NetWitness® Platform XDR

Version 12.1.0.0

NetWitness Endpoint User Guide

NETWITNESS
Platform XDR

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.

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.

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

October, 2022

Contents

Introduction to Endpoint Investigation **7**
- Endpoint Metadata 7
- Risk Score 9
  - Severity of Alerts 12
  - Global and Local Risk Score 12
  - Automated Incident Creation Based on Risk Score 13
- File Reputation 13
- File Status 13
- Remediation 14
- Network Isolation 14

Focusing on Endpoint Analysis **15**

Investigating Files **17**
- Best Practices 17
- View Files 18
- Filter Files 20
- Add and Sort Columns in the Table 20
- Analyze Files Using the Risk Score 21
- Analyze Hosts with File Activity 25
- Analyze Files Using YARA 26
- Analyze Files Using OPSWAT 31
  - Manual Scan - Scan selected files 32
  - Manual Scan - Scan all files 33
- Launch an External Lookup for a File 35
- Set Files Preference 36
- Export Global Files 37
- Analyze Certificates 38
  - Change the Certificate Status 39
  - Filter Certificates 40
- Resetting Risk Score of Files 40

Investigating Hosts **42**
- Best Practices 42
- View Hosts 43
- Manage Hosts Using Tags 44
  - Manage Tags 44
    - To Create Tags: 45

To Delete Tags: 46
Assign tags 47
Create and Assign Tags When Generating the Agent Packager 49
Unassign tags 52
What happens next after unassigning or deleting tags from hosts? 53
View Agent History 54
Filter Hosts 55
Adding and Sorting Columns in the Table 60
Scan Hosts 61
Standalone Scan on Air-gapped Windows Hosts 63
Standalone scan workflow: 64
Generate the scan configuration file 64
Install Endpoint Agent and Register for Standalone Scan 65
Start a Standalone scan 65
Upload the Standalone scan result file 66
Analyze Hosts Using the Risk Score 66
Analyze Host Details 71
Filter Host Details 71
Search Files on Host 72
Analyze Processes 73
Analyze Autoruns 76
Analyze Files 76
Analyze Libraries 76
Analyze Drivers 77
Analyze Anomalies 77
Analyze System Information 77
Analyze History 77
Export Host Details or Files to JSON File 78
Launch an External Lookup for a File 79
Delete a Host 80
Deleting Hosts with Older Agent Versions 80
Set Hosts Preference 81
Export Host Attributes 81
Migrate Hosts 82
Analyzing Risky Users 82
Resetting Risk Score of Hosts 83
Investigating a Process 86
Best Practices 86
Analyze a Process 87
Analyze Events for a Process 92

Changing File Status or Remediate **94**
Import File Hashes using the Block Hash tool 96
JSON File Format 96
Analyzing Downloaded Files **99**
Download Files to Server 99
Save Downloaded Files 101
Analyze Downloaded Files 101
Performing Host Forensics **104**
Download Master File Table 104
Analyze Downloaded MFT 106
System and Process Memory Dump 108
Download Files Using Full Path or Wildcard 110
Filter Downloaded Files 113
Save Downloaded File 113
Delete Downloaded Files 114
Analyzing Events **115**
Analyze Events from Files View 115
Analyze Events from Hosts View 115
Text Analysis for an Endpoint Event 116
Isolating Hosts from Network **118**
Edit Exclusion List 119
Release Isolated Hosts 120
NetWitness Endpoint with Third-Party Antivirus Products **122**
Troubleshooting NetWitness Endpoint **123**
General Issues 123
Multi-server Issue 124
Hosts View Issues 124
Files View Issues 125
Policy Issue 125
Driver Issue 126
Download Issue 126
File Reputation Service Issue 126
Risk Scoring for Hosts or Files Issue 126
Endpoint Broker/Server Issue 127
NetWitness Endpoint Reference Materials **129**
Files View 130
File Details View 132
Hosts View 134
Hosts View - Details Tab 138

Hosts View - Process Tab 143
Process Details 147
Hosts View - Autoruns Tab 148
Hosts View - Files Tab 152
Hosts View - Drivers Tab 156
Hosts View - Libraries Tab 160
Hosts View - Anomalies Tab 164
Image Hooks 168
Kernel Hooks 168
Suspicious Threads 169
Registry Discrepancies 169
Hosts View - Downloads Tab 170
MFT Viewer 174
Hosts View - System Information Tab 177
System Information Panel 179
Hosts View - Agent History Tab 181
Hosts View - YARA Rules Tab 182

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 Netsh helper 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 platforms.
		  • Reports IPv4 and IPv6 connections.
		• Console event (for 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.local`.
		Commands executed by `cmd.exe`, `powershell.exe` as a result of inter-process communication through anonymous pipes are captured and reported with the context `console.remote`.

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	-

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 system.
		  • Reports IPv4 and IPv6 connections.

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

Risk Score

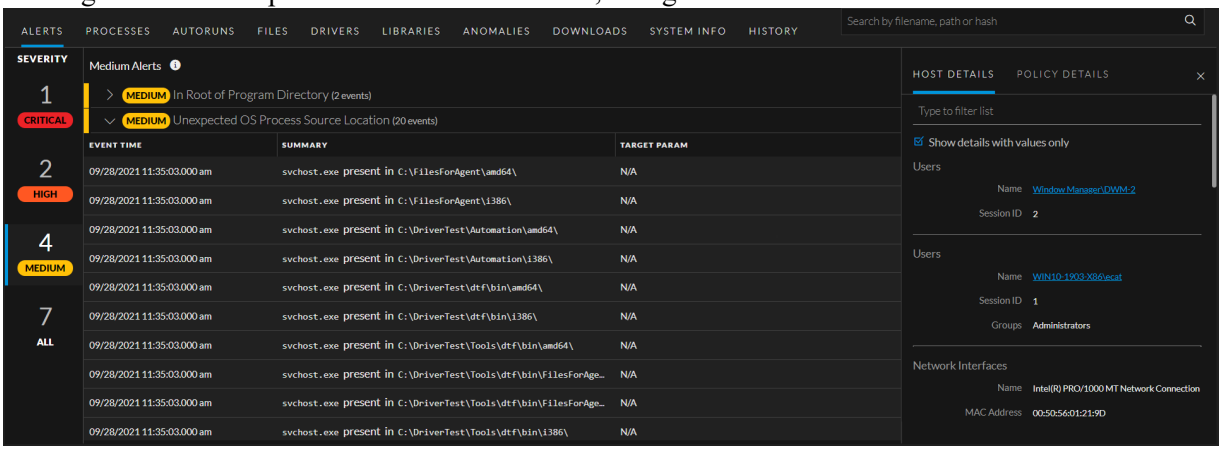
Analysts can use the risk score to begin an investigation on hosts and files. NetWitness uses a proprietary algorithm to calculate the risk scores ranging from 0 to 100. A subset of alerts associated with hosts and files contribute to the risk score calculation. Analysts can review critical and high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

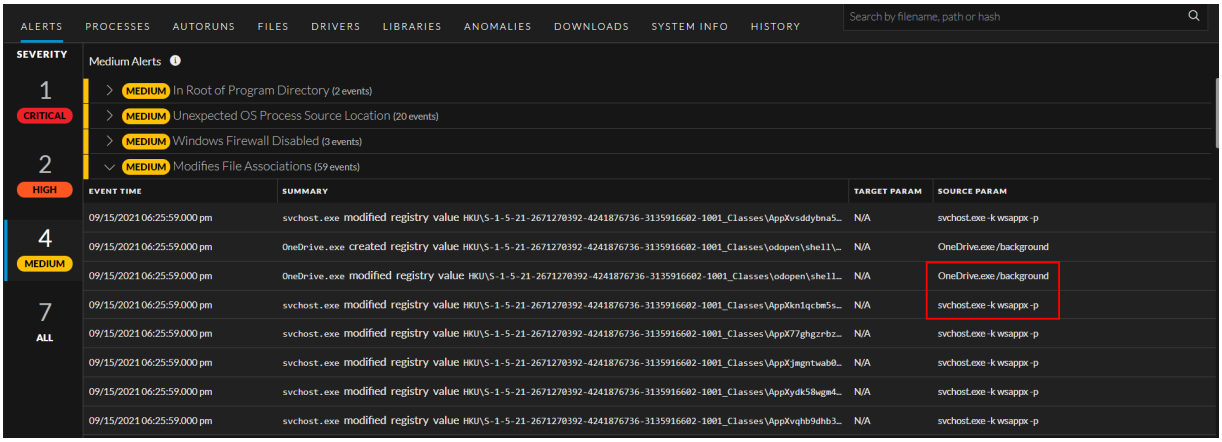
The following factors contribute to the risk score:

- **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.

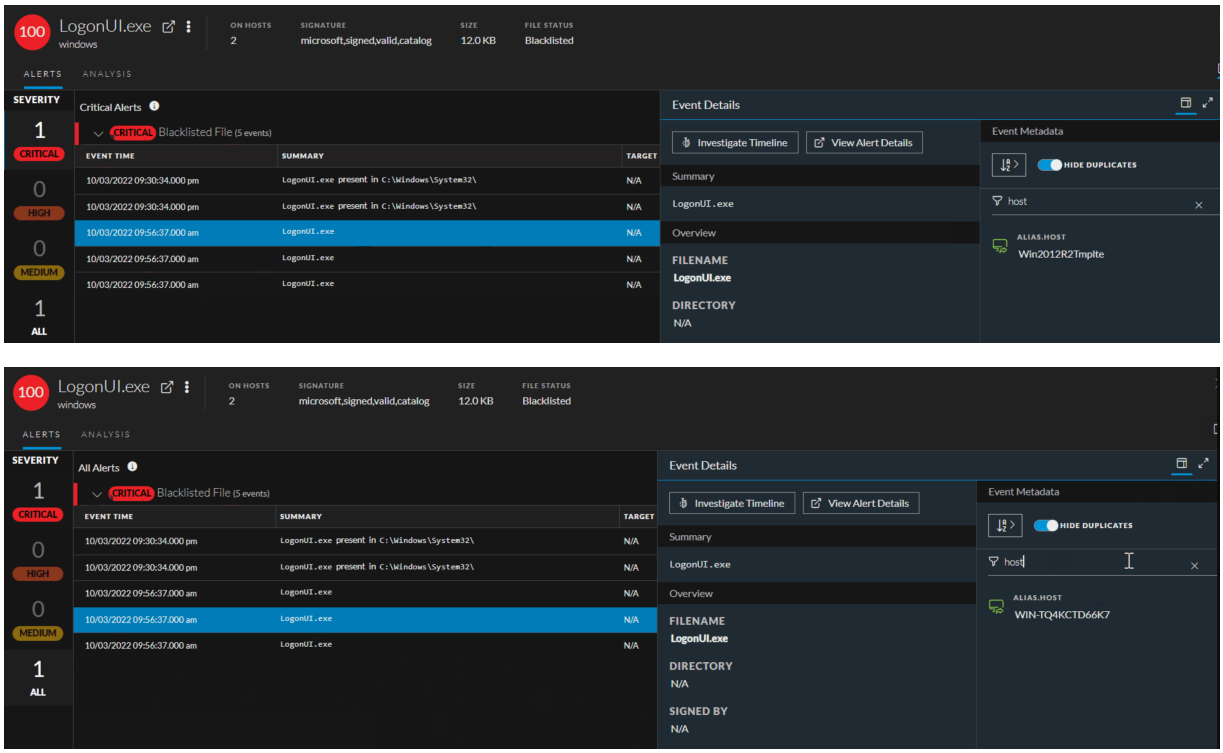
  This figure is an example of a host with 1 Critical, 2 High and 4 Medium distinct alerts.



  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`.



  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.



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 Changing File Status or Remediate.

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

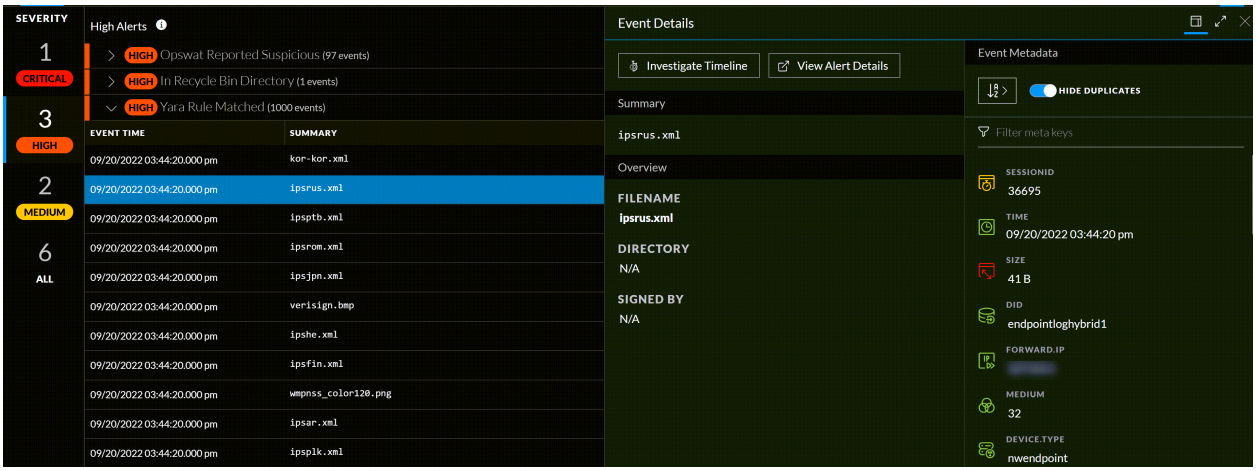
Note: For the accurate risk score calculation, the default multi-valued meta keys are required on the ESA Correlation service. For more information, see "Configure Meta Keys as Arrays in ESA Correlation Rule Values" section in the *ESA Configuration Guide*.

