NetWitness[®] Platform Version 12.4.1.0

NetWitness Endpoint User Guide



Contact Information

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

Trademarks

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.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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 NetWitness Community. 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.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

June, 2024

Contents

Introduction to Endpoint Investigation	
Endpoint Metadata	
Risk Score	
Severity of Alerts	
Global and Local Risk Score	
Automated Incident Creation Based on Risk Score	
File Reputation	
File Status	
Remediation	
Network Isolation	
Focusing on Endpoint Analysis	
Investigating Files	
Best Practices	
View Files	
Filter Files	
Add and Sort Columns in the Table	
Analyze Files Using the Risk Score	
Analyze Hosts with File Activity	
Analyze Files Using YARA	
Analyze Files Using OPSWAT	
Manual Scan - Scan selected files	
Manual Scan - Scan all files	
Launch an External Lookup for a File	
Set Files Preference	
Export Global Files	
Analyze Certificates	
Change the Certificate Status	
Filter Certificates	
Manage Blocked File Hashes	
Toolbar Actions	41
View Blocked File Hashes	41
Add File Hash	
Import File Hashes	
Delete File Hash	44
Blocked File Hashes List View	

Blocked File Hashes List	
Filter Blocked File Hashes	
Resetting Risk Score of Files	46
Investigating Hosts	
Best Practices	
View Hosts	49
Manage Hosts Using Tags	
Manage Tags	
To Create Tags:	
To Delete Tags:	
Assign tags	
Create and Assign Tags When Generating the Agent Packager	
Unassign tags	
What happens next after unassigning or deleting tags from hosts?	
View Agent History	
Filter Hosts	61
Adding and Sorting Columns in the Table	
Scan Hosts	
Analyze Hosts Using the Risk Score	
Analyze Host Details	74
Filter Host Details	75
Search Files on Host	75
Analyze Processes	
Analyze Autoruns	
Analyze Files	
Analyze Libraries	
Analyze Drivers	
Analyze Anomalies	
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	

Standalone Scan on Air-gapped Windows and Linux Hosts	
Standalone scan workflow:	
Generate the scan configuration file	
Install Endpoint Agent and Register for Standalone Scan	
Start a Standalone scan on Windows	
Start a Standalone scan on Linux	
Upload the Standalone scan result file	
Investigating a Process	
Best Practices	
Analyze a Process	
Analyze Events for a Process	
Changing File Status or Remediate	
Import File Hashes using the Block Hash tool	
JSON File Format	
Analyzing Downloaded Files	
Download Files to Server	
Save Downloaded Files	
Analyze Downloaded Files	
Performing Host Forensics	
Download Master File Table	
Analyze Downloaded MFT	114
System and Process Memory Dump	
Remote Shell	
Example Scenarios	119
RBAC Permissions for Remote Shell	
Download Files Using Full Path or Wildcard	
Filter Downloaded Files	
Save Downloaded File	
Delete Downloaded Files	
Analyzing Events	
Analyze Events from Files View	130
Analyze Events from Hosts View	
Text Analysis for an Endpoint Event	
Isolating Hosts from Network	
Edit Exclusion List	
Release Isolated Hosts	
High Availability (Endpoint Recovery)	
Endpoint Recovery Use Case Example	
Use Case: Endpoint Server EPS 1 turns unresponsive	

Pre-requisites for Endpoint Recovery Configuration	
DNS Recovery Configuration	
NetWitness Endpoint with Third-Party Antivirus Products	
Troubleshooting NetWitness Endpoint	
General Issues	
Multi-server Issue	
Hosts View Issues	
Files View Issues	
Policy Issue	143
Driver Issue	
Download Issue	
File Reputation Service Issue	144
Risk Scoring for Hosts or Files Issue	
Endpoint Broker/Server Issue	
NetWitness Endpoint Reference Materials	
Files View	
File Details View	
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	
Hosts View - YARA Rules Tab	

Introduction to Endpoint Investigation

NetWitness Investigate provides data analysis capabilities in NetWitness, 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 & Real-time events	Tracking Categories
Windows	file, service, dll, process, task, autorun, machine, kernel hook, image hook, registry discrepancies, suspicious threads and removable device(USB) detection	 Process event - Reports any process related activities, such as openprocess, openosprocess, createprocess, createremotethread, openbrowserprocess. File event - Reports any file related activities by an executable, such as readdocument, writetoexecutable, renameexecutable, selfdeleteexecutable, openphysicaldrive. Registry event - Reports activities that result in registry creation or modification, such as modifyservicesimagepath, modifyfirewallpolicy, createservicesimagepath, createsecuritycenterconfiguration, modifybadcertificatewarningsetting, Modifies Startup Folder Location, Modifies Winlogon Registry Settings, Registers Time Provider Dll, Registers Port Monitor Dll, Registers AppInit Dll, Registers AppCert Dll, System event - Reports connection of removable devices(USB devices), IP change and boot events such as, removableDeviceConnected, removableDeviceDisconnected Network event - TCP/UDP and incoming/outgoing. Reports outbound and inbound network connections on all supported Windows 8 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.remote.

Operating System	Scan Categories & Real-time events	Tracking Categories
		For example, Get-Item -Path Registry::HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion.
Linux	file, autrorun, loaded library, systemd, process, cron, initd, and machine	 Process event - Reports process related activities such as createprocess. File event - Reports any file related activities by an executable, such as writetoexecutable.
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. Network event - TCP/UDP and incoming/outgoing. Reports outbound and inbound network connections on all supported Mac operating systems. Reports IPv4 and IPv6 connections.

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

You can track Process events on Mac OS 14 after enabling audit control in your machine. For more information, see Introduction to Endpoint Agent Installation topic in *NetWitness Endpoint Agent Installation Guide for 12.3.1*.

Risk Score

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

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

The following factors contribute to the risk score:

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

This figure is an example of a host with 1 Critical, 2 High and 4 Medium distinct alerts.

ALERTS		.es drivers libraries anomalies downloa	DS SYSTEM INFO HISTORY	
SEVERITY	Medium Alerts ()			HOST DETAILS POLICY DETAILS X
1	> MEDIUM In Root of Program	Directory (2 events)		
CRITICAL	✓ MEDIUM Unexpected OS Press	ocess Source Location (20 events)		
	EVENT TIME	SUMMARY	TARGET PARAM	Show details with values only
2	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\FilesForAgent\amd64\</pre>	N/A	Users
HIGH	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\FilesForAgent\i386\</pre>	N/A	Name Window Manager/DWM-2 Session ID 2
Л	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\Automation\amd64\</pre>	N/A	
MEDIUM	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\Automation\i386\</pre>	N/A	
	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\dtf\bin\amd64\</pre>	N/A	
7	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\dtf\bin\i386\</pre>	N/A	Groups Administrators
ALL	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\Tools\dtf\bin\amd64\</pre>	N/A	
	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\Tools\dtf\bin\FilesForAge_</pre>	N/A	Network Interfaces
	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\Tools\dtf\bin\FilesForAge_</pre>	N/A	MAC Address 00:50:56:01:21:90
	09/28/2021 11:35:03.000 am	<pre>svchost.exe present in C:\DriverTest\Tools\dtf\bin\i386\</pre>	N/A	

All the distinct alert shown in the above example can be for the same file or different files. For example, Modifies File Associations alert is triggered for files, such as svchost.exe and OneDrive.exe.

ALERTS	PROCESSES AUTORUNS FI	LES DRIVERS LIBRARIES	ANOMALIES	DOWNLOADS	SYSTEM INFO				Q
SEVERITY	Medium Alerts 🕕								
1	> MEDIUM In Root of Program	n Directory (2 events)							
CRITICAL	> MEDIUM Unexpected OS Pr	ocess Source Location (20 events)							
	> MEDIUM Windows Firewall	Disabled (3 events)							
2	V MEDIUM Modifies File Asso	ciations (59 events)							
HIGH	EVENT TIME	SUMMARY					TARGET PARAM	SOURCE PARAM	
	09/15/2021 06:25:59.000 pm	svchost.exe modified registry valu	Je HKU∖S-1-5-21-267	1270392-4241876736	-3135916602-1001_C1	asses\AppXvsddybna5	N/A	svchost.exe -k wsappx -p	
4	09/15/2021 06:25:59.000 pm	OneDrive.exe created registry valu	Je HKU\S-1-5-21-267	1270392-4241876736	-3135916602-1001_C1a	asses\odopen\shell\	N/A	OneDrive.exe /background	
MEDIUM	09/15/2021 06:25:59.000 pm	OneDrive.exe modified registry va	lue HKU\S-1-5-21-26	71270392-424187673	6-3135916602-1001_C	Lasses\odopen\shell	N/A	OneDrive.exe /background	
7	09/15/2021 06:25:59.000 pm	svchost.exe modified registry valu	Je HKU\S-1-5-21-267	1270392-4241876736	-3135916602-1001_C1;	asses\AppXkn1qcbm5s	N/A	svchost.exe -k wsappx -p	
ALL	09/15/2021 06:25:59.000 pm	svchost.exe modified registry valu	Je HKU∖S-1-5-21-267	1270392-4241876736	-3135916602-1001_C1a	asses\AppX77ghgzrbz	N/A	svchost.exe -k wsappx -p	
	09/15/2021 06:25:59.000 pm	svchost.exe modified registry valu	Je HKU∖S-1-5-21-267	1270392-4241876736	-3135916602-1001_C1a	asses∖AppXjmgntwab0…	N/A	svchost.exe -k wsappx -p	
	09/15/2021 06:25:59.000 pm	svchost.exe modified registry valu	Je HKU\S-1-5-21-267	1270392-4241876736	-3135916602-1001_C14	asses∖AppXydk58wgm4…	N/A	svchost.exe -k wsappx -p	
	09/15/2021 06:25:59.000 pm	svchost.exe modified registry valu	Je HKU\S-1-5-21-267	1270392-4241876736	-3135916602-1001_C1;	asses\AppXvqhb9dhb3	N/A	svchost.exe -k wsappx -p	

This figure is an example of a file with the Critical alert. The file can have a same alert name being triggered by two different hosts as shown below.

100 Lo	DgonUI.exe 🗗 🚦 он ноэтs ndows 2	signature siz microsoft,signed,valid,catalog 12	ze File status 2.0 KB Blacklisted				
ALERTS							[
SEVERITY	Critical Alerts 0				Event Details		
1	CRITICAL Blacklisted File (5 events)					Event Metadata	
CRITICAL	EVENT TIME	SUMMARY		TARGET	Investigate limeline Z View Alert Details		
0	10/03/2022 09:30:34.000 pm	LogonUI.exe present in C:\Windows\System32		N/A	Summary		
HIGH	10/03/2022 09:30:34.000 pm	LogonUI.exe present in C:\Windows\System32	2\	N/A	LogonUI.exe	∽ host	×
0	10/03/2022 09:56:37.000 am				Overview		
MEDIUM	10/03/2022 09:56:37.000 am	LogonUI.exe		N/A	FILENAME	Win2012R2Tmplte	
THEOREM	10/03/2022 09:56:37.000 am	LogonUI.exe		N/A	LogonUl.exe		
1					DIRECTORY N/A		
ALL							
100 Lo wir	DgonUl.exe टिं : онноэтs doows 2	signature siz microsoft,signed,valid,catalog 12	ze File status 2.0 KB Blacklisted				; C
SEVERITY	All Alerts 0				Event Details		
1	CRITICAL Blacklisted File (5 events)				A Investigate Timeline	Event Metadata	
CRITICAL	EVENT TIME	SUMMARY		TARGET		$\left \frac{1}{2} \right\rangle$ — Hide Duplicates	
0	10/03/2022 09:30:34.000 pm	LogonUI.exe present in C:\Windows\System32		N/A	Summary		
HIGH	10/03/2022 09:30:34.000 pm	LogonUI.exe present in C:\Windows\System32		N/A	LogonUI.exe	V host	×
0	10/03/2022 09:56:37.000 am	LogonUI.exe		N/A	Overview	ALIAS.HOST	
MEDIUM	10/03/2022 09:56:37.000 am	LogonUI.exe		N/A	FILENAME	WIN-TQ4KCTD66K7	
	10/03/2022 09:56:37.000 am	LogonUI.exe		N/A			
1					DIRECTORY N/A		
ALL					SIGNED BY N/A		

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.

Besides the above factors, the risk score is reset when a file no longer matches Yara rules in the subsequent scans

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 Status or Remediate</u>.

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:

SEVERITY	High Alerts 🕕		Event Details	<u> </u>
1	> (HIGH) Opswat Reported	d Suspicious (97 events)	💩 Investigate Timeline 🛛 🗗 View Alert Details	Event Metadata
CRITICAL	> (нісн) In Recycle Bin Dii	rectory (1 events)		$\left \frac{1}{2} \right\rangle$ Hide duplicates
2	🗸 📊 Yara Rule Matche	ed (1000 events)	Summary	
НІСН	EVENT TIME	SUMMARY	ipsrus.xml	♥ Filter meta keys
	09/20/2022 03:44:20.000 pm	kor-kor.xml	Overview	SESSIONID
2	09/20/2022 03:44:20.000 pm		FILENAME	8 36695
MEDIUM	09/20/2022 03:44:20.000 pm	ipsptb.xml	ipsrus.xml	
6	09/20/2022 03:44:20.000 pm	ipsrom.xml	DIRECTORY	09/20/2022 03:44:20 pm
ALL	09/20/2022 03:44:20.000 pm	ipsjpn.xml	N/A	√ 41B
	09/20/2022 03:44:20.000 pm	verisign.bmp	SIGNED BY	
	09/20/2022 03:44:20.000 pm	ipshe.xml	N/A	endpointloghybrid1
	09/20/2022 03:44:20.000 pm	ipsfin.xml		FORWARD.IP
	09/20/2022 03:44:20.000 pm	wmpnss_color120.png		MEDIUM
	09/20/2022 03:44:20.000 pm	ipsar.xml		32
	09/20/2022 03:44:20.000 pm	ipsplk.xml		Revice.TYPE nwendpoint

In the above example, there are three distinct High alerts. For each alert type, associated events are displayed. The details of the 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</u> Using the Risk Score.

Global and Local Risk Score

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

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

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

For more information on the global and local risk score, see Investigating Files and Investigating Hosts.

Automated Incident Creation Based on Risk Score

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

File Reputation

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

The reputations for a file hash are:

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

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

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

File Status

To help analysts triage and focus on their investigation, NetWitness 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, the connection to the following IP addresses are allowed:

- Endpoint Server, Relay Server, DNS, DHCP, Gateways, 0.0.0.0, 255.255.255.255, and any other IP addresses that the agent connects with.
- 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 NetWitness Version 11.3 and later.

The Files view provides a holistic view of all files in your NetWitness platform. 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 <u>File Reputation</u>.
- 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>.
- Investigate files using a rule-based detection technique. YARA helps to identify threats effectively using easy-to-create malware descriptions called YARA rules. For more information, see <u>Analyze</u> <u>Files Using YARA</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:

XNETWITNESS Platform Investigate	Resp	ond Users Host	5 Files	Dashboard	Reports			Č) 2 %	⑦ admin >
∀ Filters		endpointloghy >	View	Certificates	پر Change File	e Status 🛛 🖓 Analyze E	vents	More Action	15 ∨	E.
SAVED FILTERS		endpointloobybrid1 - E	ndnoint Sen	SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCE	FILE STATUS
Select	<u> </u>	endpointloghybrid2 - E	ndpoint Serv	rer /2020 17:0		Known Good	9.5 MB	microsoft,signed,valid	Microsoft Cor	Neutral
FILE NAME		smss.exe	0	06/11/2020 17:0		Known Good	143.9	microsoft,signed,valid	Microsoft Cor	Neutral
Equals v e.g., Filename.dll	_ [wininit.exe	•	06/11/2020 17:0		Known Good	362.7	microsoft,signed,valid	Microsoft Cor	Neutral
FILE STATUS		services.exe	0	06/11/2020 17:0		Known Good	659.0	microsoft,signed,valid	Microsoft Cor	Neutral
Neutral		Isass.exe	0	06/11/2020 17:0		Known Good	56.7 KB	microsoft,signed,valid	Microsoft Cor	Neutral
Graylist		fontdrvhost.exe	0	06/11/2020 17:0		Known Good	802.6	microsoft,signed,valid	Microsoft Cor	Neutral
U Whitelist		LogonULexe	0	06/11/2020 17:0		Known Good	13.5 KB	microsoft,signed,val	Microsoft Cor	Neutral
		spoolsv.exe	0	06/11/2020 17:0		Known Good	747.5	microsoft,signed,val	Microsoft Cor	Neutral
Blocked		vmtoolsd.exe	0	06/11/2020 17:0		Known	81.5 KB	signed,valid	VMware, Inc.	Neutral
		Management	0	06/11/2020 17:0		Known	59.5 KB	unsigned		Neutral
		MsMpEng.exe	0	06/11/2020 17:0		Known	111.3	signed,valid	Microsoft Cor	Neutral
Unknown Known		VGAuthServic	0	06/11/2020 17:0		Known	160.0	unsigned	VMware, Inc.	Neutral
Known Good Invalid		msdtc.exe	0	06/11/2020 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:

4	NETWITNESS Platform	Investigate	Respond L	lsers Hosts	Files Dashboa	rd Repoi	ts				Ŏ	N	H	0	
5	'Filters endpointloghy V		X Change	File Status	🕈 Analyze Events 🗸 🗸	More Act	ions \vee		.						
	FILE NAME	RISK SCORE	FIRST SEEN TIME	ON HOSTS 🛛 🕹	REPUTATION	YARA STA	SIZE	SIGNATURE	PE.RESC 🛞	FILE DETA	ALLS R				
		70	09/19/2022 09:55		Known		2.4 KB	unsigned							
		70	09/19/2022 09:55		Known		45.5 KB	unsigned		Show de	tails with	values or	ly		
		70	09/19/2022 09:55		Known		26.4 KB	unsigned							
		70	09/19/2022 09:55		Known		174 by	unsigned			Rule nam	e 09/20/	2022 03:40 Rules (1)	:40.201 pm	ስ
		70	09/19/2022 09:55		Known		68 bytes	unsigned							
Ø	Contents1.dir	70	09/19/2022 09:55	2	Known	Δ	68 bytes	unsigned	-						
	Help.adml	70	09/16/2022 12:52	2	Known	Not Matc	5.5 KB	unsigned	-			n Known			
		۰	09/16/2022 12:19		Known Good		356.6	microsoft,signed,valid	VMware, Inc						
		۰	09/16/2022 12:19		Known Good		5.4 MB	microsoft,signed,valid	- Microsoft Cc		FileNam	e Conter	ts1.dir	045	
		٥	09/16/2022 12:19		Known Good		57.4 KB	microsoft,signed,valid	Microsoft Cc			e 68 byte	5	7745	
		٥	09/16/2022 12:19		Known Good		184.2	microsoft,signed,valid	VMware, Inc			t script			
		٥	09/16/2022 12:19		Known Good		550.9	microsoft,signed,valid	Microsoft Cc						
		٥	09/16/2022 12:19		Known Good		35.9 KB	microsoft,signed,valid	Microsoft Cc	Jignature		s unsign	d		
		٥	09/16/2022 12:19		Known Good		93.9 KB	microsoft,signed,valid	Microsoft Cc						
	vm3dservice.exe	٥	09/16/2022 12:19	2	Known Good	Not Matc	576.1	microsoft,signed,valid	VMware, Inc			5 5e98d	75dedcb6)eed7c4963	44672c5c

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

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), downloaded status, and YARA rules.

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.



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 **S** 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

Based on the Alert severity, the files can be analyzed using the following options:

- View Alert Details: This option allows you to analyze the files associated with Critical and High alerts. For more information, see <u>Investigating a Process</u>.
- Analyze Process Tree: This option allows you to analyze the files associated with Medium alerts. For more information, see <u>Investigating a Process</u>.

To analyze files associated with Critical and High alerts 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 filename to view the associated alerts and events.

The **Alerts** tab is displayed.

- 4. In the Alerts > Severity panel, click the alert severity, such as Critical or High. 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: For each alert, only the latest 1000 events are displayed.

6. To view all the details associated with a specific event, click on an event. The **Event Details** panel is displayed with the summary and overview information associated with the event.

SEVERITY	High Alerts		Event Details	<u>a</u> 2>
	> HIGH Opswat Reportes		A Investigate Timeline Di View Alext Detaile	Event Metadata
CRITICAL	> HIGH In Recycle Bin Di			
2	🗸 🔫 HICH Yara Rule Match	sci (1000 events)	Summary	
3	EVENTTIME	SUMMARY		
HIGH	07/23/2022 03:44:23.000 pm		Overview	SESSIONID
2	09/20/2022 03:44:20.000 pm		FILENAME	36695
MEDIUM	03/20/2022 03:44:21:000 pm	ipsptb.xml	lpsrus xml	[7] THE
6	03/20/2022 03:44:20.000 pm	iperom.xml	DIRECTORY	00/20/20/20/20/00/4/20 pm
	09/20/2022 03:44:20.000 pm	ipsjøn.oml		R 41B
	07/23/2022 03:44:23.000 pm	verinign.bep	SIGNED BY	
	09/20/2022 03:44:20.000 pm	ipshe.onl	NA	endpointloghybrid1
	03/23/2022 03:44:23.000 pm	ipsfin.ml		FORWARD
	09/20/2022 03:44:20.000 pm	wmpnus_color120.peg		
	09/20/2022 03:44:20.000 pm	ipsar.onl		32
	03/23/2022 03:44:23.000 pm	ipapik.xml		Revice.type nwendpoint

7. You can also view the Event Metadata such as IP, Filename, File hash, and Category in the Event Details panel.

Note: The **contexthub-server.contextlookup.read** permission is enabled only for Administrators, Analysts, Malware Analysts, SOC Managers and Respond Administrators. Administrators can enable this permission for other roles in the **Files** view to view context lookup for meta values and perform the Add/Remove from List actions. For more information, see the "Role Permissions" topic in the *System Security and User Management Guide*.

8. Click the drop-down option besides the metadata value to view additional information about the specific metadata. The **Context Highlights** dialog 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, and Feeds.



- 9. To investigate the original event and destination domain of the event, do any of the following:
 - To investigate the events in a specific time frame, click **Investigate Timeline** on the **Event Details** panel. For more information, see the *NetWitness Investigate User Guide*.
 - To investigate a particular process, click View Alert Details on the Event Details panel. For more information on process analysis, see Investigating a Process.

SEVERITY	High Alerts (1)		Event Details	<u> </u>
1	> (HIGH) Opswat Reporte	d Suspicious (97 events)	A Investigate Timeline	Event Metadata
CRITICAL	> (нідн) In Recycle Bin D	irectory (1 events)		
3	🗸 🗸 🗸 🗸 🗸 🗸 🗸 🗸 Часа Rule Match	ed (1000 events)	Summary	
HIGH	EVENT TIME	SUMMARY	ipsrus.xml	
	09/20/2022 03:44:20.000 pm	kor-kor.xml	Overview	SESSIONID
2	09/20/2022 03:44:20.000 pm		FILENAME	36695
MEDIUM	09/20/2022 03:44:20.000 pm	ipsptb.xml	ipsrus.xml	
6	09/20/2022 03:44:20.000 pm	ipsrom.xml	DIRECTORY	09/20/2022 03:44:20 pm
ALL	09/20/2022 03:44:20.000 pm	ipsjpn.xml	N/A	
	09/20/2022 03:44:20.000 pm	verisign.bmp	SIGNED BY	
	09/20/2022 03:44:20.000 pm	ipshe.xml	N/A	€⊕ endpointloghybrid1
	09/20/2022 03:44:20.000 pm	ipsfin.xml		FORWARD.IP
	09/20/2022 03:44:20.000 pm	wmpnss_color120.png		MEDIUM
	09/20/2022 03:44:20.000 pm	ipsar.xml		32
	09/20/2022 03:44:20.000 pm	ipsplk.xml		nwendpoint

To analyze files associated with Medium alerts 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 filename to view the associated alerts and events.

The Alerts tab is displayed.

- 4. In the Alerts > Severity panel, click the Medium alert severity. 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: For each alert, only the latest 1000 events are displayed.

6. To view all the details associated with a specific event, click on an event. The **Event Details** panel is displayed with the summary and overview information associated with the event.



- 7. You can also view the Event Metadata such as IP, Filename, File hash, and Category in the Event Details panel.
- 8. Click the drop-down option besides the metadata value to view additional information about the specific metadata. The **Context Highlights** dialog 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, and Feeds.



- 9. To investigate the original event and destination domain of the event, do any of the following:
 - To investigate the events in a specific time frame, click **Investigate Timeline** on the **Event Details** panel. For more information, see the *NetWitness Investigate User Guide*.
 - To investigate a particular process, click **Analyze Process Tree** on the **Event Details** panel. For more information on process analysis, see <u>Investigating a Process</u>.

ALERTS	PROCESSES AUTORUNS FIL	ES DRIVERS LIBRARIES ANOMALIES DOWN	NLOADS SYSTEM INFO HISTORY	
SEVERITY	Medium Alerts 3		Event Details	<u> </u>
1	Contraction Contractes Local /		its Investigate Timeline	Event Metadata
CRITICAL	EVENT TIME	SUMMARY		
5	09/27/2022 01:52:52.000 am		Summary	
НІСН	> MEDIUM Floating Module (4	events)	cmd.exe created process net.exe	
_	> MEDIUM In Root of Program	Directory (4 events)	Overview	
5	> MEDIUM Hidden In AppData	a (24 events)	TARGET FILENAME	50329
MEDIUM	> MEDIUM Tasks In Programda	ata Directory (8 events)	net.exe	() TIME
11			TARGET COMMAND LINE	09/27/2022 01:55:38 am
ALL			net.exe ACCOUNTS	
			TARGET DIRECTORY	
			C:\Windows\system32\	endpointloghybrid1
			TARGET USER	
			DESKTOP-R8L2BIL\;	
			TARGET HASH	
			Obd94a338eea5a4e1f2830ae326e6d19	32

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.

	NETW	ITNESS Platfo				Hosts Files					ð 🖻 %		
	⊽ Filters	\exists endpointloghy \vee	View Certificate	≍ ¥Cha	nge File Status	Analyze Events	V I More Actio	ons ∨		!	smss.exe		
0		RISK SCORE	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	FILE STATUS	R (0)		ноѕтѕ	
۵			06/11/2020 17:05:		Known Good	9.5 MB	microsoft,signed,valid	Microsoft Corpo	Neutral		100	ď	
B	z <u>smss.exe</u>		06/11/2020 17:05:	2	Known Good	143.9	microsoft,signed,valid	Microsoft Corpo	Neutral		100	്	
۵	wininit.exe		06/11/2020 17:05:	2	Known Good	362.7	microsoft,signed,valid	Microsoft Corpo	Neutral	l			
۵		٥	06/11/2020 17:05:		Known Good	659.0	microsoft,signed,valid	Microsoft Corpo	Neutral				
۵		٥	06/11/2020 17:05:		Known Good	56.7 KB	microsoft,signed,valid	Microsoft Corpo	Neutral				
C	fontdrvhost		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.

Analyze Files Using YARA

YARA helps analysts with rule-based detection capabilities in identifying and classifying malware. You can easily create malware descriptions using YARA rules. YARA scans can be performed at the Endpoint server level and Endpoint agent level.

Analyze Files at the Endpoint Server Level

Administrators must enable and configure YARA on the Endpoint server. To learn more about enabling and configuring YARA, refer to NetWitness Endpoint Configuration Guide.

Files must be downloaded to the Endpoint server and YARA scans the downloaded files automatically. The scan results are displayed under **YARA STATUS** on the **Files** tab.

To analyze the scanned files,

- 1. Go to Files.
- 2. Select the Endpoint server from the server drop-down, to view files.
- 3. Select a file that is downloaded to the Endpoint server and do any of the following:
 - Click a row to view the YARA scan details associated with the file in the File Details panel.
 - If any file matches one or more YARA rules, the **File Details** panel displays the matching rule names besides scan time.
 - YARA STATUS field displays the status of the YARA scan. Following are the available statuses and their definitions

- Matched The file matches with one or more YARA rules
- Not Matched The file does not match with any of the YARA rules
- Not Yet Scanned There is no scan performed for this file. Files will be scanned automatically once they have been downloaded. After the scan YARA status will be updated to either Matched or Not Matched

Note: When a file matches with a YARA rule, high severity alerts are triggered and, the file's risk score is updated. In the subsequent scans, If the same file doesn't match with a YARA rule, the risk score will be reset.

Note: If a downloaded file has an error, it will not be scanned by YARA and, the **Downloaded** column will display the file download status as **Error**.

