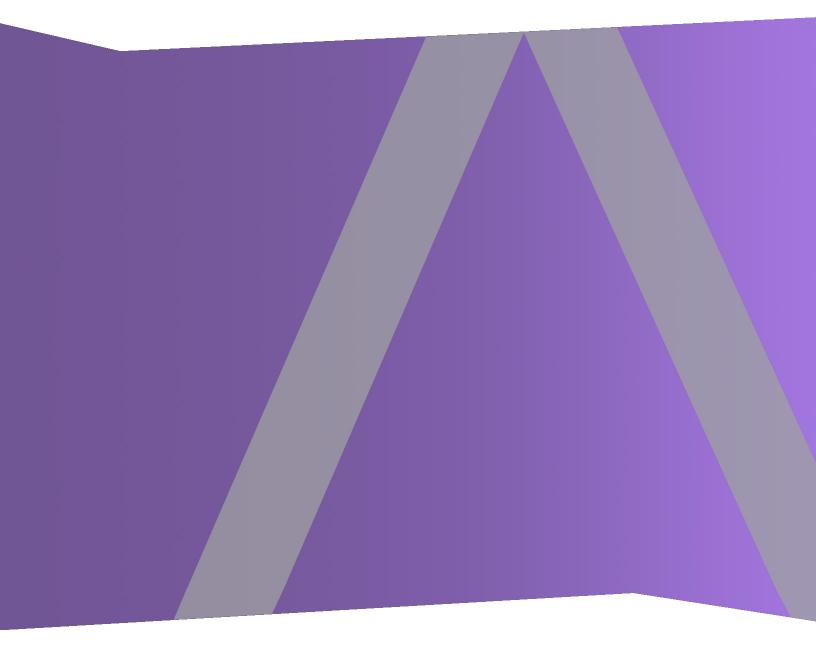


# NetWitness Endpoint User Guide

for RSA NetWitness® Platform 11.5



#### **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

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

#### **License Agreement**

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

#### **Third-Party Licenses**

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

#### Note on Encryption Technologies

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

#### Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November 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	
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	. 27
Investigating Hosts	.29
Best Practices	29
View Hosts	30
View Agent History	31
Filter Hosts	. 32
Adding and Sorting Columns in the Table	. 36
Scan Hosts	36
Analyze Hosts Using the Risk Score	37
Analyze Host Details	. 39
Filter Host Details	40

Search Files on Host	
Analyze Processes	
Analyze Autoruns	
Analyze Files	
Analyze Libraries	
Analyze Drivers	
Analyze Anomalies	45
Analyze System Information	
Analyze History	
Export Host Details or Files to JSON File	
Launch an External Lookup for a File	
Delete a Host	
Deleting Hosts with Older Agent Versions	
Set Hosts Preference	
Export Host Attributes	
Migrate Hosts	
Analyzing Risky Users	
Resetting Risk Score of Hosts	
Investigating a Process	53
Best Practices	
Analyze a Process	
Analyze Events for a Process	
Changing File Status or Remediate	
Analyzing Downloaded Files	
Download Files to Server	
Save Downloaded Files	
Analyze Downloaded Files	
Performing Host Forensics	
Download Master File Table	
Analyze Downloaded MFT	
System and Process Memory Dump	
Download Files Using Full Path or Wildcard	
Filter Downloaded Files	
Save Downloaded File	
Delete Downloaded Files	
Analyzing Events	
Analyze Events from Files View	
Analyze Events from Hosts View	
Text Analysis for an Endpoint Event	

Isolating Hosts from Network	
Edit Exclusion List	
Release Isolated Hosts	
NetWitness Endpoint with Third-Party Antivirus Products	
Troubleshooting NetWitness Endpoint	
General Issues	
Multi-server Issue	
Hosts View Issues	
Files View Issues	
Policy Issue	
Driver Issue	
File Reputation Service Issue	
Risk Scoring for Hosts or Files Issue	
NetWitness Endpoint Reference Materials	
Files View	
File Details View	95
Hosts View	
Hosts View - Details Tab	
Hosts View - Process Tab	
Process Details	
Hosts View - Autoruns Tab	
Hosts View - Files Tab	
Hosts View - Drivers Tab	
Hosts View - Libraries Tab	
Hosts View - Anomalies Tab	
Image Hooks	
Kernel Hooks	
Suspicious Threads	
Registry Discrepancies	
Hosts View - Downloads Tab	
MFT Viewer	
Hosts View - System Information Tab	
System Information Panel	
Hosts View - Agent History Tab	143

# Introduction

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

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

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

## **Endpoint Metadata**

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

Operating System	Scan Categories	Tracking Categories
Windows	file, service, dll, process, task, autorun, machine, kernel hook, image hook, registry discrepancies, and suspicious threads	<ul> <li>Process event - Reports any process related activities, such as openprocess, openosprocess, createprocess, createremotethread, openbrowserprocess.</li> <li>File event - Reports any file related activities by an executable, such as readdocument, writetoexecutable, renameexecutable, selfdeleteexecutable, openphysicaldrive.</li> <li>Registry event - Reports activities that result in registry creation or modification, such as modifyservicesimagepath, modifyfirewallpolicy, createservicesimagepath, createsecuritycenterconfiguration, modifybadcertificatewarningsetting.</li> <li>System event - Reports IP change and boot events.</li> <li>Network event - TCP/UDP and incoming/outgoing.</li> <li>Reports outbound and inbound network connections on all supported Windows platforms.</li> <li>Reports IPv4 and IPv6 connections.</li> <li>Console event (for Windows &amp; and later) - User input that is entered into a console application, such as cmd.exe, powershell.exe, is captured and reported with the context console.local.</li> <li>Commands executed by cmd.exe, powershell.exe as a result of inter-process communication through anonymous pipes are captured and reported with the context console.remote.</li> <li>For example, Get-Item -Path Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion.</li> </ul>
Linux	file, autrorun, 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 openprocess, createprocess, openosprocess, openbrowserprocess, allocateremotememory, createremotethread.
		• File event - Reports any file related activities by an executable, such as writetoexecutable, renameexecutable, createautorun, deleteexecutable, selfdeleteexecutable, writetoplist, writetosudoers, createbrowserextension.
		<ul> <li>Network event - TCP/UDP and incoming/outgoing.</li> <li>Reports outbound and inbound network connections on all supported Mac operating system.</li> <li>Reports IPv4 and IPv6 connections.</li> </ul>

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.

	-8						.,							
RSΛ	Investigate	Respond	Users Ho	osts Files Dashboards	Reports								2 % 0	admin >
100 wi	ndows		agent scan st. <b>Idle</b>	ATUS AGENT LAST SEEN a few seconds ago	agent vers 11.5.0.0			ме 06/24/2	020 21:30:33					
	PROCESSES	AUTORUNS		DRIVERS LIBRARIES AN	OMALIES	DOWNLO		STEM INFO	HISTORY					
ALERTS SEVE	RITY			© Events rolled over due to rete	ntion policies	or manual de	letion will	ot be available	•					
2	0	0	2	28 events	ntion policies	or manual de		IOL DC AVAIIADIO	-			HOST DETAILS PO		
			∠ ALL	EVENT TIME 06/29/2020 13:40:54.000	EVENT TYPE	category <b>File</b>	<b>action</b> N/A	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM	FILE	Type to filter list		
<u> </u>	-										110	Show details with va	lues only	
				FILE NAME		UMENT								
				SOURCE N/A										
Runs Blackliste	d Ell- (0)			TARGET N/A									Windows-security	
3 event(s)	a File (3)			EVENT TIME 06/29/2020 13:40:54.000	EVENT TYPE Endpoint	category File	<b>action</b> N/A	HOSTNAME	<b>USER ACCOUNT</b> N/A	OPERATING SYSTEM windows	FILE			
				FILE NAME										
				SOURCE N/A	LAUNCH ARG	UMENT							2	
				TARGET N/A										
													Administrators	
				EVENT TIME 06/29/2020 13:40:54.000	event type Endpoint	category File	<b>action</b> N/A	HOSTNAME	<b>USER ACCOUNT</b> N/A	OPERATING SYSTEM windows	nie intl			
				FILE NAME	LAUNCH ARG	UMENT			PATH					
				SOURCE N/A										
				TARGET N/A										
				EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM	FILE			
				06/29/2020 13:40:54.000	Endpoint	File	N/A		N/A	windows	jço,		Intel(R) 82574L Gigat	oit Network
				FILE NAME	LAUNCH ARG	UMENT			PATH			MAC Address	00:50:56:01:29:06	
				SOURCE N/A									001001001.27.00	

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.

RSA Investigate Respond Users Hosts	Files Dashboards Reports	🗃 💥 🕜 admin >
100 indows agent scan status Idle	AGENT LAST SEEN AGENT VERSION SNAPSHOT TIME 06/24/2020 21:30:33 ~	a   ×
DETAILS PROCESSES AUTORUNS FILES DRIVER	RS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY	ilename, path or hash Q
	Events rolled over due to retention policies or manual deletion will not be available. 2 events	HOST DETAILS POLICY DETAILS X
CRITICAL HIGH MEDIUM ALL	EVENT TIME EVENT CATEGORY ACTION HOSTNAME USER ACCOUNT OPERATING	Type to filter list
Configures Port Redirection (1)	03/01/2019 Tree Process Ev., createProc WIN-NMUEVI3DGTNLewindows 02.3308.000 Endpo pm	Show details with values only Users
1 event(s)	FILE NAME LAUNCH ARGUMENT PATH	Name WIN-NMUFVI3DGTN\ecat
Creates Shadow Volume For Logical Drive (1)	source malware7.exe malware7.exe -dll:ioc.dll -testcase:400,401 C:\Users\ecat\Desktop\	Session ID 2
1 event(s) Creates Remote Process Using WMI Command-Line Tool (1)	TARSET REG.exe REG.exe ADD C:\Windows\system32\ WGMSOTPWARE\Microsoft\Windows NTGurrent\version\Image File Execution Optionskethc.exe V gebruger / REG.52 / d	Is Admin true
1 event(s)	"C:\windows\system32\cmd.exe" /f	Groups Administrators
Enables RDP From Command-Line (1) 1 event(s)	EVENT TIME EVENT CATEGORY ACTION HOSTNAME USER ACCOUNT OPERATING 03/01/2019 TYPE Drocess Ev createProc WIN-NMUFVI3DGWIN-NMUFVI3DGTNV	Users
Configures Image Hijacking (12)	03/01/2019	Name Window Manager\DWM-1
12 event(s)	FILE NAME LAUNCH ARGUMENT PATH	Session ID 1
Stops Security Service (1)	source malware3.exe malware3.exe dll:ioc.dll -testcase:400,401 C:\Users\ecat\Desktop\	Is Admin false
1 event(s)	TARGET REG.exe ADD C:\Windows "HKI MSOFTWARE\Mirrosoft\Windows	
Creates Remote Task (4) 4 event(s)	nikosti icecce "HickMSOFTWAREMicroanfiWindows Criminomstysteriozi" NTCurrentvestionimage File Secution Optionstranging zee" // Debugger /: RES_SZ /d CliwindowsSystemS2tmd.ede" /	Name Intel(R) PRO/1000 MT Networ

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.

RSA         Investigate         Respond         Users         Hos	TUS OPERATING SYSTEM		≅ ‰ ⊘ admin > ■ >
ALERTS SEVERITY	<ul> <li>Events rolled over due to retention policies or manual deletion will ne</li> <li>3 events</li> </ul>	ot be available.	FILE DETAILS HOSTS
0 3 4 7	DVENT TIME EVENT TYPE CATEGORY ACTION HOSTNAME 02/27/2019 Endpoint File N/A 1045:50.000 am	USER ACCOUNT OPERATING SYSTEM	Type to filter list
1 event(s) Hidden Plist And Autorun (3) 3 event(s)	FILE NAME         LAUNCH ARGUMENT           SOURCE         N/A           TARGET         N/A	<b>PATH</b> N/A N/A	General FileName .MSProc Entropy 6.631475448608398
Packed And Autorun (3) 3 event(s)	EVENT TIME EVENT TYPE CATEGORY ACTION HOSTNAME 02/27/2019 Endpoint File N/A 10:45:50.000 am	USER ACCOUNT OPERATING SYSTEM	Size 12.0 KB Format macho
	FILE NAME LAUNCH ARGUMENT Source N/A N/A Target N/A N/A	<b>Path</b> N/A N/A	Signature Features <b>unsigned</b>
	EVENT TIME EVENT TYPE CATEGORY ACTION HOSTNAME 02/227/2019 Endpoint File N/A 09:35:46.000 am FILE NAME LAUNCH ARGUMENT	user account operating system N/A mac	Hash MD5 5171a462210f540a3005e361c SHA1 2369375ff825f6d5ee9bcd296 SHA256 5d0b9421c46b1d91677791d6

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 <u>Changing File</u> 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:

ALERTS SEVERIT	v						
ALLERIS SEVERI	•			2 events			
3 CRITICAL	16 нісн	20 MEDIUM	39 <sup>All</sup>	еvемт тіме 01/02/20 06:23:42. am	19 Log	CATEGORY ACTION Process createPr	Hostname User <u>Superno</u> N/A
Enables Cleartext 2 event(s)	Credential Stora	age (2)			FILE NAME	LAUNCH ARGUMENT	РАТН
Exports Sensitive I	Registry Hive (4)			SOURCE	dtf2.exe	dtf2.exe -dll:ioc.dll	C:\Users e\archiv
4 event(s) Enables Login Byp				TARGET	REG.exe	REG.exe ADD HKLM\System\Curre t\Control\SecurityPr gest /V USELOGON( 7T REG_DWORD /D 1	C:\Wind entControlSe oviders\WDi REDENTIAI
12 event(s)	(12)					7T REG_DWORD 7D	/f
				event time 01/02/20 06:23:42. am	19 Log	CATEGORY ACTION Process createPr	HOSTNAME USER SUPERIO N/A
				am	FILE NAME	LAUNCH ARGUMENT	РАТН
				SOURCE	dtf2.exe	dtf2.exe -dll:ioc.dll	C:\Users e\archiv
				TADOTT	DEC		CANNI- d

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 <u>Analyze Hosts Using the Risk Score</u> and <u>Analyze Files Using the Risk Score</u>.

#### **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 <u>Changing File Status or Remediate</u>.

## **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**

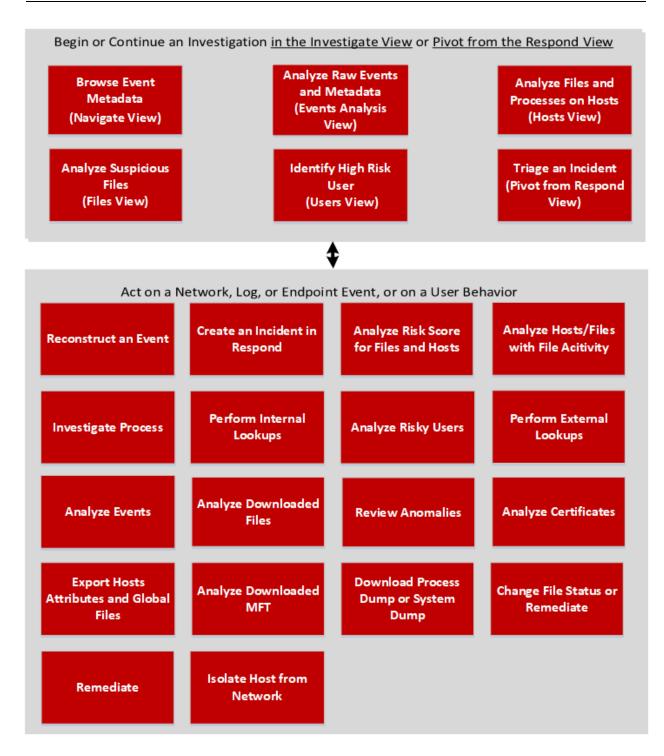
This guide provides the information needed to conduct an investigation that is focused on endpoint data from configured hosts. Analysts who conduct analysis using Investigate need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles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

You can begin the investigation on files in your deployment in the Files view (Files). (See <u>Investigating</u> 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.



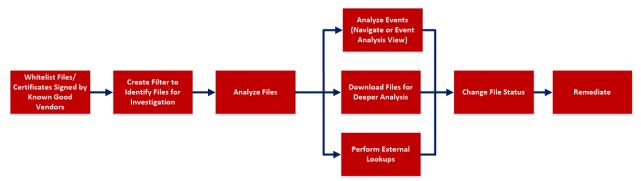
# **Investigating Files**

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 <u>Filter Files</u> and <u>Changing File Status or Remediate</u>.

**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 <u>Files Restricted from Whitelisting</u>.

- 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 <u>Analyze</u> 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 <u>Changing File Status or Remediate</u>.
- 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 <u>Analyzing Events</u>.
- Download suspicious files to the server for deeper analysis. For more information, see <u>Analyzing</u> <u>Downloaded Files</u>.
- Change the status of the file (blacklist or graylist), and block an infected or malicious file. For more information, see <u>Changing File Status or Remediate</u>.

## **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 Files.
- 2. Select one of the following:

RSA Investigate Respond Users H	osts <b>Files</b> Dashb	ooards Repo	rts					2 %	@ adn	min >
<b>∀</b> Filters ×	endpointloghy ~		icates	ଁ ୍କ Change Fil	e Status 🛛 🖓 Analyze I	vents	✓ Hore Action	15 ∨		<b>!</b>
SAVED FILTERS	endpointloghybrid1 - E		SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCE	FILE STATUS	۲
Select	endpointloghybrid2 - E		/2020 17:0		Known Good	9.5 MB	microsoft,signed,valid	Microsoft Cor	Neutral	
FILE NAME	smss.exe	0 06/1	 1/2020 17:0		Known Good	143.9	microsoft,signed,valid	Microsoft Cor	Neutral	
Equals v e.g., Filename.dll	wininit.exe	0 06/1:	1/2020 17:0		Known Good	362.7	microsoft,signed,valid	Microsoft Cor	Neutral	
FILE STATUS	services.exe	0 06/1	1/2020 17:0		Known Good	659.0	microsoft,signed,valid	Microsoft Cor	Neutral	
Neutral     Blacklist	Isass.exe	0 06/1	1/2020 17:0		Known Good	56.7 KB	microsoft,signed,valid	Microsoft Cor	Neutral	
Graylist	fontdrvhost.exe	0 06/1	1/2020 17:0		Known Good	802.6	microsoft,signed,valid	Microsoft Cor	Neutral	
Whitelist	LogonULexe	0 06/1	1/2020 17:0		Known Good	13.5 KB	microsoft,signed,val	Microsoft Cor	Neutral	
REMEDIATION	spoolsv.exe	0 06/1	1/2020 17:0		Known Good	747.5	microsoft,signed,val	Microsoft Cor	Neutral	
Biocked	vmtoolsd.exe	0 06/1	1/2020 17:0		Known	81.5 KB	signed,valid	VMware, Inc.	Neutral	
	Management	0 06/1	1/2020 17:0		Known	59.5 KB	unsigned		Neutral	
□ Suspicious	MsMpEng.exe	0 06/1	1/2020 17:0		Known	111.3	signed,valid	Microsoft Cor	Neutral	
Unknown     Known	UGAuthServic	0 06/1	1/2020 17:0		Known	160.0	unsigned	VMware, Inc.	Neutral	
Known Good     Invalid	msdtc.exe	0 06/1	1/2020 17:0		Known Good	145.0	microsoft,signed,val	Microsoft Cor	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:

R	SA Investigate Respor	nd Users H	Hosts Files	Dashboards	Reports								8	* ?	) adm	iin >
₽F	ilters 🛛 🖯 endpointloghy 🗸 🗋	View Certificates	A Change File Sta	tus 🖸 Analyz	e Events 🗸 🕻 More 🗸					•			md.exe			
	FILE NAME	RISK SCORE 🔶	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES.C	FILE STATUS	۲	FILE DETAILS					
			11/08/2019 10:51:0			230.5 KB	microsoft,signed,valid,ca	Microsoft Corpor	Neutral		Type to filter I	ist				
	<u>cmd.exe</u>		11/08/2019 10:49:3			295.5 KB	microsoft,signed,valid,ca	Microsoft Corpor	Neutral		🗹 Show detail	s with valu	ies only			
	<u>cmd.exe</u>		11/06/2019 02:42:2	1		337.0 KB	microsoft,signed,valid,ca	Microsoft Corpor	Neutral							
⊠			11/06/2019 02:41:5			273.5 KB	microsoft,signed,valid,ca	Microsoft Corpor	Neutral			FileName Entropy		98015998	20	
	MRT-KB890830.exe	70	11/17/2019 10:24:5			121.0 MB	unsigned		Neutral				6.17003 273.5 KE		20	
		20	11/11/2019 06:59:4			56.7 KB	microsoft,signed,valid	Microsoft Corpor	Neutral					í ,		
	<u>Taskmgr.exe</u>	70	11/10/2019 09:51:1			1.3 MB	microsoft,signed,valid	Microsoft Corpor	Neutral							
	Isass.exe	70	11/06/2019 02:42:4			45.9 KB	microsoft,signed,valid	Microsoft Corpor	Neutral		Signature					
	Taskmgr.exe	70	11/06/2019 02:41:5			1.0 MB	microsoft,signed,valid	Microsoft Corpor	Neutral						ilid,catalog :28.400 am	
		70	11/06/2019 02:41:5			56.7 KB	microsoft,signed,valid	Microsoft Corpor	Neutral						eec424749	
	<u>getmac.exe</u>	3	11/08/2019 10:52:1			83.5 KB	microsoft,signed,valid,ca	Microsoft Corpor	Neutral			Signer	Microso	ft Windows	s	
	MEMORY DLL 2D8708FDD4874DFCB6D8	5. 31	11/11/2019 12:31:4	1	-	0 bytes	unsigned	Microsoft Corpor	Neutral							

- File Details displays the file information. For more information, see <u>Launch an External Lookup</u> 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.