Severity of Alerts

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

Severity	Color	Risk Score Range
Critical	Red	100
High	Orange	70-99
Medium	Yellow	31-69
Low	Green	0-30

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



In the above example, there are three distinct 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 Analyze Hosts Using the Risk Score and Analyze Files Using the Risk Score.

Global and Local Risk Score

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

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

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

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

Automated Incident Creation Based on Risk Score

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

File Reputation

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

The reputations for a file hash are:

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

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

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

File Status

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

A file can be classified as follows:

- Blacklist: File that is marked suspicious, such as when ransomware is found by scan.
- Graylist: File that is marked for a later review.

- Whitelist: File that is legitimate and is not to be considered for risk scoring.
- Neutral: Default status.

For more information, see Changing File Status or Remediate.

Remediation

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

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

You can block files with the following file extension: EXE, COM, SYS, DLL, SCR, OCX, BAT, PS1, VBS, VBE, and VB. For more information, see Changing File Status or Remediate.

Network Isolation

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

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

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

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

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

For more information, see Isolating Hosts from Network.

Focusing on Endpoint Analysis

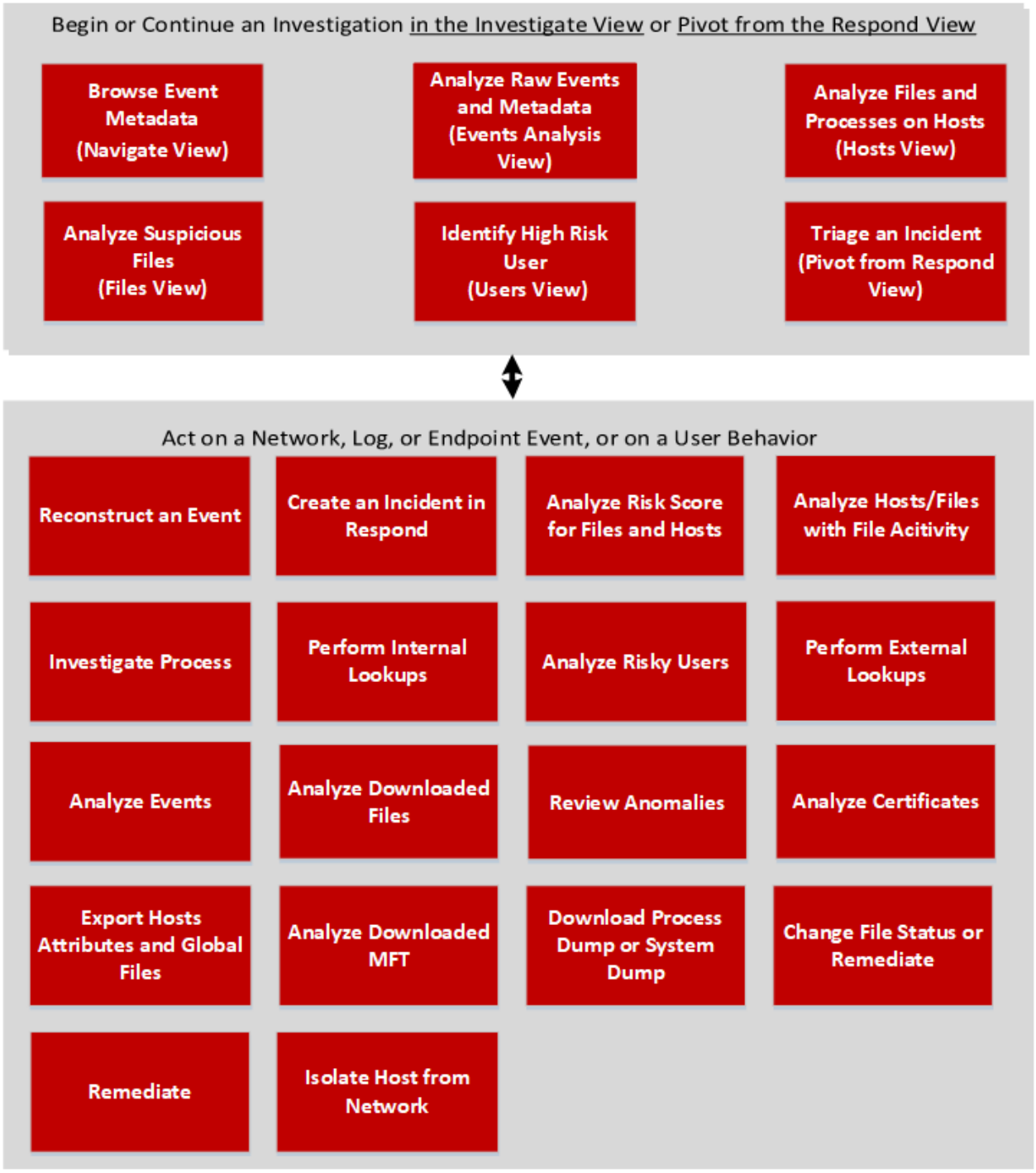
This guide provides the information needed to conduct an investigation that is focused on endpoint data from configured hosts. Analysts who conduct analysis using Investigate need to have the appropriate system roles and permissions set up for their user accounts. An administrator must configure roles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

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

You can begin the investigation on files in your deployment in the Files view (**Files**). (See Investigating Files.)

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

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


Begin or Continue an Investigation in the Investigate View or Pivot from the Respond View
Browse Event Metadata (Navigate View)
Analyze Raw Events and Metadata (Events Analysis View)
Analyze Files and Processes on Hosts (Hosts View)
Analyze Suspicious Files (Files View)
Identify High Risk User (Users View)
Triage an Incident (Pivot from Respond View)
Act on a Network, Log, or Endpoint Event, or on a User Behavior
Reconstruct an Event
Create an Incident in Respond
Analyze Risk Score for Files and Hosts
Analyze Hosts/Files with File Acitivity
Investigate Process
Perform Internal Lookups
Analyze Risky Users
Perform External Lookups
Analyze Events
Analyze Downloaded Files
Review Anomalies
Analyze Certificates
Export Hosts Attributes and Global Files
Analyze Downloaded MFT
Download Process Dump or System Dump
Change File Status or Remediate
Remediate
Isolate Host from Network

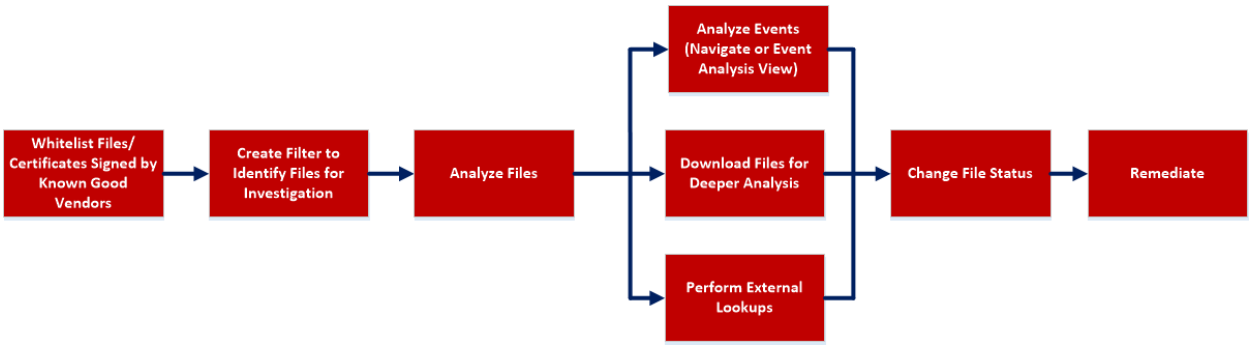
Investigating Files

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 Filter Files and Changing File Status or Remediate.

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

- Change the status of certificate and the associated files automatically. For more information, see Analyze Certificates.
- Filter to exclude whitelisted, files with valid signature, known good files based on reputation status. For more information, see Filter Files.
- Lookup Google or VirusTotal with the filename or hash to get more information about a suspected file. For more information, see Launch an External Lookup for a File.
- Analyze the files using one or more of these indicators:

  a. Risk score - Displays the risk score for a file. Analysts can view the associated alerts and events for further investigation. For more information, see Analyze Files Using the Risk Score.

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

c. File status - To manage suspected and legitimate files, analysts can use the file status to manage. For more information on the various file status, see Changing File Status or Remediate.

d. Reputation status - Indicates the reputation of a file hash for analyst to narrow-down the files to investigate. For more information, see File Reputation.

e. Signature - A valid signature on a file signed by a trusted vendor, such as Microsoft and Apple indicates that the file is not a risk. If a file is unsigned, it may be malicious, and needs investigation.

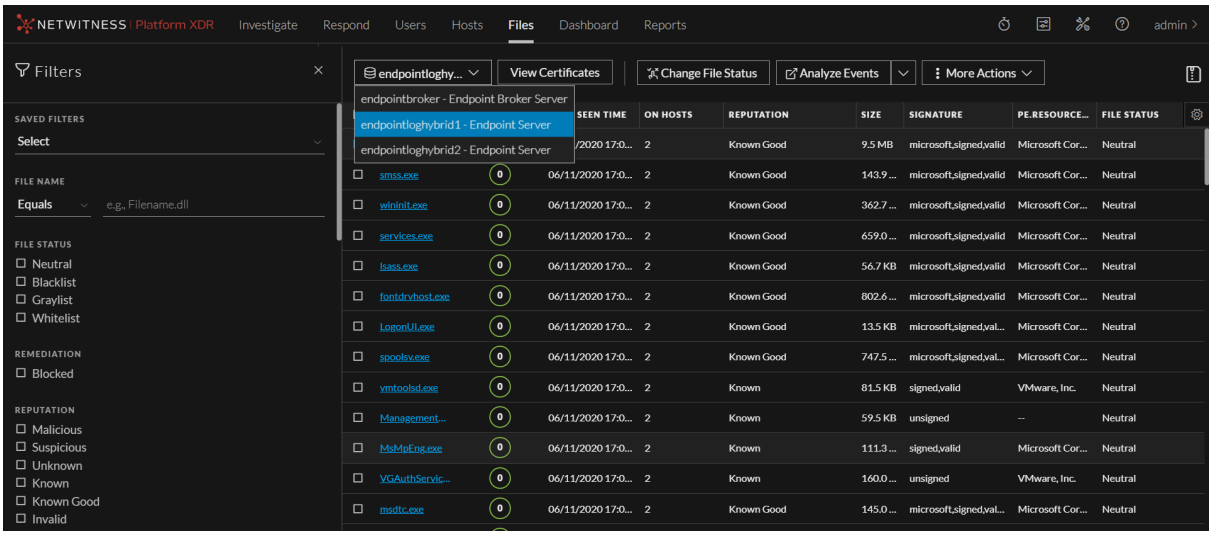
f. File name - Many trojans write random file names when dropping their payloads to prevent an easy search across the hosts in the network based on the filename. For example, if a file is named `svch0st.exe`, `scvhost.exe`, or `svchosts.exe`, it indicates that the legitimate Windows file named `svchost.exe` is being mimicked.

- Investigate a particular file name or hash by pivoting to Navigate or Events view to view context, file activity on different hosts, and any file transfers across the network through packet data. For more information, see Analyzing Events.
- 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 Analyze Files Using YARA.
- Download suspicious files to the server for deeper analysis. For more information, see Analyzing Downloaded Files.
- Change the status of the file (blacklist or graylist), and block an infected or malicious file. For more information, see Changing File Status or Remediate.

