **ThreatGRID** tab.
4. Enter your full name, job title, organization name, and email address.
5. In the User Id and Password field, create a user ID and password for logging on to ThreatGRID.
6. Click **Register**.

   Your registration is sent to ThreatGRID and an API key is displayed below the Register button. The key is automatically filled in the **General** tab.
7. Select the **General** tab to confirm that the ThreatGRID configuration now includes the API key.



8. When you receive an email from ThreatGRID with a link where you can log on, log on and accept the terms of the agreement.

   Your trial of ThreatGRID begins and Malware Analysis can send five files per day to the ThreatGRID Cloud for sandbox analysis.

Additional Procedures for Configuring Malware Analysis

This topic provides procedures that an Administrator may perform to accomplish an objective that is not part of basic Malware Analysis setup. After Malware Analysis is configured, administrators may want to fine-tune the service and implement advanced customization; an example of this is implementing custom YARA content.

- Create Custom Alert in CEF Format
- Enable Custom YARA Content

Create Custom Alert in CEF Format

This topic provides instructions for creating custom alerts in Common Event Format (CEF) to send to a service that ingests events as CEF. This is an advanced configuration task, which requires sufficient knowledge to manually edit the configuration file: `/var/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`. Before editing the file, you must stop the Malware Analysis service in the operating system. The CEF Alert becomes active when you restart the Malware Analysis service.

The CEF Template

To send events to a service ingesting events as CEF, NetWitness runs them through a configuration file that serves as a CEF template before feeding the events to a correlation technology. You can tune the configuration file, which specifies the sequence and mapping of syslog fields in each alert.

The following example syslog message shows the CEF fields in the extensions section of the alert (following the last '|' in the alert). Each field can be configured to indicate the sequence (described in the Example section below). Fields can be excluded entirely from the alert via a configuration setting.

```
CEF:0|NetWitness|Spectrum|10.3.0.7995.1.0|Suspicious Event|Detected
suspicious network event ID 4 session ID n/a|2|static=100.0 nextgen=25.0
community=100.0 sandbox=25.0 file.name=myFile.exe file.size=1234556
file.md5.hash=DEADBEEFBABECAFEDEADBEEFBABECAFE
event.source=spectrum://admin@0:0:0:0:0:0:0:1:64563 event.type=MANUAL_
UPLOAD event.id=0 country.dst.code=-- country.dst=Unavailable
ip.src=0:0:0:0:0:0:0:1 ip.dst=0:0:0:0:0:0:0:1 event.uuid=f7a6155a-31de-
4fa6-ba16-41fb9a8e5f26 ...
```

Understand a Syslog Auditing File Entry

The description of the file structure is based on the following sample.

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125

CEF: 0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected suspicious
 network event ID 857 session ID 73|2|

static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
```

```
com.netwitness.event.internal.id=73
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk filetype=rtf
alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6 tcp.flags=27
ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73 medium=1
size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_attachment.doc
server=Apache/2.2.13 (Fedora) streams=2 referer=http://qa-fc12-
149/files/MALWAREMALW...fficeDocs/DOC/ risk.info=http client server version
mismatch
```

First Line

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
```

Log Information	Description
Feb 6 10:02:28	The timestamp for the entry.
10.10.10.125	The source IP address for the event.
SpectrumServer125	The source hostname for the event.

Audit Common Event Format (CEF) Header

```
0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected suspicious network
event ID 857 session ID 73|2|
```

The audit CEF header is a pipe-separated listing of the following fields:

Log Information	Description
0	The ArcSight Common Event Format (CEF) version used for the audit syslog.
NetWitness	The service that created the syslog message.
Spectrum	Malware Analysis is the logger for the event.
1.2.1.130	Malware Analysis version.
event ID 857	Unique network event id for this event.
session ID 73	Core unique session id for the session that included this event.

Log Information	Description
2	Severity, an integer between 1 and 6 indicates the level of severity for the message. • 1 = INFORMATION_LEVEL • 2 = WARNING_LEVEL • 3 = ERROR_LEVEL • 4 = SUCCESS_LEVEL • 5 = FAILURE_LEVEL • 6 = AUDIT_FAILURE_LEVEL

Audit CEF Extension

```
static=100.0 network=29.0 community=8.0 sandbox=N/R
file.name=-CVE-00_DOC_2010-05-13_attachment.doc  file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
com.netwitness.event.internal.id=73
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk filetype=rtf
alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6 tcp.flags=27
ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73 medium=1
size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_attachment.doc
server=Apache/2.2.13 (Fedora) streams=2 referer=http://qa-fc12-
149/files/MALWAREMALW...fficeDocs/DOC/ risk.info=http client server version
mismatch
```

Analysis Scores

The first entry in the audit CEF extension provides the four Malware Analysis scores for the event: Static, Network, Community, and Sandbox.

Log Information	Sample Value
static	100.0
network	29.0
community	8.0 A score of 0.0 can be a community score for the event or can indicate that no community services were enabled.

Log Information	Sample Value
sandbox	N/R N/R means not run. This indicates that the GFI sandbox was not enabled.

File Information

The next three entries provide file information: file name, size, and hash.

Log Information	Sample Value
file.name	-CVE-00_DOC_2010-05-13_attachment.doc
file.size	0
file.md5.hash	20a29259c0e5958afb2f50c4177bb307

Event Meta Data Retrieved by NextGen

The record continues with the Core meta data for the event. The meta data in the message depends on the event. The amount of data in the message is truncated to the maximum length in bytes configured in the Syslog Settings. The default value is 1024.

Log Information	Sample Value
com.netwitness.event.internal.id	73
com.netwitness.event.internal.uuid	37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip	10.25.50.149
client	Wget/1.11.4 Red Hat modified
payload	108872
packets	136
country.dst	Private
time	Fri Jan 27 10:09:25 EST 2012
threat.source	netwitness
tcp.srcport	43580
action	get
com.netwitness.event.internal.source	http://QASpectrum2:50104/sdk
filetype	rtf

Log Information	Sample Value
alias.host	qa-fc12-149
eth.src	00:25:90:18:76:E2
ip.proto	6
tcp.flags	27
ip.src	10.25.50.61
tcp.dstport	80
threat.category	spectrum
eth.dst	00:0C:29:F8:50:2D
lifetime	0
alert.id	nw32535
sessionid	73
medium	1
size	117864
content	spectrum.consume11
extension	doc
directory	/files/MALWAREMALWARE/OfficeDocs/DOC/
eth.type	2048
ip.dst	10.25.50.149
service	80
filename	-CVE-00_DOC_2010-05-13_attachment.doc
server	Apache/2.2.13 (Fedora)
streams	2
referer	http://qa-fc12-149/files/MALWAREMALWARE/OfficeDocs/DOC/
risk.info	http client server version mismatch

Edit the Configuration File

1. Stop the Malware Analysis service.
2. Edit the configuration file as described in the Example.

3. Start the Malware Analysis service.

   The Malware Analysis service begins processing alerts through the configuration file and sending CEF alerts to designated services.

Example

The configuration file can be used to dictate which fields appear in the resulting alert as well as the label associated with each field and the order in which the data fields appear. The configuration file is composed of one or more XML `MalwareCefExtension` blocks as shown in the example below. The ordering of these blocks in the configuration file implies the order of the data fields in the CEF alert.

In the example below, the CEF alert would include two data fields, `ip.src` followed by `ip.dst`. The `customKey` is used to indicate the labeling of the data field in the alert. This allows the user to choose a custom label in order to force the alerting format to better match the expectations of the alert consumer. In other words, the format can be tuned to prevent unwanted changes to an existing alert parser. Lastly, the `isDisplay` setting determines if the field is included in the alert output. This allows the user to turn off data fields without having to physically delete the `MalwareCefExtension` block from the configuration.

```
 <config>
 <malwareExtensionList>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.src</customKey>
   <malwareKey>ip.src</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.dst</customKey>
   <malwareKey>ip.dst</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
 </malwareExtensionList>
</config>
```

At the end of the configuration file are three additional settings that can be used to further tune the alert format. They are as follows:

Setting	Description
includesUnknownMeta	This true or false setting indicates if unknown data elements are included in the resulting alert. Any NextGen session meta can be considered for inclusion into a CEF alert. Because additional session meta can be introduced via authoring new NextGen parsers, meta that is not contained in the default configuration may be encountered. You can set includesUnknownMeta to true to include the unknown meta in the alert and label it using the NextGen meta key name. To force a custom key for the unknown meta, you must edit this file and add a new MalwareCefExtension to the dictionary. To omit unknown meta from the alert, set includesUnknownMeta to false.
displayNulls	This true or false setting indicates if values that are set to null are included in the alert. If displayNulls is set to false, the null value fields are omitted even if their MalwareCefExtension isDisplay property is turned on. This allows dynamic formatting of alerts to exclude null fields.
valueIfNull	This true or false setting allows you to specify a string placeholder (n/a by default) to be used as the value for any null valued fields. If displayNulls is set to true, then null valued fields are included in the alerts. Their value is set to the value specified in valueIfNull.

The following represents the default CEF configuration file. The default configuration file includes all default NextGen session meta.

```
<config>
  <malwareExtensionList>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>static</customKey>
   <malwareKey>static</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>nextgen</customKey>
   <malwareKey>nextgen</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>community</customKey>
   <malwareKey>community</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>sandbox</customKey>
```

```
<malwareKey>sandbox</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.name</customKey>
<malwareKey>file.name</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.size</customKey>
<malwareKey>file.size</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.md5.hash</customKey>
<malwareKey>file.md5.hash</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.source</customKey>
<malwareKey>event.source</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.type</customKey>
<malwareKey>event.type</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.id</customKey>
<malwareKey>event.id</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.uuid</customKey>
<malwareKey>event.uuid</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.primary.detected</customKey>
<malwareKey>antivirus.primary.detected</malwareKey>
```

```
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.secondary.detected</customKey>
<malwareKey>antivirus.secondary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.other.detected</customKey>
<malwareKey>antivirus.other.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst.code</customKey>
<malwareKey>country.dst.code</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>city.dst</customKey>
<malwareKey>city.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>org.dst</customKey>
<malwareKey>org.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>payload</customKey>
<malwareKey>payload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>packets</customKey>
<malwareKey>packets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst</customKey>
<malwareKey>country.dst</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>time</customKey>
<malwareKey>time</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.source</customKey>
<malwareKey>threat.source</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcpport</customKey>
<malwareKey>tcp.srcpport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filetype</customKey>
<malwareKey>filetype</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.dst</customKey>
<malwareKey>latdec.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src</customKey>
<malwareKey>eth.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>agency.dst</customKey>
<malwareKey>agency.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.proto</customKey>
<malwareKey>ip.proto</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.flags</customKey>
<malwareKey>tcp.flags</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.src</customKey>
<malwareKey>ip.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.dstport</customKey>
<malwareKey>tcp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.category</customKey>
<malwareKey>threat.category</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst</customKey>
<malwareKey>eth.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>lifetime</customKey>
<malwareKey>lifetime</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.src</customKey>
<malwareKey>latdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>did</customKey>
<malwareKey>did</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>alert.id</customKey>
<malwareKey>alert.id</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.src</customKey>
<malwareKey>country.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>sessionid</customKey>
<malwareKey>sessionid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>longdec.src</customKey>
<malwareKey>longdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>medium</customKey>
<malwareKey>medium</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>size</customKey>
<malwareKey>size</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.computer.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.src</customKey>
```

```
<malwareKey>ad.username.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpackets</customKey>
<malwareKey>rpackets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>action</customKey>
<malwareKey>action</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.src</customKey>
<malwareKey>ad.domain.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src.vendor</customKey>
<malwareKey>eth.src.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpayload</customKey>
<malwareKey>rpayload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.dst</customKey>
<malwareKey>ad.username.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>content</customKey>
<malwareKey>content</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>extension</customKey>
<malwareKey>extension</malwareKey>
```

```
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst.vendor</customKey>
<malwareKey>eth.dst.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rid</customKey>
<malwareKey>rid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>directory</customKey>
<malwareKey>directory</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.suspicious</customKey>
<malwareKey>risk.suspicious</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.type</customKey>
<malwareKey>eth.type</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.dst</customKey>
<malwareKey>ip.dst</malwareKey>
<isDisplay>false</isDisplay>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>service</customKey>
<malwareKey>service</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filename</customKey>
<malwareKey>filename</malwareKey>
```

```
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>streams</customKey>
<malwareKey>streams</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.info</customKey>
<malwareKey>risk.info</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>dest.tld</customKey>
<malwareKey>dest.tld</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alias.host</customKey>
<malwareKey>alias.host</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcport</customKey>
<malwareKey>tcp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.srcport</customKey>
<malwareKey>udp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.dstport</customKey>
<malwareKey>udp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>domain.dst</customKey>
<malwareKey>domain.dst</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.name</customKey>
<malwareKey>feed.name</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.description</customKey>
<malwareKey>feed.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.description</customKey>
<malwareKey>threat.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>referer</customKey>
<malwareKey>referer</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>client</customKey>
<malwareKey>client</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>server</customKey>
<malwareKey>server</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.warning</customKey>
<malwareKey>risk.warning</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>attachment</customKey>
<malwareKey>attachment</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
    <com.netwitness.malware.core.cef.MalwareCefExtension>
    <customKey>whois.registrar</customKey>
    <malwareKey>whois.registrar</malwareKey>
    <isDisplay>false</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
    <customKey>whois.registrant</customKey>
    <malwareKey>whois.registrant</malwareKey>
    <isDisplay>false</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
    <customKey>whois.date.creation</customKey>
    <malwareKey>whois.date.creation</malwareKey>
    <isDisplay>false</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
    <com.netwitness.malware.core.cef.MalwareCefExtension>
    <customKey>whois.server</customKey>
    <malwareKey>whois.server</malwareKey>
    <isDisplay>false</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
  </malwareExtensionList>
  <includesUnknownMeta>false</includesUnknownMeta>
  <displayNulls>false</displayNulls>
  <valueIfNull>n/a</valueIfNull>
</config>
```

Enable Custom YARA Content

This topic provides instructions for enabling custom YARA content on the NetWitness host on which the Malware Analysis service is installed. In addition to the built-in Indicators of Compromise, Malware Analysis supports indicators of compromise written in YARA. YARA is a rule language that allows malware researchers to identify and classify malware samples. RSA makes built-in YARA-based Indicators of Compromise (IOCs) available in RSA Live; these are automatically downloaded and activated on subscribed appliances.