RSA Investigate Respond Users Hosts Files	Dashboards Reports		🗊 拨 🕐 admin >
<b>∀</b> Filters ×	endpointloghy View Certificates	Change File Status Analyze Ev	ents 🗸 🕻 More 🗸
SAVED FILTERS	File NAME	RISK SCORE	TS REPUTATION
Select		11/08/2019 10:51:0 1	
FILE NAME		11/08/2019 10:49:3 1	
Equals v e.g., Filename.dll		11/06/2019 02:42:2 1	
FILE STATUS	⊠ <u>cmd.exe</u>	11/06/2019 02:41:5 1	
Neutral	MRT-KB890830.exe	70 11/17/2019 10:24:5 1	
Blacklist     Gravlist	sass.exe	70 11/11/2019 06:59:4 1	
U Whitelist	Taskmgr.exe	70 11/10/2019 09:51:1 1	
REMEDIATION	sass.exe	70 11/06/2019/02:42:4 1	
Blocked	Taskmgr.exe	70 11/06/2019 02:41:5 1	
REPUTATION	C Isass.exe	70 11/06/2019/02:41:5 1	
Malicious     Suspicious	getmac.exe	33 11/08/2019 10:52:1 1	
Unknown     Known	MEMORY DLL 2D8708FDD4874DFCB6D85	31 11/11/2019 12:31:4 1	
Known Good     Invalid	[MEMORY DLL 9D305FB1E34E6FCA39695A	31 11/11/2019 12:31:4 1	
	[MEMORY DLL 21DE82DB31853248346E4C	31 11/08/2019 10:54:1 1	
RISK SCORE	[MEMORY DLL 89AE00754A7475A6763C6E	31 11/08/2019 10:54:1 1	
· • • • • • • • • • • • • • • • • • • •	crypt32.dll	31 11/08/2019 10:52:1 2	
•••••••••••••••••••••••••••••••••••••••	crypt32.dll	<b>31</b> 11/08/2019 10:52:1 1	
	regsvr32.exe	31 11/08/2019 10:52:1 1	
		31 11/06/2019/02-42-4 1	
Reset Save Save as	J	Showing 100 o	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.

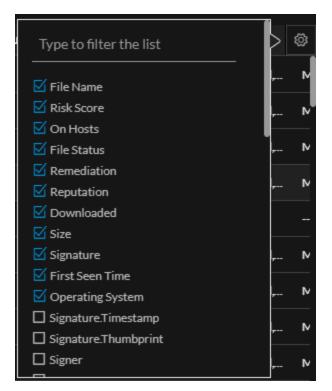
For example, to filter the files based on file reputation, select the reputation status in the Filter panel.

**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 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 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

ALERTS SEVERITY		Events rolled over due to retention policies or manual deletion will not be available.     6 events
1 1 3 скітісац нісн меріим Enables Login Вуразс (6)	5 ALL	PORT THR EVENT TWE ACTION ACTION NOTTING ACTION NOTTING UND ACCOUNT OPAIANING STITLM INDU 0.23/02/19 Endpoint Process Event createProcess contaction windows Declasbac3/dd/dd/909c66cebac3bc231f023/dd/dd/9926febac3bc231f023/dd/dd/dd/9926febac3bc231f023/dd/dd/dd/9926febac3bc231f023/dd/dd/dd/9926febac3bc231f023/dd/dd/dd/dd/dd/dd/dd/dd/dd/dd/dd/dd/dd
E erent)		SOLICEC     TARGET T     DOMAILHOOT T     EVENT SOURCE       PATI     PATI     ONAMILHOOT T     EVENT SOURCE       CUUSTINGEDDESkoph     CUWINDWINStein32h     SZE     USER SRC       RLS MASS     131144/RADODT/ORDE_20005/0008kbc/dB0     PATI     DATA       RLS MASS     131144/RADODT/ORDE_20005/0008kbc/dB0     PATA     ALUAS IP       RLS MASS     131144/RADODT/ORDE_20005/0008kbc/dB0     PATA     ALUAS IP       RLS MASS     RLS MASS     PATA     PATA       RLS MASS     RLS MASS     PATA     ALUAS IP       RLS MASS     RLS MASS     PATA     PATA       RLS MASS     RLS MASS     PATA     ALUAS IP       RLS MASS     RLS MASS     PATA     PATA       RLS MASS     PATA     RLS MASS     PATA       RLS MASS     PATA     RLS MASS
		KOTH THIS DEVIT THE CATORY OF CATORY CONTINUES OF CATORY

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.

	WHR. ( 8885) P	NUBBER WILLING		×
	CONTEXT HI	GHLIGHTS		ACTIONS
	0 INCIDENTS	0 ALERTS	0 LISTS	E Add/Remove from List ♀ Pivot to Investigate > Navigate
		View Context		
IE N	ufvi3dgtn	USER ACCOU WIN-NMU	NT IFVI3DGTN	OPERATING SYSTEM Accat windows

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

ALERTS SEVERITY				Events rolled ove 6 events	r due to retenti	ion policies or manu	al deletion will not be	available.			
1	1   нісн	3 MEDIUM	5 All	EVENT TIME 03/01/2019 02:34:08.000 pm	EVENT TYPE Endpoint	CATEGORY Process Event	ACTION createProcess	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM WINDOWS	HASH 0eda8ba34ddc46909
Enables Login Bypa 6 event(s)	ss (6)			SOURCE PATH CAUSerstecatUDe FILESMA256 Oed84bb34ddc6 O992a1eb3130b FILENAME malware10.exe LAUNCH ARGUNEN malware10.exe DEVICE N/A USER USER USER USER USER USER USER USER	sktop\ s909c66ceba5bi yry dllioc.dll-testca s909c6ceba5bi y794134c55db	ase:400,401 c231f029dedbc	1520e9c2a7 FILENAME REG.exe LAUNCH ARG REG.exe ADJ "HKLMMSOF NTCUITENT Options/dfg REG_5Z/d*4 DEVICE N/A HASH 19316d4266	5d0b776d9b2a05d5903d8ct e6d5960b6fa4dcaf UMENT	n n r ft exe* ff	DOMAIN/HOST SIZE 41 DATA mLINAME malware10.exe ssze 41 HASH 0eda8ba34ddc469099c66ceba5 debC6992a1eb31130b794134c AGENT ID 93b4/D024.9103-9792-F985-FE DEVICE TYPE nwendpoint	55db

- 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 <u>Investigating a Process</u>.

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.

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

	tigate Respo	ond Users I	Hosts Files	Dashboards	Reports					2 %	0	admin >
⊽Filters end	lpointloghy 🗸	View Certificates	; X Chan	ge File Status	🗗 Analyze Events	More Actio	ns ∨			smss.exe		
	RISK SCORE 1	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	FILE STATUS	R (\$)		ноятя	
	<u></u>	06/11/2020 17:05:		Known Good	9.5 MB	microsoft,signed,valid	Microsoft Corpo	Neutral	-	100	67	
🗹 <u>smss.exe</u>		06/11/2020 17:05:	2	Known Good	143.9	microsoft,signed,valid	Microsoft Corpo	Neutral	-	100	്	
		06/11/2020 17:05:		Known Good	362.7	microsoft,signed,valid	Microsoft Corpo	Neutral				
	٥	06/11/2020 17:05:		Known Good	659.0	microsoft,signed,valid	Microsoft Corpo	Neutral				
	٥	06/11/2020 17:05:		Known Good	56.7 KB	microsoft,signed,valid	Microsoft Corpo	Neutral				
	0	06/11/2020 17:05:		Known Good	802.6	microsoft,signed,valid	Microsoft Corpo	Neutral				

- 3. Click the host name to open the host details.
- 4. Click to analyze events on the host in the Events view. For more information, see <u>Analyzing</u> Events.

## Launch an External Lookup for a File

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

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

RSA Investigate Respond	Jsers Host	s <b>Files</b> D	ashboards Reports					2 %	② admin >
<b>▽</b> Filters		endpointloghy	View Certificates	يد Change File	Status 🖸 Analyze Ev	vents	More Action	s 🗸	<b>.</b>
	<u> </u>	File NAME	RISK SCORE 🔶 FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCE	FILE STATUS
Select	<u> </u>	🗹 <u>ntoskrnl.exe</u>			Known Good	9.5 MB	microsoft,signed,valid	Microsoft Cor	Neutral
FILE NAME		smss.exe	Change File Status Analyze Events		Known Good	143.9	microsoft,signed,valid	Microsoft Cor	Neutral
Equals v e.g., Filename.dll	L	wininit.exe	Google Lookup	File Name	Known Good	362.7	microsoft,signed,valid	Microsoft Cor	Neutral
FILE STATUS		services.exe	VirusTotal Lookup	MD5	Known Good	659.0	microsoft,signed,valid	Microsoft Cor	Neutral
		Isass.exe	View Certificates	SHA1	Known Good	56.7 KB	microsoft,signed,valid	Microsoft Cor	Neutral
<ul><li>Blacklist</li><li>Graylist</li></ul>		fontdrvhost.exe	Download File to Server	SHA256	Known Good	802.6	microsoft,signed,valid	Microsoft Cor	Neutral
Whitelist		LogonULexe	Save a Local Copy	2	J Known Good	13.5 KB	microsoft,signed,val	Microsoft Cor	Neutral
		spoolsv.exe			Known Good	747.5	microsoft,signed,val	Microsoft Cor	Neutral
Blocked		vmtoolsd.exe	Reset Risk Score		Known	81.5 KB	signed,valid	VMware, Inc.	Neutral

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

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

## **Set Files Preference**

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

1. Go to Files.

2. Select the columns by clicking 🖸 in the right-hand corner. The following example shows the dropdown list displayed while adding columns:

Type to filter the list	$\geq$	٢
	L	]
🗹 File Name	<b>*</b> **	
🗹 Risk Score		_ ∧
🗹 On Hosts	<u> </u>	
🗹 File Status	<b>,</b>	M
Kemediation		
🗹 Reputation	<del>7</del>	M
☑ Downloaded		
🗹 Size		
🗹 Signature	<b>,</b>	№
🗹 First Seen Time		
🗹 Operating System	<b>,</b>	M
Signature.Timestamp		
Signature.Thumbprint	<b>7</b>	M
Signer		N
	7	

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 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.

RSA Investigate Respond	Users Ho	osts	Files Das	shboards f	Rep	orts					E	2 %	?	admin >
<b>▽</b> Filters		8	endpointloghy	View C	erti	ificates	Change File Status	Analyze Events	/ <b>!</b> M	ore Actions $\checkmark$				<b>(</b>
			FILE NAME	RISK SCORE		FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	FILE STATUS		• @
Select	~			•		06/11/2020 17:05:		Known Good	9.5 MB	microsoft,signed,valid	Microsoft Corpo	Neutral		
				•		06/11/2020 17:05:		Known Good	143.9	microsoft,signed,valid	Microsoft Corpo	Neutral		
Equals v e.g., Filename.dll				٥		06/11/2020 17:05:		Known Good	362.7	microsoft,signed,valid	Microsoft Corpo	Neutral		
FILE STATUS				٥		06/11/2020 17:05:		Known Good	659.0	microsoft,signed,valid	Microsoft Corpo	Neutral		
Neutral				٥		06/11/2020 17:05:		Known Good	56.7 KB	microsoft,signed,valid	Microsoft Corpo	Neutral		
Blacklist     Graylist	1			0		06/11/2020 17:05:		Known Good	802.6	microsoft,signed,valid	Microsoft Corpo	Neutral		
Whitelist			LogonUl.exe	0		06/11/2020 17:05:	2	Known Good	13.5 KB	microsoft,signed,valid,	Microsoft Corpo	Neutral		-

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 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:

RSA Investigate Respond Users Ho	osts	Files	Dashboards Reports						3 %	(?) adm	nin >
<b>∀</b> Filters ×	8	endpointlo	yghy… ∨ View Certificates		ی Change File	e Status 🛛 🖓 Analyze E	vents	✓ Hore Action	<u>15 ~</u>		<b></b>
SAVED FILTERS		FILE NAME	RISK SCORE 个 FIRST SEEN	TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCE	FILE STATUS	ŝ
Select ~			0 06/11/2020	17:0		Known Good	9.5 MB	microsoft,signed,valid	Microsoft Cor	Neutral	
FILE NAME			0 06/11/2020	17:0		Known Good	143.9	microsoft,signed,valid	Microsoft Cor	Neutral	
<b>Equals</b> v e.g., Filename.dll		<u>wininit.exe</u>	Change File Status	17:0		Known Good	362.7	microsoft,signed,valid	Microsoft Cor	Neutral	
FILE STATUS		services.exe	Analyze Events	17:0		Known Good	659.0	microsoft,signed,valid	Microsoft Cor	Neutral	
Neutral			Google Lookup >	17:0		Known Good	56.7 KB	microsoft,signed,valid	Microsoft Cor	Neutral	
□ Blacklist □ Graylist		fontdrvhos	View Certificates	17:0		Known Good	802.6	microsoft,signed,valid	Microsoft Cor	Neutral	
U Whitelist		LogonUI.ex	Download File to Server	17:0		Known Good	13.5 KB	microsoft,signed,val	Microsoft Cor	Neutral	
REMEDIATION		<u>spoolsv.exe</u>		17:0		Known Good	747.5	microsoft,signed,val	Microsoft Cor	Neutral	
Blocked		vmtoolsd.e:		17:0		Known	81.5 KB	signed,valid	VMware, Inc.	Neutral	
reputation Malicious	٥	<u>Manageme</u>	Reset Risk Score	17:0		Known	59.5 KB	unsigned		Neutral	

- 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.

Change Certificate Status		×
CERTIFICATE STATUS Selected status is applied to all files signed by this certificate O Blacklist O Whitelist O Neutral COMMENTS *		
Enter comments		
	Cancel	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.

<b>▽</b> Filters	×	< Files	Certifica	ates 🙀 Cha	nge Certificate Status	🖸 Ana	alyze Events 🗸	×
SAVED FILTERS		FRIENDL		STATUS	ISSUER		THUMB PRINT	NOT VALID BEFORE UTCDAT
Select		O Microsof	t Windows Pu	Neutral	C=US, S=Washington, L=Re	edmond,	99922da31f07a02edb07cd8b60a	2018-06-06T18:57:34.000+0000
STATUS  Neutral Whitelisted Blacklisted SIGNATURE								
Is Root Microsoft  FRIENDLY NAME								
Equals <								
тнимв PRINT Equals v 99922da31f07a02edb07	cd8b60a137f144							
Reset Save	Save as				Showing 1 out of 1 ce	ertificates	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 **D**.

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 Files.
- 2. Select the Endpoint Server or Endpoint Broker.
- 3. Select one or more files and do one of the following:

RSA Investigate Respond Users Ho	sts <b>Files</b> Dashboards Reports		🗷 % 🕜 admin >
$\nabla$ Filters ×	endpointloghy View Certificates	File Status ☐ Analyze Events > Hore Actions >	
SAVED FILTERS	□ FILE NAME RISK SCORE ↑ FIRST SEEN TIME ON HO	STS REPUTATION SIZE SIGNATURE	PE.RESOURCES FILE STATUS
Select ~	□ ntoskrnl.exe 0 06/11/2020 17:05: 2	Known Good 9.5 MB microsoft,signed,valid	Microsoft Corpo Neutral
FILE NAME	□ <u>smss.exe</u> 0 06/11/2020 17:05: 2	Known Good 143.9 microsoft,signed,valid	Microsoft Corpo Neutral
Equals v e.g., Filename.dll	wininit.exe     0     06/11/2020 17:05: 2	Known Good 362.7 microsoft,signed,valid	Microsoft Corpo Neutral
FILE STATUS	Services.exe 2.05: 2	Known Good 659.0 microsoft,signed,valid	Microsoft Corpo Neutral
Neutral	Change File Status	Known Good 56.7 KB microsoft,signed,valid	Microsoft Corpo Neutral
Blacklist     Graylist	Analyze Events >     fontdrvhost.eve     Google Lookup > <sup>305</sup> 2	Known Good 802.6 microsoft,signed,valid	Microsoft Corpo Neutral
Whitelist	LosonULexe VirusTotal Lookup > 7:05: 2	Known Good 13.5 KB microsoft,signed,valid,	Microsoft Corpo Neutral
	Spoolsv.exe View Certificates 7:05: 2	Known Good 747.5 microsoft,signed,valid,	Microsoft Corpo Neutral
Blocked	Download File to Server	Known 81.5 KB signed,valid	VMware, Inc. Neutral
	ManagementAg Save a Local Copy 7:05: 2	Known 59.5 KB unsigned	Neutral
	Analyze File 7:05: 2	Known 111.3 signed,valid	Microsoft Corpo Neutral
Unknown     Known	VGAuthService, Reset Risk Score 7:05: 2	Known 160.0 unsigned	VMware, Inc. Neutral
Known Good     Invalid	□ <u>msdtc.exe</u> 0 06/11/2020 17:05: 2	Known Good 145.0 microsoft,signed,valid,	Microsoft Corpo Neutral
	UmiPrvSE.exe 0 06/11/2020 17:05: 2	Known Good 472.5 microsoft,signed,valid,	Microsoft Corpo Neutral
risk score	<u>SgrmBroker.exe</u> 0     06/11/2020 17:05: 2	Known Good 257.7 microsoft,signed,valid	Microsoft Corpo Neutral
• •	<u>SearchIndexer.exe</u> 0     06/11/2020 17:05: 2	Known Good 838.0 microsoft,signed,valid,	Microsoft Corpo Neutral
Reset Save Save as		Showing 100 out of 2480 files   1 selected	

- 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.

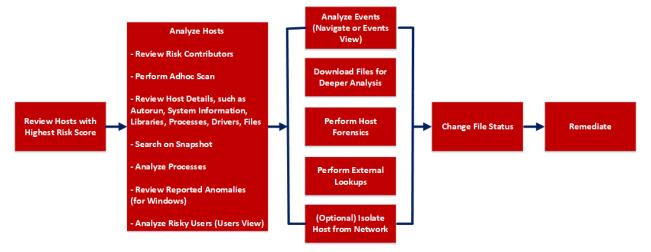
# **Investigating Hosts**

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 <u>Analyze Hosts</u> 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 <u>Analyzing Events</u>.
- 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 <u>Filter Hosts</u>.
- 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 <u>Analyze Processes</u>.
- Download suspicious files to the server for deeper analysis. For more information, see <u>Analyzing</u> <u>Downloaded Files</u>.
- Download MFT, process, or system dump to the server for forensic investigation. For more information, see <u>Performing Host Forensics</u>.
- 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 <u>Changing File Status or Remediate</u>.
- (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 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.

RSA Investigate Respo	ond Users He	osts Files Dashboards Repor	ts			[3	8 % 0	admin ≻
∀ Filters		endpointbrok V Z Analyz						<b>F</b>
		endpointloehvbrid1 - Endpoint Server	RISK SCORE	+ OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGE 🤅
Select	~ .	endpointloghybrid2 - Endpoint Server	N/A	Red Hat Enterprise Linux- 7.2	05/05/2020 05:59:16 pm	root	a day ago	Idle
HOST STATUS			N/A	Red Hat Enterprise Linux- 7.2	05/06/2020 07:38:30 am	root	a few seconds ago	ldle
Managed			N/A	Microsoft Windows 8.1 Enterprise	05/06/2020 07:47:47 am	WIN81X64-1\Administrator,Window Manager	a few seconds ago	Idle
Roaming     Isolated			31	Ubuntu 18.04.4 LTS	05/05/2020 01:07:05 pm	kslp	a day ago	Idle
RISK SCORE			٢	Red Hat Enterprise Linux 8.1 (Ootpa)	05/06/2020 07:20:35 am	kslp	a day ago	Idle

- 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 <u>Analyzing</u> <u>Risky Users</u>.
- 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.

## **View Agent History**

You can view the list of commands issued to the agents (by the server or actions performed by any analyst) in the Host view and Host details. By default, commands are sorted based on the command time.

To view the commands:

- 1. Go to **Hosts**.
- 2. Do any one of the following,
  - To view all commands, click E. You can also filter commands, for more information see Filter Hosts.

E	endpointbrok $\vee$		'Analyze Events	✓ Ø Start	Scan 🛛 🖾 Sto	p Scan	More Actions $\vee$				Ê
	HOSTNAME	RISK S	AGENT LAST	AGENT SCAN ST	AGENT GROU.	AGENT MODE	AGENT VERSION	AGENT- D	AGENT - INSTALL TI	AGENT ID	LAST SCAN TI

The Agent History view is displayed. For more details, see Analyze History.

- To view commands specific to a particular host:
  - Click the host for which you want to view the commands.
  - In the Host details view, click **History** tab. You can also filter commands, for more information see <u>Filter Host Details</u>.

The History view is d	isplayed. F	for more	details, s	see <u>Ana</u>	alyze	History.			
RSA Investigate Respond Users	Hosts Files Dash	boards Reports					[	z % 🕐 adr	min >
	sent scan status agent anning 2 day	LAST SEEN AGENT VI ago 11.5.0.0							×
DETAILS PROCESSES AUTORUNS FILES				TEM INFO HIS	TORY				Q
∇ Filters									
COMMAND TIME CUSTOM DA	TE COMMAND TIME	COMMAND TYPE	HOST NAME	USER NAME	STATUS	COMMAND PARAMETER	PROCESSED TIME	LAST RETRIEVAL TIME	-
	v 06/15/2020 08:06:29 am	Download File		system	<ul> <li></li> </ul>	path = C:\Windows\assembly	06/15/2020 08:06:35 am	06/15/2020 08:06:35 am	1
COMMAND TYPE	06/10/2020 09:00:38 am	Scan		admin	<ul> <li></li> </ul>		06/10/2020 09:12:52 am	06/10/2020 09:00:50 am	1
	06/10/2020 07:15:52 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path = C:\Windows\assembly	06/10/2020 07:16:19 am	06/10/2020 07:16:19 am	1
STATUS	06/08/2020 07:18:47 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path = C:\Windows\assembly	06/08/2020 07:19:10 am	06/08/2020 07:19:02 am	1
STATUS	06/08/2020 07:18:47 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path = C:\Windows\assembly	06/08/2020 07:19:06 am	06/08/2020 07:19:02 am	1
	06/08/2020 07:18:47 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path = C:\Windows\assembly	06/08/2020 07:19:06 am	06/08/2020 07:19:02 am	1
REQUEST TYPE	06/08/2020 07:18:47 am	Download File		system	<ul> <li></li> </ul>	path = C:\Windows\assembly	06/08/2020 07:19:05 am	06/08/2020 07:19:02 am	1
	06/08/2020 07:18:47 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path - C:\Windows\assembly	06/08/2020 07:19:05 am	06/08/2020 07:19:02 am	1
COMMAND PARAMETER	06/08/2020 07:18:47 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path = C:\Windows\assembly	06/08/2020 07:19:04 am	06/08/2020 07:19:02 am	1
Contains    Enter Value	06/08/2020 07:18:47 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path = C:\Windows\assembly	06/08/2020 07:19:04 am	06/08/2020 07:19:02 am	1
	06/08/2020 07:18:47 am	Download File		system	<ul> <li>Image: A second s</li></ul>	path = C:\Windows\assembly	06/08/2020 07:19:08 am	06/08/2020 07:19:02 am	1
	06/08/2020 07:18:47 am	Download File		system	<ul> <li></li> </ul>	path = C:\Windows\assembly	06/08/2020 07:19:08 am	06/08/2020 07:19:02 am	1
Reset	06/08/2020.07-18-47m	Download Eilo	And a second second second	odom	<u></u>	neth - Cillindounionramble	06/08/2020 07-19-07 am	06/08/2020 07-10-02 ~m	4
				Showing 1	00 out of 121 Co	ommands			

## **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.



In the **Host** view > click **EO**, to filter the commands on command type, status, host name, request type, command parameter and command time. In the Command Time field, you can filter by custom date range.