View Files

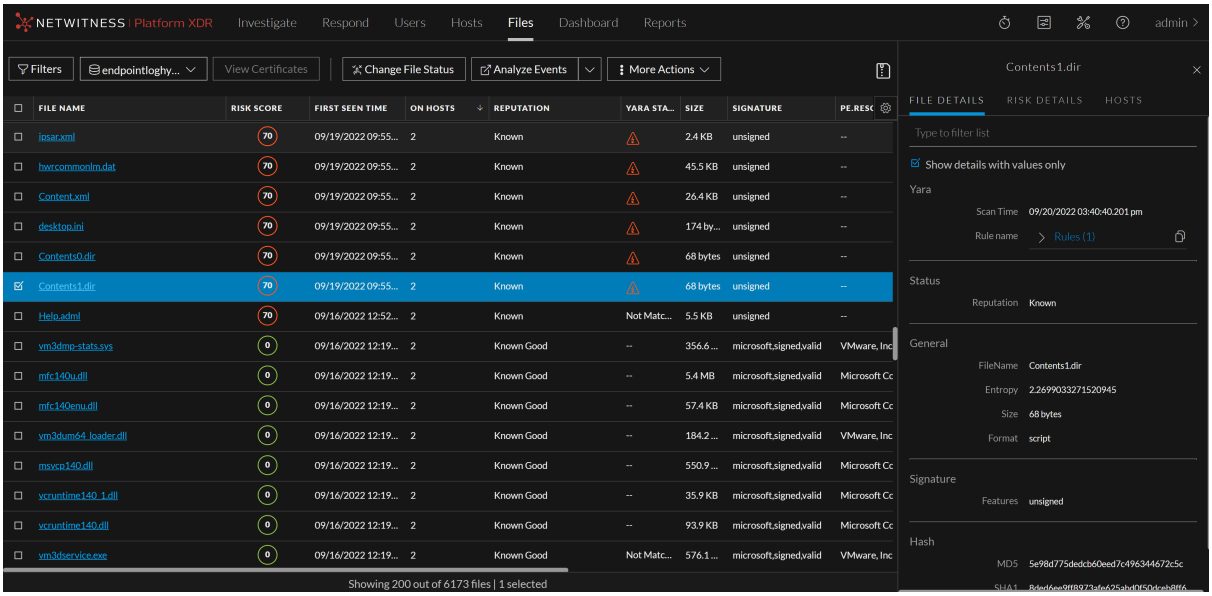
You can view all files present on a specific Endpoint server or consolidated list of all files on multiple Endpoint servers using the Endpoint Broker for analysis. To view files:

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



- **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:



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

Filter Files

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

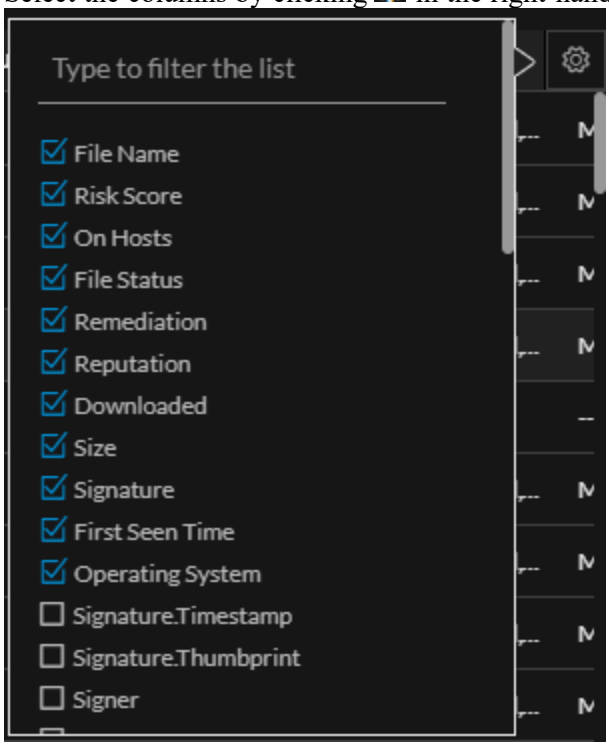
For example, to filter the files based on file reputation, select the reputation status in the Filter panel.

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 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 Investigating a Process.
- **Analyze Process Tree**: This option allows you to analyze the files associated with **Medium** alerts. For more information, see Investigating a Process.

To analyze files associated with Critical and High alerts using the risk score:

1. Go to **Files**.

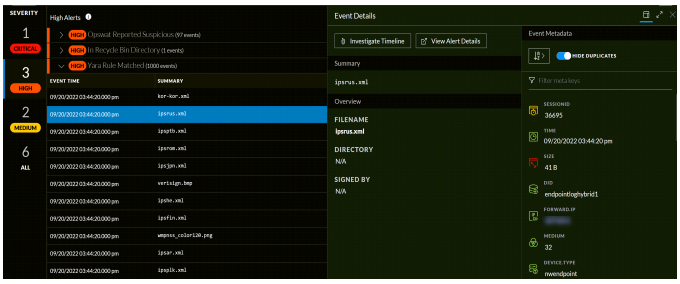
   The **Files** view is displayed.
2. In the Server drop-down list, select the Endpoint server or Endpoint Broker server to view the files.
3. Select the file and do any of the following.
   - Click a row to view the risk associated with the file in the **Risk Details** panel.
   - Click the filename to view the associated alerts and events.

The **Alerts** tab is displayed.

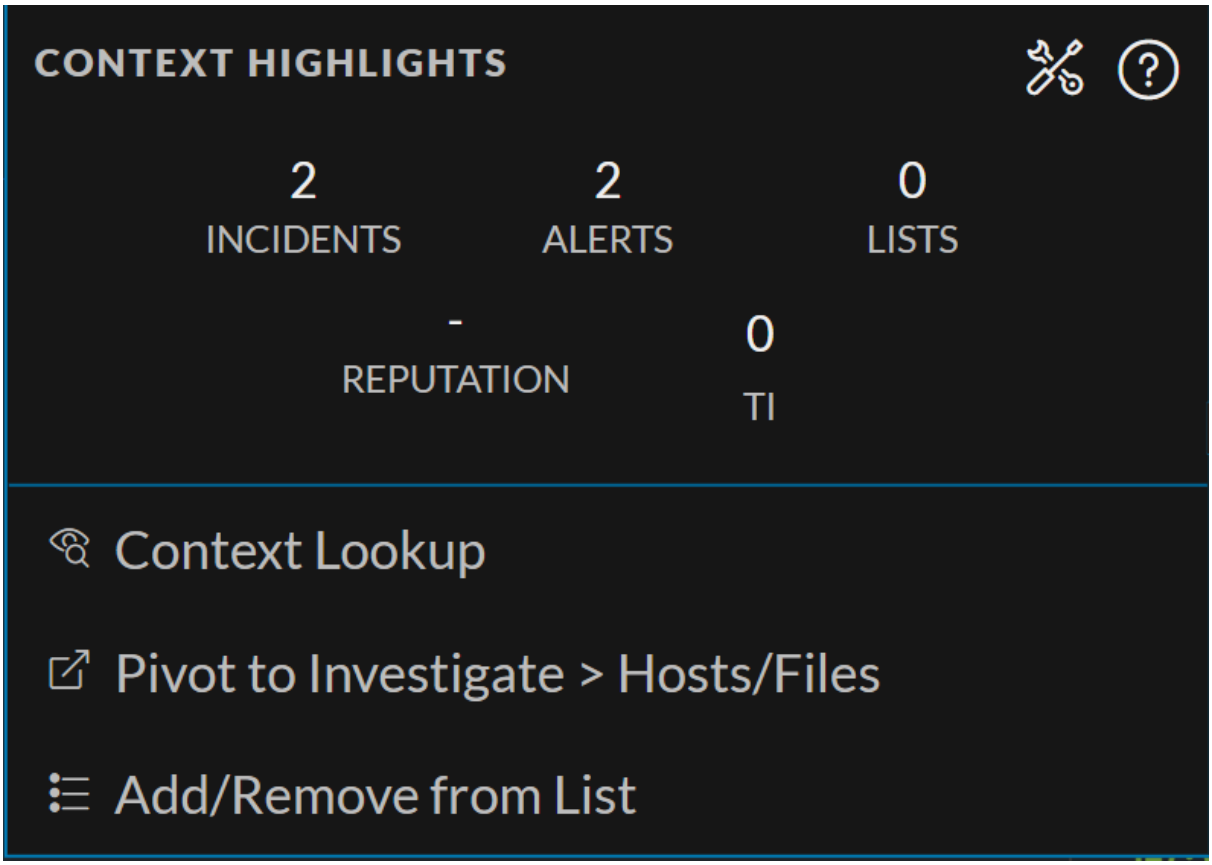
4. In the **Alerts** > **Severity** panel, click the alert severity, such as **Critical** or **High**.
   The list of distinct alerts is displayed along with the total number of events associated with the alert.
5. Click an alert to view the associated events.

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

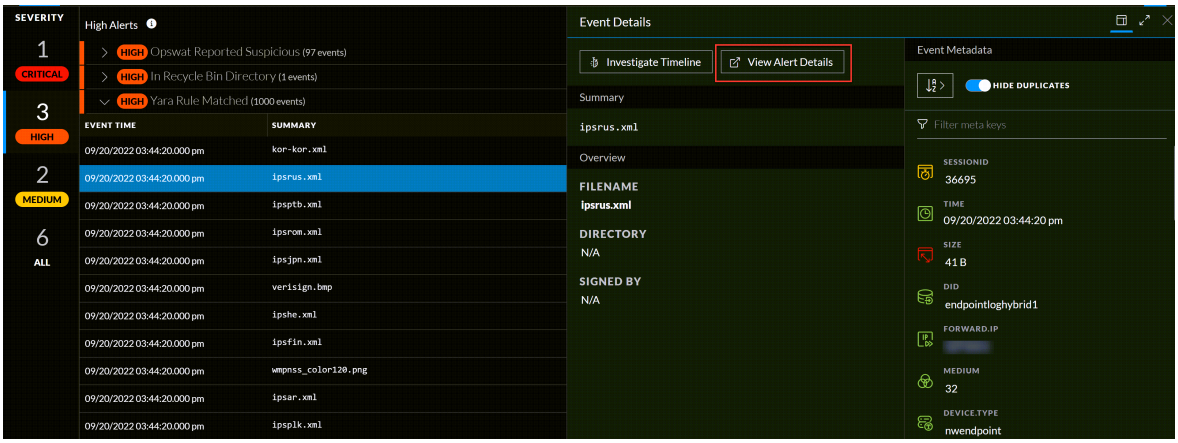
6. To view all the details associated with a specific event, click on an event. The **Event Details** panel is displayed with the summary and overview information associated with the event.



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 **View Alert Details** on the **Event Details** panel. For more information on process analysis, see Investigating a Process.



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.

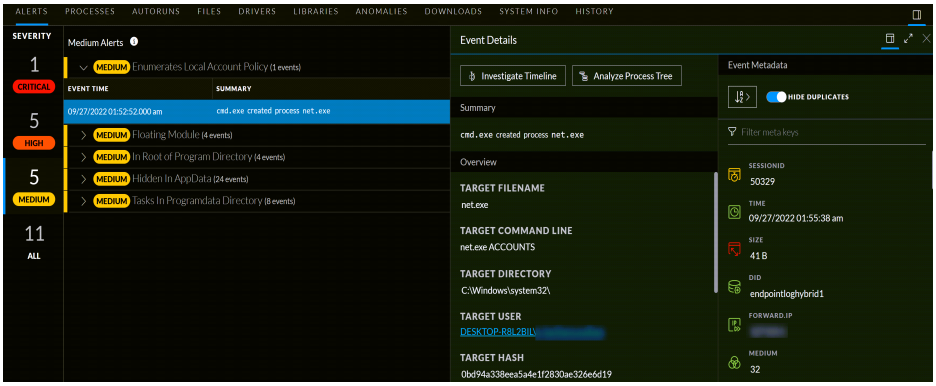
     The **Alerts** tab is displayed.

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.

