



NetWitness Endpoint User Guide

for RSA NetWitness® Platform 11.4



Copyright © 1994-2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledge base 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 <https://www.rsa.com/en-us/company/rsa-trademarks>.

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. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

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.

July 2020

Contents

Introduction	6
Endpoint Metadata	6
Risk Score	8
Severity of Alerts	10
Global and Local Risk Score	11
Automated Incident Creation Based on Risk Score	12
File Reputation	12
File Status	12
Remediation	13
Network Isolation	13
Focusing on Endpoint Analysis	14
Investigating Files	16
Best Practices	16
View Files	17
Filter Files	18
Add and Sort Columns in the Table	19
Analyze Files Using the Risk Score	20
Analyze Hosts with File Activity	22
Launch an External Lookup for a File	22
Set Files Preference	23
Export Global Files	24
Analyze Certificates	25
Change the Certificate Status	26
Filter Certificates	27
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	35
Scan Hosts	36
Analyze Hosts Using the Risk Score	37
Analyze Host Details	39
Filter Host Details	40
Search on Snapshots	40

Analyze Processes	41
Analyze Autoruns	43
Analyze Files	44
Analyze Libraries	44
Analyze Drivers	44
Analyze Anomalies	44
Analyze System Information	45
Export Host Details to JSON File	45
Launch an External Lookup for a File	45
Delete a Host	46
Deleting Hosts with Older Agent Versions	47
Set Hosts Preference	47
Export Host Attributes	48
Migrate Hosts	49
Analyzing Risky Users	49
Resetting Risk Score of Hosts	50
Investigating a Process	52
Best Practices	52
Analyze a Process	53
Analyze Events for a Process	57
Changing File Status or Remediate	59
Analyzing Downloaded Files	62
Download Files to Server	62
Save Downloaded Files	64
Analyze Downloaded Files	64
Performing Host Forensics	67
Download Master File Table	67
Analyze Downloaded MFT	69
System and Process Memory Dump	71
Filter Downloaded Files	73
Save Downloaded File	74
Delete Downloaded Files	75
Analyzing Events	77
Analyze Events from Files View	77
Analyze Events from Hosts View	77
Text Analysis for an Endpoint Event	78
Isolating Hosts from Network	80
Edit Exclusion List	82
Release Isolated Hosts	83

NetWitness Endpoint with Third-Party Antivirus Products	84
Troubleshooting NetWitness Endpoint	85
General Issues	85
Multi-server Issue	86
Hosts View Issues	86
Files View Issues	86
Policy Issue	87
Driver Issue	87
File Reputation Service Issue	87
Risk Scoring for Hosts or Files Issue	88
NetWitness Endpoint Reference Materials	90
Files View	91
File Details View	93
Hosts View	95
Hosts View - Details Tab	99
Hosts View - Process Tab	103
Process Details	107
Hosts View - Autoruns Tab	108
Hosts View - Files Tab	112
Hosts View - Drivers Tab	116
Hosts View - Libraries Tab	120
Hosts View - Anomalies Tab	124
Image Hooks	128
Kernel Hooks	128
Suspicious Threads	129
Registry Discrepancies	129
Hosts View - Downloads Tab	130
MFT Viewer	133
Hosts View - System Information Tab	136
System Information Panel	138

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	• 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. • Reports outbound and inbound network connections on all supported Windows platforms. • Reports IPv4 and IPv6 connections. • Console event (for Windows 8 and later) - User input that is entered into a console application, such as <code>cmd.exe</code>, <code>powershell.exe</code>, is captured and reported with the context <code>console.local</code>. Commands executed by <code>cmd.exe</code>, <code>powershell.exe</code> as a result of inter-process communication through anonymous pipes are captured and reported with the context <code>console.remote</code>. For example, <code>Get-Item -Path Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion</code>.
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	• Process event - Reports any process related activities, such as <code>openprocess</code>, <code>createprocess</code>, <code>openosprocess</code>, <code>openbrowserprocess</code>, <code>allocateremotememory</code>, <code>createremotethread</code>. • File event - Reports any file related activities by an executable, such as <code>writetoexecutable</code>, <code>renameexecutable</code>, <code>createautorun</code>, <code>deleteexecutable</code>, <code>selfdeleteexecutable</code>, <code>writetoplist</code>, <code>writetosudoers</code>, <code>createbrowserextension</code>. • Network event - TCP/UDP and incoming/outgoing. • 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

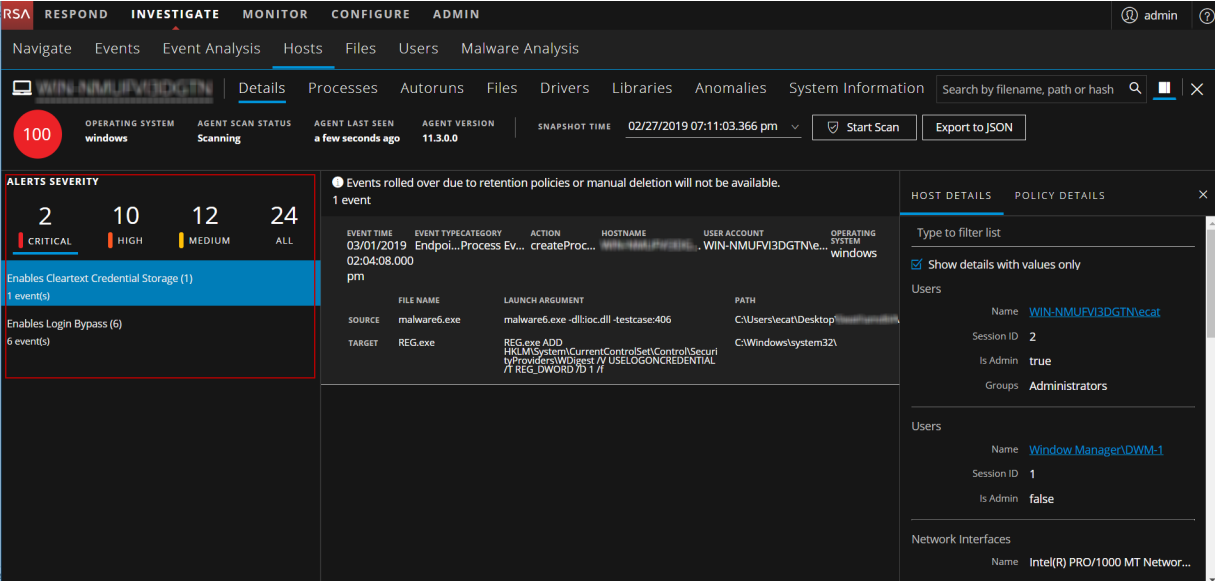
Analysts can use the risk score to begin an investigation on hosts and files. RSA uses a proprietary algorithm to calculate the risk scores ranging from 0 to 100. A subset of alerts associated with hosts and files contribute to the risk score calculation. Analysts can review critical and high alerts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

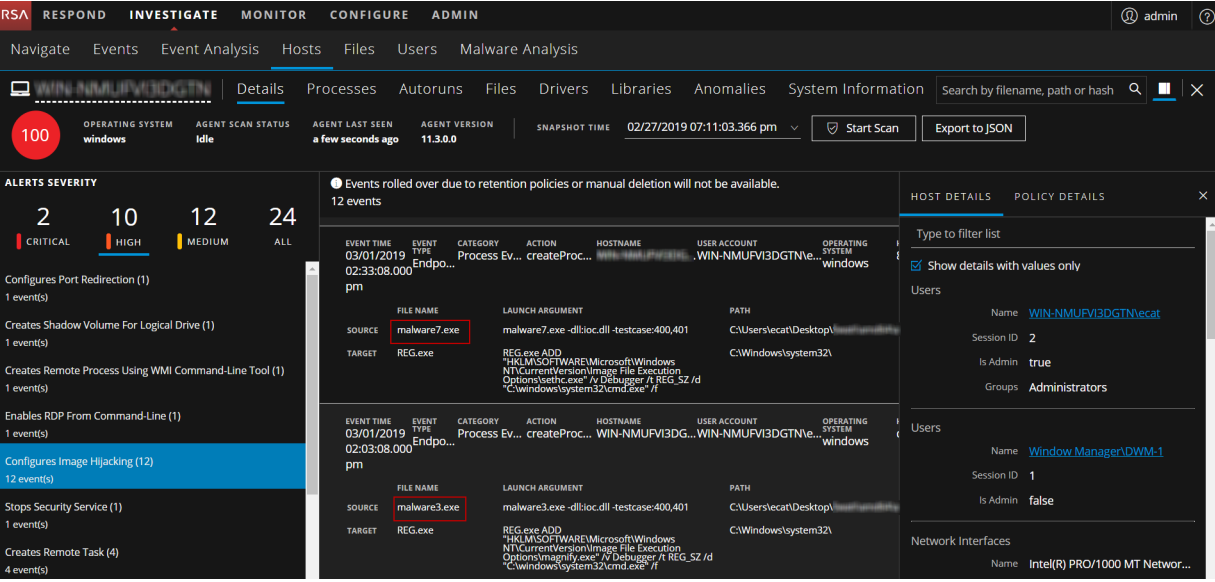
The following factors contribute to the risk score:

- **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 interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE (active), MONITOR, CONFIGURE, and ADMIN. Below this, a sub-navigation bar shows Navigate, Events, Event Analysis, Hosts, Files (active), Users, and Malware Analysis. The main content area shows details for a file named .MSProc. A risk score of 82 is highlighted in a red circle. The file is categorized as 'File' with a status of 'Neutral' and an operating system of 'mac'. The Alerts Severity section shows 0 Critical, 3 High, 4 Medium, and 7 All alerts. The Events section shows 3 events. The File Details panel on the right provides general information (FileName: .MSProc, Entropy: 6.631475448608398, Size: 12.0 KB, Format: macho), signature information (Features: unsigned), and hash data (MD5, SHA1, SHA256).

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*.

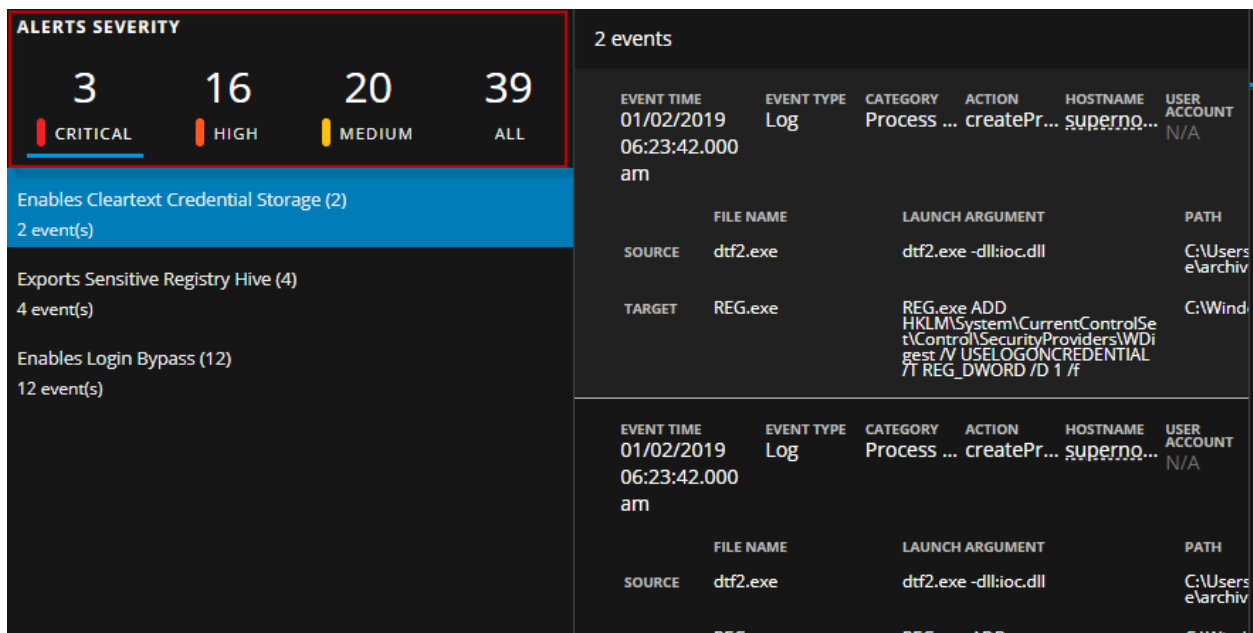
Note: For the accurate risk score calculation, the default multi-valued meta keys are required on the ESA Correlation service. For more information, see "Configure Meta Keys as Arrays in ESA Correlation Rule Values" section in the *ESA Configuration Guide*.

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
High	Orange	70-99
Medium	Yellow	31-69
Low	Green	0-30

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



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 > Events** 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.

For more information, see [Changing File Status or Remediate](#).

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. For more information, see [Changing File Status or Remediate](#).

Network Isolation

If you suspect that a host is potentially compromised with the threat still being active, you can isolate the host from the network and safely investigate possible threats within the host. By isolating the host, you can control the spread of an attack and analyze the malware behavior. When a host is isolated, only connection to the following IP addresses are allowed:

- Endpoint Server, Relay Server, DNS, DHCP, Gateways, 0.0.0.0, and 255.255.255.255.
- Other IP addresses that you include in the exclusion list.

In the isolated state, all events are reported to the Endpoint Server retaining full visibility into activities on the host. You can continue investigation by requesting scans, downloading MFT, files, and so on. The following metadata is added to the network events:

- network.isolated - indicates that the host is isolated.
- network.connectallowed - indicates that the network connection is allowed as the IP address is included in the exclusion list.
- network.connectblocked - indicates that the network connection is blocked.

Note: If the agent is enabled for log or file collection, make sure that you add the Log Decoder IP addresses in the exclusion list while you isolate the host.

For more information, see [Isolating Hosts from Network](#).

Focusing on Endpoint Analysis

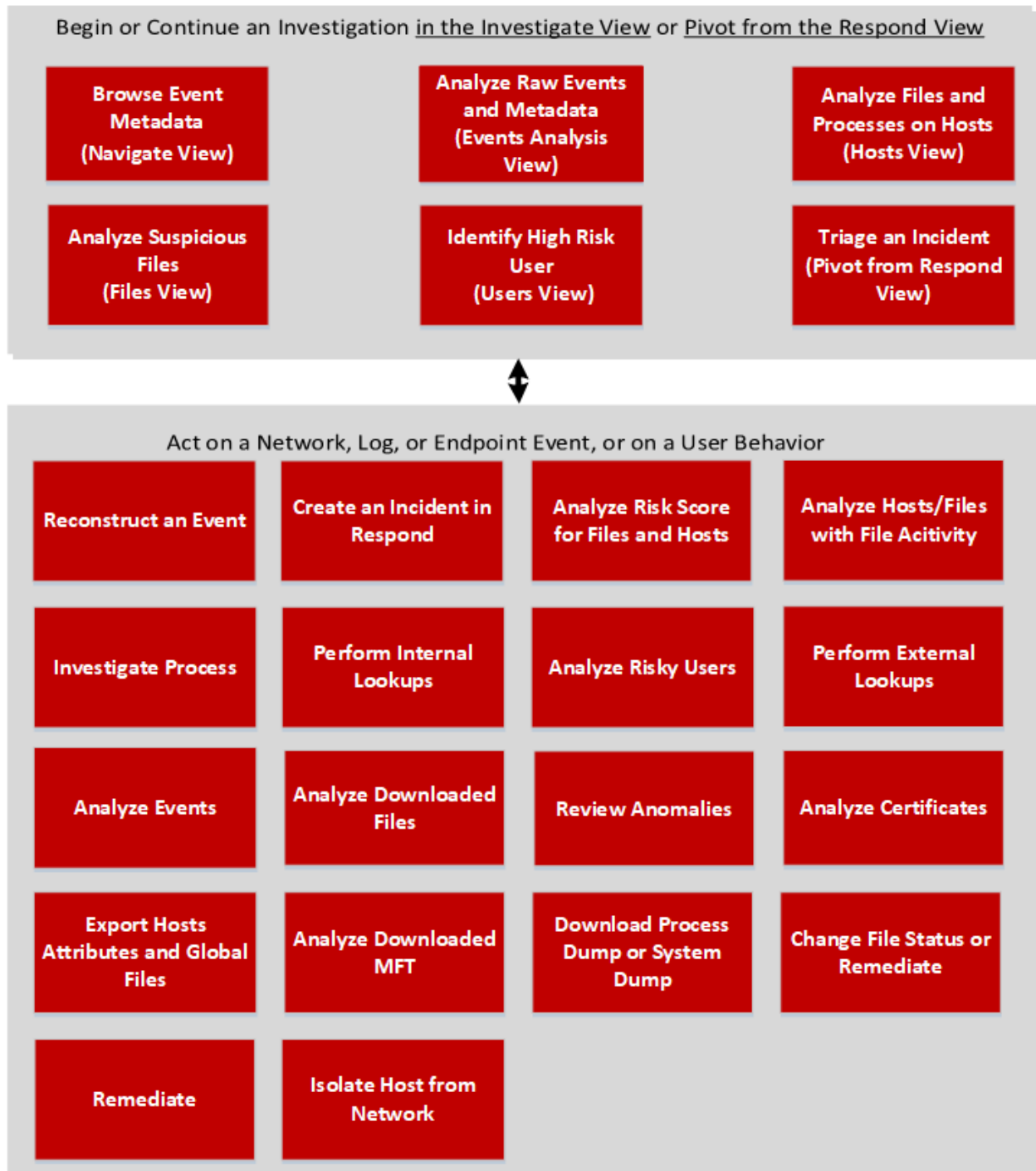
This guide provides the information needed to conduct an investigation that is focused on endpoint data from configured hosts. Analysts who conduct analysis using Investigate need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles 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.



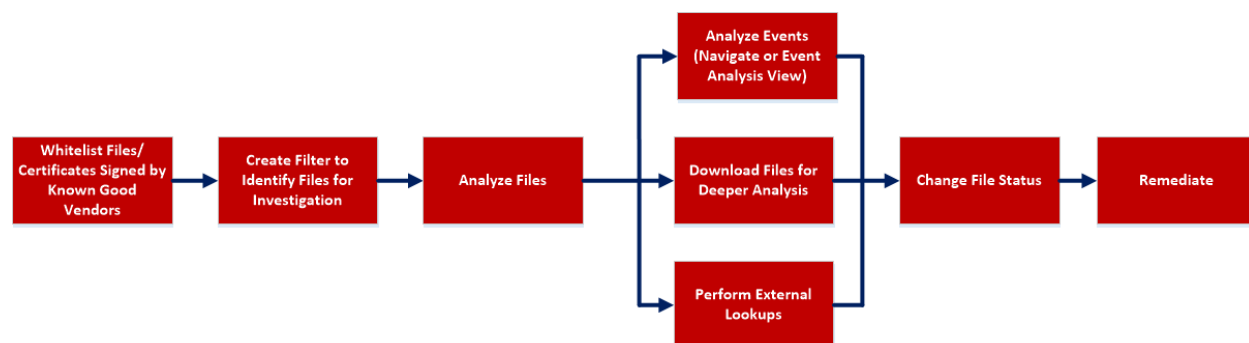
Investigating Files

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:
 - a. 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](#).
 - b. On Hosts - Indicates the number of hosts on which a file exist. If a file is present on fewer hosts with a high risk score, it may require further investigation. You can also sort or filter using On Hosts column to narrow down the search during investigation. For more information, see [Analyze Hosts with File Activity](#).

- c. File status - To manage suspected and legitimate files, analysts can use the file status to manage. For more information on the various file status, see [Changing File Status or Remediate](#).
 - d. Reputation status - Indicates the reputation of a file hash for analyst to narrow-down the files to investigate. For more information, see [File Reputation](#).
 - e. Signature - A valid signature on a file signed by a trusted vendor, such as Microsoft and Apple indicates that the file is not a risk. If a file is unsigned, it may be malicious, and needs investigation.
 - f. File name - Many trojans write random file names when dropping their payloads to prevent an easy search across the hosts in the network based on the filename. For example, 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.
- Investigate a particular file name or hash by pivoting to Navigate or Events view to view context, file activity on different hosts, and any file transfers across the network through packet data. For more information, see [Analyzing Events](#).
 - Download suspicious files to the server for deeper analysis. For more information, see [Analyzing Downloaded Files](#).
 - Change the status of the file (blacklist or graylist), and block an infected or malicious file. For more information, see [Changing File Status or Remediate](#).

View Files

You can view all files present on a specific Endpoint server or consolidated list of all files on multiple Endpoint servers using the Endpoint Broker for analysis. To view files:

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

FILE NAME	RISK SCORE	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE RESOURCES C...	FILE STATUS
endpointbroker - Endpoint Broker Server	100	11/08/2019 10:51:0...	1	--	230.5 KB	microsoft.signed.valid.ca...	Microsoft Corpor...	Neutral
endpointhybrid1 - Endpoint Server	100	11/08/2019 10:49:3...	1	--	295.5 KB	microsoft.signed.valid.ca...	Microsoft Corpor...	Neutral
endpointhybrid2 - Endpoint Server	100	11/06/2019 02:42:2...	1	--	337.0 KB	microsoft.signed.valid.ca...	Microsoft Corpor...	Neutral
cmd.exe	100	11/06/2019 02:41:3...	1	--	273.5 KB	microsoft.signed.valid.ca...	Microsoft Corpor...	Neutral
MRTx8620830.exe	70	11/17/2019 10:24:3...	1	--	121.0 MB	unsigned	--	Neutral
lsass.exe	70	11/11/2019 06:59:4...	1	--	56.7 KB	microsoft.signed.valid	Microsoft Corpor...	Neutral
Tskmgr.exe	70	11/10/2019 09:51:1...	1	--	1.0 MB	microsoft.signed.valid	Microsoft Corpor...	Neutral
lsass.exe	70	11/06/2019 02:42:4...	1	--	45.9 KB	microsoft.signed.valid	Microsoft Corpor...	Neutral
Tskmgr.exe	70	11/06/2019 02:41:5...	1	--	1.0 MB	microsoft.signed.valid	Microsoft Corpor...	Neutral
lsass.exe	70	11/06/2019 02:41:5...	1	--	56.7 KB	microsoft.signed.valid	Microsoft Corpor...	Neutral
gpmc.exe	23	11/08/2019 10:52:1...	1	--	83.5 KB	microsoft.signed.valid.ca...	Microsoft Corpor...	Neutral
MEMORY_DLL_2D8798FD04874DFC86D85	21	11/11/2019 12:31:4...	1	--	0 bytes	unsigned	Microsoft Corpor...	Neutral
MEMORY_DLL_9D302FB1E24E6FC439595A	21	11/11/2019 12:31:4...	1	--	0 bytes	unsigned	--	Neutral

- **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 shows the RSA NetWitness Investigate interface. The top navigation bar includes Respond, Investigate (selected), Monitor, Configure, and Admin. Below this is a sub-navigation bar with NAVIGATE, EVENTS, HOSTS, FILES (selected), ENTITIES, and MALWARE ANALYSIS. A filters section at the top of the main area includes 'Filters', 'endpointloghy...', 'View Certificates', 'Change File Status', 'Analyze Events', and 'More'. The main table lists files with columns: FILE NAME, RISK SCORE, FIRST SEEN TIME, ON HOSTS, REPUTATION, SIZE, SIGNATURE, PE RESOURCES C., and FILE STATUS. The file 'cmd.exe' is selected, and its details are shown on the right. The details panel includes 'FILE DETAILS', 'RISK DETAILS', and 'HOSTS' tabs. The 'FILE DETAILS' tab is active, showing general information (FileName: cmd.exe, Entropy: 6170039801599828, Size: 273.5 KB, Format: pe) and signature information (Features: microsoft_signed_valid.catalog, Timestamp: 03/19/2019 03:59:28.400 am, Thumbprint: 2e9c1ae54763822ee42474983..., Signer: Microsoft Windows).