2	NETWITNESS Platform	Investigate	e Respond	Users Hos	sts Files Dashboa	ard Re	eports			Q	1	: 0	admin >
5	Filters Sendpointbrok V		tes 🏾 🕱 Char	nge File Status	🖸 Analyze Events 🗸 🗸	: More	e Actions \vee						
	FILE NAME	RISK SCORE \downarrow	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	YARA STA	SIGNATURE	PE.RESOUI	FILE DETAILS RISK			
		100	09/08/2022 04:47		Known	270.6	Not Matc	unsigned	-	Type to filter list			
		100	08/26/2022 11:22		Known	245.9	Not Matc	unsigned	-	Show details with value	ies only		
		100	08/26/2022 11:22		Known	9.8 KB	Not Matc	unsigned					
		100	09/08/2022 04:47		Known	9.1 KB	Not Matc	unsigned			09/21/2022 0	:11:05.658 pm	
		100	09/08/2022 04:47		Known	396.0	Not Matc	unsigned		Scan details	> 2 Susp	icious	
		100	09/08/2022 04:47		Known	1 2 Ma	itches Found	unsigned		Yara			
Ø	VGAuthService.exe		08/26/2022 01:36	3	Known	160.0	Δ	unsigned	VMware, Inc.		09/21/20220	:43:37.373 am	
	dsBase.decTest	100	09/08/2022 04:47	0	Known	48.4 KB	Not Matc	unsigned	-				Ô
		100	09/08/2022 04:47		Known	11.6 KB	Not Matc	unsigned		Status			
		100	09/08/2022 04:47		Known	102.8	Not Matc	unsigned			Known		
		100	09/08/2022 04:47		Known	297.4	Not Matc	unsigned					
		100	09/08/2022 04:47		Unknown	18.0 KB	Not Matc	unsigned		General FileName	VGAuthService	evo	
		100	09/08/2022 04:47		Known	34.1 KB	Not Matc	unsigned			6.0834079603	718125	
		100	08/26/2022 11:22		Known	345 by	Not Matc	unsigned			160.0 KB		
-			Showin	g 100 out of 654	files 1 selected						pe		

- 4. On the **Filters** pane, scroll to the **YARA RULES** section. This section provides options to filter the files based on YARA scan status:
 - Select Matched to view the files that match YARA rules.
 - You can also view the files that do not match YARA rules or not yet scanned against YARA rules, by selecting **Not Matched** or **Not Yet Scanned** from the **YARA RULES** section.

NETWITNESS Platform Investigate	Respond Users Hosts Files	Dashboard Reports		ġ	2 % 0	admin >
∇ Filters ×	endpointbrok View Certificates	rs Change File Status	Analyze Events 🗸 🖬 More A	Actions 🗸		
	FILE NAME RI	ISK SCORE ψ FIRST SEEN TIME	ON HOSTS REPUTATION	SIZE YARA ST	SIGNATURE	PE.RESOUI
Valid Signature Invalid Signature Catalog		08/26/2022 01:36	3 Known Good	69.5 КВ 🛕	microsoft,signed,valid	. Microsoft Corp.
		09/08/2022 04:47	0 Known	244.0	unsigned	
Signed By Microsoft		09/08/2022 04:47	0 Known	182.5	unsigned	
Signed By Apple	http://www.interference.com/interference/interferenc	08/26/2022 04:24	3 Known	29.0 КВ 🔥	unsigned	Apache Softwar
COMPANY NAME		08/26/2022 04:24	3 Known Good	695KB	microsoft signed valid	Microsoft Corp
Equals ~ e.g., RSA Security Inc			0 Kasur		under a d	
FILE HASH		08/28/2022 04:24	3 Known	104.5	unsigned	Free Software P
Equals		09/08/2022 04:47	0 Known	380.0 🛕	unsigned	
		09/08/2022 04:47	0 Known	568.0 🛕	unsigned	
DOWNLOADED	powershell.exe	09/08/2022 02:15	2 Known Good	441.0	microsoft,signed,valid	Microsoft Corp.
Error	VGAuthService.exe	08/26/2022 01:36	3 Known	160.0	unsigned	VMware, Inc.
□ Not Downloaded	□ 21197.msi	09/08/2022 04:47	0 Known	222.0	unsigned	
YARA RULES						
Matched	schema.cpython-36.opt-2.pvc	09/08/2022 04:47	0 Unknown	52.9 KB	unsigned	
Not Matched Not Yet Scanned		80 08/26/2022 01:36	3 Known Good	273.5 🛕	microsoft,signed,valid	Microsoft Corp.
			A <i>Hanna</i>			
Keset Save Save as		Showii	ng 39 out of 39 files 0 selected			

For more information on investigating with YARA, see NetWitness Investigate User Guide.

Yara Scan at the Endpoint Agent Level

NetWitness Platform allows you to quickly perform YARA scan at the Endpoint Agent level. A snapshot of the YARA scan shall be available on the Endpoint server with the details such as:

- List of files matching the YARA rules.
- List of YARA rules ran during the scan and the YARA rules status such as Loaded or Failed to load.

Note: To perform Yara scan at the Endpoint agent level, the agent version must be higher than or equal to 12.1. This is applicable for the Advanced mode Windows Agents.

• YARA version associated with the agent.

To initiate YARA scan on the Endpoint Agent,

- 1. Click Hosts.
- 2. Select the Endpoint server from the server drop-down, to view hosts.
- 3. Select one or multiple hosts and click Scan > Start Yara Scan.

NETWITNESS Platform Investigate	Respond Users	Hosts Files Dashboar	rd Reports			0 2 %	⑦ admin >
abla Filters ×	endpointloghy ~	Analyze Events V	⊖ Scan ∨ © Tags ∨ Start Scan	Hore Actions V			ê !
SAVED FILTERS	HOSTNAME	RISK SCORE 🔶 T	Start Yara Scan	OS - DESCRIPTION	LAST SCAN TIME	AGENT SCAN STATUS	AGENT LAST SEEN
Select	DESKTOP-N6GDHEL	100	Stop Scan				2 days ago
HOST STATUS	Windows	- 100		Microsoft Windows 8.1 Enterpri	08/29/2022 12:35:08 pm	Idle	11 days ago
Managed	windows732bit			Microsoft Windows 7 Enterprise	09/08/2022 12:35:55 pm	Idle	2 days ago
Roaming	DriWin75P1x64			Microsoft Windows 7 Enterprise	08/30/2022 06:50:51 pm	Idle	a minute ago
Isolated Standalone	⊠ <u>Win8-x64</u>		нік	Microsoft Windows 8 Enterpris	08/25/2022 01:01:01 am	ldle	a minute ago
RISK SCORE	⊠ <u>Win8x64bit</u>	100	HLK	Microsoft Windows 8.1 Enterpri	08/30/2022 06:44:59 pm	Idle	2 minutes ago
100	DESKTOP-TVTASOV	- 100		Microsoft Windows 11 Home	08/26/2022 11:57:44 am	Idle	18 days ago
• • • • • • • • • • •	Win81x86-0	100	HLK	Microsoft Windows 8.1 Enterpri	08/24/2022 11:33:25 am	Idle	a minute ago
0	harihara-sudhan-mac	. 🤷 (нік	macOS 11.6.8	08/29/2022 08:04:42 pm	Scanning	15 days ago 🗟
HOSTNAME	🗆 <u>tst</u>			Microsoft Windows 10 Education		Idle	12 days ago
Equals v Enter Value	DESKTOP-T8M198V			Microsoft Windows 10 Education	08/11/2022 11:17:18 am	Idle	19 days ago 🗟

- 4. On Start Yara Scan pop-up,
 - a. Click and upload the YARA rule zip file.
 - b. Select System Drive (Default selection) or All Fixed Drives.
 - c. Enter the Max File Size in Kilo Bites (KB).
 - d. Select CPU Maximum.



5. Click Start scan. See the command status In the Host > History tab.

To analyze the scanned hosts and files:

- 1. Log in to the NetWitness Platform.
- 2. Click Hosts.
- 3. Select the Endpoint server from the server drop-down to view hosts.
- 4. Select the Host and YARA Snapshot Time, and do any of the following:
 - In the Host details view, click **Files** and select a row to view the YARA scan details associated with the file in the **Details** panel.

If any file matches with one or more YARA rules, the **Details** panel displays the matching rule names besides scan time.

ALERTS PROCESSES AUTORUNS FILES DRIVERS	5 LIBRARIES /	NOMALIES DOW	VNLOADS	SYSTEM INFO	HISTORY	YARA RULES	
▼ Filters Files X Change File Status ☑ Analyze Ev	ents 🗸 🗄 Mor	ts V I More Actions V					
FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	FILE STATUS	REPUTATION	DOWNLC 🛞	FILE DETAILS LOCAL RISK DETAILS HOSTS
□ <u>blank.ito</u>	100	100		Neutral	Known	I	
GamesXboxHubAppList.targetsize-64.png	100	100		Neutral	Known		Show details with values only
S-1-5-18 movery							
System.Management.Automation.dll	100	100	1	Neutral	Unknown		Scan Time 09/21/2022 04:08:07.218 am
<u>Notebook.jp</u>	100	100		Neutral	Known		
0000000000000.idx	100	100		Neutral	Unknown		Yara
windows10.0-kb4088779-x86_6ee12b9c03a26803a21ffd08fa8ba1f52f22.		100		Neutral	Unknown		Scan Time 09/19/2022 09:52:44.130 am
S-1-5-21-1323933191-2183225247-1742745553-500.recovery	100	100		Neutral	Unknown		Rule name 🗸 Rules (1) 🗗
GamesXboxHubStoreLogo.scale-100_contrast-high.png	100	100		Neutral	Known		domain.yar:domain
SmallLogo.scale-100.png	100	100		Neutral	Known		Status
GamesXboxHubAppList.scale-100_contrast-white.png	100	100		Neutral	Known		Reputation Unknown
GamesXboxHubAppList.targetsize-64_altform-unplated.png	100	100		Neutral	Known		
Sł	nowing 1803 out of 180	3 files 1 selected					FileName S-1-5-18.recovery

• Toggle the All Files Available on Host to view all the files irrespective of the snapshot selected.

Note: When a file matches with a YARA rule, high severity alerts are triggered and the file's risk score is updated.

	gate	Respond	Users Hosts	Files	Dashboard	Reports			া হা	* 0	admin >
NETWITNESS Flatform				1165						~~~~~	
UKHAYDENMO 🗗 🗄	AG Id	ient scan stø l e	TUS AGENT LAST S 14 days ago	SEEN AG 12	ENT VERSION	SNAPSHOT TIME 07/26/2022 0	12:46:55 pm (Yara S	can) 🗸			a
ALERTS PROCESSES AUTORUNS FIL	es d										
♥ Filters	×	Files							•	LL FILES AVAILA	BLE ON HOST
FILE NAME		0 FIL	NAME			LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	FILE STATUS	REPUTATION	DOWNL 🛞
Equals ~ e.g., Filename.dll						100	100		Neutral	Known	
FILE STATUS		🗆 win				100	100		Neutral	Known	
Neutral						100	100		Neutral	Known	
Blacklist Gravlist						100	100		Neutral	Known	
U Whitelist						100	100		Neutral	Known	
REPUTATION						100	100		Neutral	Known	
Malicious Sussicious						100	100		Neutral	Known	
Unknown		🗆 mdr				100	100		Neutral	Unknown	
Known Known Good						100	100		Neutral	Known	

- On the **Filters** pane, scroll to the **YARA Rules** section. This section provides options to filter the files based on YARA scan status: Select **Matched** to view the files that match YARA rules.
 - You can also view the files that do not match YARA rules or not yet scanned against YARA rules, by selecting **Not Matched** or **Not Yet Scanned** from the YARA rules section.

	Respond Users Hosts Files Dashboard	Reports	ý 2	% 🕐 admin >
UKHAYDENMO C : Idu	ient scan status agent last seen agent version le 14 days ago 12.3.1.0	snapshot тіме 07/26/2022 02:46:55 pm (Yara Sc	an) ~	path or hash Q
ALERTS PROCESSES AUTORUNS FILES D				
∀ Filters ×	Files 🐹 Change File Status 🗹 Analyze Events			ALL FILES AVAILABLE ON HOST
Unsigned	FILENAME	LOCAL RISK SCORE GLOBAL RISK SCORE	ON HOSTS FILE STATUS	REPUTATION DOWNL
Invalid Signature		100 100	2 Neutral	Known
Catalog Signed By Microsoft		100 100	2 Neutral	Known
Signed By Apple		100 100	3 Neutral	Known
RISK SCORE		100 100	2 Neutral	Known
100		100 100	2 Neutral	Known
• • • • • • • • • • • •		100 100	2 Neutral	Unknown
<u> </u>	<u>KetchupYC.mui</u>	100 100	2 Neutral	Known
YARA RULES	<u>mfeannOX.svs</u>	100 100	2 Neutral	Known
Matched	CourClientSvrME.mui	100 100	2 Neutral	Known
Not Yet Scanned	udfsPH.exe	100 100	3 Neutral	Unknown
OPSWAT	directOO.ps1	100 100	2 Neutral	Known

• In the Host details view, click the YARA Rules tab to know if the YARA rules used for the scan are successfully loaded or failed to load. If any of the YARA rules are failed to load, hover over

icon (Failed to load) to know the reason for failure.

ALERTS	PROCESSES	AUTORUNS	FILES	DRIVERS	LIBRARIES	ANOMALIES	DOWNLOADS	SYSTEM INFO	HISTORY	YARA RULES					
YARA RULE					STAT	status									
yara-rule\open-	-source\maldocs\Mal	doc_UserForm.yar			~	V Loaded									
yara-rule\open-	-source\maldocs\Mal	doc_VBA_macro_cod	e.yar		~	V Loaded									
yara-rule\open-	source\maldocs\Mal	doc_Word_2007_XM	L_Flat_OPC.	/ar	~	✓ Loaded									
yara-rule\open-	source\utils\base64.	/ar			~	Loaded									
yara-rule\open-	source\utils\domain.	yar			~	✓ Loaded									
yara-rule\open-	-source\utils\ip.yar				~	✓ Loaded									
yara-rule\open-	source\utils\magic.ya	ır			~	✓ Loaded									
yara-rule\open-	source\utils\suspicio	us_strings.yar			~	V Loaded									
yara-rule\open-	source\utils\url.yar				~	✓ Loaded									
yara-rule\open-	-source\utils\virustot	al.yar			~	Loaded									
yara-rule/open-	source/exploit_kits/E	K_Zeus.yar				Failed to load <	to load source/evaloit kits/FK Zeus var								
yara-rule/open-	source/deprecated/#	ndroid_AliPay_smsSl	tealer.yar			Failed to load									
yara-rule/open-	source/deprecated/#	ndroid_Amtrckr_201	160519.yar			Failed to load									
yara-rule/open-	source/deprecated/A	ndroid_ASSDdevelo	per.yar			Failed to load									
yara-rule/open-	source/deprecated/#	ndroid_AVITOMMS:	yar		\diamond	Failed to load	iled to load								

• In the Host details view, click the History tab to view the command history.

Analyze Files Using OPSWAT

OPSWAT (MetaDefender Core) provides advanced malware detection capabilities by scanning files with multiple anti-malware engines simultaneously. Administrators need to enable and configure OPSWAT on the Endpoint server. To learn more about enabling and configuring OPSWAT, see *NetWitness Endpoint Configuration Guide*.

All downloaded files (executable) will automatically be sent to OPSWAT server for scanning once OPSWAT is enabled and configured on the endpoint servers.

Ņ	NETWITNESS Platf	orm Inves	tigate Re	espond (Jsers Host	s Files Dashbo	ard Reports		Ö 🗷 % Ø admin
7	Filters endpointloghy	 View Cer 	tificates	ຸ້ ແ×് Change	File Status (🗗 Analyze Events 🛛 🗸	: More Actions	~ !) Ninite Chrome FileZilla > Installer.exe
	FILE NAME	RISK SCORE	ON HOSTS	↓ SIZE	DOWNLOADED	FIRST SEEN TIME	OPSWAT STATUS	YARA STATUS	FILE DETAILS RISK DETAILS HOSTS
Ø					~	05/10/2021 08:18:03 am		-	Type to filter list
		0		16.7 KB	 Image: A second s	05/10/2021 10:47:29 am	No Threat Detected		Show details with values only
		0		441.3 KB	 	05/10/2021 10:30:10 am	∆		OPSWAT
		0		24.0 KB	~	05/10/2021 10:08:00 am			Scan Time 05/10/2021 11:50:05.542 am
		0		638.4 KB	~	05/10/2021 10:05:21 am	∆		Scan details V 4 Infected
		0		136.7 KB	~	05/10/2021 10:05:21 am	No Threat Detected		Infected (eset) Eicar test file
		0		87.3 KB	~	05/10/2021 10:05:21 am			Infected (bitdefender) EICAR_Test_File
		0		349.0 KB	~	05/10/2021 10:05:21 am			▲ Infected (k7) Troian (000139291)
		0		5.6 MB		05/10/2021 10:05:21 am			▲ Injected (clamar)
		0		2.6 MB	~	05/10/2021 10:05:21 am	No Threat Detected		EICAK_IEST_FIIE
		0		363.7 KB		05/10/2021 10:05:21 am			
		0		352.0 KB	~	05/10/2021 10:05:21 am			FileName Ninite Chrome FileZilla Installer.exe
		0		882.0 KB	~	05/10/2021 10:05:21 am	No Threat Detected		Entropy 6.788855046872951
		0		557.5 KB	~	05/10/2021 10:05:21 am			Size 415.3 KB
		0		37.9 KB	~	05/10/2021 10:05:21 am	No Threat Detected		
		0		45.9 KB Showing 1	✓ 00 out of 130 file	05/10/2021 10:05:21 am	No Threat Detected		Signature Features signed.valid

Scan files with **OPSWAT**

Downloaded files are automatically sent to the OPSWAT server for scanning. However, you can also initiate the scan manually using options under the **More Actions** menu. Executable files with the following file extensions, *pe, script, macro*, and *elf* are supported by this feature. The maximum file size limit is set to 10MB by default. You can increase or decrease it if required.

Automatic scan:

The endpoint server will automatically send all (executable) downloaded files to the OPSWAT server. The scan results will be displayed under the**OPSWAT STATUS** column on the**Files** tab.

Manual Scan:

You can also manually initiate an OPSWAT scan using the options under the**More Actions** menu on the **Files** tab.

The More Actions menu provides the following options:

Manual Scan - Scan selected files

- 1. Select the files that need to be sent to the OPSWAT server for scanning.
- 2. Select More Actions > Scan with OPSWAT.

XNETWITNESS Platform Investigate	Respond Users Hosts Files	Dashboard	l Reports					Q	3	36	?	admin >
♥ Filters ×	Endpointloghy View Certification	ates 🛛	Change File Status	s 🖸 Anal			: More Actions \vee					Ē
SAVED FILTERS	FILE NAME	RISK SCORE	ON HOSTS 4	SIZE C	DOWNLOADED	ОР	Google Lookup	2				۲
Select	MWEAgent.exe	100		5.6 MB				2				
FILE NAME	NWEDriver15110.sys	0		237.0	~	No	Download File to Serve					
Equals – e.g., Filename.dll	⊠ <u>tzsync.exe</u>	0		61.0 KB	~	No	Save a Local Copy					
FILE STATUS	disksnapshot.exe	100		90.0 KB	~	Nc	Analyze File					
		70		68.0 KB	~	No	Beset Bick Score					
Blacklist Graylist		0		33.0 KB	~	No	Threat Detected Not Matc					
Whitelist		100		17.4 KB	~		Not Mate					

3. Click **Scan** on the confirmation pop-up.

Scan with OPSWAT	×
Selected files that are downloaded to the server will be scanned.	
Cancel	Scan

Manual Scan - Scan all files

1. Select More Actions > Scan All with OPSWAT.

NETWITNESS Platform Investigate	Respond Users Hosts Files	Dashboar	d Reports				Ŏ	8	℅	?	admin >
∀ Filters ×	Endpointloghy View Certific	ates 🛛				More Actions ~ Scan All with OPSIM					[]
SAVED FILTERS	FILE NAME	RISK SCORE	ON HOSTS	↓ size	DOWNLOADED	openness in the second se					8
Select	NWEAgent.exe	100		5.6 MB							
FILE NAME	NWEDriver15110.sys	٥		237.0	~	No Threat Detected					
Equals v e.g., Filename.dll	tzsync.exe	٥		61.0 KB	~	No Threat Detected Not Ma	с				
FILE STATUS	disksnapshot.exe	100		90.0 KB	~	No Threat Detected Not Ma	c				
Neutral Neutral	SC.exe	70		68.0 KB	~	No Threat Detected Not Ma	ю				
	userinit.exe	٥		33.0 KB	~	No Threat Detected Not Ma	ïc				

2. Click **Scan** on the confirmation pop-up.



View OPSWAT Scan Results

The scan results will be displayed under the OPSWAT STATUS column on the Files tab as follows:

- File is infected
- 🚹 Suspicious file

A - Scan failed; see troubleshooting section for more information.

No Threat Detected - The file is clean as of the last scanned time.

- Not yet scanned.

Click on a file to view scan results under the FILE DETAILS panel.

- Scan Time: States the last scanned time.
- Scan details: States whether a file is infected or suspicious or no threat detected, names of antimalware engines that identified the threat.

*	NETW	ITNESS Plat	form	Investigate Re	espond Users H	osts Files D	ashboard Report:	s		Ŏ	F % ()	admin >
٦	7 Filters BEndpointloghy View Certificates X Chan			्र्स Change File Status	Analyze Events	More Action	ns 🗸		csrss.exe			
	FILE NAME	RISK SCORE	ON HOST	s ↓ size	DOWNLOADED	OPSWAT STATUS	YARA STATUS	REMEDIATION	REPUTA 🛞	FILE DETAILS RIS		
		<u></u> 100		5.6 MB					-			
		O		237.0 KB	 	No Threat Detected			-	Show details with va	lues only	
		100		61.0 KB	 		Not Matched		-	OPSWAT		
		<u>o</u> 100		90.0 KB	 	No Threat Detected	Not Matched			Scan Time	06/09/2021 12:02:58.473 pm	י ה
		70		68.0 KB	 	No Threat Detected	Not Matched				Suspicious (eset)	
		•		33.0 KB	 	No Threat Detected	Not Matched				Eicar test file	
Ø	<u>csrss.exe</u>		4	17.4 KB	 ✓ 	۵	Not Matched	-	-		EICAR_Test_File	r)
	WmiPrvSE.	exe O	4	472.5 KB	 	No Threat Detected	Not Matched				EICAR_Test_File	
		٥		20.8 KB	 	No Threat Detected	Not Matched				EICAR_Test_File	
		× 100		111.3 KB	 		Not Matched					
		76		52.5 KB	 		Not Matched				06/09/2021 07:24:26.808 am	
		. 0		110.5 KB	 	No Threat Detected						
		1 70		37.2 KB	 						csrss.exe	
		<u>s</u> 0		49.0 KB							6.2835866986020585	
	WindowsCo	0	3	1.4 MB	-	-	-	-		Size	17.4 KB	

Alerts and Impact on Risk scores

Alerts: Critical alerts will be triggered when OPSWAT finds a file as infected, and High severity alerts when a file is found suspicious.

Risk score: If a file is found infected or suspicious by OPSWAT, the risk score of that file and the corresponding host will be increased.

2	NETW	ITNESS Plat	form	Investigate R	espond Users H	losts Files Da	ashboard Reports				\$ I	% ()	admin >
5	Filters BEndpointloghy View Certificates			View Certificates	Change File Status						csrss.ex		
	FILE NAME	RISK SCORE	ON	łosts ↓ size	DOWNLOADED	OPSWAT STATUS	YARA STATUS	REMEDIATION	REPUTA 🛞		RISK DETA	ILS HOSTS	
		.e 100		5.6 MB						ALERTS SEVERITY			
		c O		237.0 KB	~	No Threat Detected				2	1	0	3
		100		61.0 KB	~		Not Matched		1	CRITICAL	нібн	MEDIUM	ALL
		o 100		90.0 KB	~	No Threat Detected	Not Matched			Process With Opswa			
		70		68.0 KB	 ✓ 	No Threat Detected	Not Matched			22 event(s)			
		•		33.0 KB	~	No Threat Detected	Not Matched			Opswat Reported Inf 2 event(s)	ected (2)		
Ø	csrss.exe	100	4	17.4 KB	✓	۵	Not Matched	-	-				
	WmiPrvSE.	exe O	4	472.5 KB	~	No Threat Detected	Not Matched						
		٥		20.8 KB	~	No Threat Detected	Not Matched						
		xxe 100		111.3 КВ	~		Not Matched						
		76		52.5 KB	~		Not Matched						
		•		110.5 KB	~	No Threat Detected							
		1 70		37.2 KB	~								
		<u>s</u> 0		49.0 KB									

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:

XNETWITNESS Platform Investigate	Respond Users	s Hosts Files Dashl	ooard Report	s				¢ 2 %	ć ? a	dmin >
∇ Filters ×	EPS1 - Endpoi		ᆾ Change File Sta	tus	Analyze Events	More Action	s ∨			•
SAVED FILTERS	FILE NAME	RISK SCORE	↓ FIRST SEEN		N HOSTS R	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	ı ©
Select ~	gedit.dll		09/15/2021	05:58 3			536.0	microsoft,signed,valid	Microsoft Corp	Black
FILE NAME	🗹 <u>dtf.exe</u>	Change File Status	10/29/2021	02:52 4			843.5	unsigned		Neuti
Equals v e.g., Filename.dll		Analyze Events	09/27/2021	11:39 1			0 bytes	unsigned		Neuti
FILE STATUS		Google Lookup	File Name	10:32 1			45.8 MB	microsoft,signed,valid	Microsoft Corp	Neuti
Neutral		VirusTotal Lookup	MD5	05:54 1			3.6 MB	microsoft,signed,valid	Microsoft Corp	Neuti
Blacklist Gravlist		View Certificates S	SHA1	03:48 1			446.8	signed,valid		Neuti
U Whitelist			SHA256	01:59 0			445.7	signed, invalid		Neuti
REMEDIATION		Save a Local Copy	10/29/2021	05:44 2			361.5	microsoft,signed,valid	Microsoft Corp	Neuti
Blocked		Scan with OPSWAT	10/29/2021	01:31 1			3.2 MB	microsoft,signed,valid	Microsoft Corp	Neuti
		Reset Risk Score	10/25/2021	09:48 1			446.8	signed,valid		Neuti
Suspicious			10/25/2021	09:48 1			9.7 MB	signed,valid		Neuti
		(70)	09/23/2021	07:28 1			8.6 MB	unsigned	RSA	Neuti
Known Good		(70)	09/23/2021	07:28 1			8.6 MB	unsigned	RSA	Neuti
	\$R5JPOV4.exe	70	09/23/2021	07:28 1			8.6 MB	unsigned	RSA	Neuti
Reset Save Save as			Show	ing 100 out	t of 26043 files 1	1 selected				

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	>	\$
]
🗹 File Name	,	
🗹 Risk Score		_ ∧
🗹 On Hosts	<u> </u>	
🗹 File Status	,	M
Kemediation		
🗹 Reputation	,	M
☑ Downloaded		
🗹 Size		
🗹 Signature	,	M
🗹 First Seen Time		
🗹 Operating System	,	M
Signature.Timestamp		
Signature.Thumbprint	7	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.

NETWITNESS Platform Investige	ale	Respond Use	ers Hosts	Files Dashi	board Repo	ls			ð	1 %	⑦ admin >
∀ Filters >	×	endpointloghy	. View Ce	ertificates	Change File Statu	5 🖸 Analyze Events	~ ! M	lore Actions ∨			
SAVED FILTERS			RISK SCORE	↑ FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	FILE STATU	5 R 🛞
Select	<u> </u>		٥	06/11/2020 17:05:		Known Good	9.5 MB	microsoft,signed,valid	Microsoft Corpo	Neutral	
FILE NAME			٥	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			0	06/11/2020 17:05:		Known Good	659.0	microsoft,signed,valid	Microsoft Corpo	Neutral	
Neutral			0	06/11/2020 17:05:		Known Good	56.7 KB	microsoft,signed,valid	Microsoft Corpo	. Neutral	
Graylist	-		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 NetWitness 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:

NETWITNESS Platform Investigate		Jsers Hosts Files						Ö 🗟 🎖	🖁 🕜 ad	łmin≯
∀ Filters ×	EPS1-En	dpoi 🗸 View Certifica	ates	석 Change File Status	🗗 Analyze Eve	ents 🗸 🕻 More Acti	'ons∨			
SAVED FILTERS	FILE NAME		RISK SCORE	↓ FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	۱Ö
Select ~	⊠ <u>qedit.dll</u>	Change File Statue	100	09/15/2021 05:58			536.0	microsoft,signed,valid	Microsoft Corp	Black
FILE NAME	□ <u>dtf.exe</u>	Analyze Events	> 98	10/29/2021 02:52			843.5	unsigned		Neut
Equals v e.g., Filename.dll		Google Lookup	> 79	09/27/2021 11:39			0 bytes	unsigned		Neut
FILE STATUS	<u>OneDrives</u>	VirusTotal Lookup	> 70	11/08/2021 10:32			45.8 MB	microsoft,signed,valid	Microsoft Corp	Neuti
Neutral	WinSAT.ex	View Certificates	70	11/05/2021 05:54			3.6 MB	microsoft,signed,valid	Microsoft Corp	Neuti
Blacklist Graylist	U <u>VShieldSc</u>	Download File to Server	70	11/02/2021 03:48			446.8	signed,valid		Neuti
Whitelist	ARMDCH		70	11/02/2021 01:59			445.7	signed, invalid		Neuti
REMEDIATION	C regedit.ext	Scan with OPSWAT	70	10/29/2021 05:44			361.5	microsoft,signed,valid	Microsoft Corp	Neuti
□ Blocked	U WinSAT.ex	Reset Risk Score	70	10/29/2021 01:31			3.2 MB	microsoft,signed,valid	Microsoft Corp	Neuti
	VShieldSca	<u></u>	- 70	10/25/2021 09:48			446.8	signed,valid		Neuti
Malicious Suspicious			(70)	10/25/2021 09:48			9.7 MB	signed,valid		Neuti
Unknown	SREC50ZV		70	09/23/2021 07:28			8.6 MB	unsigned	RSA	Neuti
Known Good			70	09/23/2021 07:28			8.6 MB	unsigned	RSA	Neuti
	sr5jpov4	exe	(70)	09/23/2021 07:28	1	_	8.6 MB	unsigned	RSA	Neuti
Reset Save Save as				Showing 100) out of 26043 fil	es 1 selected				

- 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.