Customers with advanced skills and knowledge can add detection capabilities to RSA Malware Analysis by authoring YARA rules and publishing them in RSA Live or placing YARA rules in a watched folder for the appliance to consume. This section provides instructions for the Administrator who configures appliances to enable the creation of custom YARA content.

Prerequisites

This is an advanced configuration task, which requires sufficient privilege and knowledge to set up a GNU Compiler Collection (GCC) and C++ Python development library to build YARA. In addition, you must be thoroughly familiar with the standard YARA documentation. The following components are required:

- The Perl-Compatible Regular Expression (PCRE) library: pcre-8.33.tar.bz2
- The yara 1.7 (rev:167) stand-alone YARA command line: yara-1.7.tar
- The YARA extension for Python: yara-python-1.7.tar.gz
- YARA rules documentation: YARA User's Manual 1.6.pdf

The components are available for download here: https://code.google.com/p/yara-project/downloads/list

Note: As of writing, YARA 2.0 is available but not supported for Malware Analysis 10.5.

Install Libraries and Applications Required to Build YARA on a CentOs-Based Appliance

As a prerequisite to building YARA on a host that is running CentOS, you must install `make`, the GNU Compiler Collection, and C++ Python Development Library on the appliance. To install the applications and libraries required to build YARA:

1. To ensure the standard YUM repo and no other repo files are in the /etc/yum.repos.d folder, enter the following command:
   `ls -al /etc/yum.repos.d`
   The results should be similar to the following:
   ```
   -rw-r-r-. 1 root root 1926 Jun 26  2012 CentOS-Base.repo
   -rw-r-r-. 1 root root  637 Jun 26  2012 CentOS-Debuginfo.repo
   -rw-r-r-. 1 root root  626 Jun 26  2012 CentOS-Media.repo
   -rw-r-r-. 1 root root 2593 Jun 26  2012 CentOS-Vault.repo
   ```
2. To install `make` on the appliance, enter the following commands:
   a. **`yum search make`**
      The following message is returned: `make.x86_64 : A GNU tool which simplifies the build process for user`
   b. **`yum install make.x86_64`**
3. To install and test GCC on the host, enter the following commands:
   a. **`yum search gcc`**
      The following messages are displayed:
      ```
      gcc-c+.x86_64 : C+ support for GCC
       gcc.x86_64 : Various compilers (C, C++, Objective-C, Java, ...)
      ```
   b. Enter the following commands:
      `yum install gcc.x86_64`
      `yum install gcc-c++.x86_64`

c. To test the gcc commands, enter the following commands:

```
gcc -v
cc -v
```

4. To install the C++ Python development library on the appliance, enter the following commands:

a. **yum search python dev**
The following message is returned:
`python-devel.x86_64 : The libraries and header files needed for Python development`

b. **yum install python-devel.x86_64**

Set Up YARA

To create a GCC and C++ Python development library in which you can build YARA on the NetWitness host that is running Malware Analysis:

1. Do one of the following:

a. If the host on which you are installing is running Mac OS, install xCode for Mac OS.

b. If the host on which you are installing is running CentOS, install make, GCC and C++ Python development library using the YUM command line.

2. To Install the PCRE library on the host, open a terminal window and enter the following commands:

```
tar -xvf pcre-8.33.tar.bz2
cd pcre-8.33
./configure
make
sudo make install
```

3. To install the stand-alone YARA command line, enter the following commands:

```
tar -xvf yara-1.7.tar
cd yara-1.7
./configure
make
sudo make install
```

4. To test the stand-alone YARA command line:

a. Enter the following command:

```
yara
```

b. If the command succeeds, continue with Step 7. If the command fails and returns the `yara: error while loading shared libraries: libpcre.so.1: cannot open shared object file: No such file or directory` error, enter the following command to check the `/etc/ld.so.conf` file or `LD_LIBRARY_PATH` environment variable.

```
ldconfig -v
```

5. To install the YARA extension for Python, enter the following commands:

```
tar -xvf yara-python-1.7.tar.gz
cd yara-python-1.7
```

```
python setup.py build
sudo python setup.py install
```

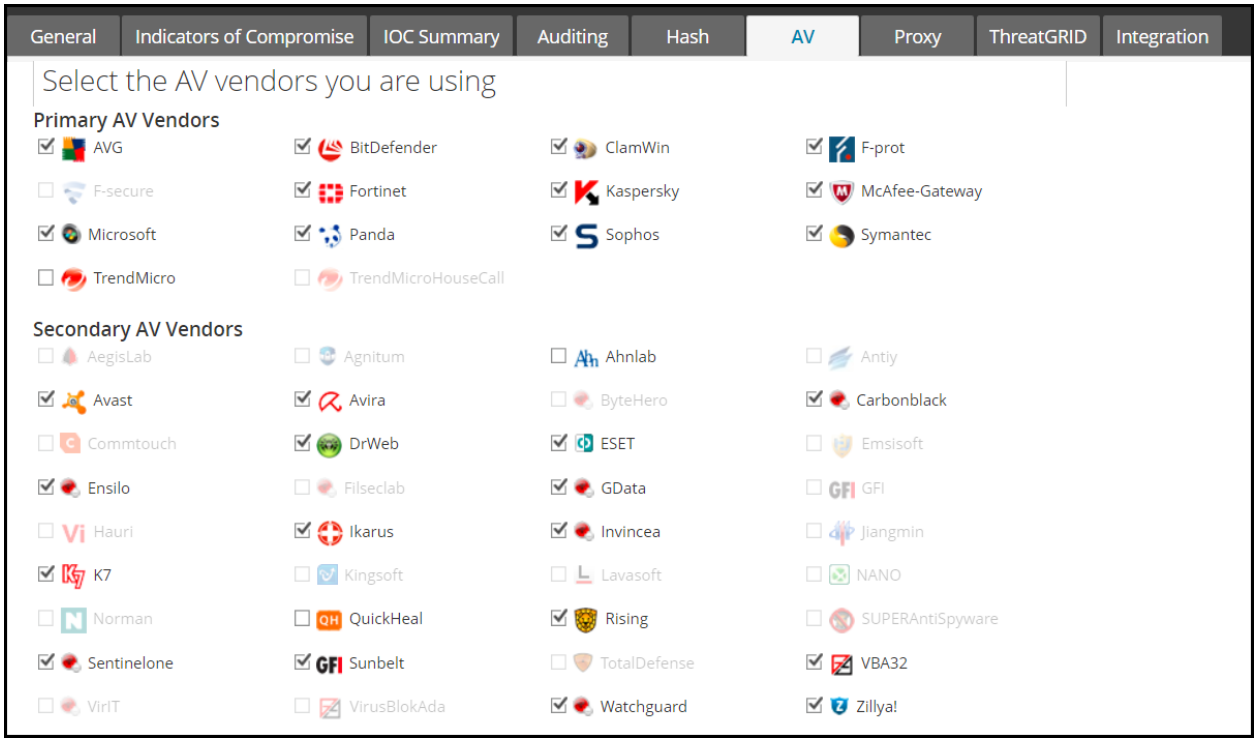
6. To test the YARA extension:
   a. Enter the following command: **python**
   b. At the Python prompt (>>>), enter the following commands:

```
import yara
exit()
```

When this configuration is complete, analysts can create custom YARA IOCs for consumption on a Malware Analysis host as described in "Implement Custom YARA Content" in the *Malware Analysis User Guide*

Supported Antivirus Vendors

This section provides detailed information about the NetWitness supported antivirus (AV) vendors.



The following are the new AV vendors supported in NetWitness version 11.4.0.1 or later.

- Panda
- Gdata
- Avast
- Carbonblack
- Dr.Web
- enSilo
- Invincea
- Rising
- SentinelOne
- Sunbelt
- VBA32
- Watchguard

The following AV vendors are not supported in NetWitness version 11.4.0.1 or later.

Note: AV vendors that are not supported by NetWitness Platform are disabled in the user interface.

- F-secure
- TrendMicroHouseCall
- AegisLab
- Agnitum
- Antiy
- ByteHero
- Commtouch
- Emsisoft
- Filseclab
- GFI
- Hauri
- Jiangmin
- Kingsoft
- Lavasoft
- NANO
- Norman
- nProtect
- SUPERAntiSpyware
- TotalDefense
- VirIT
- VirusBlokAda
- Zillya
- Zoner

Malware Analysis References

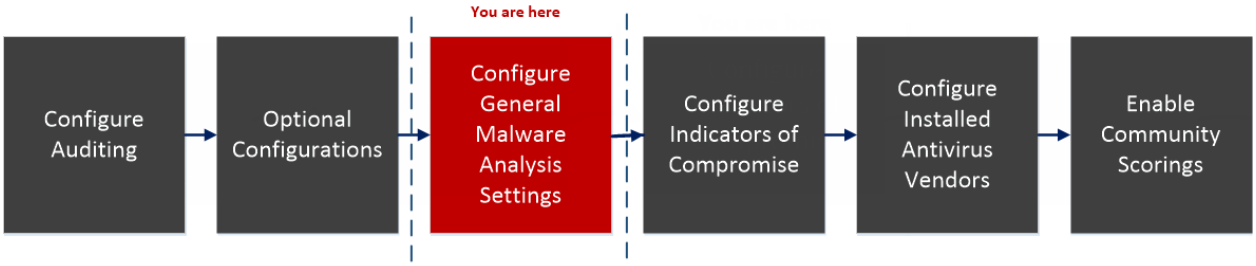
- Services Config View - General Tab
- Services Config View - Indicators of Compromise Tab
- Services Config View - IOC Summary Tab
- Services Config View - Auditing Tab
- Services Config View - Hash Tab
- Services Config View - AV Tab
- Service Config View - Proxy Tab
- Services Config View - ThreatGRID Tab
- Services Config View - Integration Tab

Services Config View - General Tab

This topic introduces the configuration settings in the Service Config view > General tab for Malware Analysis, which has parameters specific to the Malware Analysis service. In this tab, you can configure:

- The processing parameters for Core services that are capturing data.
- The repository for captured data.
- The static, community, and sandbox scoring categories used to analyze the data.

Workflow



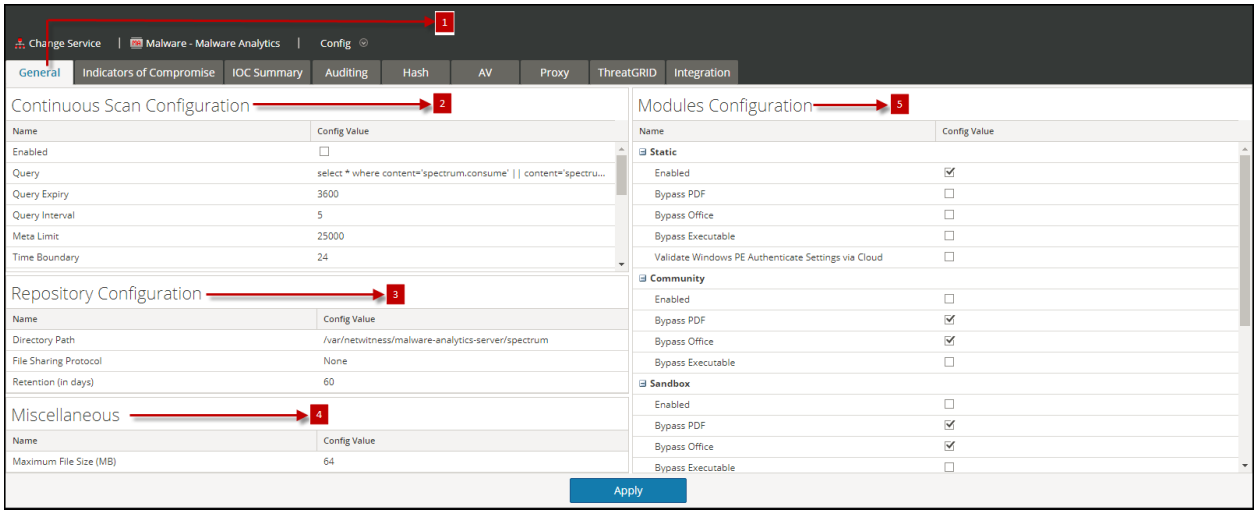
What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings*	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