FILE NAME	RISK SCORE	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE RESOURCES C.	FILE STATUS
cmd.exe	100	11/08/2019 10:51:0...	1	--	230.5 KB	microsoft_signed_valid.ca...	Microsoft Corpor...	Neutral
cmd.exe	100	11/08/2019 10:49:3...	1	--	295.3 KB	microsoft_signed_valid.ca...	Microsoft Corpor...	Neutral
cmd.exe	100	11/04/2019 02:42:2...	1	--	337.0 KB	microsoft_signed_valid.ca...	Microsoft Corpor...	Neutral
cmd.exe	100	11/04/2019 02:41:5...	1	--	273.5 KB	microsoft_signed_valid.ca...	Microsoft Corpor...	Neutral
MRTA8890830.exe	70	11/17/2019 10:24:5...	1	--	121.0 MB	unsigned	--	Neutral
lsass.exe	70	11/11/2019 06:59:4...	1	--	56.7 KB	microsoft_signed_valid	Microsoft Corpor...	Neutral
Taskmgr.exe	70	11/10/2019 09:51:1...	1	--	1.3 MB	microsoft_signed_valid	Microsoft Corpor...	Neutral
lsass.exe	70	11/04/2019 02:42:4...	1	--	45.9 KB	microsoft_signed_valid	Microsoft Corpor...	Neutral
Taskmgr.exe	70	11/04/2019 02:41:5...	1	--	1.0 MB	microsoft_signed_valid	Microsoft Corpor...	Neutral
lsass.exe	70	11/04/2019 02:41:5...	1	--	56.7 KB	microsoft_signed_valid	Microsoft Corpor...	Neutral
psimac.exe	30	11/08/2019 10:52:1...	1	--	83.5 KB	microsoft_signed_valid.ca...	Microsoft Corpor...	Neutral
MEMORY_DUMP_208708FDD48740FCB6D85...	21	11/11/2019 12:31:4...	1	--	0 bytes	unsigned	Microsoft Corpor...	Neutral

- **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 investigation by filtering files using file name, on hosts, 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, File Status, On Host, and Reputation Status.

The screenshot shows the RSA NetWitness Endpoint Investigate interface. The top navigation bar includes tabs for Respond, Investigate (selected), Monitor, Configure, and Admin. Below this is a secondary navigation bar with options: NAVIGATE, EVENTS, HOSTS, FILES (selected), ENTITIES, and MALWARE ANALYSIS. The main interface is divided into a left sidebar and a central table.

Filters Panel (Left Sidebar):

- SAVED FILTERS:** A section with a 'Select' dropdown.
- FILE NAME:** A section with a dropdown set to 'Equals' and a text input containing 'e.g., Filename.dll'.
- FILE STATUS:** A list of checkboxes: Neutral, Blacklist, Graylist, Whitelist.
- REMEDIATION:** A checkbox for Blocked.
- REPUTATION:** A list of checkboxes: Malicious, Suspicious, Unknown, Known, Known Good, Invalid.
- RISK SCORE:** A slider ranging from 0 to 100.
- ON HOSTS:** A section with 'Reset', 'Save', and 'Save as...' buttons.

Main Table:

FILE NAME	RISK SCORE	FIRST SEEN TIME	ON HOSTS	REPUTATION
cmd.exe	100	11/08/2019 10:51:0...	1	--
cmd.exe	100	11/08/2019 10:49:3...	1	--
cmd.exe	100	11/06/2019 02:42:2...	1	--
cmd.exe	100	11/06/2019 02:41:5...	1	--
MRT-K8890830.exe	70	11/17/2019 10:24:5...	1	--
lsass.exe	70	11/11/2019 06:59:4...	1	--
Taskmgr.exe	70	11/10/2019 09:51:1...	1	--
lsass.exe	70	11/06/2019 02:42:4...	1	--
Taskmgr.exe	70	11/06/2019 02:41:5...	1	--
lsass.exe	70	11/06/2019 02:41:5...	1	--
getmac.exe	33	11/08/2019 10:52:1...	1	--
[MEMORY_DLL_2D8708FDD4874DFCB4D85...	31	11/11/2019 12:31:4...	1	--
[MEMORY_DLL_9D305FB1E34E6FCA39695A...	31	11/11/2019 12:31:4...	1	--
[MEMORY_DLL_21DE82DB31853248346E4C...	31	11/08/2019 10:54:1...	1	--
[MEMORY_DLL_89AE00754A7475A6763C6E...	31	11/08/2019 10:54:1...	1	--
crypt32.dll	31	11/08/2019 10:52:1...	2	--
crypt32.dll	31	11/08/2019 10:52:1...	1	--
regsvr32.exe	31	11/08/2019 10:52:1...	1	--
wininit.exe	31	11/06/2019 02:42:4...	1	--

Showing 100 out of 10879 files | 1 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.

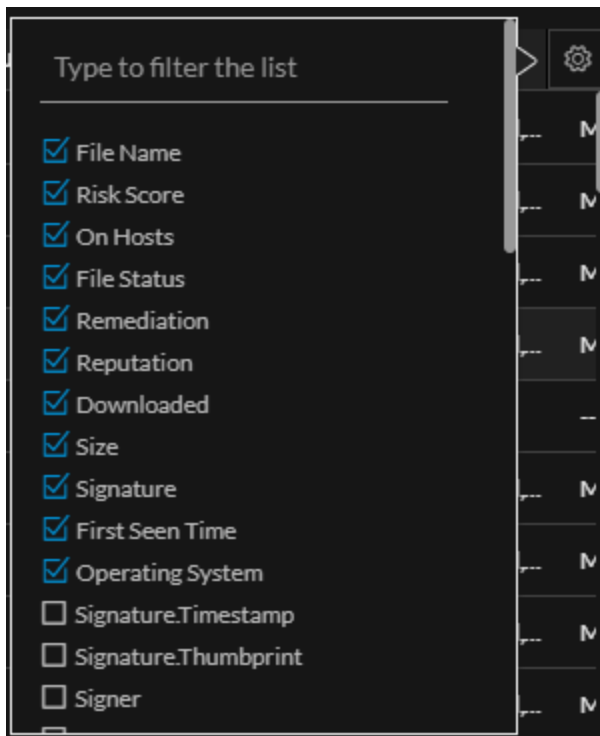
For example, to filter the files based on file reputation, select the reputation status in the Filter panel.

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.

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.

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

- 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 a file exist, do the following:

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

- In the **Investigate > Files** tab, click the row for the file you want to analyze.
- In the right panel, click the **Hosts** tab. The list of hosts along with the risk score are displayed.

FILE NAME	RISK SCORE	FIRST SEEN TL...	ON HOSTS	REPUTATION	SIZE	SIGNATURE
☒ cmd.exe	100	11/08/2019 10...	1	--	230...	microsoft,signed...
☐ cmd.exe	100	11/08/2019 10...	1	--	295...	microsoft,signed...
☐ cmd.exe	100	11/06/2019 02...	1	--	337...	microsoft,signed...
☐ cmd.exe	100	11/06/2019 02...	1	--	273...	microsoft,signed...
☐ MRT-KB890830.exe	70	11/17/2019 10...	1	--	121...	unsigned
☐ lsass.exe	70	11/11/2019 06...	1	--	56.7...	microsoft,signed...
☐ Taskmgr.exe	70	11/10/2019 09...	1	--	1.3 MB	microsoft,signed...

FILE DETAILS	RISK DETAILS	HOSTS
cmd.exe	Windows10	100

- Click the host name to open the host details.
- Click  to analyze events on the host in the Events 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:

- Go to **INVESTIGATE > Files**.
- 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.
- Select one or more files, and right-click or in the **More** drop-down list in the toolbar, do the

following:

FILE NAME	RISK SCORE	FIRST SEEN TI...	ON HOSTS	REPUTATION	SIZE	SIGNATURE
ntoskrnl.exe	0	11/06/2019 02...	2	—	9.5 MB	microsoft.signed...
smss.exe	0	11/06/2019 02...	2	—	143...	microsoft.signed...
wininit.exe	0	11/06/2019 02...	2	—	362...	microsoft.signed...
services.exe	—	—	—	—	659...	microsoft.signed...
svchost.exe	—	—	—	—	525...	microsoft.signed...
winlogon.exe	—	—	—	—	825...	microsoft.signed...
fontdrvhost.exe	—	—	—	—	802...	microsoft.signed...
dwm.exe	—	11/06/2019 02...	2	—	69.5...	microsoft.signed...
spoolsv.exe	—	11/06/2019 02...	2	—	747...	microsoft.signed...
ymtoolsd.exe	—	11/06/2019 02...	3	—	81.5...	signed.valid
VGAAuthService.exe	0	11/06/2019 02...	3	—	160...	unsigned

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

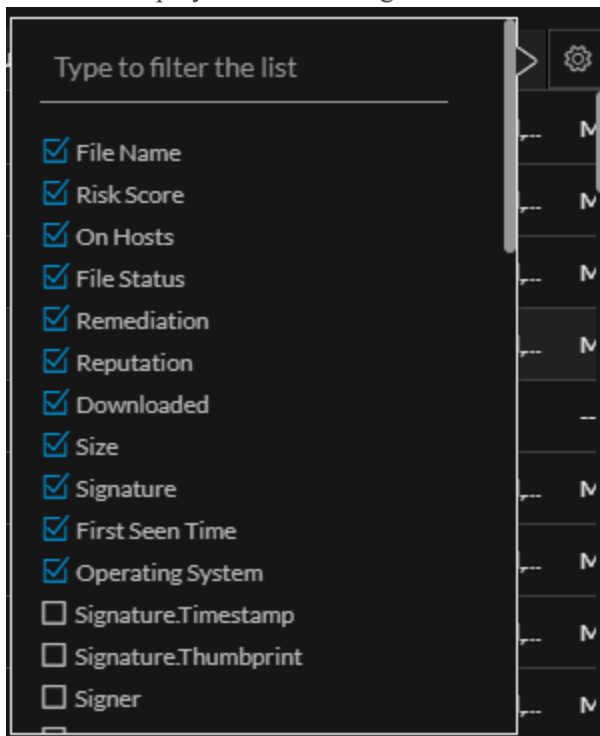
Note: To open files in multiple tabs, make sure you enable the pops-up in the browser.

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:

- 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.

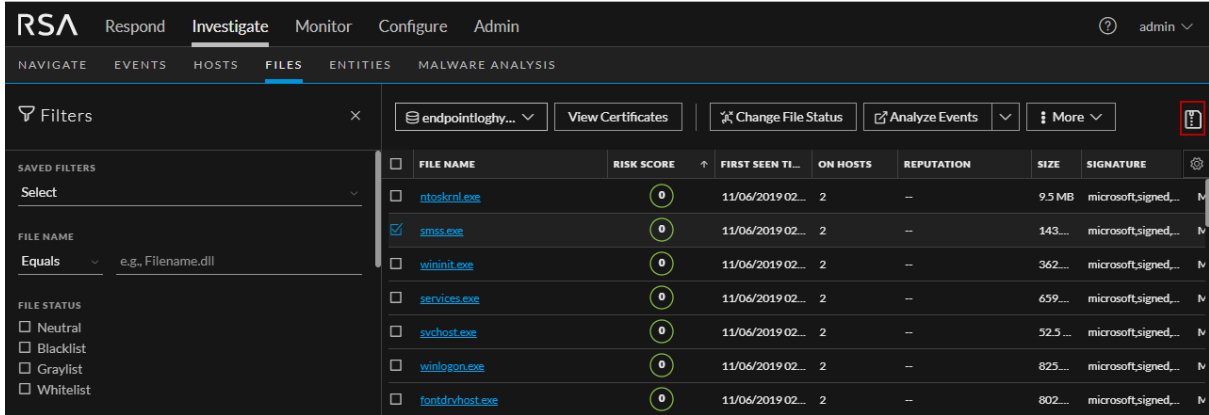
Export Global Files

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.



You can either save or open the CSV file.

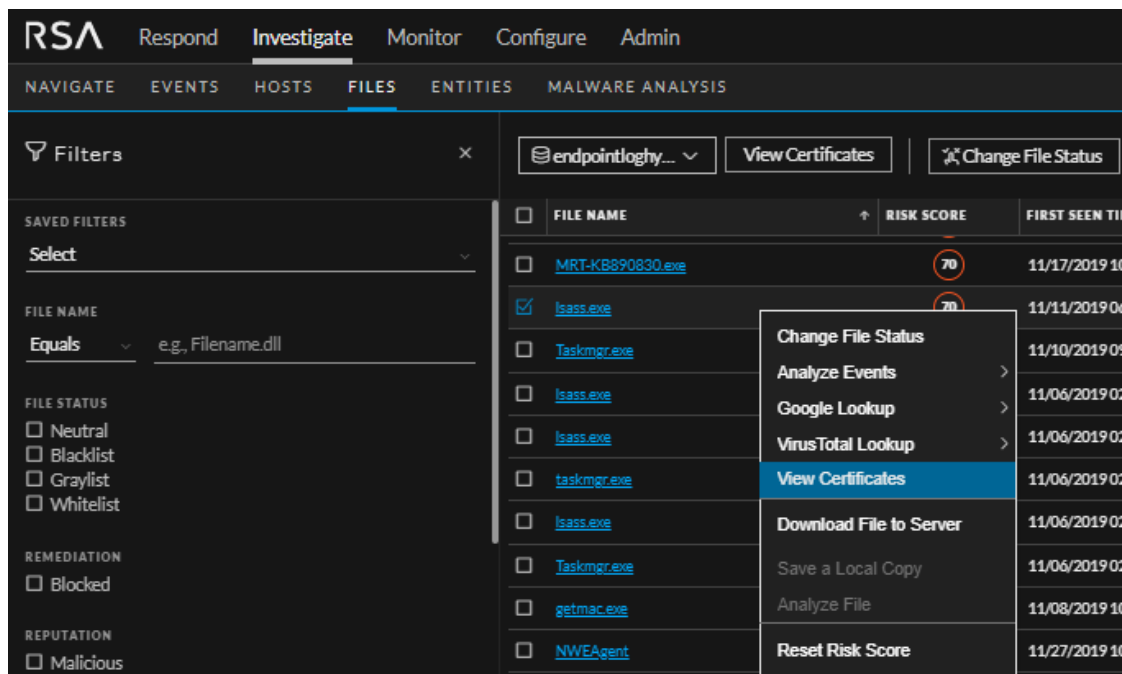
Analyze Certificates

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:



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

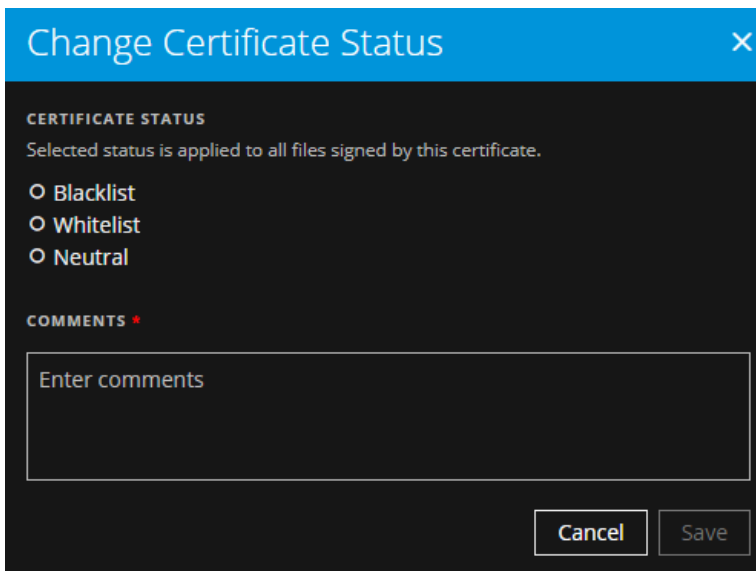
Change the Certificate Status

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 title bar is blue with the text 'Change Certificate Status' and a close button (X). The main area has a dark background. Under the heading 'CERTIFICATE STATUS', there is a note: 'Selected status is applied to all files signed by this certificate.' Below this are three radio button options: 'Blacklist', 'Whitelist', and 'Neutral'. Under the heading 'COMMENTS', there is a text input field with the placeholder text 'Enter comments'. At the bottom right are two buttons: 'Cancel' and 'Save'.

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.

The screenshot shows the RSA NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this is a secondary navigation bar with 'NAVIGATE', 'EVENTS', 'HOSTS', 'FILES' (selected), 'ENTITIES', and 'MALWARE ANALYSIS'. The main area is divided into a left sidebar and a right pane. The sidebar contains a 'Filters' panel with sections for 'SAVED FILTERS' (a 'Select' dropdown), 'STATUS' (checkboxes for Neutral, Whitelisted, Blacklisted), 'SIGNATURE' (checkbox for 'Is Root Microsoft'), and 'FRIENDLY NAME' (a dropdown set to 'Equals' with an 'Enter Value' field). Below these are 'THUMB PRINT' and 'FRIENDLY NAME' sections, each with a dropdown set to 'Equals' and a text input field. The right pane shows a table of certificates with columns: 'FRIENDLY NAME', 'STATUS', 'ISSUER', 'THUMB PRINT', and 'NOT VALID BEFORE UTCDA'. One certificate is listed: 'Microsoft Windows Pu...' with status 'Neutral', issuer 'C=US, S=Washington, L=Redmond...', thumb print '99922da31f07a02edb07cd8b60a...', and not valid before '2018-06-06T18:57:34.000+0000'. At the bottom of the sidebar are 'Reset', 'Save', and 'Save as...' buttons. At the bottom of the right pane, it says 'Showing 1 out of 1 certificates | 1 selected'.

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 RSA NetWitness Endpoint Investigate Files tab. The interface includes a top navigation bar with tabs: Respond, Investigate (selected), Monitor, Configure, and Admin. Below this is a sub-navigation bar with: NAVIGATE, EVENTS, HOSTS, FILES (selected), ENTITIES, and MALWARE ANALYSIS. A left sidebar contains a 'Filters' section with 'SAVED FILTERS' (Select), 'FILE NAME' (Equals, e.g., Filename.dll), 'FILE STATUS' (Neutral, Blacklist, Graylist, Whitelist), 'REMEDATION' (Blocked), and 'REPUTATION' (Malicious, Suspicious, Unknown). The main area displays a table of files with columns: FILE NAME, RISK SCORE, FIRST SEEN TI..., ON HOSTS, REPUTATION, SIZE, and SIGNATURE. A context menu is open for the file 'services.exe', 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). The bottom status bar indicates 'Showing 100 out of 10915 files | 1 selected'.

FILE NAME	RISK SCORE	FIRST SEEN TI...	ON HOSTS	REPUTATION	SIZE	SIGNATURE
ntoskrnl.exe	0	11/06/2019 02...	2	--	9.5 MB	microsoft,signed...
smss.exe	0	11/06/2019 02...	2	--	143...	microsoft,signed...
wininit.exe	0	11/06/2019 02...	2	--	362...	microsoft,signed...
services.exe	0	11/06/2019 02...	2	--	659...	microsoft,signed...
svchost.exe	0	11/06/2019 02...	2	--	525...	microsoft,signed...
winlogon.exe	0	11/06/2019 02...	2	--	825...	microsoft,signed...
fontdrvhost.exe	0	11/06/2019 02...	2	--	802...	microsoft,signed...
dwm.exe	0	11/06/2019 02...	2	--	695...	microsoft,signed...
spoolsv.exe	0	11/06/2019 02...	2	--	747...	microsoft,signed...
vmtoolsd.exe	0	11/06/2019 02...	3	--	815...	signed,valid
VGAuthService.exe	0	11/06/2019 02...	3	--	160...	unsigned
ManagementAgentHost.exe	0	11/06/2019 02...	3	--	595...	unsigned

- 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.

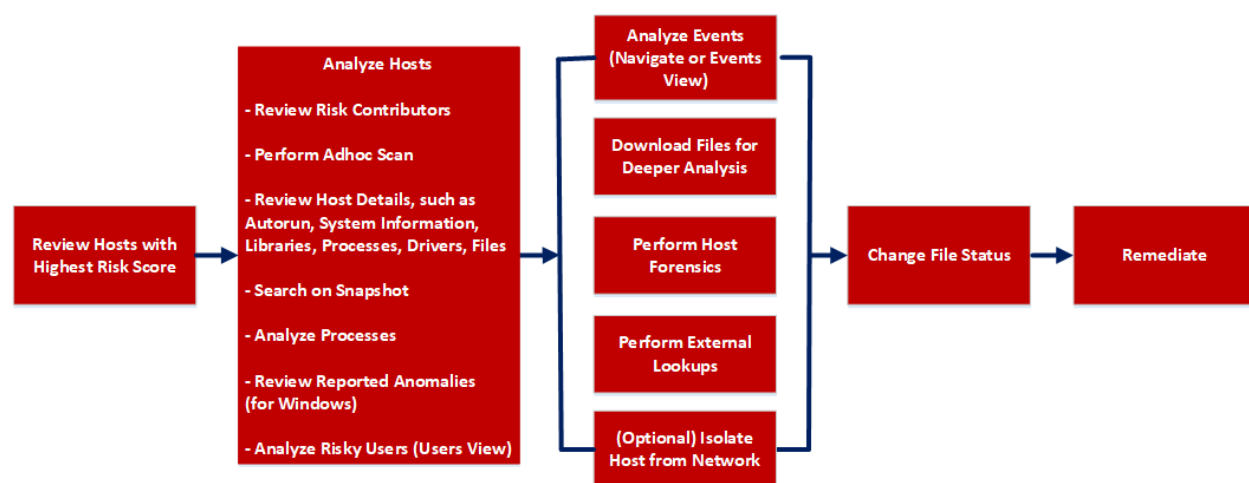
Investigating Hosts

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 Events view. For more information, see [Analyzing Events](#).
- Review hosts for rare files in the **On Hosts** column. If a file is present on 100 hosts, it can be legitimate. If a file is present on fewer hosts with a high risk score, it may be malicious and needs further investigation.
- Filter to exclude hosts on host status, risk score, hostname, and so on. For more information, see [Filter Hosts](#).
- Search Google or VirusTotal with the file hash and review any reported activities. For more information, see [Launch an External Lookup for a File](#).

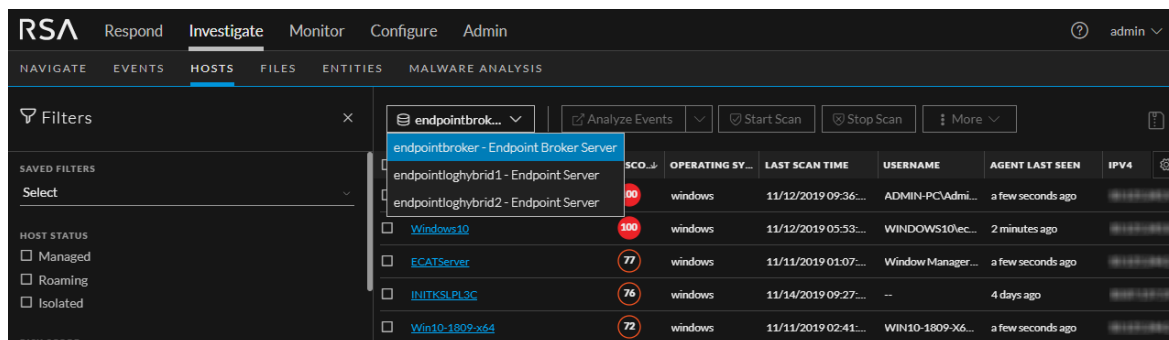
- Review the processes, autoruns, files, libraries, drivers, and system information. For example,
 - Search for files in known malware locations. For example,
 - C:\Windows\.
 - C:\Users\<name>\AppData\<uncommon folder>.
 - C:\Users\<name>\AppData\Local\Temp.
 - C:\Windows\Temp\.
 - Search for a particular 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](#).
- Download MFT, process, or system dump to the server for forensic investigation. For more information, see [Performing Host Forensics](#).
- 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](#).
- (Optional) If you suspect that a host is potentially compromised with the threat still being active, you can isolate the host from the network and safely investigate possible threats within the host. For more information, see [Isolating Hosts from Network](#).