57:34.000+000

Filter Certificates

♥ Filters		< Files Certifica	tes 🛛 🕷 Cha	nge Certificate Status	alyze Events 🗸	
SAVED FILTERS		FRIENDLY NAME	STATUS	ISSUER	THUMB PRINT	NOT VALID BEF
Select		Microsoft Windows Pu	Neutral	C=US, S=Washington, L=Redmond,	99922da31f07a02edb07cd8b60a	2018-06-06T18
sTATUS Neutral Whitelisted Blacklisted						
Is Root Microsoft						
FRIENDLY NAME						
Equals v Enter Value						
THUMB PRINT						
Equals v 99922da31f07a02edb07cd8b60a137f	144					

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

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 \square .

Showing 1 out of 1 certificates | 1 selected

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

Manage Blocked File Hashes

Save as...

Blocked File Hashes view **Files** > **Manage** > **Blocked File Hashes** allows administrators and analysts to perform the following actions.

- View already blocked File Hashes in the deployment.
- Add new File Hash and block it.
- Delete and unblock the Blocked File Hashes.
- Import and block multiple File Hashes using the CSV file.

You can block up to a maximum of 50,000 file hashes.

IMPORTANT:

Reset

Save

- Enter only valid SHA256 hashes; otherwise, the blocking functionality might break.

- Do not block any file hashes signed by RSA, Microsoft, and Apple. It might make your Endpoints unresponsive.

- If the number of already blocked File Hashes is 0, and you import more than 50K File Hashes, only the first 50K File Hashes are blocked.

Note: Analysts must have the **contexthub-server.datasource.read** permission to access the **Blocked File Hashes** view.

Toolbar Actions

The table below lists the toolbar actions available in the **Blocked File Hashes** view.

Option	Description
+ Add Hash	Select this option to block a single File Hash.
🖻 Delete	Select this option to delete the blocked File Hashes.
⊥ Import	Select this option to import and block multiple File Hashes.
< Files	Select this option to return to the Files view.

View Blocked File Hashes

You can view the File Hashes already blocked as part of NetWitness deployment in the **Blocked File Hashes** view.

To view the Blocked File Hashes:

1. Go to Files > Manage > Blocked File Hashes. The Blocked File Hashes view is displayed.

	Investigate	Respond Users	Hosts	Files Dashb	oard Rep	orts Ö	1	劣	② admin >
♥ Filters ×	< Files Blocker	File Hashes + Add Hash	î Delete	± Import ❶					
FILE HASH	FILE HASH		SOURCE	ADDED BY	ADDED DATE	COMMENTS			FILE STATUS
Equals ~ Enter Value	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
SOURCE	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
□ Import	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
Investigate	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
FILE STATUS	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
Blacklist	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
□ Graylist	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
ADDED BY	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
·	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	□ ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
	ccabe63588d5aa633	bb6ca01c69c693534651e7cd14dd533b	c500 Import	admin	05/30/2023 07:09:	demo			Blacklist
Reset				/0./005/011-1-1/1					

2. View the list of Blocked File Hashes in the File Hash column.

Add File Hash

You can add a new File Hash to the list of blocked hashes using the Add Hash option in the Blocked File Hashes view.

To block a new File Hash:

1. Go to Files > Manage > Blocked File Hashes > Add Hash.

The Add File Hash dialog is displayed.

Add File Hash ×
Block hash Instructions
 Enter only valid SHA256 hashes. You can add upto 50k hashes to the block list Do not block any file hashes signed by RSA, Microsoft, and Apple. It might make your Endpoints unresponsive.
Note : Blocking is supported only for the following file types with the windows host running in advanced mode where blocking is enabled: .exe, .com, .sys, .ocr, .bat, .ps1, .vbs, .vbe, .vb, .wsh, .wsf, .cmd
FILE HASH'
COMMENT
Enter Comments
Cancel Block Hash

- 2. Enter the File Hash.
- 3. Specify the reason for blocking the new File Hash in the Comment section.
- 4. Click Block Hash.

Import File Hashes

You can import and block the File Hashes in bulk using the **Import** option in the **Blocked File Hashes** view.

To import the File Hashes:

1. Go to Files > Manage > Blocked File Hashes > Import. The Import File Hashes dialog is displayed.



- 2. Under Import File Hashes using .csv file, do one of the following.
 - Click the block to upload the CSV file.
 - Drag and upload the CSV file in the block.
- 3. Specify the reason for blocking the File Hashes in the **Comment** section.

4. Click Import.

Note: Only the unique file hashes are imported during the Import process. If you import the .csv file with few existing blocked file hashes, the Blocked File Hashes List view is updated to reflect the corresponding changes. The duplicate file hashes are not accounted for the change in the total count of blocked file hashes.

Note: While updating the CSV file, make sure you enter each file hash value in separate rows under a single column and then upload the CSV file to block the file hashes. Refer the following figure.

	А	В	С	D	E	F	G
1	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2116
2	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2117
3	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2118
4	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2116
5	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2117
6	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2118
7	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2119
8	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2120
9	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2121
10	ccabe6358	8d5aa633b	b6ca01c69	c69353465	1e7cd14dd	533bc5008	f9a80f2122

Note: Analysts must have the **contexthub-server.datasource.manage** permission to import the file hashes.

Delete File Hash

You can delete and unblock a blocked File Hash using the **Delete** option in the **Blocked File Hashes** view.

To delete a blocked File Hash:

1. Go to Files > Manage > Blocked File Hashes.

The Blocked File Hashes view is displayed.

		Users Hosts Files	Dashboard Rep	oorts Ö 🖻 % Ö	
♥ Filters ×	< Files Blocked File Hashes	+ Add Hash 🗃 Delete	t. Import		
FILE HASH	FILE HASH	SOURCE	ADDED BY ADDED DATE	COMMENTS	FILE STATUS
Equals ~ EnterValue	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
SOURCE	Ccabe63588d5aa633bb6ca01c69c693534651	.e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
□ Import	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
Investigate	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
Blacklist	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
Graylist	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
ADDED BY	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
~	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
	Ccabe63588d5aa633bb6ca01c69c693534651	e7cd14dd533bc500 Import	admin 05/30/2023 07:09:	demo	Blacklist
Reset		Showing 22563 of 2	2563 blocked file bashes		

2. Select the blocked File Hash and click **Delete**.

The Delete Hash confirmation dialog is displayed.

3. Click Delete.

Blocked File Hashes List View

The Blocked File Hashes List view consists of a Filters panel and the Blocked File Hashes List.

Blocked File Hashes List

The Blocked File Hashes List displays all the Blocked File Hashes in the NetWitness Platform. The following table describes the columns in the Blocked File Hashes List.

Columns	Description						
	Allows you to select the required Blocked File Hash.						
File Hash	Displays the list of Blocked File Hashes						
Source	Displays the Source used for blocking the File Hashes. For Example: Import						
	Note: When you upgrade to 12.3 or later versions from the versions older than 12.0, the Source column displays Investigate for all the File Hashes blocked in the previous deployment using the Import option. The Source column displays Import only for the File Hashes you block using the Import option in NetWitness Platform 12.3 or later versions. If you upgrade to 12.3 or later versions from 12.0 or later versions, the Source column displays Import for the File Hashes blocked in the previous deployment and the current deployment using the Import option.						
Added By	Displays the name of the administrator or the analyst who blocked the File Hashes.						
Added Date	Displays the date on which the File Hashes are blocked. For Example: 03/20/2023 10:00:00AM						
Comment	Displays the comment provided by the administrator or the analyst while blocking the File Hashes.						
File Status	Displays the file status of the Blocked File Hashes. For Example: Blacklisted .						

Filter Blocked File Hashes

You can filter the Blocked File Hashes based on the following parameters.

- Value of the File Hash
- Source used for blocking the File Hashes

- File status of the Blocked File Hashes
- User who blocked the File Hashes

⊽ Filters	×
FILE HASH	
Equals 🗸	Enter Value
SOURCE	
Investigate	
FILE STATUS	
Blacklist Gravitet	
Grayiist	
ADDED BY	
	~
	Reset

Click **Reset** to remove the filters applied.

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:

NETWITNESS Platform Investigate	Respond Users Hosts Files	Dashbo	ard Reports				ð 2 %	5 🕐 ad	min >
♥ Filters ×	EPS1 - Endpoi View Certific	ates	옮 Change File Status	🗗 Analyze Ever	its V i More Actio	ons ∨			
SAVED FILTERS	FILE NAME	RISK SCORE	ψ FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE	PE.RESOURCES	• 🕸
Select ~	Change File Status		09/15/2021 05:58			536.0	microsoft,signed,valid	Microsoft Corp	Black
FILE NAME	dtf.exe Analyze Events	> 98	10/29/2021 02:52			843.5	unsigned		Neuti
Equals v e.g., Filename.dll	Google Lookup	> 79	09/27/2021 11:39			0 bytes	unsigned		Neuti
FILE STATUS	OneDrives VirusTotal Lookup	> 70	11/08/2021 10:32			45.8 MB	microsoft,signed,valid	Microsoft Corp	Neuti
Neutral	WinSATex View Certificates	70	11/05/2021 05:54			3.6 MB	microsoft,signed,valid	Microsoft Corp	Neuti
Blacklist Graylist	VShieldSc Download File to Server	70	11/02/2021 03:48			446.8	signed,valid		Neuti
Whitelist	ARMDCH Save a Local Copy	70	11/02/2021 01:59			445.7	signed, invalid		Neuti
REMEDIATION	Analyze File regedit.exe Scan with OPSWAT	70	10/29/2021 05:44			361.5	microsoft,signed,valid	Microsoft Corp	Neuti
L Blocked	WinSAT.ex Reset Risk Score	70	10/29/2021 01:31			3.2 MB	microsoft,signed,valid	Microsoft Corp	Neuti
REPUTATION	VShieldScamer	70	10/25/2021 09:48			446.8	signed,valid		Neuti
Suspicious		70	10/25/2021 09:48			9.7 MB	signed,valid		Neuti
		70	09/23/2021 07:28			8.6 MB	unsigned	RSA	Neuti
Known Good		(70)	09/23/2021 07:28			8.6 MB	unsigned	RSA	Neuti
	\$R5JPOV4.exe	(70)	09/23/2021 07:28	1		8.6 MB	unsigned	RSA	Neuti
Reset Save Save as			Showing 100) out of 26043 file	s 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 NetWitness 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> Downloaded Files.
- 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.

NETWITNESS Platform Investigate	Respond Users Hosts Files Dashboard Reports Ö 🗷 % 💿	admin >
abla Filters $ imes$	Bendpointbrok V CAnalyze Events V OScan V STags V Hore Actions V	Ê .
saved filters Select	endpointegebybrild : Endpoint Server endpointegebybrild : Endpoint Server endpointegebybrild : Endpoint Server endpointegebybrild : Endpoint Server	serv 🗇
Host STATUS Managed Roaming Isolated	Bhb/755bug2 Red Hat Enterprise Linux-7.2 08/30/2022 11:02:20 am LaiM4edin.	endpointle
HOSTNAME Equals Enter Value AGENT GROUPS		
TAGS		
Reset Save Save as	Showing 2 out of 2 hosts 0 selected	

- 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> Risky Users.
- 5. Click Show next 100 hosts to view other hosts.
- 6. Click the host name to investigate the scan results. For more information, see Analyze Host Details.

Manage Hosts Using Tags

From version 11.7 and later, NetWitness Platform allows you to create Tags to manage the hosts effectively. Tags are custom texts that you can create and assign to hosts for identifying them. A tag can contain alphabets, numbers and special characters(Except \ ', [] " and **space**). You can use these tags to create host groups. You can also filter hosts by tags using the filters pane on the Hosts screen.

Manage Tags

The Manage Tags option allows you to create and delete tags without selecting any hosts.

To Create Tags:

1. Click **Tags > Manage Tags** on the Hosts tab.



2. Enter a valid tag in the text field on the **Manage Tags** pop-up and click $\textcircled{\bullet}$.

Manage Tags	×
remote24	Ð
No Matching Tags, Click 🕀 to create this tag.	
Cancel	Delete

• The tag is created, and a success message will appear.

NETWITNESS Platform Investigate	Respond		:24		×	Ġ	5 2 3	🖌 🕜 admin >
∀ Filters ×	endpointld	ghy Y]	S lags → 🕴	More Actions \checkmark			ê H
SAVED FILTERS				LAST SCAN TIME		AGENT SCAN STATUS		AGENT VERSION
Select	🗆 wintag		100	09/21/2021 12:37:25 pm	a minute ago			
HOST STATUS	Rhel64x64	Manage Tags			× _{hutes ago}			
Managed				(ırs ago			
Roaming Isolated) Irs ago			
Standalone		remote24 音						
RISK SCORE								
100					ırs ago			
<u></u> •					ırs ago			
HOSTNAME								
Equals See Enter Value				Cancel Delet	e purs ago			
USERNAME	SALEVERT	IML1CWI-SECOND	(31)	09/23/2021 03:55:45 am	10 hours ago	Idle	142.47.142	11.7.0.0

3. Repeat step 2 to create more tags.

To Delete Tags:

1. Click **Tags > Manage Tags** on the Hosts tab.

			Users Hosts						*	
♥ Filters		endpoi	intbrok ∨		© Tags ∨ Manage Tags	: More Ac	tions ∨			Ê 🖺
SAVED FILTERS	ĺ	🗆 нозти	AME	RISK SCORE	+ OS - DESCRI	PTION	LAST SCAN TIME	USERNAME		AGENT 💮

2. Select the tags that you want to delete and click **Delete** on the **Manage Tags** pop-up.

Manage Tags	×
Search existing tags or enter a new tag)
orchestra II Windows III domainOU III newtag III mactag III eps2tag III AUI_tag III AUI_tag_manageTags III AUI_tag_eps2_manageTags III ALERTS III more_alerts III alert_demo IIII demo_tag III critical_hosts III from_mypackager III IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
▲ 2 tags will be deleted Cancel Delet	te

3. Click **Delete** on the **Delete Tags** confirmation pop-up.



Note: The tags you deleted will also be unassigned from all associated hosts. If the associated hosts are a part of groups created using these tags as one of the criteria, then the hosts will no longer be a part of those groups. Refer <u>What happens next after unassigning or deleting tags from hosts?</u> for more information.

Assign tags

- 1. Select one or more hosts on the Hosts tab.
- 2. Do one of the following.
 - Select Tags > Assign Tags from the menu.

	Investigate	Respond	Users Hosts	Files	Dashboard	Reports				ġ	۴ł	酱	?	admin >
♥ Filters		endpoint	brok ~ [[2ª Analyze E	Events 🗸	⊖ Scan ∨	© Tags ∨	: More Actions \vee						ê 🗄
SAVED FILTERS			ME		RISK SCORE	OS - DESCRIPT	Unassign Tags	SENT GROUPS	LAST SCAN TIME	TAGS	5			SER\ 💮

• Select a host, right click and select Assign Tags.

The Assign Tags pop-up will appear and shows all the existing tags.

🔆 NET \	WITNESS Platform				Hosts File					0 I %	
⊽Filters	😫 endpointbrok 🗡 🛛 🕻	🗹 Analyze Eve	ents 🗸	\odot Scan \vee	🗞 Tags 🗸	: More Actions \vee					6
I HOSTNAI IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	ME Analyze Events Delete Start Scan Stop Scan Network Isolation Assign Tags Unassign Tags Download MFT to Server Download MFT to Server Download System Dump to Server to Server to Server Download System Dump to Server to Server Delete to Server	SK SCORE	OS - DESCRI Microsoft W Red Hat Ent	PTION indows 10 Ent	AGENT GROUPS	LAST SCAN 09/08/2022 08/30/2022	TIME 04:37:08 am 11:02:20 am	TAGS allMachin. (DesseAre) (allMachin)	SERVER endpointloghybrid 1 - Endp endpointloghybrid 1 - Endp	username ~	Ar (i) a few se 23 days
	Reset Risk Score For Selected	l Host									

- 3. Do one of the following.
 - Enter a valid tag and click to create it. The newly created tag is selected by default.

Assign Tags	×
newtag	(\div)
No Matching Tags, Click 🕀 to create this tag.	
Cancel	Assign

• Search for an existing tag using the text field and select it if required.

Assign Tags		×
bulk28		(+)
bulk28		
1 tags will be assigned	Cancel	Assign

4. Click Assign. These tags will be assigned to the selected hosts.

	tigate Respond Users H	osts Files Dashboard Reports	-6.16. A	×	D E % 0	admin ≻
∇ Filters ×	😂 endpointbrok 🗡	Analyze Events				i
SAVED FILTERS	HOSTNAME	RISK SCORE 🔶 TAGS	LAST SCAN TIME	AGENT GROUPS	AGENT LAST SEEN	OS - DI 🛞
Select ~	win10-1903-x86	100 ALERTS		AgentMigration		
HOST STATUS	Iocalhost.localdomain	100 mactag AUI_tag	08/05/2021 12:42:48 pm		2 months ago	-
Managed	Eí localhost.localdomain	🚥 mactag	08/05/2021 12:42:03 pm		2 months ago 🗟	
Roaming Isolated	caxweglepm1.corp.emc.com	-	08/05/2021 11:59:44 am		2 months ago 🛕	
Standalone	ubuntu-16-3-1	- 🚥	08/05/2021 11:54:44 am	AgentMigration		
RISK SCORE	swtgforsbr2m1.corp.emc.c	100 ALERTS	08/05/2021 11:01:43 am	Mac	a month ago	
100	initsudhanm3	🚥 🧰 mactag) (risky_hosts) 🐽	08/05/2021 11:01:42 am	Mac,demo_grp100	2 months ago	
	win2k12	more_aler risky_hosts	+1 08/05/2021 12:21:32 pm	win2k*,demo_grp100	a month ago	
	win2k6R2	🚥 🛛 👘 more_aler) demo_tag 🕂	1 08/05/2021 12:21:41 pm	win2k*,demo_grp100	a month ago	

Create and Assign Tags When Generating the Agent Packager

You can add tags to the hosts while installing the Endpoint agents. When generating the agent packager on the Agent Packager tab, you can either create new tags or select already existing tags. These tags will automatically be assigned to the host in which the agent will be installed.

1. Click Assign Tags under TAG CONFIGURATION on the Agent Packager tab.

General	Data Retention Scheduler	Agent Packager	Relay Server	3rd Party Scan	Permissions	
Agent	t Packager					
ENDPOINT	SERVER SETTINGS					
ENDPOI	NT SERVER					
endpo	intloghybrid1 - Endpoint Server					
	NT SERVER FORWARDER (OPTION)	4L)				
HTTP5 P	PORT					
SERVER VA						
O None	Oertificate Thumbprint					
CERTIFICA	TE PASSWORD"					
AUTO UNII	NSTALL					
TAG CONF	IGURATION					
SELECTED	TAGS					
Force	Overwrite	and loss of the unstage				
> AG	ENT CONFIGURATION	ar cress of the version.				
Genera	ate Agent Packager Cance	1				
	WITNESS*PLATFORM					

- 2. On the Assign Tags pop-up, do one of the following.
 - Search for an existing tag using the text field and click Assign.

Assign Tags	×
ag	\oplus
newtag mactag eps2tag AUI_tag AUI_tag_manageTags AUI_tag_eps2_manageTags demo_tag from_mypackager	_
4 tags will be assigned Cancel	Assign

Enter a new tag in the text field and click **(b)** to add it to the selection. Click **Assign**.

3. Assigned tags will appear under SELECTED TAGS.

SERVER VALIDATION O None O Certificate Thumbprint	
CERTIFICATE PASSWORD	
AUTO UNINSTALL	
TAG CONFIGURATION	
SELECTED TAGS	
 Force Overwrite Overwrites the installed Windows agent regardless of the version. 	
> AGENT CONFIGURATION	
Generate Agent Packager Cancel	

Note: The tags added while generating the Agent Packager are applicable only to the newly installed agents and not to the manually upgraded agents.

Unassign tags

- 1. Select one or more hosts on the **Hosts** tab.
- 2. Do one of the following.
 - Select Tags > Unassign Tags from the menu.

XNETWITNESS Platfor		Hosts File					* 0	
♥ Filters ♥ endpointbrok ∨	🖓 Analyze Events 🗸 🔿 Scan 🗸	🖏 Tags 🗸	: More Actions \checkmark					Ê .
HOSTNAME	RISK SCORE ψ OS - DESCRIPTION	Assign Tags Unassign Tags	LAST SCAN TIME	TAGS	SERVER	USERNAME		AC 🛞
	Microsoft Windows 10 Ent		09/08/2022 04:37:08 am	allMachin theseAre	endpointloghybrid1 - Endp			a few se

• Right click a host and select **Unassign Tags**. The **Unassign Tags** pop-up will appear and show all the tag assigned to the selected hosts.

X NET	WITNESS Platform				Hosts Fi							* 0	
⊽Filters	🖯 🖯 endpointbrok 🗡	🖞 Analyze Eve	ents 🗸 🤆	∋Scan ∨	🗞 Tags 🗸	: More	Actions \checkmark						ê 🖺
	ME RIS	sk score ↓	OS - DESCRIPTI	ION	AGENT GROUPS		LAST SCAN TIME	TAGS		SERVER	USERNAME		AC S
	Analyze Events Delete		Red Hat Enterp	rise Linux- 7.2			08/30/2022 11:02:20 am	allMachin)	endpointloghybrid1 - Endp	root		23 da
	Start Scan Stop Scan												
	Network Isolation												
	Unassign Tags												
	Download MFT to Server Download System Dump to Se	rver											
	Download Files to Server Reset Risk Score For Selected	l Host											
	Uninstall Selected Agent												

3. Search for the tags you want to unassign, select them and click Unassign.

Unassign Tags		×
Search existing tags		
from_mypackager		
1 tags will be Unassigned	Cancel	Unassign

4. Click Unassign on the confirmation pop-up.

Unassign Tags	×
Tags will be removed from the selected hosts. Note: Selected hosts will no longer be a part of groups that have these tags as criteria.	
No	'n

5. These tags will be Unassigned from the selected hosts.

XNETWITNESS Platform	Investiga	ate Respond Users Hos	i ts Liles Das	hboard Reports		×	z % 0	admin >
♥ Filters		endpointbrok 🗡		Successfu	lly unassigned the Tags			i
SAVED FILTERS		HOSTNAME	RISK SCORE 🔶	TAGS	LAST SCAN TIME	AGENT GROUPS	AGENT LAST SEEN	OS - DI 🛞
Select	<u>, </u>	ubuntu-16-3-1	100		08/30/2021 01:49:11 pm	AgentMigration	a minute ago	
HOST STATUS		win10-1903-x86		ALERTS	09/03/2021 10:15:29 am	AgentMigration	6 days ago	
Managed Roaming		EÍ <u>Rhel67x86 EPS2</u>	•	from_myp		from_packager_grp	15 days ago	

What happens next after unassigning or deleting tags from hosts?

Unassigning/deleting tags from hosts will immediately initiate group & policy evaluation. For example, if a host is a part of the group created using only the unassigned/deleted tag as criteria, the host will no longer be a part of that group. Refer to the following scenarios to understand more.

Example Scenario 1: Assume you create a group with a couple of tags as grouping criteria, all the hosts with these tags assigned will be a part of the group. And, if you delete these two tags(or unassigning from the hosts), the hosts may no longer be a part of this group.

Example Scenario 2: Assume you create a group with a couple of tags and IP addresses as grouping criteria; all the hosts assigned with these tags and IP addresses will be a part of the group. And, if you delete(or unassigning from the hosts) the tags alone, the hosts may still be a part of this group as they are still grouped using the IP addresses.

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 comma	ands, for more information see Filter
	Hosts.	
	Bindker - Endp v C [*] Analyze Events V O Scan V Tags V I More Actions V	
	Destiname RISK S., Agent LAST., Agent Scan St., Agent groud 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 Filter Host Details.

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

₽ Filters ×								
	COMMAND TIME	COMMAND TYPE	USER NAME	STATUS	COMMAND PARAMETER	PROCESSED TIME	LAST RETRIEVAL TIME	TOTAL RETRIEV/ 🔅
	09/16/2022 12:53:17 pm	Download File	system	~	path = C:\cygwin64\usr\sha	09/16/2022 12:53:21 pm	09/16/2022 12:53:18 pm	
COMMAND TYPE	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\Windows\WinSxS	09/16/2022 12:53:18 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\usr\sha	09/16/2022 12:53:18 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\usr\sha	09/16/2022 12:53:19 pm	09/16/2022 12:53:18 pm	
STATUS	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\usr\sha	09/16/2022 12:53:19 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\Jib\pyt	09/16/2022 12:53:18 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\Windows\WinSxS	09/16/2022 12:53:18 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	~	path = C:\Program Files\V	09/16/2022 12:53:19 pm	09/16/2022 12:53:18 pm	
COMMAND PARAMETER	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\usr\sha	09/16/2022 12:53:19 pm	09/16/2022 12:53:18 pm	
Contains ~ Enter Value	09/16/2022 12:53:17 pm	Download File	system	~	path = C:\ProgramData\N	09/16/2022 12:53:20 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\usr\sha	09/16/2022 12:53:20 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	~	path = C:\cygwin64\usr\sha	09/16/2022 12:53:21 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\usr\sha	09/16/2022 12:53:21 pm	09/16/2022 12:53:18 pm	
	09/16/2022 12:53:17 pm	Download File	system	 Image: A second s	path = C:\cygwin64\usr\sha	09/16/2022 12:53:20 pm	09/16/2022 12:53:18 pm	1
Reset				Showin	g 20 out of 20 Commands			

Filter Hosts

You can filter hosts on agent version, agent ID, agent mode, agent upgrade, 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.

C '' `
I-ċ

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.

KINETWITNESS Plat	form Investigate	Respon	d Users	Hosts	Files	Dashboard	Rep	oorts			
▽ Filters		E	Broker - End	lp ∨					© Tags ∨	More Actions ∨	
SAVED FILTERS			HOSTNAME					RISK SCORE	AGENT VERSI	LAST SCAN TIME	16
Select								0	11.6.0.0 🛕		1
HOST STATUS								0	11.6.0.0 🛕		
Managed								0	11.6.0.0 🛕	09/29/2020 04:36:32	1
 Roaming Isolated 								0	11.6.0.0 🛕	09/29/2020 04:22:54	1
								0	11.6.0.0 🛕		1
RISK SCORE	100							0	11.6.0.0 🛕		1
• • • • • •								0	11.6.0.0 💿	09/28/2020 08:34:35	1
0								0	11.6.0.0 🛕	09/29/2020 05:01:05	1
HOSTNAME								0	11.5.1.0 🛕		
Equals ~ Enter Value								0	11.5.1.0 🛕		
USERNAME								0	11.5.1.0 🛕		
Equals ~ Enter Value								0	11.5.1.0 🛕		
								0	11.5.1.0 🔨		
Reset Save	Save as						Show	wing 100 out of 1	1000+ hosts 0 se	elected	

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 ||.

Y Filters		×						
USERNAME		▲						
Equals \vee	Enter value							
AGENT GROUPS								
Equals \vee	Enter value							
NIC MAC ADDRESS	NIC MAC ADDRESS							
	e.g.,00:00:00:00:00	.00						
IPV4								
Equals \vee	10.87.225.68 10.4	40.7.11						
AGENT LAST SEEN		~						
LAST SCAN TIME								
OPERATING SYSTE UNINDOWS Linux Mac	м							
Reset	Save	Save as						

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

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

Y Filters	X	
RISK SCORE	100	
0		
hostname Equals v	Enter value	
username Equals \checkmark	Enter value	
agent groups Equals v	Enter value	l
	e.g. 00:00:00:00:00	
IPV4		
Equals V AGENT LAST SEEN	e.g., 1.1.1.1 1.1.1.1	
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 $\mathbf{\overline{\square}}$.

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

To filter the agents based on the upgrade status, select one of the upgrade statuses. For example, select the **Upgrade Available** checkbox to get the list of agents available for an upgrade.

▽ Filters		×
AGENT LAST SEEN		CUSTOM DATE
LAST SCAN TIME		CUSTOM DATE
OPERATING SYSTEM Windows Linux Mac		
AGENT UPGRADE Failed Pending Upgrade Availal	ble	
AGENT MODE Insights Advanced		
AGENT- DRIVER ERRC		l
Equal ~	Enter Value	
Reset	Save	Save as

To filter the agents based on single or multiple agent groups, select a group from the drop-down list. You can also search the name of the groups from this list.

▽ Filters	×					
HOSTNAME						
Equals ~ Enter Value						
	ĺ					
Equais ~ Enter value						
AGENT GROUPS						
× allgrps × Group1 lin ×	~					
linuxGrps						
pureLinuxGrps	pureLinuxGrps					
WindowsAndLinuxGrps						
LinuxRhelGrps						
Equals ~ e.g., 1.1.1.1 1.1.1.1						
AGENT LAST SEEN	CUSTOM DATE					
Reset Save	Save as					

To filter the agents based on the installation status, select one of the installation statuses. For example, select the **Uninstalled** checkbox to get the list of agents for which the uninstall is initiated or successfully completed.

♥ Filters						
□ Failed						
Pending						
Upgrade Available						
AGENT MODE						
Insights						
□ Advanced						
AGENT INSTALLATION STATUS						
□ Installed						
🗹 Uninstalled						
AGENT- DRIVER ERROR CODE						
Equal ~ Enter Value						
SECURITY CONFIGURATIONS						
AGENT ID						
Fault v Enter Value						
Enter value						
AGENT VERSION						
Equals v e.g., 11.0.0.0						
Reset Sa	ve	Save as				

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

In 12.3 and later versions, you can filter the hosts on specific versions of Windows, Mac, and Linux using the **Operating System Description** field.