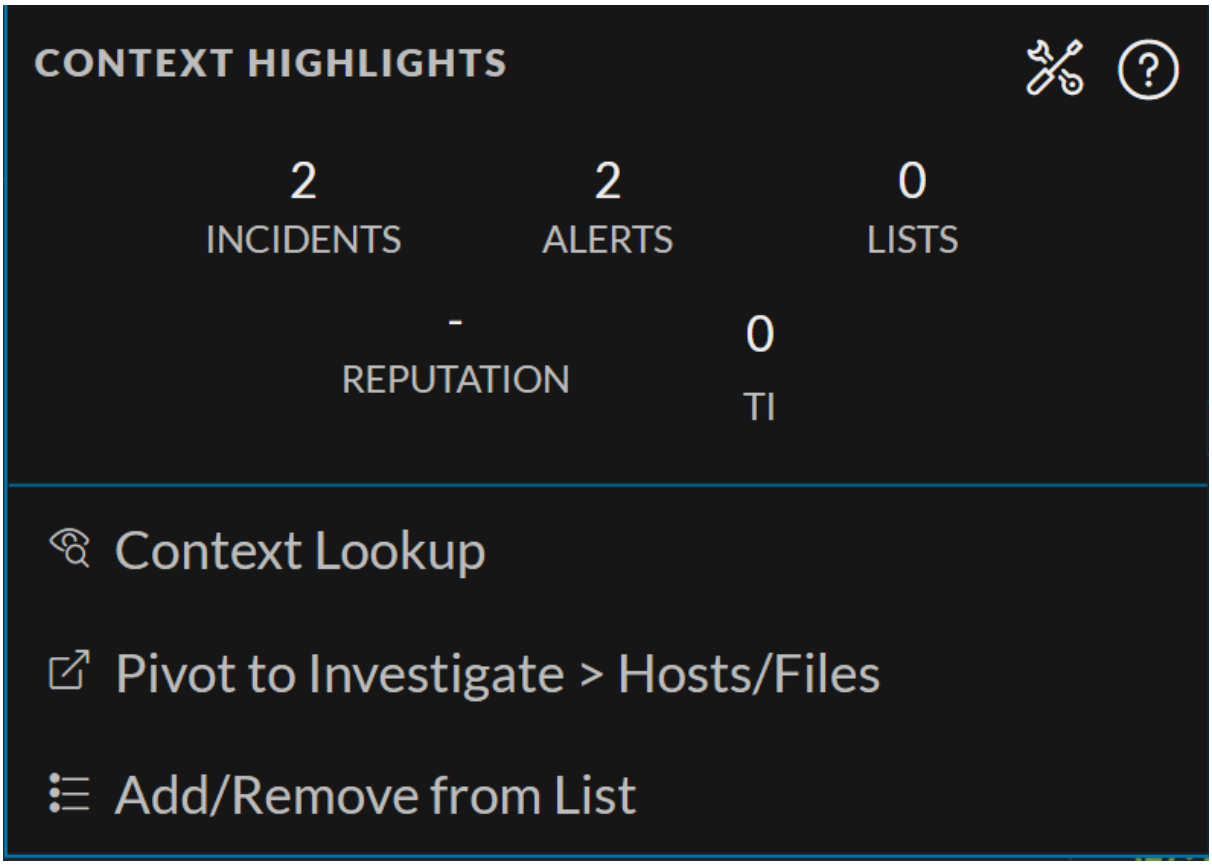
   Note: For each alert, only the latest 1000 events are displayed.

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.

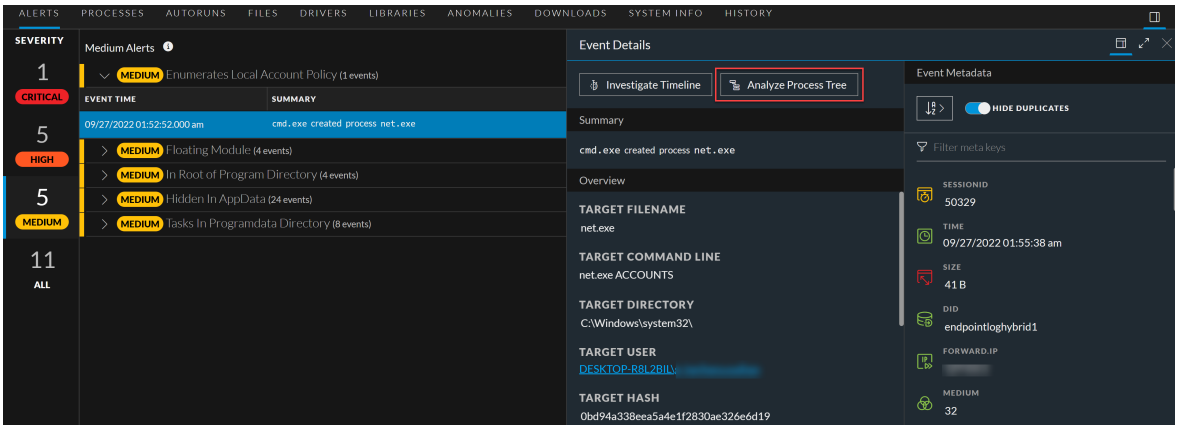


7. You can also view the Event Metadata such as IP, Filename, File hash, and Category in the **Event Details** panel.

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 Investigating a Process.

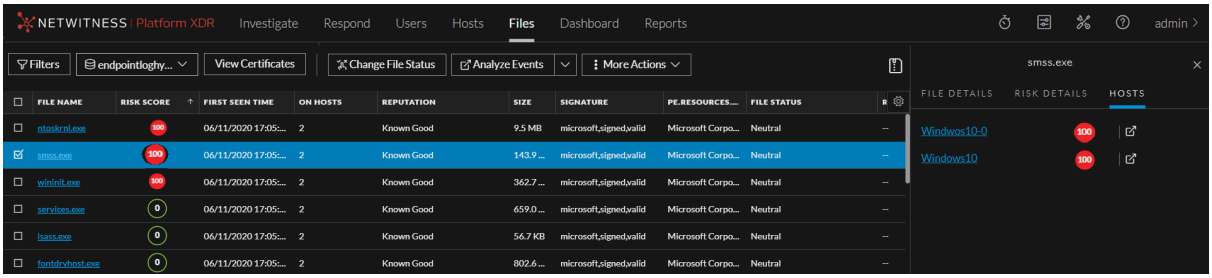


Analyze Hosts with File Activity

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.



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 Analyzing 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.

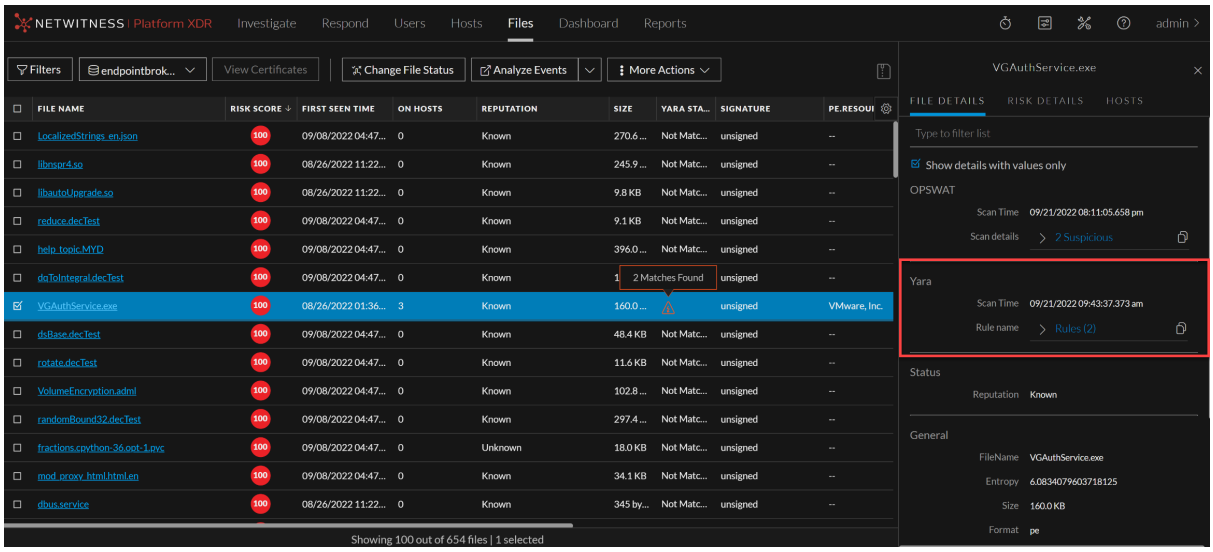
To analyze the scanned files,

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

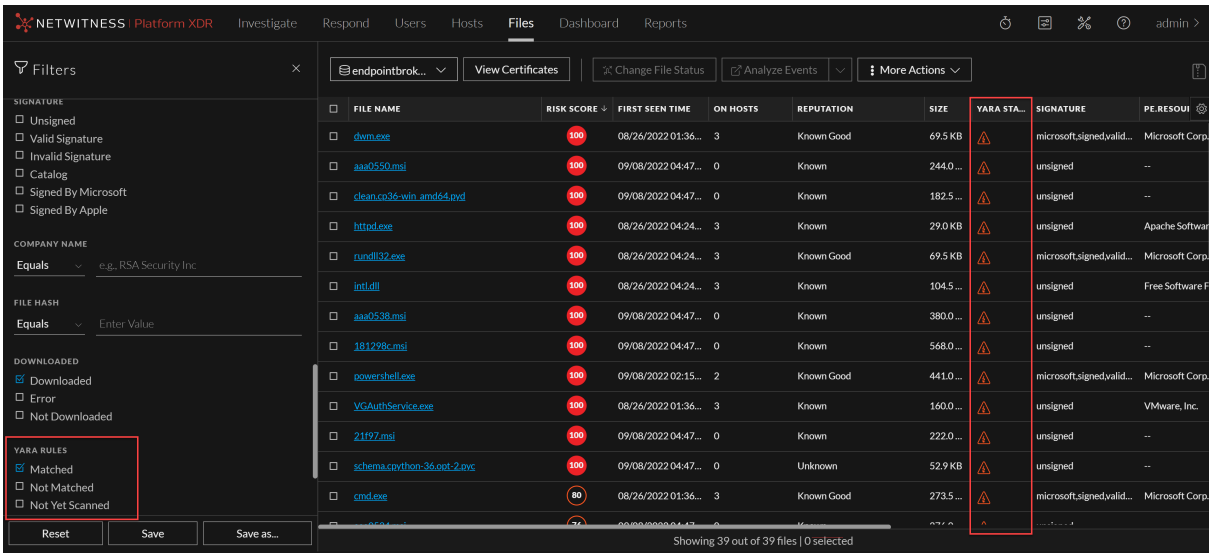
- **Matched** - The file matches with one or more YARA rules
- **Not Matched** - The file does not match with any of the YARA rules
- **Not Yet Scanned** - There is no scan performed for this file. Files will be scanned automatically once they have been downloaded. After the scan YARA status will be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



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.



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

Yara Scan at the Endpoint Agent Level

NetWitness Platform XDR 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:

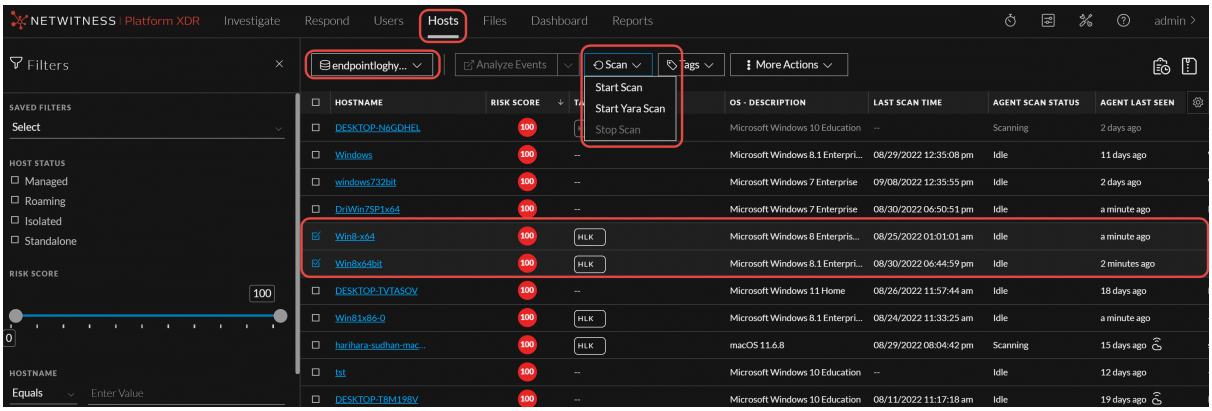
- List of files matching the YARA rules.
- List of YARA rules ran during the scan and the YARA rules status such as Loaded or Failed to load.

  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**.



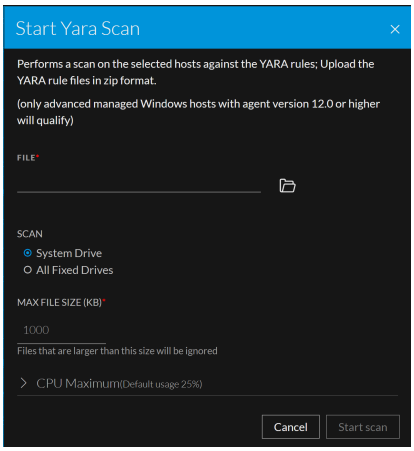
4. On **Start Yara Scan** pop-up,

   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.