*You can perform this task in the current view

Quick Look

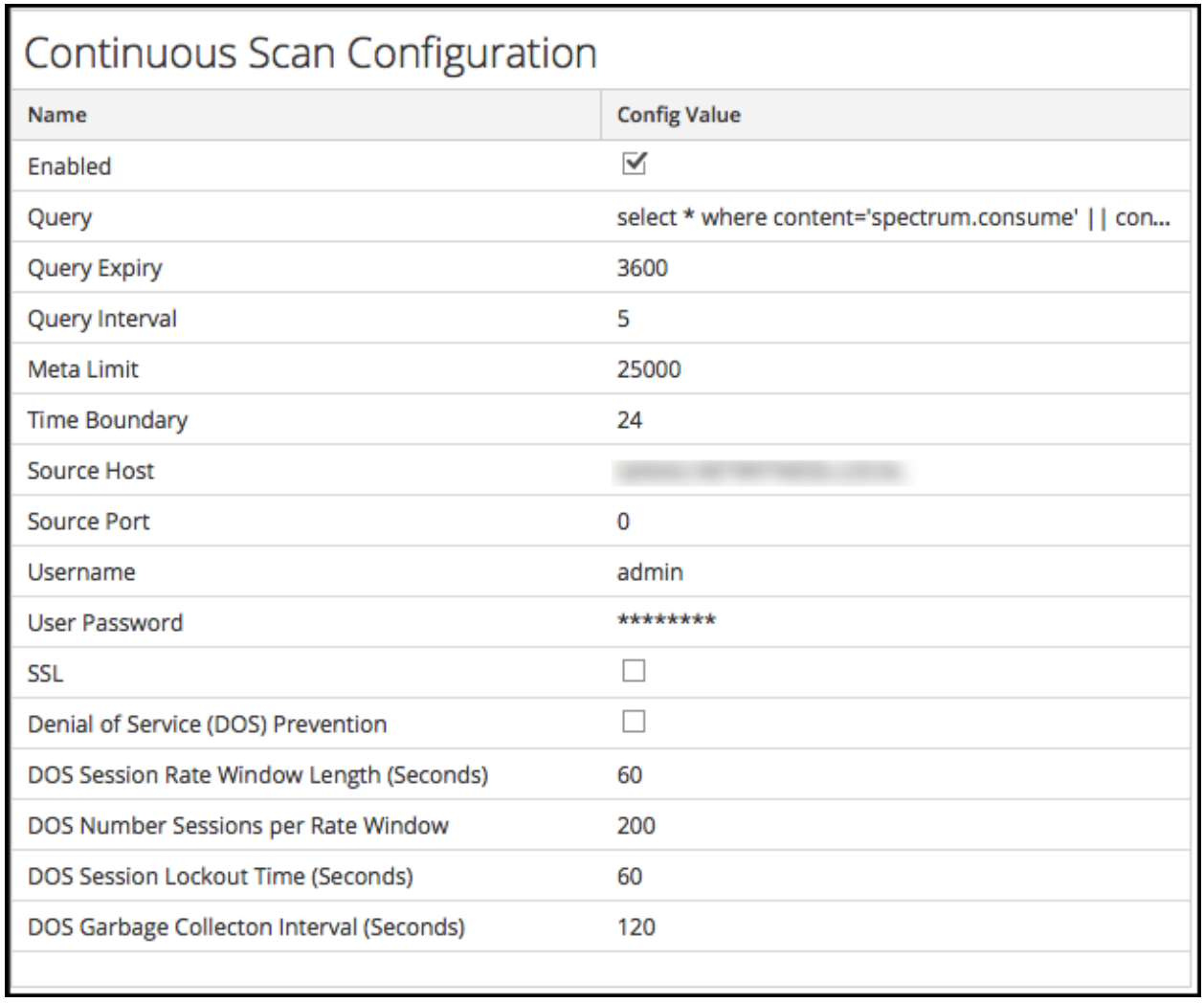
This is an example of the General tab.



1 Displays the General Tab.
2 Allows you to Configure Continuous Scan.
3 Allows you to Configure Repository.
4 Displays Miscellaneous Settings.
5 Allows you to Configure Modules.

This tab has four sections: Continuous Scan Configuration, Repository Configuration, Miscellaneous, and Modules Configuration.

Continuous Scan Configuration Section



Continuous Scan Configuration

Name	Config Value
Enabled	☑
Query	select * where content='spectrum.consume' || con...
Query Expiry	3600
Query Interval	5
Meta Limit	25000
Time Boundary	24
Source Host	[redacted]
Source Port	0
Username	admin
User Password	********
SSL	☐
Denial of Service (DOS) Prevention	☐
DOS Session Rate Window Length (Seconds)	60
DOS Number Sessions per Rate Window	200
DOS Session Lockout Time (Seconds)	60
DOS Garbage Collecton Interval (Seconds)	120

This table describes the features of the Continuous Scan Configuration section.

Parameter	Description
Enabled	Completely disable or enable continuous polling of the Core service. By default this is not selected (**disabled**).
Query	While the Decoder is analyzing network traffic, it creates a meta field called content with a value of **spectrum.consume** in sessions that are likely to contain malware. By default, Malware Analysis only performs analysis on events that have this particular meta value. By changing this query, Malware Analysis can be configured to analyze different types of events. Making this query too broad may force Malware Analysis to analyze too many events, causing it to fall behind or perform poorly. The default query is **select * where content='spectrum.consume'**

Parameter	Description
Query Expiry	When Malware Analysis queries the Core service for meta, it gets a result back within a few seconds. If there is a problem, such as a network connectivity issue, Malware Analysis abandons the query after this configured amount of time. The default value is **3600 seconds**.
Query Interval	How often, in minutes, to query for new session meta and files.
Meta Limit	Each time Malware Analysis queries the Core service, it pulls an amount of meta, up to this meta limit. Using this setting, in conjunction with the query interval, you can tune the performance of Malware Analysis in the Core infrastructure. The default value is **25000**.
Time Boundary	Malware Analysis analyzes sessions that occurred after the Time Boundary. This setting is most important when installing a new Malware Analysis appliance, because it determines how far back in time to begin analysis. Setting the boundary too many hours in the past may cause Malware Analysis to analyze too many past events, causing a large delay before you see any traffic happening in real time. The default value is **24 hours**.
Source Host	Hostname of the Malware Analysis appliance. This is the IP address, or the hostname, of the service that Malware Analysis queries to retrieve its data for analysis. Do not use localhost as the source host. Depending on the model of the appliance and the configuration of the NetWitness infrastructure, this source host can vary. **Note:** When you change the host name or the host IP address, ensure that you re add the Source Host in the Malware Service config page, and restart the service to take the source host field changes into effect.
Source Port	Malware Analysis communicates with the NetWitness infrastructure using the REST service listening on this port. This port number is specific to the type of the Core service that is being used as the Source host. This corresponds to the outbound connections for your Core service.
Username	Username. The default value is **admin**. Malware Analysis must authenticate to the Source host each time it queries for data. In most cases, the account used by Malware Analysis is the same account used to access the Core service through NetWitness. However, it is recommended to create a new account on the Core service dedicated to Malware Analysis.
User Password	User password. The default value is **netwitness**.
SSL	Use SSL when communicating with Core. If Malware Analysis is using an SSL connection to communicate with a Core service, check this option. The default value is unchecked.

Parameter	Description
Denial of Service (DOS) Prevention	The Denial of Service Prevention feature provides safeguards against malware that intentionally generates high volumes of network connections between two endpoints containing Windows PE content. Generating a high volume of connections artificially inflates the amount of traffic that security services monitoring the network must consume and analyze resulting in a denial of service. This feature helps identify these sessions so that you can have the analysis processing disregard them. The default value is unchecked.
DOS Session Rate Window Length (Seconds)	Malware Analysis uses this parameter with the **DOS Number Sessions per Rate Window** and **DOS Session Lockout Time (Seconds)** parameters to identify a Denial of Service Attack and determine how long to disregard sessions from a single IP address. To identify a Denial of Service Attack, Malware Analysis monitors the number of sessions established by a single IP address during a specific time frame. The **DOS Session Rate Window Length (Seconds)** defines this time frame. If the number of sessions exceeds the **DOS Number Sessions per Rate Window** setting within the number of seconds defined in **DOS Session Rate Window Length**, Malware Analysis identifies the activity as a Denial of Service attempt. In this case, traffic from the IP address is disregarded for the length of time specified in **DOS Session Lockout Time (Seconds)**. The default value is: **60** seconds.
DOS Number Sessions per Rate Window	Malware Analysis uses this parameter with the **DOS Session Rate Window Length (Seconds)** and **DOS Session Lockout Time (Seconds)** parameters to identify a Denial of Service Attack and determine how long to disregard sessions from the IP address. To identify a Denial of Service Attack, Malware Analysis monitors the number of sessions established by a single IP source during a specific time frame. The **DOS Session Rate Window Length (Seconds)** defines this time frame. If the number of sessions exceeds the **DOS Number Sessions per Rate Window** setting within the number of seconds defined in **DOS Session Rate Window Length**, Malware Analysis identifies the activity as a Denial of Service attempt. In this case, traffic is disregarded for the length of time specified in **DOS Session Lockout Time (Seconds)**. The default value is: **200** sessions
DOS Session Lockout Time (Seconds)	Malware Analysis uses this parameter with the **DOS Session Rate Window Length (Seconds)** and **DOS Number Sessions per Rate Window** parameters to identify a Denial of Service Attack and determine how long to disregard such an attack. To identify a Denial of Service Attack, Malware Analysis monitors the number of sessions established by a single IP address during a specific time frame. The **DOS Session Rate Window Length (Seconds)** defines this time frame. If the number of sessions exceeds the **DOS Number Sessions per Rate Window** setting within the number of seconds defined in **DOS Session Rate Window Length**, Malware Analysis identifies the activity as a Denial of Service attempt. In this case, traffic is disregarded for the length of time specified in **DOS Session Lockout Time (Seconds)**. The default value is: **60** seconds

Parameter	Description
DOS Garbage Collection Interval (Seconds)	Performs garbage collection on the internal memory structure used to track Denial of Service attempts. If memory usage is abnormally high, you can decrease this setting to free unused memory more often. If CPU usage is abnormally high, you can increase this setting to eliminate processing overhead (at the expense of memory usage). The default value is: **120** seconds

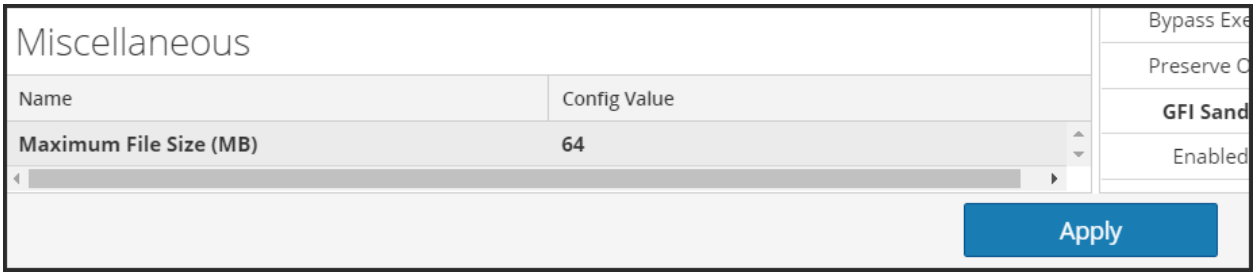
Repository Configuration Section

Malware Analysis stores all of the files that are analyzed for future use. These files can be downloaded through the user interface or accessed via one of the file sharing protocols.

This table describes the features of the Repository Configuration section.

Parameter	Description
Directory Path	All files are stored in the following directory on the Malware Analysis appliance: **/var/lib/netwitness/spectrum**
File Sharing Protocol	Possible values for the file sharing protocol are FTP, SAMBA, and None. You can enable FTP access and SAMBA file sharing to allow a user access to the stored files on the Malware Analysis from a remote location. No credentials are required to access these files. The port required for FTP access is TCP/21. The default file sharing protocol is **None**.
Retention (in days)	Malware Analysis maintains files stored in the repository for a specified number of days. You can set the number of days that files are retained before being deleted. The default value is **60** days.

Miscellaneous Configuration Section (10.3 SP2 and Later)



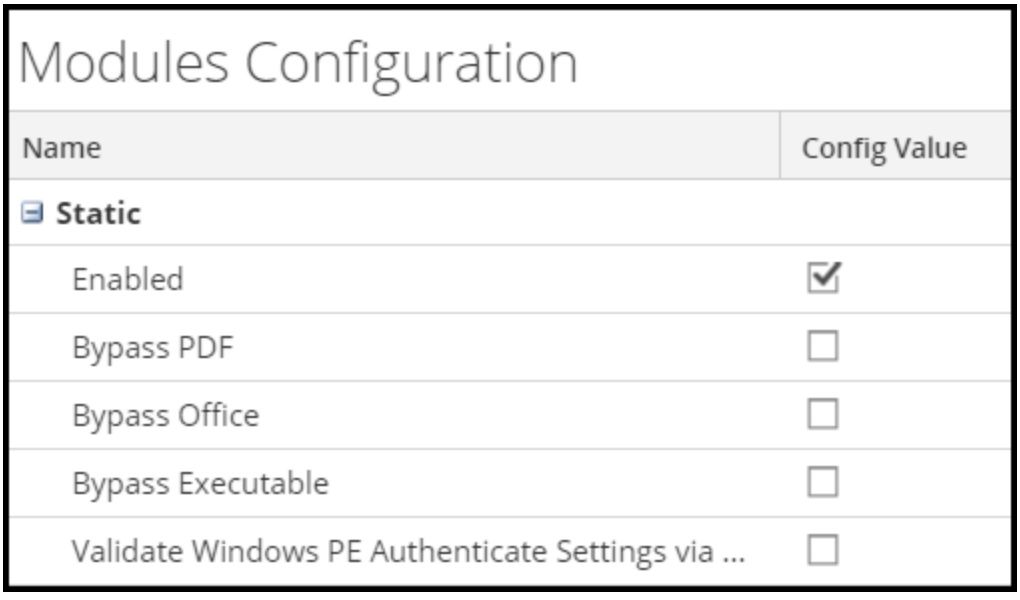
This table describes the features of the Miscellaneous Configuration section.