For Example: CentOS Linux 7 (Core), Microsoft Windows 10 Enterprise, and Microsoft Windows Server 2016 Standard. Refer the following figure.

♥ Filters		×
AGENT LAST SEEN		CUSTOM DATE
LAST SCAN TIME		CUSTOM DATE
OPERATING SYSTEM Windows Linux Mac		
OPERATING SYSTEM I	DESCRIPTION	~
CentOS Linux 7 (Core)	
Microsoft Windo	ows 10 Enterprise	
Microsoft Windo	ows Server 2016 Sta	ndard
Upgrade Availat	ble	
AGENT MODE		
Insights		
□ Advanced		
AGENT STATUS		
Reset	Save	Save as

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.

Type to filter the list	>	ŝ
	5.24	5.9
🗹 Hostname	⊢_	
🗹 Risk Score	5.24	5.8
🗹 Agent Last Seen		
🗹 Agent Scan Status	5.244	4.2
🗹 Agent Groups	4.57	
🗹 IPv4	157.	2/
🗹 Policy Status	5.244	4.2
🗹 Agent Mode		
🗹 Last Scan Time	157.	64
🗹 Username		
🗹 Agent Version	5.24	5.9
🗹 Agent- Driver Error Code	5 244	42
🗹 Operating System		
OS - Description	.157.	69

- 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.

You can either choose to perform a quick scan or a full system scan.

Quick scan - Scans all executable files that are loaded in memory. Both Insights and Advanced agents support quick scan.

Full System Scan - Scans all fixed drives or the system drive You can perform a full system scan only on advanced agents that are in version 11.6 or later. Native executables are included in the full system scan, by default

When 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 perform a Quick Scan:

- 1. Go to Hosts.
- 2. Select one or more hosts (up to 100) at a time, and do one of the following:

- Click Scan > Start Scan from the menu (Or)
- Right-click and select Start Scan from the context menu

3. Click Start Scan on the pop-up. Quick scan is initiated for 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.

Note: By default, the scan utilizes 25% of the CPU. You can click CPU Maximum and select a value from 5% to 100%. Increasing the CPU Maximum limit reduces the scan time but could lead to more CPU usage.

To perform a Full System 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:
 - Click Scan > Start Scan from the menu bar (Or)
 - Right-click and select Start Scan from the context menu

NETWITNESS Platform Investi	gate		Hosts Files				ð 2 % () admin >
♥ Filters ×		∃ endpointbrok ∨		⊖ Scan ∨ Start Scan	S Tags ∨ I More Actions ∨			ê
SAVED FILTERS		HOSTNAME	RISK SCO	Stop Scan	SCRIPTION	LAST SCAN TIME	USERNAME	tags 🔅
Select ~	Ø			Microso	oft Windows 10 Enterprise	11/15/2021 03:46:07 pm	WINTAG\Administrator,WINTAG\ecat,Window M.	validation
HOST STATUS	Ø			Microso	oft Windows 10 Enterprise	10/29/2021 06:38:48 am	DESKTOP-5QIN3DU\kslp	kslp-agent kslp
Managed				Red Hat	t Enterprise Linux Server release 6.4 (Santiago)	11/15/2021 07:41:34 am		
Roaming Isolated			1	Red Hat	t Enterprise Linux Server release 6.4 (Santiago)	11/03/2021 10:08:50 am		kslp-pack
Standalone			3	3 Microso	oft Windows 10 Home			
RISK SCORE			3	1 Microso	oft Windows Server 2016 Standard	11/11/2021 09:29:34 pm	Window Manager\DWM-3,Window Manager\DW.	
100			3	1 Microso	oft Windows 10 Pro for Workstations	11/02/2021 06:16:39 pm	WINDOWS\ecat,Window Manager\DWM-1	validation
• • • • • • • • • •				Microso	oft Windows 10 Enterprise	11/11/2021 01:18:03 pm	CORP\dhd,CORP\dhd	
HOSTNAME								
Equals ~ Enter Value								
AGENT GROUPS								
TAGS								
~								
	1_							
Reset Save Save as					Showing 8 out of 8 hosts 2 sele	ted		

1. From the Start Scan pop-up, select Full System Scan (Only on advanced agents that are 11.6 or higher.)

- 2. Select System Drive(Default selection) or All Fixed Drives
- 3. Click **Start Scan** on the pop-up.

Start Scan ×
Performs a quick scan of all executable files available in the memory. The total time to complete the scan depends on CPU Maximum.
✓ Full System Scan (For advanced agents that are in version 11.6 or higher) Select the drives and file types that need to be scanned. This selection will have a direct impact on the performance and duration of the scan. By default, native executables are included in the scan.
 DRIVE O System Drive O All Fixed Drives
> CPU Maximum (Default usage 25%)
Cancel Start Scan

Note: An Endpoint server supports up to 10k Full System Scans in a rollover period.

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.

Based on the severity of the alert triggered by the host, you can analyze the host using the following options:

- View Alert Details: This option allows you to analyze the host when Critical and High alerts are triggered. For more information, see Investigating a Process.
- Analyze Process Tree: This option allows you to analyze the host when Medium alerts are triggered. For more information, see Investigating a Process.

To analyze the hosts (which trigger Critical or High alerts) 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.

The Alerts tab is displayed.

4. In the Alerts > Severity panel, click the alert severity such as Critical or High.

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.

SEVERITY	High Alerts		Event Details	<u> </u>
1	> HIGH Opswat Reporte	d Suspicious (97 events)	to be under the second	Event Metadata
CRITICAL	> нідн) In Recycle Bin D	irectory (1 events)	Investigate filleline	
2	🗸 н нан Yara Rule Match	ed (1000 events)	Summary	
ЫСИ	EVENT TIME	SUMMARY	ipsrus.xml	🖓 Filter meta keys
HIGH	09/20/2022 03:44:20.000 pm	kor-kor.xml	Overview	SESSIONID
2	09/20/2022 03:44:20.000 pm	ipsrus.xml	FILENAME	 36695
MEDIUM	09/20/2022 03:44:20.000 pm	ipsptb.xml	ipsrus.xml	
6	09/20/2022 03:44:20.000 pm	ipsrom.xml	DIRECTORY	09/20/2022 03:44:20 pm
ALL	09/20/2022 03:44:20.000 pm	ipsjpn.xml	N/A	
	09/20/2022 03:44:20.000 pm	verisign.bmp	SIGNED BY	
	09/20/2022 03:44:20.000 pm	ipshe.xml	N/A	←⊕ endpointloghybrid1
	09/20/2022 03:44:20.000 pm	ipsfin.xml		FORWARD.IP
	09/20/2022 03:44:20.000 pm	wmpnss_color120.png		A MEDIUM
	09/20/2022 03:44:20.000 pm	ipsar.xml		32
	09/20/2022 03:44:20.000 pm	ipsplk.xml		DEVICE.TYPE

Note: For each alert, only the latest 1000 events are displayed.

6. To view all the details associated with a specific event, click on an event. The **Event Details** panel is displayed with the summary and overview information associated with the event.

SEVERITY	High Alerts		Event Details	<u> </u>
1	> High Opswat Reports		1 Investigate Timeline P1 View Alert Details	Event Metadata
CRITICAL	High In Recycle Bin D			
2	🗸 🔫 🖓 🗸 🗸 Vara Rule Match		Sunnary	
3	EVENT TIME	SUMMARY		
HIGH	03/20/2022 03:44:20.000 pm	ker-ker.and	Overview	SESSIONID
2	09/20/2022 03:44:20.000 pm		FILENAME	36695
MEDIUM	0%/20/2022/03.44/20.000 pm	ipsptb.xml	lpsrus xml	08/30/2022/03-44-20-mm
6	09/23/2022 03:44:23.000 pm		DIRECTORY	
ALL	09/20/2022 03:44:20.000 pm	ipsjon.oml		418
	03/20/2022 03:44:20.000 pm	verisign.bep	SIGNED BY	B ⁰¹⁰
	09/20/2022 03:44:20.000 pm	ipshe.onl		endpoint/oghybrid1
	03/20/2022 03:44:20.000 pm	ipsfin.xml		8
	03/20/2022 03:44:20.000 pm	wmpnss_color120.peg		MEDIUM
	09/20/2022 03:44:20.000 pm			32 00000 000
	010000000000000000000000000000000000000	(anally and)		R

7. You can also view the Event Metadata such as IP, Filename, File hash, and Category in the **Event Details** panel.

Note: The **contexthub-server.contextlookup.read** permission is enabled only for Administrators, Analysts, Malware Analysts, SOC Managers and Respond Administrators. Administrators can enable this permission for other roles in the **Hosts** view to view context lookups for meta values and perform the Add/Remove from List actions. For more information, see the "Role Permissions" topic in the *System Security and User Management Guide*.

8. Click the drop-down option besides the metadata value to view additional information about the specific metadata. The **Context Highlights** dialog 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, and Feeds.



- 9. To investigate the original event and destination domain of the event, do any of the following:
 - To investigate the events in a specific time frame, click **Investigate Timeline** on the **Event Details** panel. For more information, see the *NetWitness Investigate User Guide*.
 - To investigate a particular process, click View Alert Details on the Event Details panel. For more information on process analysis, see Investigating a Process.

To analyze the hosts (which trigger Medium alerts) 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.

The Alerts tab is displayed.

4. In the Alerts > Severity panel, click the Medium alert severity.

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: For each alert, only the latest 1000 events are displayed.

6. To view all the details associated with a specific event, click on an event. The **Event Details** panel is displayed with the summary and overview information associated with the event.



- 7. You can also view the Event Metadata such as IP, Filename, File hash, and Category in the Event Details panel.
- 8. Click the drop-down option besides the metadata value to view additional information about the specific metadata. The **Context Highlights** dialog 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, and Feeds.



- 9. To investigate the original event and destination domain of the event, do any of the following:
 - To investigate the events in a specific time frame, click **Investigate Timeline** on the **Event Details** panel. For more information, see the *NetWitness Investigate User Guide*.
 - To investigate a particular process, click **Analyze Process Tree** on the **Event Details** panel. For more information on process analysis, see Investigating a Process.

ALERTS	PROCESSES AUTORUNS FIL	ES DRIVERS LIBRARIES ANOMALIES DOWN	NEOADS SYSTEM INFO HISTORY	
SEVERITY	Medium Alerts 🚯		Event Details	<u> </u>
1	Contraction Contraction Contraction	Account Policy (1 events)	.is Investigate Timeline S⊨ Analyze Process Tree	Event Metadata
CRITICAL	EVENT TIME	SUMMARY		
5	09/27/2022 01:52:52.000 am		Summary	
Л	> MEDIUM Floating Module (4	events)	cmd.exe created process net.exe	♥ Filter meta keys
	> MEDIUM In Root of Program	Directory (4 events)	Overview	SESSIONID
5	> MEDIUM Hidden In AppData	a (24 events)	TARGET FILENAME	छ। 50329
MEDIUM	> MEDIUM Tasks In Programda	ata Directory (8 events)	net.exe	
11 all			TARGET COMMAND LINE net.exe.ACCOUNTS TARGET DIRECTORY	09/27/2022 01:55:38 am size 41 B D D
			C:Wundowskystens2\ TARGET USER DESKTOP-R8L2BIA TARGET HASH Obd94s338eea3a4e1/2830ae326e6d19	endpointloghybrid1 rotwako IP rotwako IP MEDIUM 32

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.

ALERTS	PROCESSES AUTORUNS	FILES DRIVERS LIBRARIES ANOMALIES DOWNL	OADS SYSTEM INFO HISTORY YARA RULES	<u> </u>
SEVERITY	Critical Alerts			HOST DETAILS POLICY DETAILS
3	V CRITICAL Runs Blacklist	ed File (5 events)		
CRITICAL	EVENT TIME	SUMMARY	TARGET PARAM	
5	09/21/2022 03:00:32.000 pm	scp.exe created process ssh.exe	ssh.exe "-x" "-oForwardAgent=no" "-oPermitLocalCommand=no" "	☑ Show details with values only
НІБН	09/21/2022 03:00:21.000 pm	scp.exe created process ssh.exe	ssh.exe "-x" "-oForwardAgent=no" "-oPermitLocalCommand=no" "	Network Interfaces
_	09/21/2022 02:58:43.000 pm	scp.exe created process ssh.exe	ssh.exe "-x" "-oForwardAgent=no" "-oPermitLocalCommand=no" "	Name Intel(R) 82574L Gigabit Network Connecti
5	09/21/2022 02:58:34.000 pm	powershell.exe created process ssh.exe	ssh.exe \ma-log4cpp.log root@10.125.250.71:/root	IPv4
MEDIUM	09/21/2022 01:07:42.000 pm	explorer.exe created process ssh.exe	ssh.exe	IPv6
13	> CRITICAL Blacklisted Fil	e (5 events)		Gateway 10.118.128.1
ALL	> CRITICAL Opswat Repo	rted Infected (104 events)		DNS fec0:0:0:ffff::1,fec0:0:0:ffff::2,fec0:0:0:ffff::3
				Promiscous false
				Operating System
				Description Microsoft Windows 10 Enterprise
				Build Number 18362
				Kernel Name ntoskrnl.exe

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

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

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 Alerts 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, there are some unsigned file that might be malicious. If the search is executed on an Endpoint Broker server, it queries all the Endpoint servers.

C:\USERS

$\, arsigma \,$ all files available on host (100)

sftp_si.cpython-36.pyc Unsigned C:\Users\ecat\App Data\Local\Programs\Python\Python36\Lib\site-package s\paramiko_pycache_\ ffffca8b45a2874af02648b07 242cc4d7a83fea8ed45b8c65b64c43e2f31785d

pefile.cpython-36.pyc Unsigned C:\Users\ecat\Docu ments\sharemanu\Python36\Lib\site-packages_pycach e_\ 9628ba2dc73f6bdc20d089d21e0f3594000922cb 133420a2906630ea3b661d50

__init__.py Unsigned C:\Users\ecat\Documents\share manu\Python36\Lib\site-packages\PyInstaller\utils\hook s\ f2e623d83823fa691b74665a9eef91581e1c1d319f 13dda3d0a90449657eddbd

dqNextMinus.decTest Unsigned C:\Users\ecat\Docu ments\sharemanu\Python36\Lib\test\decimaltestdata \ ea952da312fbc0a138f7093f9d98bde6c2864fb833e b5a2c8dbd336854a535bf

inbox_client_10.cpython-36.pyc Unsigned C:\Users \ecat\Documents\ \Python36\Scripts_pycach e_\ 8d33b3589921194b9800c6faf911c39ebe3c86a4 2817b45d46a8d4d7e036f418

TAXII_XMLMessageBinding_Schema_11.xsdUnsignedC:\Users\ecat\AppData\Local\Programs\Python\Python36\Lib\site-packages\libtaxii\xsd\2cc298edada05bf1200c8218c7e039881a6fa7f74bcae3512a7805df7810ad94

_policybase.cpython-36.pyc Unsigned C:\Users\ecat \Documents\ Python36\Lib\site-packages\fut ure\backports\email_pycache_\ 1ce1999e0364a3da 62336eaa2bb3eea75acd7fbdce5747f9473f361374d624 7b

htest.py Unsigned C:\Users\ecat\Documents\sharem

This file is run as a Process.

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

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

Analyze Processes

To analyze the process:

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

NETWITNESS Platform Investigate	Respond Users Hosts Files	Dashboard	Reports			Ŏ	8	⑦ admin >
100 🗹 i Agen Idle	nt scan status agent last seen ag 10 minutes ago	GENT VERSION	NAPSHOT TIME 11/03/	/202105:24:1	9 pm 🗸			
ALERTS PROCESSES AUTORUNS FILES	DRIVERS LIBRARIES ANOMALIES	DOWNLOADS	SYSTEM INFO HI	STORY				Q
₽ Filters ×	Processes	💥 Change File Status	Analyze Events		lore Actions \vee			TREE VIEW
PROCESS NAME		LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILE PATH
Equals v e.g., Filename.dll	WmiPrvSE.exe	٥	٥			Neutral		C:\Windows\Syst
FILE STATUS	WmiPrvSE.exe	٥	٥			Neutral		C:\Windows\Syst
	vinlogon.exe	٥	٥			Neutral		C:\Windows\Syst
Graylist	winlogon.exe	٥	٥			Neutral		C:\Windows\Syst
Whitelist	wininit.exe	٥	٥			Neutral		C:\Windows\Syst
REPUTATION	WindowsInternal.ComposableShell.Experi.	. 0	٥			Neutral		C:\Windows\Syst
Malicious Suspicious		0	0			Neutral		C:\Program Files
	vmtoolsd.exe	•	•			Neutral		C:\Program Files\
□ Known Good		•	•			Neutral		C:\Windows\Syst
	vm3dservice.exe	0	0			Neutral		C:\Windows\Syst
Reset]		Showing 95 out of 95	processes 0	selected			

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

	Respond Users Hosts File	s Dashboard	Reports			Č	8	② admin >
100 🗗 agent Idle	t scan status agent last seen a 20 minutes ago	GENT VERSION	NAPSHOT TIME 11/03	/202105:24:1	9 pm 🗸			
ALERTS PROCESSES AUTORUNS FILES D	DRIVERS LIBRARIES ANOMALIES	DOWNLOADS	SYSTEM INFO H	ISTORY				۹
⊽ Filters ×	Processes C Analyze Process	💥 Change File Status	Analyze Events					
PROCESS NAME		LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	LAUNCH AR
Equals – e.g., Filename.dll	ntoskrnl.exe	٥	0			Neutral		
FILE STATUS	ntoskrnl.exe	0	0			Neutral		
Neutral	smss.exe	•	0			Neutral		
Blacklist Graylist		•	•			Neutral		
Whitelist	□ ∽ <u>winlogon.exe</u>	0	•			Neutral		
REPUTATION	dvm.exe		0	2		Neutral		
Malicious Suspicious			0			Noutral		/flags:0v0 /state(
Unknown			•			Noutral		/nags.ox0/statet
Known Known Good		•		2		Neutral		
Invalid			0	2		Neutral		
Reset			Showing 95 out of 9	5 processes 0	selected			

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

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

	orm Investigate Re	espond Users	Hosts F	iles Dashboar	d Reports			🖒 🗷 拨 🕐 admin >
100	AGENT SCA	in status agent 20 mi	LAST SEEN	AGENT VERSION		11/03/2021 05:2	•4:19 pm →	
ALERTS PROCESSES AUTO	RUNS FILES DRIV	ERS LIBRARIES	ANOMALII	S DOWNLOAD	S SYSTEM INI	O HISTORY		ename, path or hash Q
▼ Filters Processes	Analyze Process 🛛 🗶 Cl	hange File Status	🖓 Analyze Even	ts 🗸 🗄 More	Actions 🗸) TREE VIEW	OneDrive.exe ×
	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILE PATH	FILE DETAILS LOCAL RISK DETAILS HOSTS
MsMpEng.exe	70	70			Neutral		C:\Program Files	
explorer.exe	31	31			Neutral		C:\Windows\	Show details with values only
⊠ <u>OneDrive.exe</u>	31	31	3	-	Neutral	-	C:\Users\ecat\Ap	General
sychost.exe	31	31	2	-	Neutral	-	C:\Windows\Syst	FileName OneDrive.exe
sychost.exe	31	31			Neutral		C:\Windows\Syst	Entropy 4.283913667539894
Sychost.exe	31	31			Neutral		C:\Windows\Syst	Size 1.4MB
sychost.exe	(31)	31			Neutral		C:\Windows\Syst	Deleted false
sychost.exe	31	(31)			Neutral		C:\Windows\Syst	
sychost.exe	(31)	(31)			Neutral		C:\Windows\Syst	Hash
svchost.exe	(31)	(31)			Neutral		C:\Windows\Syst	MD5 9edb70213f7015a92e374a82725af2bf
		Chandra OF and a fo	F	-lt-d				SHA1 clb3401a77045db132d9681b89a17b33 SHA256 44bd2686cd0(31edf3da1616a955e1687

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

NETWITNESS Platform Investigate Respond Users Hosts Files Dashboard Reports	ġ	*	admin >
100 C ² : Acent scale status Acent Last steen Acent Version SNAPSHOT TIME 11/03/2021 05:24:19 pm →			
ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY			Q
< Process Details			
PROCESS NAME OWNER PPID PATH LAUNCH ARGUMENTS			
OneDrive.com ecat 6900 C:\Users\ecal\AgoData\Local\Microsoft;OneDrive\ Abadground			
> Loaded Libraries (30)			
> Image Hooks (0)			
> Suspicious Threads (0)			

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

For example,

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

Analyze Autoruns

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

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

Note: The Endpoint Broker queries the Hosts present across multiple Endpoint Servers for each Autorun and displays the total count of the hosts for the respective Autoruns in the **On Hosts** column in the **Hosts** > **Autoruns** Broker view.

For Example:

If an Autorun is running on 2 different hosts present across multiple Endpoint Servers, the **On Hosts** count of the Autorun is displayed as 2 in the **Hosts** > **Autoruns** Broker view.

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.

ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY YARA RULES										
abla Filters ×	File							C ALL FILES AVA	ILABLE ON HOST	
FILE NAME		FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	FILE STATUS	REPUTATION	DOWNLOADED	PATH 🛞	
Equals ~ e.g., Filename.dll			100	100		Neutral	Known	✓	C:\Users\ecat\Do	
FILE STATUS			100	100		Neutral	Known	✓	C:\Program Files\	
Neutral			100	100		Neutral	Unknown	✓	C:\Users\ecat\Ap	
□ Blacklist □ Graylist			100	100		Neutral	Known	✓	C:\Users\ecat\Do	
Whitelist			100	100		Neutral	Known	✓	C:\Python34\Lib\	
REPUTATION			100	100		Neutral	Known	✓	C:\Windows\Insta	
Malicious Suspicious			100	100		Neutral	Known	✓	C:\Users\ecat\Do	
Unknown			100	100		Neutral	Known	✓	C:\rama\Lib\test\	
Known Known Good			100	100		Neutral	Known	✓	C:\rama\Lib\test\	
Invalid			100	100		Neutral	Known	✓	C:\Users\ecat\Do	
SIGNATURE			100	100		Neutral	Known	✓	C:\Users\ecat\Do	
Unsigned Valid Signature			100	100		Neutral	Known	 ✓ 	C:\Python34\Lib\	
Reset										
				Showir	ng 3039 out of 3	3039 files 0 selecte	d			

• To view the files reported as part of scan snapshot, you must disable All Files Available On Host toggle and select the scan time from 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:

ALERTS PROCESSES AUTORUNS FILES D	ORIVERS	LIBRARIES ANOMA	ALIES DOWN	LOADS S	YSTEM INFO HISTO	RY YARA RU	LES		
₽ Filters ×	Files	ス Change File Status		ents 🗸	More Actions V	1		All Files Avai	LABLE ON HOST
FILE NAME	D FI	ILENAME LO	CAL RISK SCORE	GLOBAL RISI	Google Lookup	FILE STATUS	REPUTATION	DOWNLOADED	PATH Ö
Equals v e.g., Filename.dll	⊠ <u>d</u> a	d <u>MinMag.decTest</u>	100	100	VirusTotal Lookup	Neutral	Known	✓	C:\Users\ecat\Do
EII E STATUS	⊠ <u>lic</u>		100	100	Download File to Server	Neutral	Known	✓	C:\Program Files\
□ Neutral	⊠ <u>in</u>	ibox client <u>10.py</u>	100	10(Save a Local Copy	Neutral	Unknown	✓	C:\Users\ecat\Ap
□ Blacklist		aEncode.decTest	100	100	Analyze File	Neutral	Known	✓	C:\Users\ecat\Do
□ Graylist □ Whitelist		nΔdd decTest	100	100		Neutral	Known		C:\Pvthon34\Lih\
PEDIITATION		220550 mci		100		Neutral	Known	 J	C:\Windows\Inst
□ Malicious				100	1	Neutral	KIIOWII		C. (Willow) and D.
□ Suspicious		<u>ervice-2.json</u>	<u></u>			Neutral	Known	•	C:\Users\ecat\Do
Unknown		<u>dXor.decTest</u>	100	100		Neutral	Known	✓	C:\rama\Lib\test\
□ Known □ Known Good		dClass.decTest	100	100		Neutral	Known	✓	C:\rama\Lib\test\
🛛 Invalid	Ω <u>α</u>		100	100		Neutral	Known	√	C:\Users\ecat\Do
SIGNATURE		dClass.decTest	100	100		Neutral	Known	✓	C:\Users\ecat\Do
Unsigned		dXor.decTest	100	100		Neutral	Known	✓	C:\Python34\Lib\
U Valid Signature									
Reset					Showing 3039 out of 303	39 files 3 selected			

- 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:

NETWITNESS Platform Investigate	Respond Users Hosts	s Files Dashboard Reports		ð 2 % () admin >
∇ Filters ×	🖯 EPS1 - Endpoi 🗸	CrAnatyze Events ∨ ⊖ Scan ∨ © Tags ∨	More Actions V		Ê
SAVED FILTERS	- HOSTNAME	RISK SCORE 🤟 AGENT SCAN STATUS	Delete	SION TAGS	AGENT GR 🛞
Select ~	windows	🚥 Idle	Reset Risk Score	64BitWin_	LegacyValidatic
HOST STATUS	windows	1dle	Download MFT to Server		
Managed	⊠ <u>win10-1903-x86</u>	Analyze Events	Download System Dump to Server	test	-
Roaming	win10-1903-x86	Delete	Download Files to Server		-
Standalone		Start Scan	Upgrade Selected Agent		-
N// CODF	DESKTOP-OJRGDOB		16 days aso 11 7 10 @		_
RISK SCORE		Assign Tags	9 daw sen		_
•		Unassign Tags	24 days ago 11.7.10 @		
0		Download MFT to Server	24 cays ago CS 11.7.1.0 @		-
HOSTNAME	WIN-EMONAJ9783N	Download System Dump to Server	23 days ago 11.7.1.0 🕑		isolatéd_agents
Equals ~ Enter Value	DESKTOP-K1B9UQH	Download Files to Server	a month ago 11.7.1.0 🕥		
		Reset Risk Score			
AGENT GROUPS			24 days ago 💪 11.7.1.0 🛞		
		Upgrade Selected Agent			
Reset Save Save as	DESKTOP-VN5G4IH	Uninstall Selected Agent	2 months ago 44.7.4.0 @		
		Showing 38 out of	f 38 hosts 1 selected		

- 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.

NETWITNESS Platform Invest		Respond Users Ho	sts Files Dashboard					*	
♥ Filters		😫 EPS1 - Endpoi 🗡	Analyze Events V	⊖ Scan ∨ Ŝags ∨	t More Actions ∨				Ê 🖺
SAVED FILTERS		HOSTNAME	RISK SCORE 🔶	AGENT SCAN STATUS	AGENT LAST SEEN	AGENT VERSION	TAGS		AGENT GR 🛞
Select	~		100	Idle	a month ago	11.7.1.0 💿	64BitWin		LegacyValidatio
HOST STATUS			100						-
Managed			100	Idle	a few seconds ago	11.7.1.0 💿	test		-
Roaming Isolated			100	Idle	2 months ago	11.7.0.0 💿			_
Standalone			98	Idle	14 days ago	11.7.1.0 💿			-
RISK SCORE			98	Idle	16 days ago	11.7.1.0 💿			
[100		98	Idle	9 days ago	11.7.1.0 💿			
• • • • • • • • • •			78	Idle	24 days ago යි	11.7.1.0 💿			
0			DLATED 70	Scanning	23 days ago	11.7.1.0 💿			isolated_agents
HOSTNAME			33	Idle	a month ago	11.7.1.0 💿			
Equals ~ Enter Value			(33)			11.7.1.0 🛞			
AGENT GROUPS			31		24 days ago 🗟	11.7.1.0 🛞			
			31			11.7.1.0 🛞			
		DESKTOP-VN5G4JH	31	Idle	2 months ago				
Reset Save Save as				Showing 38 out of 3	38 hosts 1 selected				

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.

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

HOST DETAILS PO	DLICY DETAILS X								
Type to filter list									
Show details with values only									
Users									
Name	WIN-Q83MT84GBN5								
Session ID	1								
Groups	Administrators, Users								

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 the selected 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:

*	NETWITN	NESS Platform	Investigate	Respond	Users	Hosts Files	s Dashboard Reports
7	Filters en	ndpointbrok 🗸 📗	🖸 Analyze Eve	ents 🗸	\odot Scan \checkmark	🔊 Tags 🗸	: More Actions \checkmark
	HOSTNAME		RISK SCORE \downarrow	OS - DESCRI	PTION	AGENT GROUPS	LAST SCAN TIME
Ø			100	_Microsoft W	indows 10 Ent		09/08/2022 04:37:08 am
		Analyze Eve	ents		rise Linux- 7.2		08/30/2022 11:02:20 am
		Delete Start Scan			lows 10 Ent		10/04/2022 08:04:59 am
		Stop Scan			lows 10 Ent		10/03/2022 05:59:18 am
		Network Iso	Network Isolation				
		Assign Tags					
		Unassign Ta	ags				
		Download N	IFT to Server				
		Download S	system Dump to S	Server			
	Download Files to Server						
	Reset Risk Score For Selected Host						
		Uninstall Se	lected Agent				

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

All the alerts associated with the score are deleted.

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

To reset the risk score of all the available hosts simultaneously:

- 1. Go to Hosts.
- 2. Click More Actions > Reset Risk Score For All Hosts in the toolbar.