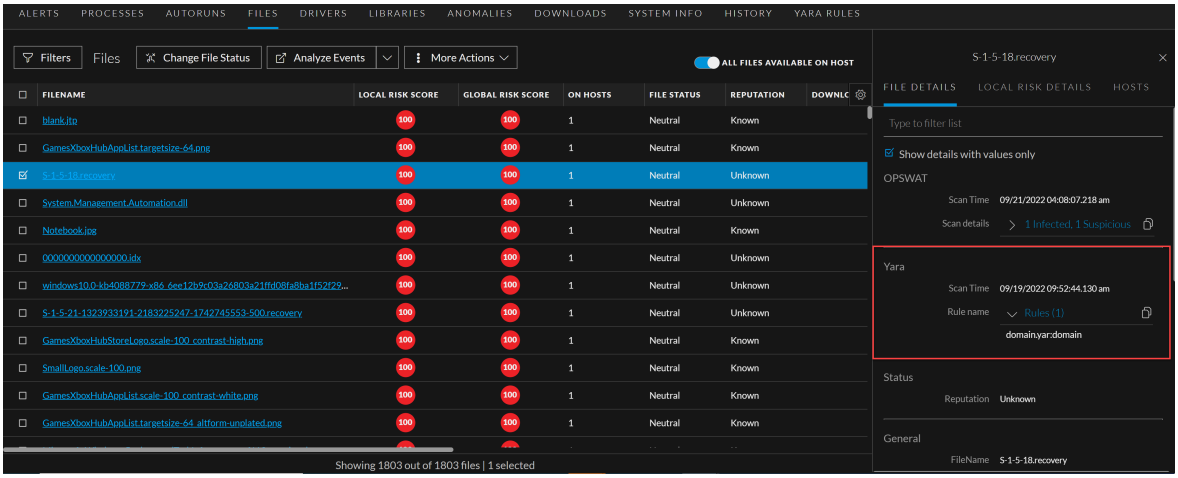


5. Click **Start scan**. See the command status In the **Host** > **History** tab.

To analyze the scanned hosts and files:

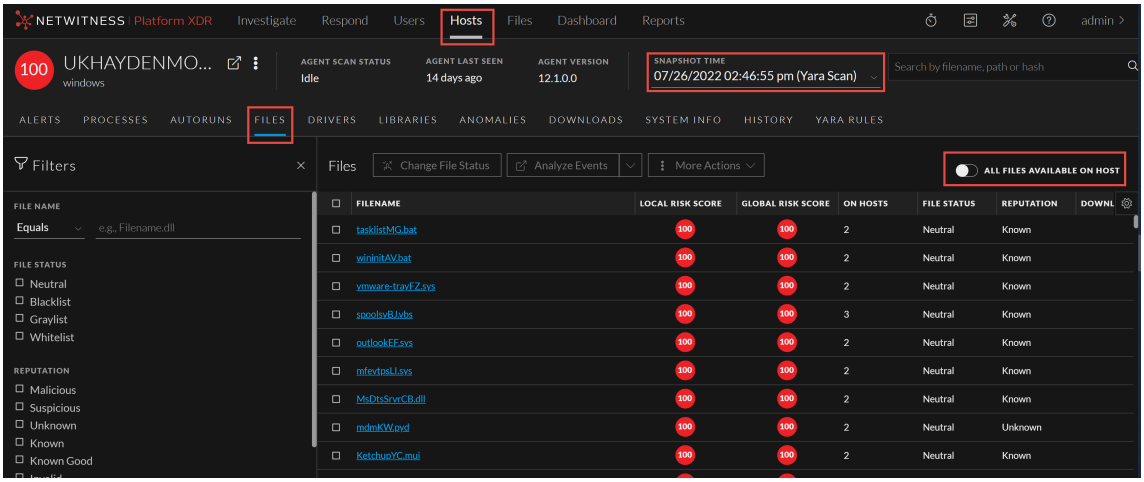
1. Log in to the NetWitness Platform XDR.
2. Click **Hosts**.
3. Select the Endpoint server from the server drop-down to view hosts.
4. Select the **Host** and **YARA Snapshot Time**, and do any of the following:
   - In the Host details view, click **Files** and select a row to view the YARA scan details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

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

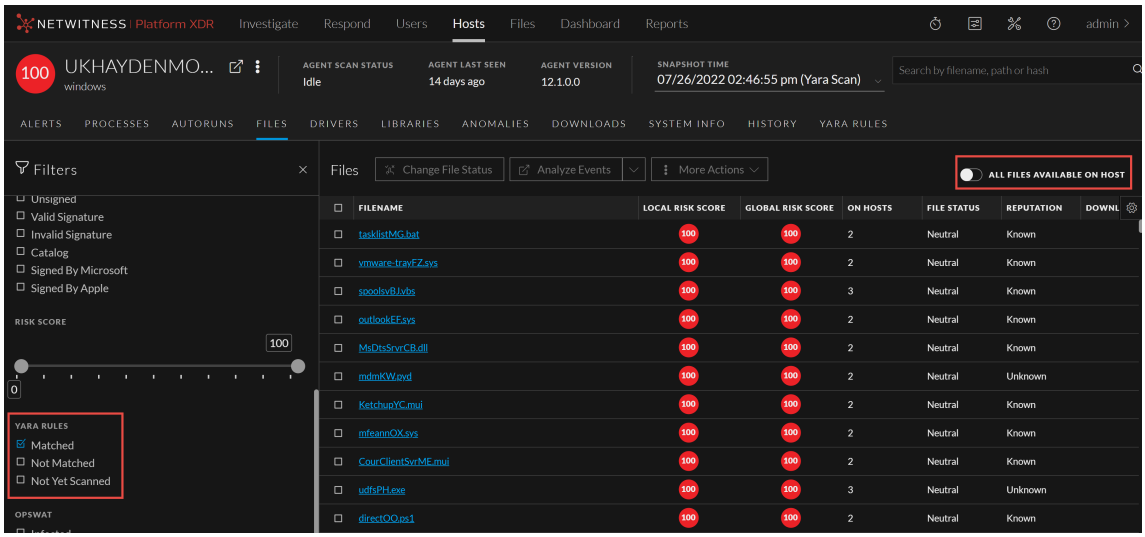


- Toggle the **All Files Available on Host** to view all the files irrespective of the snapshot selected.

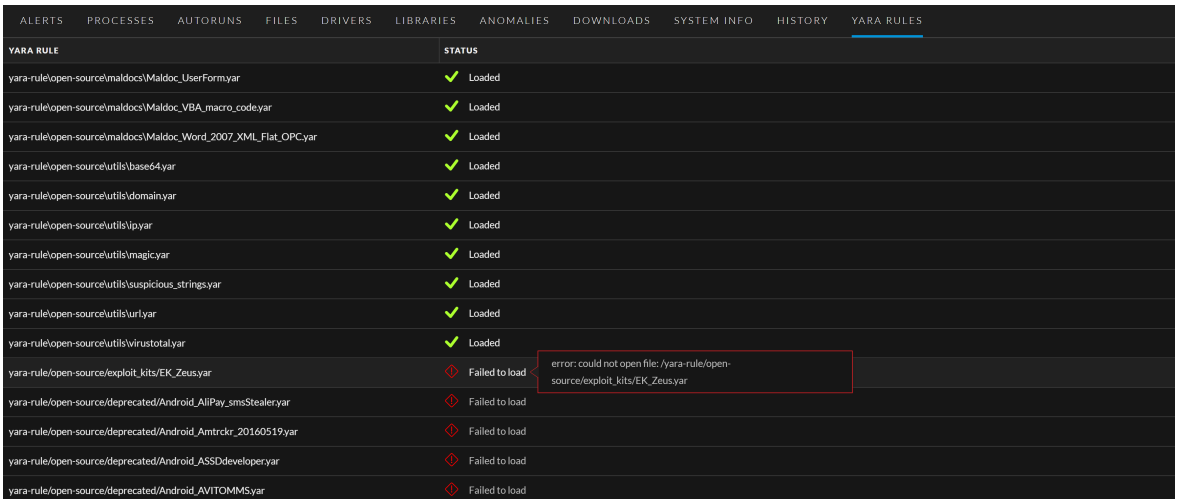
Note: When a file matches with a YARA rule, high severity alerts are triggered and the file's risk score is updated.



- 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.



- 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.

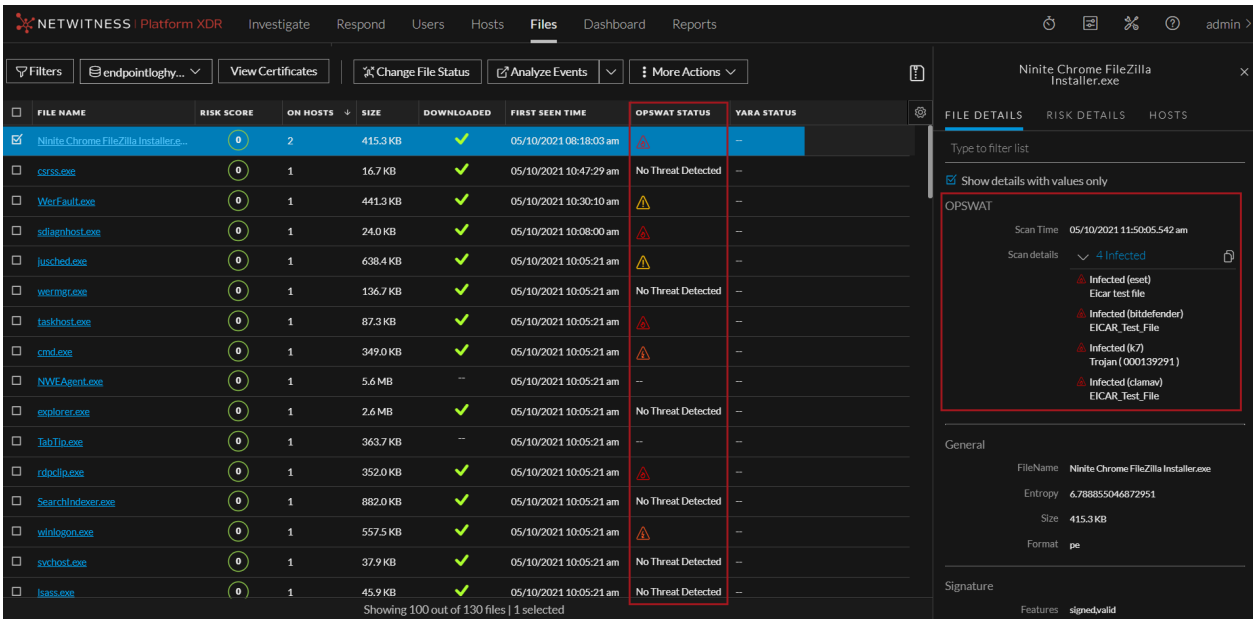


- In the Host details view, click the **History** tab to view the command history.

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.



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.

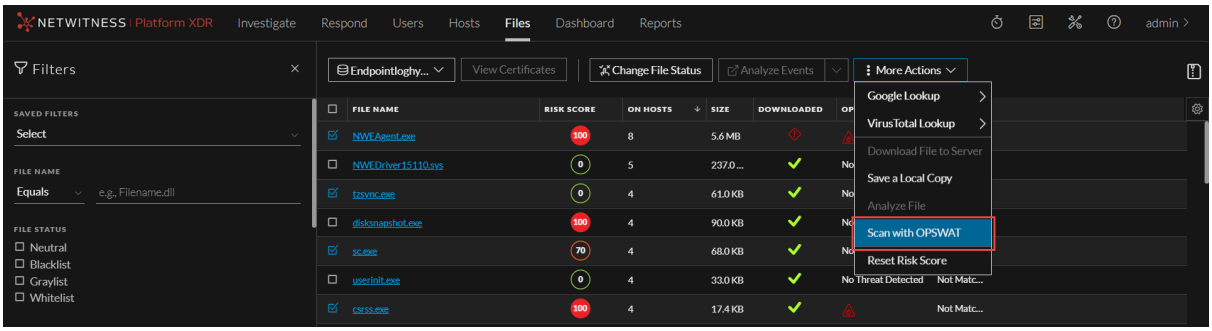
Manual Scan:

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

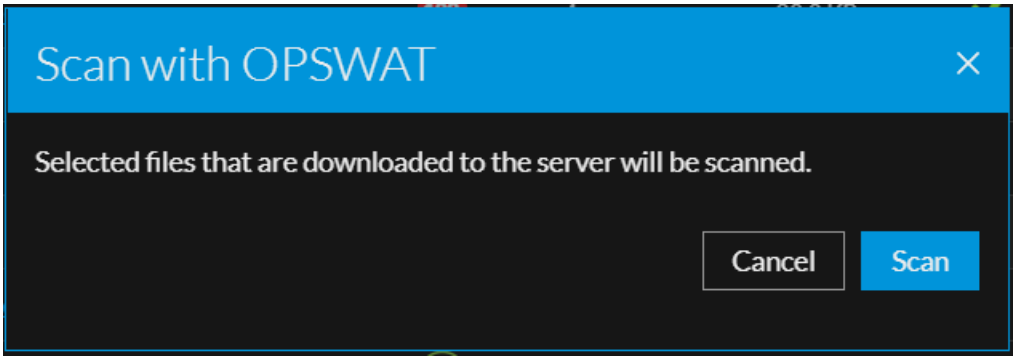
The **More Actions** menu provides the following options:

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**.