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, last scan time, operating system, hostname, username, Mac address, risk score, IPV4, driver error code, security configurations, agent groups, and host status - managed, roaming, and isolated.

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.

Filters

SAVED FILTERS
Select

HOST STATUS
☐ Managed
☐ Roaming
☐ Isolated

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

Table Data:

HOSTNAME	RISK SCORE	OPERATING SYSTEM	LAST SCAN TIME
[redacted]	100	windows	11/12/2019 09:36:33 am
[redacted]	100	windows	11/12/2019 05:53:25 pm
[redacted]	77	windows	11/11/2019 01:07:04 pm
[redacted]	76	windows	11/14/2019 09:27:54 am
[redacted]	72	windows	11/11/2019 02:41:06 pm
[redacted]	70	windows	11/11/2019 12:35:19 am
[redacted]	33	windows	11/08/2019 10:45:15 am
[redacted]	N/A	windows	11/18/2019 08:45:34 am
[redacted]	0	windows	11/11/2019 06:46:15 am
[redacted]	0	windows	11/14/2019 12:35:50 pm
[redacted]	0	windows	11/14/2019 10:23:25 pm
[redacted]	0	windows	11/15/2019 12:01:28 am

Showing 12 out of 12 hosts | 0

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 `||`.

Filters

×

USERNAME

Equals ▾ Enter value

AGENT GROUPS

Equals ▾ Enter value

NIC MAC ADDRESS

Equals ▾ e.g.,00:00:00:00:00:00

IPV4

Equals ▾ 10.87.225.68 | 10.40.7.11

AGENT LAST SEEN

▾

LAST SCAN TIME

☐ CUSTOM DATE ▾

OPERATING SYSTEM

☐ Windows

☐ Linux

☐ Mac

AGENT MODE

Reset

Save

Save as...

To filter on the agent last seen or last scan time, select the option from the drop-down list. If you select 3 Hours ago for the Last Scan Time, the result displays hosts that were last scanned 3 hours ago or earlier.

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...

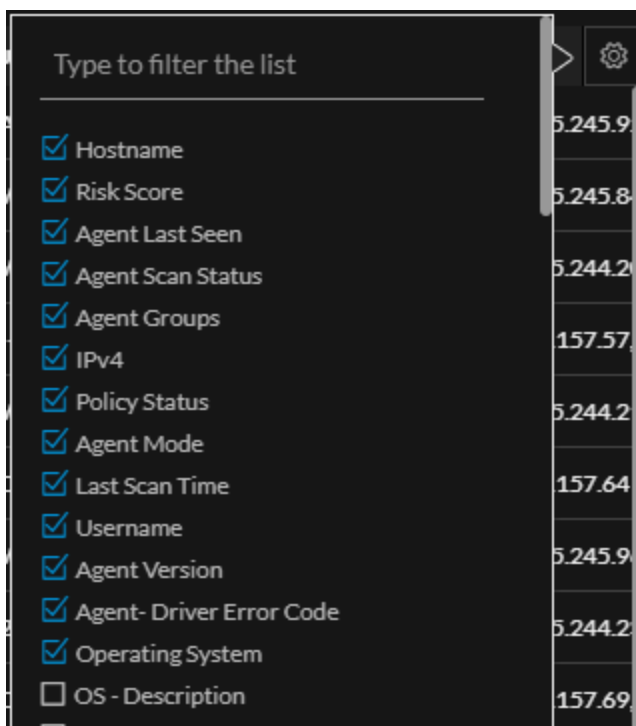
Click **Save** to save the filter and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters panel on the left. To delete a filter, hover over the filter name and click .

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.

- 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:

- Go to **INVESTIGATE > Hosts**.
The Hosts view is displayed.
- In the Server drop-down list, select the Endpoint server or Endpoint Broker server to view the hosts.
- 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.
- 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.
- Click an alert to view the associated events.

The screenshot displays the NetWitness Endpoint interface. On the left, the **ALERTS SEVERITY** panel shows counts for Critical (2), High (10), Medium (13), and All (25) alerts. Below this, it lists specific alerts like 'Enables ClearText Credential Storage (1)' and 'Enables Login Bypass (18)'. The main area shows a list of events with columns for Event Time, Event Type, Category, Action, Hostname, User Account, Operating System, and Hash. The first event is a 'createProcess' action on 03/01/2019 at 02:34:08.000 pm, involving 'malware10.exe' and 'REG.exe'. The right panel, titled **HOST DETAILS**, shows information for the selected host, including its name 'WIN-NMUFV3DGTNecat', session ID '2', and network interfaces like 'Intel(R) PRO/1000 MT Networ...'. A note at the top of the events list states: 'Events rolled over due to retention policies or manual deletion will not be available.'

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.

- 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.

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

- 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 Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this, a sub-navigation bar shows 'NAVIGATE', 'EVENTS', 'HOSTS' (selected), 'FILES', 'ENTITIES', and 'MALWARE ANALYSIS'. The main content area is divided into several panels:

- Host Summary:** Shows '100 windows' with a status of 'Idle'. It also displays 'AGENT LAST SEEN' as 'a few seconds ago' and 'AGENT VERSION' as '11.4.0.0'. The 'SNAPSHOT TIME' is '11/12/2019 05:53:25 pm'.
- Alerts Severity:** A summary of alerts by severity: 2 CRITICAL, 1 HIGH, 1 MEDIUM, and 4 ALL. Specific alerts listed include 'Login Bypass Configured (20)' and 'Possible Login Bypass (20)', both with 20 event(s).
- Event List:** A table of events with columns for EVENT TIME, EVENT TYPE, CATEGORY, ACTION, FILE NAME, and HASH. Two events are shown, both at '11/12/2019 10:58:53.000 am' with 'Endpoint' type and 'Autorun' category. The first event has a file name 'cmd.exe' and a hash '6aeea6272e1c304d1b8907b2...'. The second event has a file name 'cmd.exe' and a hash 'd0ceb18272966ab62b8edff10...'. Both events have 'N/A' for source and target.
- Host Details Panel:** A sidebar on the right with tabs for 'HOST DETAILS' and 'POLICY DETAILS'. It includes a search bar 'Search by filename, path or hash' and a section for 'Users' with details for 'WINDOWS10\ecat' (Session ID 2, Administrators group) and 'Window Manager\DWM-1' (Session ID 1).

Filter Host Details

In the Processes, Autoruns, Files, Drivers, Libraries, and Anomalies tabs, you can filter the processes or files on file status, reputation, file or process name, signature, and risk score. Click **Save** to save the filter 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.

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.

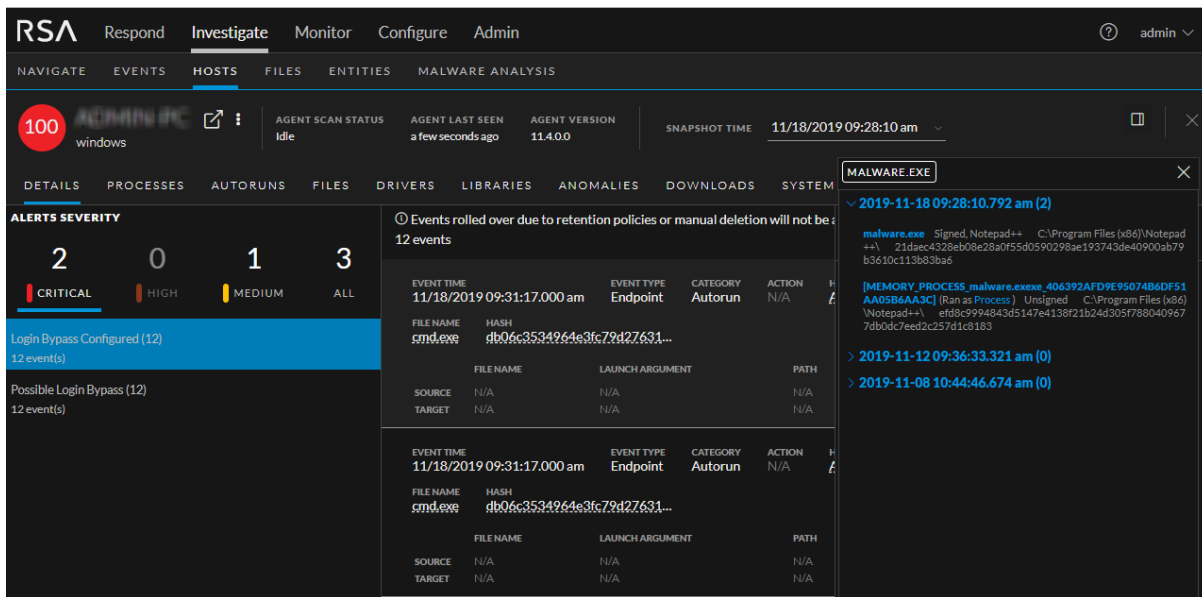
Note: To search for a SHA-256 checksum, provide the entire hash string in the search box.

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 RSA NetWitness Investigate interface. The top navigation bar includes Respond, Investigate (selected), Monitor, Configure, and Admin. The left sidebar shows the host 'ADMIN-PC' with a status of 'Idle' and a snapshot time of '11/18/2019 09:28:10 am'. The main panel displays the 'DETAILS' tab for the host, showing a list of alerts and events. A search box in the top right of the main panel contains the text 'malware.exe'. The search results show a list of events, including a file named 'cmd.exe' with a SHA-256 hash of 'db06c3534964e3fc79d27631...'. The interface also displays a list of alerts on the left, including 'Login Bypass Configured (12)' and 'Possible Login Bypass (12)'.

This file is run as a Process.

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

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

Analyze Processes

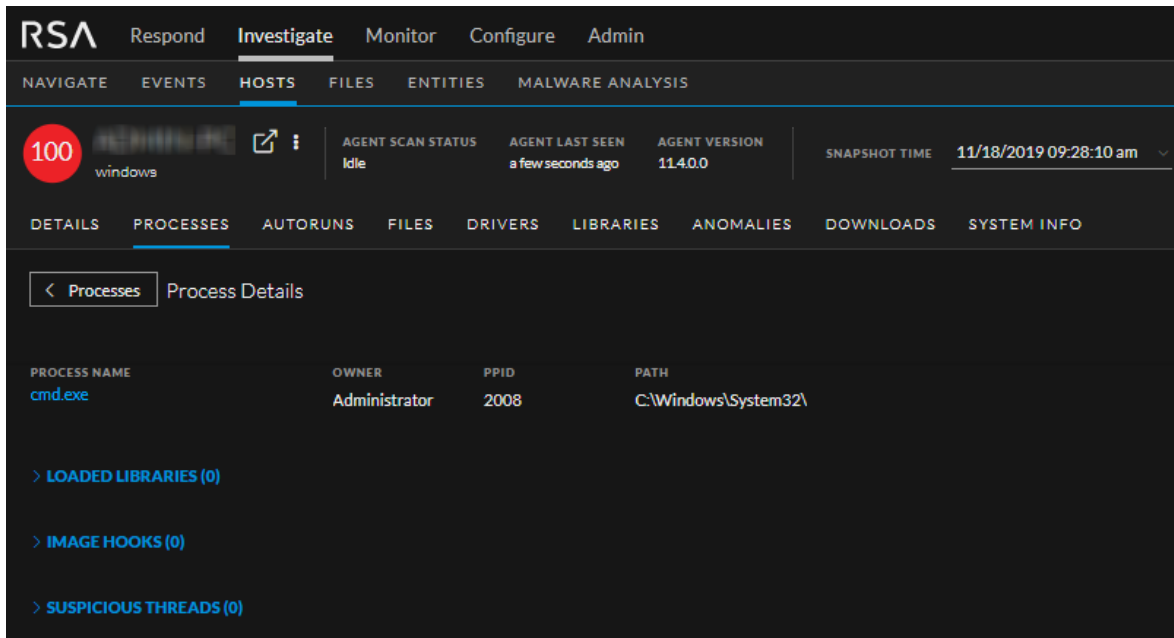
To analyze the process:

- In the **Hosts** details, select the **Processes** tab.

To view the process tree, click the toggle switch. The following is an example of the tree view:

2. In the **Processes** Tab, do one of the following:
 - Click a row to view the properties of a process in the right panel.

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



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 details, 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 details, 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 details, 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 details, 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 details, 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 details, 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 to JSON file:

1. Go to **INVESTIGATE > Hosts**.
2. Select the hostname to open the host details.
3. Click  (**More**) beside the hostname, and select **Export Host Details**. This exports host details and file context for the host.

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 displays the RSA NetWitness Investigate interface. The top navigation bar includes tabs for Respond, Investigate (selected), Monitor, Configure, and Admin. Below this, a sub-navigation bar shows NAVIGATE, EVENTS, HOSTS (selected), FILES, ENTITIES, and MALWARE ANALYSIS. The main content area shows a host named 'windows' with a risk score of 100. A sidebar on the left contains filters for Process Name, File Status, Reputation, and Signature. The main table lists processes with columns for Process Name, Local Risk Score, and Global Risk Score. A context menu is open over the 'calc.exe' process, showing options: Analyze Process, Change File Status, Analyze Events, Google Lookup, VirusTotal Lookup, Download Process Dump to Server, Download File to Server, Save a Local Copy, and Analyze File.

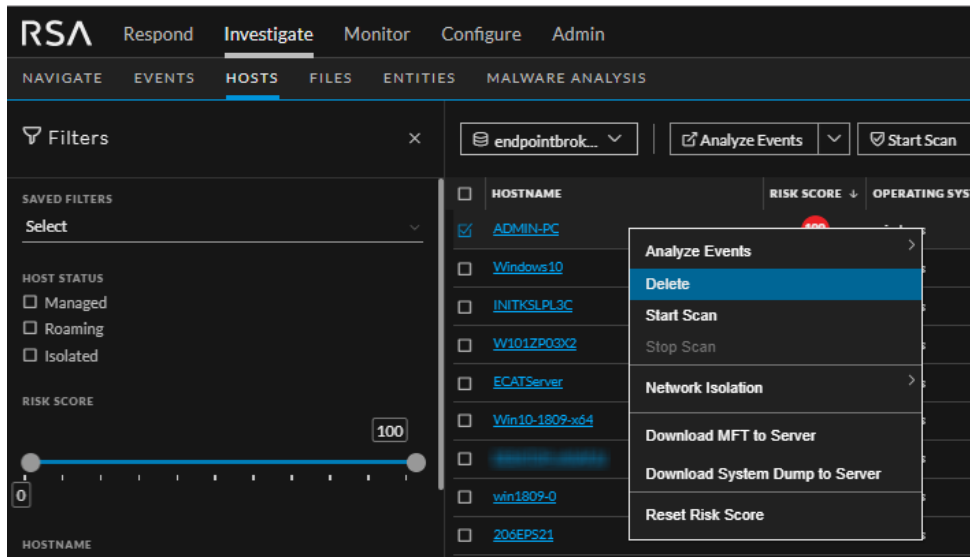
- Select **Google Lookup** to perform a search on the filename, MD5, SHA1, or SHA256.
- Select **VirusTotal Lookup** to perform a search on MD5, SHA1, or SHA256.

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:



- 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 or later, if you want to delete the hosts with older versions:

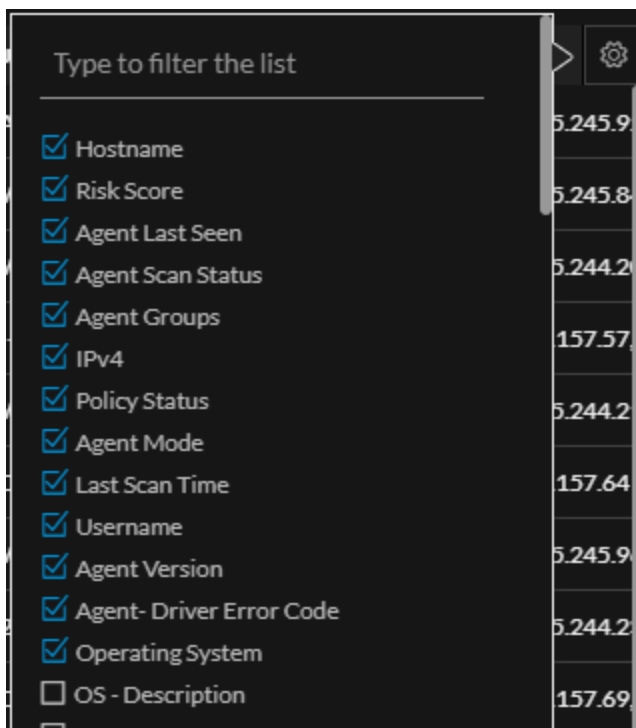
1. Go to **Investigate > Hosts** view.
2. Filter the hosts based on the Agent version, and delete these hosts.

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.
4. Sort the data on the required column.

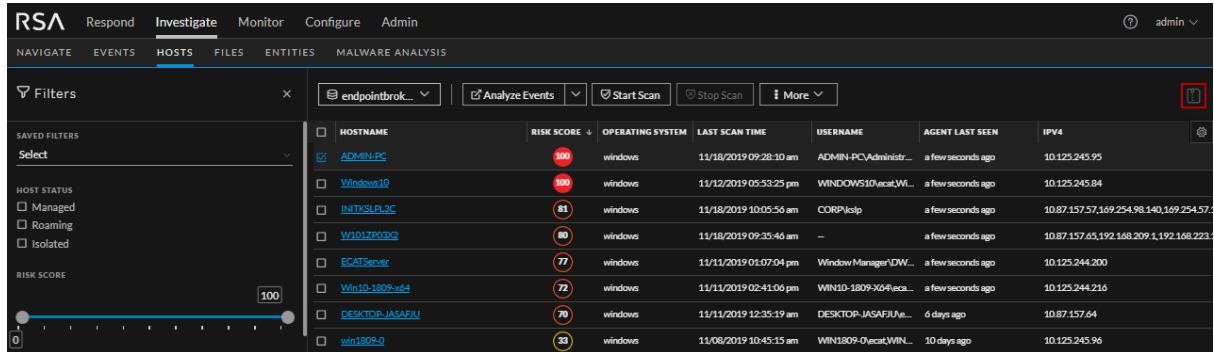
Note: The selections you make here become your default view every time you log in to the Hosts view.

Export Host Attributes

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

1. Go to **INVESTIGATE > Hosts**.
2. Filter the hosts by selecting the required filter options.
3. Add columns by clicking  in the right-hand corner.

4. Click  to export the host attributes to a csv file.



HOSTNAME	RISK SCORE	OPERATING SYSTEM	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	IPV4
ADMIN-PC	100	windows	11/18/2019 09:28:10 am	ADMIN-PC\Administr...	a few seconds ago	10.125.245.95
Windows10	100	windows	11/12/2019 05:33:25 pm	WINDOWS10\ecat.Wi...	a few seconds ago	10.125.245.94
initKSLPL3C	81	windows	11/18/2019 10:05:56 am	CORP\calp	a few seconds ago	10.87.157.57,169.254.98.140,169.254.57...
W1012P0302	80	windows	11/18/2019 09:35:46 am	--	a few seconds ago	10.87.157.65,192.168.209.1,192.168.223...
ECATServer	77	windows	11/11/2019 01:07:04 pm	Window Manager\DW...	a few seconds ago	10.125.244.200
Win10-1809-x64	72	windows	11/11/2019 02:41:06 pm	WIN10-1809-X64\eca...	a few seconds ago	10.125.244.216
DESKTOP-JASAFU...	70	windows	11/11/2019 12:35:19 am	DESKTOP-JASAFU...	6 days ago	10.87.157.64
win1809-0	33	windows	11/08/2019 10:45:15 am	WIN1809-0\ecat.WIN...	10 days ago	10.125.245.96

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:

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

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

The screenshot displays the RSA NetWitness Investigate interface. The top navigation bar includes tabs for Respond, Investigate, Monitor, Configure, and Admin. Below this, a sub-navigation bar shows options like NAVIGATE, EVENTS, HOSTS, FILES, ENTITIES, and MALWARE ANALYSIS. The main content area is divided into several sections. On the left, there's an 'ALERTS SEVERITY' section with counts for CRITICAL (2), HIGH (1), MEDIUM (1), and ALL (4). Below this, there are two alert entries: 'Login Bypass Configured (20)' and 'Possible Login Bypass (20)'. The central pane shows event details for a specific host, including event time (11/12/2019 10:58:53.000 am), event type (Endpoint), category (Autorun), and action (N/A). The right pane shows host details, including the host name 'WINDOWS10.ecat', session ID '2', and groups 'Administrators'.

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:

HOSTNAME	RISK SCORE	OPERATING SYSTEM	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	IPV4
204EPS21	N/A	windows	11/18/2019 1	Windo...	a few seconds ago	10.125.244.236
ADMIN-PC	100	windows	11/18/2019 0	ministr...	a few seconds ago	10.125.245.95
Windows10	100	windows	11/12/2019 0	catWi...	a few seconds ago	10.125.245.84
DESKTOP-OSEVSL3	100	windows	11/14/2019 1		4 days ago	10.87.157.66
DESKTOP-OSEVSL3	100	windows	11/11/2019 1	FJU/ve...	6 days ago	10.87.157.64
INITKSLPL3C	81	windows	11/18/2019 10:05:56 am	CORP\kslp	a few seconds ago	10.87.157.57,169.2

- 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, risk score, 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.
- On Hosts - Determines on how many hosts on which a file exist. If a file is present on fewer hosts with a high risk score, it may be malicious and needs further investigation.
- 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, the file `powershell` has invoked `mimikatz`, which is a tool to extract plain text passwords, hashes, and kerberos tickets from memory.

The screenshot displays the RSA NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this, a sub-navigation bar shows 'NAVIGATE', 'EVENTS', 'HOSTS' (selected), 'FILES', 'ENTITIES', and 'MALWARE ANALYSIS'. The main content area is divided into several sections:

- Alerts Severity:** A summary bar showing 3 Critical, 3 High, 15 Medium, and 21 All alerts.
- Event List:** A table of events with columns for Date/Time, Event Type, Category, Action, Hostname, User Account, Operating System, File Name, Hash, and User Src. The selected event is dated 11/29/2019 09:59:25.000 am, categorized as 'Endpoint', 'Process Event', and 'CreateProcess'.
- Process Details:** A detailed view of the selected process, showing source and target information, file SHA256 hashes, file names, and launch arguments. The process is identified as 'cmd.exe' and is running on a Windows system.
- Related Links:** A section with links to 'Investigate Original Event', 'Investigate Destination Domain', and 'Analyze Process'.

Clicking **Analyze Process** displays the process visualization. For each node, the process name, risk score, and type of activity the selected process has performed (network , file , or registry ) are displayed. Optionally, you can change the time range to view data.

You can view the properties, such as process execution details, file properties of the selected process in the bottom of the view.