**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.

RSA Investigate Respond Users H	osts Files Dashboa	rds Reports		
$\nabla$ Filters ×	endpointbrok V			
SAVED FILTERS		RISK SCORE 🛛 🗸	OS - DESCRIPTION	LAST SCAN TIME
Select ~		N/A	Microsoft Windows 10 Pro for Workstati	05/08/2020 02:21:35 pm
HOST STATUS		N/A	Red Hat Enterprise Linux- 7.2	05/05/2020 05:59:16 pm
Managed		N/A	Red Hat Enterprise Linux- 7.2	05/06/2020 07:38:30 am
Roaming     Isolated		31	Microsoft Windows 8.1 Enterprise	05/06/2020 07:47:47 am
		(31)	Ubuntu 18.04.4 LTS	05/05/2020 01:07:05 pm
RISK SCORE		 (0)	Red Hat Enterprise Linux 8.1 (Ootpa)	05/06/2020 07:20:35 am
100	—			
···············		N/A	Microsoft Windows 10 Education	
			Microsoft Windows 7 Enterprise	
HOSTNAME		N/A	Microsoft Windows 10 Enterprise	
Equals ~ Enter Value		•	Ubuntu 16.04.6 LTS	05/07/2020 08:44:18 am
USERNAME		•	CentOS Linux 8 (Core)	05/06/2020 07:32:31 am
Equals v Enter Value		N/A	Microsoft Windows 10 Education	
AGENT GROUPS		N/A	Microsoft Windows 7 Enterprise	05/08/2020 06:53:58 am
Equals v Enter Value				
Equals ~ e.g.,00:00:00:00:00				
Reset Save Save as			Showing 13 out of 13	hosts   0 selected

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 ||.

<b>Y</b> Filters		×				
USERNAME		<b>^</b>				
Equals $\lor$	Enter value					
AGENT GROUPS						
Equals $\vee$	Enter value					
NIC MAC ADDRES	5					
Equals $\vee$	e.g.,00:00:00:00:00:00					
IPV4						
Equals $\vee$	10.87.225.68  10.40.7.11					
AGENT LAST SEEM		~				
LAST SCAN TIME	) ci	USTOM DATE				
OPERATING SYST	M					
Windows						
🗆 Mac						
AGENT MODE						
Reset	Save S	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.

<b>Y</b> Filters		×	
RISK SCORE		100	•
0		· · · ·	
HOSTNAME			
Equals ~	Enter value		
USERNAME			
Equals ~	Enter value		
AGENT GROUPS			
Equals $\vee$	Enter value		
NIC MAC ADDRESS			
	e.g.,00:00:00:00:00:00:	:00	
IPV4			
Equals $\vee$	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  $\mathbf{\overline{u}}$ .

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

You can also filter the commands on command type, status, host name, request type, command

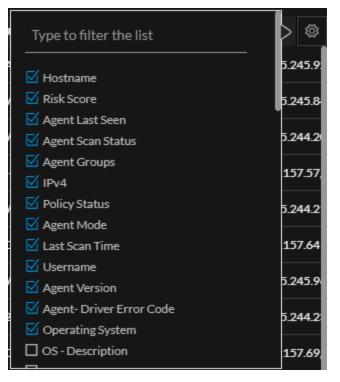


parameter and command time (In which you can filter by custom date range), by clicking

## 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 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 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 dialog.

**Note:** (Version 11.5.1) By default, the scan utilizes 25% of the CPU. You can click CPU Maximum and select a value between 5% and 100%. A lower CPU Maximum value increases the scan time but allows other processes to utilize the CPU. Increasing the CPU Maximum limit reduces the scan time but may result in more CPU usage.

3. Click **Start Scan** in the dialog. This performs a quick scan of all executable modules loaded in memory.

The following are the scan statuses:

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

## Analyze Hosts Using the Risk Score

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

To analyze the hosts using the risk score:

1. Go to Hosts.

The Hosts view is displayed.

- 2. In the Server drop-down list, select the Endpoint server or Endpoint Broker server to view the hosts.
- 3. Select the host and do any of the following.
  - Click a row to view the risk associated with the host in the **Risk Details** panel.
  - Click the hostname to investigate the host.
- 4. In the Alert Severity panel, click the alert severity such as Critical, High, Medium, or All.

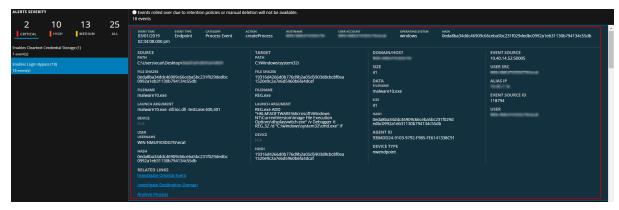
The list of distinct alerts is displayed along with the total number of events associated with the alert.

5. Click an alert to view the associated events.

ALERTS SEVERITY $2 10 12 25$	Events rolled over due to retention policies or manual deletion will not be available. 18 events	HOST DETAILS POLICY DETAILS X
2 10 13 25 critical high medium all	EVENT TIME EVENT TYPE CATEGORY ACTION HOTTNAME USER ACCOUNT OPERATING SYSTEM HASH 03/01/2019 Endpoint Process Event createProcess windows 0eda8/	Type to filter list
Enables Cleartext Credential Storage (1) 1 event(s)	02:34:38:000 pm	Show details with values only Users
Enables Login Bypass (18)	FILE NAME LAUNCH ARGUMENT PATH SOURCE malware10.exe malware10.exe -dllioc.clll testcase:400,401 C.\Users\ecat\Desktop\	Name WIN-NMUFVI3DGTN\ecat
18 event(s)	TARGIT REG.exe REG.exe ADD "HKLM-COTMAREIMErrowsfitWindows C-Windows\system32\ MTCurrentWindows/aligable/alignerrowsfitWindows C-Windows\system32\ Optionstaligable/alignerrowsfitWindows/ "C-Windows\system32\cnd access" A Bebugger A REG.52 /d	Session ID <b>2</b> Is Admin <b>true</b>
	"C-windows/system/s/ctrid.exe" //	Groups Administrators
	03/01/2019 Endpoint Process Event createProcess Oeda81 02:34:08.000	Users
	pm FILE NAME LAUNCH ARGUMENT PATH	Name <u>Window Manager\DWM-1</u> Session ID 1
	SOURCE malware10.exe malware10.exe dillioc.dll-testcase400,401 C:\Userstean\Desktop\ TARGT REG.exe ADD 'HKLM/SOFTWARE\Microsoft\Windows C:\Windows\opstem32\	Is Admin false
	NTCurrentVersionUmage File Execution Optionstullina ace? // Debuger / REG.sz //d "C/windows/system32/cmd.exe? /f	Network Interfaces
	EVENT TIME EVENT TYPE CATEGORY ACTION HOSTNAME USER ACCOUNT OPERATING SYSTEM HASH 03/01/2019 Endpoint. Process Event createProcess windows Oeda88	Name Intel(R) PRO/1000 MT Networ MAC Address
	02:34:08.000 pm	IPv4 10.40.7.16

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.

100.000	NATION CONTRACTORS		×
CONTEXT HI	GHLIGHTS		ACTIONS
0	0	0	≣ Add/Remove from List
INCIDENTS	ALERTS	LISTS	Q Pivot to Investigate > Navigate
- ENDPOINT	- CRITICALITY	- ASSET RISK	Q Pivot to Investigate > Hosts/Files
ENDPOINT	CRITICALITY	ASSET KISK	Q Pivot to Endpoint Thick Client
	View Context		Q Pivot to Archer
ACTION createProc	HOSTN		USER ACCOUNT

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

	vents		eletion will not be a	wailable.			
CRITICAL HIGH MEDIUM ALL 03/ 02:			ACTION createProcess	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM WINDOWS	назн 0eda8ba34d
Paralles Login Bypass (18) Enables Login Bypass (18) 18 event(s) Fill	NUSers\ \Desktop\ LE SHA256 edskba34dc45909c66ceba5bc231 992a1eb31130b794134c55db LENAME alware10.exe AUNCH ARGUMENT halware10.exe ALDC-dll-testcase4 VA SER SERNAME	f029dedbc 400,401	1520e9c2a7ed FILENAME REG.exe LAUNCH ARGUI REG.exe ADD "HKLMSOFIV NTCLUTENTVE Options/displ REG.52 /d "C: DEVICE N/A HASH 19316d4266d	- 0b776d9b2a05d5903d8cbr 6d5960b6fa4dcaf MENT	c8f0ea D Fin m f f f f f xe" /f f	ATA ILENAME nalware10.exe Ize	i5db

- 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 ondemand 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.

RSΛ	Investigate	Respond	Users	Hosts Files	Dashboards	Reports					2 %	?	admin >
100 wind	lows	ď :	agent scan Idle		LAST SEEN seconds ago	agent versi 11.5.0.0	ON s	NAPSHOT	тіме <b>(</b>	06/24/2020 21:30:33			
DETAILS	PROCESSES	AUTORUNS	FILES	DRIVERS LIE	BRARIES AN	OMALIES	DOWNLO	NDS S	YSTEM				Q
ALERTS SEVER	Тү	0	2	<ul><li>③ Events rolle</li><li>28 events</li></ul>	d over due to rete	ention policies	or manual de	letion wil	l not be a			LS	
	нідн	MEDIUM	ALL	EVENT TIME 06/29/2020	0 13:40:54.000	event type Endpoint	category File	<b>action</b> N/A	HOST				
Blacklisted File (2 28 event(s)	28)			FILE NAME sigc-2.0.dll							l		
Runs Blacklisted	File (3)				<b>ile name</b> I/A	LAUNCH ARG	JMENT		<b>path</b> N/A		S Windows-sec	urity	
3 event(s)				TARGET N									
				EVENT TIME 06/29/2020	0 13:40:54.000	EVENT TYPE Endpoint	category File	<b>action</b> N/A	HOST		WINDOWS1		
				FILE NAME intl.dll	HASH 639ff2ef6bcbaa						<ul><li>2</li><li>Administrato</li></ul>	rs	
					<b>ile name</b>	LAUNCH ARG	JMENT		<b>PATH</b> N/A	Users			
											Window Man	ager\DWN	

### **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 **\overline{\mathbf{u}}**.

In the **Host** view > **Files** tab, you can filter the files available on host, and files deleted from host. The result of files deleted from host depends on the data retention policy configured in the **Endpoint Config** view > **Data Retention Scheduler** tab. By default, data retention policy is configured for 30 days, this means only 30 days of deleted files are stored in the Endpoint server. These filter options are disabled if **All Files Available on Host** toggle is disabled.

In the **Host** view > **History** tab, you can filter the commands on command type, status, host name, request type, command parameter and command time. In the Command Time field, you can filter by custom date range.

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  $\mathbf{\overline{u}}$ .

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

### **Search Files on Host**

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 the matching files present on the host in **All Files Available on Host** category and in the respective **snapshot** category with the details, such as file name, signature information, and checksum. In addition, the **snapshot** category displays the system interaction, for example, ran as process, library, autorun, service, task, or driver. To view more details, click the **filename** or **system interaction** link.

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 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.

100	vindows		AGENT SCAN STATU Idle	JS AGENT LAST S a few seconds		510N 51	NAPSHOT TIME	11/18/201	.909:28:10 am 🗸 🔲 👋
DETAILS	PROCESSES	AUTORUN	S FILES	DRIVERS LIE	BRARIES ANO	MALIES D	OWNLOADS	SYSTEM	MALWARE.EXE
		ACTORON	3 11223						ightarrow all files available on host (0)
ALERTS SEV	(ERITY			(1) Events rolle 12 events	d over due to retent	ion policies or	manual deletic	on will not be	2019-11-18 09:28:10.792 am (2)
2	0	1	3	12 events					
	AL HIGH	MEDIUN		EVENT TIME 11/18/2019	9 09:31:17.000 am	event type Endpoint	CATEGORY Autorun	<b>action</b>	malware.exe Signed, Notepad++ C:\Program Files (x86)\Notepad ++\ 21daec4328eb08e28a0f55d0590298ae193743de40900ab79 b3610c113b83ba6
Login Bypass 12 event(s)	Configured (12)			FILE NAME CMd.exe	HASH db06c3534964e3 ILE NAME	fc79d27631	FNT	РАТН	[MEMORY_PROCESS_malware.exexe_406392AFD9E9507486DF51 AA0586AA3C] (Ran as Process) Unsigned C:\Program Files (x86) \Notepad+\ efd8c9994843d5147e4138f21b24d305f788040967 7d604c7ead2c377d128183
Possible Logir 12 event(s)	n Bypass (12)			SOURCE					> 2019-11-12 09:36:33.321 am (0)
									> 2019-11-08 10:44:46.674 am (0)
				EVENT TIME 11/18/2019	9 09:31:17.000 am	EVENT TYPE Endpoint	CATEGORY Autorun	action P	
				FILE NAME	назн db06c3534964e3	fc79d27631			
					ILENAME	LAUNCH ARGUM	ENT	PATH	

This file is run as a Process.

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

100 windows	5 AGENT LAST SEEN AGENT VERSION a few seconds ago 114.0.0	<u>11/18/2019 09:28:10 am</u> ×
DETAILS PROCESSES AUTORUNS FILES	DRIVERS LIBRARIES ANOMALIES DOWNLOADS	MALWARE.EXE
		v all files available on host (0)
	<ul> <li>Events rolled over due to retention policies or manual deletion</li> <li>events</li> </ul>	on will not be a ~ 2019-11-18 09:28:10.792 am (2)
2 0 1 3	EVENT TIME EVENT TYPE CATEGORY 11/18/2019 09:31:17.000 am Endpoint Autorun	ACTION         H         ++         21daec4328eb08e28a0f55d0590298ae193743de40900ab79           N/A         K         b3610c113b83ba6         b3610c113b83ba6
Login Bypass Configured (12) 12 event(s)	FILE NAME HASH STILL RAME HASH FILE NAME LAUNCH ARGUMENT	[MEMORY_PROCESS_malware.exexe_406392AFD9E9507486DF51           AA05B6AA3C[ (Ran as Process)         Unsigned         C.\Program Files (x86)           Vlotepad++\efd8c999483d5147e4138f21b24d305f788040967         7dbddr2ed2c57df1813
Possible Login Bypass (12)	FILE NAME LAUNCH ARGUMENT SOURCE N/A N/A	N/A > 2019-11-12 09:36:33.321 am (0)
12 event(s)	target N/A N/A	> 2019-11-12 09:36:33.321 am (0) > 2019-11-08 10:44:46.674 am (0)
	EVENT TIME EVENT TYPE CATEGORY 11/18/2019 09:31:17.000 am Endpoint Autorun	action f N/A <i>E</i>
	FILE NAME HASH cmd.exe db06c3534964e3fc79d27631	
	FILE NAME LAUNCH ARGUMENT	ратн
	SOURCE N/A N/A TARGET N/A N/A	

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

### **Analyze Processes**

To analyze the process:

1. In the Hosts details, select the Processes tab.

	igate Respond	Users Ho	osts Files	Dashboards	Reports					2 %	⑦ admin >
100 windows		agent scan st <i>i</i> <b>Idle</b>		LAST SEEN Seconds ago	agent version 11.5.0.0 snapshot	тіме 06/24/2020 21:	30:33 🗸				
DETAILS PROCI	ESSES AUTORUNS		DRIVERS LIB	RARIES AN	OMALIES DOWNLOADS	SYSTEM INFO HIS	TORY	MALWARE.EXE			×
<b>▽</b> Filters			Processes								
				NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILE PATH
Equals v e.g., F						100		Known Good	Blacklisted		C:\Windows\System
					100	100		Known Good	Blacklisted		C:\Windows\System
Neutral Blacklist					<b>100</b>	100		Known Good	Neutral		C:\Windows\System
Graylist						100		Known Good	Neutral		C:\Windows\System
Whitelist					100	100		Known Good	Neutral		C:\Windows\System
REPUTATION						100		Known Good	Neutral		C:\Windows\System
Suspicious						100		Known Good	Neutral		C:\Windows\System3
Unknown Known						100		Known Good	Neutral		C:\Windows\System
☐ Known Good ☐ Invalid			svchost.ex	2		100	2	Known Good	Neutral	-	C:\Windows\System3

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

RSA Investigate Respond Users Hosts Files D	ashboards Reports			11 %	⑦ admin >
100 AGENT SCAN STATU	S AGENT LAST SEEN AGENT VERSION a few seconds ago 11.4.0.0	snapshot time 11/18	/2019 09:28:10 am		
DETAILS PROCESSES AUTORUNS FILES	DRIVERS LIBRARIES ANOMALIES	DOWNLOADS SYS	TEM INFO HISTO	DRY	MALWARE.EX
<b>∀</b> Filters ×	Processes 🖸 Analyze Process	🕅 Change File Status 🛛 🖸	Analyze Events	/ i More /	]
PROCESS NAME		LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION
Equals v e.g., Filename.dll		٩	0	1	-
FILE STATUS	ntoskml.exe	٥	0	1	-
Neutral     Blacklist	Smss.exe	•	•	1	-
Graylist	GoogleCrashHandler64.exe	٥	0	4	-
Whitelist	□ ~ <u>csrss.exe</u>	•	•	1	-
		٥	٥	1	-
Malicious     Suspicious		•		1	-
Unknown Known	🗋 🖌 <u>winlogon.exe</u>	•	 (0)	1	
Known Good     Invalid		<u> </u>	<u>)</u>	1	-

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

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

RSA Investigate Res	pond Users <b>Hosts</b>	Files Dashbo	ards Rep	orts					🖻 拨 🕐 admin >
100 vindows			NT VERSION		11/18/2019 09:28::	10 am 🗸			
DETAILS PROCESSES AUT	ORUNS FILES DRIV	ERS LIBRARIES	ANOMALIE	S DOWNLOADS	SYSTEM INFO	HISTORY	MALWA	ARE.EXI	E X
▼ Filters         Processes         ⊡	Analyze Process 🛛 🛱 Cha	nge File Status	analyze Events	More V			TREE VIEV	v	calcexe X
PROCESS NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	SIGNATURE	DOWNLOADED		FILE DETAILS LOCAL RISK DETAILS HOSTS
		100			Neutral	microsoft,			Type to filter list
MEMORY PROCESS malware.execution	4063 0	٢			Neutral	unsigned		-	Show details with values only
🗹 <u>calc.exe</u>	$\odot$	٥	1	-	Neutral	microsoft,	-		General
conhost.exe	٥	۲	1	-	Neutral	microsoft,	-	-10	FileName calc.exe
	•	•			Neutral	microsoft,		Obje	Entropy 6.962615335730437
<u>Grss.exe</u>	•	•			Neutral	microsoft,		Obje	Size 897.0 KB
G1755.000	•	•	1		Neutral	microsoft		Obje	Format pe
	•	•	1		Neutral	microsoft			Signature
		•	1		Neutral	microsoft			- Features microsoft,signed,valid,catalog
									Timestamp 11/20/2010 07:35:27.000 pm
GoogleCrashHandler.exe	<u> </u>	<u> </u>			Neutral	signed,valid			Thumbprint 02eceea9d5e0a9f3e39b6f4ec3f
GoogleCrashHandler64.exe	•	•			Neutral	signed_valid			Signer Microsoft Windows
jusched.exe		0	1	-	Neutral	signed,valid			

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

RSΛ	Investigate	Respond	Users Hos	t <b>s</b> Files Dashbo	oards Reports		
100 win	dows	:	agent scan stat Idle	us AGENT LAST SEEN a few seconds ag		SNAPSHOT TIME	06/24/2020 21:30:33 🗸
DETAILS	PROCESSES	AUTORUNS	FILES DI	RIVERS LIBRARIES	ANOMALIES DOV	WNLOADS SYSTE	MINFO HISTORY
< Process	ses Process E	Details					
PROCESS N	AME		OWNER	PPID	РАТН		
dwm.exe			DWM-2	1460	C:\Windows\System32	2\	
> Loade	d Libraries (8)						
> Image	Hooks (0)						
✓ Suspic	ious Threads (0	)					

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

For example,

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

### 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

To analyze the files, you can do either one of the following based on your requirement.

• In the Hosts view, select the Files tab.

You can view the list of all files (reported as part of scan and tracking) on the host including the deleted files.

RSA Investigate Respond	Users H	losts Files Dashboards	s Reports						🛃 % 🕐 admin >
31 windows	AGENT	r scan status agent last se ing 2 days ago	en agent version 11.5.0.0		06/20/202	20 06:30:11 am 🔗 🔗			
<b>▽</b> Filters	×	Files 🙀 Change File Sta							ALL FILES AVAILABLE ON HOST
		FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	FILE STATUS	REPUTATION	DOWNLOADED	PATH
Equals v e.g., Filename.dll		powershell.exe	31	31		Neutral	Known Good		C:\Windows\System32\Window
FILE STATUS		dwm.exe	٥	٥		Neutral	Known Good		C:\Windows\System32\
Neutral		pnrpnsp.dll	0	•		Neutral	Known Good		C:\Windows\SysWOW64\
Blacklist     Graylist		Microsoft.WSMan.Manage.	. (0)	•		Neutral	Known Good		C:\Windows\Microsoft.NET\as
Whitelist		msidle.dll	•	•		Neutral	Known Good		C:\Windows\System32\
		advapi32.dll	•	•		Neutral	Known Good		C:\Windows\System32\
Malicious     Suspicious			•	•		Neutral	Known Good		C:\Windows\System32\
Unknown			•	•		Neutral	Known Good		C:\Windows\System32\wbem\
C Known Good			•	•		Neutral	Known Good		C:\Windows\System32\drivers
Invalid			 (0)	•		Neutral	Known Good		C:\Windows\System32\drivers
SIGNATURE			•	•		Neutral	Known Good		C:\Windows\System32\drivers
Reset					showing 3622	out of 3622 files   0 sel	erted		

• To view the files reported as part of scan snapshot, you must disable All Files Available On Host toggle and select the scan time form the Snapshot drop-down list.

Example for analyze files, 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.

### **Analyze History**

In the Host details, select the **History** tab. This tab lists the commands along with the respective status and additional details.

When you review the history, look for the command status and retrieval count to check if the agent retrieved the commands.

Below are some examples:

- A file download command is issued, but the file is deleted on the host. In this case status of the command is failed as the file is not downloaded.
- The retrieval count increases, but the command is not processed. This happens when an analyst requests a large number of files (For example, MFT, system dump, or process dump), and the connection breaks when the agent uploads these files.
- If the agent command is not retrieved, the agent is either offline or busy processing other commands (For example, uploading a system dump). In this case, the status of the command shows pending.

To view more details, click the **Hostname** link highlighted in blue. The Hosts details view is displayed. In the case of MFT, download file, system dump, and process dump command types, **Downloads** tab is displayed with details such as file name, type, status, size, downloaded time and SHA256 of the file, when you click on the **Hostname** link.