Parameter	Description
Maximum File Size	Limits the size of each file that you can scan for manually. This parameter applies to the feature described in "Upload Files for Malware Scanning" in the Investigation and Malware Analysis Configuration Guide. The default value is **64 MB**. If the file size limit is exceeded, prevents you from scanning the file.

Modules Configuration Section

The Modules Configuration section allows configuration of the static, community, and sandbox scoring categories.

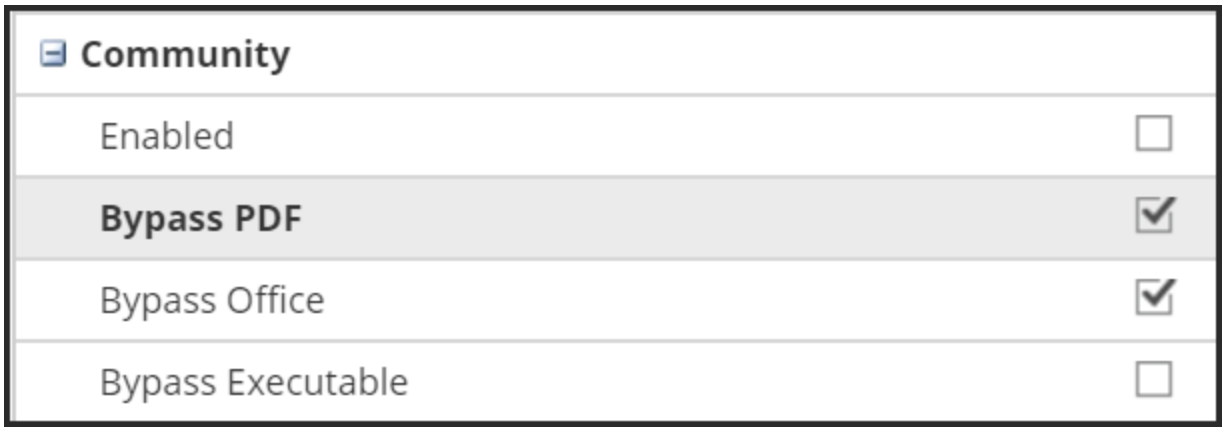
Static Analysis Configuration



The static module is the only scoring category that is enabled by default. This table describes the parameters for configuring static analysis.

Feature	Description
Enabled	Completely disable or enable static analysis. By default this is selected (**enabled**).
Bypass PDF	Disable analysis of PDF documents. By default this is not selected; all PDF files undergo static analysis.
Bypass Office	Disable analysis of Office documents. By default this is not selected; all MS Office files undergo static analysis.
Bypass Executable	Disable analysis of Windows PE documents. By default this is not selected; all Windows PE files undergo static analysis.
Validate Windows PE Authenticate Settings via Cloud	Specify whether or not Windows PE files are sent to the RSA-Netwitness Cloud for Authenticode validation. The default value is selected. • When selected, any Windows PE file that is digitally signed is transmitted over the network (in its entirety) to the RSA-Netwitness Cloud for validation. If the intent is to prevent Windows PE files from leaving the customer network, you should disable this option. • When not selected, ALL static analysis is performed locally (skipping Authenticode validation). Regardless of this setting, PDF and M/S Office documents are not subject to Authenticode validation and are not transmitted over the network during static analysis.

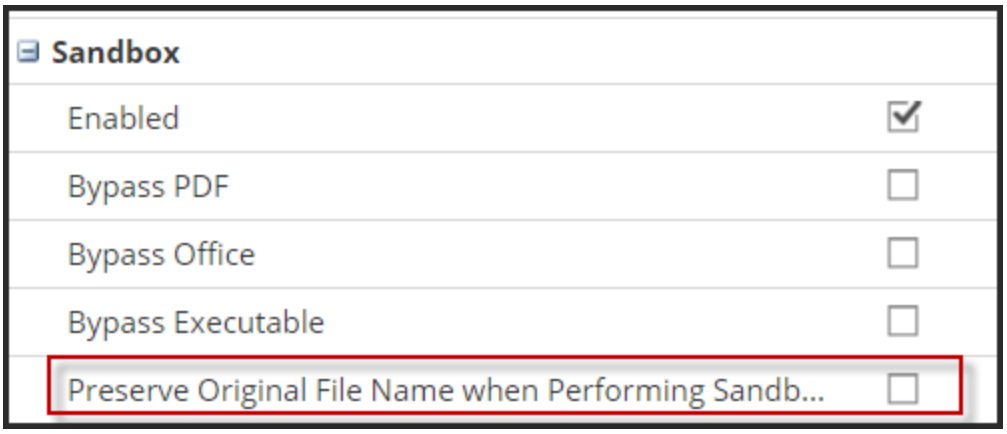
Community Analysis Configuration



By default, the community module is disabled and the options are selected to prevent PDFs and MS Office documents from being processed. The intent is to default the settings to the most restrictive choices so that no sensitive documents leave the network unless the user chooses. This table describes the parameters for configuring Community analysis.

Feature	Description
Enabled	Completely disable or enable community analysis. By default this is not selected (**disabled**). **Note:** Before you enable community, you must log in to live account. For more information about live account, see Live Services Management Guide.
Bypass PDF	Disable analysis of PDF documents. By default this is selected; PDF files are not processed.
Bypass Office	Disable analysis of Office documents. By default this is selected; Microsoft Office documents are not processed.
Bypass Executable	Disable analysis of Windows PE documents. By default this is selected; Windows PE documents are not processed

Sandbox Analysis Configuration



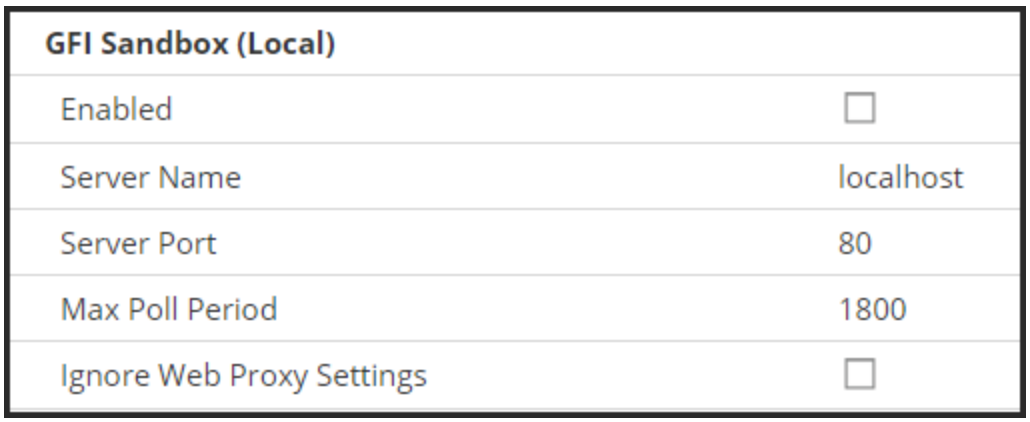
By default, the sandbox module is disabled and MS Office and PDF files are prevented from being processed. The intent is to set the most restrictive settings to force the user to specifically choose whether or not potentially sensitive information is sent outside of the network for processing. If the document type is not prevented from being processed, the file is sent to the destination sandbox server in its entirety (not limited to a hash of the file contents).

This table describes the parameters for configuring Sandbox analysis.

Feature	Description
Enabled	Completely disable or enable sandbox analysis. By default this is not selected **(disabled)**.
Bypass PDF	Disable analysis of PDF documents. By default this is selected; PDF files are not processed. When not selected, all PDF files are submitted in their entirety to the Sandbox for analysis.

Feature	Description
Bypass Office	Disable analysis of Office documents. By default this is selected; Microsoft Office documents are not processed. When not selected, all MS Office files are submitted in their entirety to the Sandbox for analysis.
Bypass Executable	Disable analysis of Windows PE documents. By default this is selected; Windows PE documents are not processed. When not selected, all Windows PE documents are submitted in their entirety to the Sandbox for analysis.
Preserve Original File Name when Performing Sandbox Analysis	In 10.3 SP2 and later, enable the ability to hash for filenames when they are sent to a local sandbox. By default this is not selected. **Note:** If you do not select this parameter, NetWitness hashes the files.

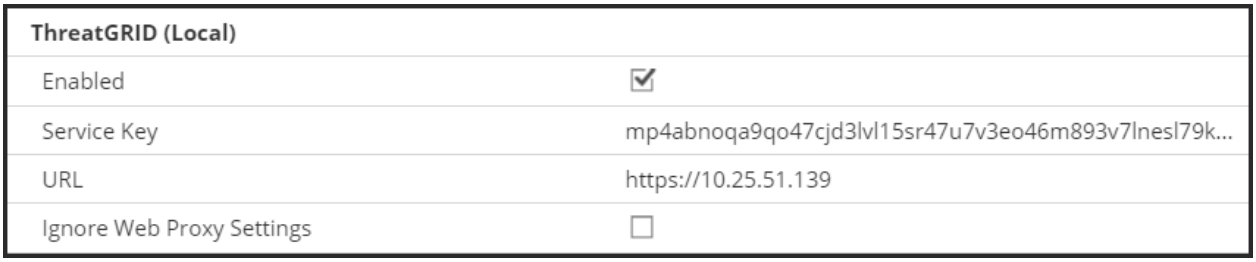
GFI Sandbox Settings



In the GFI Sandbox section, you can enable sandbox processing by GFI and configure the locally installed GFI sandbox. The table describes the parameters for configuring the GFI sandbox.

Feature	Description
Enabled	When enabled, sandbox processing is performed by a local copy of GFI. The default value is **disabled**. If you enable GFI, you need to configure the remaining parameters.
Server Name	The GFI Sandbox server name. No default value.
Server Port	The GFI Sandbox server port. Default value is **80**.
Max Poll Period	Determines how long to wait for a submitted sample to finish processing. Default value is **600 seconds**.
Ignore Web Proxy Settings	Tells Malware Analysis to bypass the web proxy, if a web proxy is configured, when making this connection. If no web proxy has been configured in Malware Analysis, the setting is ignored.

ThreatGRID Sandbox Settings



In the ThreatGRID Sandbox section, you can enable sandbox processing by ThreatGRID and choose whether to use the locally installed ThreatGRID or the ThreatGRID Cloud for sandbox analysis.

- If you have a local copy of ThreatGRID, configure sandbox processing to use the local copy.
- If no local instance of ThreatGRID has been purchased and installed, configure the ThreatGRID Cloud.

The table describes the parameters for configuring the ThreatGRID sandbox.

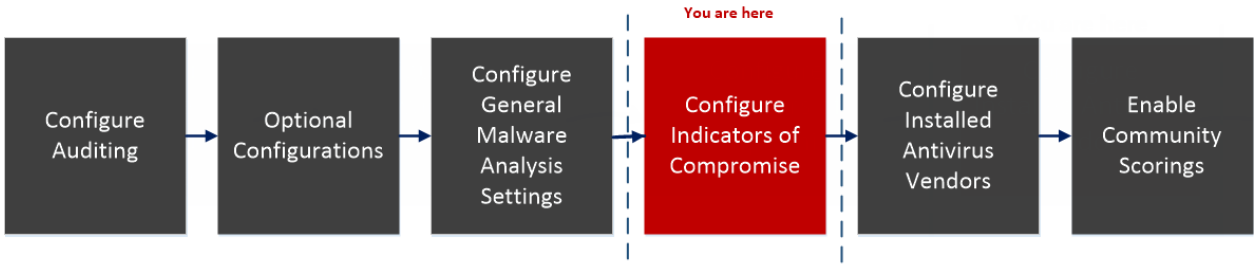
Note: Before enabling this service, you must configure a ThreatGRID-supplied Service Key. The service key allows ThreatGRID to recognize that samples submitted from this site are legitimate.

Feature	Description
Enabled	When enabled, sandbox processing is performed by ThreatGRID, either a local copy or the ThreatGRID Cloud. The default value is **disabled**.
Service Key	Before enabling the sandbox module, a ThreatGRID-supplied Service Key must be configured. The service key allows ThreatGRID to recognize that samples submitted from this site are legitimate.
URL	The URL for the ThreatGRID server to be used (if you are not using a locally installed ThreatGRID). The ThreatGRID Cloud is reachable via https://panacea.threatgrid.com
Ignore Web Proxy Settings	Tells Malware Analysis to bypass the web proxy, if a web proxy is configured, when making this connection. If no Web Proxy has been configured in Malware Analysis, the setting is ignored.