All the alerts associated with the score are deleted.

Standalone Scan on Air-gapped Windows and Linux Hosts

The Standalone scan feature allows administrators to run scans on the air-gapped Windows and Linux hosts that are disconnected from the network. Administrators can download the scan command once from UI and execute it on multiple hosts. For the best utilization of resources, NetWitness recommends running standalone scan every two weeks. Policies do not apply on air-gapped hosts, and features such as downloading MFT to the server, upgrading agents through UI, downloading a file to the server are not available for standalone agents.

The scan process involves two files:

- Offline Scan Configuration Contains the configuration information needed to run the scan.
- Scan Results File This contains the results of the Scan, which you can upload using the Scan > Upload Offline Scan File option on the Hosts view. This file will be imported and processed by NetWitness.

Standalone scan workflow:



Note: Both Download Offline Scan Configuration and Upload Offline Scan File options are available only on the Endpoint server view. These options can't be accessed from Broker view.

Generate the scan configuration file

1. Click Scan > Download Offline Scan Configuration on the Hosts screen.

	Invest	tigate	Respond	Users	Hosts	F	iles	Das	hboard	Reports				ġ
▽ Filters		€End	¦ Ipoint-Serv∨				⊖Sc Dow	an ∨	🔊 Tags 🗸		Actions ~			ê !
SAVED FILTERS		П ноя	STNAME	RI	SK SCORE	v A	Uplo	ad Offlin	ne Scan File	oninguration	POLICY STATUS	AGENT GROUPS	AGENT SCAN STATUS	TAGS 🛞
Select	~	DES	SKTOP-LE7L8HU		100		9 days ag	şo			Pending	GauravGroup,standalone5	ldle	
HOST STATUS					100		days ago		15/09/2	2021 09:41:25 am	Updated	Monitor System	Idle	SysMon

On the Download Offline Scan Configuration pop-up,

- 2. (Optional) Select CPU Maximum.
- 3. Enter a Password. (not more than 31 characters long)
- 4. Click Download.

Download Offline Scan Configuration ×							
Download the scan configuration to perform a scan of all executable files available in the memory. The total time to complete the scan depends on CPU Maximum.							
> CPU Maximum (Default usage 25%)							
PASSWORD	1						
	_						
	Cancel Download						

5. Transfer the Offline Scan Configuration file to the air-gapped host.

Install Endpoint Agent and Register for Standalone Scan

- 1. Install the Endpoint Agent on the air-gapped host. Refer to *Endpoint Agent Installation Guide* for more information.
- 2. Register the agent for standalone scan (required only when an agent is installed).
 - If you are using a Windows machine, open command prompt in administrator mode and execute the following command:

ServiceName.exe /standalone

Example: NWEAgent.exe /standalone

• If you are using a Linux machine, open the terminal as a root user and execute the following

command:

/opt/rsa/nwe-agent/bin/nwe-agent /standalone

Start a Standalone scan on Windows

1. Open the command prompt in Administrator mode, on the air-gapped host.

2. Execute the scan using the following command (syntax):

ServiceName.exe /scan /password "<password>" /scanfile "<filepath>"

```
Example: NWEAgent.exe /scan /password "Abc123$" /scanfile
"C:\Users\johndoe\Downloads\2021-12-06-Full Scan Configuration.scanfile"
```

- <password> is the password entered while generating the Offline Scan Configuration File.
- <filepath> is name of the scan configuration file with full path.
- 3. Wait until the scan is completed.
- 4. Transfer the scan result file (password protected .zip file) to upload to the UI.

Start a Standalone scan on Linux

- 1. Open the terminal as a root user, on the air-gapped host.
- 2. Execute the scan using the following command (syntax):

/opt/rsa/nwe-agent/bin/nwe-agent /scanfile "<file path>" /password "<pwd>"

Example: /opt/rsa/nwe-agent/bin/nwe-agent /scanfile "/home/ubuntu/Desktop/2024-02-04-Full Scan Configuration.scanfile" /password "abc@123"

- 3. Wait until the scan is completed.
- 4. Transfer the scan result file (password protected .zip file) to upload to the UI.

Upload the Standalone scan result file

1. Click Scan > Upload Offline Scan File on the Hosts screen.

Upload Offline Scan File	×
Select file to upload	
FILE* WIN-6DOQ1D01L03-1d79056756e9e51.zip	
PASSWORD*	
	Cancel Upload

- 2. Click and upload the scan result file.
- 3. Enter the same password that was entered while downloading the offline scan configuration file.
- 4. The Endpoint server will process the scan result file once successfully uploaded.

X NETWITNESS Platform	Investigate	Respond		×	Ŏ	8	*	0	admin >
▽ Filters		EPS1 - Endpoi	Successfully uploaded the scan file.	Tags ~ Hore Actions ~					ê !
							-	0	

Note: Standalone agents can only be upgraded manually using the Endpoint agent packager. Refer to *Generate an Endpoint Agent Packager* on *Endpoint Agent Installation Guide* for more information.

Investigating a Process

Note: The information in this topic applies to NetWitness 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

Based on the Alert severity, you can analyze the processes using two different options:

- View Alert Details: This option allows you to analyze the processes associated with Critical and High Alerts.
- Analyze Process Tree: This option allows you to analyze the processes associated with Medium Alerts.

To analyze the process associated with Critical and High Alerts:

- 1. Go to Hosts and click on a host.
- 2. Click on an event associated with the **Critical** or **High** alert on the Host Details view. The **Event Details** panel appears.

3. Click **View Alert Details** to analyze the process activities of a file associated with the **Critical** or **High** Alerts.



The Process Tree Viewer is displayed in the Respond service.

- 4. Select the process in the **Process Tree Viewer** and click **File Actions** in the **Details** panel to perform the following actions:
 - Google Lookup
 - VirusTotal Lookup
 - Change File Status
 - Download File to Server
 - Analyze File
 - Save a Local Copy

• Reset Risk Score

NETWITNESS Platform Investigate	Respond Users Hosts	Files Dashboard Repo	rts	0 Z	🗶 🕐 admin >
< 🔊 Unexpected Isass.exe Parent					
INCIDENT ID CREATED HOSTNAME INC-149 09/21/2022 03:56:34 pm	TACTIC TECHNIQUE defense-evasion masqueradii				
EVENT TIME SUMMARY	TARGET PARAM	SOURCE PARAM	USER SOURCE	Details	
09/21/2022 03:53:46.000 pm cmd.exe created process lsass.exe			WINDOW5\ecat		
Process Tree Viewer				1 Investigate Timeline	File Actions 🗸
				Summary	< Google Lookup
ntoskrnl.exe				cmd.exe created process 1s	 VirusTotal Lookup Change File Status
smss.exe				> Event Details	Download File to Server
				✓ Process Details	Analyze File
• smss.exe				Filename	Save a Local Conv
				Isass.exe Command Line	Reset Risk Score
	guitexe				
				File Status Neutral	
	→ 100 explorer.exe			Reputation Status Known Good	
				Signed By Microsoft Windows Publisher	
) cmd.exe		Directory	
				C:\Windows\System32\ User	

To analyze the process associated with Medium Alerts:

- 1. Go to Hosts and click on a host.
- 2. Click on an event associated with the **Medium** alert on the Host Details view. The **Event Details** panel appears.
- 3. To analyze the process activities of a file associated with the **Medium** Alerts, do one of the following:
 - In the Event Details panel, click Analyze Process Tree.
 - 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 cmd.exe has created process net.exe.

ALERIS	PROCESSES AUTORONS FIL	LES DRIVERS LIBRARIES ANOMALIES DOWI	NLUADS SYSTEM INFO HISTORY		
SEVERITY	Medium Alerts 🚯		Event Details		🗖 🖉 🗡
1	✓ MEDIUM Enumerates Local.		Analyza Descare Tran	Event Metadata	
CRITICAL	EVENT TIME	SUMMARY	g Analyze Process nee		
5			Summary		
НІСН	> MEDIUM Floating Module (4	events)	cmd.exe created process net.exe		
	> MEDIUM In Root of Program	Directory (4 events)	Overview		
5	> MEDIUM Hidden In AppData		TARGET FILENAME	 50329	
MEDIUM	> MEDIUM Tasks In Programd	ata Directory (8 events)	net.exe	TIME 00/07/2022 01/55/28	
11 All			TARGET COMMAND LINE net.exe ACCOUNTS	SIZE 41B	
			TARGET DIRECTORY C:\Windows\system32\	endpointloghybrid1	
			TARGET USER DESKTOP-R8L2BIL\	FORWARD.IP	
			TARGET HASH Obd94a338eea5a4e1f2830ae326e6d19	меріим 32	

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 1, file \blacksquare , or registry 1) 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 \vee 1	11/25/2019 05:26am - 12/02/2019 05:2	ó₂m ∨ Analyze			⊞ Events List (96)	🗄 Hosts (1) 🛛 🗘 Risk Deteils (13) 🕐
	_ ([®] ∲ ∉ □ powershell.ese				
	_ (© ∯ eventoreste.cse				
	- © 	© ¢ eventoreste se				
		® & ond.exe				
PROCESS EXECUTION DETAILS		FILE.GENERAL				
EVENT TIME 11/27/2019 02:34:00.000 pm	USER NAME NT AUTHORITY\SYSTEM	FILENAME cmd.exe	TIMESTAMP 11/20/1975 08:18:58.000 pm	FEATURES file.exe.file.arch64,file.iconPresent,file.versionI	IMPORTED LIBRARIES msvcrt.dll,ntdll.dll,api-ms-win-core-kernel32-le	MD5 Od088f5bcfa8f086fba163647cd80cab
PROCESS NAME cmd.exe	LAUNCH ARGUMENTS cmd.exe c:\Suspicious.bat c:\Suspicious.ps1	ENTROPY 6.172248861723813	IMAGE SIZE 404.0 KB	FILENAME Cmd.Exe	SECTION NAMES .text,rdata,data,pdata,didat,rsrc,reloc	SHA1 08cc2e8dca652bdda1acca9c446560d4bc1b
FILE LOCATION c:\windows\system32\		SIZE 272.0 KB	EXPORTED FUNCTIONS	COMPANY Microsoft Corporation		SHA256 9023f8aaeda4a1da45ac477a81b5bbe4128e
CHECKSUM 9023f8aaeda4a1da45ac477a81b5bbe4128e4		FORMAT pe	EXPORTED NAMES	DESCRIPTION Windows Command Processor		
SESSION ID 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.

)	cmd.exe		
All (70) 👲 Network (12)	🗆 File(6)	🖽 Registry (0)	
PROCESS NAME	RISK SCORE 🕁	LAUNCH ARGUMENTS	EVENT TYPES
🗹 cmd.exe	70	cmd.exe /c certutil.exe -urlcache -split -f https://raw	\$D#
Conhost.exe		conhost.eve 0xffffffff-ForceV1	
🗹 cmd.exe		cmd.exe /c dir /b /a-d \test-sets\"collection"\tbat	
PING.EXE		ping -n 5 127.0.0.1	
🗹 7z.exe		7z.exe e -bb0 -paptsimulator "c:\mimikatz\\enc-files	
🗹 7z.exe	۲	7z.exe e -bb0 -paptsimulator "c:\mimikatz\\enc-files	
🗹 cmd.exe	۲	cmd.exe /c dir /b /a-d \test-sets\"command-and-con	
	Showing 70	Dout of 70 70 selected	
70 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 To analyze the process associated with Medium Alerts:.
- 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).

Analyze				Events Events	List (96) 묘 Hosts (1) 🗘 Risk Details (13)
∀Filters ×	EVENT TIME	CATEGORY	ACTION	SOURCE FILE NAME	SOURCE PARAMETER	SOURCE DIRECTORY	sou 🔅
_	11/25/2019 06:5	Process Event	openPr	explorer.exe		C:\Windows\	
Category	11/25/2019 03:0	Process Event	openPr	explorer.exe		C:\Windows\	
Process Event	11/25/2019 11:1	Process Event	openPr	explorer.exe		C:\Windows\	
(File Event)	11/26/2019 07:1	Process Event	openPr	explorer.exe		C:\Windows\	
Network Event	11/27/2019 02:3	Process Event	openPr	explorer.exe		C:\Windows\	
Console Event	11/27/2019 10:3	Process Event	openPr	explorer.exe		C:\Windows\	
	11/28/2019 06:4	Process Event	openPr	explorer.exe		C:\Windows\	
Action	11/28/2019 02:5	Process Event	openPr	explorer.exe		C:\Windows\	
openProcess	11/28/2019 10:5	Process Event	openPr	explorer.exe		C:\Windows\	
openBrowserProcess	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\	
(createRemoteThread)	11/29/2019 09:3	Process Event	openPr	Isass.exe		C:\Windows\System32\	
Reset				Showing 19 out o	of 19		

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.

Note: At any given time, if the number of process events created from a single source VPID in Linux exceeds the count of **100**, only the first **100** events are displayed in the Process Visualization > Events view for a time interval of **8** hours. Only after the time interval of **8** hours, the new set of events created from the same source VPID (maximum **100** process events) will be displayed along with the existing set of events.

For Example: At **12PM** IST, if **1000** process events are created from a single source VPID, only the first **100** events are displayed in the Process Visualization > Events view until **8PM** IST. After **8PM** IST on the same day, the new set of **100** events created after **8PM** IST from the same source VPID will be displayed along with the existing set of events.

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:

	ate Respond Users Hosts	Files Dashboard Reports	Ŏ	🗃 % 🕜 admin >
∇ Filters ×	EPS1 - Endpoi View Certificates	6 X Change File Status Z Analyze Events V More Actions V		
SAVED FILTERS	FILE NAME	RISK SCORE ψ FIRST SEEN TIME ON HOSTS REPUTATION	SIZE SIGNATURE	PE.RESOURCES.C FILE STATUS
Select	🗆 <u>gedit.dll</u>	09/15/2021 05:58:3 3	536.0 KB microsoft,signed,valid,ca	Microsoft Corpor Blacklisted
FILE NAME	Change File Status	99 10/29/2021 02:52:1 4	843.5 KB unsigned	Neutral
Equats v e.g., Filename.dll	MEMORY D Analyze Events	> 09/27/2021 11:39:1 1	0 bytes unsigned	Neutral
FILE STATUS	OneDriveSet Google Lookup	> 70 11/08/2021 10:32:4 1	45.8 MB microsoft,signed,valid	Microsoft Corpor Neutral
Neutral	WinSAT.exe VirusTotal Lookup	> 11/05/2021 05:54:1 1	3.6 MB microsoft,signed,valid,ca	Microsoft Corpor Neutral
Blacklist Gravlist	View Certificates	70 11/02/2021 03:48:2 1	446.8 KB signed,valid	Neutral
D Whitelist	ARMDCHam Download File to Server	70 11/02/202101:59:4 0	445.7 KB signed, invalid	Neutral
REMEDIATION	Save a Local Copy	70 10/29/2021 05:44:0 2	361.5 KB microsoft,signed,valid,ca	Microsoft Corpor Neutral
Blocked	WinSAT.exe Analyze File	70 10/29/2021 01:31:0 1	3.2 MB microsoft,signed,valid,ca	Microsoft Corpor Neutral
REPUTATION	Scan with OPSWAT	(70) 10/25/2021 09:48:0 1	446.8 KB signed,valid	Neutral
Malicious Suspicious	Reset Risk Score	70 10/25/2021 09:48:0 1	9.7 MB signed,valid	Neutral
Unknown		70 09/23/202107:28:3 1	8.6 MB unsigned	RSA Neutral
C Known Good		70 09/23/2021 07-28-3 1	8.6 MB unsigned	RSA Neutral
Invalid		70 09/92/2021 07:29:2 1	9.4 MD unclaned	PSA Neutral
RISK SCORE			o.o mis unsigned	NSA Neutrai
100	SRC6HQ4E.exe	09/23/20210/:28:3 1	8.6 MB unsigned	RSA Neutral
<u></u>		(70) 09/23/2021 07:28:3 1	115.0 KB signed,valid	RSA Neutral
0		70 09/23/2021 07:28:3 1	8.6 MB unsigned	RSA Neutral
Reset Save Save as		Showing 100 out of 26043 files 1 selected	<u> </u>	

- 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		
I Blacklist		
CATEGORY		
Select ~		
Applies to Windows hosts running in advanced mode where blocking is enal terminates all processes associated with the selected file hashes.	oled and	ł
Note: Blocking is supported only for the following file types: .exe, .com, .sys, .dll, .scr, .ocx, .bat, .ps1, .vbs, .vbe, .vb, .wsh, .wsf, .cmd		
▲ Files signed by RSA and Microsoft cannot be blocked. □ Block		
O Gravlist		
O Whitelist		
O Neutral		
COMMENTS .		
Enter comments		
Cancel	Save	2

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 that are running in advanced mode. All PE files along with the following file extensions can be blocked. *.exe*, .com, .sys, .dll, .scr, .ocx, .bat, .ps1, .vbs, .vbe, .vb, .wsh, .wsf, .cmd
You cannot block the following:.
Memory DLL and floating code
Files that are signed by Microsoft or RSA.
To delete a blocked file, users can log in to the host and execute the delete command using the elevated command prompt.

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).

Import File Hashes using the Block Hash tool

The Block Hash tool allows you to import a set of file hashes which can be set to block state and change the file bias status (whitelist, blacklist, and graylist). The tool allows you to block the imported file hashes (suspicious, invalid, and malicious) and prevent them from opening or executing on the hosts. You can block up to a maximum of **50,000** file hashes using this tool.

Note: For more information on changing the file status or blocking the file, see <u>Changing File Status</u> or Remediate.

IMPORTANT:

- Enter only valid SHA256 hashes; otherwise, the blocking functionality might break.

- Do not block any file hashes signed by RSA, Microsoft, and Apple. It might make your Endpoints unresponsive.

- Make sure the number of hashes entered in the JSON file is less than the number of the available limit of hashes that can be blocked (the maximum limit is **50,000**).

For example: If 100 file hashes are already blocked as part of NetWitness deployment, you can only block 49,900 more file hashes using this tool.

JSON File Format

The example below describes the JSON file format for blocking and blacklisting the file hashes.

Sample demoblock.JSON:

```
[{
   "checksums":
   ["lb30e463ebe0131db66fce7d4aa43f3e149064d85c4c0dc5218b077886da2804","67fa30e4
   63ebe0131db66fce7d4aa43f3e149064d85c4c0dc5218b077dsbhb561","78vbba909e463ebe0
   131dsdsdb66fce7d4aa43f3e1dsdsd49064d85dsdsman61n"],
   "fileStatus": "Blacklist",
   "comment": "File blocking set through new tool",
   "remediationAction": "Block"
}]
```

The example below describes the JSON file format only for blacklisting the file hashes.

Sample demoblock.JSON:

```
[{
  "checksums":
  ["2b30e463ebe0131db66fce7d4aa43f3e149064d85c4c0dc5218b077886da2800","97fa30e4
63ebe0131db66fce7d4aa43f3e149064d85c4c0dc5218b077dsbhb500","38vbba909e463ebe0
131dsdsdb66fce7d4aa43f3e1dsdsd49064d85dsdsman68c"],
  "fileStatus": "Blacklist",
  "comment": "File status change set through new tool",
}]
```

To block the file hashes using the Block Hash tool:

- 1. SSH to node 0 and copy the JSON file (containing the file hashes to be blocked) stored in it.
- 2. Run the tool.

```
nw-block-hashes-tool <absolute path of json residing on node 0> <ESA node
IP/hostname>
```

Note: Enter the JSON file path in <absolute path of json residing on node 0> and enter the ESA node IP in <ESA node IP/hostname>. For Example: nw-block-hashes-tool /root/demoblock.json 10.125.250.118.



- 3. Enter the Admin Server password.
- 4. Follow the instructions displayed on the screen. Enter any one of the following options when prompted.

- yes: Enter yes to proceed with the execution of the script.
- no: Enter no to stop the execution of the script.

Note: At this stage, the tool validates the number of incoming file hashes through the JSON file and the number of existing file hashes already blocked in the deployment. If the total of the file hashes (incoming through JSON file and existing as blocked in the deployment) exceeds the maximum limit of **50,000**, the tool stops the execution, and it will not proceed further.

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, NetWitness 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.warning-percent and rsa.endpoint.file-download-disk-thresholds.fatal-percent parameters respectively.

For the downloaded file, you can:

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

Download Files to Server

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

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

Automatic File Download

By default, the files that are unsigned and size lesser than or equal to 1 MB are downloaded automatically to the NetWitness Endpoint server. And, only single copy of each file is downloaded

automatically. You can limit the volume of files to be downloaded in the **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 *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:

XNETWITNESS Platform Investigate	Respond Users	Hosts Files Dashboard F	Reports			ġ	8	🖌 🕜 admin >
100 🗗 : AGENT SCAN STATUS Scanning	AGENT LAST SEEN AGI	INT VERSION SNAPSHOT TIME	1/15/2021 03:46:07 pr	n ~				
ALERTS PROCESSES AUTORUNS FILES D	RIVERS LIBRARIES	ANOMALIES DOWNLOADS	SYSTEM INFO HI	STORY				٩
∇ Filters ×	Processes 📝 Ana	yze Process X Change File Status	Analyze Events	~	More Actions ∨			
PROCESS NAME		↑ LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HC	Google Lookup VirusTotal Lookup		DOWNLOAD	ed File Path
Equals v e.g., Filename.dll	ର୍ <u>ମ୍ cmd.exe</u>	Analyze Process			Download Process Dump to Se	al		C:\Windows\Sys
FILE STATUS	cmd.exe	Change File Status	100		Download File to Server	al		C:\Windows\Sys
	cmd.exe	Analyze Events	> 100			əl		C:\Windows\Sys
	explorer.exe	Google Lookup	> 100		Save a Local Copy Analyze File	al	~	C:\Windows\
U whiteist	C explorer.exe	VirusTotal Lookup	> 100		Known Good	Neutral	~	C:\Windows\
	<u>ManagementAgentHos</u>	Download Process Dump to Server	100		Known	Neutral	~	C:\Program Files
Suspicious	Microsoft.Photos.exe	Download File to Server	100	2	Known	Neutral	~	C:\Program Files
Unknown	Microsoft.Photos.exe	Save a Local Copy	100		Known	Neutral	~	C:\Program Files
Known Good	powershell.exe		100		Known Good	Blacklisted		C:\Windows\Sys
	D powershell.exe		100		Known Good	Blacklisted		C:\Windows\Sys
SIGNATURE					K C4	D1		CNIE-110
					Known Good	biackristed		C.\Windows\Sys
Reset		100		1	Known Good	Riachlicted		C-\Windowe\Sve
			Showing 205 out of 20	5 proce	esses 1 selected			

- 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:
| NETWITNESS Platform Investigate | Respond | Users Hosts Files | Dashb | oard Repor | ts | | | <u>ة</u> 0 | 3 % (| ?) admin > |
|-----------------------------------|--------------------|--------------------------|----------|------------|------------------------|-----------|-------------------------|-----------------|-------------|------------|
| ♥ Filters × | endpoint | rok 🗸 🛛 🖓 Analyze Ever | | | © Tags ∨ ‡ More | Actions \ | ~ | | | |
| SAVED FILTERS | FILE NAME | RISK SCORE 🔶 FIRST SEE | N TIME | ON HOSTS | REPUTATION | SIZE | SIGNATURE | PE.RESOURCES | FILE STATUS | R (\$ |
| Select ~ | svck.so | 0 06/12/202 | 0 11:16: | | Known | 117.1 | unsigned | | Neutral | - |
| FILE NAME | ⊠ <u>vsock.svs</u> | | 0 11:32: | | Known | 89.6 KB | signed,valid | VMware, Inc. | Neutral | |
| Equals v e.g., Filename.dll | libstdc++.sc | Change File Status | 11:16: | | Known | 908.4 | unsigned | | Neutral | |
| FILE STATUS | libsoftokn3 | Google Lookup | 11:16: | | Known | 256.0 | unsigned | | Neutral | |
| Neutral | 🗆 <u>sic.dli</u> | VirusTotal Lookup | 11:32: | | Known Good | 137.5 | microsoft,signed,valid, | Microsoft Corpo | Neutral | |
| Blacklist Graylist | usermgrcli.c | View Certificates | 11:32: | | Known Good | 74.1 KB | microsoft,signed,valid | Microsoft Corpo | Neutral | |
| Whitelist | | Download File to Server | 07:57: | | Known Good | 35.3 KB | microsoft,signed,valid | Microsoft Corpo | Neutral | |
| | | Save a Local Copy | 11:16: | | Known | 14.1 KB | unsigned | | Neutral | |
| L Blocked | | | 11:16: | | Known | 2.6 KB | unsigned | | Neutral | |
| REPUTATION
Malicious | | 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.

XNETWITNESS Platform Investigate Respo	nd Users Hosts File	s Dashboard	I Reports	Ö 🛃 拨 🕜 admin >
100 Z ² : AGENT SCAN STATUS AGENT Scanning 8 days	LAST SEEN AGENT VERSION	SNAPSHOT TIN	11/15/2021 03:46:07 pm	
ALERTS PROCESSES AUTORUNS FILES DRIVERS	ELIBRARIES ANOMALIES	DOWNLOAD	S SYSTEM INFO HIS	STORY Search by filename, path or hash Q
Files File Analysis - Strings View		er strings Ent	er Value	VgAuthIntegrationSubsys.dll $ imes$
STRING	OFFSET	UNICODE	LENGTH	DETAILS
@@@Z	0x00014A15			Type to filter list
?Oexception@std@@QEAA@AEBQEBD@Z	0x00015110		32	Show details with values only
H9zu	0x000010A8			File Details
allocator@D@2@@std@@QEAA@H@Z	0x00014FDD		28	Format pe
getSignedSamlToken	0x0000CF80		18	checksumMd5 2f3da6196682a24b2aa72e1b2f78f511
H;S0s	0x00000800			checksumSha1 dbb95ab38635d35bc488ae890fbb87d5ed14303c
Before beginning impersonation	0x0000D190		30	Size 95.5 KB
KPEBD11@Z	0x00012D92			Downloaded FileName 748248cf4ecd6f72c36105fe2b977b1b12ddfc268ccc4c695
TCafSmartPtr@UIVariant@Caf@@U12@@@V?	0x000130BB		36	Downloaded Path /var/netwitness/endpoint-server/files/7d824
num properties - %d	0x0000C758		19	
D8PhuZH	0x00001300			Architecture AMD64/x64
allantaraDa?aartidaaDEAAaV7 Showi	ng 517 of 517 strings			Characteristics Executable Large Address Aware DLL

- 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 🗹 🗄	AGENT SCAN STATUS AGENT LAST SEEN Idle a month ago	AGENT VERSION			·
ALERTS PROCESSES AU	TORUNS FILES DRIVERS LIBRARIE	S ANOMALIES DOWNLO	ADS SYSTEM INFO HISTORY	EXEC	
< Files File Analysis - Strin	ngs View Filter strings			Exec	exe
STRING	OFFSET	UNICODE	LENGTH	DETAILS	
*-m3 msupdater.com	0x00000A07			Type to filter list	
*-m3 twitterdocs.com	0x00000A96	 Image: A set of the set of the		Show details with values only	
*-m3 freenow.chickenkiller.com	0x00000828			File Details Format pe checksumMd5 (15(27)	1c8d94437h751917d87ddc8d91
				checksumSha1 60ec5cz	33072dff849a1d9eac946c20834a4
ᆋᅜ				chedisumSha256 b266aft	0334f3dec596dac6501f70994c8f942
				Size 6.0 KB	
				Downloaded FileName b266aft	334f3dec596dac6501f70994c8f942
C2 info visible				Downloaded Path /var/net	witness/endpoint-server/files/b266a
In File Content				Image Details	
				Architecture 1386/x8	6
				Characteristics Executa	ble.Large Address Aware
				Compile Time 01/14/2	019 10:20:25.000 am
				Entry Point 0x0000	2C4A
				Imported DLLs > Impo	
				Section Names > Section	
				Subsystem Window	rs Console
				Packing Detection	
		Showing 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 E i Agent scan status Idle	AGENT LAST SEEN AGEN a month ago	TVERSION SNAPS		~		O ×
ALERTS PROCESSES AUTORUNS FILES DRI	VERS LIBRARIES AND	MALIES DOWNLO	DADS SYSTEM IN	FO HISTORY	KEYLC	G Q
Files File Analysis - Strings View FILTER STRINGS						KeyLogger.exe
STRING	OFFSET	UNICODE	LENGTH			DETAILS
[Del]	0x00055070	-	5			Type to filter list
[Esc]	0x00055128		5			Show details with values only
[Right]	0x00055068		7			File Details
SVJAJJZ	0x0004612F	-	7			Format pe
292[2b2m2t2	0x00061B1D					checksumMd5 5242de7eee306123c50c1d0dcad83062
[Up]	0x00055050		4			checksumSha1 dacc40cf0edb8d55cdce6615e506209c8f18
delete[]	0x00056100		9	\sim	Indicators of	checksumSha256 c9eb0aa40eaa22685a6aceaa24136e98472
7K80858W818	0x00062368					3/20 401.0 KB
[aOni*	0x0005C2F4				keystroke logging	Downloaded Path Avar/netwitness/endpoint-server/files/c9eb0
7C7K757[7n9?	0x00062D15					
[PageDown]	0x0005511C	-	10			Image Details
newf	0x000560F8		6			Characteristics Executable 32-bit
frhankli	0-00056510		•			Compile Time 02/22/2019 11:46:23.000 am
	0.00050010					Entry Point 0x000275FF
01,1[181	0800061809					Imported DLLs > Imported DLLs (1) And Functions (83)
55515	0x00052489					Section Names > Section Names (8)
['93	0x0005C5CB		4			Subsystem Windows Console
[Num Lock]	0x00055218					
[End]	0x00055060	-	5			Packing Detection
	c h-					Entry Point Valid true

Performing Host Forensics

Note: The information in this topic applies to NetWitness 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, NetWitness 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 one or more hosts and select **Download MFT to Server** from the right-click context menu, or from the **More Actions** drop-down list in the toolbar.

	ate Respond	Users Hosts Fi	iles Dashboard	Reports			Q	14	%	?	admin >
∇ Filters ×	Broker - Endp	V 🛛 🖓 Analyze Even	nts 🗸 OScan 🗸	🖏 Tags 🗸	More Actions	1					ê
SAVED FILTERS	⊟ → HOSTNAME			RISK SCORE	Reset Risk Score	r version	AGENT ID				
Select	•			٥	Download MFT to Server	4	C8DDF10	07-1343-9	564-1D40	9EAEB786	8681
HOST STATUS	Ø	Analyze Events		٥	Download System Dump to Server	۵ 🛦	B0BAD20	E-96C0-2	C8F-8EFC-	31FA289A	5223
Managed		Delete Start Scan		٥	Download Files to Server	• •	89A2B44	A-76BC-2F	44-A8B6-	85ABDF0B	DEB9
Roaming Isolated		Stop Scan		٥	Upgrade Agent		BC7DCE6	0-95AD-8	F9E-FB05	75DA3D40	01D9
		Download MFT to Server Download System Dump to Server		•	Uninstall Agent	4	6F7008E4	-0F1B-4A	7B-BC70-:	3FBFDBC3	1AB6
RISK SCORE		Download Files to Server		•	6 days ago 11.5.:	.0	5CFE11D	C-F91D-43	IC5-B3FA-	FBD464DF	7A4F
••		Upgrade Agent		•	6 days ago 11.5.:	.0	F5489124	-E77E-402	2D-A636-9	AD3553D	0477
0		Unirotal Agent		•	6 days ago 11.5.3	.0	861381D	8-AB24-4E	FF-9F2A-I	OCDA314	1026

- Select the hostname to open the host details, click (More) beside the hostname, and select **Download MFT to Server**.
- 2. In the Download MFT to Server dialog, select one of the following:
 - System Drive to download MFT to the system drive.
 - Select Drive to download MFT on assigned drive. You can select any drive from the Drive drop-down list. By default the selected drive is C.
 - Specify NTFS mount path to download MFT on the path to the folder where it is mounted

Click Download.