### **Export Host Details or Files to JSON File**

Note: Export Host details option is disabled if there is no snapshot time.

To export host details or files to JSON file:

- 1. Go to Hosts.
- 2. Select the hostname to open the host details.
- 3. Click (More) beside the hostname and do any of the following:
  - To export the scan data categories for the host, select **Export Host Details**. This exports files such as:
    - allfiles.json This file consists of the file name, file path, signature, file checksum, and so on that is reported as part of scan and tracking.
    - fileContext.json This file consists of the file name, file path, signature, file checksum, and so on that is reported during the host scan.
    - machinedetails.json This file consists of the machine details, including hardware, operating system, interfaces, and so on, along with the agent details like version, policy details.

**Note:** If Endpoint Broker is selected and a host is communicated with multiple Endpoint servers, during the host details export, all files and details of the host are exported from the Endpoint server where the selected snapshot is stored.

Note: allfiles.json file is exported irrespective of the selected snapshot.

- To export all the files available on the host, select Export Files. This exports:
  - allfiles.json This file consists of the file name, file path, signature, file checksum, and so on that is reported as part of scan and tracking.

### 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 Hosts > Host Details (Autorun, Files, Drivers, Libraries, or Anomalies tab).
- 2. Right-click one or more files, or in the More Actions drop-down list in the toolbar, do the following:

RSA Investigate Respond Users H	osts Files Das	hboards Reports					2 %	() admin >				
100 vindows Idle	ATUS AGENT LAST S a few second	SNADSHOT	TIME 06/24/2020 21	30:33 v				Х				
DETAILS PROCESSES AUTORUNS FILES	DETAILS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY											
∇ Filters           ×           Processes           ×           ×           ×           ×           ×           ×           ×           ×           ×           ×           ×           ×         ×           ×         ×           ×         ×           ×         ×         ×												
PROCESS NAME		LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILE PATH				
Equals v e.g., Filename.dll	dwm.exe		100	2	Known Good	Blacklisted		C:\Windows\System3				
FILE STATUS	⊠ <u>dwm.exe</u>	<b>^</b>	100		Known Good	Blacklisted		C:\Windows\System3				
□ Neutral □ Blacklist	svchost.exe	Analyze Process	100	2	Known Good	Neutral		C:\Windows\System3				
🗆 Graylist	svchost.exe	Change File Status Analyze Events	100	2	Known Good	Neutral		C:\Windows\System3				
U Whitelist	svchost.exe	Google Lookup	100	2	Known Good	Neutral		C:\Windows\System3				
REPUTATION	svchost.exe	VirusTotal Lookup	100	2	Known Good	Neutral		C:\Windows\System3				
□ Suspicious	svchost.exe	Download Process Dump to Server	100		Known Good	Neutral		C:\Windows\System3				
🗆 Unknown 🗆 Known	svchost.exe	Download File to Server	100	2	Known Good	Neutral		C:\Windows\System3				
Known Good     Invalid	svchost.exe		100		Known Good	Neutral		C:\Windows\System3				
	svchost.exe		100	2	Known Good	Neutral		C:\Windows\System3				
SIGNATURE	svchost.exe	 <sup>10</sup>	100	2	Known Good	Neutral		C:\Windows\System3				

• 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 **Hosts**.
- 2. Select the hosts that you want to delete from the Hosts view and do one of the following:

RSΛ	Investigate Respond Use	ers H	osts	Files	Dashboards	Reports			٩ţ	% 0	admin >
<b>▽</b> Filters			e	endpointb	orok 🗸 🕴	Analyze Events	✓ 🖉 Start Scan		: More Act	ions ∨	Ê .
SAVED FILTERS				HOSTNAME	RISK SCO	OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGENT SCAN STA	A AGEN 🔅
Select		~			100	Microsoft Windows 10	06/28/2020 21:30:08	WINDWOS	a few seconds ago	Scanning	Windows-s
HOST STATUS			Ø				16/24/2020 21:30:33	WINDOWS	a few seconds ago	ldle	Windows-s
□ Managed				-	Analyze Events		> )6/28/2020 14:30:22		a few seconds ago	ldle	
Roaming			—		Delete						
□ Isolated					Start Scan						
RISK SCORE					Stop Scan						
RISK SCORE		100			Network Isolation	n	>				
• •		-•			Download MFT	to Server					
0					Download Syst	em Dump to Server					
HOSTNAME					Download Files	to Server					
Equals $\vee$	Enter Value				Reset Risk Sco	re					

- 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:

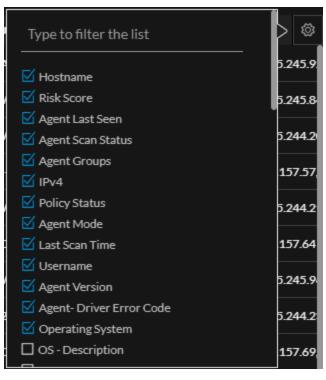
- 1. Go to **Hosts** view.
- 2. Filter the hosts based on the Agent version, and delete these hosts.

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 **Hosts**.
- 2. Select the columns by clicking 🖸 in the right-hand corner. The following example shows the dropdown 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 **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.

RSA Investigate Respond	Users H	losts	Files Dashb	oards Reports			٦	9 % 0	admin >
<b>∀</b> Filters		E	$\exists$ endpointbrok $\vee$						E
		0	HOSTNAME	RISK SCORE +	OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGE
Select				N/A	Microsoft Windows 10 Pro for Workstati	05/08/2020 02:21:35 pm	Window Manager\DWM-2,WIN1909-64B-0\e	a few seconds ago	Idle
HOST STATUS				N/A	Red Hat Enterprise Linux- 7.2	05/05/2020 05:59:16 pm	root	2 days ago	Idle
Managed				N/A	Red Hat Enterprise Linux- 7.2	05/06/2020 07:38:30 am	root	a few seconds ago	Idle
Roaming     Isolated				31	Microsoft Windows 8.1 Enterprise	05/06/2020 07:47:47 am	WIN81X64-1\Administrator,Window Manager	a few seconds ago	ldle
RISK SCORE				31	Ubuntu 18.04.4 LTS	05/05/2020 01:07:05 pm	ksip	3 hours ago	ldle
	100			٢	Red Hat Enterprise Linux 8.1 (Ootpa)	05/06/2020 07:20:35 am	kstp	2 days ago	Idle
• · · · · · · · ·				N/A	Microsoft Windows 10 Education			20 minutes ago	Idle
0				N/A	Microsoft Windows 7 Enterprise			a few seconds ago	Idle

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**. On all the tabs within the Hosts view, the message Host is migrated to <Server-name> is displayed. You view the host details by clicking the <Server-name>. 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 Hosts.
- 2. Click the host name you want to analyze.
- 3. In the Host Details panel, under the Users category, click the name.

RSA 🗉	nvestigate	Respond	Users H	osts Files Dashboards	Reports			📰 % 🕜 admin >
100 Win window	dwos10- <sup>"s</sup>	0 2 :	agent scai <b>Idle</b>	n status Agent Last seen a few seconds ago	AGENT VERSION 11.5.0.0	SNAPSHOT TIME 06/25/2020 21:30:30		
DETAILS P	ROCESSES	AUTORUNS		DRIVERS LIBRARIES AN	OMALIES DOWNLOA	DS SYSTEM INFO HISTORY		
ALERTS SEVERIT		0	1	© Events rolled over due to rete 70 events	ntion policies or manual de	letion will not be available.		HOST DETAILS POLICY DETAILS X
	<b>О</b>   нібн	0 MEDIUM	<b>1</b>	EVENT TIME 06/25/2020 14:01:27.000	event type category Endpoint File	action hostname user account N/A <b>Windwos10-0</b> N/A	OPERATING SYSTEM F	Type to filter list
Blacklisted File (70) 70 event(s)				FILE NAME SOURCE N/A TARGET N/A	<b>LAUNCH ARGUMENT</b> N/A N/A			Show details with values only Groups
				EVENT TIME 06/25/2020 14:01:26.000	event type category Endpoint File	ACTION HOSTNAME USER ACCOUNT N/A Windwos10-0 N/A	OPERATING SYSTEM F windows ji	Groups Windows-security Users
				FILE NAME SOURCE N/A	LAUNCH ARGUMENT			Name WINDWOS10-0\ecat Session ID 2
				TARGET N/A				Groups Administrators
				EVENT TIME 06/25/2020 14:01:26.000 HASH	EVENT TYPE CATEGORY Endpoint File	ACTION HOSTNAME USER ACCOUNT N/A <b>Windwos10:Ω</b> N/A		Users Name Window Manager\DWM-1
				36526070f52c86b6d8ac7cf	040b014bd			
				SOURCE N/A TARGET N/A	N/A N/A	N/A N/A		Network Interfaces

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

## **Resetting Risk Score of Hosts**

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

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

#### To reset the risk score of a host:

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

R	SA Invest	igate Respond	U	sers Hosts	Files Dashbo	oards Rep	orts
٦	Filters 🛛 🖯 endp	pointbrok 🗸 📗		Analyze Events	✓ Start Scan	Stop Scan	i More V
	HOSTNAME		R	ISK SCORE 🛛 🗸	OS - DESCRIPTION		LAST SCAN TIME
				N/A	Microsoft Windows 10 Pro	o for Workstati	05/08/2020 02:21:35 pm
				N/A	Red Hat Enterprise Linux-	7.2	05/05/2020 05:59:16 pm
Ø	Balliani)			N/A	Red Hat Enterprise Linux-	7.2	05/06/2020 07:38:30 am
	404614655	Analyze Events	>	31	Microsoft Windows 8.1 Er	terprise	05/06/2020 07:47:47 am
	And a state of the	Delete		31	Ubuntu 18.04.4 LTS		05/05/2020 01:07:05 pm
	644-846-63	Start Scan Stop Scan		0	Red Hat Enterprise Linux 8	3.1 (Ootpa)	05/06/2020 07:20:35 am
Ø		Reset Risk Score		N/A	Microsoft Windows 10 Ed	ucation	
	-	Reset Hisk Score		N/A	Microsoft Windows 7 Ente	erprise	

- 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 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 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 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.

RSA Investigate Respond Use	rs <b>Hosts</b> Files Dashboards Reports	2 % 0	
100 windows	N STATUS AGENT LAST SEEN A CENT VERSION SNAPSHOT TIME 11/11/2019/02-41.06.pm		
DETAILS PROCESSES AUTORUNS FILES D	RIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY		
ALERTS SEVERITY 3 3 15 21	© Events rolled over due to retention policies or manual deletion will not be available. 3 events		
CRITICAL HIGH MEDIUM ALL	DYDRTINKE DYDRTTYK CATEORY ACTION HOSTNAMS USERACCOUNT OVERATING/SYSTEM RELINANS HASH 11/29/2019 09-59 25,5000 am Endpaint Process Event createProcess	81b5bbe4128e413f19a0	ēp
Enables Login Bypass (1) 1 event(s) Possible Mimikata Activity (3)	SOURCE TARGET TARGET DOMAIN/HOST USER SRC WITH CUM/indow15ystem32, CUMindow15ystem32, DATA CUM/indow15ystem32, PIELNASE PIELNASE ALLAS IP		
Seventia Journ Powershell Involte Minikats Function (1) Farvettia	FILE SU236         FILE SU		
	RELATED UNKS Investigate Original Event Investigate Original Event Investigate Destination Domain Analyza Process		

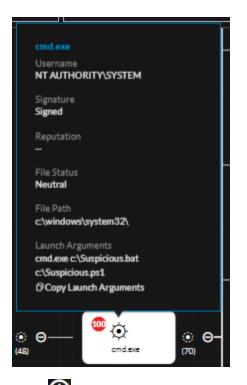
Clicking **Analyze Process** displays the process visualization. For each node, the process name, risk score, and type of activity the selected process has performed (network (1996)), file (1996), or registry (1996)), are displayed. Optionally, you can change the time range to view data.

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

endpointloghybrid1 - Concentrator > 11/25/2019 05:26am - 12/02/2019 0	i:2óam ∨ Analyze				🕀 Hosts (1) 🗘 Risk Details (13) 🔞
F	® ∰ eventcreate.exe				
	© ☆ eventoreste.ose				
<sup>©</sup> ♀ ♀ □ (0) ⊖ − (0) ↔ 0 ↔ 0 ↔ 0 ↔ 0 ↔ 0 ↔ 0 ↔ 0 ↔ 0 ↔ 0 ↔					
-	Cind.exe				
VPROCESS EXECUTION DETAILS           VENT TIME         USER NAME           L1/27/2019 02:34:00.000 pm         NT AUTHORITY\SYSTEM	FILE.GENERAL FILENAME cmd.exe	FILE.PE TIMESTAMP 11/20/1975 08:18:58.000 pm	FEATURES file.exe.file.arch64.file.iconPresent.file.versionI	IMPORTED UBRARIES msvcrt.dll.ntdll.dll.api-ms-win-core-kernel32-le	FILE HASH MD5 0d088f5bcfa8f08ófba1ó3ó47cd80cab
ROCESS NAME LAUNCH ARGUMENTS md.exe cmd.exe <->Suspicious.bat c:\Suspicious.p	ENTROPY 6.172248861723813	IMAGE SIZE 404.0 KB	FILENAME Cmd.Exe	SECTION NAMES .text_rdata_data_pdata_didat_rsrc_reloc	SHA1 08cc2e8dca652bdda1acca9c446560d4bc1b
ILELOCATION :\windows\system32\	SIZE 272.0 KB	EXPORTED FUNCTIONS 0	COMBANY Microsoft Corporation		SHA256 9023f8aaeda4a1da45ac477a81b5bbe4128e
HECKSUM 2023f8aaeda4a1da45ac477a81b5bbe4128e4	FORMAT <b>PE</b>	EXPORTED NAMES 0	DESCRIPTION Windows Command Processor		
ESRONID 15844030		EXECUTE WRITE SECTIONS 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, 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.

🕽 👳 ( iost.exe	- • •	cmd.exe							
A	ll (70)	🗆 File (6)	🖽 Registry (0)						
Ø	PROCESS NAME	RISK SCORE 4	LAUNCH ARGUMENTS	EVENT TYPES					
8	cmd.exe		cmd.exe /c certutil.exe -uricache -split -f https://raw						
Ø	Conhost.exe		conhost.exe 0xffffffff-ForceV1						
Ø	cmd.exe		cmd.exe /c dir /b /a-d .\test-sets \"collection"\".bat						
Ø	PING.EXE	۲	ping-n 5 127.0.0.1						
Ø	7z.exe		7z.exe e -bb0 -paptsimulator "c:\mimikatz\\enc-files						
Ø	7z.exe		7z.exe e -bb0 -paptsimulator "c:\mimikatz\\enc-files						
Ø	cmd.exe		cmd.exe /c dir /b /a-d .\test-sets\"command-and-con						
Showing 70 out of 70   70 selected									
70 P	Process selected		Cancel View All View	ew Selected					

### **Analyze Events for a Process**

To analyze events for the selected process:

- 1. Perform steps 1 to 3 in <u>Analyze a Process</u>.
- 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).

			Events	List (96) 🛛 🖓 Hosts (1	1) 🗘 Risk Details (	13)
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 netsvcs -p	C:\Windows\System32\	
11/29/2019 09:3	Process Event	openPr	Isass.exe		C:\Windows\System32\	
			Showing 19 out o	f19		
	11/25/2019 06:5 11/25/2019 03:0 11/25/2019 11:1 11/26/2019 07:1 11/27/2019 02:3 11/27/2019 10:3 11/28/2019 06:4 11/28/2019 02:5 11/28/2019 10:5 11/29/2019 07:0 11/29/2019 09:3	11/25/2019 06:5         Process Event           11/25/2019 03:0         Process Event           11/25/2019 11:1         Process Event           11/25/2019 07:1         Process Event           11/26/2019 07:1         Process Event           11/27/2019 02:3         Process Event           11/27/2019 10:3         Process Event           11/28/2019 00:4         Process Event           11/28/2019 02:5         Process Event           11/28/2019 10:5         Process Event           11/28/2019 07:0         Process Event	11/25/2019 06:5         Process Event         openPr           11/25/2019 03:0         Process Event         openPr           11/25/2019 11:1         Process Event         openPr           11/26/2019 07:1         Process Event         openPr           11/27/2019 02:3         Process Event         openPr           11/27/2019 10:3         Process Event         openPr           11/27/2019 06:4         Process Event         openPr           11/28/2019 06:4         Process Event         openPr           11/28/2019 02:5         Process Event         openPr           11/28/2019 10:5         Process Event         openPr           11/28/2019 07:0         Process Event         openPr           11/28/2019 07:0         Process Event         openPr           11/29/2019 07:0         Process Event         openPr           11/29/2019 07:0         Process Event         openPr           11/29/2019 07:0         Process Event         openPr	EVENT TIMECATEGORYACTIONSOURCE FILE NAME11/25/2019/06:5Process EventapenPrexplorer.exe11/25/2019/03:0Process EventapenPrexplorer.exe11/25/2019/11:1Process EventapenPrexplorer.exe11/26/2019/07:1Process EventapenPrexplorer.exe11/27/2019/02:3Process EventapenPrexplorer.exe11/27/2019/02:3Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/06:4Process EventapenPrexplorer.exe11/28/2019/07:0Process EventapenPrexplorer.exe11/29/2019/07:0Process EventapenPrsychast.exe11/29/2019/09:3Process EventapenPrsychast.exe11/29/2019/09:3Process EventapenPrsychast.exe	EVENT TIMECATEGORYACTIONSOURCE FILE NAMESOURCE PARAMETER11/25/2019 06:5Process EventopenPrexplorer.eve11/25/2019 03:0Process EventopenPrexplorer.eve11/25/2019 01:1Process EventopenPrexplorer.eve11/25/2019 01:1Process EventopenPrexplorer.eve11/25/2019 01:1Process EventopenPrexplorer.eve11/25/2019 01:1Process EventopenPrexplorer.eve11/27/2019 02:3Process EventopenPrexplorer.eve11/25/2019 10:3Process EventopenPrexplorer.eve11/28/2019 06:4Process EventopenPrexplorer.eve11/28/2019 02:5Process EventopenPrexplorer.eve11/28/2019 01:5Process EventopenPrexplorer.eve11/28/2019 10:5Process EventopenPrexplorer.eve11/28/2019 01:5Process EventopenPrexplorer.eve11/28/2019 01:5Process EventopenPrexplorer.eve11/28/2019 01:5Process EventopenPrexplorer.eve11/28/2019 01:5Process EventopenPrexplorer.eve11/29/2019 07:0Process EventopenPrexplorer.eve11/28/2019 01:5Frocess EventopenPrexplorer.eve11/29/2019 07:0Process EventopenPrexplorer.evesvchost.eve-k.netsvcs-p11/29/2019 09:3Process EventopenPrsvchost.evesvchost.eve-k.netsvcs-p <td>EVENT TIME         CATEGORY         ACTION         SOURCE FILE NAME         SOURCE PARAMETER         SOURCE DIRECTORY           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 01:1         Process Event         openPr         explorer.exe         C:Windows\           11/25/2019 01:1         Process Event         openPr         explorer.exe         C:Windows\           11/25/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/27/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/27/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 00:4         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 02:5         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 01:5         Process Event         openPr         explorer.exe</td>	EVENT TIME         CATEGORY         ACTION         SOURCE FILE NAME         SOURCE PARAMETER         SOURCE DIRECTORY           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 01:1         Process Event         openPr         explorer.exe         C:Windows\           11/25/2019 01:1         Process Event         openPr         explorer.exe         C:Windows\           11/25/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/27/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/27/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 02:3         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 00:4         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 02:5         Process Event         openPr         explorer.exe         C:Windows\           11/28/2019 01:5         Process Event         openPr         explorer.exe

For example, to view only process events, select the Process Event category, and filter on action.

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 Hosts (Processes, Autoruns, Files, Drivers, Libraries, or Anomalies tab).
  - Go to Files.
- 2. Select one or more files and do one of the following:

RSA Investigate Respond Users	H	osts	F	iles Dashboards	Rep	orts				2 %	<b>\$</b> ? ?	admin >
𝖁 Filters		E	end	dpointloghy 🗸 🛛 Vie	w Cert	ificates	ູ້ ແ <sup>x</sup> Cha	ange File Status	🖸 Analyze Ev	vents 🗸 🗄	More Actions 丶	× .
SAVED FILTERS			FILE	E NAME RISK SCORE 个	FIRST	SEEN TI	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOUR	FILE 🛿 🔅
Select	~	ø	ntos	skrnl.exe 0	06/11	/2020 17		Known Good	9.5 MB	microsoft,signed,	Microsoft C	Neutral
FILE NAME			sn	Change File Status		2020 17		Known Good	143	microsoft,signed,	Microsoft C	Neutral
Equals v e.g., Filename.dll	[		wi	Analyze Events		2020 17		Known Good	362	microsoft,signed,	Microsoft C	Neutral
FILE STATUS			se	Google Lookup VirusTotal Lookup		2020 17		Known Good	659	microsoft,signed,	Microsoft C	Neutral
□ Neutral □ Blacklist			lsa	View Certificates		2020 17		Known Good	56.7	microsoft,signed,	Microsoft C	Neutral
□ Blacklist □ Graylist			fo	Download File to Server		2020 17		Known Good	802	microsoft,signed,	Microsoft C	Neutral
Whitelist			Lo			2020 17		Known Good	13.5	microsoft,signed,	Microsoft C	Neutral
			sp			2020 17		Known Good	747	microsoft,signed,	Microsoft C	Neutral
Blocked			vo	Reset Risk Score		2020 17		Known	81.5	signed,valid	VMware, Inc.	Neutral
REPUTATION												

- 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.

Change File Status	0	×
STATUS		
<ul> <li>Blacklist</li> </ul>		
CATEGORY		
Select v		
REMEDIATION		
Applies to hosts where blocking is enabled and terminates all processes associated with the selected file hashes.		
Files signed by RSA and Microsoft cannot be blocked. Block		
O Graylist		
O Whitelist		
O Neutral		
COMMENTS *		
Enter comments		
Cancel	Sav	

Change File Status	?	×
STATUS		
<ul> <li>Blacklist</li> </ul>		
CATEGORY		
Select ~		
REMEDIATION		
Applies to Windows hosts running in advanced mode where blocking is ena terminates all processes associated with the selected file hashes.	bled and	d
O Graylist O Whitelist O Neutral		
COMMENTS *		
Enter comments		
Cancel	Save	

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 codeFiles 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 **Services** > **Endpoint Server** > **view** > **Explore** > **rsa.endpoint.file-download-disk-thresholds.warningpercent** 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 **Policies** > **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 Files tab > Downloaded column.