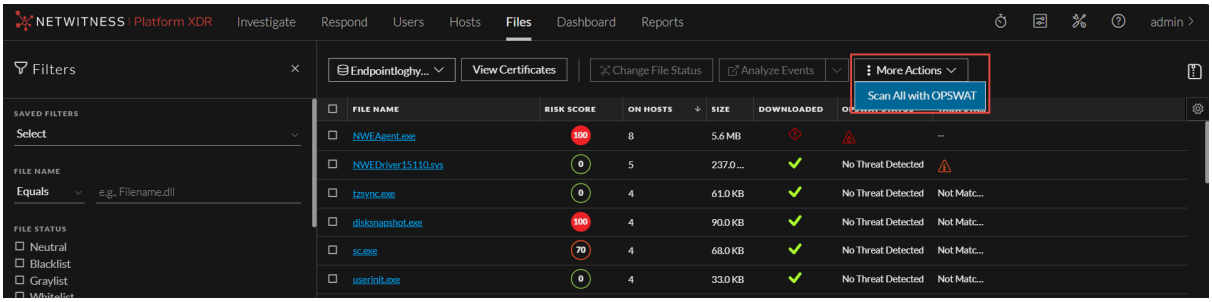


3. Click **Scan** on the confirmation pop-up.

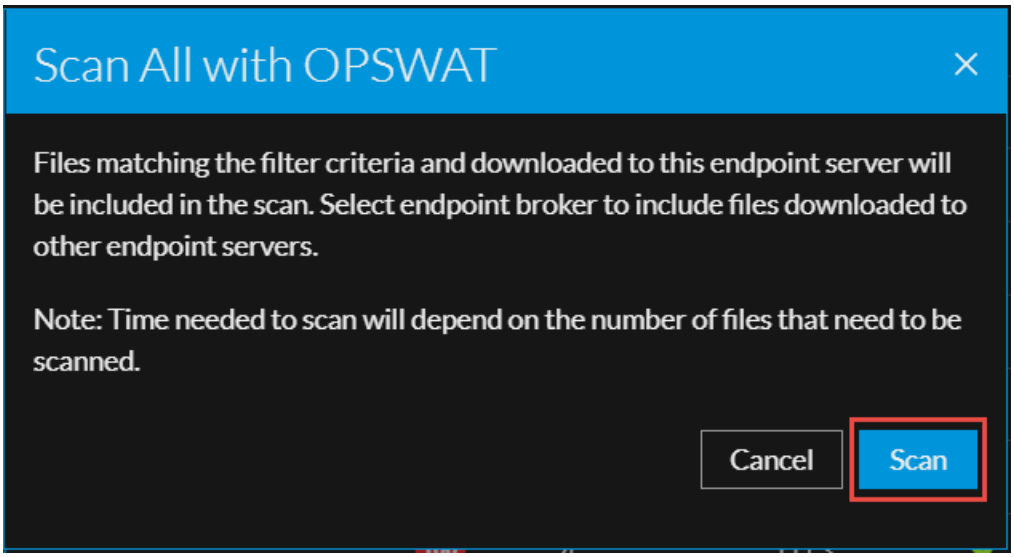


Manual Scan - Scan all files

1. Select **More Actions > Scan All with OPSWAT**.



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

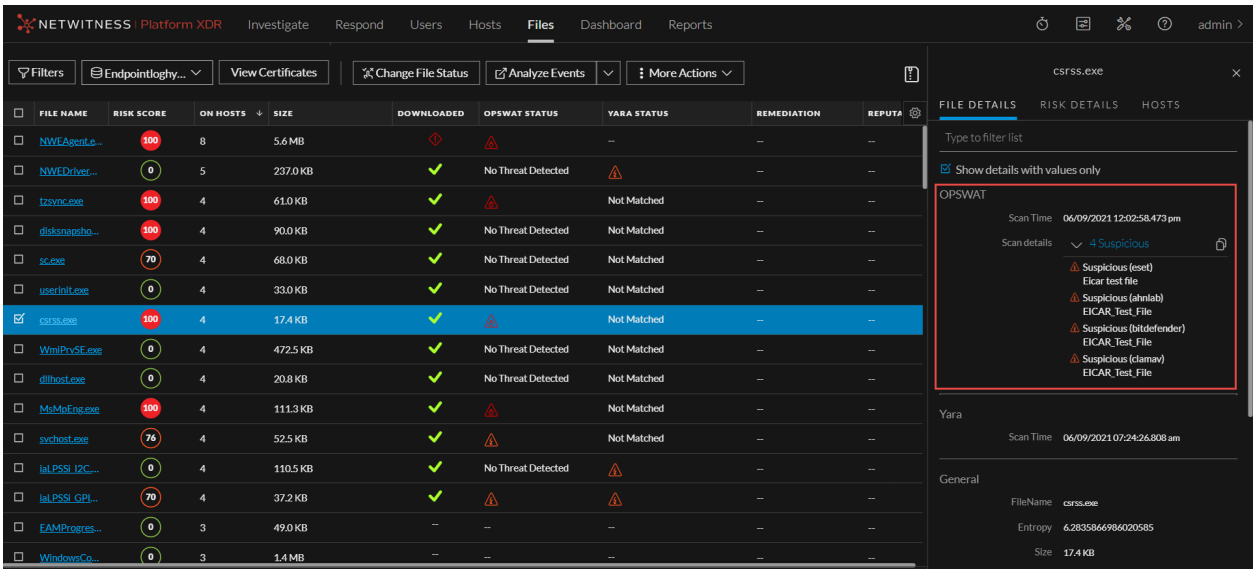
- Scan failed; see troubleshooting section for more information.

- 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.

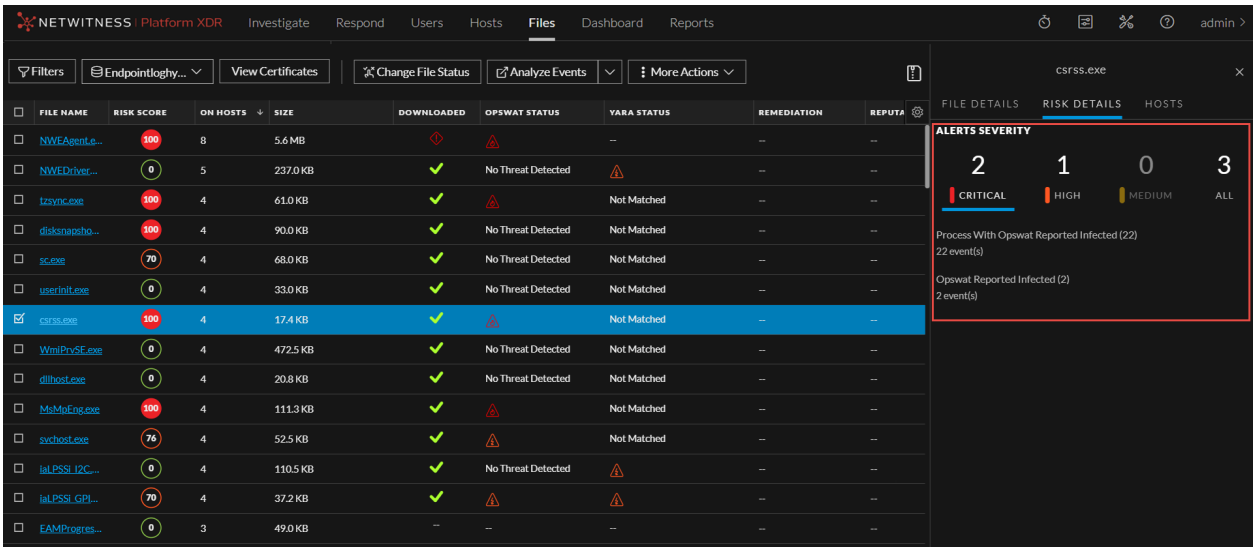
- **Scan Time**: States the last scanned time.
- **Scan details**: States whether a file is infected or suspicious or no threat detected, names of anti-malware engines that identified the threat.



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.

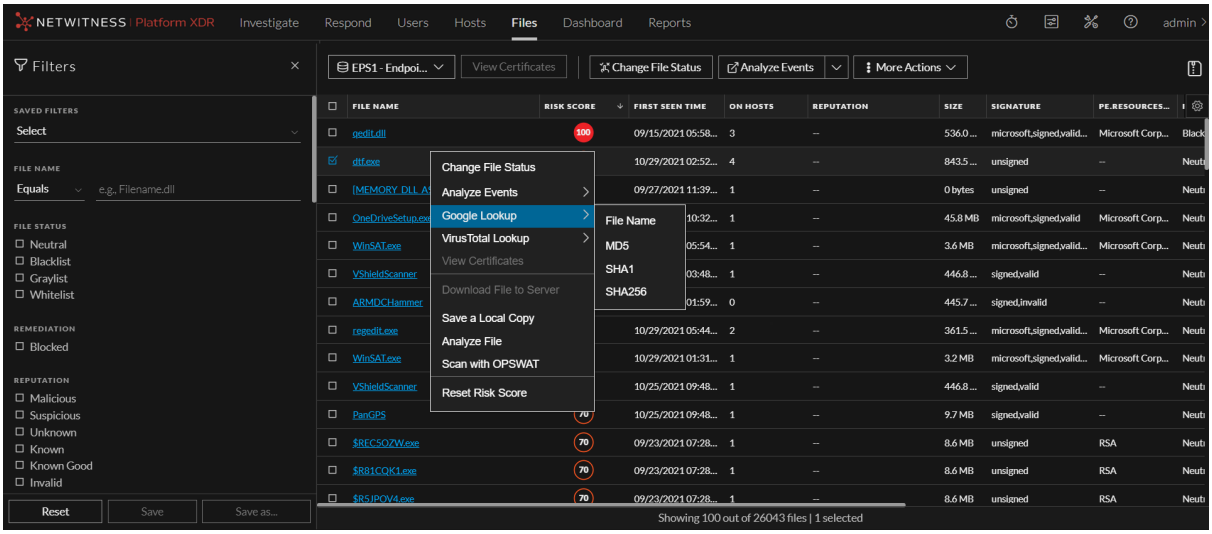
Risk score: If a file is found infected or suspicious by OPSWAT, the risk score of that file and the corresponding host will be increased.



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:



   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.

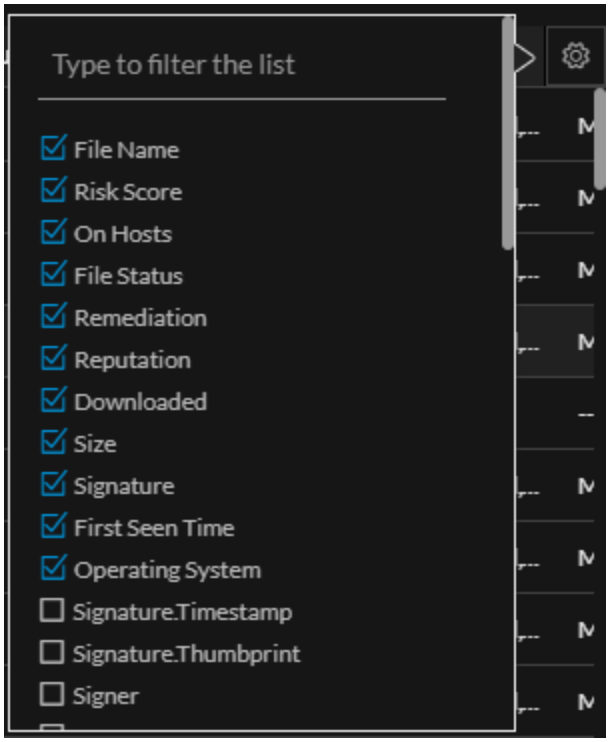
Note: To open files in multiple tabs, make sure you enable the pops-up in the browser.