3. View details of the downloaded MFT in the **Downloads** tab within the host details. For more information, see <u>Hosts View - Downloads Tab</u>.

NETWITNESS Platform Investigat	e Respond Users Hosts F	iles Dashl	board Reports			,	ඊ 🖃 拨 ⑦ admin >
100 AGENT SC Idle	AN STATUS AGENT LAST SEEN AGEN a few seconds ago	VERSION					
ALERTS PROCESSES AUTORUNS FILES	DRIVERS LIBRARIES ANOMALIES	DOWNLO	DADS SYSTEM IN	NFO HIST			
∀ Filters ×	Downloads Save a Local Copy	Delete File					
SAVED FILTERS		туре	DOWNLOADED	SIZE	DOWNLOADED TIME	U SHA256	FILE PATH
Select	mft-C-Win1909-64b-0-2020-03-13T08-39	MFT	 Image: A second s	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		
	□ > eV		✓		2 days ago		
Process Dump System Dump	C:\Users\"\		~		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.

🔆 NETWITNESS Platform	Investigate Respond Users	Hosts Files	Dashboard Reports			
100 Contraction age in the interval of the int	FILES DRIVERS LIBRARIES AN	VERSION OMALIES DOWNL	OADS SYSTEM INFO			
✓ Downloads ✓ Filters	MFT Viewer Download File to	o Server				
MFT-C-WINDOWS10-2019-11-14T06-47-52-777Z	I NAME	SIZE	CREATION TIME (\$FN)			
✓ ⊖ C:	RWE-Trace-Oct.ctxt	0 bytes	11/12/2019 07:02:03 pm			
> 🗅 inetpub	B NWE-Trace-Oacc.rar	2.0 MB	11/12/2019 11:54:16 am			
> 🗅 wampó4	NWE-Trace-Oacc.txt	0 bytes	11/12/2019 12:48:33 am			
> 🗅 Windows	NWE-Trace-Of80.rar	1.0 MB	11/12/2019 12:08:39 am			
> 🖸 Users		0 bytes	11/11/2019 09:25:01 nm			
 Program Files (x86) 		00,00				
> SRecycle.Bin	WE-Trace-0a3c.txt	0 bytes	11/11/2019 07:32:11 pm			
> D PerfLogs	B NWE-Trace-0c44 - Copy.txt	49.8 MB	11/11/2019 06:56:29 pm			
> D Program Files SExtend	RWE-Trace-1fc0.txt	8.5 KB	11/11/2019 05:44:35 pm			
C Recovery	E NWE-Trace-0c44.txt	0 bytes	11/11/2019 05:43:31 pm			
 Documents and Settings 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 EUES	NWE-Trace-264c - Copy.txt	21.0 MB	11/11/2019 05:02:52 pm			
	RWE-Trace-264c.bxt	0 bytes	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.

X NETWITNESS Platform	n Investigate Respond Users	Hosts	Files Dashboard	Reports			Ó II 🖇	🖌 🕜 admin >
71 C2 I AGENT SCAN STATUS AGENT LAST SEEN AGENT VIESION X								
ALERTS PROCESSES AUTORUNS	FILES DRIVERS LIBRARIES ANO	MALIES D	OWNLOADS SYSTEM					
C Downloads V Filters	MFT Viewer Download File to Server							
MFT-C-INGSMUDALPL6C-2019-11-29T09-10-45-317Z	I NAME	SIZE	CREATION TIME (\$FN)	CREATION TIME (\$51)	MODIFICATION TIME (\$FN)	MODIFICATION TIME (\$51)	ACCESS TIME (\$FN)	ACCESS TIME (\$SI)
Git Origin Feature Branch	🗆 🖻 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
> C Temp	Camileme	0 bytes	11/07/2019 01:03:38 pm	11/07/2019 01:02:38 pm	11/07/201901:03:38 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]	R 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	11/07/201901:01:54 pm
SysintematsSuite		0 bytes	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm 💧	11/07/2019 12:57:32 pm 🔺	11/07/2019 12:57:32 pm 💧	11/07/2019 12:57:32 pm
> 🗅 50	🗆 🖻 setuperclog	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	C R diagovro.com	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
Windows Recovery	🗆 🖻 diagerr.xml	1.9 KB	08/22/201901:54:19 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
> D Users	B DiskOleanupV3.exe	280.5 KB	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am 🧥	05/26/2019 10:44:40 am 💧	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am
> Program Files (x86)	C C mmuq	0 bytes	06/06/2019 05:31:54 pm	06/06/2019 05:31:54 pm	06/06/201905:31:54 pm 💧	06/06/201905:31:54 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 (\$FN), update time (\$SI), modified time (\$FN), and modified time (\$SI).

VIC ALTENT ME MENTIONAL ALTENT ME MENTIONAL ALTENT ME MENTIONAL V DOWNLOADS SYSTEM INFO HISTORY V DOWNLOADS SYSTEM INFO HISTORY SALET S AUTORUM FILES DOWNLOADS SYSTEM INFO HISTORY V Downloads MET Viewer Downloads Bitter Sectory CEATION THE (FFM) CEATION THE (FM) C	NETWITNESS Platform Investigate	Respond Users Hosts Files I	Dashboard Reports		୦ ଅ	% 🕐 admin >		
ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANMALIES DOWNLOADS SYSTEM INFO HISTORY V Filters X Commloads MFT Viewer Download file to Server SAVTO FILTESS Select Introduction time (SFN) CERATION TIME (SFN)	71 C i AGENT	SCAN STATUS AGENT LAST SEEN AGENT VERSION a few seconds ago	4					
V Filters x Conviloads MFT Viewer Download File to Server SAVED FILTERS Select IMFC Research IMAG SIZE CECATION TIME (FFN)	ALERTS PROCESSES AUTORUNS FILES DI	RIVERS LIBRARIES ANOMALIES DO	WNLOADS SYSTEM INFO HISTORY					
SAVED FILTES INTECREMENTAGE CONSIDER TATION SUBJECT ON SUB	⊽ Filters ×	C Downloads	MFT Viewer Download File to Server					
Select I Gt Origin Fature Branch I B stupact/og 19K8 11/11/2019/0617/00 am 11/11/2019/0617/00 am 11/11/2019/0617/00 am FILE NAMK S Git Origin Master C ComTimm? Objets 11/07/2019/010338.pm 11/07/2019/010338.pm Equals e.g. Filename.dll Deep Web (2015)[YTS.AG] S StaddwarceClientconfemgr1810-dise. 18K8 11/07/2019/010338.pm 11/07/2019/010338.pm FILE TYPE S pinternalsSuite S StaddwarceClientconfemgr1810-dise. 18K8 11/07/2019/01257/32.pm 11/07/2019/01257/32.pm 11/07/2019/01257/32.pm TIMESTOMPING Documents and Settings S Intel B stuper.log Objets 09/14/2019/1154/02 am 09/14/2019/1154/02 am 09/14/2019/1154/02 am 09/14/2019/0154/19 pm 08/22/2019/0154/19 pm	SAVED FILTERS	MFT-C-INGSMUDALPL6C-2019-11-29709-10-45-317Z		SIZE	CREATION TIME (\$FN)	CREATION TIME (\$51)		
FILE NAME > Git Origin Master > Git Origin Master 0 bytes 11/07/2019 010338 pm 11/07/2019 010338 pm Equals e.g. Filename.dll > Git > Git <td>Select</td> <td>🗀 Git Origin Feature Branch</td> <td>E setupact log</td> <td>1.9 KB</td> <td>11/11/2019 06:17:06 am</td> <td colspan="2">11/11/2019 06:17:06 am</td>	Select	🗀 Git Origin Feature Branch	E setupact log	1.9 KB	11/11/2019 06:17:06 am	11/11/2019 06:17:06 am		
FILE NAME > Drap Cmlmp Optes 11/07/2019/01/338.pm 11/07/2019/01/338.pm Equals e.g. Filename.dll Deep Web (2015) (YTS.AG] Deep Web (2015) (YTS.AG] Deep Web (2015) (YTS.AG] 18/8 11/07/2019/01/338.pm 11/07/2019/01/338.pm File TYPE Deep Web (2015) (YTS.AG] Deep		> 🖸 Git Origin Master						
Equals e.g. Filename.dll I 00-0ep Web(2015)(YTS.AG] I II 007/2019 010154 pm 1107/2019 010154 pm 107/2019 01054 19 pm 09/2019 0154 19 pm 09/2019 0154 19 pm 09/2019 0154 19 pm 09/202019	FILE NAME	> 🗅 Temp	C CcmTemp	0 bytes	11/07/2019 01:03:38 pm	11/07/2019 01:03:38 pm		
FILE TYPE > Git Equals e.g. dil TIMESTOMPING > infei Documento and Settings > Windows > Mindows > infei > Mindows > infei > Windows > infei > infei > infei > Windows > infei > infei > infei	Equals 🤟 e.g. Filename.dll	Deep Web (2015) [YTS.AG]	SMSAdvancedClient.configmgr1810-clien	1.8 KB	11/07/2019 01:01:54 pm	11/07/2019 01:01:54 pm		
FILE TYPE [©] m [®] [©] 0 bytes ¹ 107/20191257:32 pm ¹ 107/20191257:32 pm Equals [©] e.g.dll [©] 100 [©] m [®] ⁰ bytes ¹ 107/20191257:32 pm ¹ 107/20191257:32 pm ITIMESTOMPING [©] 100 [©] 100 [©] stuper:log ⁰ bytes ⁰ /14/20191154:02 am ⁰ /14/20191154:02 am ITIMESTOMPING [©] 0 custrot and Settings [©] 0 diager:smit ¹ 9/18 ⁰ /9/14/20191154:19 pm ⁰ /9/14/20191154:19 pm ⁰ /9/22/20190154:19 pm ⁰ /9/22/2019/0154:19 pm ⁰		> 🗅 Git						
Equals e.g. dll 0 b/14/2019 113402 am 0/9/14/2019 113402 am 0/9/20/20191034142 am C EL	FILE TYPE	SysinternalsSuite		0 bytes	11/07/2019 12:57:32 pm	11/07/2019 12:57:32 pm		
TIMESTOMPING Indi Indi Indiana India I	Equals v e.g. dll	> 🗅 ISO			09/14/2019 11:54:02 am	54:02 am 09/14/2019 11:54:02 am		
TIMESTOMPING Documents and Settings I diagwn.cml 19K8 08/22/20190154:19 pm 08/22/20190154:19 pm 08/22/20190154:19 pm CREATION TIME (FFN) CUSTOM DATE > Program Files (bd8) I B diagwn.cml 19K8 08/22/20190154:19 pm 08/22/20190154:19 pm 08/22/20190154:19 pm 08/22/20190154:19 pm 08/22/201910154:19 pm 08/22/20191015		> 🗅 Intel						
LimiteStomped Files > Windows □ III diager.cml 19KB 08/22/2019/0154:19 pm 08/22/2019/0154:19 pm 08/22/2019/0154:19 pm CREATION TIME (5FN) > Ustrom Date > Degram Data □ IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Documents and Settings	🗆 🖻 diagwm.xml	1.9 KB	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm		
CREATION TIME (\$\$1) CUSTOM DATE > CREATION TIME (\$\$1) > CREAT	Li Timestomped Files	> C Windows	C E diaserrami	1.9 KB	08/22/2019 01:54:19 pm	08/22/2019 01:54:19 pm		
Creation time (151) Custom Date Stacycle.Bin Disk/Cleanup/Save 220.5 KB 0x/2x/2019 10.44.42 am 0x/2x/2019 10.44.42 am > D Program Data > D Program File (560) D momule 0 bytes 0x/0x/2019 05.31.54 pm 0x/0x/2019 05.31.54 pm C relation time (151) > D Stacycle.Bin D momule 0 bytes 0x/0x/2019 05.52.20 am 0x/2x/2019 05.52.20	CREATION TIME (\$FN)	> 🗅 Recovery						
CREATION TIME (\$51) Custom Data Degram Dias Digram Files (\$60) Odd/06/2019/05/31:54 pm Odd/06/2019/05/31:54 pm Odd/06/2019/05/31:54 pm CREATION TIME (\$51) D Custom Date D Program Files (\$60) D Program Files (\$60) D Program Files (\$60) D 1/2/3/2016/01:49:18 am D 1/2/3/2016/01:49:18 am		> 🖸 Users	DiskCleanupV3.exe	280.5 KB	06/26/2019 10:44:42 am	06/26/2019 10:44:42 am		
CREATION TIME (\$51) CUSTOM DATE > © Program File (\$58) > © SkeydelSin □ 🖻 pyw.cne 869.1 KB 05/29/2019.05.52:20 am @ 12/23/2016.01:49.18 am @		> ProgramData		0 bytes	06/06/2019 05:31:54 pm	06/06/2019 05:31:54 pm		
→ Skeyde.Bin D Pyw.exe 869.1KB 05/29/2019.05.22.0a A 12/23/2016.01.49.18a A	CREATION TIME (\$SI) CUSTOM DATE	> Program Files (x8ó)						
		> SRecycle.Bin	D D 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 \blacksquare .

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.

XNETWITNESS Platform Investigate	Resp	oond	Users Hosts	Files Dasht	ooard Repor	rts			
∀ Filters		8	Broker - Endp 🗡	Analyze E	Events 🗸	⊖Scan∖	✓ 🔊 Tags ∨	: More A	actions ∨
SAVED FILTERS			HOSTNAME		RISK SCORE	√ C	S - DESCRIPTION		LAST SC
Select	~				N/A	,	Microsoft Windows	10 Pro for Worksta	ati 05/08/20
HOST STATUS					N/A	F	Red Hat Enterprise	Linux- 7.2	05/05/20
Managed					N/A	F	Red Hat Enterprise	Linux- 7.2	05/06/20
Roaming		R				;	4	a Enterprise	05/06/20
□ Isolated					Analyze Ever	nts		>	05/05/25
RISK SCORE		L			Delete				05/05/20
100]				Start Scan			к 8.1 (Ootpa)	05/06/20
	•							Education	
0					Network Isola	ation		> nterprise	
HOSTNAME						ET to So		Enterprise	
Equals ~ Enter Value					Download with		vei		05/07/20
licenname					Download Sy	ystem Du	mp to Server		05/06/20
Foulds V Enter Value					Download Fil	ies to Sei	iver		20,00,20
					Reset Risk S	Score		ducation	
AGENT GROUPS						i	viicrosoft Windows	7 Enterprise	05/08/20

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

NETWI	TNESS Platform	Investigate Respond Users	Hosts Files	Dashboard Agent V	Reports TERSION	рѕнот тіме 1	1/30/2021 12:02:28 pn
ALERTS SEVERITY	PROCESSES AUT	Start Scan Export Host details Export Files	LIBRARIES	ANOMALIES	DOWNLOADS	SYSTEM IN	FO HISTORY
6 CRITICAL	CRITICAL Pos	Download MFT to Server Download System Dump to Server	events)				
40	CRITICAL Exp CRITICAL Bla	Download Files to Server Uninstall Agent)				
HIGH	CRITICAL Drop CRITICAL Enat	ps Credential Dumping Tools (78 e bles Login Bypass (24 events)	vents)				
93 MEDIUM							
139 All							

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

Remote Shell

From version 12.3 or later, NetWitness Remote Shell feature (Hosts > Select the hostname > click (More) beside the hostname > Remote Shell) allows you to access the agents installed on your Windows machine remotely and execute a list of commands to perform certain actions such as deleting the files, changing the directories, terminating specific processes, and executing the processes on the remote host.

Warning:

- Use **NetWitness Remote Shell** feature with utmost caution to avoid the potential for negative impact on the system. NetWitness Platform is not responsible for any damages, loss of data, or other consequences that may arise after using **NetWitness Remote Shell** feature.

- If you are an administrator, NetWitness recommends you to add roles and assign the role permissions only for the selected users in the **Security** > **Roles** view to avoid any damages to the system.

Note:

- NetWitness Remote Shell feature can be used only if Windows Advanced mode Agents are installed on the machine. The agent version must be 12.3 or higher to access the NetWitness Remote Shell feature.

- NetWitness Remote Shell feature is not supported if the agent is communicating with the server through proxy.

- **NetWitness Remote Shell** feature supports connection with the agents that communicate through the relay servers (RAR). To access the **NetWitness Remote Shell** feature for the agent that communicates through the relay servers (RAR), you must download the latest relay packager from the Endpoint Server (EPS) and install it on the existing relay server.

For more information, see https://community.netwitness.com/t5/netwitness-platform-online/optional-installing-and-configuring-relay-server/ta-p/669551.

List of Supported Commands

The following table provides information about the list of supported commands displayed in the **NetWitness Remote Shell** console.

Supported Commands	Description
help	View the list of available commands
cd	Change the current working directory
del	Delete a file
rmdir	Delete a folder
dir	List the contents of a directory
mkdir	Create a new directory
tasklist	List all the active processes on the computer
taskkill	Terminate a process

Supported Commands	Description
call	Execute a process on the remote computer
reg	View or modify Windows registry settings

Note:

- You must use only the silent commands to perform the required actions.

- You must end the session and re-connect if you run any command that requires user inputs. Refer the following figure.

\$ dir	
dir	
Volume in drive C has no label.	
Volume Serial Number is	
Directory of C:\Users\ \Desktop	
04/04/2823 04:23 PM <dir> .</dir>	
64/64/2823 04:23 PM <dir></dir>	
03/30/2023 11:51 AM 49 doc.txt	
04/04/2023 04:10 PM <dir> testdir</dir>	
1 File(s) 49 bytes	
3 Dir(s) 39,369,228,288 bytes free	
C:\Users\ \Desktop>	
\$ del testdir	
\$ help	Send Command

Example Scenarios

Example 1: If you want to delete a specific file that exists in different subfolders, you must run the following command.

```
del /s /q <full_file_path>
```

Here,

- del refers to delete.
- /s refers to the deletion of the file from all the subfolders.
- /q refers to quiet or silent mode execution.
- <full_file_path> refers to the location where the file exists.

Example 2: If you want to terminate a specific process running on your Windows machine, you must run the following commands.

```
taskkill /f /im <process-name>
taskkill /f /pid <process-id>
```

Here,

- taskkill refers to terminate.
- /**f** refers to force shutdown.
- /im refers to image name.
- **<process-name>** refers to the specific process.
- **<process-id>** refers to the specific process ID.
- /pid refers to process ID.

Example 3: If you want to delete a specific registry, you must run the following command.

```
reg delete /f <keyname> [/v ]
```

Here,

- **reg delete** refers to deleting a registry key.
- /f refers to deleting the existing registry subkey or entry without asking for the confirmation.
- **<keyname>** refers to the registry key name.
- [/v] refers to deleting a specific entry under the subkey.

To execute commands using NetWitness Remote Shell:

- 1. Go to Hosts. Do one of the following.
 - Click a row in the Hosts list view and go to More Actions > Remote Shell.



The NetWitness Remote Shell window is displayed.

Ne	Witness Remote Shell		×
P	DESKTOP- windows		
		 Connecting to the Agent. This may take a few minutes. 	

Click the Hostname and click (More) beside the hostname in the Host Details view to select **Remote Shell**.

The NetWitness Remote Shell window is displayed.



• Right-click a row in the Hosts list view and select Remote Shell.



The NetWitness Remote Shell window is displayed.

2. Enter the commands once the Agent is connected.



3. Click Send Command or press the Enter key.

4. Click End Session in the NetWitness Remote Shell window once the required action is performed.

The confirmation window is displayed.

5. Click End Session to close the NetWitness Remote Shell window.

RBAC Permissions for Remote Shell

Users with Analysts and other roles must have the **endpoint-server.remoteshell.manage** permission to view and access **the NetWitness Remote Shell** feature. Administrators can assign the **endpoint-server.remoteshell.manage** role permission to a specific user or to a specific role. The existing roles must be duplicated in the **Security** > **Roles** view and the new users must be assigned to the duplicated roles to assign the **endpoint-server.remoteshell.manage** role permission only to the specific new users.

You must go to *(Admin)* > Services > select the Endpoint Server Service > View > Config > Permissions view to assign the endpoint-server.remoteshell.manage permission to the specific users. For more information on duplicating a role, adding a role and assigning permissions, and editing the role permissions, see System Security and User Management Guide for 12.3.

Administrators can configure the RBAC Permission at Endpoint Server level. You can allow the users assigned to a specific role to view and access the **NetWitness Remote Shell** feature on any specific Endpoint Server. When you allow the user to view and access the **NetWitness Remote Shell** feature only on a specific Endpoint Server such as EPS1, the user cannot view or access the **NetWitness Remote Shell** feature on any other Endpoint Servers such as EPS2 and EPS3. If the user has the access to the **NetWitness Remote Shell** feature on one of the Endpoint Server view for all the agents. In this case, the user can access the feature and connect with the remote agent from the **Broker** view, if the selected remote agent is present only in EPS 1 and not in any other Endpoint Servers such as EPS2, the **NetWitness Remote Shell** console screen keeps loading. This happens since the user can access the feature only on EPS1 and not on EPS 2.

Note: If you configure the **endpoint-server.remoteshell.manage** permission at the role level in the **Security** > **Roles** view, the users assigned to the role can access the **NetWitness Remote Shell** feature on any Endpoint Servers such as EPS 1, EPS 2, and EPS 3.

For more information on Configuring the RBAC permissions at the role level, see (Optional) Add a Role and Assign Permissions section in the System Security and User Management Guide for 12.3.

To configure Remote Shell RBAC permission to the specific users at the endpoint server level:

- 1. Go to (Admin) > Services.
- 2. In the Services view, select the required Endpoint Server service.
- 3. Click \bigcirc and select View > Config.
- 4. Go to **Permissions** tab.
- 5. Select the role you duplicated in the Security > Roles view from the Roles panel on the left.
- 6. Select the permission endpoint-server.remoteshell.manage from the Permissions section.

🔆 NETWITNESS Platform Investigate Respond Users Hosts Files Dashboard Reports 🔗 🔍 🗵 🛠 🔿 admin 🗸									
HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY									
A Change Service endpointighybridt - Endpoint Server Config General Data Retention Scheduler Agent Packager Relay Server 3rd Party Scan Permissions									
Roles (17) Mahuare Analysts	Analysts Permissions Select permissions for this rate in this server. You can modify the diabled permissions only on the security server. Click tory to access.	Assigned Following are the	Users (2) existing users with Analy	ntis permissions					
Analysts	D PERMISSION	USERNAME	NAME	EMAIS ADDRESS					
UEBA, Analysts		analyst1	analyst1	analyst1@na.com					
Reporting_Engine_Content_A		analyst2	analyst2	analyst2@na.com					
Apprepation	endpolet serverprocesumanage								
Manage_Users									
Read_Central_Config									
Kibana Administrator	ngendpoint server/encleshell.manage								
eps1_role	endpoint serversecurity-manage								
eps2_role									
Analyst_2_role									
Analyst_1_role									

7. Click Save.

For more information on configuring the permissions at the Endpoint Server level, see Manage Role Permissions at Endpoint Server Level.

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 Actions** drop-down list in the toolbar.

	igate Respond Users	Hosts Files Dashboard	Report				Ó E	3 % ()	admin >
100 E A	GENT SCAN STATUS AGENT L dle a few se	AST SEEN AGENT VERSION	SNAPS	нот тіме 06/24/	2020 21:30:3	33 🗸			
ALERTS PROCESSES AUTORUNS FIL	LES DRIVERS LIBRARIES	S ANOMALIES DOWNLOADS		MINFO HISTO	RY				۹
▽ Filters	× Processes [☑ Analyze Process 黛 Change	e File Statu	ıs 🛛 🖓 Analyze E	vents 🗸	: More Actions V		TRE	EVIEW
PROCESS NAME		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	🗹 dwm.exe		<u> </u>	100		Known Good	Blacklisted		C:\Wind
	svchost.exe	Analyze Process		100		Known Good	Neutral		C:\Wind
Graylist	svchost.exe	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
Suspicious	svchost.exe	Download Process Dump to Serve	r	100		Known Good	Neutral		C:\Wind
Unknown Known	svchost.ext:	Download File to Server		100		Known Good	Neutral		C:\Wind
Known Good	sychost.ext:	Save a Local Copy		100		Known Good	Neutral		C:\Wind
	svchost.exe			100	2	Known Good	Neutral		C:\Wind
CICNATURE									

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

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

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 Actions** drop-down list in the toolbar. You can download files from only top 100 selected hosts at a time.

*NETWITNESS Platform Investigate	Respond	Users Hosts Files Dashboa	ard	Reports			Š 🗟	% 0	admin >
∇ Filters ×	Broker - End	p ✔ 🕑 Analyze Events ✓ ⊙ Sc		No Tags V 🚺 M	Nore Actions \checkmark				ê
SAVED FILTERS	HOSTNAME	RISK SCORE ψ OS - DESCRIPTION		LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGENT SCAN STATUS	AGENT GROUPS	IPV4
Select ~		100 Microsoft Windows 10 F	oter	06/28/2020 21:30:08	WHENEYS I.	a few seconds ago	Idle	Windows-security	10.125.245.1
HOST STATUS	0	Analyze Events >	oter	06/24/2020 21:30:33	whereas the	a few seconds ago	Idle	Windows-security	10.125.245.1
Managed	0	Delete	ļ	06/29/2020 14:30:23		a few seconds ago	ldle		10.125.244.2
Roaming		Start Scan							
L Isolated		stop scan							
		Network Isolation >							
		Download MFT to Server							
		Download System Dump to Server							
		Download Files to Server							
HOSTNAME		Reset Risk Score							
Equals v Enter Value									

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

Download Files to Server.

NETWI	TNESS Platform	Investigate Respond User	ers Hosts Files Dashboard Reports
100	ď	AGENT SCAN STATUS	agent last seen agent version snapshot time 11/30/2021 12:02:28 pm
ALERTS	PROCESSES AUT	Start Scan Export Host details	LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY
SEVERITY	Critical Alerts 🕕	Doursload MET to Server	
6 CRITICAL	> CRITICAL Pos	Download System Dump to Ser	rver } events)
	> CRITICAL Exp	Download Files to Server	
40		· · · · · · · · · · · · · · · · · · ·	
HIGH	> CRITICAL Dro	ps Credential Dumping Tools ((78 events)
93	> CRITICAL Ena	bles Login Bypass (24 events)	
MEDIUM			
139			
ALL			

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 to Server								
FILE PATH Enter the path where files may be	present. For wildcard search, a '*' can be							
used at a folder and file level. C:\Users*\NTUSER.DAT								
NUMBER OF FILES Maximum of 500	FILE SIZE (MB) Downloads all files upto the specified size limit							
500								
	Cancel Download							

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.

Note: You can set a limit to the Maximum Number of Files field on the explore page of the

Endpoint server (> [Endpoint server] > explore > endpoint/command > max-file-count). By default, the limit is set to 100, and you can change it to any value between 100 - 1000 in each Endpoint server. In broker view, if the Endpoint servers have different max-file-count, the lesser value will be taken as the limit.

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.