#### Manual File Download

To manually download files to the server from the Hosts view:

- 1. Go to 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:

<b>RSA</b> Investigate Respond Users <b>H</b>	osts Files Dasł	hboards Reports					8 %	⑦ admin >
100 vindows i ldle	n status agent las <b>a few secc</b>		snapshot time 06/28/2020	21:30:08 ~				
DETAILS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY								
♥ Filters ×	Processes 2	Analyze Process 🛛 🏹 Change File Sta	itus 🛛 🖓 Analyze Events	V I More Actio	ons ~			
PROCESS NAME		LOCAL RISK SC	ORE GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILE PATH
Equals v e.g., Filename.dll	🗹 dwm.exe	alyze Process	· · · · · · · · · · · · · · · · · · ·		Known Good	Blacklisted		C:\Windows\System3
FILE STATUS	D dwm eve	ange File Status			Known Good	Blacklisted		C:\Windows\System3
Neutral     Blacklist	_	alyze Events >	•		Known Good	Neutral		C:\Windows\System3
Graylist	Drowser to Goo	ogle Lookup >	٥		Known Good	Neutral		C:\Windows\System3
		isTotal Lookup >			Known Good	Neutral		C:\Windows\System3
REPUTATION	Conhoster Dow	wnload Process Dump to Server	•		Known Good	Neutral		C:\Windows\System3
Malicious  Suspicious		wnload File to Server	•		Known Good	Neutral		C:\Windows\System3
Unknown Known	Carss.exe Sav	re a Local Copy	 (0)		Known Good	Neutral		C:\Windows\System3
Known Good     Invalid	ana csrss.exe	alyze File			Known Good	Neutral		C:\Windows\System3

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

To download files to the server from the Files view:

- 1. Go to Files.
- 2. Select the file and do one of the following:

RSA Investigate Respond Users	Ho	sts Files	Dashboards Reports						[	z % 0	admin >
<b>∀</b> Filters		endpointbro	ok View Certificates	x	Change File Status	Analyze Events	/ <b>:</b> M	ore Actions 🗸			
			RISK SCORE 🔶 FIRST SEE	N TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	FILE STATUS	R ()
Select	~		0 06/12/202	20 11:16:		Known		unsigned		Neutral	
		🗹 <u>vsock.svs</u>	0 06.492/90	11:32:		Known	89.6 KB	signed,valid	VMware, Inc.	Neutral	
Equals v e.g., Filename.dll	_ [	libstdc++.so	Change File Status Analyze Events	11:16:		Known	908.4	unsigned		Neutral	
FILE STATUS		libsoftokn3.s	Google Lookup	11:16:		Known	256.0	unsigned		Neutral	
Neutral		🗆 <u>sic.dii</u>	VirusTotal Lookup	11:32:		Known Good	137.5	microsoft,signed,valid,	Microsoft Corpo	Neutral	
Blacklist     Graylist	-	usermarclid	View Certificates	11:32:		Known Good	74.1 KB	microsoft,signed,valid	Microsoft Corpo	Neutral	
Whitelist		devicecensu s	Download File to Server	07:57:		Known Good	35.3 KB	microsoft,signed,valid	Microsoft Corpo	Neutral	
		D pam cracklit	Save a Local Copy	11:16:		Known	14.1 KB	unsigned		Neutral	
Blocked				11:16:		Known	2.6 KB	unsigned		Neutral	
REPUTATION		TextInputFra	Reset Risk Score	11:32:		Known Good	627.2	microsoft,signed,valid	Microsoft Corpo	Neutral	

- Right-click and select Download File to Server from the context menu.
- Select Download File to Server from the More Actions 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 Hosts 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 Hosts or Files.
- 2. Right-click the downloaded file and select **Analyze File**. The File Analysis view opens and properties of the are is displayed in the right panel.

	Analysis NATURE rosoft,signed,valid,catalog	SIZE 227.5 KB	FILE STATUS OPERATING SYSTE Neutral windows	X
File Analysis - Strings View	FILTER STRINGS E	inter Value	LENGTH	DETAILS
usebackq	0x00027C88	1		Type to filter list
XA\]	0x0000C64A			
NtOpenProcessToken	0x0002DFE0		18	File Details
fE9d	0x0001F9AA			Format <b>pe</b>
ReadConsoleW	0x0002D184			checksumMd5 f4f684066175b77e0c3a000549d2922c
wcscmp	0x0002E0BC			checksumSha1 99ae9c73e9bee6f9c76d6f4093a9882df068
/dpiAware	0x00030C8F		9	checksumSha256 935c1861df1f4018d698e8b65abfa02d7e90
%2d%s%02d%s%02d%s%02d	0x00027EC0		21	Size 227.5 KB Downloaded FileName 935c1861df1f4018d698e8b65abfa02d7e90
AcquireSRWLockShared	0x0002D202		20	Downloaded Path /var/netwitness/endpoint-server/files/935c1
	0x00030B00			
fD9,pu	0x0001FE72			Image Details
POPD	0x00028268	1	4	Architecture AMD64/x64 Characteristics Executable,Large Address Aware
/t9A	0x0000C236		4	Compile Time 07/16/2016 07:53:21.000 am
				Entry Point 0x00015190
tj9L	0x00012488			Imported DLLs > Imported DLLs (31) And Functions (239)
/K %s	0x00028C48	1		Section Names > Section Names (7)
PD9(H	0x0000D10C			Subsystem Windows Console
PATHEXT	0x00027CD0	1		

- 3. 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.
- 4. 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 Mainachonan	si0 🗹 i			SENT VERSION	SNAPSHOT TIME	11/12/2019 05:53	<u>25 pm ~</u> ×
DETAILS PROCES	SSES AUTORUN	NS FILES DRIVE	RS LIBRARIES		DOWNLOADS	SYSTEM EXEC	۹
Files   File Analysis - Strin	ngs View Filter strings	mäj					Exec.exe
STRING	01	USET	UNICODE	LENGTH			
*-m3 msupdater.com	0x	00000A07					Type to filter list
*-m3 twitterdocs.com'	0×	00000A95					Show details with values only
*-m3 freenow.chickenkiller.com	0×	00000B2B					
							Format pe
	1						checksumMd5 d16f277c8d94437b751917d87ddc8d91
							checksumSha1 60ec5ca33072dff849a1d9eac946c20834a4
イフ							checksumSha256 b266afb334f3dec596dac6501f70994c8f942
							Size 6.0 KB
C2 info visible							Downloaded FileName b266afb334f3dec596dac6501f70994c8f942
in File Content							Downloaded Path /var/netwitness/endpoint-server/files/b266a
in File Content							Image Details
							Architecture 1386/x86
							Characteristics Executable.Large Address Aware
							Compile Time 01/14/2019 10:20:25.000 am
							Entry Point 0x00002C4A
							Subsystem Windows Console
							Packing Detection
		Sho	owing 3 of 123 strings				Entry Point Valid true

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.

100 windows	AGENT SCAN STATUS  Idle	AGENT LAST SEEN a few seconds ago	AGENT VERSION 11.4.0.0		11/12/2019 05:53:2	5 pm \vee	
DETAILS PROCESSES AUT	FORUNS FILES DE	RIVERS LIBRARI	ES ANOMALIES	DOWNLOADS	SYSTEM KEYLOG	i	
✓ Files   File Analysis - Strings View FILTE						DETAILS	KeyLogger.exe
ITRING	OFFSET		LENGTH				
Del]	0x00055070					Type to filter list	
Esc]	0x00055128					Show details with values onl	
Right]	0x00055068		<sup>,</sup>				
vjaljz	0x0004612F		,				
92[2b2m2t2	0x00061B1D		11				5242de7eee306123c50c1d0dcad83062
lp]	0x00055050	-	,				dacc40cf0edb8d55cdce6615e506209c8
elese[]	0x00056100		,		ators of		c9eb0aa40eaa22685a6aceaa24136e984
K8O858W8[8	0x00062368		11				401.0 KB c9eb0aa40eaa22685a6aceaa24136e984
i0ni*	0x0005C2F4		5	keyst	roke logging		/var/netwitness/endpoint-server/files/c9
C7K7S7[7n9?			12				warneen as en quineservernies es
	0x00062D15						
ageDown]	0x0005511C		10				1386/x86
ew[]	0x000560F8		5				Executable,32-bit
hunk]:	0x00056610		3				02/22/2019 11:46:23.000 am
1,1[1a1	0x00061809		•				0x000275FF
55(5	0x00062489		s /				
93	0x0005C5C8		4				
Num Lock]	0x00055218		10				Windows Console
End]	0x00055060		,			Packing Detection	
							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 stomping 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 stomped. For more information, see <u>Analyze Downloaded MFT</u>.

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:

- 1. Go to **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.

RSA Investigate Respond Users H	osts F	iles Dashboards Reports					l	<b>z %</b> (?	admin >
abla Filters ×	🖯 🖯 en	dpointbrok 🗡 🛛 🗗 🗗 Analyze Event	s ∨ ØStar	rt Scan 🛛 🛛 Stop Scan	: More Acti	ons ∨			<b>6</b>
SAVED FILTERS	П но	STNAME RISK SCORE 🔶 OS - DESC	RIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGENT SCAN STATUS	AGENT GROUPS	IPV4
Select ~	S -	Microsoft	Windows 10 Enter	06/28/2020 21:30:08	WINDWOS10-0	a few seconds ago	Idle	Windows-security	10.125.245.1
HOST STATUS		Analyze Events >	ndows 10 Enter	06/24/2020 21:30:33	WINDOWS10\e	a few seconds ago	Idle	Windows-security	10.125.245.1
Managed		Delete	use 6.7 (Final)	06/29/2020 14:30:23		a few seconds ago	Idle		10.125.244.2
Roaming     Isolated		Start Scan Stop Scan							
RISK SCORE		Network Isolation							
100		Download MFT to Server							
		Download System Dump to Server							
		Download Files to Server							
HOSTNAME Equals v Enter Value		Reset Risk Score							

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

RSΛ	Investigate	Respor	nd Users	Hosts	Files	Dashboards	Reports
	dows		AGEN Start Scan Export Host d	t scan status etails	; ,	AGENT LAST SEEN	
DETAILS	PROCESSES	AUTOI	Export Files			BRARIES AT	NOMALIES
1	0	(	Network Isola		>	-	EVENT TYPE
	HIGH	ME	Download MF Download Sys		Server	0 14:02:41.000 TILE NAME	Endpoint
Blacklisted File ( 91 event(s)	91)		Download File		ARGET	N/A N/A	N/A N/A

2. View details of the downloaded MFT in the **Downloads** tab within the host details. For more information, see Hosts View - Downloads Tab.

RSA Investigate Respond Users	Hosts Files Dashboards Report	:5					2 % ()	) admin >		
100     vindows     Agent scan status     Agent Last stein     Agent version     X       100     vindows     Idle     a few seconds ago     11.5.0.0     X										
DETAILS PROCESSES AUTORUNS FILES	DETAILS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY									
<b>∀</b> Filters ×	C Downloads Save a Local Copy	Delete File								
SAVED FILTERS		түре	DOWNLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH			
Select ~	mft-C-Win1909-64b-0-2020-03-13T08-39-	MFT	~	197.3 MB	7 minutes ago	NA				
Wildcard Downloads	C:\Users\"\NTUSER.DAT		~		24 minutes ago					
FILE TYPE	C:\Users\ exe\exe\*		~		a day ago					
D MFT	□ > c/'		~		2 days ago					
File  Process Dump  System Dump	C:\Users\*\		<b>~</b>		10 days ago					
FILE NAME										
Equals v e.g., Filename.dll										
SHA256										
Equals v Enter Value										

## 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 timestomped.

#### View MFT

To view the content of the downloaded MFT:

- 1. Go to 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.

RSA Investigate Respond	Users <b>Hosts</b> Files Dash	nboards Re	eports								
100       windows       Image: Agent scan status agent last seen agent version lidle       agent scan status afew seconds ago       114.0.0         DETAILS       PROCESSES       AUTORUNS       FILES       DRIVERS       LIBRARIES       ANOMALIES       DOWNLOADS       SYSTEM INFO											
✓ Downloads     ▼   Filters	MFT Viewer Download File to Server	]									
MFT-C-WINDOWS10-2019-11-14T06-47-52-777Z		SIZE	CREATION TIME (\$FN)								
✓ A C:	RWE-Trace-Oc1c.txt	0 bytes	11/12/2019 07:02:03 pm								
> 🗅 inetpub	Image: NWE-Trace-Oacc.rar	2.0 MB	11/12/2019 11:54:16 am								
> 🗅 wamp64	B NWE-Trace-0acc.txt	0 bytes	11/12/2019 12:48:33 am								
> C Windows	RWE-Trace-Of80.rar	1.0 MB	11/12/2019 12:08:39 am								
> D ProgramData	RWE-Trace-Of80.txt	0 bytes	11/11/2019 09:25:01 pm								
>      Program Files (x86)     SRecycle.Bin	RWE-Trace-0a3c.txt	0 bytes	11/11/2019 07:32:11 pm								
> 🗅 PerfLogs	RWE-Trace-0c44 - Copy.txt	49.8 MB	11/11/2019 0ó:5ó:29 pm								
>      Program Files     >      \$     \$     \$Extend	NWE-Trace-1fc0.txt	8.5 KB	11/11/2019 05:44:35 pm								
C Recovery	RWE-Trace-0c44.txt	0 bytes	11/11/2019 05:43:31 pm								
<ul> <li>Documents and Settings</li> <li>System Volume Information</li> </ul>	RWE-Trace-0c30.txt	101.9 KB	11/11/2019 05:42:05 pm								
DELETED FILES	DataCollector01.csv	642.9 KB	11/11/2019 05:03:16 pm								
ALL FILES	Image: NWE-Trace-264c - Copy.txt	21.0 MB	11/11/2019 05:02:52 pm								
	RWE-Trace-264c.txt	0 bytes	11/06/2019 09:38:24 pm								
	Directory path: C:   ♡ No filters applied										

4. Click  $\triangleright$  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 (1990) indicating that it is time stomped.

RSA Investigate Respond	Users <b>Hosts</b> Files Dashbo	ards Repo	rts				8	🕻 🕐 admin >			
71 Windows	kile alfewsecondrago 11400										
C Downloads 7 Filters	MFT Viewer Download File to Server							×			
MFT-C-INGSMUDALPL6C-2019-11-29T09-10-45-317Z		SIZE	CREATION TIME (\$FN) 4	CREATION TIME (\$51)	MODIFICATION TIME (\$FN)	MODIFICATION TIME (\$SI)	ACCESS TIME (\$FN)	ACCESS TIME (\$5I)			
Git Origin Feature Branch Git Origin Master	🗆 🖻 setupact.log	1.9 KB	11/11/2019 06:17:06 am	11/11/2019 06:17:06 am	11/11/201906:17:06 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] Git	SMSAdvancedClient.configmgr1810-client-kb4	1.8 KB	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm	11/07/201901:01:54 pm	11/07/2019 01:01:54 pm 💧	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm			
SysinternalsSuite		0 bytes	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm 💧						
> 12 150 > 12 Intel	🗆 🖻 setuperr.log	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			
Documents and Settings		1.9 KB	08/22/201901:54:19 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     C: Recovery	🗆 🖻 diagercami	1.9 KB	08/22/2019 01-54:19 pm	08/22/2019 01:54:19 pm	08/22/201901:54:19 pm 💧	08/22/2019 01:54:22 pm 💧	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm			
> 🗈 Users	B DiskCleanupV3.exe	290.5 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     Program Files (x86)	C C <u>nvmup</u>	0 bytes	06/06/2019 05:31:54 pm	06/06/2019 05:31:54 pm	06/06/2019 05:31:54 pm	06/06/2019 05:31:54 pm 💧	06/06/2019 05:31:54 pm 💧	06/06/2019 05:31:54 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 (\$SI), update time (\$SI), modified time (\$SI), and modified time (\$SI).

RSA Investigate Respond Users Hosts Files Dashboards Reports 🖻 % 🕐 admin >											
Vindows       Ide       AGENT SCAN STATUS       AGENT LAST SEEN       AGENT VERSION         DETAILS       PROCESSES       AUTORUNS       FILES       DRIVERS       LIBRARIES       ANOMALIES											
$\nabla$ Filters ×	< Downloads	MFT Viewer Download File to Server									
SAVED FILTERS	MFT-C-INGSMUDALPL6C-2019-11-29709-10-45-317Z		SIZE	CREATION TIME (\$FN)	CREATION TIME (\$51)						
Select	Git Origin Feature Branch	setupact.log	1.9 KB	11/11/2019 06:17:06 am	11/11/2019 06:17:06 am						
FILE NAME	<ul> <li>C Git Origin Master</li> <li>Temp</li> </ul>	ComTemp	0 bytes	11/07/2019 01:03:38 pm	11/07/2019 01:03:38 pm						
Equals e.g. Filename.dll	Deep Web (2015) [YTS.AG] Git	SMSAdvancedClient.configmgr1810-clien	1.8 KB	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm						
FILE TYPE	<ul> <li>SysintemalsSuite</li> </ul>		0 bytes	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm						
Equals v eg.dll	> 🗅 150 > 🗀 Intel	🗆 🖻 setuperr.log	0 bytes	09/14/2019 11:54:02 am	09/14/2019 11:54:02 am						
TIMESTOMPING	<ul> <li>Documents and Settings</li> </ul>	🗆 🖻 diagwrn.xml	1.9 KB	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm						
Timestomped Files	Windows     D Recovery	🗆 🖻 diagerr.xml	1.9 KB	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm						
CREATION TIME (\$FN) CUSTOM DATE	> C Users	DiskCleanupV3.exe	280.5 KB	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am						
<u>~</u>	> 🗅 ProgramData > 🗀 Program Files (x86)		0 bytes	06/06/2019 05:31:54 pm	06/06/2019 05:31:54 pm						
CREATION TIME (\$SI) CUSTOM DATE	C \$Recycle.Bin     Dell	C 🖻 pyw.exe	869.1 KB	05/29/2019 05:52:20 am 🧥	12/23/2016 01:49:18 am 🧥						

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  $\mathbf{III}$ .

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

To filter, save, and delete MFT, see <u>Filter Downloaded Files</u>, <u>Save Downloaded File</u>, and <u>Delete</u> <u>Downloaded Files</u>.

## 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 **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.

RSA Investigate Respond Users H	osts	Files Dashboards Reports	s		
♥ Filters ×	E	endpointbrok 🗡 🛛 🖾 Analyze	Events 🗸 🖉 Start Scan 🛛 🖾 Stop	Scan <b>i Mor</b>	e 🗸
SAVED FILTERS		HOSTNAME	RISK SCORE $\psi$ OS - DESCRIPTION		LAST SC/
Select v			N/A Microsoft Windows 1	0 Pro for Workstati	05/08/20
HOST STATUS			N/A Red Hat Enterprise Li	nux- 7.2	05/05/20
Managed			N/A Red Hat Enterprise Li	nux- 7.2	05/06/20
Roaming	Ø			4 Enterprise	05/06/20
□ Isolated			Analyze Events		05/05/2
RISK SCORE			Delete		
100			Start Scan	x 8.1 (Ootpa)	05/06/20
• · · · · · · · · · · · •				iducation	
0			Network Isolation	nterprise	
HOSTNAME			Download MFT to Server	interprise	
Equals ~ Enter Value					05/07/20
USERNAME			Download System Dump to Server Download Files to Server		05/06/20
Equals ~ Enter Value				ducation	
			Reset Risk Score		
AGENT GROUPS			Microsoft Windows 7	Enterprise	05/08/20

• Select the hostname to open the host details and select Download System Dump to Server from

RSΛ	Investigate	Respond	Users	Hosts	File	es Dashboard	ds Reports
100 win	dows	Start S		AN STATUS	А	gent last seen few seconds ago	agent versi 11.5.0.0
DETAILS	PROCESSES	AU Export	t Host detail t Files	ls		LIBRARIES /	ANOMALIES
2	0	Netwo	ork Isolation	I	>	_	
CRITICAL	нісн	Down	load MFT to	Server		<sup>NE</sup> 2020 13:40:54.000	EVENT TYPE D Endpoint
Blacklisted File (2	28)	Down	load System	Dump to Sei	rver	<b>FILE NAME</b>	LAUNCH ARGU
28 event(s)		Down	load Files to		ARGET	N/A N/A	N/A N/A

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 <u>Hosts View</u> - Downloads Tab.

#### Download Process Dump to Server

To download process dump to the server:

- 1. Go to 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.

RSA Investigate Respond Users H	osts Files	Dashboards Repo	rts				8	* ?	admin >
100 indows		AST SEEN AGENT V econds ago 11.5.0.0		shot тіме 06/24,	/2020 21:30:3	3 ~			
DETAILS PROCESSES AUTORUNS FILES	DRIVERS LIBR	RARIES ANOMALIES	DOWNLOADS	SYSTEM INFO					Q
♥ Filters ×	Processes	☑ Analyze Process	旗 Change File Sta	tus 🕜 Analyze E	Events 🗸	: More Actions $\vee$	]	TF	EE VIEW
PROCESS NAME	PROCESS N/	AME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILI 🛞
Equals v e.g., Filename.dll	dwm.exe		100	100		Known Good	Blacklisted		C:\Wind
FILE STATUS	🗹 <u>dwm.exe</u>			] 💷		Known Good	Blacklisted		C:\Wind
Neutral     Blacklist	Svchost.exe	Analyze Process		100		Known Good	Neutral		C:\Wind
Graylist	svchost.exe	Change File Status Analyze Events	>	100		Known Good	Neutral		C:\Wind
Whitelist	svchost.exe	Google Lookup	>	100		Known Good	Neutral		C:\Wind
	svchost.exe	VirusTotal Lookup	>	100		Known Good	Neutral		C:\Wind
Malicious     Suspicious	svchost.exe	Download Process Du	mp to Server	100		Known Good	Neutral		C:\Wind
Unknown Known	svchost.exe	Download File to Serve	er	100		Known Good	Neutral		C:\Wind
Known Good	svchost.exe			100		Known Good	Neutral		C:\Wind
		Analyze File		100		Known Good	Neutral		C:\Wind

4. View the details of the download process dump in the **Downloads** tab within the host details. For more information, see <u>Hosts View - Downloads Tab</u>.

To filter, save, and delete system dump or process dump, see <u>Filter Downloaded Files</u>, <u>Save</u> 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.

### **Download Files Using Full Path or Wildcard**

You can manually download files that help in investigations by either providing full path of the file or using wildcard.

**Note:** This is applicable only for agents in Advanced mode with NetWitness Platform version 11.5 and later.

To download files to the server:

- 1. Go to **Hosts** and do one of the following:
  - Select one or more hosts from the same operating system, and select **Download Files to Server** from the right-click context menu, or from the **More** drop-down list in the toolbar. You can download files from only top 100 selected hosts at a time.