PROCESS EXECUTION DETAILS		FILE GENERAL	FILE PE	IMPORTED LIBRARIES	FILE HASH
EVENT TIME	11/27/2019 02:34:00.000 pm	FILENAME	cmd.exe	FEATURES	MD5
PROCESS NAME	cmd.exe	DATE	11/20/1975 08:18:58.000 pm	FILENAME	0d088f5bfa8f086fba163647cd90cab
FILE LOCATION	c:\windows\system32\	SIZE	404.0 KB	SECTION NAMES	08cc2e8dca652b8da1acca9c44550d4bc1b
CHECKSUM	9023f8aada4a1da45ac477a81b5bbe4128e4...	EXPORTED FUNCTIONS	0	DESCRIPTION	9023f8aada4a1da45ac477a81b5bbe4128e4...
SESSION ID	15844030	EXPORTED NAMES	0	VERSION	

Note: No result is displayed in the process visualization view if there is no data for last seven days or if there is no createprocess event.

4. On the right side of the process visualization view:
 - Click **Events List** to view the associated events. You can also filter events based on the events category. For more information on filtering, see [Analyze Events for a Process](#).
 - Click **Hosts** to view the hosts on which this file is present and the associated risk score. For more information, see [Analyze Hosts with File Activity](#).
 - Click **Risk Details** to view the list of distinct alerts, such as Critical, High, Medium and All. For more information, see [Analyze Hosts Using the Risk Score](#).
5. Hover over the process name to analyze important process attributes, such as username, launch arguments, reputation, file status, signer, signature, and file path.

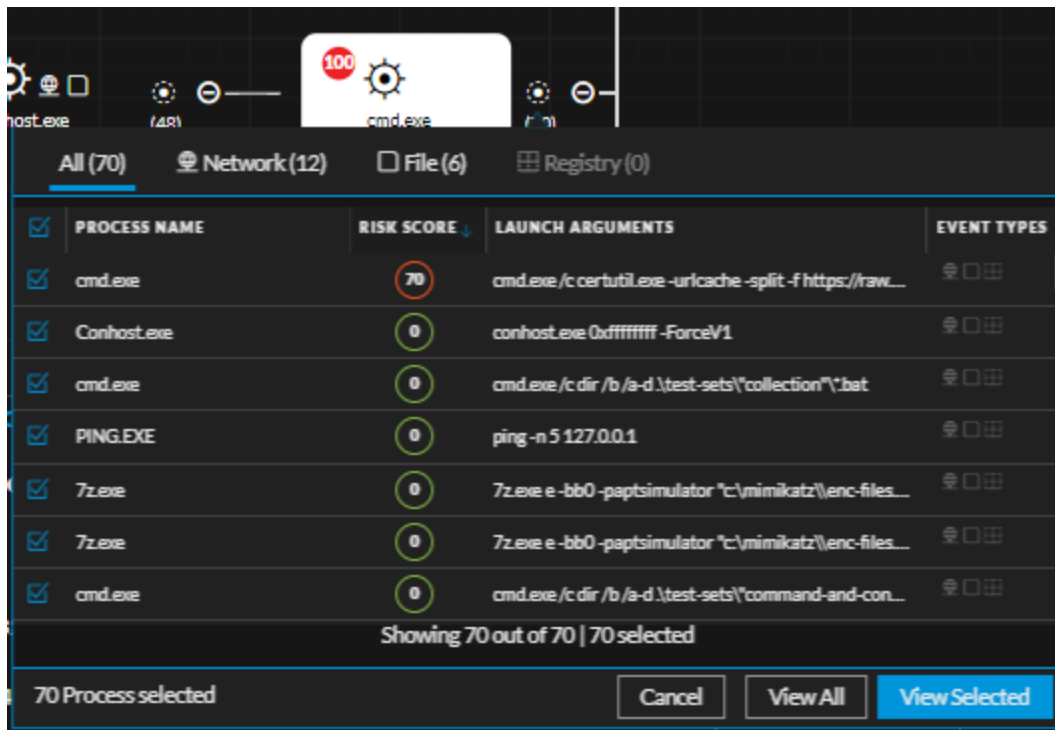


6. Click  to view the child processes. The Process selection dialog is displayed with the child processes associated with the process based on the risk score. You can filter the result on the event type by clicking icons on the top panel. When no matching event types are available, these filter options are disabled.

Depending on the type of event, the icons are highlights in the Event Types column.

- a. Click **View All** to view all child processes or select the required processes and click **View selected**. The associated events and properties are displayed in the right panel.

- b. Click  to change the process selection and click  to collapse the view.



Analyze Events for a Process

To analyze events for the selected process:

1. Perform steps 1 to 3 in [Analyze a Process](#).
2. In the process visualization, click the **Events** tab.
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, to view only process events, select the **Process Event** category, and filter on action.

The screenshot shows the NetWitness Analyze interface. On the left, the 'Filters' panel is open, showing 'Category' with 'Process Event' selected and 'Action' with 'openProcess' selected. The main table displays a list of events filtered by these criteria. The table has columns: EVENT TIME, CATEGORY, ACTION, SOURCE FILE NAME, SOURCE PARAMETER, SOURCE DIRECTORY, and SOURCE. The events listed are all 'Process Event' with the action 'openPr...' (truncated) and the file name 'explorer.exe' or 'svchost.exe' or 'lsass.exe'. The source directory is 'C:\Windows\' for most, and 'C:\Windows\System32\' for the last two. The status bar at the bottom indicates 'Showing 19 out of 19'.

EVENT TIME	CATEGORY	ACTION	SOURCE FILE NAME	SOURCE PARAMETER	SOURCE DIRECTORY	SOU
11/25/2019 06:5...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/25/2019 03:0...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/25/2019 11:1...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/26/2019 07:1...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/27/2019 02:3...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/27/2019 10:3...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/28/2019 06:4...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/28/2019 02:5...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/28/2019 10:5...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/29/2019 07:0...	Process Event	openPr...	explorer.exe		C:\Windows\	
11/29/2019 09:3...	Process Event	openPr...	svchost.exe	svchost.exe -k netsvc -p	C:\Windows\System32\	
11/29/2019 09:3...	Process Event	openPr...	lsass.exe		C:\Windows\System32\	

The result displays the sequence of activities involving this process for the selected filters.

Note: For the console events, the context for local and remote are available only if the data is sent from 11.4 or later agents.

Changing File Status or Remediate

Note: By default, the blocking option is disabled in the policy. 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 RSA NetWitness Investigate interface. The 'FILES' tab is active. A context menu is open for 'OneDrive.exe', with 'Change File Status' selected. The toolbar includes buttons for 'View Certificates', 'Change File Status', 'Analyze Events', and 'More'. The table lists files with columns for File Name, Risk Score, First Seen Time, On Hosts, and Reputation.

FILE NAME	RISK SCORE	FIRST SEEN TIME	ON HOSTS	REPUTATION
OneDrive.exe	100	11/06/2019 02:41...	2	--
lsass.exe		11/06/2019 02:41...	3	--
cmd.exe		11/08/2019 10:49...	1	--
cmd.exe		11/08/2019 10:51...	4	--
cmd.exe		11/06/2019 02:42...	1	--
cmd.exe		11/06/2019 02:41...	3	--
services.exe		11/06/2019 02:41...	3	--
Taskmgr.exe		11/18/2019 09:38...	1	--
Taskmgr.exe		11/06/2019 02:41...	2	--
PowerShell.exe	70	11/18/2019 09:47...	1	--
Taskmgr.exe	70	11/10/2019 09:51...	1	--

- 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 or automatically download the file to the server.

Note: Saving or analyzing downloaded file works the same way irrespective of whether the file is downloaded manually or automatically.

Note: Downloaded files are stored in the Endpoint Server which may fill up the disk space. To utilize the storage efficiently without impacting the health of Endpoint Server, RSA recommends you to configure an external storage mount, so all the Endpoint Server can use the configured location to store the downloaded data.

By default, all files are downloaded to `/var/netwitness/endpoint-server/<files>/`. If you want to change the location, make sure that you have **endpoint-server.configuration.manage** permissions and do the following:

1. In the Explore view, go to **endpoint/download**,
2. In the base-path, provide the location of the directory.

Caution: By default, the status **File Download Disk Usage** stats in the **Health and Wellness** view shows unhealthy if the disk usage reaches 60% and the file download stops automatically when the disk usage is 70%. You can customize the warning or fatal thresholds in the **ADMIN > Services > Endpoint Server > view > Explore > rsa.endpoint.file-download-disk-thresholds.warning-percent** and **rsa.endpoint.file-download-disk-thresholds.fatal-percent** parameters respectively.

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

Downloading file to server is not supported for memory DLL and floating code.

Note: Downloading files may take significant time. Additional requests to the agent during download are queued and processed when the download is complete.

Automatic File Download

By default, the files that are unsigned and size lesser than or equal to 1 MB are downloaded automatically to the NetWitness Endpoint server. And, only single copy of each file is downloaded automatically. You can limit the volume of files to be downloaded in the **ADMIN > Endpoint Sources > Policies** tab, so the files matching certain criteria are only downloaded automatically. For more information on automatic file download settings, see "Create an EDR Policy" section in the *RSA NetWitness Endpoint Configuration Guide*.

The status of the download is displayed in the **INVESTIGATE > Files** tab > **Downloaded** column.

Manual File Download

To manually download files 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:

The screenshot shows the NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this is a sub-navigation bar with 'NAVIGATE', 'EVENTS', 'HOSTS' (selected), 'FILES', 'ENTITIES', and 'MALWARE ANALYSIS'. The main header area displays '100 windows' with a red circle, 'AGENT SCAN STATUS: Idle', 'AGENT LAST SEEN: a few seconds ago', 'AGENT VERSION: 11.4.0.0', and 'SNAPSHOT TIME: 11/12/2019 05:53:25 pm'. The sub-navigation bar below the header includes 'DETAILS', 'PROCESSES' (selected), 'AUTORUNS', 'FILES', 'DRIVERS', 'LIBRARIES', 'ANOMALIES', 'DOWNLOADS', and 'SYSTEM INFO'. On the left, there is a 'Filters' panel with 'PROCESS NAME' (set to 'Equals e.g., Filename.dll') and 'FILE STATUS' (Neutral, Blacklist, Graylist, Whitelist) and 'REPUTATION' (Malicious, Suspicious, Unknown, Known, Known Good, Invalid). The main content area shows a table of processes. The 'lsass.exe' process is selected, and a context menu is open over it, showing options: 'Analyze Process', 'Change File Status', 'Analyze Events', 'Google Lookup', 'VirusTotal Lookup', 'Download Process Dump to Server', 'Download File to Server' (highlighted in blue), 'Save a Local Copy', and 'Analyze File'. The table has columns: 'PROCESS NAME', 'LOCAL RISK SCORE', 'GLOBAL RISK SCORE', and 'ON HOSTS'. The 'lsass.exe' process has a local risk score of 100, a global risk score of 100, and is on 3 hosts. Other processes listed include 'OneDrive.exe', 'services.exe', 'Taskmgr.exe', 'ApplicationFrameHost.exe', 'browser_broker.exe', 'conhost.exe', 'csrss.exe', and 'csrss.exe'.

- 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:

The screenshot shows the RSA NetWitness Investigate interface. The top navigation bar includes Respond, Investigate (selected), Monitor, Configure, and Admin. Below this, the main navigation bar has tabs for NAVIGATE, EVENTS, HOSTS, FILES (selected), ENTITIES, and MALWARE ANALYSIS. On the left, there's a 'Filters' panel with 'SAVED FILTERS' and 'FILE NAME' (set to 'Equals' with 'e.g., Filename.dll'). The main area displays a table of files. A context menu is open over the first row, showing options like 'Change File Status', 'Analyze Events', 'Google Lookup', 'VirusTotal Lookup', 'View Certificates', 'Download File to Server' (highlighted), 'Save a Local Copy', 'Analyze File', and 'Reset Risk Score'. The table columns are: FILE NAME, RISK SCORE, FIRST SEEN TIME, ON HOSTS, and REPUTATION.

FILE NAME	RISK SCORE	FIRST SEEN TIME	ON HOSTS	REPUTATION
OneDrive.exe		11/06/2019 02:41:5...	2	--
lsass.exe		11/06/2019 02:41:5...	3	--
cmd.exe		11/08/2019 10:49:3...	1	--
cmd.exe		11/08/2019 10:51:0...	4	--
cmd.exe		11/06/2019 02:42:2...	1	--
AdversarySimulator.bat		11/19/2019 06:15:1...	1	--
cmd.exe		11/06/2019 02:41:5...	3	--
services.exe		11/06/2019 02:41:5...	3	--
Taskmgr.exe		11/18/2019 09:38:5...	1	--

- 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.

Cmd.Exe | Details | Analysis

70 ACTIVE ON 0 SIGNATURE microsoft.signed.valid.catalog SIZE 227.5 KB FILE STATUS Neutral OPERATING SYSTEM windows

File Analysis - Strings View FILTER STRINGS Enter Value

STRING	OFFSET	UNICODE	LENGTH
usebackq	0x00027C88	✓	8
XAV]	0x0000C64A	—	4
NtOpenProcessToken	0x0002DFE0	—	18
fE9d	0x0001F9AA	—	4
ReadConsoleW	0x0002D184	—	12
wscmp	0x0002E0BC	—	6
/dpiAware	0x00030CBF	—	9
%2d%2s%02d%2s%02d%2s%02d	0x00027EC0	✓	21
AcquireSRWLockShared	0x0002D202	—	20
	0x00030B00	—	4
fD9,pu	0x0001FE72	—	6
POPD	0x00028268	✓	4
/9A	0x0000C236	—	4
ti9L	0x00012488	—	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: 99ae9c73e9bee6f9c76d6f4093a9882df068...

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.

100 Windows 10 | AGENT SCAN STATUS Idle | AGENT LAST SEEN a few seconds ago | AGENT VERSION 11.4.0.0 | SNAPSHOT TIME 11/12/2019 05:53:25 pm

DETAILS | PROCESSES | AUTORUNS | FILES | DRIVERS | LIBRARIES | ANOMALIES | DOWNLOADS | SYSTEM

< Files | File Analysis - Strings View FILTER STRINGS m3

STRING	OFFSET	UNICODE	LENGTH
*m3.m3update.com	0x0000A07	✓	19
*m3.twitterdoc.com	0x0000A96	✓	22
*m3.freemove.chickenkiller.com	0x0000B28	✓	32

C2 info visible in File Content

Exec.exe

Type to filter list

☒ Show details with values only

File Details

Format: pe

checksumMd5: d16f277c8d94437b751917d87dd8d91

checksumSha1: 60ec5ca33072dffa9a1d9eac946c20834a4...

checksumSha256: b266afb334f3dec596dac650170994c8f942...

Size: 6.0 KB

Downloaded FileName: b266afb334f3dec596dac650170994c8f942...

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 (8)

Subsystem: Windows Console

Packing Detection

Entry Point Valid: true

Showing 3 of 123 strings

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 File Analysis - Strings View for the file KeyLogger.exe. The table lists strings found in the file, with columns for STRING, OFFSET, UNICODE, and LENGTH. Red boxes highlight specific strings that are indicators of keystroke logging. A red arrow points to these boxes with the text "Indicators of keystroke logging".

STRING	OFFSET	UNICODE	LENGTH
[Del]	0x00055070	--	5
[E+]	0x00055128	--	5
[Pgdn]	0x00055068	--	7
59A42	0x0004012F	--	7
202[2]2m2[2]	0x0006181D	--	11
[Up]	0x00055050	--	4
delete]	0x00056100	--	9
7XBOS8WQ8	0x00062368	--	11
[O+*	0x0005CF4	--	6
7CN75T[+8P	0x00062D15	--	12
[PageDown]	0x0005511C	--	10
new[	0x000560F8	--	6
[hunk]	0x00056610	--	8
01,1[1a1	0x00061809	--	9
5595	0x00062489	--	5
[93	0x0005C3C8	--	4
[Num Lock]	0x00055218	--	10
[End]	0x00055060	--	5

Showing 29 of 1510 strings

Indicators of keystroke logging

File Details

Type to filter list

Show details with values only

File Details

Format: pe

checksumMd5: 5742d67ee306123c55c1dbdcad83062

checksumSha1: dacc40cfeddb8d55cdce615e506209c8f18...

checksumSha256: c9eb0aa40eaa22685afacaa24136e98472...

Size: 401.0 KB

Downloaded FileName: c9eb0aa40eaa22685afacaa24136e98472...

Downloaded Path: \\nar\netwitness\endpoint-server\files\c9eb0

Image Details

Architecture: i386/x86

Characteristics: Executable, 32-bit

Compile Time: 03/22/2019 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 Found: true

Performing Host Forensics

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.4 and later.

You can perform the following forensic investigation on a host:

- Master File Table (MFT)
- System Dump
- Process Dump

Note: This is applicable only for Windows agent (in Advanced mode) with NetWitness Platform version 11.4. Downloading system dump files may take significant time. Additional requests to the agent during system dump download are queued and processed when the download is complete. MFT, system dump, and process dump downloads are not supported for agents communicating through Relay server.

Note: MFT, system dump, and process dump are stored in the Endpoint Server which may fill up the disk space. For large deployments, to utilize the storage efficiently without impacting the health of Endpoint Server, RSA recommends you to configure an external storage mount, so all the Endpoint Server can use the configured location to store the downloaded data.

By default, all files are downloaded to `/var/netwitness/endpoint-server/<file type>/`, where `<file type>` is MFT, system dump, or process dump. If you want to change the location, make sure that you have `endpoint-server.configuration.manage` permissions and do the following:

1. In the Explore view, go to **endpoint/download**.
2. In the base-path, provide the location of the directory.

Download Master File Table

Master File Table contains metadata of every file on the host. It keeps track of information, such as filename, size, timestamps, permissions, and location of the file on the host. It consists of two sets of timestamps - Standard Information (\$SI) and File Name (\$FN). Each set has the following timestamps - creation, access, update, and modification.

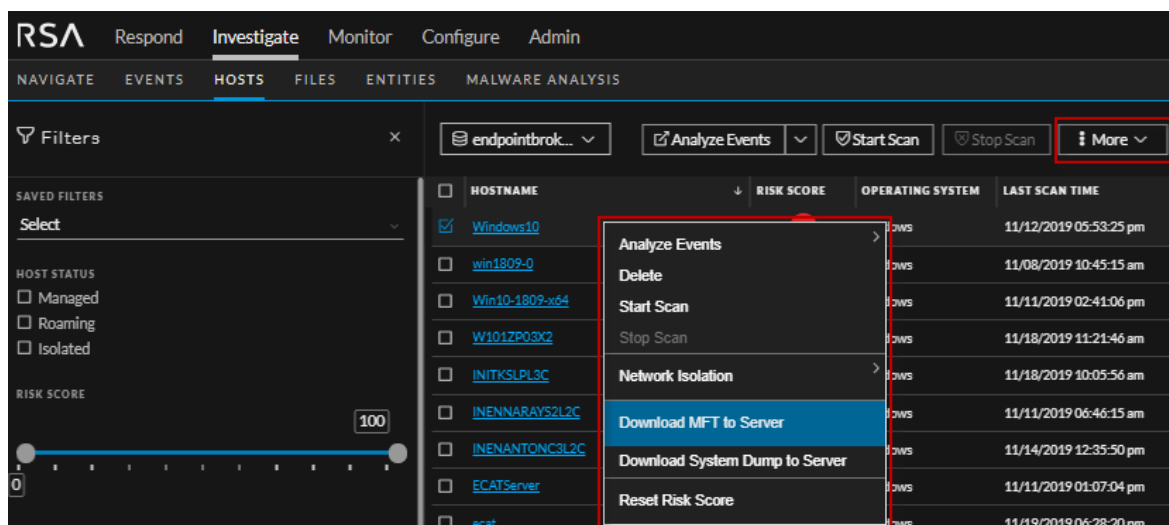
Time stamping is a technique that modifies the timestamps for a file (creation, access, update, and modification time) to mimic files that are in the same folder, making it difficult to identify suspicious files on a host. To perform forensic investigation of a suspicious file, you can download and analyze the MFT, and focus on files that are time stamped. For more information, see [Analyze Downloaded MFT](#).

During MFT analysis, you can also search for suspicious filenames, and also files that were created before or after a known malicious event. You can also download files from the MFT viewer for further analysis.

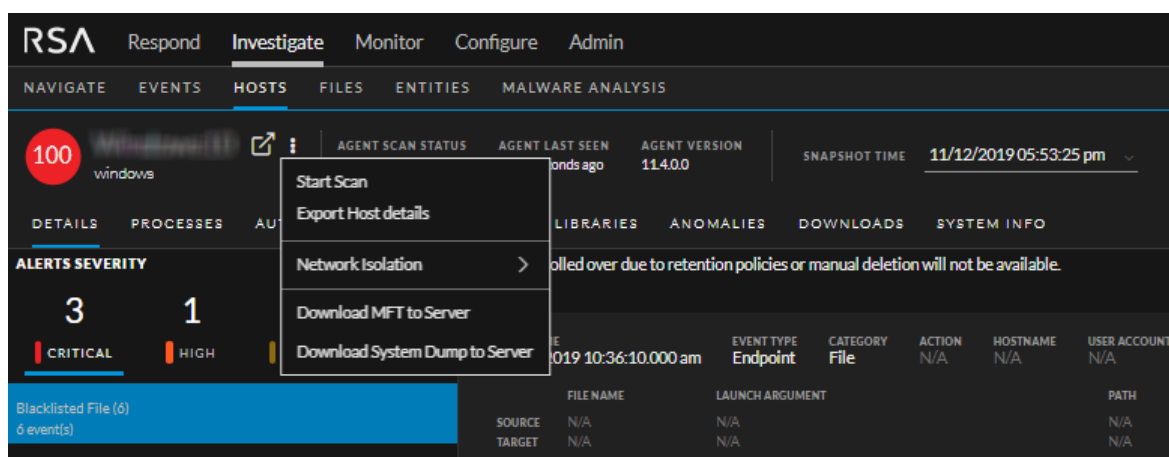
Download MFT to Server

To download MFT to the server from the Hosts view:

- Go to **INVESTIGATE > Hosts** and do one the following:
 - Select a host and select **Download MFT to Server** from the right-click context menu, or from the **More** drop-down list in the toolbar.



- Select the hostname to open the host details, click **(More)** beside the hostname, and select **Download MFT to Server**.



- View details of the downloaded MFT in the **Downloads** tab within the host details. For more information, see [Hosts View - Downloads Tab](#).

The screenshot shows the RSA NetWitness Investigate interface. The top navigation bar includes Respond, Investigate (selected), Monitor, Configure, and Admin. Below this is a sub-navigation bar with NAVIGATE, EVENTS, HOSTS (selected), FILES, ENTITIES, and MALWARE ANALYSIS. The main content area is titled '71 windows' and shows the 'Downloads' tab. A sidebar on the left contains filters for FILE TYPE (MFT, File, Process Dump, System Dump) and FILE NAME (Equals, e.g., Filename.dll). The main table lists downloaded files with columns for FILE NAME, TYPE, DOWNLOADED status, SIZE, DOWNLOADED TIME, and SHA256.

FILE NAME	TYPE	DOWNLOADED	SIZE	DOWNLOADED TIME	SHA256
systemdump-INGSMUDALPL6C-2019-...	SYSTEMDUMP	⚠	0 bytes	an hour ago	NA
processdump-19628-git-bash.exe-ING...	PROCESSDUMP	✓	51.7 MB	an hour ago	NA
systemdump-INGSMUDALPL6C-2019-...	SYSTEMDUMP	⚠	0 bytes	an hour ago	NA
processdump-18676-notepad++ exe-L...	PROCESSDUMP	✓	138.8 MB	an hour ago	NA
processdump-6328-cmd.exe-INGSMU...	PROCESSDUMP	⚠	0 bytes	an hour ago	NA
mft-C:INGSMUDALPL6C-2019-11-29...	MFT	✓	756.0 MB	an hour ago	NA
MSIPAuth.ni.dll	FILE	✓	122.0 KB	2 hours ago	2d0a2b32cd6c2f7f90760fc23...
libatk-1.0-0.dll	FILE	✓	159.6 KB	2 hours ago	718e569d24e6a6a0dfe44efaa...