NETWITNESS Platform Investigate Respond Users Hosts Files Dashboard Reports & 🕑 🗟 % 🕐 admin >											
0 Idle a few seconds ago											
ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY											
∀ Filters ×	Downloads Save a Local Copy	Delete File									
SAVED FILTERS		ТҮРЕ	DOWNLOADED	SIZE	DOWNLOADED TIME	4 SHA256		FILE PATH			
Select 🗸	C:\Users*\NTUSER.DAT		~		8 minutes ago						
Wildcard Downloads			~		a day ago						
FILE TYPE	o > 🥌		~		2 days ago						
MFT File		-	~	-	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.

	Respond Users Hosts F	iles Dasł	nboard Reports		ć	5 🗷 % 🕐 admin >					
0 Idle a few seconds ago											
ALERTS PROCESSES AUTORUNS FILES DRI	VERS LIBRARIES ANOMALIES DO	WNLOADS	SYSTEM INFO HISTORY								
∇ 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		 ✓ 	24 minutes ago							
FILE TYPE	C:\Users\ \Desktop\exe\exe*		 - 	a day ago							
MFT File	□ > c:*		 - 	2 days ago							
Process Dump System Dump	C:\Users\"\ \N"		 ✓ 	10 days ago							
FILE NAME											
Equals v e.g., Filename.dll											
SHA256											
Equals V 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 $\overline{\mathbf{M}}$.

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.

NETWITNESS Platform	Respond Use	ers Hosts Fi	les Dashbo	oard Repo	rts		Š 🗟	🔏 🕐 admin >
0 AGENT SCAN ST	ATUS AGENT LAST S a few second	een agent ver Is ago						
ALERTS PROCESSES AUTORUNS FILES	DRIVERS LIBRAI	RIES ANOMALIE	S DOWNLO	DADS SYST	EM INFO HI			
∇ Filters \times	Downloads s	Save a Local Copy	Delete File					
FILE TYPE				DOWNLOADED		DOWNLOADED TIME	SHA256	
MFT File		Save a Local	Conv			days ago		
Process Dump		Save a Local	гсору			days ago		
System Dump		Files are ready to do	wnload.	t hast the downl	aad will stop	days ago		
FILE NAME Equals - e.g., Filename.d8		II you havigate away	rion die curren	C	ancel Downl	oad days ago	0adabf60afa537c2e99ba5377	C:\Program Files\VMware\VMware
	e e			~	353.5 KB	ZI days ago	230b0b13bac36e40947d550	C:\Program Files\VMware\VMware
sHa256 Equals v Enter Value				~		21 days ago	717873c479bc23fdb956ce19	C:\Program Files\VMware\VMware
				~	46.0 KB	21 days ago	e16170f46148220fb5348a30	C:\Windows\WinSxS\amd64_micros
				~	256.0 KB	25 days ago		C:\mnt\NTFS
DOWNLOADED Downloaded Error								
Reset Save Save as				Sh	owing 106 out of 1	106 files 1 selected		

4. In the Save a Local Copy dialog, click Download.

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.

NETWITNESS Platform Investigate	Respond Users Hosts	Files Dashboard	Reports			Ŏ	2 % 0	admin >			
100 windows A GENT SCAN STATUS A GENT VERSION Scanning a few seconds ago A MENT VERSION											
ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY											
∇ Filters $ imes$	Downloads Save a Local Copy	Delete File									
SAVED FILTERS		TYPE DO	WNLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH				
<u>Select</u>	M 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	~		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.

NETWITNESS Platform Investigate	Respond Users Hosts Files Dashboard Reports	Ŏ 로 % ⑦ admin>
♥ Filters ×	😂 endpointbrok V View Certificates 🛛 🖾 Change File Status 🗍 🖾 Analyze Events 🗸 🖬 More Actions V	
SAVED FILTERS	□ FILE NAME RISK SCORE ↓ FIRST SEEN TIME ON HOSTS REPUTATION	SIZE SIGNATURE PE.R 🛞
Select	VourPhone.exe	23.5 KB unsigned Microsoft
FILE NAME	microsoft.noversit Analyze Events Console Events 02107/44.07 am Known	52.0 KB unsigned Microsoft
Equals v e.g., Filename.dll	Microsoft,Pay,Bac Google Lookup Network Events 02107:44:07 am 2 Known	15.0 KB unsigned Microsoft
FILE STATUS	SystemNumerics VirusTotal Lookup > File Events 021.04:40-28 am 1 Known	314.5 unsigned
Neutral Neutral	AppCoreFramewo Process Events 02104:40:28 am 1 Known	670.5 unsigned
Graylist	AppInstallerBacka	2.5 KB unsigned
Whitelist	Save a Local Copy 100 10/29/202107-44.07 am 1 Unknown Analyze File 100 10/29/202107-44.07 am 1 Unknown	106.5 unsigned RSA
	SharedMemoryUV Scan with OPSWAT 10/29/2021 07:44:07 am 1 Known	3.0 KB unsigned
Diocrea	restorecond.org Reset Risk Score 10/29/2021.05:06:01 am 2 Malicious	69 bytes unsigned
	iconv.dll 10/29/2021 07:51:29 am 2 Known	920.5 unsigned Free Soft
	StoreRatingPromotion.dll 10/29/2021 07:44:07 am 2 Known	264.5 unsigned
	PaintStudio Model CX.winmd 10/29/2021 07-51:29 am Xnown Known	3.5 KB unsigned
Known Good Invalid	Microsoft.Wallet.coe 100 10/29/20210744:07 am 2 Known	18.0 KB unsigned -
Reset Save Save as	Showing 100 out of 1000+ files 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*.

Note: If the values are not indexed, the results take time to load. For more information, see <u>Troubleshooting NetWitness Endpoint</u>.

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.

ALERTS PROCESSES AUTORUNS FILES D	RIVERS LIBRARIES ANOMALIES DOWI	NLOADS SYSTEM I	NFO HISTORY	
∀ Filters ×	Autoruns Services Tasks			
	🛃 Analyze Events			
Equals v e.g., Filename.dll	REGISTRY PATH	ON HOSTS TYPE	LAUNCH ARGUMENTS FILENAME	FILE PATH
	HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsoc	«Provide	C:\Windows\System32\
	HKEY_LOCAL_MACHINE\System\CurrentControl	2	Demuide Change File Status	C:\Windows\System32\
	HKEY_LOCAL_MACHINE\System\CurrentControl	2 Console	Events	C:\Windows\System32\
	HKEY_LOCAL_MACHINE\System\CurrentControl 2 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432 2	2 Network Events	Events VirusTotal Lookup	C:\Windows\System32\
		2 Process	Download File to Server Events	C:\Program Files (x86)\Common Files\Java\Java Update\
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\	2 Registry	Events Save a Local Copy	C:\Program Files\VMware\VMware Tools\
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro	EY_LOCAL_MACHINE\SYSTEM\CurrentContro 2 logon	cmd.exe	C:\Windows\SysWOW64\
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro	2 logon		C:\Windows\System32\
	HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsoc	«Provide <u>vsocklib.dll</u>	C:\Windows\SysWOW64\
	HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsoc	«Provide <u>vsocklib.dll</u>	C:\Windows\SysWOW64\
	HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsoc	«Provide <u>vsocklib.dll</u>	C:\Windows\SysWOW64\
Reset		Showing	13 out of 13 autoruns 1 selected	

The following figure is an example of the Autoruns tab.

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

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

Text Analysis for an Endpoint Event

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

- Event Header, which provides summary information about the event. (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 🗸	02/27/2019 07:43am - 03/	/2019 07:42em V alias.host = x action = openbrowserprocess x		()
			Guided Made Free-Form Made		
5,423 Events (Asc)	Endpoint Analysis	s _ 2 ×	Endpoint Event Details Text Analysis		<u>■</u> * ×
COLLECTION TIME	ТҮРЕ	EVENT TIME D	Download Log V F2 Pivot to Endpoint Thick Client F2 Analyze Process F2 Pivot to Host Overview		
03/14/2019 09:41:34 am	Endpoint				
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw	NW SERVICE ESSION ID NW CATGOY COLLECTION THE EPS1-Server - Concentrator 6965 Process Event 03/14/2019/09/41/34 am	EVENT TIME 03/14/2019 09:36:26 am	
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw	PROCESS EVENT		A
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw	© 03/14/2019 09:36:26 am □ ① NT AUTHORITY\NETWORK SERVICE	SESSIONID	6965 03/14/2019 09:41:34 am
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw		SIZE FORWARD.IP IP.ALL	606
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw	Lance Mein VALUS param.dst-chrome.exe - type-crashpad-handler " user-data-dir-C:\Users\ \ \AppData\Local\Google\Chrome\User nata: "research 7monitor.cal_connettion_strached_handler "	MEDIUM DEVICE.TYPE	32 nwendpoint
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw	database-C:\Users\ \AppData\Local\Google\Chrome\User Data\rushpad" "metrics- din-C:\Users\ \AppData\Local\Google\Chrome\User Data"url=https://clients2.google.com/cr/report	DIR.PATH.SRC DIR.PATH.ALL DIR.PATH.SRC	windows windows windowsSumm 32
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw	annotation-channel=annotation-plat-kin64annotation-prod-Chromeannotation-ver-73.0.3683.75initial- client-data-0xte0,0xte4,0xte0,0xtdc,0xtec,0x7ffa64916830,0x7ffa64916840,0x7ffa64916850	DIR.PATH.ALL CONTEXT.SRC	windowsSystem32 file:found
03/14/2019 09:41:34 am	Endpoint	2019-03-14T09:36: nw		CONTEXT.ALL	file.found
				CONTEXT.ALL	file.protected

Below is an example of the Network event:

EPS1-Server - Concentrator ∨	02/27/2019 07:43am - 03/26/2019	9 07:42em v alias.host = " x category = network event x		<u>۵</u>
		Guided Mode Free-Form Mode		
22,535 Events (Asc)		ndpoint Event Details Text Analysis		<u>■</u> * ×
Endpoint Analysis v		Download Log 🗸 🖸 Pivot to Endpoint Thick Client 🛛 🖸 Analyze Process 🔀 Pivot to Host Overview		
COLLECTION TIME TYPE	EVENT TIME D 🔅		50007 XIII	
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe	STANLES ESSUA D'ANNE ANTONIOUS COLLECTION AND STANLES COLLECTION AND STANLES STANLES COLLECTION AND STANLES STANL	03/14/2019 09:34:15 am	1 10003
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe			-
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe	NETWORK EVENT () 03/14/2019 09:34:15 am	EVENT META SESSIONID 6768 TIME 03/14/2019 (19-41-24 am
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe	SecureConnector.exe MADE A NETWORK CONNECTION TO 10.254.20.237 FROM 10.87.157.55	SIZE 332 FORWARD.IP	
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe	LARGE META VALUES param.src-SecureConnector.exe -performer -id AD6A82C2CA554F8F9AC31898870C7148 -token	IP.ALL MEDIUM 32	1
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe	c22114e7017e841b0392af5404293ee4600269dc -ip 10.254.20.237 -port 10003 -sha256 34E3868148C6F9C8D0E08C08A891F442F7291DB80FD40935588D22025202885D -lcif 7 -event	PORT.DST 10003 PORT.ALL 10003	
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe	FSA_TMP_5388_5C890E73_0002PERFORMER_CNTL -rrd 0	PORT.DST.ALL 10003 DIR.PATH.SRC programFiles	;
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe		DIR.PATH.ALL programFiles CONTEXT.SRC file-autorun	•
			CONTEXT.ALL file.autorun	
03/14/2019 09:41:34 am Endpoint	2019-03-14T09:34: nwe		CONTEXT.SRC file.found	
			CONTEXT.ALL file.found	l astMonth

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.

	Investigate Respon	d Users Host	s Files Dashboard Reports	
∀ Filters		🖯 Broker - Endp 🗸	Y │ │ │ Analyze Events │ ↓ ↓ ○ Scan ∨ │ € Tags ∨	More Actions V
SAVED FILTERS		HOSTNAME	RISK SCORE ψ OS - DESCRIPTION	LAST SCAN TIME
Select	~ [46.5995-596-5	N/A Microsoft Windows 10	Pro for Workstati 05/08/2020 02:2
HOST STATUS		(halisain)	N/A Red Hat Enterprise Line	ux- 7.2 05/05/2020 05:5
□ Managed		(Institutin)	N/A Red Hat Enterprise Line	ux- 7.2 05/06/2020 07:3
 Roaming Isolated 	E			rprise 05/06/2020 07:4
RISK SCORE			Delete	05/05/2020 01:0
	100	tim the line is a second s	Start Scan	l (Ootpa) 05/06/2020 07:20
	<u> </u>		Stop Scan	ation
0	C	AMAGED DESIGN	Network Isolation	> Isolate from Network
HOSTNAME	C	********	Download MFT to Server	Edit Exclusion List
Equals ~ Enter Value	C		Download System Dump to Server	05/07/2020 08:4
USERNAME	C	Realized in all mail	Download Files to Server	05/06/2020 07:3
Equals ~ Enter Value			Reset Risk Score	ation
		AND STREET	N/A Microsoft Windows 7 E	ntorprico 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.

X NETV	VITNESSIPI	atform Investigate Re	espor	nd Users	Hosts	Files
100		AGENT SCAN STATUS	AGI fe	ENT LAST SEEN	AGENT	VERSION
ALERTS	PROCESSES	Start Yara Scan Export Host details	5	LIBRARIES	ANOMA	LIES
SEVERITY	Critical Alerts	Export Files				
3 CRITICAL	> CRITICAL	Network Isolation	>	Isolate from Netv	work	
F	> CRITICAL	Download MFT to Server		Edit Exclusion Lis	t	
НІБН		Download System Dump to Serve Download Files to Server	er			
5		Uninstall Agent				
13 ALL						

 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	t					

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

Note: When a host is isolated, the connection to the following IP addresses are allowed: - Endpoint Server, Relay Server, DNS, DHCP, Gateways, 0.0.0, 255.255.255.255, and any other IP addresses that the agent connects with.

- Other IP addresses that you include in the exclusion list.

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.

	Investigate Respor	nd Users Hosts Files	Dashboard Reports	
▽ Filters		⊖ Broker - Endp ∨	alyze Events 🗸 🛇 Scan 🗸 🔊 🕻 Mor	e Actions ∨
SAVED FILTERS		HOSTNAME	RISK SCORE ψ OS - DESCRIPTION	LAST SCAN TIME
Select	C	NATES AND A STREET	N/A Microsoft Windows 10 Pro for Workst	ati 05/08/2020 02:21:
HOST STATUS	C	(insidents)	N/A Red Hat Enterprise Linux- 7.2	05/05/2020 05:59:
Managed		inalijadni	N/A Red Hat Enterprise Linux-7.2	05/06/2020 07:38:
□ Roaming			termise	05/06/2020 07•47•
□ Isolated			Analyze Events >	05/00/2020 07171
RISK SCORE			Delete	05/05/2020 01:07:
	100		Start Scan .1 (Ootpa)	05/06/2020 07:20:
•	• 🗖	(MEMORIALIS/11/	Stop Scan	
0			Network Isolation > Release	e from Isolation
HOSTNAME		WHEELE	Download MFT to Server	clusion List
Equals ~ Enter Value			Download System Dump to Server	05/07/2020 08:44:
USERNAME	C	acalises is salismate	Download Files to Server	05/06/2020 07:32:
Equals ~ Enter Value		miniture contract	Reset Risk Score ucation	-
AGENT GROUPS		ANAL ALEXCETANCE	N/A Microsoft Windows 7 Enterprise	05/08/2020 06:53:

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

X NETV	VITNESS Platfo	orm Investigate Respond	Users Hosts	Files Dashboa	rd Reports
100	ď	AGENT SCAN STATUS	GENT LAST SEEN	AGENT VERSION	snapshot тіме 09/16/2022 12:05:20 pm (Yara Scan)
ALERTS		Start Scan Start Yara Scan Export Host details			DS SYSTEM INFO HISTORY
SEVERITY	Critical Alerts 🕚	Export Files			
1 CRITICAL	> CRITICAL Op	Network Isolation >	Release from Isolatio	in	
2		Download MFT to Server	Edit Exclusion List		
HIGH		Download System Dump to Server			
1		Download Files to Server			
		Uninstall Agent			
1					
4 ALL					

- 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.

NETWITNESS Platform Investigate Re	espond	Users Hosts Files	Dashboard Reports		
∀ Filters ×	E	∃ Broker - Endp ➤	Analyze Events 🗸 🕤 Scan 🗸 📎	Tags V i More Action	ns 🗸
SAVED FILTERS		HOSTNAME	RISK SCORE 🛛 🕹 OS - DESCR		LAST SC
Select ~			N/A Microsoft V	Windows 10 Pro for Workstati	05/08/20
HOST STATUS			N/A Red Hat En	terprise Linux- 7.2	05/05/20
Managed			N/A Red Hat En	Iterprise Linux- 7.2	05/06/20
Roaming				Vindows 8.1 Enterprise	05/06/20
□ Isolated			Analyze Events		05/05/2
RISK SCORE			Delete	04.4 LTS	05/05/20
100			Start Scan	terprise Linux 8.1 (Ootpa)	05/06/20
• <u>•</u> ••••••••••••••••••••••••••••••••••			Stop Scan	Vindows 10 Education	
0			Network Isolation >	Release from Isolation	
HOSTNAME			Download MFT to Server	Edit Exclusion List	
Equals v Enter Value			Download System Dump to Server	04.6 LTS	05/07/2
USERNAME			Download Files to Server	ux 8 (Core)	05/06/2
Equals ~ Enter Value			Reset Risk Score	Vindows 10 Education	
AGENT GROUPS			N/A Microsoft V	Vindows 7 Enterprise	05/08/2

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

XNET V	WITNESSIP	latf	orm Investigate Res	pond	Users	Hosts	Files	Dashboa	rd	Reports	
100		ď	AGENT SCAN STATUS		AGENT LAST SEEN	;o	AGENT VEI		snap 09/1	shot тіме .6/2022 12:05:20	pm (Yara Scan)
ALERTS		AUT	Start Yara Scan Export Host details								
1	Critical Alerts		Export Files								
CRITICAL	CRITICAL		Network Isolation		Release from	n Isolatior	1				
2			Download MFT to Server		Edit Exclusio	n List					
HIGH			Download Files to Server	erver							
1			Uninstall Agent								
MEDIUM											
4 ALL											

2. Enter comments and click Release Host.

High Availability (Endpoint Recovery)

The High Availability or Endpoint recovery configuration feature in the Admin Server - Source Server

Explore view (Admin > Services > select the Source Server > View > Explore > endpoint/recovery) allows administrators to map the service ID of an Endpoint server with the recovery Endpoint service ID as part of recovery configuration.

Note: Map the service IDs of multiple Endpoint servers in the form of comma separated Key Value pairs. You must enter ':' in between the Key Value pairs. The Key refers to the service ID of the unavailable Endpoint server and the Value refers to the service ID of the recovery Endpoint server. For Example: <Unresponsive EPS ServiceId-1>: <Recovery EPS ServiceId-2>, < Unresponsive EPS ServiceId-3>: < Recovery EPS ServiceId-4>

To configure the Endpoint Recovery

1. Go to **Admin** > Services.

The Services view is displayed.

2. Select the Source Server. Go to **View** > **Explore**.

The Explore view is displayed.

- 3. Click endpoint/recovery.
- 4. Enter the service IDs of the Endpoint servers in failover-service-id-mapping field.

Anarge Service Admin-Server - Source Server Explore		
₽ Admin-Server - Sourc	/rsa/endpoint/recovery	Admin-Server - Source Server
	fallover-service-id-mapping	
Central/content		
central/policy		
C central/service		
Centralpolicy		
Cmc/client		
C cms/subscription		
C configuration		
data/control		
indpoint/recovery		
in features		
filesystem		
C formats	1	
grouppolicy		
in health		
logging		
C metrics		
nextgen/client/cache		
nextgen/connection-attributes		

Endpoint Recovery Use Case Example

The following use case provides an example of an Endpoint administrator using the High Availability feature in the NetWitness Platform to configure the Endpoint recovery.

Use Case: Endpoint Server EPS 1 turns unresponsive

Administrator Steven finds that an Endpoint server EPS 1 in the environment is not responding from a long time and the communication between the agents and the Endpoint server EPS 1 is failing. Steven navigates to the Admin Server - Source Server Explore view and selects endpoint/recovery configuration. As part of the Endpoint recovery configuration, Steven maps the service ID of EPS1 with the service ID of an active Endpoint server EPS 2.

Pre-requisites for Endpoint Recovery Configuration

Make sure the following pre-requisites are met before you perform Endpoint Recovery Configuration.

• Before you install the recovery Endpoint server EPS 2 and perform Endpoint recovery configuration, make sure you copy the **nwerootca-key.pem** and **nwerootca-cert.pem** certificate files from EPS 1 (unresponsive Endpoint server) to EPS 2 (recovery Endpoint server). If the certificate files in EPS 1 and EPS 2 do not match, the agent fails to communicate with EPS 2 in case of EPS 1 failure.

IMPORTANT: Once you install EPS 1 on your machine, backup the **nwerootca-key.pem** and **nwerootca-cert.pem** certificate files. If you fail to do so and the EPS 1 fails due to some disaster, you cannot copy the **nwerootca-key.pem** and **nwerootca-cert.pem** certificate files in EPS 1 to EPS 2.

For more information on how to backup and copy the certificate files, see **Configuring Multiple Endpoint Log Hybrids** section in **Install NetWitness Platform Virtual Host in Virtual Environment** topic in the *Virtual Host Installation Guide for 12.3.1*.

- When you replace an unresponsive relay server configured on an Endpoint server with the new relay server, make sure you re-use the same Fully Qualified Domain Name (FQDN) or IP address of the unresponsive relay as part of the relay recovery configuration.
- You must enter the Forwarder address of the recovery Endpoint server in **Endpoint Sources** > **Policies** view immediately after mapping the service IDs of the Endpoint servers in the **Admin Server Source Server Explore** view. During the failure of an Endpoint server EPS 1, if the IP address of the recovery Endpoint server EPS 2 changes, and you do not provide the Forwarder address of the recovery Endpoint in **Endpoint Sources** > **Policies** view, the agent fails to communicate with the recovery Endpoint server EPS 2.
- The HTTPS ports of the Primary Endpoint server and the recovery Endpoint server must match during the Endpoint recovery configuration.

DNS Recovery Configuration

Note: The agent cannot establish communication through RAR mode as part of DNS Recovery. If Endpoint server is not directly reachable, the DNS recovery fails.

When all the Endpoint servers in the deployment are unresponsive, the agent searches for the recovery Endpoint server through the DNS entry. You must configure the new recovery Endpoint server in the deployment and include it in the DNS record to allow the agent to communicate with the newly added recovery Endpoint server.

To add the recovery Endpoint server to the DNS entry

- 1. Enter the following in DNS server.
 - **Domain Name**: Enter the domain name of the recovery Endpoint server in the form of <service ID>.nwrecovery.local.

For example: Domain Name must be entered in the form of 5bdv7ado-69a0-41f2- 8574-d3ffc78b9.nwrecovery.local.

Here, **<service ID>** is the service ID of the unresponsive Endpoint server which is variable and **nwrecovery.local** is a static element in all the domain names.

- IP Address: Enter the IP address of the recovery Endpoint server as the IP address for the domain name.
- 2. Perform Endpoint recovery configuration in Admin Server Source Server Explore view. For more information, see <u>To configure the Endpoint Recovery</u>.

The agent establishes communication with the newly added recovery Endpoint server.

NetWitness Endpoint with Third-Party Antivirus Products

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

Troubleshooting NetWitness Endpoint

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

General Issues

Issue	Some of the hosts or files data are not displayed when Endpoint Broker is selected for querying.
Solution	The Endpoint Broker aggregates data from all Endpoint Servers, which responds within 10 seconds. You must increase the query timeout value to see the result of Endpoint server that is online. Perform the following:
	1. Go to (Admin) > Endpoint Broker service.
	2. Click Set
	3. Click endpoint/broker node.
	4. In the query-timeout field increase the value, for example, 30 seconds.

Issue	The Endpoint Agent is unable to communicate with the Endpoint Server. The connection may not be established due to any of the following issues:
	• UDP
	• HTTPS
	• Firewall
	• 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:
a 1 .:	cd C:\Windows\System32
Solution	2. Execute the following command:
	<agent name="" service="">.exe /testnet</agent>
	For example, NWEAgent.exe /testnet
	• If the issue is with the firewall, check the incoming and outgoing firewall rules.
Issue	The Endpoint Agent is unable to communicate with the Log Decoder. The connection may not be established due to any of the following issues:
	• UDP
	• TCP
	• TLS

	• Firewall
Solution	• 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
	2. Execute the following command:
	<agent name="" service="">.exe /testlognet</agent>
	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> .

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</i> <i>Host Installation Guide</i> or <i>Virtual Host Installation Guide</i> . If the service is not running, start the Endpoint Server.	
Issue	 Hosts view shows 'No Results Found.' error in the following scenario: Host A belongs to Endpoint server A and does not exist in Endpoint server B. Endpoint server B is selected in Hosts view. In a new window/tab, open the Host details page (of Host A) Navigate to Hosts view using [<i>Host Name</i>] > Actions > Pivot to Investigate 	

Hosts View Issues

	> Hosts/Files	
	Endpoint server B is selected by default, and the page shows 'No results found.' error.	
Explanation	This is expected behavior. The Endpoint server that is selected first is considered to be current /active throughout the session.	
Workaround	Ensure the correct Endpoint server is selected, and Pivot to Investigate > Hosts/Files will behave normally.	
	For MFT download:	
Issue	1. The request fails with file not found error for drives/mount paths created on the machine after agent is installed.	
	2. Incorrect MFT is downloaded for the provided NTFS mount path.	
Solution	Make sure that the agent version is 11.6 or later.	

Files View Issues

Issue Explanation	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 Analyze Events from Hosts and Files view for this Endpoint server may not work. To resolve this issue:
	Note: To get the investigate-service-id: 1) Go to (Admin) > Services > Concentrator service. 2) Click > View > Explore tab. 3) Expand the sys/stats node list. 4) In the UUID filed, copy the value.
	 Go to (Admin) > Services > Endpoint Server service. Click Server > View > Employee tel
	 Click > View > Explore tab. In the endpoint/investigate field, specify the investigate-service-id
	or in the endpoint in resultance herd, speenly the investigate service rat

Policy Issue

Issue	Policy status in the Policy Details panel is not updated or shows Policy Unavailable/Permission Required.
Explanation	Policy Unavailable - Hosts belong to previous versions, such as NetWitness Platform 11.1 or 11.2, where a policy is not applied.

details.

	Permission Required - If you do not have permissions, see the "Role Permissions" topic in the <i>System Security and User Management Guide</i> .
Issue	Policy Status shows error.
Explanation	Policy may have wrong configurations. Check the error description, logs in Endpoint server, and audit logs for details. Contact your system administrator with the error

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.

Download Issue

Issue	Downloads (Files, MFT, System/Process dumps, etc.) fail at times.
Explanation	Downloads fail when there is not sufficient disk space on the Endpoint Server.
Workaround	Clean up some disk space and try downloading again. We recommend you keep sufficient disk space before initiating any download.

File Reputation Service Issue

Issue	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 3 (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.
	Ch	eck 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.
		b. Click \diamond \sim > View > Explore.
		c. Expand the respond/scheduled/jobs node list.
		d. In the risk-scoring-enabled field, set the value to false.
a 1 .	4.	To disable Endpoint ESA alerts:
Solution		a. To disable NetWitness Endpoint ESA alerts generation for severity; Critical, High and Medium.
		i. Go to Configure) > ESA Rules.
		The Configure view is displayed with the Rules tab open.
		ii. In the Options panel, under Deployments, select the Endpoint deployment to delete.
		A confirmation dialog is displayed.
		iii. Click Yes.
		b. To disable only Medium severity NetWitness Endpoint ESA alerts:
		i. Go to (Admin) > ESA Correlation service (on which Endpoint deployment is added).
		ii. Click 🔅 🕑 > View > Explore.
		iii. Expand the correction/alert node list.
		iv. In the transient-enabled field, set the value to false.

Endpoint Broker/Server Issue

Issue	User have access to one Endpoint server and unable to access the other.
Explanation	Reach out to the administrator and check if you have access to that endpoint servers. Request for access if required.

Issue	In the Endpoint Server Broker view, the user can scan hosts that belong to a particular Endpoint server but cannot scan hosts that belong to another Endpoint server.
Explanation	User may not have access to that endpoint server. Check with the Administrator to see if the user has access.

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
- Hosts View YARA Rules Tab

Files View

Note: The information in this topic applies to NetWitness latest version.