Services Config View - Indicators of Compromise Tab

This topic introduces the features and functions available in the Service Config view > Indicators of Compromise tab, which applies to the Malware Analysis service. This tab provides a way to configure the way each of the four scoring modules uses the available rules to score data.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise*	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

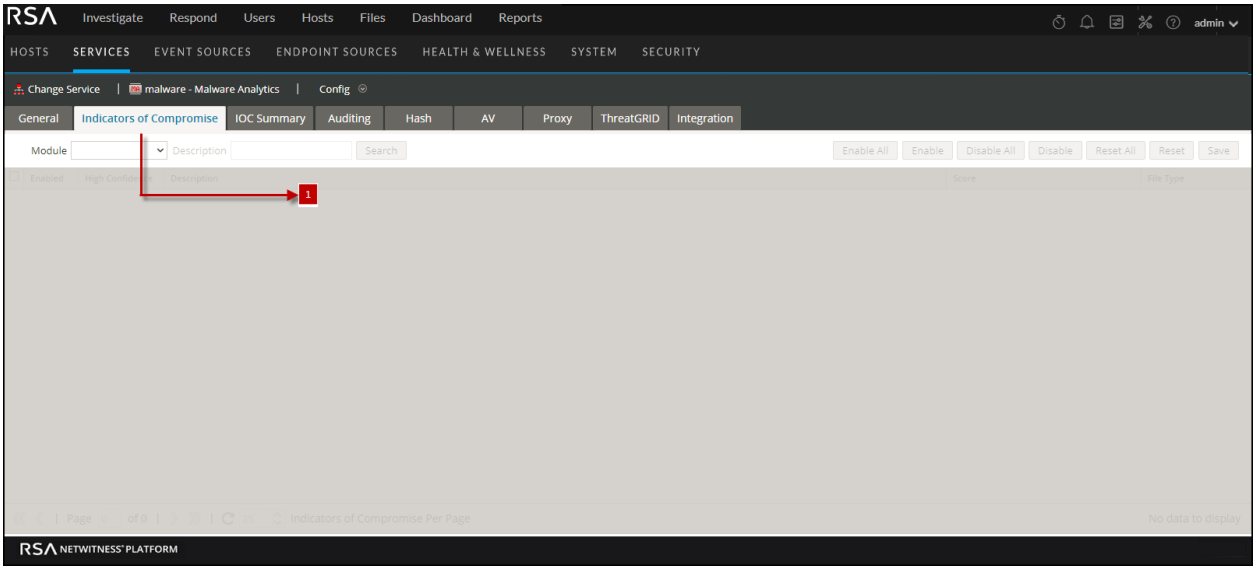
*You can perform this task in the current view

Related topic

Basic Setup

Quick Look

This is an example of the Indicators of Compromise tab.



1 Displays the Indicators of Compromise Tab.

Features

The Indicators of Compromise tab consists of a toolbar and page-able grid.

This table describes the features of the grid.

Feature	Description
Module selection list	Selects the scoring module for which you want to view the Indicators of Compromise: All, Network, Static, Community, Sandbox, or Yara.
Search field	Type text for which you are searching in the Description field.
Search option	Filters the grid to display only Descriptions that match the Description search term.
Enable All option	Click to enable all rules for the scoring module, as opposed to enabling all rules on the page using the checkbox.
Enable option	Click to enable selected rules.
Disable All option	Click to disable all rules for the scoring module, as opposed to disabling all rules on the page using the checkbox.
Disable option	Click to disable selected rules.

Feature	Description
Reset All option	Click to reset all rows on the page to their default values.
Reset option	Click to reset selected rows to their default values.
Save option	Click to save changes you made on this page. If you leave the page without saving, the changes are lost. The description of each row with unsaved changes has a red corner.

This table describes the features of the toolbar.

Column	Description
Selection checkbox	Checkboxes for selecting individual rows or all rows on the page.
Enabled checkbox	If the indicator of compromise is enabled, Malware Analysis uses the rule for scoring session data.
High Confidence checkbox	If checked, Malware Analysis treats the rule as one very likely to indicate the presence of malware, and an event that triggers that rule is marked in the results grid.
Description	Describes the Indicator of Compromise.
Score	Specifies the score that you want to factor in to the total score for any event that triggers the rule. The default score is displayed and you can raise or lower the score by dragging the slider or typing a number in the score box.
File Type	Displays the file types to which the rule applies. Possible values are **ALL**, **PDF**, **MS Office**, and **Windows PE**.

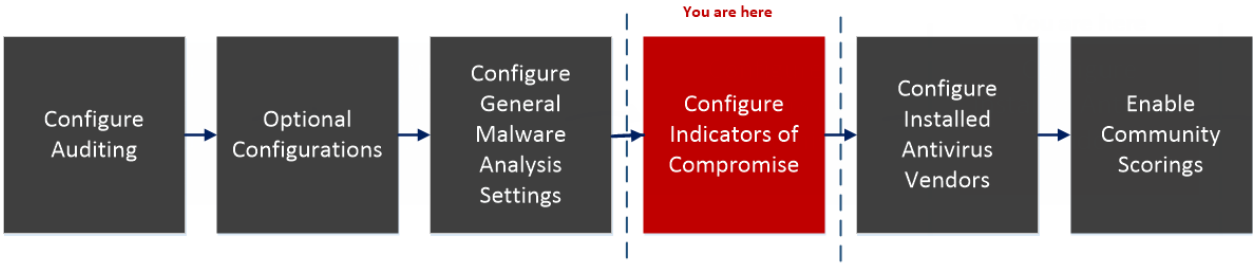
Services Config View - IOC Summary Tab

This topic introduces the features and functions available in the Service Config view > IOC Summary tab. This tab provides a way to view summary information for any IOC. A grid for each scoring module lists the configured IOCs along with statistics associated with that IOC of a specific range of time. The statistics include:

- The number of events for a network session or the number of files for a static, community, or sandbox event that were flagged with the IOC.
- The current score configured for the IOC in the Indicators of Compromise tab.
- The scores returned by each of the scoring modules.

When you select an event, you can show the Malware Events view or Malware Files view for the IOC. You can also open the selected IOC in the Indicators of Compromise tab to edit the Current Score.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise*	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings

Role	I Want to...	Show me how
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

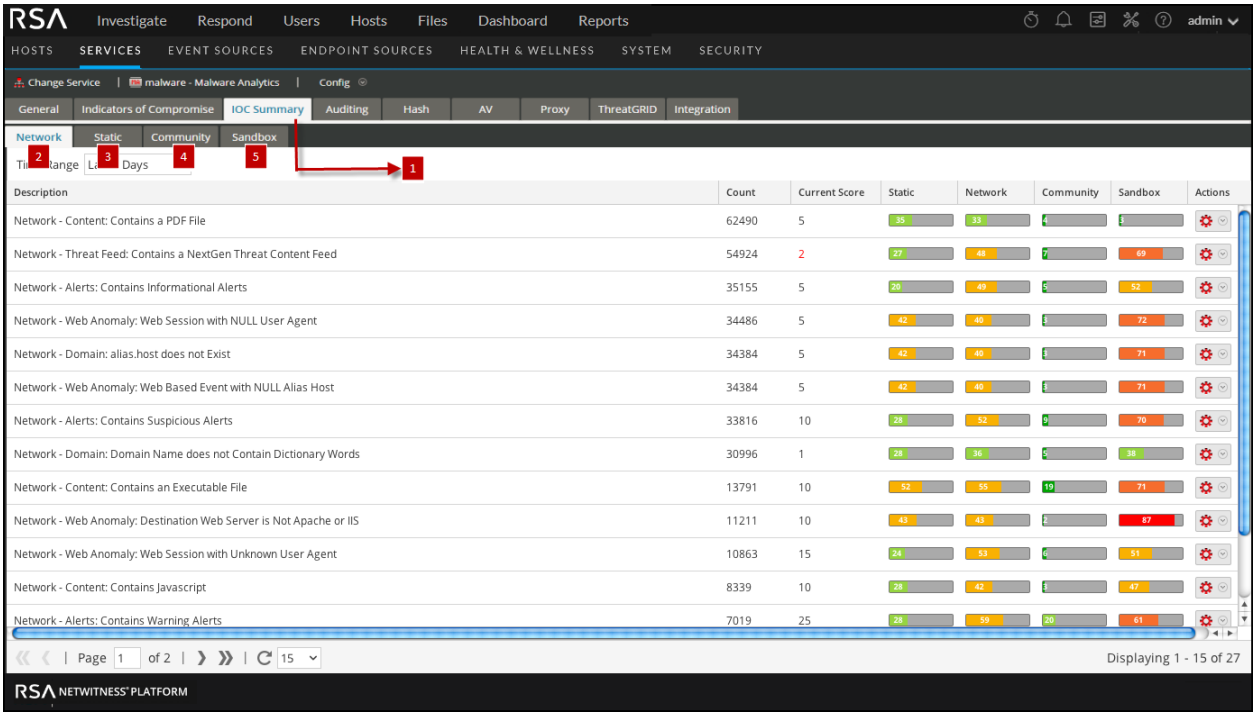
*You can perform this task in the current view

Related Topic

Basic Setup

Quick Look

This is an example of the IOC Summary tab for the Network scoring module.



1 Displays the IOC Summary Tab.
2 Displays the Network View.
3 Displays the Static View.
4 Displays the Community View.
5 Displays the Sandbox View.

Features

The IOC Summary consists of four tabs, one for each scoring module: Network, Static, Community, and Sandbox. Each tab has the same form and same information with a toolbar and page-able grid.

This table describes the features of each tab.

Feature	Description
Time Range	Selects the time range for the IOC Summary. Possible values are: Last 5 Minutes, Last 15 Minutes, Last 30 Minutes, Last Hour, Last 3 Hours, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 2 Days, Last 5 Days, Early Morning, Morning, Afternoon, Evening, All Day, Yesterday, This Week, Last Week, or Custom.
Description column	Lists the descriptions for the IOCs.
Count column	Lists the number of occurrences of the IOCs. In the Network tab, the count is the number of events in which the IOC was found. In the other tabs, the count is the number of files in which the IOC was found.
Current Score column	Lists the current score for the IOCs as configured in the Indicators of Compromise tab.
Static, Network, Community, and Sandbox columns	List the scores that each of the scoring modules gave the IOCs.
Actions drop-down	The Actions drop-down menu has two options: • Show Events/Files: opens the IOC in the Investigation Events view or Files view. This view can also be opened by double-clicking on the IOC. • Edit: opens the IOC in the Indicators of Compromise tab to edit the Current Score.

Services Config View - Auditing Tab

This topic introduces the features and functions of the Auditing tab in the Services Config view for Malware Analysis. The Auditing tab in the Services Config view for Malware Analysis provides a way to configure the auditing feature. Malware Analysis has an automated auditing system capable of sending alerts (syslog, snmp, audit log file entries) as Malware Analysis exceeds configured score value thresholds for each scoring module (Network, Static, Community, Sandbox). Malware Analysis can automatically feed any external system capable of ingesting the supported audit formats. One alert is generated for each file in an analyzed session that meets or exceeds the configure threshold.

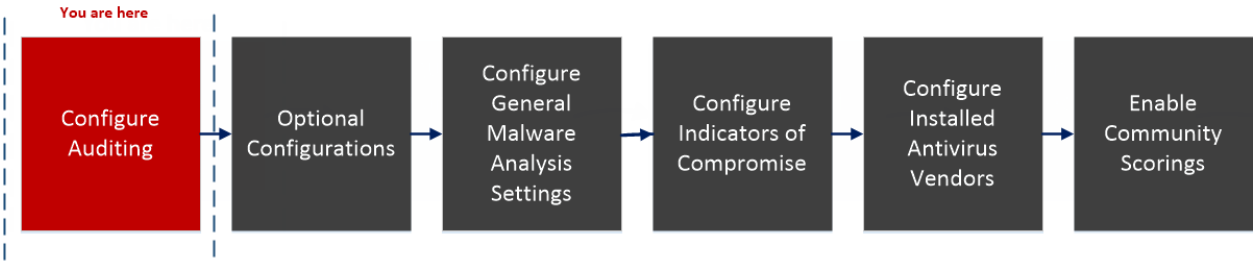
The audit log is a log file maintained on the Malware Analysis appliance for every significant event or action. Audit logs are rolled out and archived over time as they become large so an audit history is maintained. The size of these audit logs and their number are both configurable.