Analyze Downloaded MFT

You can use the MFT viewer to begin analysis where you can search for files based on file name, time stamps, and identify files that are timestamped.

View MFT

To view the content of the downloaded MFT:

1. Go to **INVESTIGATE > Hosts**.
2. Select the hostname to open the host details and select the **Downloads** tab.
3. Click the file name. The MFT viewer is displayed.

All available files are displayed in a tree view similar to the Windows Explorer in the All Files folder. The Deleted Files folder contains a sequential list of all deleted files.

The screenshot shows the RSA NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this is a 'NAVIGATE' section with tabs for 'EVENTS', 'HOSTS' (selected), 'FILES', 'ENTITIES', and 'MALWARE ANALYSIS'. A sidebar on the left shows a file tree for 'C:\', including folders like 'inetpub', 'TMP', 'wamp64', 'Windows', 'Users', 'ProgramData', 'Program Files (x86)', '\$Recycle.Bin', 'PerfLogs', 'Program Files', '\$Extend', 'Recovery', 'Documents and Settings', and 'System Volume Information'. The main area displays the 'MFT Viewer' for host 'MFT-C-WINDOWS10-2019-11-14T06-47-52-777Z'. It shows a table of files with columns: NAME, SIZE, and CREATION TIME (\$FN). The table lists various trace files and a data collector CSV file.

NAME	SIZE	CREATION TIME (\$FN)
NWE-Trace-0c1c.txt	0 bytes	11/12/2019 07:02:03 pm
NWE-Trace-0acc.rar	2.0 MB	11/12/2019 11:54:16 am
NWE-Trace-0acc.txt	0 bytes	11/12/2019 12:48:33 am
NWE-Trace-0f80.rar	1.0 MB	11/12/2019 12:08:39 am
NWE-Trace-0f80.txt	0 bytes	11/11/2019 09:25:01 pm
NWE-Trace-0a3c.txt	0 bytes	11/11/2019 07:32:11 pm
NWE-Trace-0c44 - Copy.txt	49.8 MB	11/11/2019 06:56:29 pm
NWE-Trace-1fc0.txt	8.5 KB	11/11/2019 05:44:35 pm
NWE-Trace-0c44.txt	0 bytes	11/11/2019 05:43:31 pm
NWE-Trace-0c30.txt	101.9 KB	11/11/2019 05:42:05 pm
DataCollector01.csv	642.9 KB	11/11/2019 05:03:16 pm
NWE-Trace-264c - Copy.txt	21.0 MB	11/11/2019 05:02:52 pm
NWE-Trace-264c.txt	0 bytes	11/06/2019 09:38:24 pm

Directory path: C:\ | No filters applied

4. Click to view the folder structure. Click the row to view the folder content.

The details of the MFT is displayed in the table. By default, the table is sorted on the creation time (\$FN). If the \$SI and \$FN timestamps are different, the columns are highlighted in red () indicating that it is time stomped.

The screenshot shows the RSA NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this is a 'NAVIGATE' section with tabs for 'EVENTS', 'HOSTS' (selected), 'FILES', 'ENTITIES', and 'MALWARE ANALYSIS'. A sidebar on the left shows a file tree for 'C:\', including folders like 'Git', 'Temp', 'Deep Web (2015) [YTS.AG]', 'Git', 'SystematicSuite', 'ISO', 'Intel', 'Documents and Settings', 'Windows', 'Recovery', 'Users', 'ProgramData', and 'Program Files (x86)'. The main area displays the 'MFT Viewer' for host 'MFT-C:\WINDOWS\SYSTEM32\config\SMI-client-hb4'. It shows a table of files with columns: NAME, SIZE, CREATION TIME (\$FN), CREATION TIME (\$SI), MODIFICATION TIME (\$FN), MODIFICATION TIME (\$SI), ACCESS TIME (\$FN), and ACCESS TIME (\$SI). The table lists various files, including 'Git', 'Temp', 'Deep Web (2015) [YTS.AG]', 'Git', 'SystematicSuite', 'ISO', 'Intel', 'Documents and Settings', 'Windows', 'Recovery', 'Users', 'ProgramData', and 'Program Files (x86)'. The table highlights rows where the \$SI and \$FN timestamps are different, indicated by a red triangle icon.

NAME	SIZE	CREATION TIME (\$FN)	CREATION TIME (\$SI)	MODIFICATION TIME (\$FN)	MODIFICATION TIME (\$SI)	ACCESS TIME (\$FN)	ACCESS TIME (\$SI)
Git	1.9 KB	11/11/2019 06:17:06 am	11/11/2019 06:17:06 am	11/11/2019 06:17:06 am	11/20/2019 07:32:03 am	11/11/2019 06:17:06 am	11/11/2019 06:17:06 am
Temp	0 bytes	11/07/2019 01:03:38 pm	11/07/2019 01:03:38 pm	11/07/2019 01:03:38 pm	11/29/2019 05:53:57 am	11/07/2019 01:03:38 pm	11/29/2019 05:53:57 am
Deep Web (2015) [YTS.AG]	1.8 KB	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm
Git	0 bytes	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm
ISO	0 bytes	09/14/2019 11:54:02 am	09/14/2019 11:54:02 am	09/14/2019 11:54:02 am	09/14/2019 11:54:02 am	09/14/2019 11:54:02 am	09/14/2019 11:54:02 am
Intel	1.9 KB	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm	08/22/2019 01:54:22 pm	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm
Documents and Settings	1.9 KB	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm	08/22/2019 01:54:22 pm	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm
Windows	280.5 KB	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am	06/26/2019 10:44:40 am	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am
ProgramData	0 bytes	06/06/2019 05:21:54 pm	06/06/2019 05:21:54 pm	06/06/2019 05:21:54 pm	06/06/2019 05:21:54 pm	06/06/2019 05:21:54 pm	06/06/2019 05:21:54 pm

5. Select one or more files and click **Download File to Server** on the toolbar to download files to the server.

Note: Downloading a folder is not supported and hence the option is grayed out for folders.

Filter MFT

You can filter files on file name, creation time (\$FN), creation time (\$SI), access time (\$FN), access time (\$SI), update time (\$FN), update time (\$SI), modified time (\$FN), and modified time (\$SI).

Click **Save** to save the filter 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.

To filter, save, and delete MFT, see [Filter Downloaded Files](#), [Save Downloaded File](#), and [Delete Downloaded Files](#).

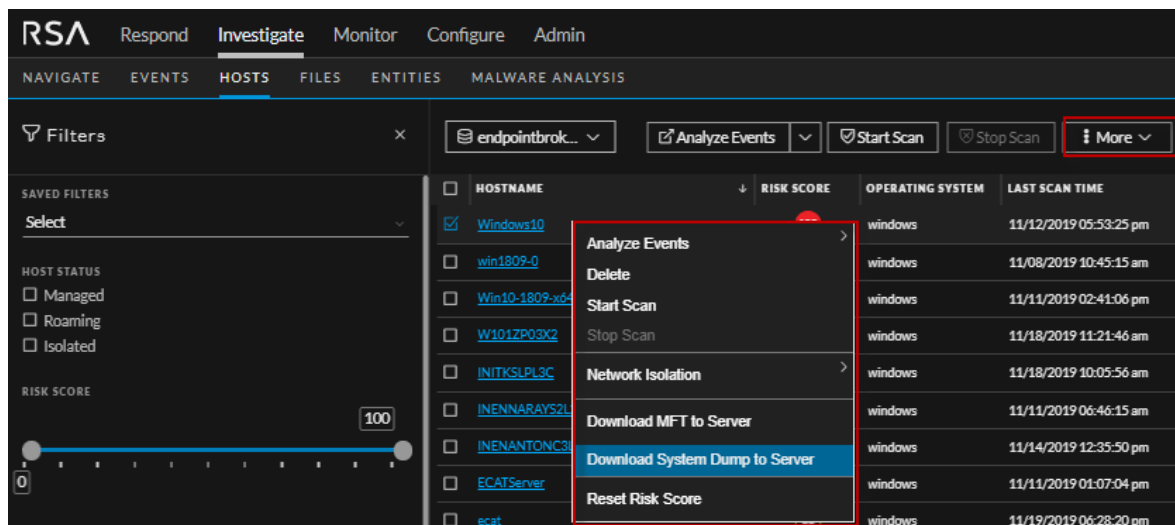
System and Process Memory Dump

To perform forensic investigation during an incident response, you can request a memory dump of a host or a process running on the host. You can analyze these dumps using third-party tools, such as Volatility, Rekall.

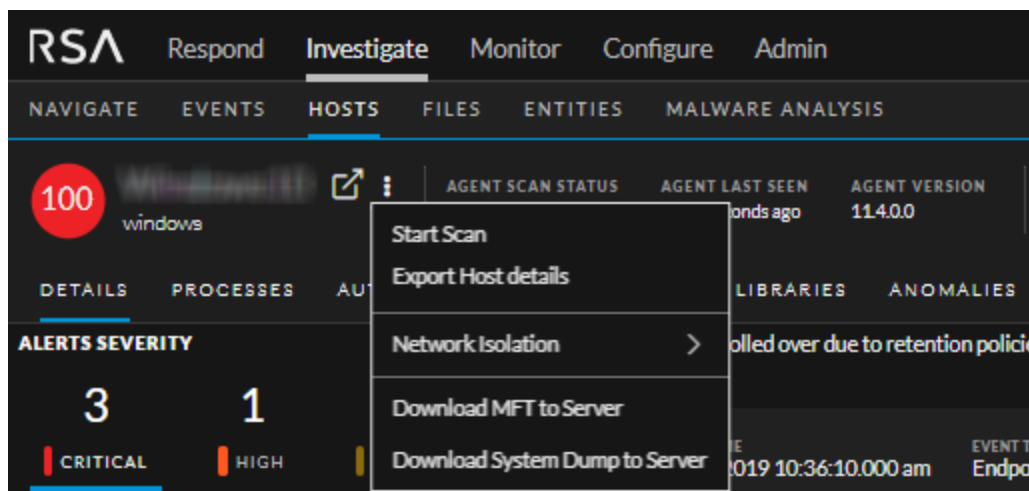
Download System Dump to Server

To download system dump to the server from the Hosts view:

1. Go to **INVESTIGATE > Hosts** and do one the following:
 - Select a host and select **Download System Dump to Server** from the right-click context menu, or from the **More** drop-down list in the toolbar.



- Select the hostname to open the host details and select **Download System Dump to Server** from the **More** option besides the hostname.

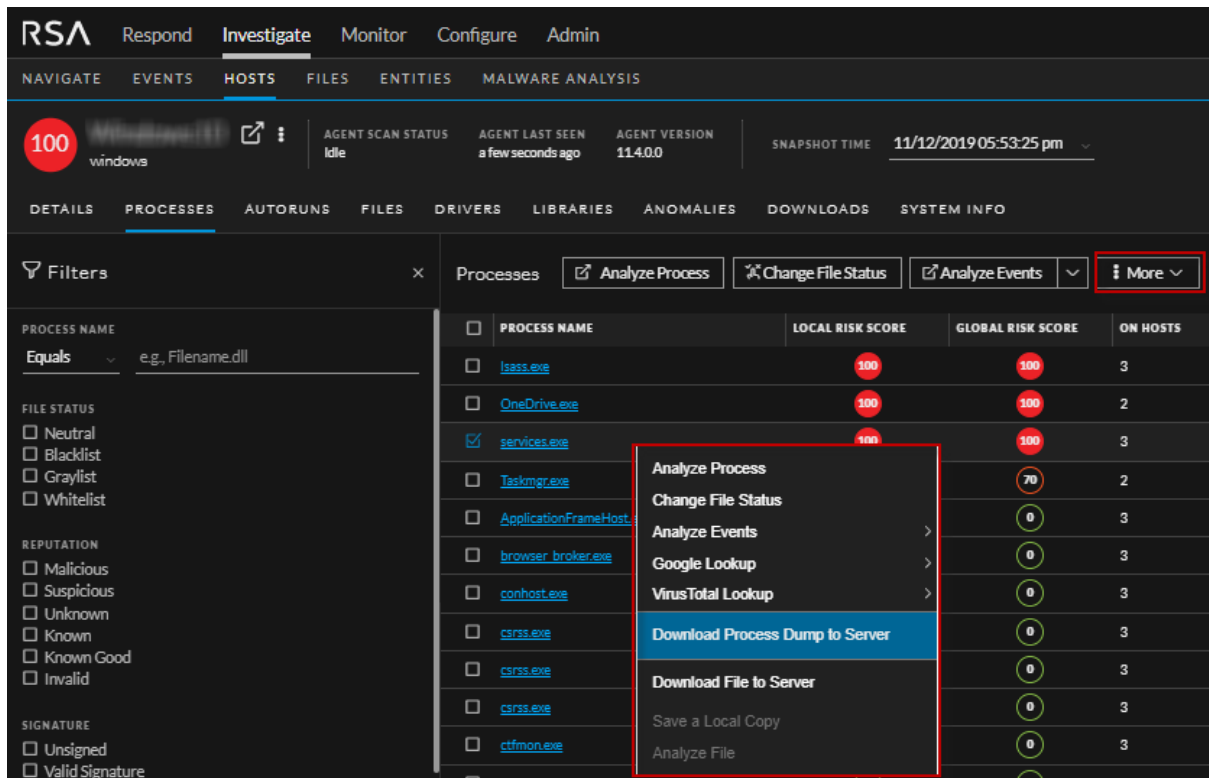


2. View the details of the downloaded system dump in the **Downloads** tab within the host details. For more information, see [Hosts View - Downloads Tab](#).

Download Process Dump to Server

To download process dump to the server:

1. Go to **INVESTIGATE > Hosts**.
2. Select the hostname to open the host details.
3. In the Processes, Libraries, or Anomalies tab, select **Download Process Dump to Server** from the right-click context menu, or from the **More** drop-down list in the toolbar.



4. View the details of the download process dump in the **Downloads** tab within the host details. For more information, see [Hosts View - Downloads Tab](#).

To filter, save, and delete system dump or process dump, see [Filter Downloaded Files](#), [Save Downloaded File](#), and [Delete Downloaded Files](#).

The following are some errors you might encounter during system and process dump download:

Issue	Explanation
Parameter is incorrect.	The process for which the dump is requested might be running with a different process ID.
Element not found	The process for which the dump is requested is no longer active.
java.io.IOException:Unable to unwrap data, invalid status [CLOSED]	Connection to the agent is interrupted.
java.net.SocketTimeoutException	The network is slow or the system is down.
One or more arguments are not correct	Agent might be in the Insight mode or driver is not running.

Filter Downloaded Files

You can filter the downloaded files on file type, file name, SHA256 (for files), and downloaded time. In the Downloaded Time field, you can also filter by custom date.

The screenshot shows the NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this is a sub-navigation bar with 'NAVIGATE', 'EVENTS', 'HOSTS' (selected), 'FILES', 'ENTITIES', and 'MALWARE ANALYSIS'. The main header area shows '71 windows' with a status of 'Idle' and 'AGENT VERSION 11.4.0.0'. The 'DOWNLOADS' tab is selected in the sub-navigation bar. On the left, there is a 'Filters' panel with 'SAVED FILTERS' and 'FILE TYPE' (MFT, File, Process Dump, System Dump). The 'FILE NAME' filter is set to 'Equals' with the value 'e.g., Filename.dll'. The 'SHA256' filter is set to 'Equals' with the value 'Enter Value'. The 'DOWNLOADED TIME' filter is set to 'CUSTOM DATE'. The main table displays a list of downloaded files with columns: FILE NAME, TYPE, DOWNLOADED, SIZE, DOWNLOADED TIME, and SHA256. The table shows 51 files, with the first 10 visible. The 'Save a Local Copy' and 'Delete File' buttons are visible above the table.

FILE NAME	TYPE	DOWNLOADED	SIZE	DOWNLOADED TIME	SHA256
systemdump-INGSMUDALPL6C-2019-...	SYSTEMDUMP	⚠	0 bytes	an hour ago	NA
processdump-19628-git-bash.exe-ING...	PROCESSDUMP	✓	51.7 MB	2 hours ago	NA
systemdump-INGSMUDALPL6C-2019-...	SYSTEMDUMP	⚠	0 bytes	2 hours ago	NA
processdump-18676-notepad++.exe-L...	PROCESSDUMP	✓	138.8 MB	2 hours ago	NA
processdump-6328-cmd.exe-INGSMU...	PROCESSDUMP	⚠	0 bytes	2 hours ago	NA
mft-C:INGSMUDALPL6C-2019-11-29...	MFT	✓	756.0 MB	2 hours ago	NA
MSIPAuth.ni.dll	FILE	✓	122.0 KB	2 hours ago	2d0a2b32cd6c2f7f90760fc23...
libatk-1.0-0.dll	FILE	✓	159.6 KB	2 hours ago	718e569d24ea6a0dfe44efaa...
harpoon.dll	FILE	✓	65.0 KB	2 hours ago	946fb8f6a2292ed048a6b77f...
libwimp.dll	FILE	✓	96.8 KB	2 hours ago	670205c1fd046a50f6a9c82d...
MSIPRMS.ni.dll	FILE	✓	394.0 KB	2 hours ago	22915b5e5bd443e9db19c85b...

Showing 51 out of 51 files | 0 selected

Click **Save** to save the filter 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.

Save Downloaded File

You can retrieve the downloaded file and save it to your local file system for further analysis. To save the file:

1. Go to **INVESTIGATE > Hosts**.
2. Select the hostname to open the host details and select the **Downloads** tab.
3. Right-click the file you want to save and select **Save a Local Copy** from the context menu or from the toolbar.



3. Right-click one or more files you want to delete, and select **Delete File** from the context menu or

from the toolbar.

The screenshot shows the NetWitness Investigate interface. The top navigation bar includes 'Respond', 'Investigate' (selected), 'Monitor', 'Configure', and 'Admin'. Below this is a sub-navigation bar with 'NAVIGATE', 'EVENTS', 'HOSTS' (selected), 'FILES', 'ENTITIES', and 'MALWARE ANALYSIS'. The main header area displays '71 windows' with a status of 'Idle', 'AGENT LAST SEEN' as 'a few seconds ago', and 'AGENT VERSION' as '11.4.0.0'. The sub-navigation bar also includes 'DETAILS', 'PROCESSES', 'AUTORUNS', 'FILES', 'DRIVERS', 'LIBRARIES', 'ANOMALIES', 'DOWNLOADS' (selected), and 'SYSTEM INFO'. The 'Downloads' section is active, showing a list of files with columns for 'FILE NAME', 'TYPE', 'DOWNLOADED', and 'SIZE'. A 'Filters' sidebar on the left allows filtering by 'FILE TYPE' (MFT, File, Process Dump, System Dump) and 'FILE NAME' (Equals, e.g., Filename.dll). The 'Downloads' table lists several files, including system and process dumps, and DLLs. A context menu is open over the file 'mft-C-INGSMUDALPL6C-2019-11-29-...', showing 'Save a Local Copy' and 'Delete File' options.

FILE NAME	TYPE	DOWNLOADED	SIZE
systemdump-INGSMUDALPL6C-2019-...	SYSTEMDUMP	⚠	0 bytes
processdump-19628-git-bash.exe-ING...	PROCESSDUMP	✓	51.7 MB
systemdump-INGSMUDALPL6C-2019-...	SYSTEMDUMP	⚠	0 bytes
processdump-18676-notepad++.exe-I...	PROCESSDUMP	✓	138.8 MB
processdump-6328-cmd.exe-INGSMU...	PROCESSDUMP	⚠	0 bytes
mft-C-INGSMUDALPL6C-2019-11-29-...			756.0 MB
MSIPAuth.ni.dll			122.0 KB
libatk-1.0-0.dll			159.6 KB

Analyzing Events

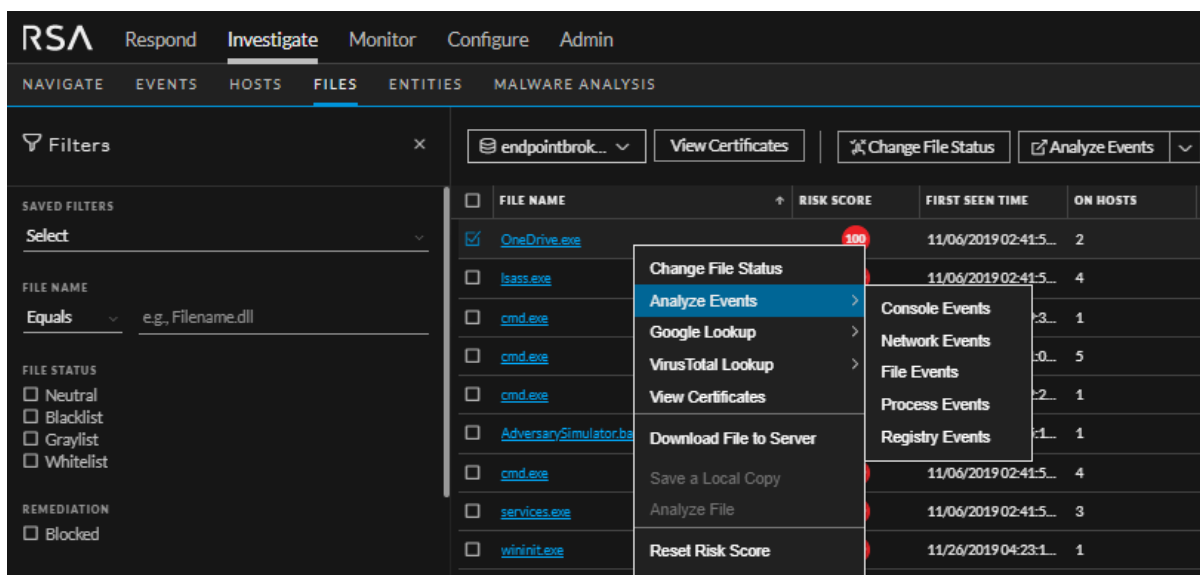
If you need to investigate a particular host, IP address, username, filename, or hash to look for related activity across a time range, you can pivot to Navigate view to get the entire context of the activity. By default, the time range is set to 7 days. You can change the time range.

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 Events views, see the *NetWitness Investigate User Guide*.