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
- Manage Blocked File Hashes
- Changing File Status or Remediate

Quick Look

Below is an example of the Files view:

🔆 NETW	ITNESS Platform				Files D				6			% 0	
⊽ Filters	🖯 endpointbrok 🗡	Manage 🗸	X Change File S	tatus 🛛 🖄 Ana	lyze Events 🛛 🗸	More Actions	× 1	2	Ě		cmd.exe	1	
	1	RISK SCORE 4	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNA	Type to filter the 4	- @	FILE DETAILS		LS 5 STS	
1 imd.exe	3						micros	File Name	Neuti				
<u>SearchInde</u>	xer.exe	٥	05/25/2023 10:22			882.0	micros	Risk Score	Neuti	🗹 Show details wi	h values only		
SkyDrive.e:		٥	05/25/2023 10:36			1.1 MB	micros	File Status	Neuti	General			
ntoskrnl.ex		٥	05/25/2023 10:22			7.1 MB	micros	Remediation Reputation	Neuti	FileN	ame cmd.exe		
D <u> premove.e</u>		0	05/25/2023 11:47			65.5 KB	micros	Downloaded Size	Neuti		Opy 4.666021	122233989	
<u>ByteCodeC</u>		٥	05/25/2023 10:36			28.0 KB	micros	Signature	Neuti		mat pe		
sdiagnhost.		•	05/25/2023 10:36			24.0 KB	micros	 First Seen Time Operating System 	Neuti				
DiagTrackR		0	05/25/2023 07:32			86.2 KB	micros	Signature.Timestamp Signature Thumborint	Neuti	Signature		deve of exteriors	
generaltel.		0	05/25/2023 07:32			606.0	micros	Signer	Neuti		amp 11/07/20	signed,catalog 14 08:02:40.305 al	m
AM Delta		٥	05/30/2023 10:22			465.5	micros	II MD5	Neuti		orint df3b9b7e	5aea1aa0b82ea25	1542a6a0096
Trustedinst		0	05/25/2023 10:36			104.0	micros	□ SHA256	Neuti		gner Microsoft	Windows	
D ngen.exe		٥	05/25/2023 10:36			167.1	microso	ft,signed Microsoft Corp	Neuti				
AM Delta		0	05/28/2023 10:22			845.4	microso	ft,signed Microsoft Corp	Neuti		иD5 f5ae03de	Dad60f5b17b82f2	cd68402fe
<u>svchost.exe</u>		٥	05/25/2023 10:22			37.9 KB	microso	ft,signed Microsoft Corp	Neuti		HA1 7c3d728	e1151fe4127923	14b4c3cd3643
□ <u>taskhost.ex</u>		0	05/25/2023 10:22			87.3 KB	microso	ft,signed Microsoft Corp	Neuti		256 6f88fb88	fb0f1d5465c2826	e5b4f523598
		0	05/25/2023 10:36	0		20.5 KB	microso	ft,signed,catal Microsoft Corp	Neuti				
			Showing 7	9 out of 79 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.
	Manage - You can select any of the following drop-down options in the Manage drop-down list.
	• Certificates - Allows you to view a list of code-signing certificates reported by hosts found in your deployment and their associated properties. For more information, see <u>Analyze</u> <u>Certificates</u> .
	• Blocked File Hashes - Allows you to add or import new file hashes and manage the existing blocked file hashes.
	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 Set Files Preference.
5	Show/Hide File Properties Panel. Click a row to show or hide the File Properties panel. It displays the following tabs:
	File Details - Displays the file information.
	Risk details - Displays the distinct alerts associated with the risk score.
	Hosts - Displays the top 100 hosts based on the risk score on which the file is present. For more information, see <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:

NETV	VITNESS Platform	estigate Respond Users Ho	sts Files Dashboard Reports	Č 🗷 拨 🕜 admin >
100	ол новтя 1	s signature size File sta unsigned 2.7 KB Neutra	TUS - I	×
ALERTS	ANALYSIS			<u>_</u>
SEVERITY	Critical Alerts 🚯			FILE DETAILS HOSTS X
1	✓ CRITICAL Opswat Report	ed Infected (1 events)		Type to filter list
CRITICAL	EVENT TIME	SUMMARY	TARGET PARAM	
0	10/03/2022 07:50:46.000 am	ufw-init	N/A	Show details with values only
HIGH				Scan Time 10/03/2022 07:50:46.130 am
0				Scan details > 2 Infected, 1 Suspicious D
MEDIUM				
1			<u>↑</u>	Reputation Known
<u>Т</u>			3	
ALL				General
2				FileName utw-init
				Size 2.7 KB
				Format script

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 Alerts Severity 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> Hosts with File Activity.

Hosts View

Note: The information in this topic applies to NetWitness latest version.

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



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

Related Topics

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

Quick Look

Below is an example of the Hosts view:

XNETWITNESS Platform	nvestigate Respond Users	Hosts Files D			3	4		🔏 🕐 admin >
▼ Filters →	😫 Broker - Endp 🗡 🛛 🖓 Al	nalyze Events 🗸 O Scan	✓ S Tags ∨ 🚦	More Actions ∨	← 2 ↓	7	w	indows10 X
SAVED FILTERS	HOSTNAME RISK SCORE	↓ OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN	AGENT SCAN ST/	HOST DETAILS RI	SK DETAILS 6
Select	🗹 <u>Windows10</u> 🚥				a few seconds ago	Idle	Type to filter list	
HOST STATUS	Windwost0-0 ISOLATED	Microsoft Windows 10 Enterprise	06/28/2020 21:30:08	WINDWOS10-0/ec	a few seconds ago	Idle 🚺	Show details with va	ues only
Managed	centos1 31	CentOS release 6.7 (Final)	06/29/2020 14:30:23		a few seconds ago	tdie 5	Groups	
Roaming							Groups	Windows-security
L Isolated								
RISK SCORE							Users	
100							Name	WINDOWS10\ecat
<u></u>							Session ID	2
0							Groups	Administrators
HOSTNAME							Users	
Equals ~ Enter Value							Name	Window Manager\DWM-1
USERNAME							Session ID	1
Equals - Enter Value								
							Network Interfaces	Intol/D\82574L Gigshit Notwork
AGENT GROUPS							MAC Address	00-50-54-01-20-04
							IPv4	10 125 245 185
NIC MAC ADDRESS							IPv6	49244784-3926978 fa80-94c6476b4234-249
Equals ~ e.g.,00:00:00:00:00							Gateway	10 125 244 1
19V4							DNS	10 31 64 22 10 31 64 23
Equals v e.g., 11.1.1 1.1.1.1							Promiscous	folca
AGENT LAST SEEN OCUSTOM DAT							Operating System	
							Description	Microsoft Windows 10 Enterprise
Reset Save Save as		Showing	g 3 out of 3 hosts 1 selected				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 Delete a Host.
- Download MFT to the server. For more information, see Performing Host Forensics.
- Download System Dump to the server. For more information, see <u>System and Process</u> Memory Dump.
- Isolation host from the network. For more information, see Isolating Hosts from Network.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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> Attributes.
- 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 NetWitness latest version.

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

Workflow



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 Hose
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

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:

🔆 NET \	WITNESS Platform Invest	igate Respond Users Hosts Files Dashboa		👌 🗟 % 🕐 admin >
100	⊠ : AGI Idia	ENT SCAN STATUS AGENT LAST SEEN AGENT VERSION 9 24 days ago	SNAPSHOT TIME	Search by filename, path or hash Q ×
ALERTS				2
SEVERITY	Critical Alerts			HOST DETAILS POLICY DETAILS X
	CRITICAL Blacklisted File (6 e	events)	TARGET PARAM	Type filter list 5
	08/30/2022 11:02:20.000 am	libnspr4.so present in /usr/lib64	N/A	Show details with values only
HIGH	08/30/2022 11:02:20.000 am	lvm2-monitor.service present in /usr/lib/systemd/system	N/A	
1	08/30/2022 11:02:20.000 am	libgcrypt.so.11.8.2 present in /usr/lib64	N/A	
	08/26/2022 12:58:21.000 pm	lvm2-monitor.service	N/A	
2	08/26/2022 11:28:37.000 am	libgcrypt.so.11.8.2	N/A	Network Interfaces Name ens192
	08/26/2022 11:23:29.000 am	Libnspr4.so	N/A	MAC Address 00:50:56:01:39:87
└_ _				
6	1			Gateway 10.125.248.1
				Promiscous false
				Description Red Hat Enterprise Linux- 7.2

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</u> Memory Dump.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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 Search Files on Host.
- 3 Show/Hide Right Panel Displays host and policy details panel.
- 4 Host Details Panel Displays all properties of the selected host. It is grouped as follows:

Groups - Groups on which the host is added on.

User - Information related to the user.

Network Interfaces - Network adapter information, such as Mac Address, Gateway.

Operating System - Operating system version and build information.

Agent - Agent-related information, such as agent ID, driver error code, install time, and agent mode.

Hardware - Information related to the architecture.

Locale - Time zone and language that is local to the host.

- 5 **Policy Details Panel** Displays the following:
 - Policy Status -
 - Updated Host has the latest policy.
 - Pending Policy is resolved but the latest policy is not updated on the host. When the host communicates with the Endpoint server next time, the latest policy is applied if there are no errors.
 - Unavailable Hosts that belong to previous versions, such as NetWitness Platform 11.1 or 11.2, or the source server is not installed.
 - Error Problem applying the latest policy along with the error description.
 - 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 NetWitness latest version.

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



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

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:

*	NETWITNESS Pla	<mark>tform</mark> Investigate F	tespond Users	Hosts Fi	les Dashboard	d Reports			3	Ŏ		% ©		iin >
10	0 windows	AGENT SCAN STATU	s AGENT LAST SEEF a few seconds a	agen go	TVERSION 5	тарshot тіме 12/13/2022 07:39	13 am 🗸 🔸	-11	Search by 1					
AL	ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEMINFO HISTORY													
7	Filters Processes	🖄 Analyze Process	Change File Status	⊠ Analyze Even	ts 🗸 🕻 More	Actions V	2	TREE VIEW						×
	PROCESS NAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILE PATH	DETAILS					
		5						C:\Windows\Syst						
	<u>csrss.exe</u>	٥	•	2	Known Good	Neutral	-	C:\Windows\Syst	Show d	etails with va	lues only			
		٥	٥		Known Good	Neutral		C:\Windows\Syst	Status					
		٥	۰		Known Good	Neutral	✓	C:\Windows\Syst			Known Go	bd		
		•	•		Known Good	Neutral	✓	C:\Windows\Syst	General					
		0	0		Known Good	Neutral		C:\Windows\			csrss.exe			
		٥	0		Known	Neutral		C:\Program Files			6.2854768	350818055		
		•	0		Known Good	Neutral		C:\Windows\Syst	0		16.7 KB			
		•	•		Known Good	Neutral		C:\Windows\Syst						
		•	•		Known Good	Neutral		C:\Windows\Syst			false			
		0	0		Known Good	Neutral		C:\Progran Files	Hash					
		0	(0)		Known Good	Neutral		C:\Windows\Syst			b2d3f07f5	e8a13af988a8t	3c0a800880	
			<u> </u>	_							c79e4586	989ebb8e8f808	4b5eb49afbf	fd2
	Showing 43 out of 43 processes 1 selected									SHA256	ch41e9dO	8107aa9337d	d1c56f2246	11

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.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</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 Investigating a Process.

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see <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:
 - **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:

XNETWITNESS Platform Investigate Respond Users Hosts Files Dashboard Reports	Q	8	*	?	admin >
100 C : AGENT SCAN STATUS AGENT LAST SEEN AGENT VERSION SNAPSHOT TIME 11/03/202105:24:19 pm -					
ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY					۹
< Processes Details					
PROCESS NAME OWNER PPID PATH LAUNCH ARGUMENTS					
Visual mediae erat 6000 Countriest/UppUsta/Local/Microsoft/Debutwe/					
> Loaded Libraries (30)					
> Image Hooks (U)					
7 Suspicious Tineaus (o)					

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 NetWitness latest version.

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



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

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 Autoruns tab:

	stigate Respond User:	s Hosts Files	Dashboa	rd Reports	3	👌 🗃 % 🕐 admin >
100 C i Ager Idle	NT SCAN STATUS AGENT LAST a few secon	seen Agent ve ds ago	RSION	snapshot Time 12/13/2022 07:39:13 am v	Search by fi	ilename, path or hash Q X
ALERTS PROCESSES AUTORUNS F	ILES DRIVERS LIBRAR	ES ANOMALIES	DOWNLOA	ADS SYSTEM INFO HISTORY		
7 Filters Autoruns Services T			4			vsocklib.dll X
Analyze Events V					8 DETAILS	
REGISTRY PATH	ON HOSTS TYPE	LAUNCH ARGUMENTS	FILENAME	FILE PATH	Type to filt	
HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsockProvide		vsocklib.dll	C:\Windows\System32\	Show de	etails with values only
HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsockProvide		vsocklib.dll	C:\Windows\System32\	Autoruns	
HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsockProvide		vsocklib.dll	C:\Windows\System32\	5	Type winsockProviders
HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsockProvide		vsocklib.dll	C:\Windows\System32\		
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432	2 logon	- 6 ->	j <u>usched.exe</u>	C:\Program Files (x86)\Common Files\Java\Java Update\	Status	
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\	2 logon	-n vmusr	vmtoolsd.exe	C:\Program Files\VMware\VMware Tools\		Reputation Known
HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro	2 logon		cmd.exe	C:\Windows\SysWOW64\	General	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro	2 logon		cmd.exe	C:\Windows\System32\		FileName vsocklib.dll
HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsockProvide		vsocklib.dll	C:\Windows\SysWOW64\		Entropy 6.137908757322461
HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsockProvide		vsocklib.dll	C:\Windows\SysWOW64\		Size 66.7 KB
HKEY_LOCAL_MACHINE\System\CurrentControl	2 winsockProvide		<u>vsocklib.dll</u>	C:\Windows\SysWOW64\		Deleted false
	Showing 12 out	of 12 putorups 1 coloct	od			

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>.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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

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

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

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

Signature - Provides signatory information.

- Hash Hash type of the file (MD5, SHA1, and SHA256).
- Time Time when the file was created, modified, or accessed.

Location - Location of the file.

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

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

Note: The information in this topic applies to NetWitness latest version.

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



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	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

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 Files tab:

	K NETWITNES	S Platform Inve		Users Hosts Files Dashbo				3			* (ව adı	
100 windows AGENT SCAN STATUS AGENT LAST SEEN AGENT VERSION SNAPSHOT TIME 100 Idle a few seconds ago 12/13/2022 07:39:13 am 12/13/2022 107:39:13 am 12/13/2022 107:39:13/2022 107:39:13 am 12/13/2022 107:39:13/2022 107:39:13 am 12/13/2022 107:39:130/2022 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/2020 107:39:130/20200								Search by fil				۹	
	ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY												
Files X Change File Status C Analyze Events Image Actions Image 2								nrpnsp.dll					
	FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	PATH	ON HOSTS	SIZE	DOWNLOAI	DETAILS					
₽	pnronsp.dll		100	C:\Windows\SysWOW64\				Type to filte					
		٥	٥	C:\Windows\System32\		110.5 KB		Show det	ails with va	lues only			
		٥	٥	C:\Windows\System32\		720.0 KB							
		٥	•	C:\Windows\SysWOW64\		67.5 KB				Known Goo	d		
		← <u>6</u> 0	٥	C:\Windows\SysWOW64\		548.5 KB		General					
C	keyiso.dll	٥	٥	C:\Windows\System32\		61.0 KB				pnrpnsp.dll			
C		٥	٥	C:\Windows\System32\		14.5 KB		- 3		6.4448209	52398581		
		0	0	C:\Windows\System32\		11.0 KB				68.5 KB			
C		٥	0	C:\Windows\System32\		669.4 KB							
	WSDMon.dll	•	0	C:\Windows\System32\		302.5 KB				false			
		•	0	C:\Windows\System32\		106.5 KB							
C	xerces-c 3 1.dll	0	0	C:\Program Files\VMware\VMware Tools\VMware		2.5 MB				19275944	74155ad367	7aba500337	/db9
L		^								f30c9dd1d	L5f91abda64	8b388ede7e	98db2
			Show	ring 1315 out of 1315 files 1 selected					SHA256	ac2425958	67154f527f	:4d7e3768c2	2526

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>.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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

1

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:								
	• 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 <u>Set Hosts Preference</u> .								

Hosts View - Drivers Tab

Note: The information in this topic applies to NetWitness latest version.

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



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

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 Drivers tab:

¥	NETWITNES	S Platform Invest			Hosts Files				3			劣			in >
10	100 windows AGENT SCAN STATUS AGENT LAST SEEN AGENT VERSION SNAPSHOT TIME 101 102 102 102 102 102 102 102 102 102														
ALE	ALERTS PROCESSES AUTORUNS FILES DRIVERS LIBRARIES ANOMALIES DOWNLOADS SYSTEM INFO HISTORY														
♥ Filters Drivers														×	
	FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	PATH 🛞	DETAILS						
						Neutral	-	C:\Windows							
	<u>vm3dmp.sys</u>	٥	٥		Known Good	Neutral	-	C:\Windows	Show det	ails with va	lues only				
	vm3dmp_loader.sys	٥	٥		Known Good	Neutral		C:\Windows	Status						
	NWEDriver16918.sys	٥	٥		Known Good	Neutral		C:\Windows			Known Go	od			
	rdpudd.dll	٥	٥		Known Good	Neutral		C:\Windows	General						
	terminpt.sys	٥	٥		Known Good	Neutral		C:\Windows			vmci.sys				
	WUDFPf.sys	•	0		Known Good	Neutral		C:\Windows	5		6.382686	89041889			
	tsusbhub.sys		٥		Known Good	Neutral		C:\Windows			102.4 KB				
	rdpdr.sys	•	•		Known Good	Neutral		C:\Windows							
	rdpvideominiport.sys	•	0		Known Good	Neutral		C:\Windows		Deleted	false				
	tunnel.sys		•		Known Good	Neutral		C:\Windows	Hash						
	<u>srv.sys</u>	•	(0)		Known Good	Neutral		C:\Windows			339e79b2	1cd73fe1	174b56d60	032e40d	32
											d85e6a6a	585fe4eb	a6f2601ae	97a9db1	.71
			Showi	ng 151 out of	151 drivers 1 selected					SHA256	91e68a98	91339a8r	ib757c9ec	eb65371	db

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.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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

1

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 <u>Search Files on Host</u> .							
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:							
	• 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 NetWitness latest version.

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



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

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:

×	NETWITNESS				Hosts				_1	3 👌 🗟 % 🕐 admin >	
	100 windows Life a GENT LAST SEEN a GENT VERSION SNAPSHOT TIME										
7	Filters Libraries	s 🗐 🛣 Change	desktopEvents.dll X								
	PROCESS C 7 T	FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	FILE STATUS	DOWNLOADED	FILE PATH	DETAILS LOCAL RISK DETAILS HOSTS	
	vmtoolsd.exe : 3728						Neutral		C:\Program Files\VMware	Type to filter list	
	vmtoolsd.exe : 3728	sigc-2.0.dll	٥	٥		Known	Neutral	 	C:\Program Files\VMware	☐ Show details with values only	
	vmtoolsd.exe : 3728	<u>vmtray.dll</u>	٥	٢		Known	Neutral		C:\Program Files\VMware	Status	
	vmtoolsd.exe : 3728	dndcp.dll	٥	٥		Known	Neutral		C:\Program Files\VMware	Reputation Known	
	vmtoolsd.exe : 3728	gmodule-2.0.dll	٥	٥		Known	Neutral		C:\Program Files\VMware	General	
	vmtoolsd.exe : 1512	gmodule-2.0.dll	6	•		Known	Neutral		C:\Program Files\VMware	FileName desktopEvents.dll	
	vmtoolsd.exe : 3728	intl.dll	•	٥		Known	Neutral		C:\Program Files\VMware	Entropy 6.160123657169687	
	vmtoolsd.exe : 1512	intl.dll	٥	•		Known	Neutral		C:\Program Files\VMware	Size 78,7 KB	
	vmtoolsd.exe : 3728	gobject-2.0.dll	•	•		Known	Neutral		C:\Program Files\VMware	Format pe	
	vmtoolsd.exe : 1512	sobject-2.0.dll	•	•		Known	Neutral		C:\Program Files\VMware	Deleted false	
	vmtoolsd.exe : 3728	gthread-2.0.dll	0	0	2	Known	Neutral		C:\Program Files\VMware	Hash	

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>.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

Snapshot Time - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.
hash to get the entire context of the activity. For more information, see Analyzing Events. 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. 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 information, such as process context, filename, local risk score, global 4 risk score, on hosts, reputation status, file status, and others. Show/Hide Right Panel - Displays the following properties in the right panel: • **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. Filter Files. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details. Settings Menu. You can set Hosts view preferences by selecting columns from the Settings

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

Analyze Events - Lets you investigate a particular host, IP address, username, filename, or

menu. For more information, see Set Hosts Preference.

Actions in the toolbar:

information, see Changing File Status or Remediate.

Hosts View - Anomalies Tab

Note: The information in this topic applies to NetWitness 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
- Analyzing Downloaded Files
- Changing File Status or Remediate
- Analyzing Events
- Performing Host Forensics
- Isolating Hosts from Network

Quick Look

Below is an example of the Anomalies tab:

¥	NETWITNESS Platfor		Hosts Files			1		3			% 0	
10	windows	AGENT SCAN STATUS AGENT LAST SEEN Idle a few seconds ag	AGENT VERSIO	on snapshot t 12/13/202	^{IME} 22 07:39:13	am v	_	Search by fil				a ×
ALE	RTS PROCESSES AUTO	DRUNS FILES DRIVERS LIBRARIES	ANOMALIES [DOWNLOADS SYS	TEM INFO	HISTORY	4					
7	Filters Filters	Kernel Hooks Suspicious Threads	Registry Discr						vmi	memctl.sys		×
ж	Change File Status	lyze Events 🗸 😧 🕻 More Actions 🗸	2			8		DETAILS)STS
	түре	FILENAME	LOCAL RISK SCORE	GLOBAL RISK SCORE	ON HOSTS	REPUTATION	SIGN/ 🗇	Type to filte				
Ø	basicObjectPointer						signed,valid	Show det	ails with val	ues only		
	basicObjectPointer	vsock.sys 6	٥	٥		Known	signed,valid	Status				
								• !	5	Known		
								General				
										vmmemctl.s		
										6.34682683	0514844	
										24.2 KB		
									Enrmot	00		

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 <u>Isolating Hosts from Network</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> Memory Dump.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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

Change File Status - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see Changing File Status or Remediate. Analyze Events - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see Analyzing Events. More - Provides options to: • Perform external lookups. • Download process dump to server. • Download files to server, save a local copy, and analyze files for deeper analysis. Note: You can perform some of the above actions from the right-click context menu. 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 • Image Hooks Kernel Hooks • Suspicious Threads **Registry Discrepancies** • Show/Hide Right Panel - Displays the following properties in the right panel: • **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. Clicking a filename lets you navigate to the Files view for further analysis. 6 Filter Files. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details.

Actions in the toolbar:

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.

Category	Description
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.
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 NetWitness Version 11.4 and later.

The Downloads tab provides information about all downloads (MFT, files, system dump, and process dump) performed on the host. To access this tab, select a host from the **Hosts** view and click the **Downloads** tab.

Workflow



What do you want to do?

User Role	I want to	Show me how
Threat Hunter	review hosts with highest risk score	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts	Investigating Hosts
Threat Hunter	perform adhoc scan	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot	Search 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:

	nvestigate Respond Users H	osts Files	Dashboa	rd Repor	ts			Q	8	*	?	admin >
100 vindows 2	AGENT SCAN STATUS AGENT LAST SEEN Idle a few seconds ago	AGENT VERSIO	N	1								×
DETAILS PROCESSES	FILES DRIVERS LIBRARIES AN	OMALIES DO	WNLOADS	SYSTEM I	NFO HISTORY							
∀ Filters ×	Downloads Save a Local Copy Delete	File - 3										
SAVED FILTERS	□ NAME	TYPE DO	WNLOADED	SIZE	DOWNLOADED TIME	SHA256	FILE PATH					
Select ~	dvm.oz	FILE	~	69.5 KB	20 days ago	df84c92b9745f11cab22460e						
Wildcard Downloads	DXCore.dl	FILE	~	109.7 KB	20 days ago	2e5a3168700ba8c2555b4de7						
		FILE	~	143.9 KB	20 days ago	14a5fb352fd89a8969147feee						
	mft-C-Win101903x6-0-2020-03-04T03-30-15-414Z	MFT	~	121.8 MB	20 days ago	NA						
File Frocess 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]			Sho	wing 4 out of 4 files 1 selected							

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 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.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.
- 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 <u>MFT Viewer</u>.

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:			
	- Download successful		
	- 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:

	stigate Respond Users Host	s Files [Dashboard Reports
100 vindows DETAILS PROCESS AUTORUNS FILE	IN STATUS AGENT LAST SEEN AGENT VERSION a few seconds ago ES DRIVERS LIBRARIES ANOMAL	IES DOWNLOA	ADS SYSTEM INFO
✓ Downloads	MFT Viewer Download File to Server	3	
MFT-C-WINDOWS10-2019-11-14T06-47-52-777Z		SIZE	CREATION TIME (\$FN)
~ ⊟ C:	RWE-Trace-Oc1c.txt	0 bytes	11/12/2019 07:02:03 pm
> 🗅 inetpub	RWE-Trace-Oacc.rar	2.0 MB	11/12/2019 11-54:16 am
> 🗅 wampó4	E NWE-Trace-Oacc.txt	0 bytes	11/12/2019 12:48:33 am
> C Windows	RWE-Trace-0f80.rar	1.0 MB	11/12/2019 12:08:39 am
	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
	RWE-Trace-0c44 - Copy.txt	49.8 MB	11/11/2019 06:56:29 pm
	RWE-Trace-1fc0.txt	8.5 KB	11/11/2019 05:44:35 pm
	RWE-Trace-0c44.txt	0 bytes	11/11/2019 05:43:31 pm
	B NWE-Trace-0c30.txt	101.9 KB	11/11/2019 05:42:05 pm
	DataCollector01.csv	642.9 KB	11/11/2019 05:03:16 pm
ALL FILES	RWE-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: Y 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.
- **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 NetWitness latest version.

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*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

*You can perform this task in the current view.

Related Topics

- Focusing on Endpoint Analysis
- Investigating Hosts

Quick Look

Below is an example of the System Information tab:

X NETWITNESS Platform		Users Hosts		ර් 로 % (?) admin >
31 windows	agent scan status Idle	agent last seen 5 days ago	AGENT VERSION SNAPSHOT TIME 01/09/2024 08:44:05 am	Search by filename, path or hash Q X
ALERTS PROCESSES AUTORUNS			LIES DOWNLOADS SYSTEM INFO HISTORY	Î Î
Host File Entries Network Shar	es Security Produc	ts Windows Pati	hes Security Configuration Installed Applications	2
IP ADDRESS			DNS NAME	3
-			scinstallcheck.mcafee.com	

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.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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 - 10.10.10.3 and DNS Name - localhost, localhost.localdomain, localhost4, localhost4.localdoma in4
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.

Tabs	Description
Security Products	Installed security products (for Windows only). For example, Display Name - Windows Defender, Instance - D68DDC3A-831F-4FAE-9E44-DA132C1ACF46, Features - Enabled, Type - antiVirus.
Windows Patches	List of patches applied by Windows update (for Windows only). For example, KB2959936.
Security Configuration	Security configuration details on the host. For example, firewall disabled or enabled, smart screen filter disabled or enabled. This field is only applicable for Windows and Mac.
Installed Applications	Displays the information about the various applications installed on a Windows machine.

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:

NETWITNESS Platform Investigate	e Respond Users Hosts F	iles Dashboard Reports 1	ð	🗷 💥 🕐 admin >
0 WIN81x64-1 127 € AGENT SCAN ? windows	STATUS AGENT LAST SEEN AGENT VER a few seconds ago	510N	2	
ALERTS PROCESSES AUTORUNS FILES	DRIVERS LIBRARIES ANOMALI	ES DOWNLOADS SYSTEM INFO HIS		
		3		
Filters 5 ×	Agent History			4
	HOST NAME	COMMAND TIME	COMMAND TYPE	USER NAME 5 17 🛞
	<u> WIN81x64-1</u>	04/24/2020 07:03:34 am	Scan	admin 🦉
	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>WIN81x64-1</u>	04/21/2020 09:33:03 pm	Download File	system 🗸
REQUEST TYPE	<u>WIN81x64-1</u>	04/21/2020 09:33:03 pm	Download File	system 🗸
~	<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	WIN81x64-1	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 11	13 Commands	

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.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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, agent upgrade, and uninstall agent) 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 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 Filter Host Details.
- 5 Settings Menu. You can set History view preferences by selecting columns from the Settings menu.

Hosts View - YARA Rules Tab

Note: The information in this topic applies to NetWitness Version 12.0 and later.

The **YARA Rules** tab lists the various YARA rules used for the scan and their status. To access this tab, select a host from the **Hosts** view and click the **YARA Rules** 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
Threat Hunter	perform external lookups	Launch an External Lookup for a File
Threat Hunter	change file status or remediate	Changing File Status or Remediate
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

*You can perform this task in the current view.

Related Topics

- Focusing on Endpoint Analysis
- Investigating Hosts

Quick Look

Below is an example of the YARA Rules tab:

	Investigate Respond Users H	osts Files Dashboard Reports	<u> </u>	ैं 🗷 % 🧿 ad	
100 🗹 🗄	AGENT SCAN STATUS AGENT LAST SEEN Idle a few seconds ago	AGENT VERSION SNAPSHOT TIME 09/16/2022 12:05:2	20 pm (Yara Scan) 🗸 Se	arch by filename, path or hash	٩
ALERTS PROCESSES AUTORUNS			HISTORY YARA RULES	2	
YARA RULE	STATUS				
Rules\all-yara-FireEye.yar	۷ لە	aded			
Rules\match-rule-yara-psr.yar	🗸 Lo	aded	← 3		

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, 12.0.0.0.

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.
- Perform remediation actions using the Remote Shell option. For more information, see <u>Performing Host Forensics</u>.

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 YARA Rules Panel Displays the following tabs:
 - YARA Rule: This tab lists all the YARA rules used for the scan.
 - **Status**: This tab displays the status of the YARA rules.

For Example: If the YARA rule is successfully loaded, the status is displayed as Loaded.

For more information on YARA Scans, see *Analyze Files Using YARA* section in Investigating Files topic.