RSA Investigate Respond Users	losts Files I					[	3 % 0	
∀ Filters ×	endpointbro	k ∨   🗗 Analyze Events   ∨   🖾 St	art Scan 🛛 🐨 Stop Scan	: More Acti	ons ∨			<b>i</b>
		RISK SCORE $\psi$ OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGENT SCAN STATUS	AGENT GROUPS	IPV4
Select ~	Ø	Microsoft Windows 10. Enter	06/28/2020 21:30:08		a few seconds ago	Idle	Windows-security	10.125.245.1.
HOST STATUS		Analyze Events >	06/24/2020 21:30:33	where the	a few seconds ago	Idle	Windows-security	10.125.245.1.
Managed C Roaming I Isolated	-	Delete Start Scan Stop Scan	06/29/2020 14:30:23		a few seconds ago	Idle		10.125.244.2
nisk score 100		Network Isolation > Download MFT to Server						
• • • • • • • • • •	•	Download System Dump to Server Download Files to Server						
nostname Equals – Enter Value		Reset Risk Score						

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

#### Download Files to Server.

RSΛ	Investigate	Res	spond	Users	Hosts	File	es Dashboards	s Reports
100 win	dows	ď	Start S		AN STATUS	A	gent last seen few seconds ago	agent versi 11.5.0.0
DETAILS	PROCESSES	AU	Export Export	t Host detai t Files	ls		LIBRARIES A	NOMALIES
2	0		Netwo	ork Isolatior	1	>		
CRITICAL	нісн	I	Down	load MFT to	Server		<sup>NE</sup> 2020 13:40:54.000	EVENT TYPE Endpoint
Blacklisted File (	28)		Down	load System	n Dump to Se	rver	FILE NAME	LAUNCH ARGL
28 event(s)			Down	load Files to		IARGET	N/A N/A	N/A N/A

2. In the **Download Files to Server** dialog, enter the full path where the files may be present or search using wildcard. For wild card search, you can use a maximum of two \*, one at a folder level and the other at a file level.

For example, to retrieve the registry hive, you can enter the full path, C:\Windows\System32\config\SYSTEM.

If you want to retrieve user settings and configuration preferences for all users, download all files using the wildcard C:\Users\\*\NTUSER.DAT.

Download Files		×
FILE PATH Enter the path where files may be press folder and file level.	ent. For wildcard search, a '*' can be used at a	
C:\Users\*\NTUSER.DAT		
NUMBER OF FILES Maximum of 100	FILE SIZE(MB) Downloads all files upto the specified size limit	
10	100	
	Cancel Download	d

- 3. For wildcard search, enter the number of files to download and size of the file. By default, the number of files is set to 10 and file size is set to 100 MB. For example, if the maximum number of files is set to 10 and file size is set to 10 MB, first 10 files within 10 MB are downloaded.
- 4. Click Download.

All files downloaded as a part of wildcard search are grouped together based on the search criteria. For example, all files downloaded using C:\Users\\*\NTUSER.DAT are grouped, and you can click to expand and view all files under this group. You can sort the groups on the downloaded time and view the status of the download in the **Downloaded** column.

RSA Investigate Respond Users H	osts Files Dashboards Report	s				Ē	3 % (	⑦ admin ≻
0 windows C AGENT SC	AN STATUS AGENT LAST SEEN AGENT VER a few seconds ago 11.5.0.0							×
DETAILS PROCESSES AUTORUNS FILES	DRIVERS LIBRARIES ANOMALIES	DOWNLOADS	SYSTEM INFO					
$\nabla$ Filters ×	Downloads Save a Local Copy	Delete File						
SAVED FILTERS		түре	DOWNLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH	
Select ~	C:\Users\*\NTUSER.DAT		<ul> <li>✓</li> </ul>		8 minutes ago			
Wildcard Downloads			<b>~</b>		a day ago			
FILE TYPE			<ul> <li></li> </ul>		2 days ago			
		-	<b>~</b>		10 days ago	-	-	

### **Filter Downloaded Files**

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

RSA Investigate Respond Users	Hosts Files Dashboards Reports	i				[	3 % 0	admin >
0 vindows	can status agent Last seen agent vers a few seconds ago 11.5.0.0							×
DETAILS PROCESSES AUTORUNS FILES	DRIVERS LIBRARIES ANOMALIES	DOWNLOADS	SYSTEM INF					
<b>∀</b> Filters ×	Downloads Save a Local Copy	Delete File						
SAVED FILTERS		ТҮРЕ	DOWNLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH	
Select ~	mft-C-Win1909-64b-0-2020-03-13T08-39	MFT	~	197.3 MB	7 minutes ago	NA		
Wildcard Downloads	C:\Users\"\NTUSER.DAT		<b>~</b>		24 minutes ago			
FILE TYPE	C:\Users\ Desktop\exe\exe\"		<ul> <li>Image: A second s</li></ul>		a day ago			
MFT   File	□ > c/'		<b>~</b>		2 days ago			
Process Dump System Dump	□ > C:\Users\*\ \N*		<b>~</b>		10 days ago			
FILE NAME Equals v e.g., Filename.dll								
	•							
SHA256								
Equals ~ Enter Value								

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 **D**.

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 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.

RSA Investigate Respond	d Users <b>Hosts</b> Files Dashboards F						2 % 0	
0 vindows	AGENT SCAN STATUS AGENT LAST SEEN AGE Idle a few seconds ago 11.9	nt version 5.0.0						
DETAILS PROCESSES AUTORI	JNS FILES DRIVERS LIBRARIES ANOMA	LIES DOWNLOADS	SYSTEM INF	O HISTORY				
<b>∀</b> Filters	× Downloads Save a Local Cop	y Delete File						
SAVED FILTERS		ТҮРЕ	DOWNLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH	
Select	<u>mft-C-Win1909-64b-0-2020-03-13T0</u>	8-39-, MFT	<u> </u>	197.3 MB	7 minutes ago	NA		
Wildcard Downloads	C:\Users\"\NTUSER.DAT	Save a Local Copy	~		24 minutes ago			
	C:\Users'	Delete File	~		a day ago			
		FILE		0 bytes	a day ago	NA	/root/	
File  Process Dump  States Dump			<b>~</b>		2 days ago			

4. Browse the location and click Save.

**Note:** For wildcard downloads, select a file from the group that are downloaded successfully to save a local copy. You cannot save multiple files in the group at a time or save files with errors.

### **Delete Downloaded Files**

If you want to delete the downloaded file from the server:

- 1. Go to **Hosts**.
- 2. Select the hostname to open the host details and select the **Downloads** tab.
- 3. Right-click one or more files you want to delete, and select **Delete File** from the context menu or from the toolbar.

RSA Investigate Respond Users Ho	osts Files Dashboards Repor	ts				Į	2 %	⑦ admin >
100 i AGENT SCAN STA Scanning	atus agent last seen agent vi a few seconds ago 11.5.0.0							
DETAILS PROCESSES AUTORUNS FILES E	DRIVERS LIBRARIES ANOMALIES	DOWNLOADS SY	STEM INF	D HISTORY				
abla Filters $ imes$	Downloads Save a Local Copy	Delete File						
SAVED FILTERS		TYPE DOWN	NLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH	
Select v	mft-C-Win1909-64b-0-2020-03-13T08-39-	MFT	~	197.3 MB	7 minutes ago	NA		
Wildcard Downloads	C:\Users\"\NTUSER.DAT	Save a Local Copy	~		24 minutes ago			
FILE TYPE	C:\Users\	Delete File	<b>~</b>		a day ago			
		FILE		0 bytes	a day ago	NA	/root/	
File Process Dump			~		2 days ago			
System Dump			~		10 days ago			

Note: For wildcard downloads, you can select the group to delete all files that are downloaded.

# **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 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.

RSA Investigate Respond Users H	osts Files	Dashboards Reports					(	3 % 0	admin >
$\nabla$ Filters ×	endpoint	brok View Certificates	پَرْ Change File Status	Analyze Events	́!М	ore Actions ∨			
SAVED FILTERS	File NAM	E RISK SCORE 🕆 FIRST S	EEN TIME ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	FILE STATUS	R 🛞
Select		0 06/12/	2020 11:16: 1	Known	117.1	unsigned		Neutral	
FILE NAME		Change File Status	020 11:32: 2	Known	89.6 KB	signed,valid	VMware, Inc.	Neutral	-
Equals v e.g., Filename.dll		Analyze Events	Console Events	Known	908.4	unsigned		Neutral	
FILE STATUS		Google Lookup >	Network Events	Known	256.0	unsigned		Neutral	
Neutral		VirusTotal Lookup >	File Events	Known Good	137.5	microsoft,signed,valid,	Microsoft Corpo	Neutral	
Blacklist     Graylist		View Certificates	Process Events	Known Good	74.1 KB	microsoft,signed,valid	Microsoft Corpo	Neutral	
Whitelist		Download File to Server	Registry Events	Known Good	35.3 KB	microsoft,signed,valid	Microsoft Corpo	Neutral	
REMEDIATION			020 11:16: 1	Known	14.1 KB	unsigned		Neutral	
Blocked			020 11:16: 1	Known	2.6 KB	unsigned		Neutral	
REPUTATION		Reset Risk Score	020 11:32: 2	Known Good	627.2	microsoft,signed,valid	Microsoft Corpo	Neutral	

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 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.

RSA Investigate Respond Users	<b>losts</b> Files	Dashboards Repo	orts		٩	% ?	admin >
100 vindows			INT VERSION 5.0.0 SNAPSH	от тімеОб/25/2020 2	1:30:30 🗸		
DETAILS PROCESSES AUTORUNS FILES	DRIVERS L	IBRARIES ANOMALIE	S DOWNLOADS S	Search by filena			Q
$\nabla$ Filters ×	Autoruns	Services Tasks					
FILE NAME	ູ້ມ* Change	File Status	e Events 🗸 🕻 More	Actions V			
Equals v e.g., Filename.dll	Filenam	IE LOCAL RISK SCO	GLOBAL RISK SC ON HO	STS REPUTATION	FILE STATUS	DOWNLOADED	) FILE 🔅
FILE STATUS	⊠ <u>NapiNSP</u>		0 2	Known	Neutral		03/19/2
Neutral     Blacklist	🗆 <u>N</u> Cha	ange File Status	0 2	Known	Neutral		03/19/2
□ Graylist □ Whitelist	na wi Ana	alyze Events	Console Events	Known	Neutral		03/19/2
		ogle Lookup	Network Events	Known	Neutral		03/19/2
REPUTATION		usTotal Lookup >	File Events	Known	Neutral		03/19/2
Suspicious		wnload File to Server	Process Events	Known	Neutral		03/19/2
Unknown Known Known			Registry Events	Known	Neutral		03/19/2
Reset			Showing 143 out of 1	43 autoruns   1 selected			

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. (Version 11.5 and Later) The event header includes host name, process, and user name details in addition to other event details if the selected Endpoint event contains these metadata.
- 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.

EPS1-Server - Cor	ncentrator V 02	2/27/2019 07:43am - 03	6/2019 07:42am V ((alias.host =X) (action = _openbrowserprocess _ X) Guide Mole   free-form Mole	0	2
5,423 Events (Asc)	Endpoint Analysis TYPE Endpoint	✓ 2 <sup>A</sup> > EVENT TIME D 2019-03-14T09-36 m	Endpoint Event Details   Text Analysis Download Log   V   C Pivot to Endpaint Thick Client   C Analyze Process   C Pivot to Host Overview	<u> </u>	×
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09-36: m	NW SERVICE SESSION ID NWE CATEGORY COLLECTION THE EPST-Server - Concentrator 5955 Process Event 03/14/2019/05/41:34 am	EVENT TIME 03/14/2019 09:36:26 am	
03/14/2019 09:41:34 am 03/14/2019 09:41:34 am	Endpoint Endpoint	2019-03-14T09:36: m 2019-03-14T09:36: m	PROCESS EVENT     O 03/14/2019 09:36:26 am     O IT AUTHORITY/NETWORK SERVICE     MIDPMSE.cere PHILIPANED openBrookserProcess = chrome.exe	EVENT META sessionito 6965 TMME 03/14/2019 09-41:34 am size 605	*
03/14/2019 09:41:34 am 03/14/2019 09:41:34 am	Endpoint Endpoint	2019-03-14T09:36: m 2019-03-14T09:36: m	LARGE META VALUES     paras.dst-chrome.exetype-crashpad-handler "user-data-dir-C:\Users\         VapData\Local\Google\Chrome\User     Data' (refich);sonitor-self-annotation=btyse-crashpad-handler "	FORWARD.IP IP-ALL MEDIUM 32 DEVICE.TYPE revendpoint	
03/14/2019 09:41:34 am 03/14/2019 09:41:34 am	Endpoint Endpoint	2019-03-14T09:36: m	<pre>uuta /prefetch:/annites-ser-annitationpypeer/ashpor-hanite*</pre>	DIR.PATH.IBC windows DIR.PATH.IBC windows DIR.PATH.IBC windows5ystem32 DIR.PATH.IBL windows5ystem32 CONTECT.SR file found	
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: m		CONTEXT.ALL file_found CONTEXT.SRC file_protected CONTEXT.ALL file_protected	

Below is an example of the Network event:

EPS1-Server - Co	oncentrator 🗸	02/27/2019 07:43am -	03/26/	2019 07:42am V alias.host = " * Category = 'network event ' ×		(D)
				Guided Mode   Free-Form Mode		
22,535 Events (Asc				Endpoint Event Details   Text Analysis		<u>■</u>   * ×
Endpoint Analysis	V TYPE	EVENT TIME	• 🔅	Download Log 🗸 Karl Version Client 🛛 🖸 Proot to Endpoint Thick Client 🗧 🗗 Analyze Process 🛛 🖸 Proot to Host Overview		
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe	NW SERVICE SESSION ID NWE CATEGORY COLLECTION THE EPS1-Server - Concentrator 6768 Network Event 03/14/2019 09:41:34 am	EVENT TIME 03/14/2019 09:34:15 am	NETWORK REMOTE ADDRESS 1 : 10003
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe		EVENT META	A
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe	• NETWORK (VENT           • 0 02/14/2019 09:34:15 am           • • • • • • • • • • • • • • • • • • •	SESSIONID	5768 )3/14/2019 09:41:34 am
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe	SecureConnector.exe MADEA NETWORK CONNECTION TO 10.254.20.237 FROM 10.87.157.55	SIZE S	332
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe	LARGE META VALUES     param.src-SecureConnector.exe -performer -1d AD6A82C2CA554FBF9AC3109807DC7148 -token	MEDIUM	32 Iwendpoint
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe	c22114e7017e841b8392af5404293ee46609269dc -ip 10.254.20.237 -port 10003 -sha256 3453860145C49C50806600608091F44277931D808076409355800220252028850 -lcif 7 -event	PORT.DST PORT.ALL	10003 10003
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe	FSA_TMP_5388_SC890E73_0002PERFORMER_CNTL -rrd 0	DIR.PATH.SRC	0003 orogramFiles orogramFiles
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe		CONTEXT.SRC CONTEXT.ALL	ile-autorun ile-autorun
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:34:	nwe		CONTEXT.ALL	ile.found ile.found ile.createdInLastMonth

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

## **Isolating Hosts from Network**

**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 **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.

RSA Investigate Respond Users	losts Files Dashboards Reports	
$\nabla$ Filters ×	😫 endpointbrok 🗡 🛛 🖾 Analyze Ever	nts 🗸 🖉 Start Scan 🛛 😨 Stop Scan 📄 🖬 More 🗸
SAVED FILTERS		RISK SCORE 🔸 OS - DESCRIPTION LAST SCAN TIME
Select ~	NATES AND A STREET AND A STR	N/A Microsoft Windows 10 Pro for Workstati 05/08/2020 02:2:
HOST STATUS	(hullball)	N/A Red Hat Enterprise Linux- 7.2 05/05/2020 05:51
Managed	- maileani	N/A Red Hat Enterprise Linux- 7.2 05/06/2020 07:38
		rprise 05/06/2020 07:47
□ Isolated		Analyze Events >
100		Start Scan (Ootpa) 05/06/2020 07:20
•		Stop Scan
0		Network Isolation > Isolate from Network
HOSTNAME		Download MFT to Server
Equals ~ Enter Value		Download System Dump to Server 05/07/2020 08:4-
USERNAME		Download Files to Server 05/06/2020 07:33
Equals ~ Enter Value		Reset Risk Score ation
A SENT SEGURG	NUR. SETUIETAALIT	N/A Microsoft Windows 7 Enterprise 05/08/2020 06:5:

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

RSΛ	Investigate	Respond	Users	Hosts	File	es Dashboards	Reports
100 win	dows	: Start		AN STATUS		GENT LAST SEEN few seconds ago	agent versi 11.5.0.0
DETAILS	PROCESSES	AU .	t Host detai t Files	ls		LIBRARIES AN	OMALIES
ALERTS SEVER	ITY					olled over due to rete	ention policies
2	0	Netwo	ork Isolatior	ı	>	Isolate from Netwo	ork
	нісн	Down	load MFT to	Server		Edit Exclusion List	INT TYPE dpoint
	·	Down	load System	Dump to Se	rver		
Blacklisted File (2 28 event(s)			load Files to			7f01540c1e3eadfb4	b063e8

 In the Isolate from Network dialog, by default, a set of IP addresses are excluded from isolation. For more information, see <u>Network Isolation</u>. 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.

Isolate from Network	×
Network Isolation blocks the host from connecting to the network. All attempted network connections are monitored and reported to the Endpoint Server.	
Add IP addresses to the Exclusion List Default IP addresses excluded from isolation include Endpoint Server, Relay Server, DNS, DHCP, Gateways, 0.0.0.0 and 255.255.255.255.	
Enter one or more valid IPv4 and IPv6 addresses. Use commas to separate multiple values.	
COMMENTS'	
Enter comments	
Cancel Isolate Hos	

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

## **Edit Exclusion List**

To edit the exclusion list:

- 1. Go to 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.

RSA Investigate Respond Users	losts Files Dashboards Rep	ports	
$\nabla$ Filters ×	🖯 🗄 endpointbrok 🗡	alyze Events V 🛛 Start Scan 🛛 Stop Scan 🕻 M	ore 🗸
SAVED FILTERS	HOSTNAME	RISK SCORE $\psi$ OS - DESCRIPTION	LAST SCAN TIME
Select ~		N/A Microsoft Windows 10 Pro for Workstati	05/08/2020 02:2
HOST STATUS		N/A Red Hat Enterprise Linux- 7.2	05/05/2020 05:5
Managed		N/A Red Hat Enterprise Linux- 7.2	05/06/2020 07:3
		terprise	05/06/2020 07:4
Isolated		Analyze Events >	05/05/2020 01:0
RISK SCORE			
100		Start Scan .1 (Ootpa)	05/06/2020 07:2
• • • • • • • • • • • •		Stop Scan	
ο		Network Isolation > Release fi	om Isolation
HOSTNAME		Download MFT to Server Edit Exclu	sion List
Equals v Enter Value		Download System Dump to Server	05/07/2020 08:4
USERNAME		Download Files to Server	05/06/2020 07:3
Equals ~ Enter Value		Reset Risk Score lication	
AGENT GROUPS		N/A Microsoft Windows 7 Enterprise	05/08/2020 06:

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

RSΛ	Investigate	Respon	id Users	Hosts	Files	Dashboards	Reports
100 win	dows ISOLATED	-	• Start Scan	T SCAN STATUS	5 A	gent last seen few seconds ago	agent vei 11.5.0.0
DETAILS	PROCESSES	Αυτο	Export Host de Export Files	etails		BRARIES AN	ention policies o
1	0	¢	Network Isola	tion	>	Release from l	solation
	нідн	ME	Download MF	T to Server		Edit Exclusion	List nt
Blacklisted File (	71)		Download Sys		Server	f <b>ile name</b> N/A	<b>launch argu</b> N/A
FI EVENIL(S)					PCET	N/A	Ν/Δ

- 2. Add or modify the IP addresses in the list.
- 3. 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:

- 1. Go to 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.

RSA Investigate Respond Users H	osts	Files Dashboards	Reports		
$\nabla$ Filters ×	E	∃endpointbrok ∨	🕈 Analyze Events 🛛 🗸 🖾 Start Sca	n 🛛 🕄 Stop Scan 📑 Mo	re 🗸
SAVED FILTERS		HOSTNAME	RISK SCORE 🛛 🗸 OS - I	DESCRIPTION	LAST
Select ~			N/A Micro	osoft Windows 10 Pro for Workstati	. 05/08
HOST STATUS			N/A Red H	lat Enterprise Linux- 7.2	05/05
□ Managed			N/A Red H	lat Enterprise Linux- 7.2	05/06
Roaming	M			Vindows 8.1 Enterprise	05/06
□ Isolated			Analyze Events		
RISK SCORE			Delete	04.4 LTS	05/0
100			Start Scan	terprise Linux 8.1 (Ootpa)	05/0
••			Stop Scan	Vindows 10 Education	
			Network Isolation	> Release from Isolation	
HOSTNAME			Download MFT to Server	Edit Exclusion List	
Equals ~ Enter Value			Download System Dump to Server	04.6 LTS	05/07
USERNAME			Download Files to Server	ux 8 (Core)	05/0
Equals ~ Enter Value			Reset Risk Score	Vindows 10 Education	
AGENT GROUPS			N/A Micro	osoft Windows 7 Enterprise	05/0

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

RSΛ	Investigate	Respor	id Users <b>Hos</b>	<b>ts</b> Files	Dashboards	Reports
100 win	dows ISOLATED	ď	AGENT SCAN S	TATUS A	AGENT LAST SEEN	agent vei 11.5.0.0
DETAILS	PROCESSES	Αυτο	Export Host details Export Files		BRARIES ANC	MALIES
1	0	(	Network Isolation	>	Release from Iso	lation
CRITICAL	нібн	<b>M</b> E	Download MFT to Ser	ver	Edit Exclusion Li	st <sup>'PE</sup> nt
Blacklisted File (	91)		Download System Du	mp to Server	FILE NAME	LAUNCH ARGU
91 event(s)			Download Files to Ser	Ver		N/A N/A

2. 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.

 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:

 Solution
 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.

The Endpoint Agent is unable to communicate with the Endpoint Server. The connection may not be established due to any of the following issues:

 Issue
 • UDP

 • HTTPS

 • Firewall

 • 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:

 cd C:\Windows\System32

 2. Execute the following command:

 <Agent Service name>.exe /testnet

 For example, NWEAgent.exe /testnet

 • If the issue is with the firewall, check the incoming and outgoing firewall rules.