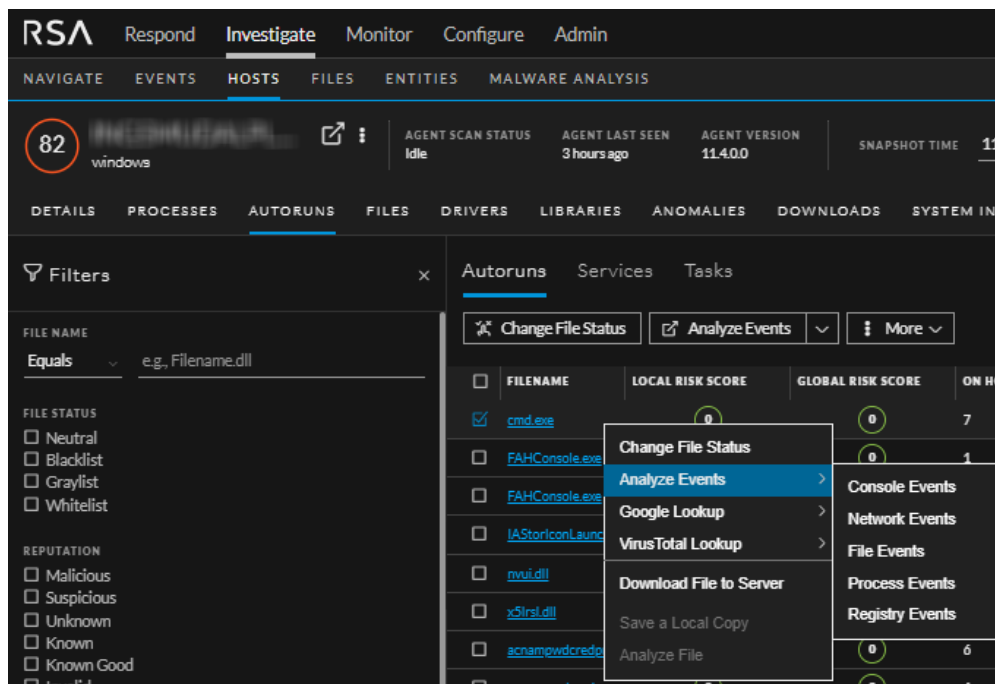
Note: If the values are not indexed, the results take time to load. For more information, see [Troubleshooting NetWitness Endpoint](#).

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:
 - Right-click a host, select **Analyze Events** from the right-click context menu or in the toolbar, and select a specific event type (such as network events, file events) that you want to view.
 - Select the hostname to open the host details. Right-click a file or in the toolbar, select **Analyze Events**, and select a specific event type 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 Events 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 Events 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 shows the NetWitness Endpoint interface. On the left, a list of events is displayed with columns for Collection Time, Type, and Event Time. The selected event is a Process event for Endpoint, dated 03/14/2019 09:41:34 am. The detailed view on the right shows the event details, including the process name, session ID, and a large meta value containing a long command string.

COLLECTION TIME	TYPE	EVENT TIME
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36...

SESSION ID	TIME	SIZE	FORWARD.IP	IP.ALL	MEDIUM	DEVICE TYPE	DIR.PATH.SRC	DIR.PATH.ALL	DIR.PATH.SRC	DIR.PATH.ALL	CONTEXT.SRC	CONTEXT.ALL	CONTEXT.SRC	CONTEXT.ALL
6965	03/14/2019 09:36:26 am	606	10.10.10.10	10.10.10.10	32	endpoint	windows	windows	windowsSystem32	windowsSystem32	file found	file found	file protected	file protected

PROCESS EVENT

03/14/2019 09:36:26 am WmiPrvSE.exe PERFORMED openBrowserProcess chrome.exe

LARGE META VALUES

param.dst=chrome.exe --type=crashpad-handler --user-data-dir=C:\Users\...AppData\Local\Google\Chrome\User Data --prefetch:7 --monitor-self-annotation-type=crashpad-handler --database=C:\Users\...AppData\Local\Google\Chrome\User Data\Crashpad --metrics-dir=C:\Users\...AppData\Local\Google\Chrome\User Data --url=https://clients2.google.com/cr/report --annotation-channel= --annotation-plat-win64 --annotation-prod-chrome --annotation-ver=73.0.3683.75 --initial-client-data=0x1e0,0x1e4,0x1e8,0x1ec,0x7fa64916830,0x7ffa64916840,0x7ffa64916850

Below is an example of the Network event:

The screenshot shows the NetWitness Endpoint interface. On the left, a list of events is displayed with columns for Collection Time, Type, and Event Time. The selected event is a Network event for Endpoint, dated 03/14/2019 09:41:34 am. The detailed view on the right shows the event details, including the network connection, session ID, and a large meta value containing a long command string.

COLLECTION TIME	TYPE	EVENT TIME
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34...

SESSION ID	TIME	SIZE	FORWARD.IP	IP.ALL	MEDIUM	DEVICE TYPE	PORT.DST	PORT.ALL	PORT.DST.ALL	DIR.PATH.SRC	DIR.PATH.ALL	CONTEXT.SRC	CONTEXT.ALL	CONTEXT.SRC	CONTEXT.ALL
6768	03/14/2019 09:41:15 am	332	10.10.10.10	10.10.10.10	32	endpoint	10003	10003	10003	programFiles	programFiles	file.autorun	file.autorun	file found	file.creandir.asMorph

NETWORK EVENT

03/14/2019 09:41:15 am SecureConnector.exe MADE A NETWORK CONNECTION TO 10.254.20.237 FROM 10.87.157.55

LARGE META VALUES

param.src=SecureConnector.exe --performer -id AD6AB2C2CA554FB9AC31998B7DC7148 -token c22114e7017e841b6392af5404293ee4608269dc -ip 10.254.20.237 -port 10003 -sha256 34E3B6B14BC6F9C0D0E8BC0B891F442F7291DB8F04093558BD220252028B50 -l cif 7 -event FSA_THP_5388_5C89DE73_0002PERFORMER_CMTL -rrd 0

For more information on Events view, see the *NetWitness Investigate User Guide*.

Isolating Hosts from Network

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.4 and later.

Note: By default, the network isolation option is disabled in the policy, and you cannot view options mentioned in this section. To enable network isolation, in the policy configuration, select **Enabled** in the **Network Isolation** option under Response Action Settings. For more information, see the *NetWitness Endpoint Configuration Guide*.

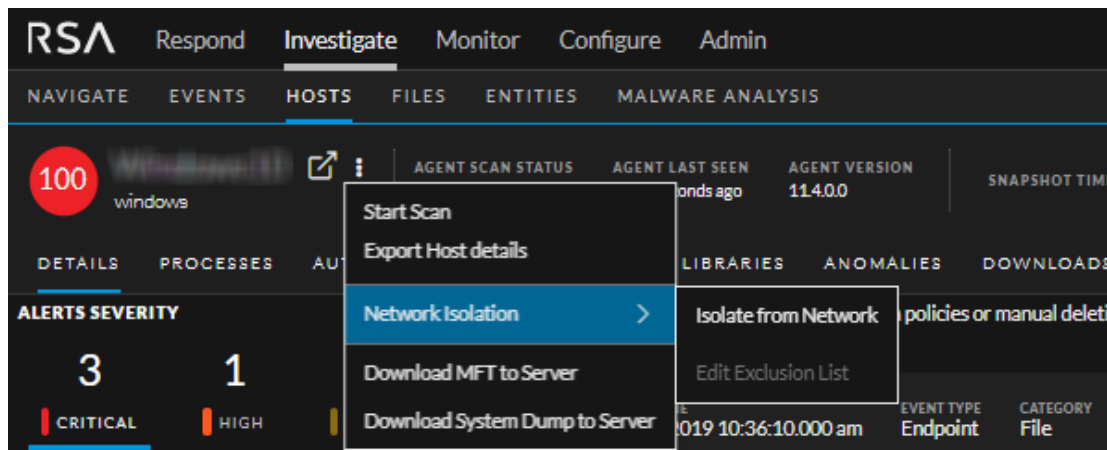
To isolate a host from the network:

1. Go to **INVESTIGATE > Hosts** and do one of the following:
 - Select a host and select **Network Isolation > Isolate from Network** from the right-click context menu, or from the **More** drop-down list in the toolbar.

The screenshot shows the RSA NetWitness Investigate interface. The 'HOSTS' tab is selected in the top navigation bar. On the left, there are filters for Host Status (Managed, Roaming, Isolated) and Risk Score (0 to 100). The main table lists hosts with columns: HOSTNAME, RISK SCORE, OPERATING SYS, LAST SCAN TIME, USERNAME, and AGENT LAST SEEN. A context menu is open for a host, showing options: Analyze Events, Delete, Start Scan, Stop Scan, Network Isolation (highlighted), Download MFT to Server, Download System Dump to Server, and Reset Risk Score. The 'Network Isolation' option has a sub-menu with 'Isolate from Network' and 'Edit Exclusion List'.

HOSTNAME	RISK SCORE	OPERATING SYS	LAST SCAN TIME	USERNAME	AGENT LAST SEEN
WIN101511X64...	100	windows	11/29/2019 05:23:41 ...	WIN101511X64...	a few seconds ago
DESKTOP-FQJ50E...	100	windows	11/28/2019 04:54:45 ...	DESKTOP-FQJ50E...	a day ago
206EPS21ecatWL...	N/A	windows	11/18/2019 10:40:28 ...	206EPS21ecatWL...	2 days ago
WIN10-1809-X64...			11/11/2019 02:41:06 ...	WIN10-1809-X64...	a few seconds ago
WINDOWS10\ecat...			11/12/2019 05:53:25 ...	WINDOWS10\ecat...	a few seconds ago
ADMIN-PC\Admini...			11/18/2019 09:28:10 ...	ADMIN-PC\Admini...	3 days ago
Window Manager\...			11/27/2019 06:30:05 ...	Window Manager\...	5 hours ago
					4 days ago
					a day ago
Window Manager\...			11/11/2019 01:07:04 ...	Window Manager\...	a few seconds ago
			11/25/2019 05:33:36 ...		3 days ago
WIN1809-0\ecatW...			11/08/2019 10:45:15 ...	WIN1809-0\ecatW...	21 days ago

- Select the hostname to open the host details, click **(More)** beside the hostname, and select

Network Isolation > Isolate from Network.

2. In the Isolate from Network dialog, by default, a set of IP addresses are excluded from isolation. For more information, see [Network Isolation](#). To add IP addresses to the list, select the **Add your IPs to Exclusion List** checkbox. You can enter up to 100 IP addresses separated by comma.

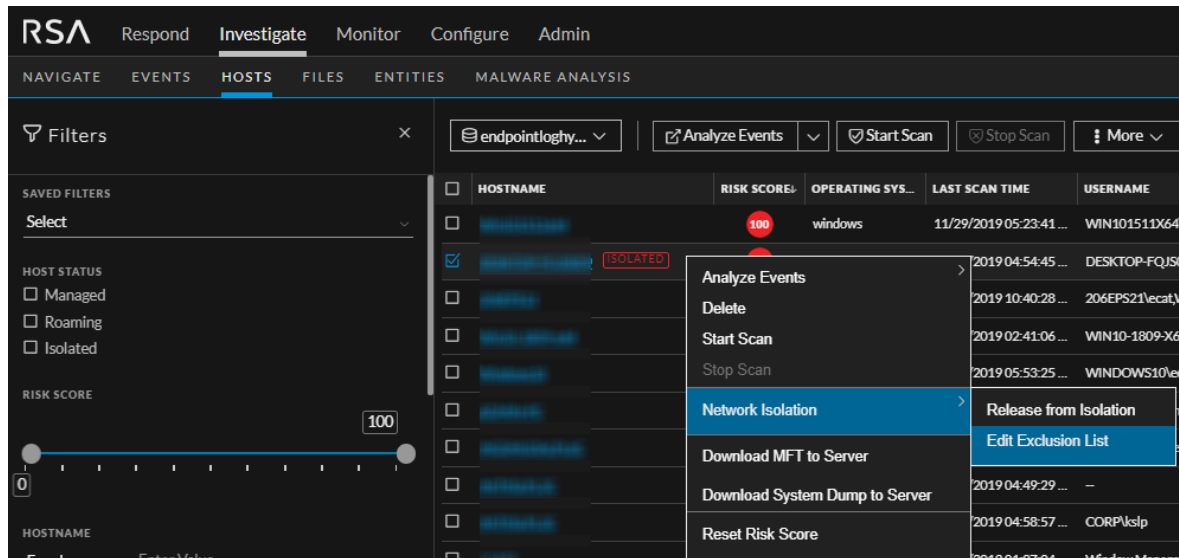
A screenshot of the 'Isolate from Network' dialog box. The title bar is blue with the text 'Isolate from Network' and a close button (X). The main content area has a dark background with white text. It starts with a description: 'Network Isolation blocks the host from connecting to the network. All attempted network connections are monitored and reported to the Endpoint Server.' Below this is a checkbox labeled 'Add IP addresses to the Exclusion List' which is checked. Under the checkbox, it says: 'Default IP addresses excluded from isolation include Endpoint Server, Relay Server, DNS, DHCP, Gateways, 0.0.0.0 and 255.255.255.255.' There is a text input field with the placeholder text: 'Enter one or more valid IPv4 and IPv6 addresses. Use commas to separate multiple values.' Below the input field is a section labeled 'COMMENTS' with a text area containing the placeholder 'Enter comments'. At the bottom right are two buttons: 'Cancel' and 'Isolate Host'.

3. Enter comments.
4. Click **Isolate Host**.

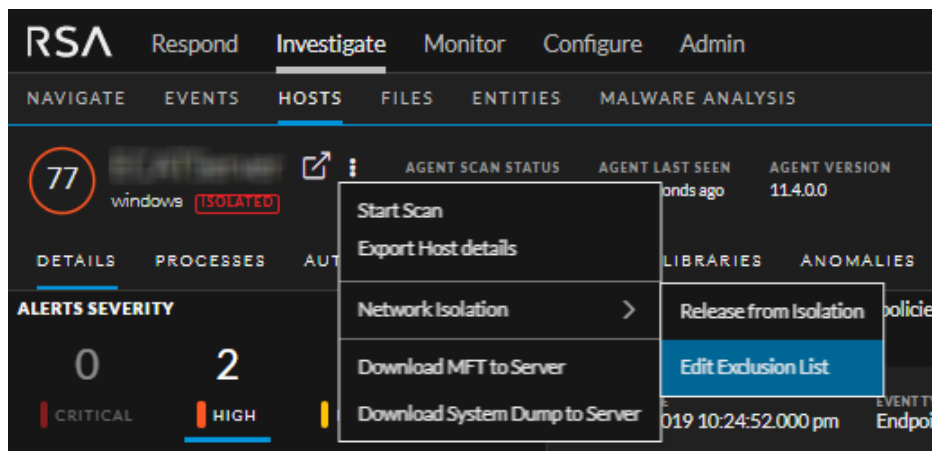
Edit Exclusion List

To edit the exclusion list:

- Go to **INVESTIGATE > Hosts** and do one of the following:
 - Select a host and select **Network Isolation > Edit Exclusion List** from the right-click context menu, or from the **More** drop-down list in the toolbar.



- Select the hostname to open the host details, click **(More)** beside the hostname, and select **Network Isolation > Edit Exclusion List**.

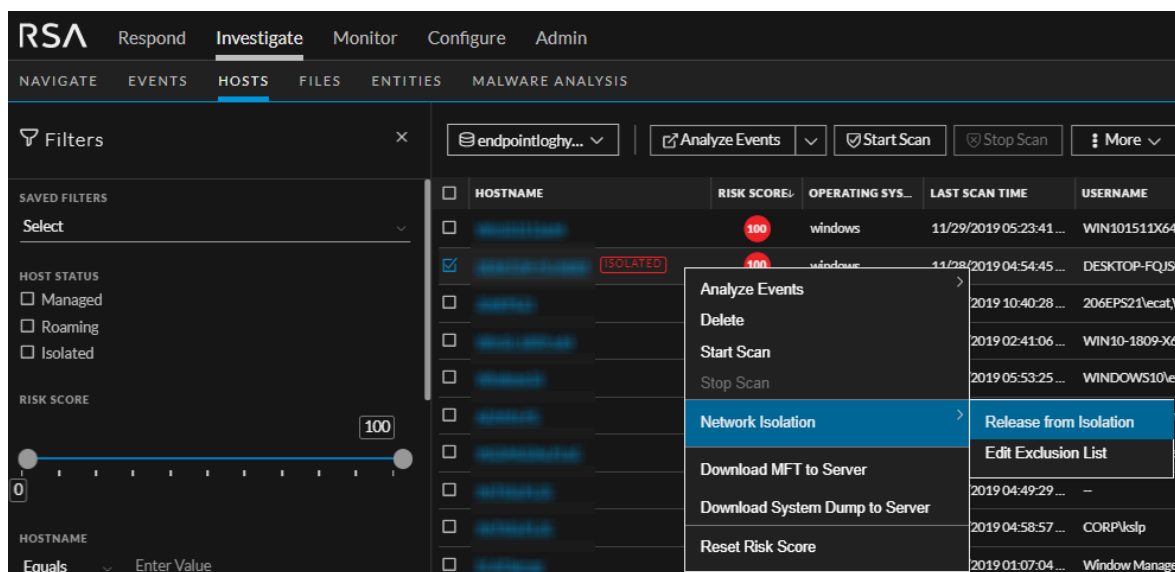


- Add or modify the IP addresses in the list.
- Enter comments and click **Save**.

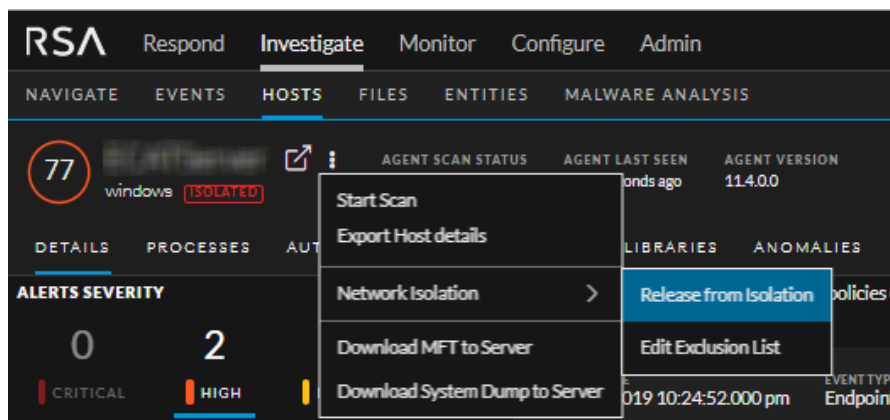
Release Isolated Hosts

Releasing the isolated host restores the network connection and removes IP addresses added to the Exclusion list. To release the host from isolation:

- Go to **INVESTIGATE > Hosts** and do one of the following:
 - Select a host and select **Network Isolation > Release from Isolation** from the right-click context menu, or from the **More** drop-down list in the toolbar.



- Select the hostname to open the host details, click **(More)** beside the hostname, and select **Network Isolation > Release from Isolation**.



- Enter comments and click **Release Host**.

NetWitness Endpoint with Third-Party Antivirus Products

If you want the NetWitness Endpoint agent to coexist with any of the security products, make sure to whitelist the agent. For more information, see the respective third-party product documentation.

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	The Endpoint Broker aggregates data from all Endpoint Servers, which responds within 10 seconds. You must increase the query timeout value to see the result of Endpoint server that is online. Perform the following: 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	The Endpoint Agent is unable to communicate with the Endpoint Server. The connection may not be established due to any of the following issues: • UDP • HTTPS • Firewall
Solution	• To verify the UDP or HTTPS connection, you must verify the connection between Windows Endpoint Agent and Endpoint Server: 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> For example, NWEAgent.exe /testnet • If the issue is with the firewall, check the incoming and outgoing firewall rules.

Issue	The Endpoint Agent is unable to communicate with the Log Decoder. The connection may not be established due to any of the following issues: • UDP • TCP
-------	--

Solution	• TLS • Firewall
	• To verify the UDP, TCP, and TLS connection, you must verify the connection between Windows Endpoint Agent and the Log Decoder: 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> For example, NWEAgent.exe /testlognet
	• If the issue is with the firewall, check the incoming and outgoing firewall rules.

Multi-server Issue

Issue	Agent is not communicating with the Endpoint Server after migration.
Solution	Check the Nginx logs of the Endpoint Server to which the agent has migrated, and if the agent is communicating with error code 403, that means the certificate of the first Endpoint Server and second Endpoint Server are different. This is because during the installation of second Endpoint Server, the certificate of first Endpoint Server is not copied to the second Endpoint Server. Reinstall the second Endpoint Server by copying the certificate of first Endpoint Server, and reinstall the agent. For more information, see the <i>Physical Host Installation Guide</i>.

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.

Files View Issues

Issue	Unable to analyze events from Investigate > Hosts and Files view.
Explanation	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:

Note: To get the investigate-service-id:

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.

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

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 in the Agent-Driver Error Code column under Investigate > Hosts view. 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	You must manually enable the File Reputation service. To enable the File Reputation service: 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	Check the backlog of alerts for risk scoring. 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()' --quiet</pre> 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 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 - Downloads Tab](#)
- [Hosts View - System Information Tab](#)

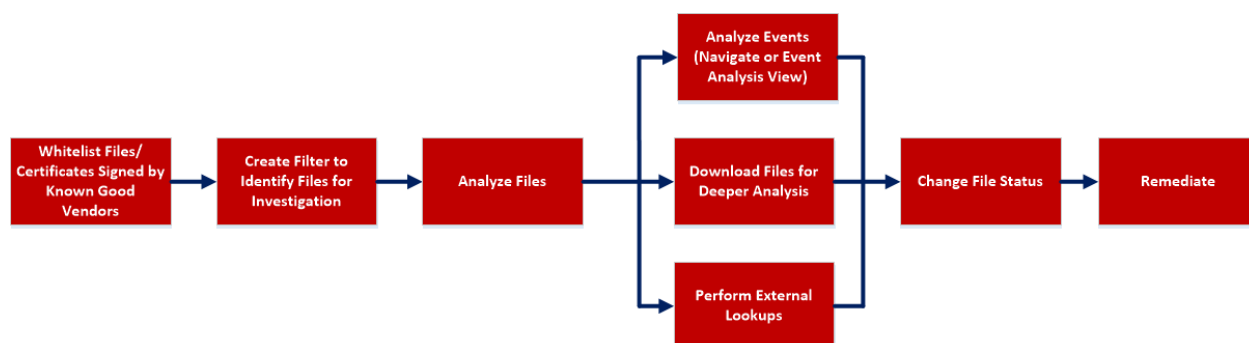
Files View

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:

The screenshot shows the NetWitness Endpoint interface with the 'Files' view selected. The interface includes a top navigation bar with tabs for 'Investigate', 'Monitor', 'Configure', and 'Admin'. The 'Files' tab is active, and the ' endpointlook' dropdown is set to 'View Certificates'. The main panel displays a table of files with columns for File Name, Risk Score, First Seen Time, On Hosts, Reputation, Size, and Signature. A 'Filters' panel on the left allows filtering by File Name, File Status, Remediation, Reputation, and Risk Score. A 'File Details' panel on the right shows details for the selected file, 'OneDrive.exe'. A context menu is open over the table, showing options like 'Type to filter the list', 'File Name', 'Risk Score', 'On Hosts', 'File Status', 'Reputation', 'Downloaded', 'Size', 'Signature', 'First Seen Time', 'Operating System', 'Signature Timestamp', 'Signature', and 'MD5'. The table shows 100 files, with the first 10 displayed. The 'OneDrive.exe' file is highlighted in the table and its details are shown in the right panel.

- 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 top 100 hosts based on the risk score on which the file is 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](#).

File Details View

To access this view, go to **INVESTIGATE > Files**, and select a file. Below is an example of the File Details view:

The screenshot displays the NetWitness Endpoint Investigate interface. At the top, the navigation bar includes Respond, Investigate (selected), Monitor, Configure, and Admin. Below this, the main navigation tabs are NAVIGATE, EVENTS, HOSTS, FILES, ENTITIES, and MALWARE ANALYSIS. The FILES tab is active, showing a summary of 100 files, 2 on hosts, a signed valid signature, 1.4 MB size, and a Blacklisted status. A red box labeled '1' highlights this summary. Below the summary, the DETAILS tab shows ALERTS SEVERITY with counts for CRITICAL (1), HIGH (0), MEDIUM (0), and ALL (1). A red box labeled '2' highlights the CRITICAL alert. The ANALYSIS tab shows a list of events with columns for EVENT TIME, EVENT TYPE, CATEGORY, ACTION, HOSTNAME, USER ACCOUNT, OPERATING SYSTEM, and FILE NAME. A red box labeled '3' highlights the first event row. On the right, the FILE DETAILS panel is open, showing general information (File Name: OneDrive.exe, Entropy: 4.283913667539894, Size: 1.4 MB, Format: pe) and signature information (Features: signed valid, Timestamp: 01/12/2019 12:33:39.626 am, Thumbprint: 23710f52824b1c361649ed4a3d..., Signer: Microsoft Corporation). A red box labeled '4' highlights the FILE DETAILS panel.