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 drop-down list displayed while adding columns:



3. Sort the data on the required column.

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

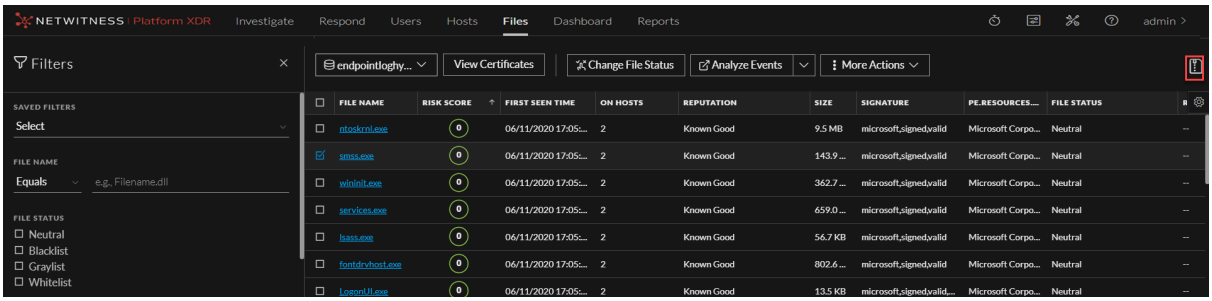
Export Global Files

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

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

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

4. Click to export the files to a csv file.



You can either save or open the CSV file.

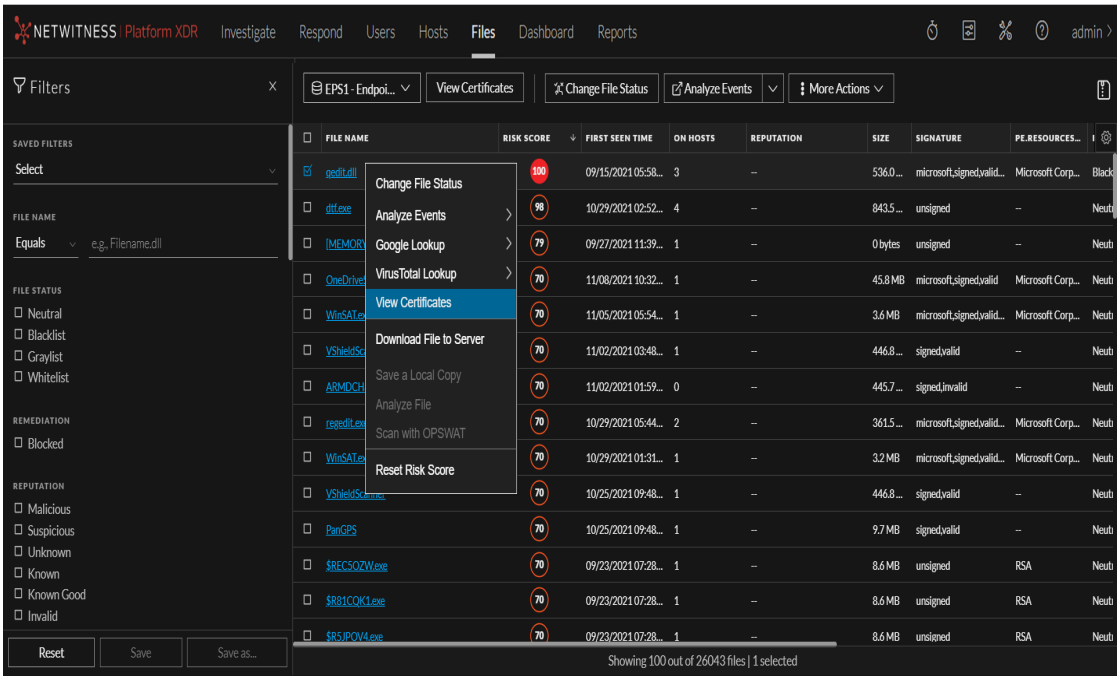
Analyze Certificates

Note: The information in this topic applies to 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:



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

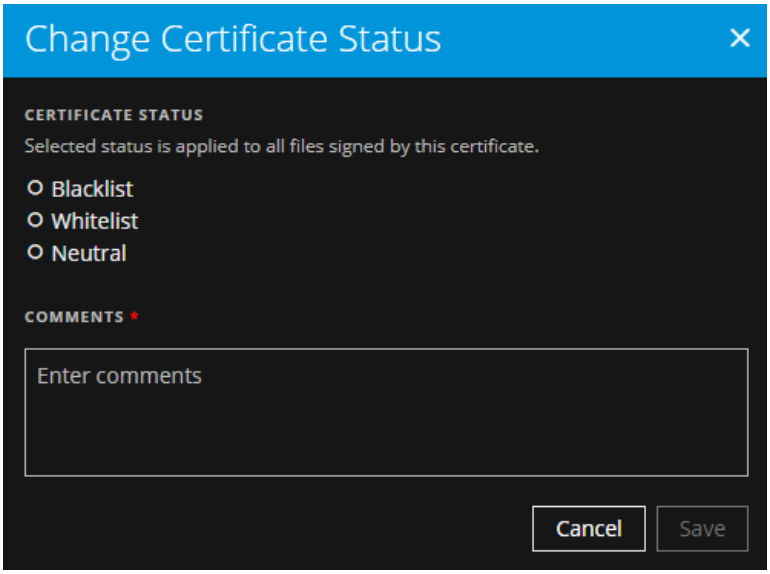
Change the Certificate Status

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**.



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

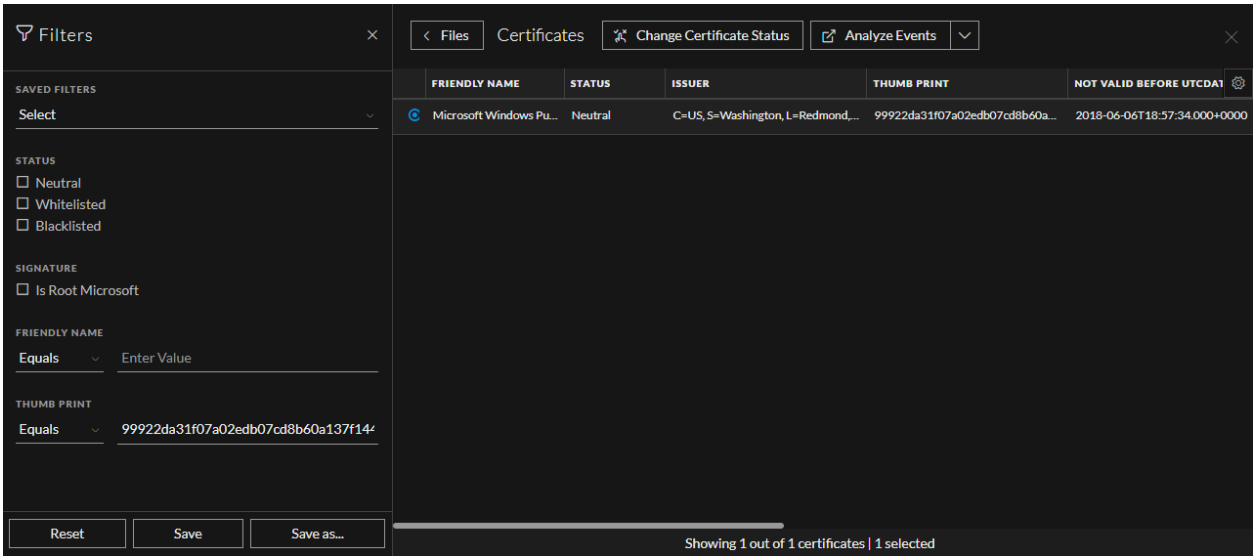
   Note: If you have manually updated a file status in the Files or Hosts view, changing the status in the Certificate view does not impact the file status as the manual update takes precedence. For example, if you have whitelisted the file vmci.sys that is signed by VMware, Inc. in the Files or Hosts view,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

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

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

Filter Certificates

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



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

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

Resetting Risk Score of Files

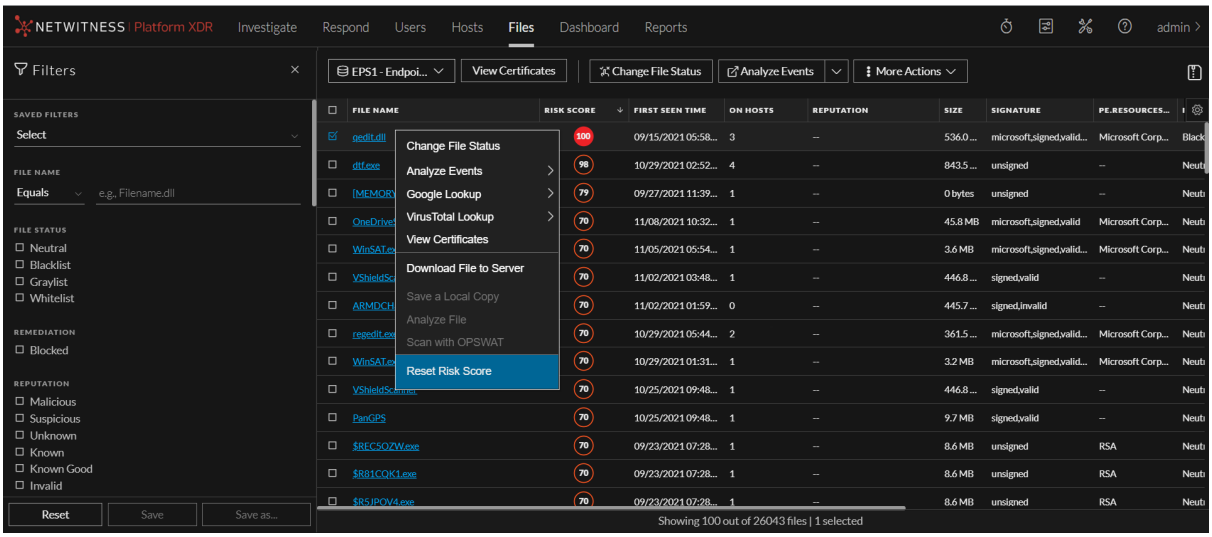
You can reset the risk score for a file in these situations:

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

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

To reset the risk score of a file:

1. Go to **Files**.
2. Select the Endpoint Server or Endpoint Broker.
3. Select one or more files and do one of the following:



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

All the alerts associated with the score are deleted.

Note: You can select a maximum of 100 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.

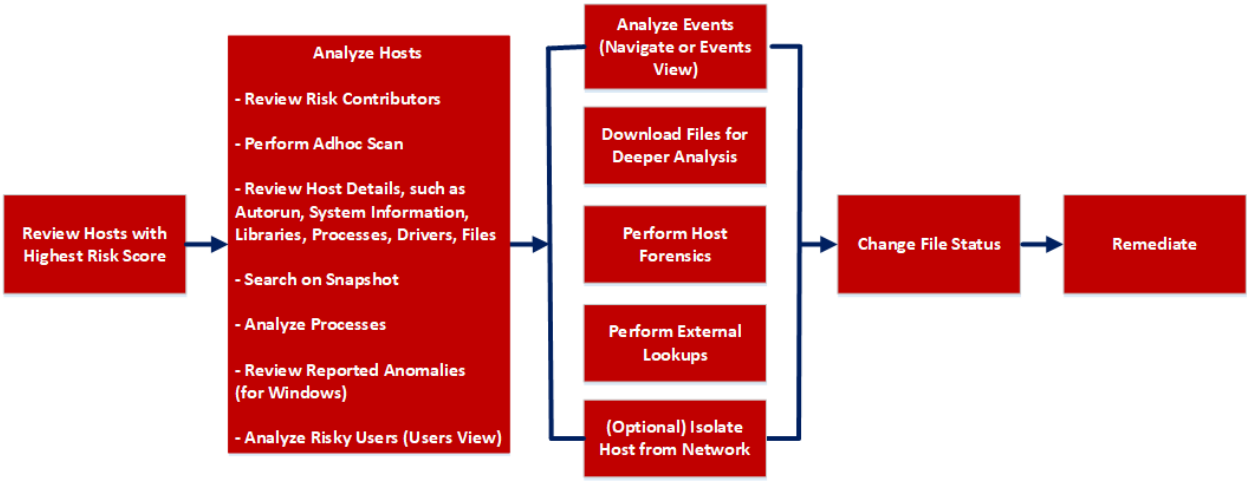
Investigating Hosts

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 Analyze Hosts Using the Risk Score.
- Review files or processes that created this suspected file, and check if any other files are accessed or created in the Events view. For more information, see Analyzing Events.
- Review hosts for rare files in the **On Hosts** column. If a file is present on 100 hosts, it can be legitimate. If a file is present on fewer hosts with a high risk score, it may be malicious and needs further investigation.
- Filter to exclude hosts on host status, risk score, hostname, and so on. For more information, see Filter Hosts.
- Search Google or VirusTotal with the file hash and review any reported activities. For more information, see Launch an External Lookup for a File.