Some examples of events that are logged are:

- User login successes and failures
- Changes to system configuration settings
- Server restart
- Server version upgrade and install
- Suspicious events that exceed the Audit Thresholds

Malware Analysis can send audit events as an SNMP trap to a configured SNMP trap host, and consolidate logs in syslog format. Refer to the following task topic for detailed procedures: (Optional) Configure Auditing on Malware Analysis Host.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host*	(Optional) Configure Auditing on Malware Analysis Host

Role	I Want to...	Show me how
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

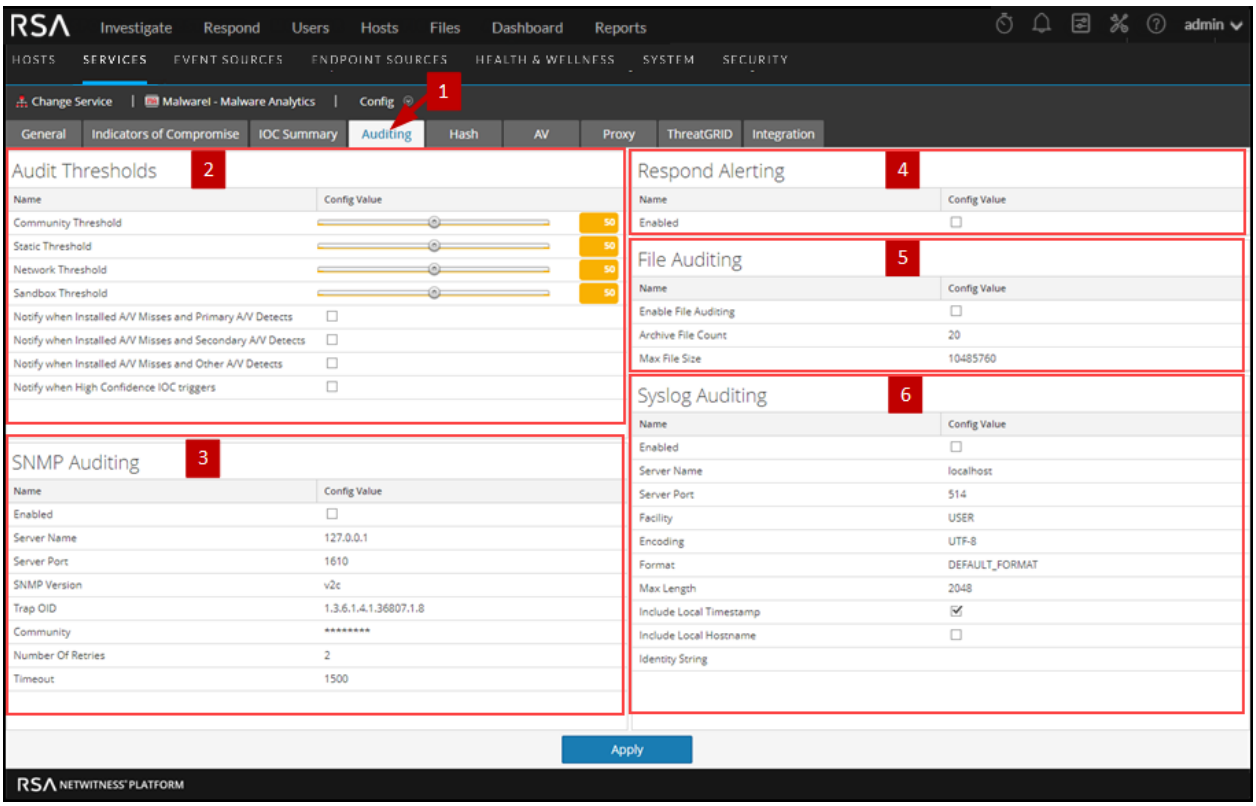
*You can perform this task in the current view

Related Topics

Basic Setup

Quick Look

This is an example of the Auditing tab.



1 Displays the Auditing Tab.
2 Displays the Audit Thresholds section.

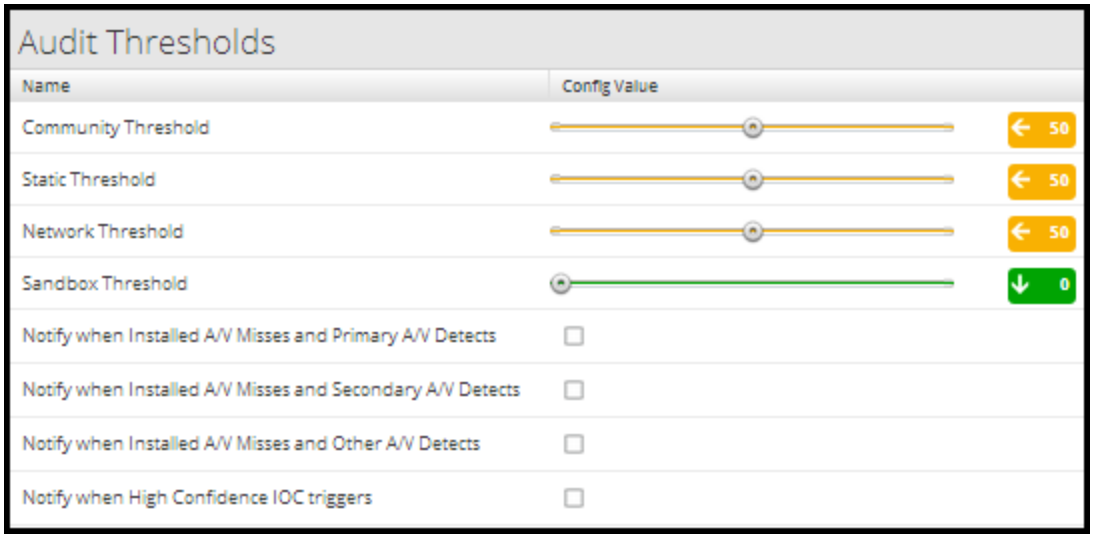
3 Displays the SNMP Auditing section.
4 Displays the Respond Alerting section.
5 Displays the File Auditing section.
6 Displays the Syslog Auditing section.

Features

The Auditing tab includes five sections and an Apply button used to save changes made in this tab and put them into effect.

- Auditing Thresholds
- SNMP Auditing
- Respond Alerting
- File Auditing
- Syslog Auditing

Audit Thresholds



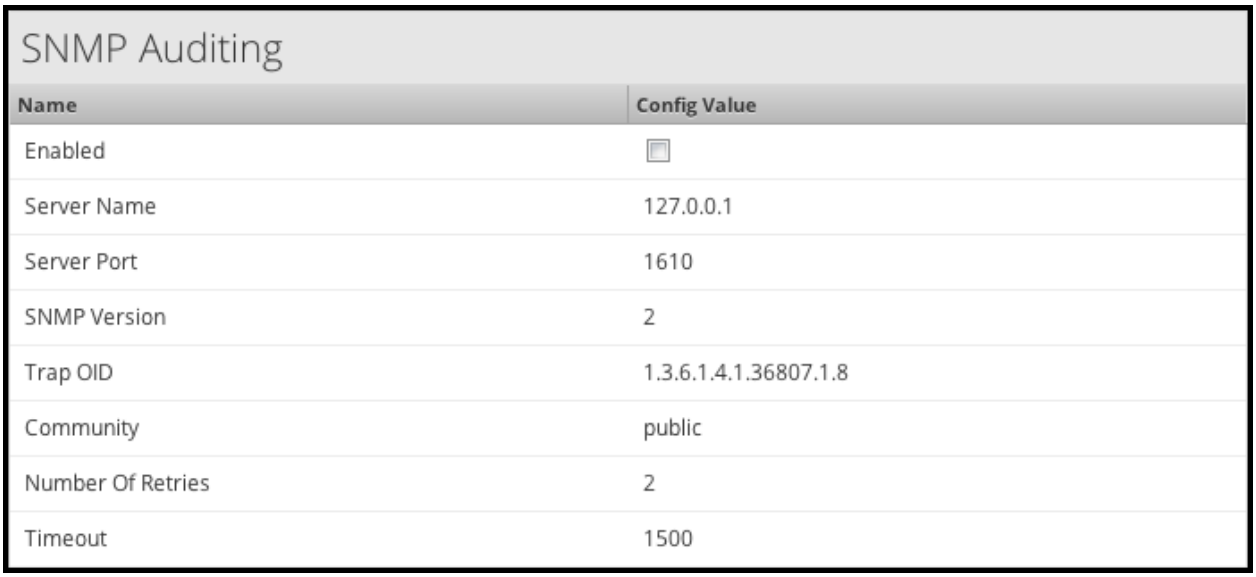
This table describes the features in the Audit Thresholds section.

Name	Config Value
Community, **Static**, **Network**, and **Sandbox Thresholds**	Malware Analysis scoring module thresholds for recording event information in a log file. Malware Analysis records the event information in a log file if the event scored high enough to satisfy all of the auditing thresholds. Each scoring category that completed analysis (for example, not all sessions invoke sandbox analysis) is compared against the configured audit threshold for that category. Any one of the category must exceed the threshold in order for an audit event to be triggered. An integer between 0 and 100 is a valid value. Setting these thresholds too low may cause a very large volume of audit events and notifications.

Name	Config Value
Notify when Installed A/V Misses and Primary A/V Detects	Records a message in a log file when installed antivirus software misses a virus and the primary antivirus software detects that virus. The recorded message is sent through all enabled auditing methods: SNMP, File, and Syslog. The default value is unchecked.
Notify when Installed A/V Misses and Secondary A/V Detects	Records a message in a log file when installed antivirus software misses a virus and the secondary antivirus software detects that virus. The recorded message is sent through all enabled auditing methods: SNMP, File, and Syslog. The default value is unchecked.
Notify when Installed A/V Misses and Other A/V Detects	Records a message in a log file when installed antivirus software misses a virus and the other antivirus software detects that virus. The recorded message is sent through all enabled auditing methods: SNMP, File, and Syslog. The default value is unchecked.
Notify when High Confidence IOC triggers	Records a message in a log file when a high confidence IOC (Indicators of Compromise) triggers. The recorded message is sent through all enabled auditing methods: SNMP, File, and Syslog. The default value is unchecked.

SNMP Auditing

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing services on IP networks. When SNMP auditing is enabled, Malware Analysis can send an audit event as an SNMP trap to a configured SNMP trap host.

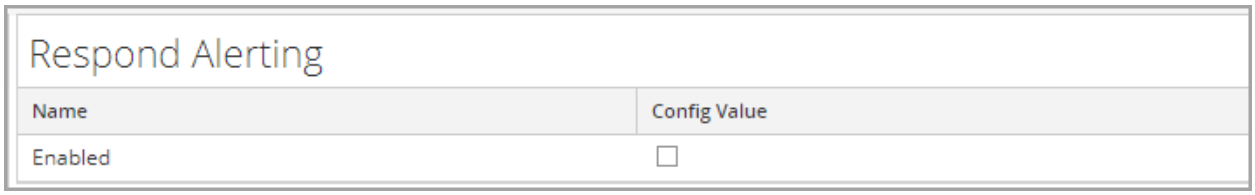


This table describes the features in the SNMP Auditing section.

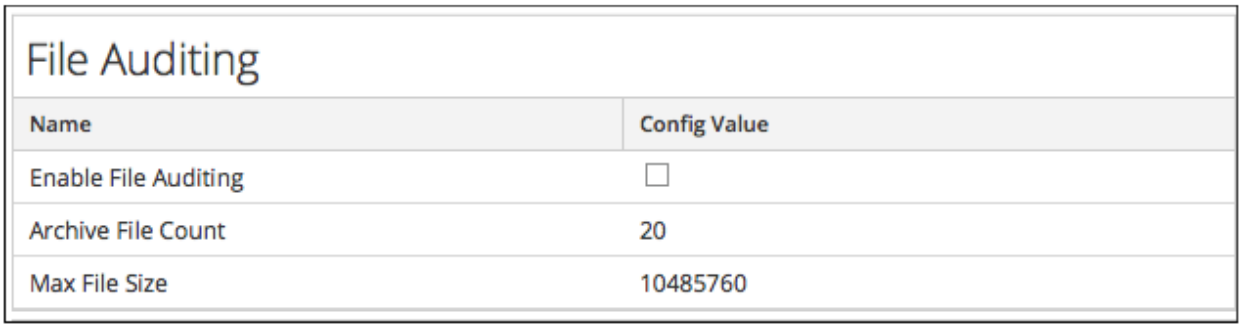
Name	Config Value
Enabled	Click to enable or disable SNMP auditing.
Server Name	The host where the target SNMP server is running.
Server Port	The port used where the SNMP trap receiver is listening.
SNMP Version	The version of the SNMP protocol to use when sending traps.
Trap OID	The object ID to use to identify the type of trap to send.
Community	The SNMP group to which Malware Analysis belongs.
Number Of Retries	The number of retries for sending a trap.
Timeout	The timeout period to wait for acknowledgment.

Respond Alerting

The Respond Alerting section enables NetWitness Respond to receive alerts from Malware Analysis. Select Enabled to forward alerts to the Respond view.



File Auditing

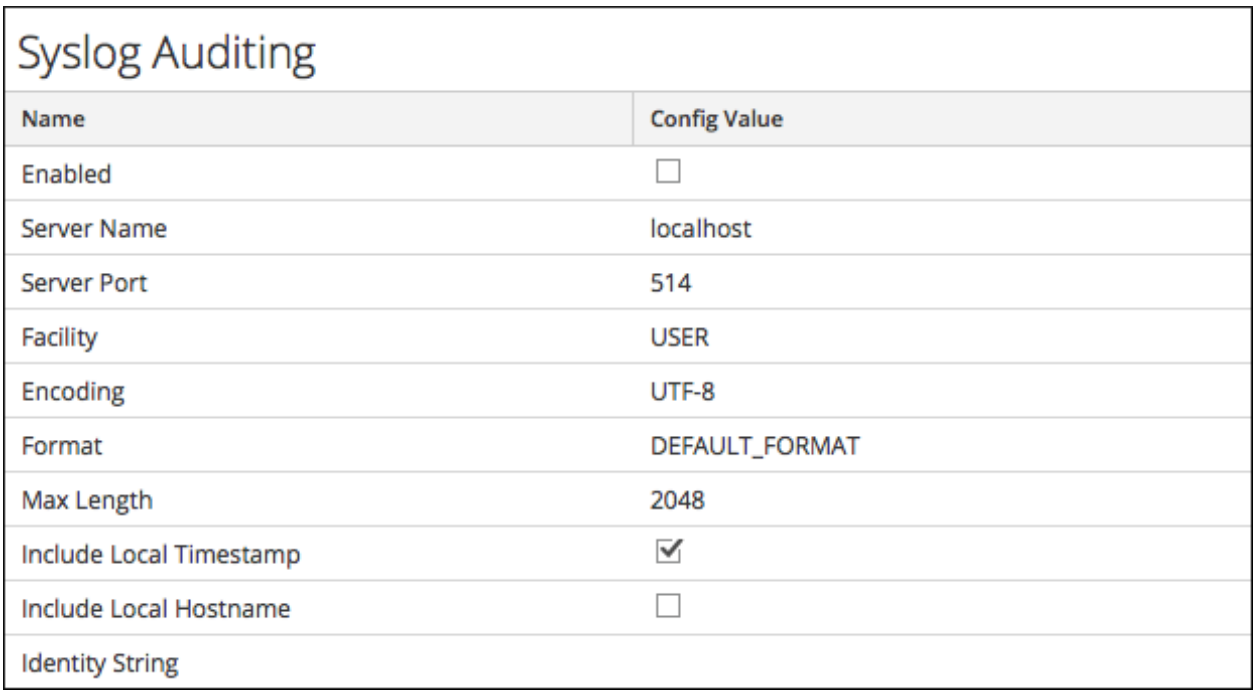


This table describes the features in the File Auditing section. Avoid setting the max file size and archive file count too high because it may have an adverse effect on the available disk space on the Malware Analysis appliance.