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).

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.

On Hosts - Indicates the number of hosts on which a file exist.

Signature - Provides signatory information.

Size - Size of the file.

File Status - Status of the file. For example, Neutral.

2 Details tab - Displays list of distinct alerts, such as Critical, High, Medium and All, along with the total number of events associated with the alert.

Analysis tab - Provides detailed information about a downloaded file. For more information, see [Analyzing Downloaded Files](#).

3 Displays events for an alert and metadata associated with a specific event.

4 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.

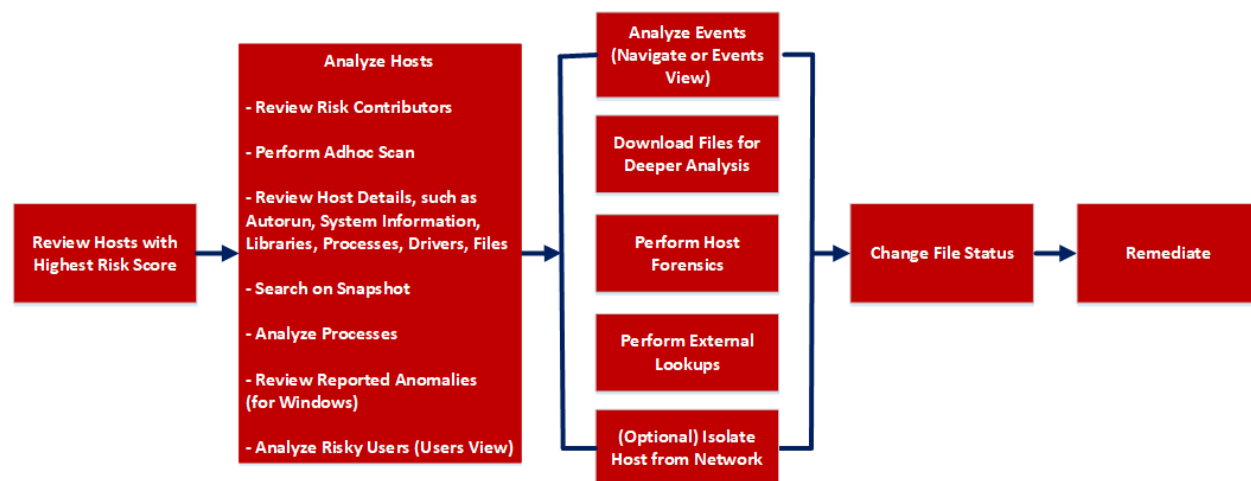
Hosts - Displays the hosts on which file activities are present. For more information, see [Analyze Hosts with File Activity](#).

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

User Role	I want to ...	Show me how
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
Threat Hunter	filter files*	Investigating Hosts
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT*, system dump*, or process dump	Performing Host Forensics

*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](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

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](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).

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

3 Sort Columns. Lets you sort 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.

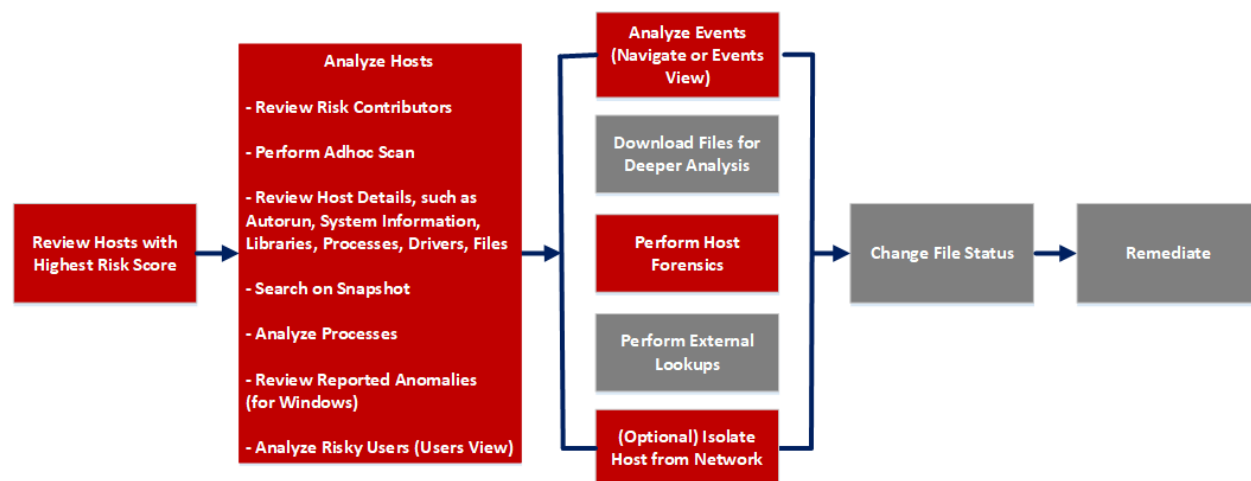
Risk details - Displays the distinct alerts associated with the risk score.

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

User Role	I want to ...	Show me how
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
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT* , system dump, or process dump*	Performing Host Forensics

*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Events](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

Quick Look

Below is an example of the 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 tabs for NAVIGATE, EVENTS, HOSTS, FILES, ENTITIES, and MALWARE ANALYSIS. The main content area is divided into several sections:

- Alerts Severity:** A summary of alerts categorized by severity: 5 Critical, 2 High, 10 Medium, and 17 All.
- Host Details:** A section for the selected host (WIN101511X64) showing scan status (Idle), agent last seen (5 hours ago), agent version (11.4.0.0), and snapshot time (01/02/2020 02:32:50 pm).
- Processes:** A list of processes running on the host, including cmd.exe and reg.exe.
- Host Details (WIN101511X64):** A detailed view of the host's session, including session ID (2), groups (Administrators, Remote Desktop, etc.), and network interfaces.
- Host Details (WIN101511X64):** A detailed view of the host's session, including session ID (1), groups (Administrators, Remote Desktop, etc.), and network interfaces.
- Host Details (WIN101511X64):** A detailed view of the host's session, including session ID (1), groups (Administrators, Remote Desktop, etc.), and network interfaces.
- Host Details (WIN101511X64):** A detailed view of the host's session, including session ID (1), groups (Administrators, Remote Desktop, etc.), and network interfaces.

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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

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

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

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

4 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.

5 Policy Details Panel - Displays the following:

- 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.
- Relay Server. Displays the Relay Server details.
 - Server - Host name or IP address of the Relay Server.
 - Port - Port number.
 - HTTP Beacon Interval - HTTP beacon interval value in minutes.
- Complete resolved policy settings. For more information, see "Managing Policies" in the *NetWitness Endpoint Configuration Guide*.

Note: The values that are not set in the policy are not displayed.

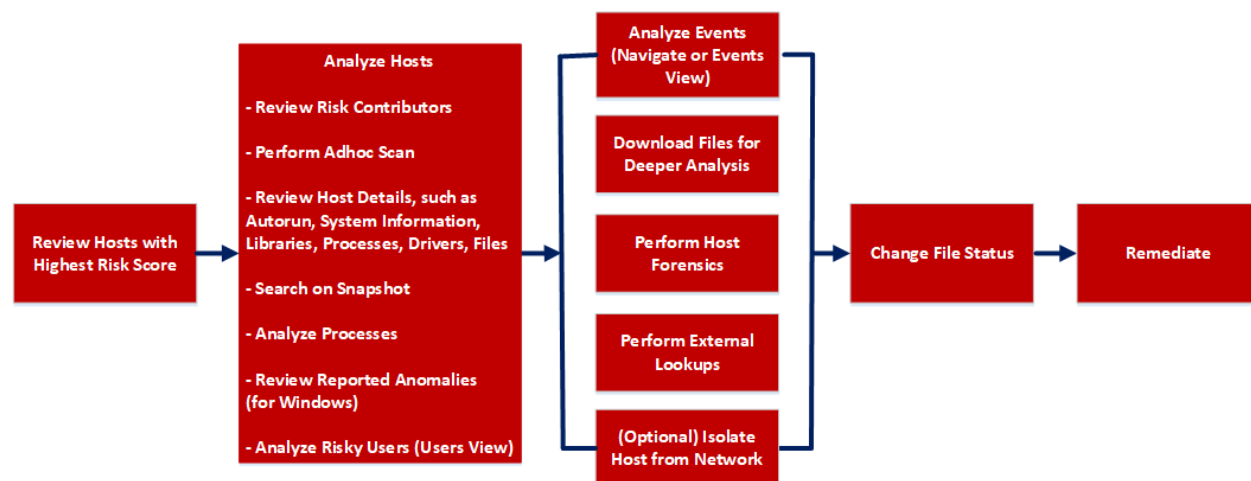
6 Alerts Severity - Displays list of distinct alerts, such as Critical, High, Medium and All, along with the total number of events associated with the alert.**7** Displays events for an alert and metadata associated with a specific event. For more information, see [Analyze Hosts Using the Risk Score](#).

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

User Role	I want to ...	Show me how
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
Threat Hunter	filter files*	Investigating Hosts
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

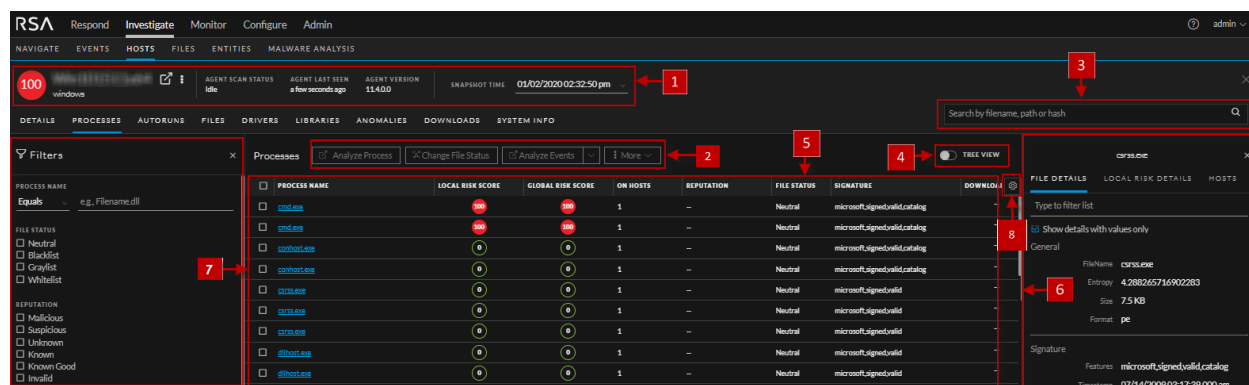
*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Downloaded Files](#)
- [Changing File Status or Remediate](#)
- [Investigating a Process](#)
- [Analyzing Events](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

Quick Look

Below is an example of the Process 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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

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

2 Actions in the toolbar:

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.
- Download process dump to server.

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, On Hosts, reputation status, file status, and others.

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

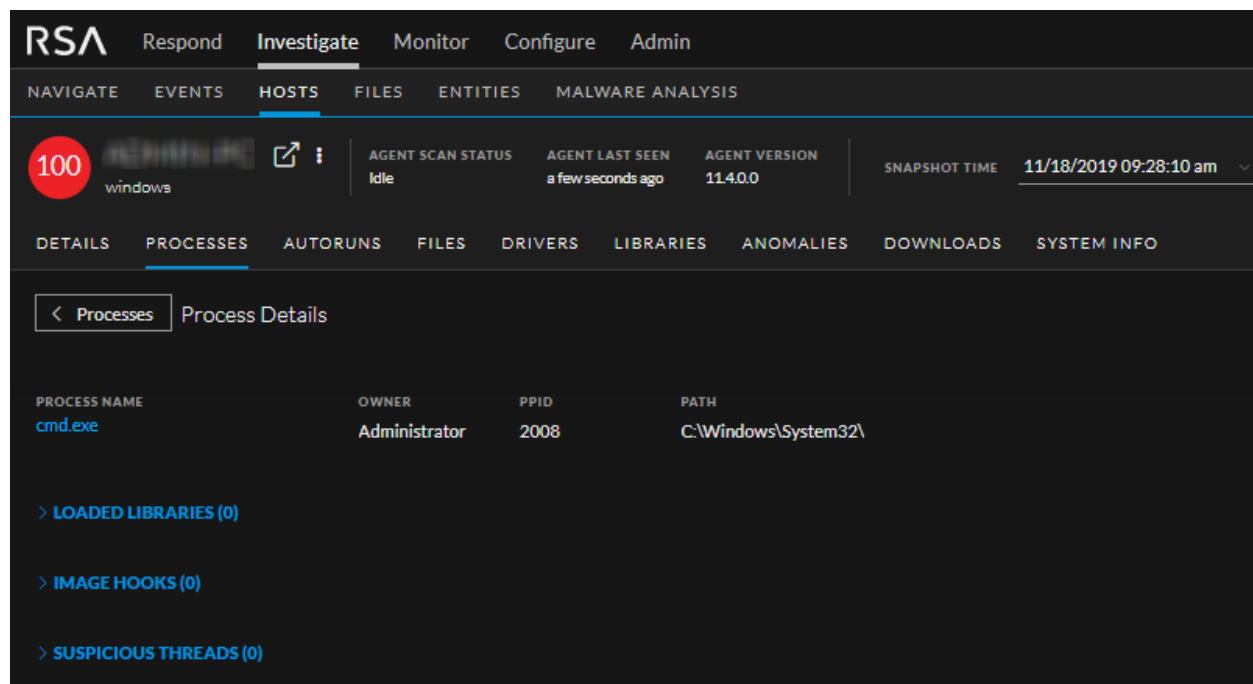
- File Details - Displays all properties of the selected process. It is grouped as follows:
 - General** - General information about the file, such as file name, entropy, size, and format.
 - Signature** - Provides signatory information.
 - Hash** - Hash type of the file (MD5, SHA1, and SHA256).
 - Time** - 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.
- Hosts - Displays the top 100 hosts based on the risk score on which the file is present.

7 Filter Files. You can filter processes by selecting the options in the Filters panel and create filters. For more information, see [Investigating Hosts](#).

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

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> .

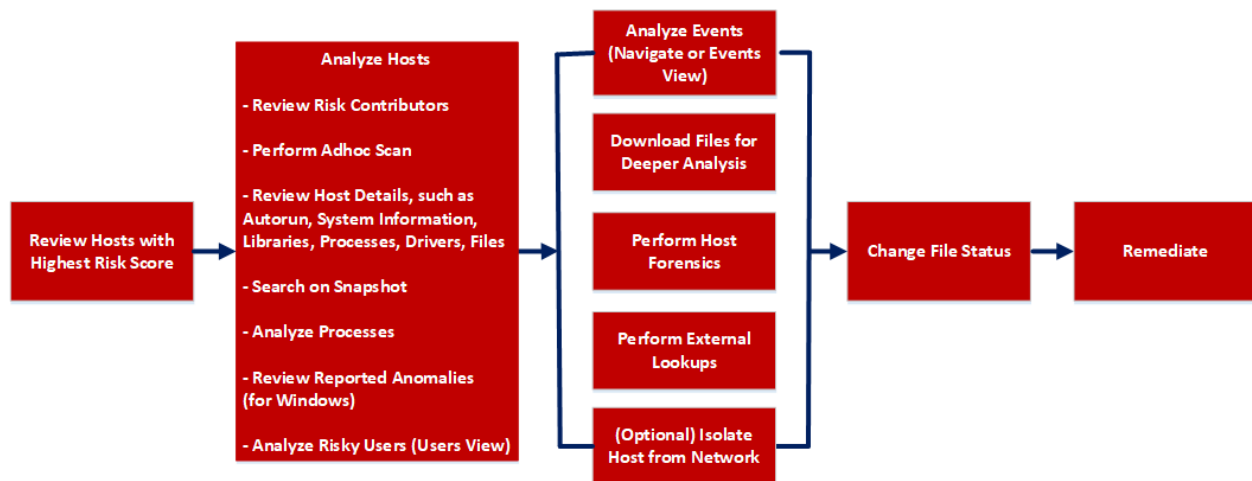
- List of loaded libraries for the selected process, such as DLLs (for Windows), Dylibs (for Mac), or .SO (for Linux).
- List of autoruns (if configured).
- List of image hooks and suspicious threads (for Windows).

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

User Role	I want to ...	Show me how
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
Threat Hunter	filter files	Investigating Hosts
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

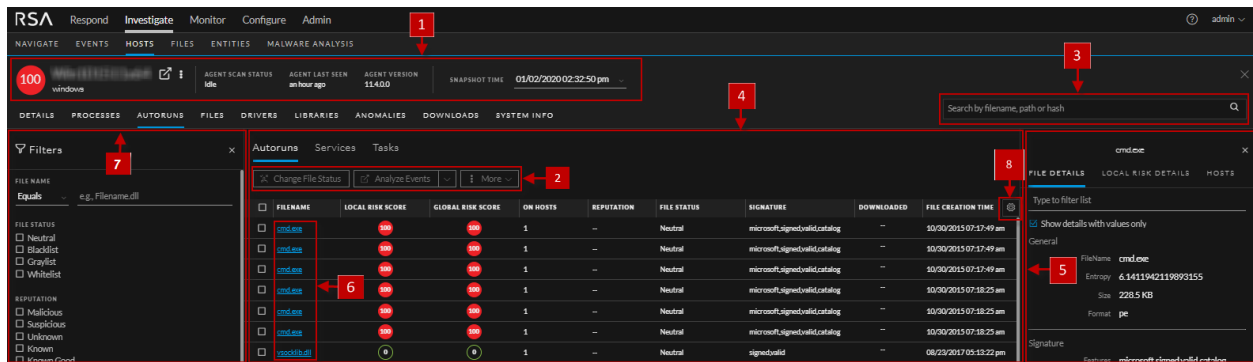
*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Downloaded Files](#)
- [Changing File Status or Remediate](#)
- [Analyzing Events](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

Quick Look

Below is an example of the Autoruns 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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

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

2 Actions in the toolbar:

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 process dump to server.
- 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 autrouns, services, or tasks.

- Local Risk Details - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.
- Hosts -Displays the top 100 hosts based on the risk score on which the file is present.

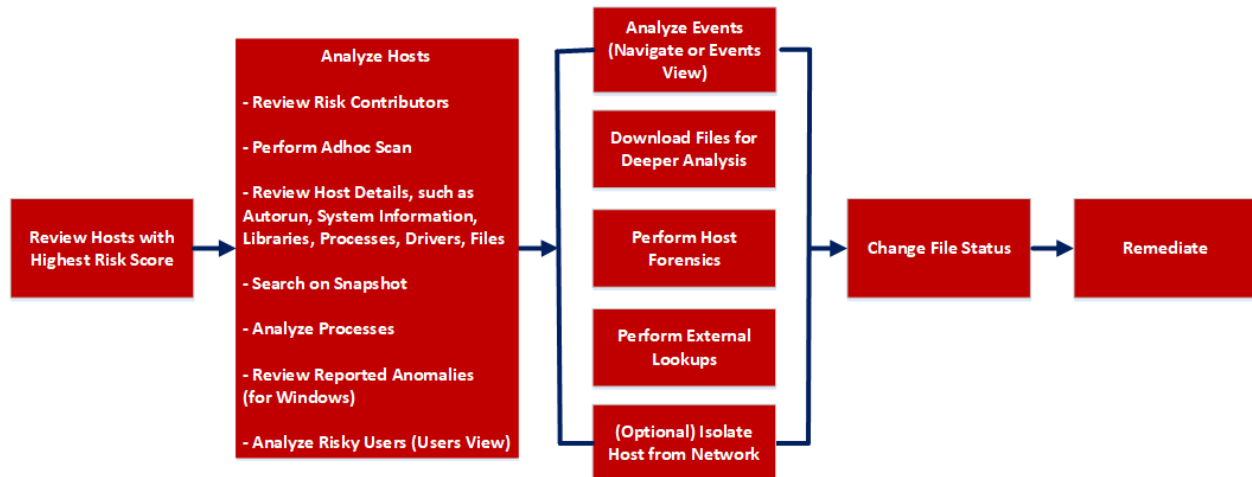
6 Clicking a filename lets you navigate to the Files view for further analysis.**7 Filter Files.** You can filter files by selecting the options in the Filters panel and create filters. For more information, see [Investigating Hosts](#).**8 Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see [Set Hosts Preference](#).

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

User Role	I want to ...	Show me how
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
Threat Hunter	filter files*	Investigating Hosts
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT*, system dump, or process dump*	Performing Host Forensics

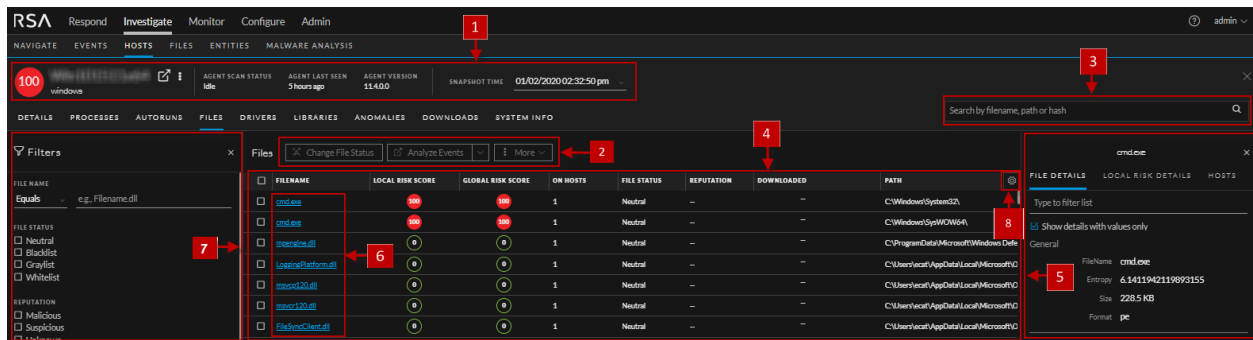
*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Downloaded Files](#)
- [Changing File Status or Remediate](#)
- [Analyzing Events](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

Quick Look

Below is an example of the Files 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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

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

2 Actions in the toolbar:

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 information, such as filename, local risk score, global risk score, on hosts, 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.
- Hosts - Displays the top 100 hosts based on the risk score on which the file is present.