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					

- 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:

cd C:\Windows\System32

Solution
 2. Execute the following command:
 <Agent Service name>.exe /testlognet
 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) > Services or check if the Endpoint Server host IP address is registered with the Admin Server. For more information, see the <i>Physical Host</i> <i>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 Hosts and Files view.	
-------	---	--

	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 <b>Analyze Events</b> from <b>Hosts</b> and <b>Files</b> view for this Endpoint server may not work. To resolve this issue:								
	Note: To get the investigate-service-id:         1) Go to         (Admin) > Services > Concentrator service.								
E	1) Go to $(Admin) > Services > Concentrator service.$ 2) Click $(Admin) > View > Explore tab.$								
Explanation	<ul> <li>3) Expand the sys/stats node list.</li> <li>4) In the UUID filed, copy the value.</li> </ul>								
	<ol> <li>Go to (Admin) &gt; Services &gt; Endpoint Server service.</li> </ol>								
	2. Click $\stackrel{\textcircled{\scriptsize O}}{\longrightarrow}$ > 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	<b>Policy Unavailable</b> - Hosts belong to previous versions, such as NetWitness Platform 11.1 or 11.2, where a policy is not applied.
	<b>Permission Required</b> - 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 Hosts view. Contact your system administrator with the error code.

## File Reputation Service Issue

Is	ssue	When you configure RSA Live for the first time and the File Reputation service is not connected.							
		You must manually enable the File Reputation service. To enable the File Reputation service:							
Solution	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.									
	Check the backlog of alerts for risk scoring.									
	1. SSH to the ESA Primary appliance.									
	2. Execute the following command:									
	<pre>mongo respond-serverauthenticationDatabase admin -u deploy_ admin -p <deploy_admin_password>eval 'db.staging.find({"\$or": [{state:"STAGED"},{state :"WORKING"}]}).count()'quiet</deploy_admin_password></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) > Services > Respond service.									
Solution	b. Click $\diamond$ $\diamond$ $>$ View $>$ Explore.									
Solution	c. Expand the <b>respond/scheduled/jobs</b> node list.									
	d. In the <b>risk-scoring-enabled</b> field, set the value to <b>false</b> .									
	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.									
	<ul><li>ii. In the <b>Options</b> panel, under Deployments, select the Endpoint deployment to delete.</li><li>A confirmation dialog is displayed.</li></ul>									
	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
- Hosts View Agent History Tab

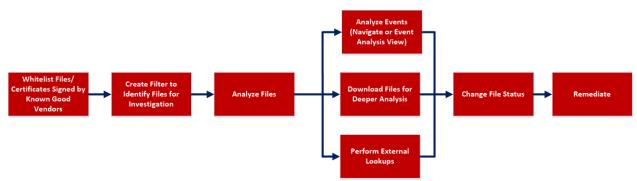
### **Files View**

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 **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
- <u>Analyzing Downloaded Files</u>
- Analyzing Events
- Analyze Certificates
- Changing File Status or Remediate

#### **Quick Look**

Below is an example of the Files view:

RSA Investigate Respond Users H	osts <b>Files</b> Dashboard Reports		6	🖬 💥 🕐 admin >
<b>∀</b> Filters ×	endpointbrok View Certificates	: More Actions V		nlaspi.dll 🔺 🗙
SAVED FILTERS	FILE NAME  FILE NAME  FILE NAME  N HOSTS  FILE NAME  FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME FILE NAME F	REPUTATION Type to filter the list	4	FILE DETAILS RISK DETAILS HOSTS 5
Select ~	Ibdw-0.161.so     06/23/2020.06:36:49 am 2	Eile Name	-	Type to filter list
FILE NAME	🗆 <u>pickup</u> 😳 06/23/2020.08.36:49 am 2	🗹 Risk Score		Show details with values only
Equals v e.g., Filename.dll	MpCmdRun.exe     31 07/06/2020 07:10:58 am 3	- On Hosts	gned,v	General
FILE STATUS	<u>msrawimage.dll</u> 0     07/06/2020.07:10:58 am 1	E Remediation	gned,v	FileName nlaapi.dll
Neutral		🗹 Downloaded	gned,v	Entropy 6.426718559932449
Blacklist     Graylist	<u>hyhostsycdll</u> 07/06/202007:10:58 am 1	🗹 Size	gned,v	Size 68.5 KB
Whitelist	stepstor.pys     0     07/06/202007:10:58 am 1	- First Seen Time	gnedy	
REMEDIATION	(0) 07/08/2020 12:50:26 pm 0		gnedy	Signature
Blocked	Contractor activity of the second part of the	- Signature.Thumbprint	gnedy	Features microsoft,signed,valid,catalog
REPUTATION	Control of the second sec		microsoft,signedy	Timestamp 06/06/2020 07:29:28.356 am
Malicious     Suspicious	~			Thumbprint a4341b9fd50fb9964283220a36
Unknown	StarthémuExperienceHisstean     O     O7/07/2020 05:52:22 am     O		microsoft,signed,v	Signer Microsoft Windows
Known     Known Good	voruntime140.dl     0     07/06/202007:10:38 am 1	73.4KB	microsoft,signed,v	Hash
Invalid	hespidl     0 07/06/202007:10:38 am 1	555.0 KB	microsoft,signed,v	MD5 fb7ddd5b0f0da76c4ed1943233
RISK SCORE	07/06/202007:10:58 am 1	327.6 KB	microsoft,signed,v	SHA1 0e472395e6999e0b22116c298
100	imaadp32.acm     07/06/202007:10:58 am 1	36.1 KB	microsoft,signed,v	SHA256 b487a51f296c9feea8619eb4223
• • • • • • • • • • •	deviceaccess dll     07/06/2020 07:10:58 am 1	181.6 KB	microsoft,signed,v	
0	accase.372     0     07/06/2020 07:10:58 am 1	129.0 KB	microsoft,signed,v	
ON HOSTS	bidsei sys     07/06/2020 07:10:58 am 1	62.5 KB	microsoft,signed,v	
Greater than  v Enter Value	TemTasks.dll     07/06/2020 07:10:58 am 1	105.5 KB	microsoft,signed,v	
OPERATING SYSTEM	regicile dil     0     07/06/2020 07:10:58 am 1	- 155КВ	microsoft,signed,v	
Reset Save Save as	Showing 100 out of 1000+ files   1 selected			

**Filter Files**. You can filter the files by selecting the options in the Filters panel and create filters. For more information, see <u>Filter Files</u>.

#### 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 <u>Analyze Certificates</u>.

**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 <u>Changing File Status or Remediate</u>.

**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 <u>Analyzing Events</u>.

More Actions - 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 <u>Set Files Preference</u>.
- 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 <u>Analyze Hosts with File Activity</u>.

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 Files, and select a file. Below is an example of the File Details view:

RSA Investigate Respond Users Hosts Files Dashboards Reports										📰 % 🕐 admin )					
100 windows 2 signedvalid 14 MB Blacklisted										<b>4</b> <u>■</u> >					
DETAILS A															
ALERTS SEVERITY				① Events ro 4 events	olled over due to retent	tion policies or n	nanual deleti	on will not	be available.				FILE D	ETAILS HO	
1 CRITICAL	О ніgн	0 MEDIUM	<b>1</b> All	EVENT TIM 11/18/2	E 019 10:45:41.000 am	EVENT TYPE Endpoint	CATEGORY Autorun	action N/A	HOSTNAME 206EPS21	<b>user account</b> N/A	OPERATING SYSTEM	FILE NAME OneDrive.exe		o filter list	
Blacklisted File (4) 4 event(s)					<b>FILE NAME</b> N/A	<b>LAUNCH ARGUMEN</b> N/A							<b>⊠ Sho</b> Genera		
	4			TARGET		N/A EVENT TYPE	CATEGORY	ACTION	HOSTNAME	N/A USER ACCOUNT	OPERATING SYSTEM	FILE NAME			OneDrive.exe 4.283913667539894
	2				019 10:45:41.000 am	Endpoint	File	N/A	206EPS21	N/A	windows	OneDrive.exe			14 MB
					FILE NAME	LAUNCH ARGUMEN									pe
				SOURCE TARGET									Signatu		
				EVENT TIM 11/18/2	E 019 10:36:10.000 am	EVENT TYPE Endpoint	CATEGORY File	action N/A	hostname N/A	user account N/A	<b>OPERATING SYSTEM</b> N/A	FILE NAME OneDrive.exe			signed,valid 01/12/2019 12:33:39.626 am
					FILE NAME	LAUNCH ARGUMEN									23710f52824b1c3616496d4a3d
				SOURCE											Microsoft Corporation
				TARGET											
				EVENT TIM 11/18/2	E 019 10:36:10.000 am	EVENT TYPE Endpoint	CATEGORY File	action N/A	hostname N/A	<b>user account</b> N/A	<b>OPERATING SYSTEM</b> N/A	FILE NAME OneDrive.exe	Hash		9edb70213f7015a92e374a8272.
					FILENAME	LAUNCH ARGUMEN				PATH					
				SOURCE TARGET											44bd2686cd0f31edf3da1616a9
				<u> </u>											

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 <u>Analyzing Events</u>.

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 <u>Analyzing Downloaded Files</u>.

- 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.

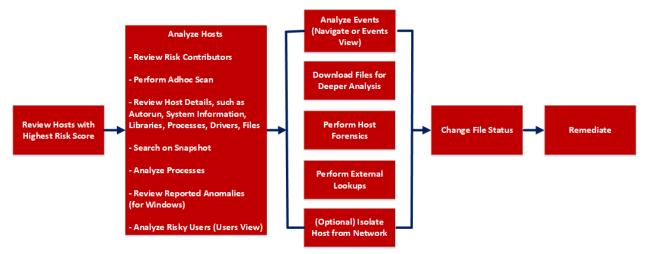
**Hosts** - Displays the hosts on which file activities are present. For more information, see <u>Analyze</u> <u>Hosts with File Activity</u>.

### **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 **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 Files on Host
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*	Filter Host Details
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
- <u>Analyzing Downloaded Files</u>
- 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:

RSA Investigate Respond Users	Hosts Files Dashboards	s Report:	8			3	4		🗷 % 🕐 admin )
▼ Filters ×	🖨 endpointloghy 🗸	🗗 Analyze	Events 🗸 🖉 Start Scan	Stop Scan I Mor	e Actions 🗸 🔶	2	7 🛱 🗓	v	Vindows10
SAVED FILTERS		RISK SCORE	↓ OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGENT SCAN ST/ 🚫	HOST DETAILS	
Select ~	Vindows10	- 200	Microsoft Windows 10 Enterprise	06/24/2020 21:30:33	WINDOWS10\ecat,	a few seconds ago	Idle	Type to filter list	
HOST STATUS	Windwos10-0 ISOLATED	100	Microsoft Windows 10 Enterprise	06/28/2020 21:30:08	WINDWOS10-0\ec.	a few seconds ago	Idle	Show details with v	alues only
Managed	centos1	(31)	CentOS release 6.7 (Final)	06/29/2020 14:30:23		a few seconds ago	Idle 5	Groups	
□ Roaming									Windows-security
□ Isolated									
RISK SCORE								Users	
100									
•									
									Administrators
								Users	
Equals v Enter Value									
Equals v Enter Value									
								Network Interfaces	
									Intel(R) 82574L Gigabit Network.
quals v Enter Value									00:50:56:01:29:06
									10.125.245.185
Equals v e.g.,00:00:00:00:00									fe80::8dc6:d76b:f23d:249
									10.125.244.1
									10.31.64.22,10.31.64.23
Equals ~ e.g., 1.1.1.1  1.1.1.1									false
AGENT LAST SEEN OV CUSTOM DATE								On with the Carton	
								Operating System	
Reset Save Save as									Microsoft Windows 10 Enterprise
Save Save Save as	4		Showin	g 3 out of 3 hosts   1 selecte	d			Build Number	18362

**Filter Hosts**. You can filter the hosts by selecting the options in the Filters panel and create filters. For more information, see <u>Filter Hosts</u>.

#### 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 <u>Analyzing Events</u>.

Start Scan - Starts a scan for the selected hosts.

Stop Scan - Stops a scan for the selected hosts.

More Actions - 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 <u>Delete a Host</u>.
- Download MFT to the server. For more information, see Performing Host Forensics.
- Download System Dump to the server. For more information, see <u>System and Process</u> <u>Memory Dump</u>.
- 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 <u>Export Host</u> <u>Attributes</u>.

- 5 Settings Menu. You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see <u>Set Hosts Preference</u>.
- **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.

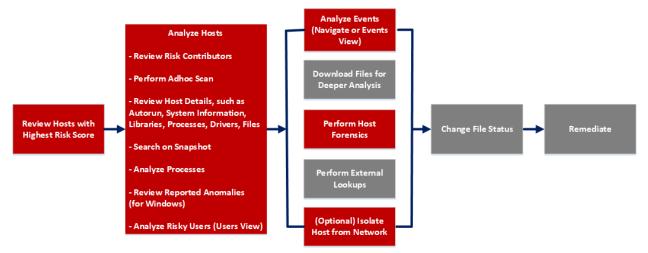
7 View Agent History - Displays the list of commands issued to the agent. For more information, see View Agent History.

### **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 **Hosts** view, and select a host.

#### 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 files on host*	Search Files on Host
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 <u>File</u>
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:

RS/	Investigate	Respond	Users	Hosts Files Dashb	boards Reports					3	🔏 🕐 admin 🕽
100	windows	ď:	AGENT SC Idle		AGENT VERSION SNAP	SHOT TIME 01/02/2020	02:32:50 pm 🐰	-1			
DETAIL	S PROCESSES	AUTORUNS	FILES	DRIVERS LIBRARIES A	NOMALIES DOWNLOA	DS SYSTEM INFO	HISTORY	-	Search by filename,	path or hash	
ALERTS SE	EVERITY 2	10	17	① Events rolled over due to re 1 event	etention policies or manual del	etion will not be available				HOST DETAILS POLIC	
			ALL	EVENT TIME 01/03/2020 07:13:12.000 a	EVENT TYPE CATEGORY am Endpoint Process		HOSTNAME Win101511x64	USER ACCOUNT WN1015112	OPERATING S	Type to filter list	5
Enables Log 1 event(s)				e6c49f7ce186dc4c9da2c3	193469b070c0f1b95a		PATH				
3 event(s) Runs Power	mikatz Activity (3) shell Invoke-Mimikatz F	Function (1)	6 -)	SOURCE <u>cridesse</u> TARGET <b>regesse</b>	cmd.exe reg.add "HKLM/SOFTWARE" NT/CurrentVersion/Image Fi Debugger /t REG_SZ /d "C/W	MicrosoftWindows le Execution Options\sethc.ex /indows\System32\cmd.exe* /	C:\Windows\Syst			Session ID 2	<u>v101511X64\ecat</u> ninistrators,Remote,Desktop,
1 event(s) Possible Loj 4 event(s) Login Bypas 4 event(s)	gin Bypass (4) is Configured (4)					7					
(crent(s)										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 <u>Scan Hosts</u>.

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.

**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:

- 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 Attributes.
- 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 <u>System and Process Memory</u> 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 files on host. Lets you search the files on the host (file name, file path, and SHA-256 checksum). For more information, see <u>Search Files on Host</u>.
- 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.

- **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.
  - Blocked Hashes Status -
    - Updated Host has the latest blocked hashes.
    - Pending Hashes are blocked but the latest hashes are not updated on the host. When the host communicates with the Endpoint server next time, the latest hashes are applied if there are no errors.
  - 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.

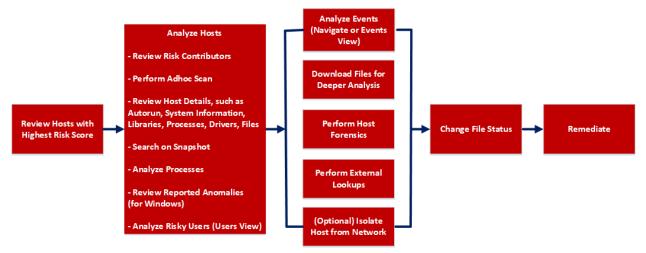
- 6 Alerts Severity Displays list of distinct alerts, such as Critical, High, Medium and All, along with the total number of events associated with the alert.
- 7 Displays events for an alert and metadata associated with a specific event. For more information, see Analyze Hosts Using the Risk Score.

### **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*	<u>Scan Hosts</u>
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
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 <u>File</u>
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files*	Filter Host Details
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
- <u>Analyzing Downloaded Files</u>
- 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:

RSA Investigate	Respon	d U	sers	Hosts	Files Dash	boards Reports									2 %	0	admin >
100 windows		IGENT SCAN		AGENT LAST S a few seconds a		SNAPSHOT TIME	01/02/2020 02:32:50 pm							3			×
DETAILS PROCESSES AUTO	RUNS FI	LES D	RIVER	S LIBRARIE:	S ANOMALIES	DOWNLOADS SYST	EM INFO			5		Search by file	ename,	, path or hash			۹
<b>▽</b> Filters			Proc	esses 🗹 A	inalyze Process	Change File Status	Analyze Events 🛛 🗸	🗄 More 🗸		<b>F</b>	4 ->	TREE VIEW	"		caras.ex	E SK DETAILS	×
PROCESS NAME				PROCESS NAME		LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	SIGNATURE	DOWNLO	<b>41</b> 🔅	FILE DETAILS	LOCAL RI	SK DETAILS	HOSTS
Equals v e.g., Filename.dll										Neutral	microsoft,signed,valid,catalog		4	Type to filter lis			
FILE STATUS						<b></b>				Neutral	microsoft,signed,valid,catalog		8	Show details	with values on	v	
Neutral     Blacklist						•	•			Neutral	microsoft,signed,valid,catalog		°.	General			
Graylist	7		0			•	•			Neutral	microsoft,signed,valid,catalog			R	eName csrss.e	982	
Whitelist						<u> </u>	•			Neutral	microsofLsigned.valid			6	Entropy 4.288	265716902283	
REPUTATION						•	•			Neutral	microsoft.signed.valid				Size 7.5 KE		
Malicious     Suspicious						•	•			Neutral	microsoft.signed.valid				Format pe		
Unknown														Signature			
Known     Known Good										Neutral	microsoft,signed,valid				estures micros	oftsignedvalid	catalog
Invalid				<u>dlihost.exe</u>		٢	۲	1	-	Neutral	microsoft,signed,valid		_			/2009 03:17:39	

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 <u>Scan Hosts</u>.

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 Attributes.
- 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 <u>System and Process</u> <u>Memory Dump</u>.

**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 <u>Investigating a Process</u>.

**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 <u>Changing File Status or Remediate</u>.

**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 <u>Analyzing Events</u>.

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 Files on Host.
- 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 <u>Filter Host Details</u>.
- 8 Settings Menu. You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see <u>Set Hosts Preference</u>.

#### **Process Details**

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

RSΛ	Investigate	Respond	Users	Hosts	Files	Dashboar	ds Reports						
100 win	dows	:	agent scan Idle	I STATUS		.AST SEEN econds ago	AGENT VERS 11.5.0.0	ION	SNAPSHO	DT TIME	06/24/20	20 21:30:33	~
DETAILS	PROCESSES	AUTORUNS	FILES	DRIVER	S LIBF	RARIES	ANOMALIES	DOWN	LOADS	SYSTE	MINFO	HISTORY	
< Process	es Process [	Details											
PROCESS N dwm.exe	AME		owner DWM-2		<sup>ppid</sup> 1460		PATH C:\Windows\Sys	tem32\					
> Loade	d Libraries (8)												
> Image	Hooks (0)												
✓ Suspic	ious Threads (0												

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

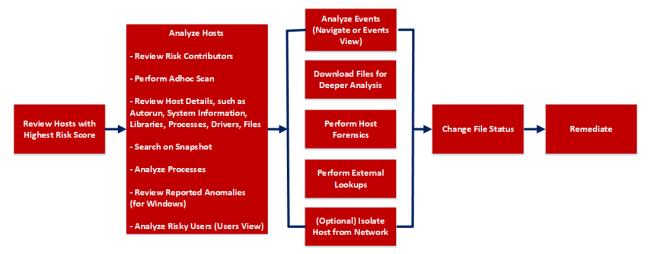
- List of loaded libraries for the selected process, such as DLLs (for Windows), Dylibs (for Mac), or .SO (for Linux).
- List of autoruns (if configured).
- List of image hooks and suspicious threads (for Windows).

# 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*	<u>Scan Hosts</u>
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
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	Filter Host Details
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:

RSA Investigate Respond Users Ho	sta Files Dashboards Reports		🗷 % 🕜 admin >							
100 vindows	100 SNAPSHOT TIME 06/24/2020 21:30:33									
DETAILS PROCESSES AUTORUNS FILES D	Search by filename, path or hash	Q								
<b>∀</b> Filters ×	Autoruns Services Tasks	8	dssvc.dll ×							
File NAME Equals ∨ e.g., Filename.dll	'A'     Change File Status     Of     Analyze Events     V     I     More Actions V	$\Box$	FILE DETAILS LOCAL RISK DETAILS HOSTS							
<u> </u>	□ FILENAME LOCAL RISK SCORE GLOBAL RISK SCORE ON HOSTS REPUTATION FILE STATUS	DOWNLOADED FILE CREATI	Type to hiter list							
FILE STATUS 7	🛛 wildove.dll 🕡 🕡 2 Known Neutral	- 03/19/2019 10:14	Show details with values only							
Neutral	□ <u>amer.dll</u> ← 6 0 0 2 Known Neutral	- 03/19/2019 10:14	Status							
Blacklist     Gravlist		03/19/2019 10:14	Reputation Known							
Whitelist	With Stredil         Ø         Ø         2         Known         Neutral	- 03/19/2019 10:1/								
REPUTATION	CatabilityAcces_ 0 0 2 Known Neutral	03/19/2019 10:1-	General							

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 <u>Scan Hosts</u>.

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 Attributes.
- 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 <u>System and Process</u> 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 <u>Changing File Status or Remediate</u>.

**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 <u>Analyzing Events</u>.

More Actions - 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 Files on Host.

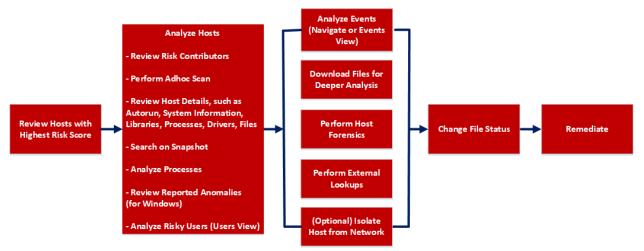
- **Details Panel** Displays the following tabs: 4 • Autoruns - Files that are executed at start-up. • Services - Files that are running as a service for the selected host. • Tasks/Cron jobs - Files that are configured to run as scheduled tasks along with the trigger. Show/Hide Right Panel - Displays 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. Filter Files. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details.
  - 8 **Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see <u>Set Hosts Preference</u>.