Name	Config Value
Enable File Auditing	Click to enable or disable file auditing.

Name	Config Value
Archive File Count	Malware Analysis keeps only as many log files as defined by this setting. When the maximum number is reached, the oldest log files are deleted and cannot be recovered. The default value is 20. Valid value: Integer between 1 and 50, inclusive.
Max File Size	The maximum file size for a single auditing log before it is archived. The default value is 10485760 bytes.

Syslog Auditing



This table describes the features in the Audit Thresholds section.

Feature	Description
Enabled	Click to enable or disable syslog auditing.
Server Name	This is the host where the target syslog process is running.
Server Port	This is the port where the target syslog process is listening.
Facility	This is the designated syslog facility to use for all outgoing messages. Possible values are KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, and LOCAL1 through LOCAL7.
Encoding	This is the encoding to use for text in syslog messages; for example, UTF-8.
Format	This is the desired message format. Possible values are: Default, PCI DSS, or SEC.

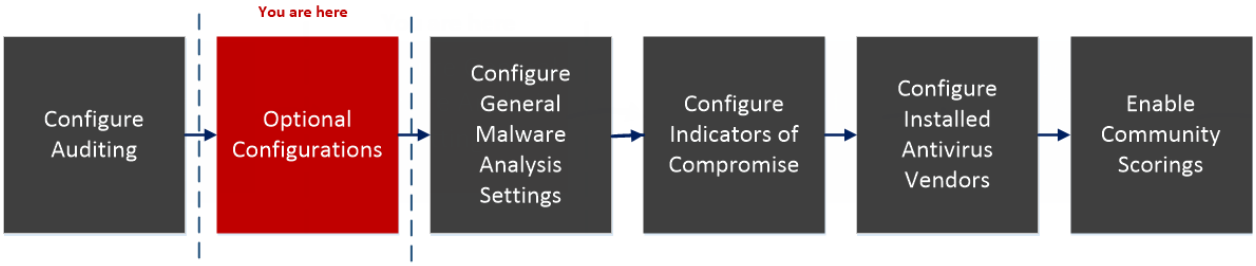
Feature	Description
Max Length	This is the maximum length in bytes that any syslog message can be. Default is 1024. Messages that exceed the maximum length are truncated.
Include Local Timestamp	Check this box to include the local timestamp in messages.
Include Local Hostname	Check this box to include the local hostname.
Identity String	This is an identity string to be prepended to each syslog alert. If the string is blank, no identity string is prepended to the outgoing syslog alerts. You can use this to identify the source of the alert. Users conventionally set it to the name of the program that will submit the messages to a syslog auditing.

Services Config View - Hash Tab

This topic introduces the features and functions available in the Service Config view > Hash tab for Malware Analysis.

In this tab, you can manage hash filtering in Malware Analysis. The hash grid is initially empty; the grid lists filters that have been added to Malware Analysis. In this view, you can add a hash filter, delete a hash filter, mark a hash filter as trusted or untrusted, and save changes.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter*	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

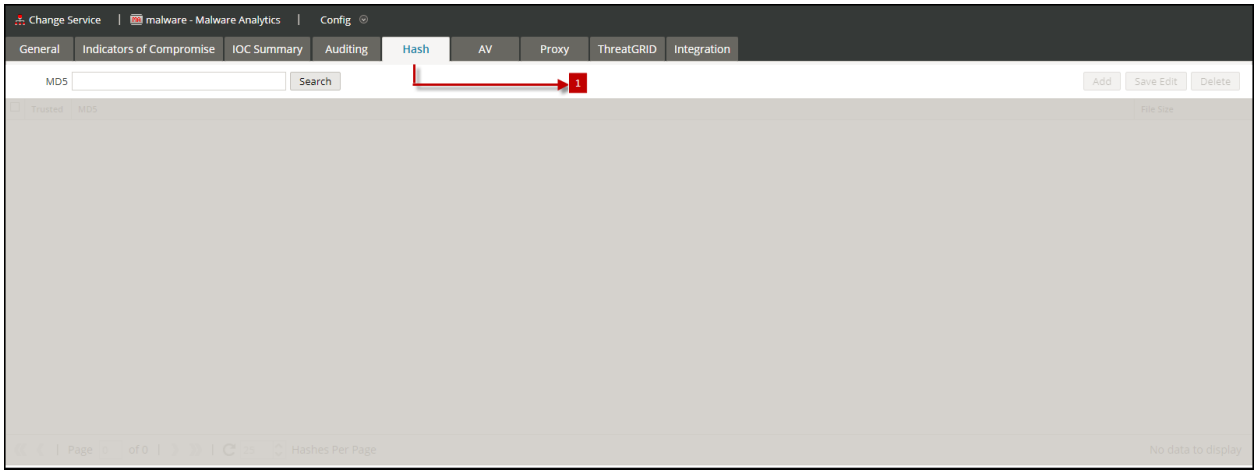
*You can perform this task in the current view

Related Topic

Basic Setup

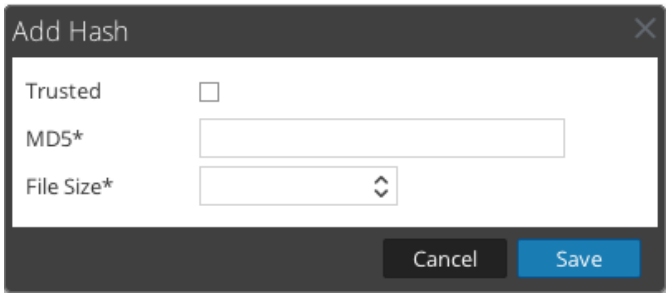
Quick Look

This is an example of the Hash tab.



1 Displays the Hash Tab.

This is an example of the Add Hash dialog.



Features

The **Hash** tab consists of a toolbar and a pageable hash grid.

This table describes the Hash tab toolbar.

Feature	Description
MD5 Search	Enter an MD5 hash for which you want to search the results in the grid. The search function is case-insensitive.
Add	Displays the Add Hash dialog in which you can add a new hash to the hash grid, specify whether the hash is trusted or not, and provide the hash file size.
Save Edit	Saves any additions or edits to hashes in the grid.
Delete	Deletes selected hashes from the grid.

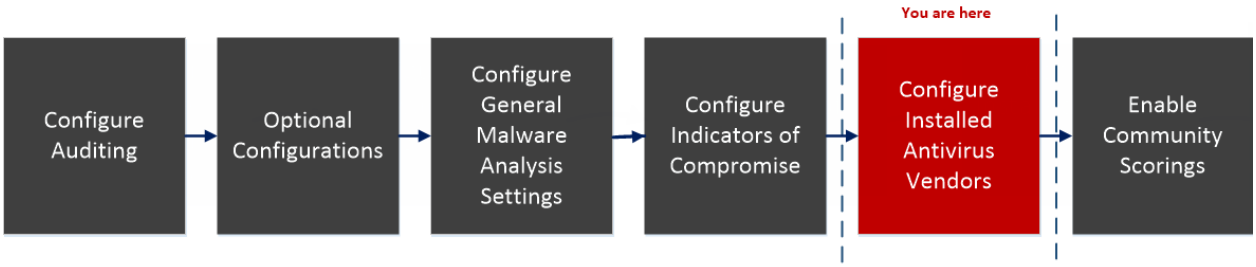
This table describes the Hash grid columns.

Feature	Description
Select Checkbox	Click to select a row. Click in the column header to select a header.
Trusted	Marks a hash as trusted or untrusted.
MD5	Identifies the MD5 hash.
File Size	Identifies the hash file size in kilobytes.

Services Config View - AV Tab

This topic introduces the features and functions of the AV tab in the Service Config view for a Malware Analysis service. The AV tab provides a way to identify the anti-virus software vendors whose software is in use on your network. NetWitness can include the results from these vendors in the detailed results view of an event that has been analyzed using Malware Analysis.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor*	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

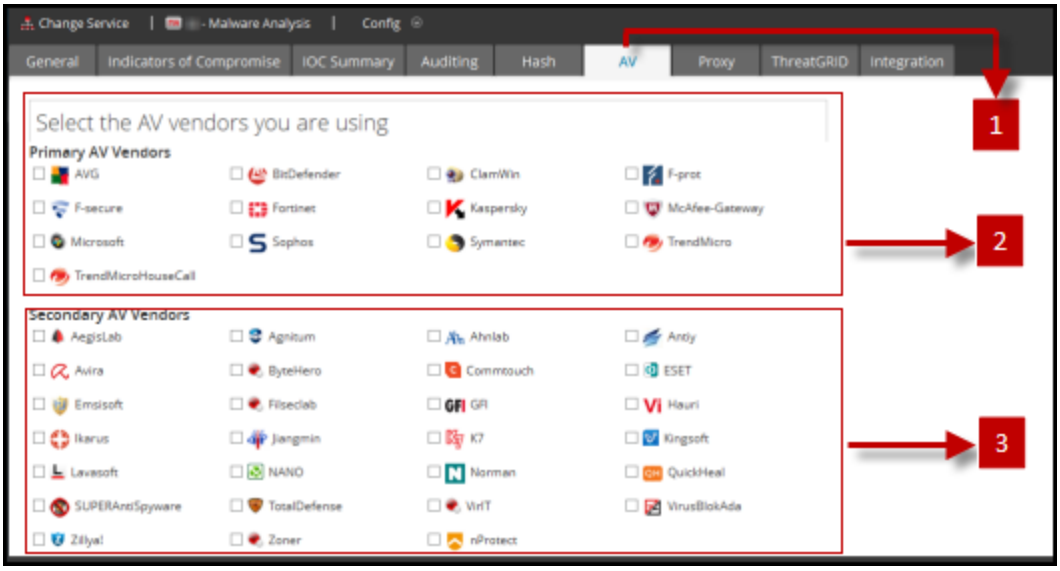
*You can perform this task in the current view

Related Topic

Configure Installed Antivirus Vendors

Quick Look

This is an example of the AV tab.



1 Displays the Av Tab.
2 Allows you to select the AV vendor that you are using.
3 Displays the Secondary AV vendors.

Features

The AV tab lists anti-virus vendors whose software may be installed in your network. There are two categories for vendors: Primary, which are the most trusted, and Secondary, which are less known. Each vendor name has a checkbox and an icon. Checking a vendor name indicates that you have installed the selected AV software from that vendor in your environment.

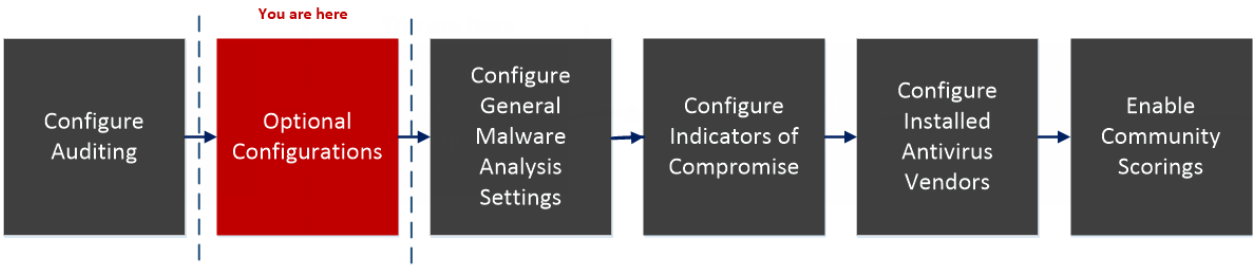
This table describes the options in the AV tab.

Feature	Description
Vendor Checkbox	Choose one or more Anti Virus vendors from the supplied list to indicate which products have been installed in the local organization.
Apply	Saves changes made in the AV tab.
Reset	Resets the AV list to the default state, which has no vendors selected.