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

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

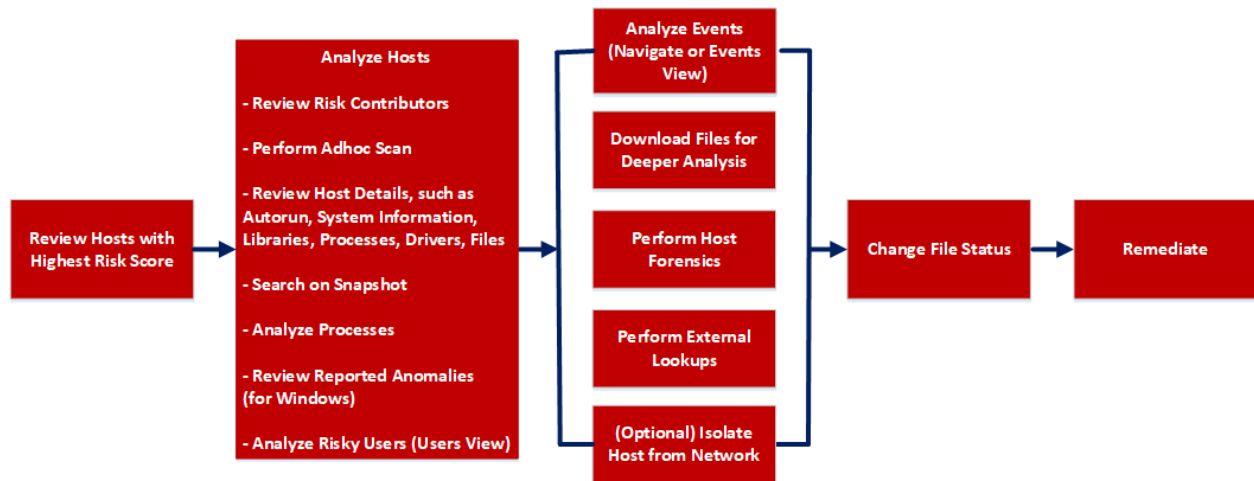
8 Settings Menu. You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see [Set Hosts Preference](#).

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

User Role	I want to ...	Show me how
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
Threat Hunter	filter files*	Investigating Hosts
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT*, system dump, or process dump*	Performing Host Forensics

*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](#)
- [Analyzing Events](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

Quick Look

Below is an example of the Drivers tab:

The screenshot shows the RSA NetWitness Endpoint console. The top navigation bar includes tabs for Respond, Investigate, Monitor, Configure, and Admin. Below this is a search bar and a filter section. The main area displays a table of drivers with columns for File Name, Local Risk Score, Global Risk Score, On Hosts, Reputation, File Status, Signature, and Downloaded. A sidebar on the right shows file details for 'NWEDriver2303.sys'.

FILE NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	SIGNATURE	DOWNLOADED
NWEDriver2303.sys	0	0	2	Neutral	signed/valid		
Meta1442b8d1.sys	0	0	1	Neutral	signed/valid		
NWEDriver2303.sys	0	0	1	Neutral	signed/valid		
cdmapi.dll	0	0	1	Neutral	signed/valid		
cdmapi.dll	0	0	1	Neutral	signed/valid		
cdmapi.dll	0	0	1	Neutral	signed/valid		
cdmapi.dll	0	0	1	Neutral	signed/valid		

File Details for NWEDriver2303.sys:

- FileName: NWEDriver2303.sys
- Entropy: 6.423240674371036
- Size: 243.0 KB
- Format: pe

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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

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

2 Actions in the toolbar:

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, on hosts, reputation status, file status, and others.

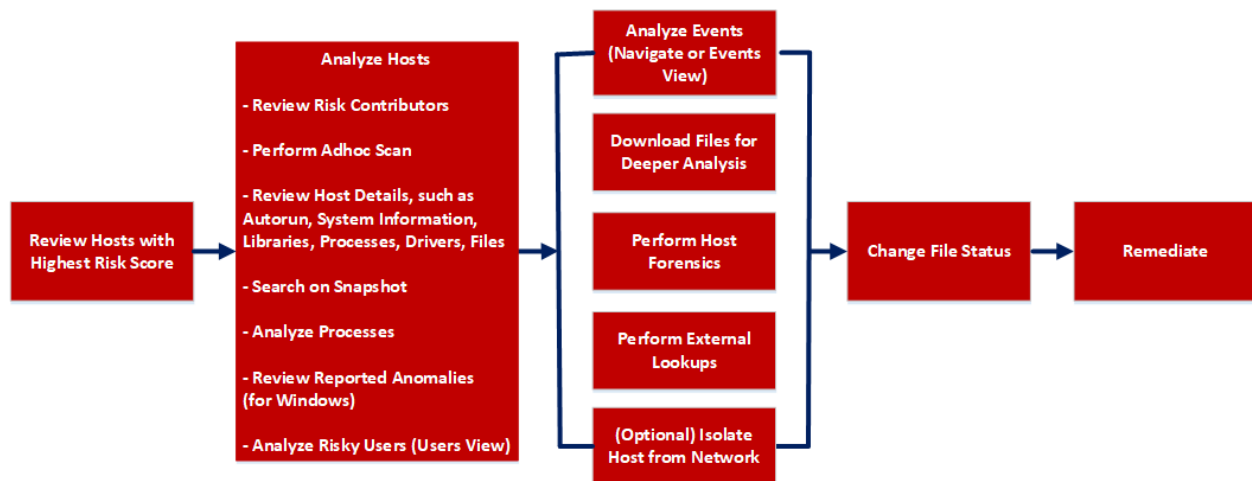
- 5 **Show/Hide Right Panel** - Displays the following properties in the right panel:
 - **File Details** - Displays all properties of the selected process. It is grouped as follows:
 - General** - General information about the file, such as file name, entropy, size, and format.
 - Signature** - Provides 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.
 - **Hosts** - Displays the top 100 hosts based on the risk score on which the file is present.
- 6 Clicking a filename lets you navigate to the Files view for further analysis.
- 7 **Filter Files.** You can filter files by selecting the options in the Filters panel and create filters. For more information, see [Investigating Hosts](#).
- 8 **Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see [Set Hosts Preference](#).

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

User Role	I want to ...	Show me how
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
Threat Hunter	filter files*	Investigating Hosts
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

*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](#)
- [Analyzing Events](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

Quick Look

Below is an example of the Libraries tab:

The screenshot shows the NetWitness Endpoint interface with the Libraries tab selected. Red callouts highlight specific features:

- 1**: Top navigation bar (Respond, Investigate, Monitor, Configure, Admin).
- 2**: Filter buttons (Change File Status, Analyze Events, More).
- 3**: Search bar (Search by filename, path or hash).
- 4**: Libraries table header (PROCESS CONTEXT, FILENAME, LOCAL RISK SCORE, ON HOSTS, GLOBAL RISK SCORE, REPUTAT., FILE STATUS, SIGNATURE, DOWNLOAD, FILE PATH).
- 5**: File details panel (mpengine.dll).
- 6**: File entry in the Libraries table (mpengine.dll).
- 7**: Filters panel (FILE NAME, FILE STATUS, REPUTATION).
- 8**: File details panel (mpengine.dll).

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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

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

2 Actions in the toolbar:

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 process dump to server.
- 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, on hosts, reputation status, file status, and others.

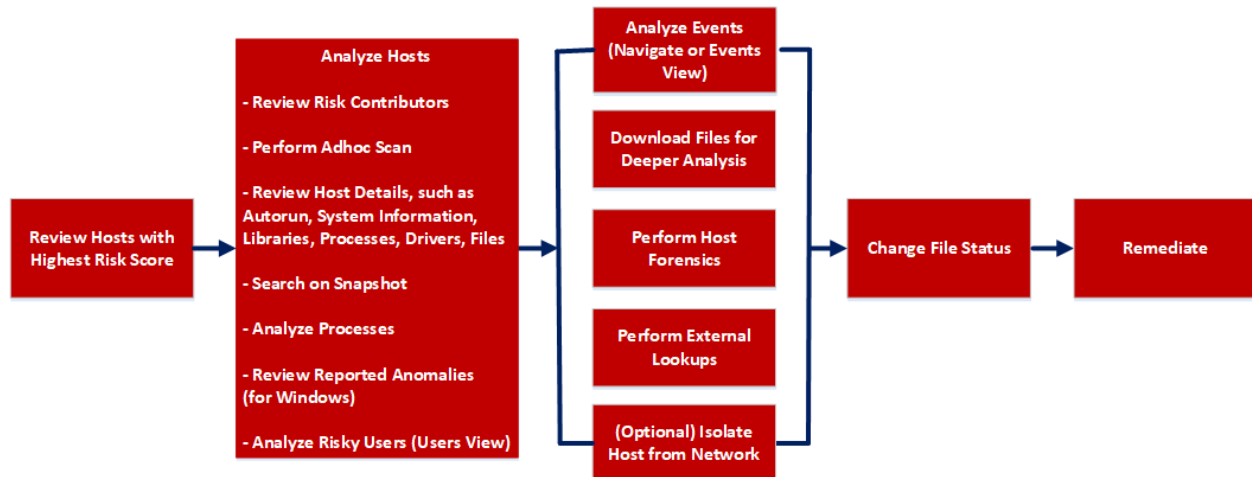
- 5 **Show/Hide Right Panel** - Displays the following properties in the right panel:
 - **File Details** - Displays all properties of the selected process. It is grouped as follows:
 - General** - General information about the file, such as file name, entropy, size, and format.
 - Signature** - Provides 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.
 - **Hosts** - Displays the top 100 hosts based on the risk score on which the file is present.
- 6 Clicking a filename lets you navigate to the Files view for further analysis.
- 7 **Filter Files.** You can filter files by selecting the options in the Filters panel and create filters. For more information, see [Investigating Hosts](#).
- 8 **Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see [Set Hosts Preference](#).

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

User Role	I want to ...	Show me how
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
Threat Hunter	filter files	Investigating Hosts
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

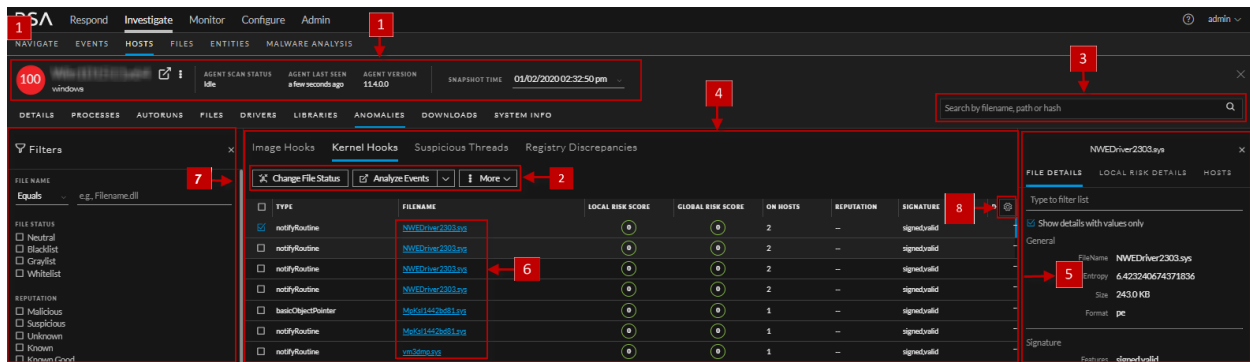
*You can perform this task in the current view.

Related Topics

- [Focusing on Endpoint Analysis](#)
- [Investigating Hosts](#)
- [Analyzing Downloaded Files](#)
- [Changing File Status or Remediate](#)
- [Analyzing Events](#)
- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

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

2 Actions in the toolbar:

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 process dump to server.
- 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.
- Hosts - Displays the top 100 hosts based on the risk score on which the file is present.

6 Clicking a filename lets you navigate to the Files view for further analysis.**7 Filter Files.** You can filter files by selecting the options in the Filters panel and create filters. For more information, see [Investigating Hosts](#).

8

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

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.

Category	Description
Signature	Provides signatory information.
Downloaded	Indicates the status of the downloaded file - Downloaded, Not Downloaded, and Error.
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.

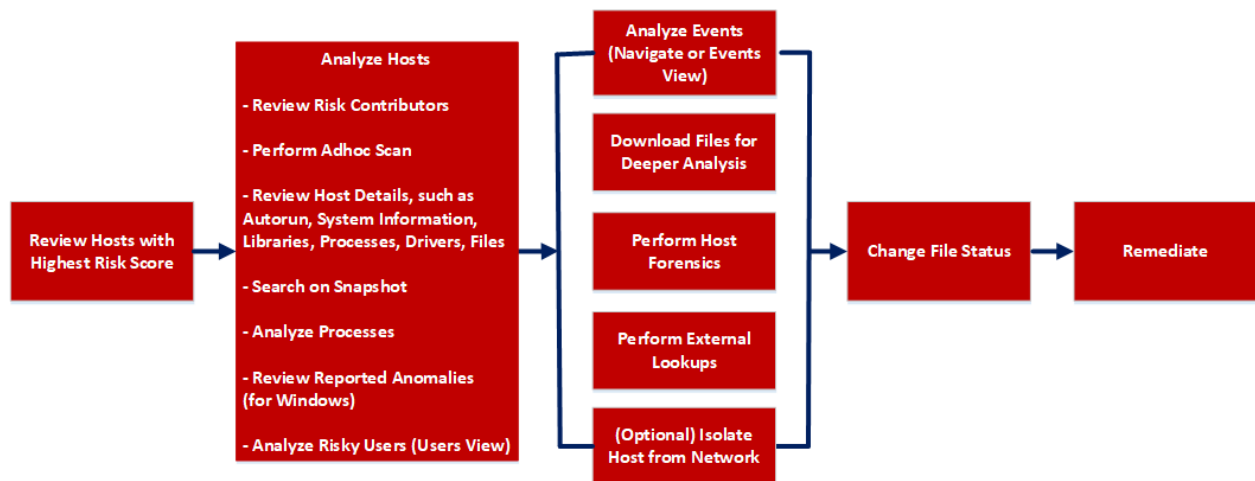
Category	Description
Hive	Name of the registry hive when possible, otherwise it displays the hive ID. Possible values are: <code>hkeyClassesRoot</code> , <code>hkeyCurrentUser</code> , <code>hkeyLocalMachine</code> , <code>hkeyUsers</code> , or <code>hkeyPerformanceData</code> .
Reason	Type of registry discrepancy. Possible values are: <code>notFound</code> , <code>embeddedNull</code> , <code>accessDenied</code> , <code>parentIsHidden</code> , or <code>dataMismatch</code> .
Registry Path	Registry path that is affected. The value is separated by a <code>@</code> 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 - Downloads Tab

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.4 and later.

The Downloads tab provides information about all downloads (MFT, files, system dump, and process dump) performed on the host. To access this tab, select a host from the **Hosts** view and click the **Downloads** 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
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

*You can perform this task in the current view.

Related Topics

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

- [Performing Host Forensics](#)
- [Isolating Hosts from Network](#)

Quick Look

Below is an example of the Downloads 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.

More - Provides options to:

- Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
- Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
- Download MFT to the server. For more information, see [Performing Host Forensics](#).
- Download System Dump to the server. For more information, see [System and Process Memory Dump](#).

2 Filter Files. You can filter downloaded files by selecting the options in the Filters panel and create filters. For more information, see [Performing Host Forensics](#).

3 Actions in the toolbar:
Save a Local Copy - Lets you retrieve the downloaded MFT and save it to your local file system for further analysis.

Delete File - Deletes the downloaded MFT from the server.

For more information, see [Performing Host Forensics](#).

4 View MFT Details. Click the filename to view the MFT details. For more information, see [MFT Viewer](#).

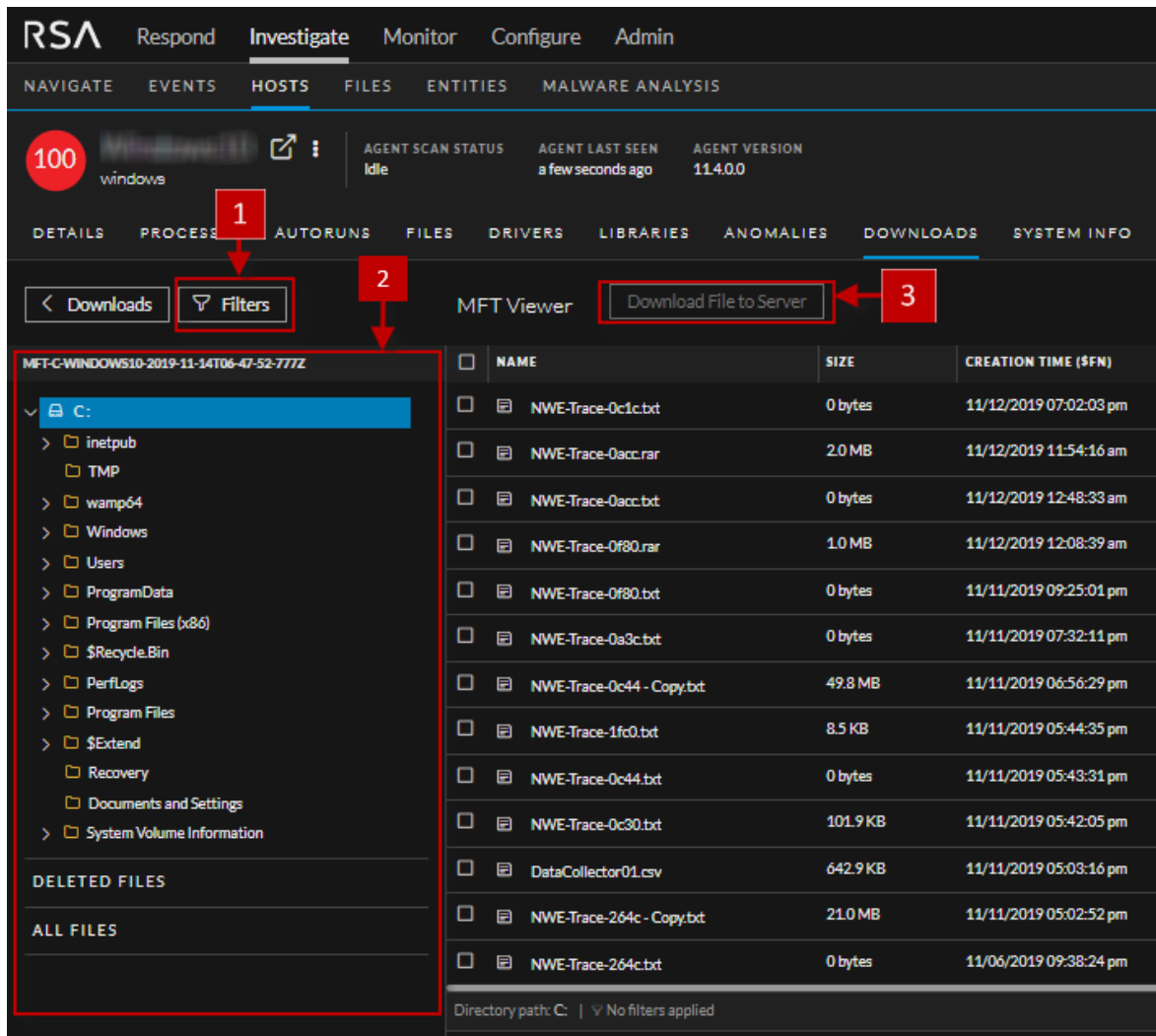
The table displays the following information:

Column	Description
File Name	Name of the file that is downloaded. For example, VGAuthService.exe.
Type	Type of file downloaded - MFT, file, memory dump.
Downloaded	Status of the download:  - Download successful  - Processing the downloaded file  - Errors including download failed
Size	Size of the downloaded file.
Downloaded Time	Time when the MFT was downloaded.
SHA256	SHA256 of the file. Note: This is applicable only for files.

MFT Viewer

You can analyze the downloaded MFT using the MFT Viewer. For more information, see [Analyze Downloaded MFT](#)

Below is an example of the MFT Viewer:



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

2 Folder Details. Lets you view the content of the MFT.

3 Download File to Server. Downloads files to the server.

The table displays the following information:

Column	Description
Name	Name of the file. For example, <code>dtf.exe</code> .
Size	Size of the file.
Creation Time (\$FN)	File Name (\$FN) creation time.
Creation Time (\$SI)	Standard Information (\$SI) creation time.

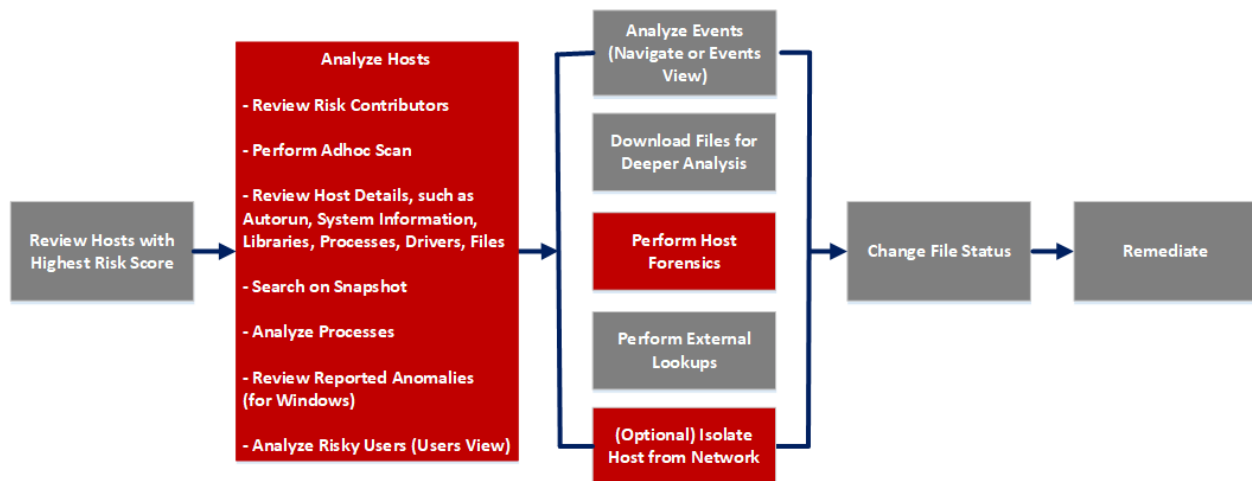
Column	Description
Modification time (\$FN)	\$FN modified time.
Modification time (\$SI)	\$SI modified time.
Access time (\$FN)	\$FN access time.
Access time (\$SI)	\$SI access time.
Update time (\$FN)	\$FN updated time.
Update time (\$SI)	\$SI updated time.
Full Path	Path of the file.
Allocated Size	File size on the disk.
Archive	Indicates if a file is archived.
Compressed	Indicates if a file is compressed.
Encrypted	Indicates if a file is encrypted.
Hidden	Indicates if a file is hidden.
Directory	Indicates if it is a directory.
Extension	Type of the file. For example, exe, pdf, txt.

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

User Role	I want to ...	Show me how
Threat Hunter	perform external lookups	Launch an External Lookup for a File
Threat Hunter	change file status or remediate	Changing File Status or Remediate
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

*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:

The screenshot shows the NetWitness Endpoint interface. At the top, the 'Investigate' tab is selected. Below it, the 'HOSTS' sub-tab is active. A red box labeled '1' highlights the 'HOSTS' sub-tab. Another red box labeled '2' highlights the search bar labeled 'Search by filename, path or hash'. A third red box labeled '3' highlights the 'Host File Entries' table. The table has two columns: 'IP ADDRESS' and 'DNS NAME'. The data rows are as follows:

IP ADDRESS	DNS NAME
10.2.2.2	update.microsoft.com
127.0.0.1	www.virustotal.com
127.0.0.1	www.owncloud.com
127.0.0.1	dcl.soghozup.com

- 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.
 - More** - Provides options to:
 - Start a scan for the selected hosts. For more information, see [Scan Hosts](#).
 - Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see [Export Host Details to JSON File](#).
 - Isolation host from the network. For more information, see [Isolating Hosts from Network](#).
 - Download MFT to the server. For more information, see [Performing Host Forensics](#).
 - Download System Dump to the server. For more information, see [System and Process Memory Dump](#).
 - Snapshot Time** - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.
- 2 **Search on Snapshots.** Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see [Search on Snapshots](#).
- 3 **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.

Tabs	Description
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.