# **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 on the host including the files deleted within last 30 days. 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*	<u>Scan Hosts</u>				
Threat Hunter	review host details	Analyze Host Details				
Threat Hunter	search files on host*	Search Files on Host				
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*	Filter Host Details
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:

RSA Investigate Res	pond	Use	rs Hosts	Files	Dashbo	oards Reports								≅ % 0 3	admin >
100 vindova C <sup>2</sup> # Activit Status Activit Latificity Activit Version skapshot Time <u>01/02/2020/02:32:50 pm</u> - 1												<b>₽</b>			
DETAILS PROCESSES AUTORUNS	DETAILS PROCESSES AUTORINS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO											e, path or hash		٩	
<b>▽</b> Filters		File	Change Fil				2							cmd.exe	
FILE NAME			FILENAME	LOCAL	ISK SCORE	GLOBAL RISK SCORE	ON HOSTS	FILE STATUS	REPUTATION	DOWNLOADED	PATH	4	FILE DETAI	LS LOCAL RISK DETAILS	
Equals v e.g., Filename.dll					100			Neutral			C'\Windows\System32	<u>م ا</u>	Type to filte		
FILE STATUS					100			Neutral			C\Windows\SysWOW	64\ 8	Show det	ails with values only	
	7		moengine.dll		•			Neutral			C:\ProgramData\Micro	soft\Windows De	General		
Graylist	· •			6	•	•		Neutral			C\Users\ecat\AppDat	a\Local\Microsoft		FileName cmd.exe	
Whitelist					•	•		Neutral			C:\Users\ecat\AppDat	NLocal/Microsoft	5	Entropy 6.1411942119893	155
REPUTATION					0	•		Neutral			C\Users\ecat\AppDat	a\Local\Microsoft	D	Size 228.5 KB	
Malicious  Suspicious			FileSyncClient.dll		٢	۲	1	Neutral	-	-	C:\Users\ecat\AppDat	i\Local\Microsoft		Format pe	

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 <u>Scan Hosts</u>.

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 Attributes.
- 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 <u>System and Process</u> 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 <u>Changing File Status or Remediate</u>.

**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 <u>Analyzing Events</u>.

More Actions - 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 files on host. Lets you search the files on the host (file name, file path, and SHA-256 checksum). For more information, see Search Files on Host.
- 4 All Files Available on Host Lists all files (reported as part of scan and tracking) on the host. By default, All Files Available on Host toggle is enabled for Windows and Mac.
- 5 **Details Panel** Displays information, such as filename, local risk score, global risk score, on hosts, reputation status, file status, package details and others.

- 6 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.
- 7 Clicking a filename lets you navigate to the Files view for further analysis.
- 8 Filter Files. You can filter files by selecting the options in the Filters panel and create filters.

Note: In the Deleted column, a trash icon appears next to the deleted file. The Deleted column is not displayed if you disable All Files Available On Host.

For more information, see Filter Host Details.

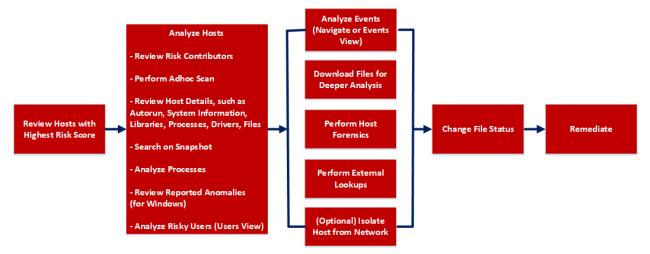
9 Settings Menu. You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.

# **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 Files on Host						
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*	Filter Host Details
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:

RSA Investigate Respond	Use	ers <b>Hosts</b>	Files	1 ashboa	ards Reports	i -						🖃 拨 🕜 admin >
windowa E <sup>2</sup> I Addrest SCAN STATUS ADDREST LASS SEEN ADDRESS A												3
DETAILS PROCESSES AUTORUNS FILES	DRIVE	LIBRARIES	ANOMALIE	S DOWNL	DADS SYSTEM INF			4		Search by fi	lename,	path or hash Q
<b>⊽</b> Filters ×										NWEDriver2303.sys		
FILE NAME		FILENAME	LOCAL R	ISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	SIGNATURE	DOWNLOADED	\$	FILE DETAILS LOCAL RISK DETAILS HOSTS
Equals _ e.g., Filename.dll		NWEDriver2303.pvs						Neutral	signedvalid		4	
FILE STATUS		MpKs11442bd81.sys						Neutral	signed,valid		8	Show details with values only
Neutral     Blacklist								Neutral	signed,valid			General
Graylist			< <u>6</u>					Neutral	signedvalid			FileName NWEDriver2303.sys
Whitelist				٢	۲			Neutral	microsoft.signed.valid.catalog			
REPUTATION				•				Neutral	microsoft,signed,valid			Size 243.0 KB
Malicious	o	condrv.svs		0	Ô	1	-	Neutral	microsoft,signed,valid	-		Format <b>pe</b>

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 <u>Scan Hosts</u>.

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 Attributes.
- Isolation host from the network. For more information, see Isolating Hosts from Network.
- Download MFT to the server. For more information, see <u>Performing Host Forensics</u>.
- Download System Dump to the server. For more information, see <u>System and Process</u> 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 <u>Changing File Status or Remediate</u>.

**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 <u>Analyzing Events</u>.

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 Files on Host.

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.

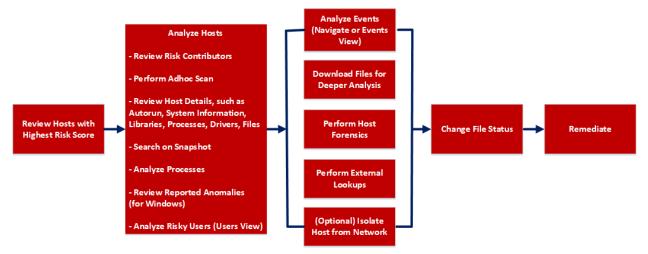
- Local Risk Details Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.
- Hosts Displays the top 100 hosts based on the risk score on which the file is present.
- 6 Clicking a filename lets you navigate to the Files view for further analysis.
- 7 **Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see <u>Filter Host Details</u>.
- 8 **Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see <u>Set Hosts Preference</u>.

# **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*	<u>Scan Hosts</u>
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
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 <u>File</u>
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files*	Filter Host Details
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
- <u>Analyzing Downloaded Files</u>
- Changing File Status or Remediate
- Analyzing Events
- Performing Host Forensics
- Isolating Hosts from Network

### **Quick Look**

Below is an example of the Libraries tab:

RSA Investigate Respond Users H	osts Files Dashboards Reports					<b>≅ % </b> ⑦ admin >			
100 windows i Agent scan sta	atus agent last seen agent vers a few seconds ago 11.5.0.0	33 -			××				
DETAILS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO MISTORY									
P Filters     X     Libraries     X Change File Status     X Analyze Events     Y     I More Actions									
FILE NAME	PROCESS CONTEXT     FILENAME	LOCAL RISK SCORE GLOBAL RISK SC	CORE ON HOSTS R	EPUTATION FILE STATUS		FILE DETAILS LOCAL RISK DETAILS HOSTS			
Equals v e.g., Filename.dll	🗹 vmtoolsd.exe : 8888 sige-2.0.dll	<b>0</b>		nown Blacklisted	✓ 1	Type to filter list			
FILE STATUS	ManagementAgentHost.ec. intLdll	<b>1</b> 100 100	2 к	nown Blacklisted	<ul> <li>Image: A main sector</li> </ul>	Show details with values only			
Neutral     7	UGAuthService.exe: 2096		2 к	nown Blacklisted	<ul> <li>Image: A second s</li></ul>	Status			
Blacklist     Graylist	ManagementAgentHost.ex iconv.dll	6 100 100	) 2 К	nown Blacklisted	🗸 (	Reputation Known			
Whitelist	□ VGAuthService.exe:2096 iconv.dll		2 к	nown Blacklisted	✓ (	General			
REPUTATION	□ VGAuthService.exe:2096 <u>verces-c.3</u>	d 🔟 🔟	2 к	nown Blacklisted	- c	FileName sigc-2.0.dll			
Malicious     Suspicious	svchost.exe:10972 msauserext	. 0 0	) 1 к	nown Neutral	- c	45 Entropy 4.496548278504887			
Unknown	svchost.exe: 10972 wlidsvc.dll	<u> </u>		nown Neutral	- (	Size 76.5 KB			
Known     Known Good	svchost.exe: 4532 bitsperfdll	<u> </u>		nown Neutral	- (	Format <b>pe</b>			
🗆 Invalid	svchost.exe: 4532 bitsigd.dll	<ul> <li>()</li> <li>(</li></ul>		nown Neutral		Deleted false			

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 <u>Scan Hosts</u>.

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 Attributes.
- 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 <u>System and Process</u> 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 <u>Changing File Status or Remediate</u>.

**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 <u>Analyzing Events</u>.

More Actions - 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 Files on Host.
- 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.

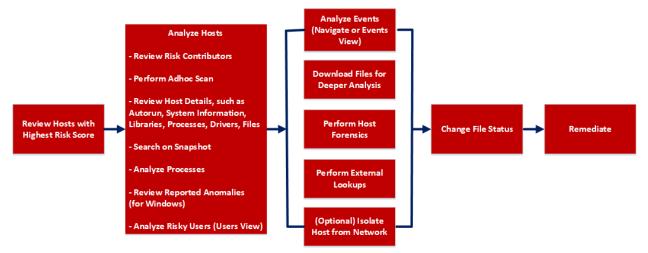
- Local Risk Details Displays the alerts associated with the local risk score, such as Critical, High, Medium and All.
- Hosts Displays the top 100 hosts based on the risk score on which the file is present.
- 6 Clicking a filename lets you navigate to the Files view for further analysis.
- 7 **Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see <u>Filter Host Details</u>.
- 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 Files on Host
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 <u>File</u>
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files	Filter Host Details
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
- <u>Analyzing Downloaded Files</u>
- Changing File Status or Remediate
- Analyzing Events
- Performing Host Forensics
- Isolating Hosts from Network

### **Quick Look**

Below is an example of the Anomalies tab:

RSA Investigate Respond	Users <b>Hosts</b> Files	Dashboards Reports						📰 拨 🕜 admin >
100 vindous 21 i AGENT SCAN STATUS AGENT VESION SNAAPSHOT TIME 01/02/2020/023250 pm 1 4								
DETAILS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO								path or hash Q
♥ Filters         NMEDrier2003ape           NMEDrier2003ape         NMEDrier2003ape								NWEDriver2303.sys ×
FILE NAME 7	🛠 Change File Status 🛛 🖉 Anal	rze Events 🗸 👔 More 🗸 🗲 2						FILE DETAILS LOCAL RISK DETAILS HOSTS
	TYPE	FILENAME		GLOBAL RISK SCORE	ON HOSTS	REPUTATION	IIGNATURE 8	Type to filter list
FILE STATUS	🗹 notifyRoutine	outine <u>NWEDriver2003.pvp</u> (					igned,valid	Show details with values only
Blacklist	notifyRoutine <u>NWEDriver2303.pv</u>	NWEDriver2303.pvs			2 – si	igned,valid -	General EleName NWEDriver2303.sys	
Graylist Whitelist	notifyRoutine	NWEDriver2303.svs 4 6					igned,valid -	5 Entropy 6423240674371836
REPUTATION	notifyRoutine						igned,valid -	Size 243.0 KB
Malicious	basicObjectPointer	MpKa11442bd81.avs					ignedyalid <sup>–</sup>	Format <b>pe</b>
Suspicious Unknown	notifyRoutine	MpKs11442bd81.sys					ignedyalid -	
Known     Known     Kood	notifyRoutine	vm3dme.ns	۲	۲	1	- :	ignedvalid -	Signature Features <b>ciencelvalid</b>

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 <u>Scan Hosts</u>.

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 Attributes.
- 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 <u>System and Process</u> 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 <u>Changing File Status or Remediate</u>.

**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 <u>Analyzing Events</u>.

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 Files on Host.

- 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 <u>Filter Host Details</u>.

**Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see <u>Set Hosts Preference</u>.

#### **Image Hooks**

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

Columns	Description
Туре	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
Туре	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.

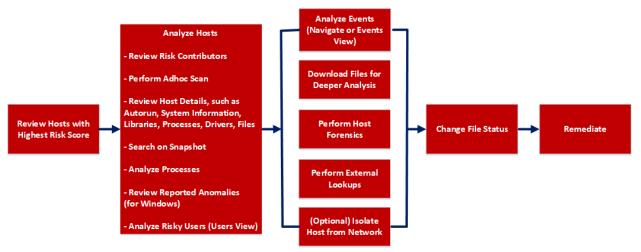
Category	Description
Hive	Name of the registry hive when possible, otherwise it displays the hive ID. Possible values are: hkeyClassesRoot, hkeyCurrentUser, hkeyLocalMachine, hkeyUsers, or hkeyPerformanceData.
Reason	Type of registry discrepancy. Possible values are: notFound, embeddedNull, accessDenied, parentIsHidden, or dataMismatch.
Registry Path	Registry path that is affected. The value is separated by a @ character.
Raw Type	Value type found in the low-level parsing.
Raw Data	Value data extracted from the low-level parsing.
API Type	Value type from the Win32 registry API.
API Data	Value data from the Win32 registry API.

# Hosts View - 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	<u>Scan Hosts</u>
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot	Search Files on Host
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, download files, 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:

RSA Investigate Respond Us	sers <b>Hosts</b> Files Dashboards	Reports						8	% 0	admin >
100 vindows 2										
DETAILS PROCESSES AUTORUNS	FILES DRIVERS LIBRARIES AN	OMALIES DO	WNLOADS		NFO HISTORY					
<b>∀</b> Filters ×	Downloads Save a Local Copy Delete	File - 3	]							
SAVED FILTERS	NAME	TYPE D	OWNLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH			
Select v	dvm.exe	FILE	~	69.5 KB	20 days ago	df84c92b9745f11cab22460e				
	DXCore.dll	FILE	~	109.7 KB	20 days ago	2e5a3168700ba8c2555b4de7				
Wildcard Downloads										
FILE TYPE	smss.exe	FILE	×	143.9 KB	20 days ago	14a5fb352fd89a8969147feee				
	C mft-C-Win101903x6-0-2020-03-04T03-30-15-414Z	MFT	<ul> <li>Image: A second s</li></ul>	121.8 MB	20 days ago	NA				
File Process Dump										
System Dump										
FILE NAME	4									
Equals v e.g., Filename.dll										
SHA256										
Equals v Enter Value										
DOWNLOADED TIME CUSTOM DATE										
Reset Save Save as				Shr	wing 4 out of 4 files   1 selected	1				
				500	ming root of shires [ 1 selected					

1	Agent and Scan Details. You can view the following agent and scan details of the selected	d
	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 <u>Scan Hosts</u>.

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 <u>Scan Hosts</u>.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host Attributes.
- 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 files to the server. For more information, see <u>Download Files Using Full Path or</u> Wildcard.
- Download System Dump to the server. For more information, see <u>System and Process</u> 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 <u>Performing Host Forensics</u>.
- 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.
Туре	Type of file downloaded - MFT, file, memory dump.

Column	Description
Downloaded	Status of the download:
	<ul> <li>Download successful</li> </ul>
- Processing the downloaded file	
	- Errors including download failed
	- Errors downloading one or more files in the group.
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 <u>Analyze</u> <u>Downloaded MFT</u>.

Below is an example of the MFT Viewer:

#### NetWitness Endpoint User Guide

RSA Investigate Respond	Users <b>Hosts</b> Files Dasł	hboards Reports					
100       windows       AGENT SCAN STATUS       AGENT LAST SEEN       AGENT VERSION         ble       afew seconds ago       114.0.0         DETAILS       PROCESS       AUTORUNS       FILES       DRIVERS       LIBRARIES       ANOMALIES       DOWNLOADS       SYSTEM INFO         Image: Complexity of the system in							
MFT-C-WINDOWS10-2019-11-14T06-47-52-777Z		SIZE CREATION TIME (\$FN)					
✓ ➡ C:	RWE-Trace-Oc1ctxt	0 bytes 11/12/2019 07:02:03 pm					
> 🗅 inetpub	RWE-Trace-Oacc.rar	2.0 MB 11/12/2019 11:54:16 am					
> 🗅 wamp64	RWE-Trace-Oacc.txt	0 bytes 11/12/2019 12:48:33 am					
> 🗅 Windows > 🗅 Users	RWE-Trace-0f80.rar	1.0 MB 11/12/2019 12:08:39 am					
ProgramData     Program Files (x86)     SRecycle.Bin	RWE-Trace-0f80.txt	0 bytes 11/11/2019 09:25:01 pm					
	RWE-Trace-0a3c.txt	0 bytes 11/11/2019 07:32:11 pm					
> C Perflogs	RWE-Trace-0c44 - Copy.txt	49.8 MB 11/11/2019 06:56:29 pm					
Program Files     D \$Extend	RWE-Trace-1fc0.txt	8.5 KB 11/11/2019 05:44:35 pm					
<ul> <li>Recovery</li> <li>Documents and Settings</li> </ul>	RWE-Trace-0c44.txt	0 bytes 11/11/2019 05:43:31 pm					
System Volume Information	RWE-Trace-0c30.txt	101.9 KB 11/11/2019 05:42:05 pm					
DELETED FILES	DataCollector01.csv	642.9 KB 11/11/2019 05:03:16 pm					
ALL FILES	Image: NWE-Trace-264c - Copy.txt	21.0 MB 11/11/2019 05:02:52 pm					
	RWE-Trace-264c.txt	0 bytes 11/06/2019 09:38:24 pm					
	Directory path: C:   ♥ No filters applied						

- 1 **Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see <u>Filter MFT</u>.
- 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, dtf.exe.
Size	Size of the file.
Creation Time (\$FN)	File Name (\$FN) creation time.
Creation Time (\$SI)	Standard Information (\$SI) creation time.

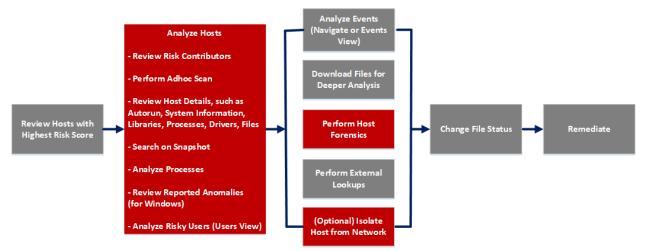
Column	Description
Modification time (\$FN)	\$FN modified time.
Modification time (\$SI)	\$SI modified time.
Access time (\$FN)	\$FN access time.
Access time (\$SI)	\$SI access time.
Update time (\$FN)	\$FN updated time.
Update time (\$SI)	\$SI updated time.
Full Path	Path of the file.
Allocated Size	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 Files on Host	
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*	<u>Isolating Hosts from</u> <u>Network</u>
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:

RSA Investigate Respond Users Hosts	Files Dashboards Reports	2 🗷 😹 🔿 admin >
100 windows	AGENT LAST SEEN AGENT VERSION a few seconds ago 11.5.0.0 SNAPSHOT TIME 06/24/2020 21:30:33	■×
DETAILS PROCESSES AUTORUNS FILES DRIVERS	LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY	Search by filename, path or hash Q
Host File Entries Network Shares Security Produ	ucts Windows Patches Security Configuration	
IP ADDRESS	оля наме 3	
127.0.0.1	localhost	
=1	localhost	

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 <u>Scan Hosts</u>.

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 <u>Scan Hosts</u>.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host Attributes.
- 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 <u>System and Process</u> 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 <u>Search Files on Host</u>.

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 - 10.10.3 and DNS Name - localhost, localhost.localdomain, localhost4, localhost4.localdomain 4
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 Configuratio n	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.

# **Hosts View - Agent History Tab**

The Agent History tab lists the commands along with the respective status and additional details.

## Quick Look

Below is an example of the Agent History tab:

RSA Investigate Respond Users H	osts Files Dashboards Reports -			<u>%</u>	admin >
0 WIN81x64-1 Z : Agent scan windows	STATUS AGENT LAST SEEN AGENT VERS a few seconds ago 11.5.0.0				×
DETAILS PROCESSES AUTORUNS FILES		DOWNLOADS SYSTEM INFO AGENT HISTORY			۹
$\nabla$ Filters ×	Agent History				4
	HOST NAME	COMMAND TIME	COMMAND TYPE	USER NAME	ST# 🛞
COMMAND TIME CUSTOM DATE	WIN81x64-1	04/24/2020 07:03:34 am	Scan	admin	e
	WIN81x64-1	04/22/2020 09:29:38 am	Reset File LogBookmark	admin	~
COMMAND TYPE	<u>WIN81x64-1</u>	04/22/2020 08:12:41 am	Download File	admin	~
`	<u>WIN81x64-1</u>	04/22/2020 07:58:05 am	Reset File LogBookmark		~
STATUS	<u>WIN81x64-1</u>	04/21/2020 09:33:03 pm	Download File	system	~
<u> </u>	WIN81x64-1	04/21/2020 09:33:03 pm	Download File	system	~
REQUEST TYPE	WIN81x64-1	04/21/2020 09:33:03 pm	Download File	system	~
<u> </u>	<u>WIN81x64-1</u>	04/21/2020 09:33:03 pm	Download File	system	~
COMMAND PARAMETER	<u>WIN81x64-1</u>	04/21/2020 06:26:02 pm	Download File	system	~
Contains ~ Enter Value	<u>WIN81x64-1</u>	04/21/2020 06:26:02 pm	Download File	system	~
	<u>WIN81x64-1</u>	04/21/2020 06:26:02 pm	Download File	system	~
Reset		Showing 100 out of 113 Comman	nds		

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 <u>Scan Hosts</u>.

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 Attributes.
- 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 <u>System and Process</u> Memory Dump.

- 2 Search files on host. Lets you search the files on the host (file name, file path, and SHA-256 checksum).
- 3 **Details Panel-** Displays information, such as:
  - Command Time Command issued time.
  - **Command Type** Type of the command (Identity, scan, stop scan, download file, MFT, process dump, system dump, start isolation, update isolation exclusion list, stop isolation, reset file logbookmark, and download multiple files) issued.
  - User Name User who issued the command. For example, Analyst, System.
  - Status Status (success, pending, expired, failed, or cancelled) of the command issued.

**Note:** If the command's status is expired, it means that the agent is unable to process the command even after five retries.

• Command Parameter - Parameters associated with the command. For example, Command parameter for command type Download File is path = C:\Windows\System32\ | filename = cmd.exe | hash = 6f88fb88ffb0f1d5465c2826e5b4f523598b1b8378377c8378ffebc171bad18b

**Note:** Command types such as identity, scan, stop scan, stop isolation, system dump do not contain any associated command parameters.

- **Processed Time** Time at which the command is completed, pending, expired, failed, or cancelled.
- Last Retrieval time Last time when the command is issued to the agent.
- Total Retrieval The number of times the command is issued to the agent.

**Note:** After you upgrade to NetWitness Platform version 11.5, the commands executed in the previous versions are displayed automatically. The fields such as last retrieval time, total retrieval, and user do not contain any values. For system generated commands, the user field value shows as system.

- 4 **Filter Files**. You can filter commands by selecting the options in the Filters panel. For more information, see <u>Filter Host Details</u>.
- 5 Settings Menu. You can set History view preferences by selecting columns from the Settings menu.