Service Config View - Proxy Tab

This topic introduces the parameters configured in the Proxy tab in the Service Config view for a Malware Analysis service. This tab configures Malware Analysis communication via web proxy with the RSA Cloud for community analysis and with the sandbox service for sandbox analysis to preserve anonymity. If you are using a local sandbox service, communications via web proxy are unnecessary and may slow performance. When configuring the sandbox module in the **General** tab, you can choose to bypass the configured web proxy.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings*	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

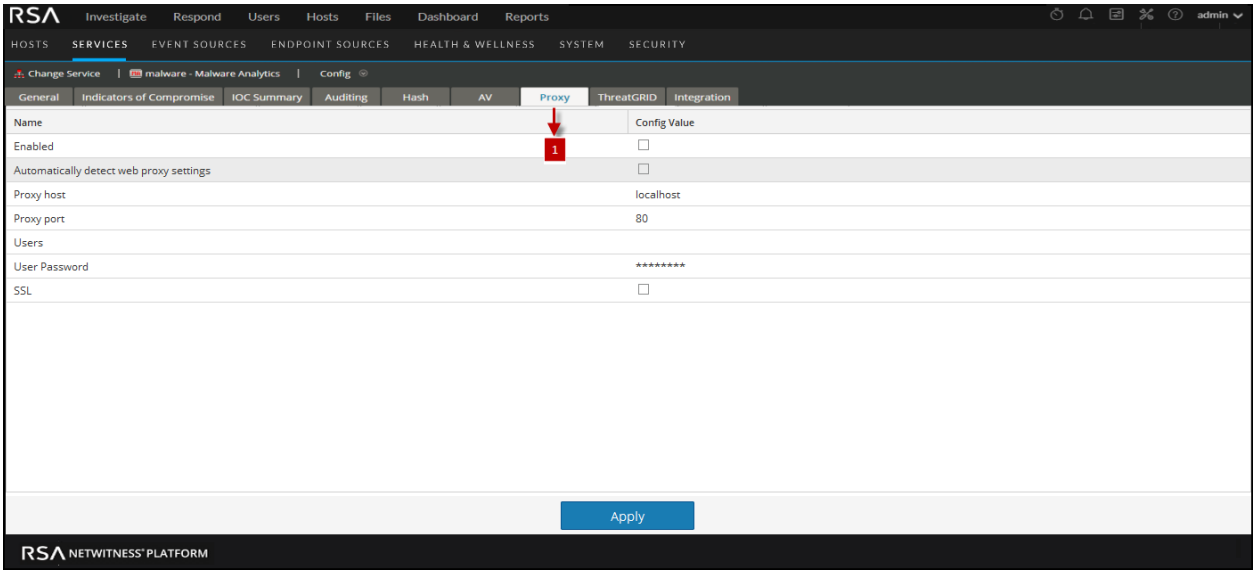
*You can perform this task in the current view

Related topic

Basic Setup

Quick Look

This is an example of the Proxy tab.



1 Displays the Proxy Tab.

Features

This table describes the features in the Proxy tab.

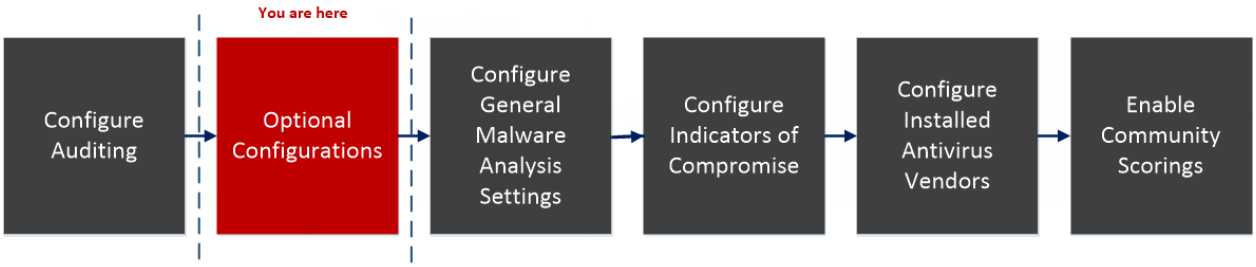
Feature	Description
Enabled	Select the checkbox to enable communication via web proxy with the RSA Cloud for community analysis and with the sandbox service for sandbox analysis to preserve anonymity.
Automatically detect web proxy settings	Select the checkbox to use settings configured in the System settings.
Proxy host	Enter the hostname for the proxy host.
Proxy port	Enter the port used for communication on the proxy host
Users	Enter the username used to log on to the proxy host.
User Password	Enter the user password used to log on to the proxy host.
SSL	(Optional) Select the checkbox to enable communication using SSL.
Apply button	Click the **Apply** button to submit chosen settings.

Services Config View - ThreatGRID Tab

This topic introduces the parameters required to obtain a trial ThreatGRID API key in the Malware Analysis **ThreatGRID** tab, which provides a method of obtaining a trial ThreatGRID API key for use in the ThreatGRID Cloud sandbox. Before enabling ThreatGRID as the sandbox service in the Sandbox module, a ThreatGRID-supplied Service Key must be configured so that ThreatGRID can recognize that samples submitted from this site are legitimate.

If you do not have a ThreatGRID-supplied Service Key, you can obtain a key using this tab. The key is provided on a trial basis.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key*	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis	Enable Community Analysis

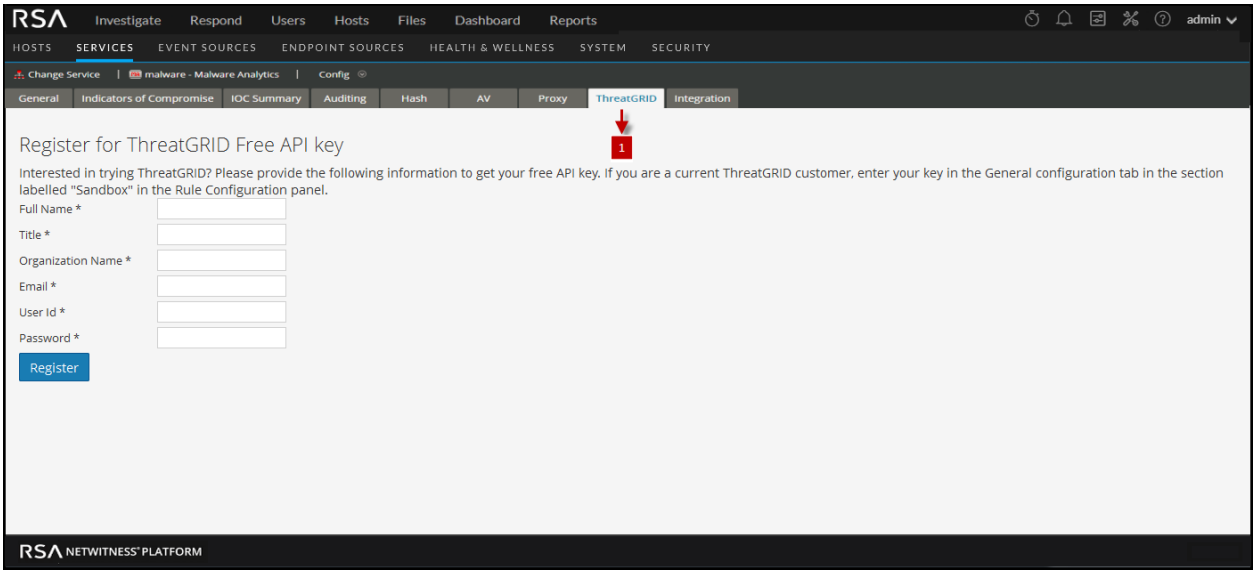
*You can perform this task in the current view

Related Topic

Basic Setup

Quick Look

This is an example of the ThreatGRID tab.



1 Displays the ThreadGRID Tab.

Features

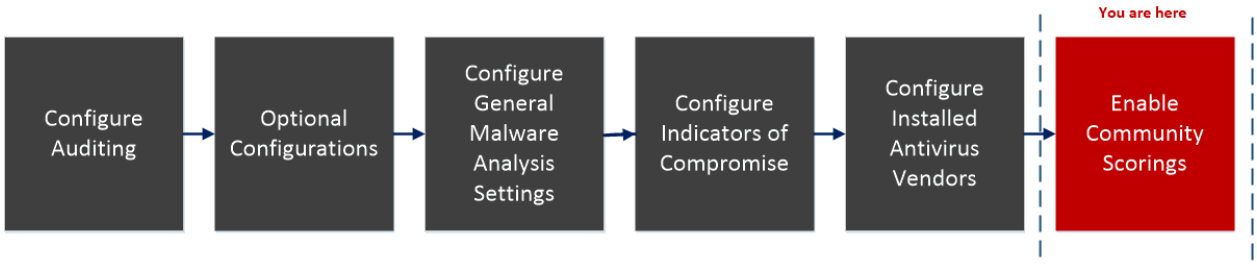
This table describes the features of the **ThreatGRID** tab.

Feature	Description
Full Name	Your first and last name.
Title	Your job title.
Organization Name	The name of your organization.
Email	Your email address.
User Id	Your user ID for ThreatGRID access.
Password	Your password for ThreatGRID access.
Register button	Click the **Register** button to submit the request.

Services Config View - Integration Tab

This topic introduces the features and functions of the Integration tab in the Administration Services Config view for Malware analysis. This tab provides a way to test connections and enable Community scoring by registering the Malware Analysis service. An administrator can test the connection to `cloud.netwitness.com` and to a core service that was configured for continuous scan.

Workflow



What do you want to do?

Role	I Want to...	Show me how
Administrator	Configure General Malware Analysis Settings	Configure General Malware Analysis Settings
Administrator	Configure Indicators of Compromise	Configure Indicators of Compromise
Administrator	Configure Auditing on Malware Analysis Host	(Optional) Configure Auditing on Malware Analysis Host
Administrator	Configure Hash Filter	(Optional) Configure Hash Filter
Administrator	Configure Installed Anti virus Vendor	Configure Installed Antivirus Vendors
Administrator	Configure Malware Analysis Proxy Settings	(Optional) Configure Malware Analysis Proxy Settings
Administrator	Register a TreadGRID API Key	(Optional) Register for a ThreatGRID API Key
Administrator	Enable Community Analysis*	Enable Community Analysis

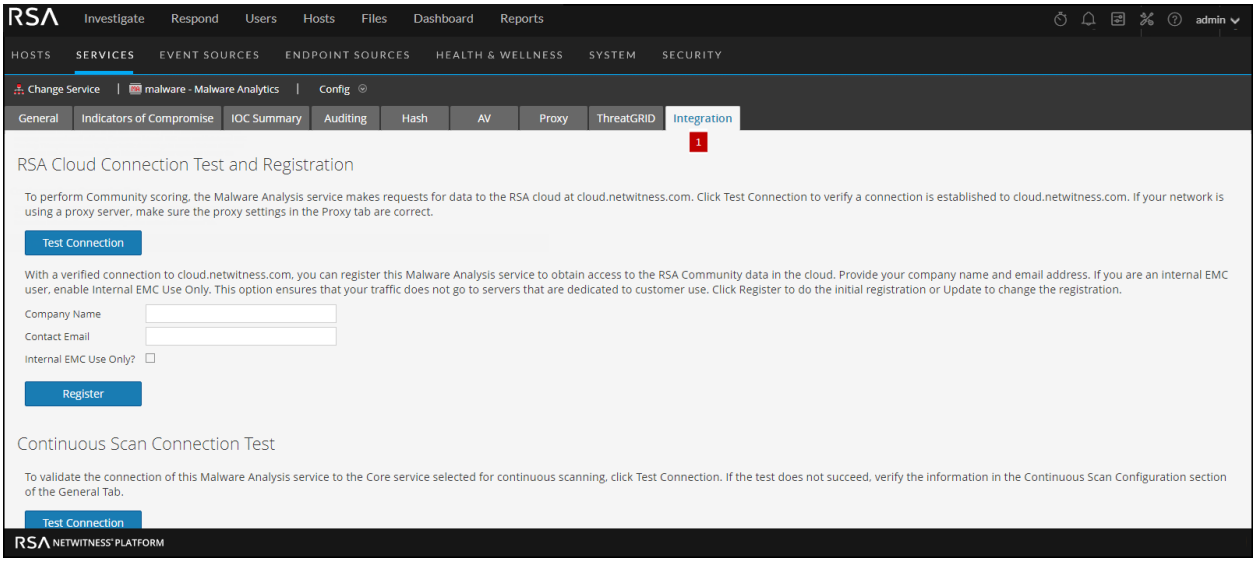
*You can perform this task in the current view

Related Topic

Basic Setup

Quick Look

The following figure is an example of the Integration tab.



1 Displays the Integration Tab.

Features

This tab has two sections: RSA Cloud Connection Test and Registration and Continuous Scan Connection Test. The following table describes the features.

Feature	Description
RSA Cloud Connection Test and Registration button	Clicking this button tests for an active connection to cloud.netwitness.com. NetWitness tests communications with the site and checks Proxy settings. A valid connection is required in order to register with the RSA Community Service.
Company Name	This is the name of your company. This is a required field.
Contact Email	This is the contact email. This is a required field.
Internal EMC Use Only Check box	This is an optional field. EMC customers, salespersons, or demo users should check this option to ensure that their requests do not use bandwidth on the production server. When the box is checked the following warning is displayed: `Checking this box may cause a less robust performance because the production server isn't being used.`
Register button	Clicking the Register button completes registration if all required fields are filled in. The Register button becomes the Update button after registration is complete.
Update button	The Update button is displayed after registration is complete.

Feature	Description
Continuous Scan Connection Test button	Clicking this button initiates a check to verify that the Malware Analysis service can connect to the Core service selected for continuous scanning (the Source Host, Source Port, Username, and User Password as specified in the General tab).