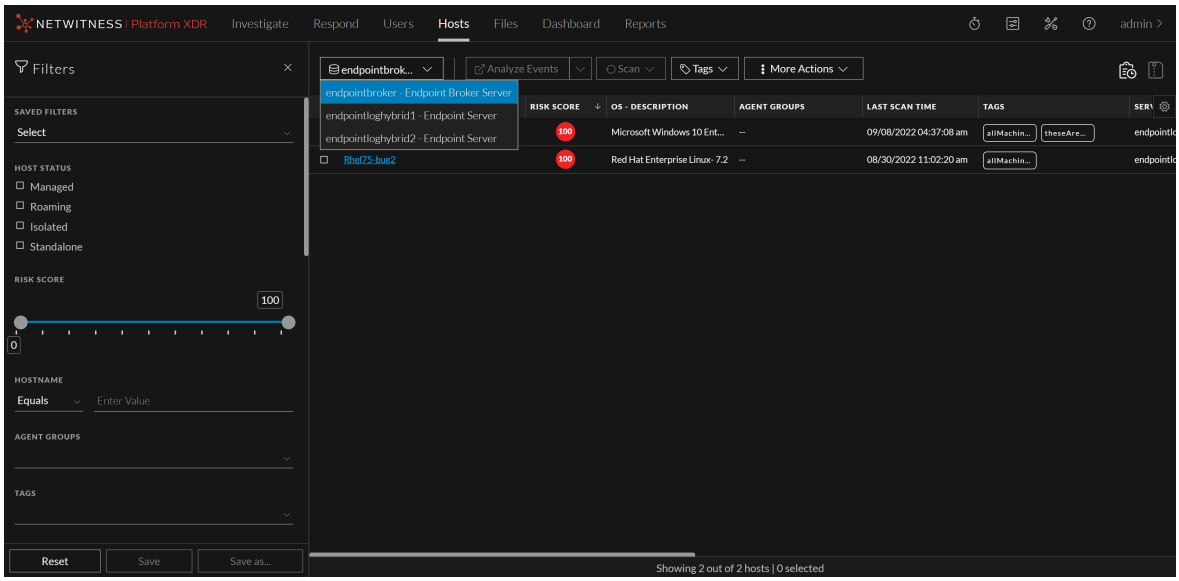
- Review the processes, autoruns, files, libraries, drivers, and system information. For example,
  - Search for files in known malware locations. For example,
    - C:\Windows\.
    - C:\Users\<name>\AppData\<uncommon folder>.
    - C:\Users\<name>\AppData\Local\Temp.
    - C:\Windows\Temp\.
  - Search for a particular file name or hash and review the snapshot to check when the file was first seen.
  - Review any network connections established by the process, such as:
    - Domain or IP address.
    - Ports used (common (80 and 443) versus uncommon ports (8080 , 8888, and 3465)) and check if the ports are listening actively.
  - Check the file compile time. If the date is recent, it could be malicious.
  - Check the file creation time on the host.
- Review reported anomalies, such as suspicious threads, kernel hooks, image hooks, and registry discrepancies. For more information, see Analyze Anomalies.
- Launch Process Analysis to view the sequence of activities performed on the host by the file or process. For more information, see Analyze Processes.
- Download suspicious files to the server for deeper analysis. For more information, see Analyzing Downloaded Files.
- Download MFT, process, or system dump to the server for forensic investigation. For more information, see Performing Host Forensics.
- After investigation if a file is found to be malicious you change the status of the file (blacklist or graylist) and block infected or malicious file. For more information, see Changing File Status or Remediate.
- (Optional) If you suspect that a host is potentially compromised with the threat still being active, you can isolate the host from the network and safely investigate possible threats within the host. For more information, see Isolating Hosts from Network.

View Hosts

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

1. Go to **Hosts**.
2. Select from the following:

- **Endpoint Broker Server** to view all hosts across all Endpoint servers. When querying, the Endpoint Broker ignores Endpoint servers that are offline. If the Endpoint server is online but is not responding, the Endpoint Broker waits for 10 seconds, and ignores if it does not respond.
- **Endpoint Server** to view hosts on a specific Endpoint server.



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

Manage Hosts Using Tags

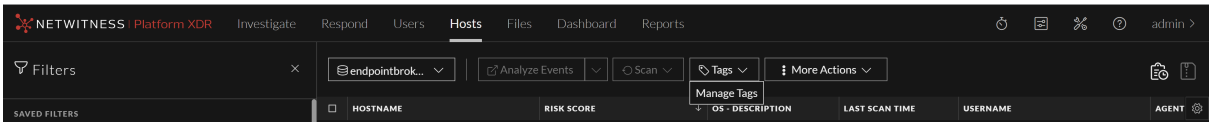
From version 11.7 and later, NetWitness Platform allows you to create Tags to manage the hosts effectively. Tags are custom texts that you can create and assign to hosts for identifying them. A tag can contain alphabets, numbers and special characters(Except \ **' , [ ] "** and **space**). You can use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

Manage Tags

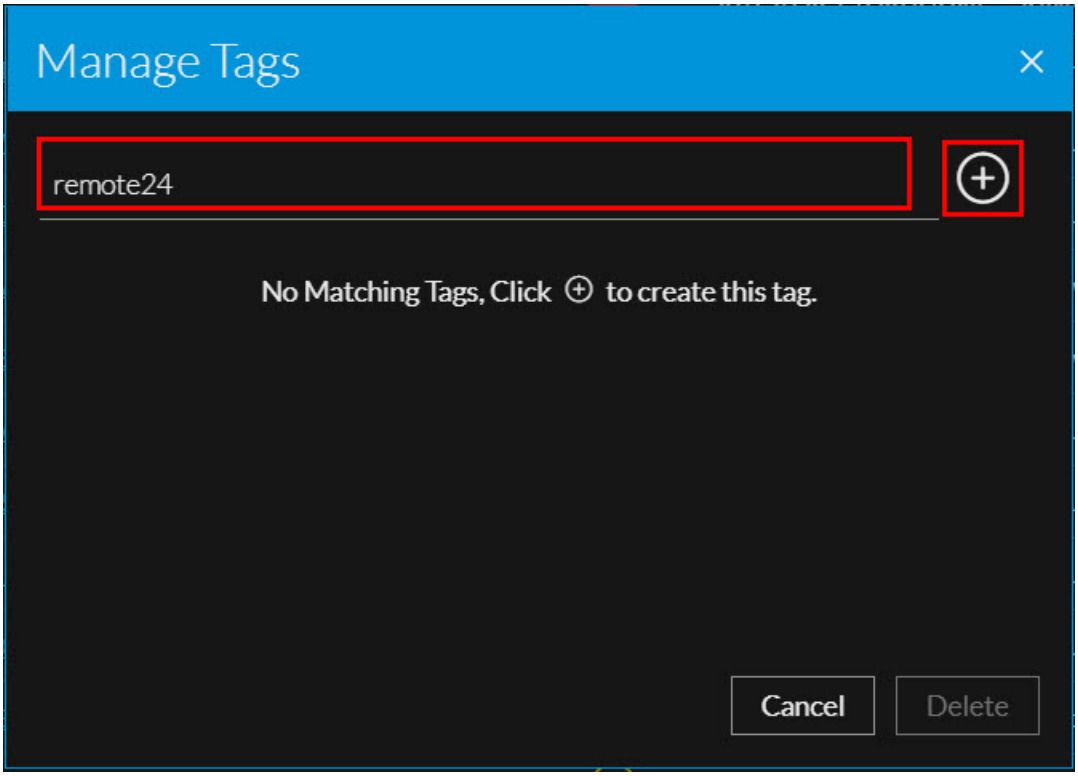
The Manage Tags option allows you to create and delete tags without selecting any hosts.

To Create Tags:

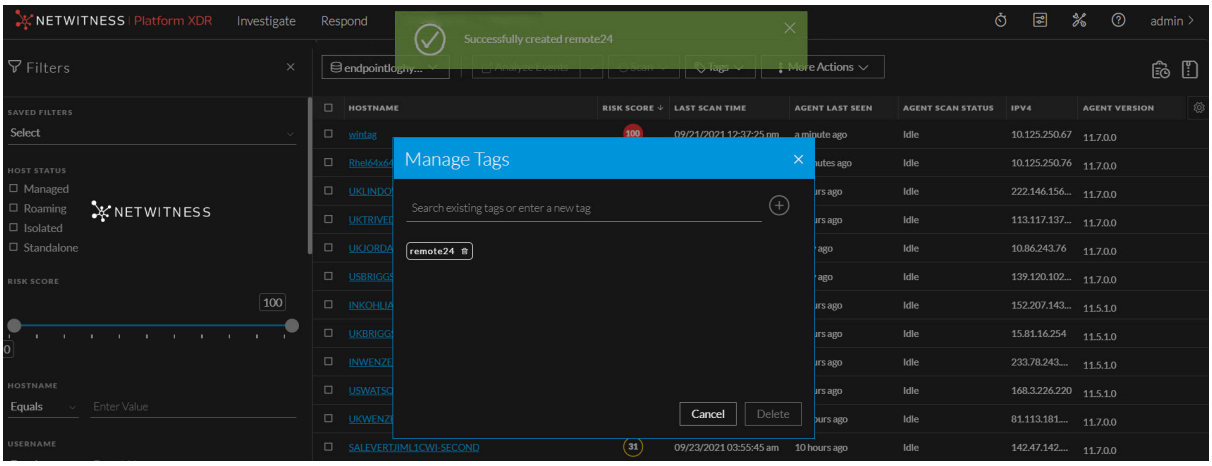
1. Click **Tags > Manage Tags** on the Hosts tab.



2. Enter a valid tag in the text field on the **Manage Tags** pop-up and click .



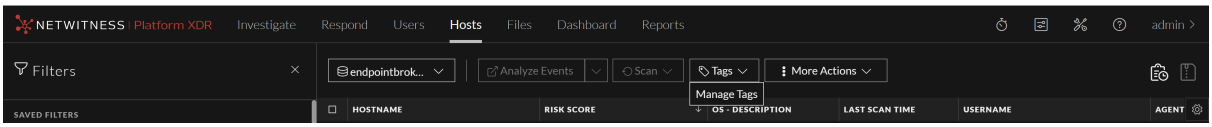
- The tag is created, and a success message will appear.



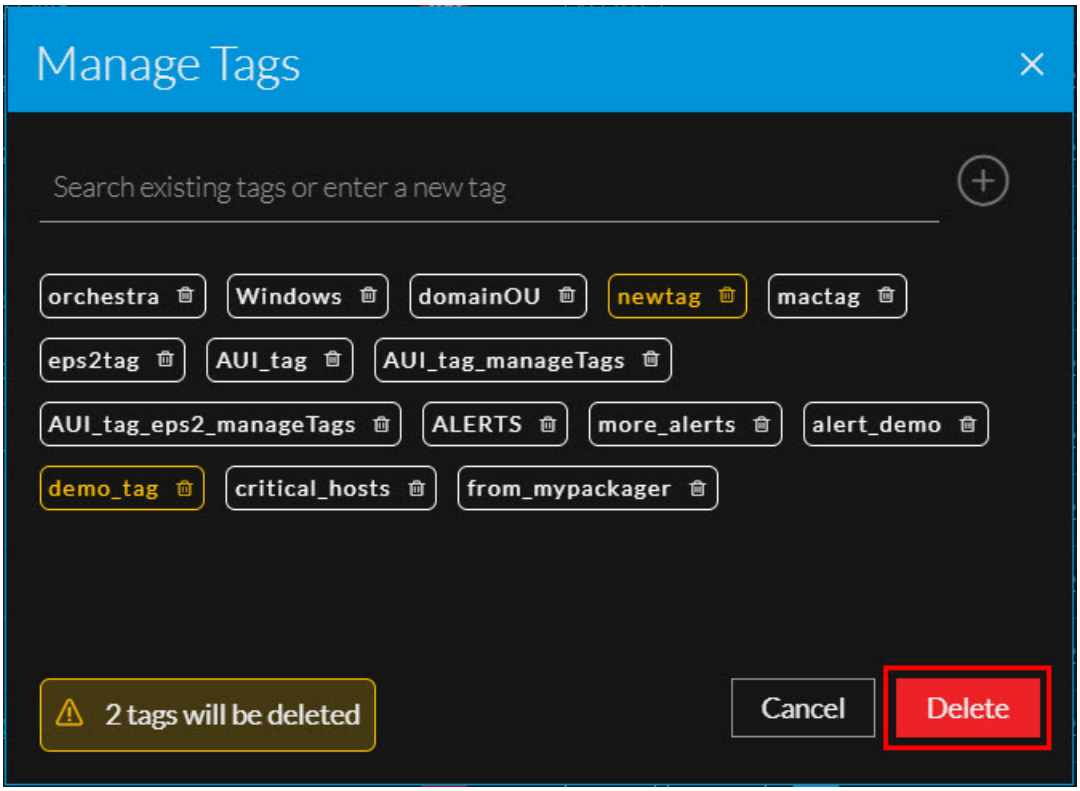
3. Repeat step 2 to create more tags.

To Delete Tags:

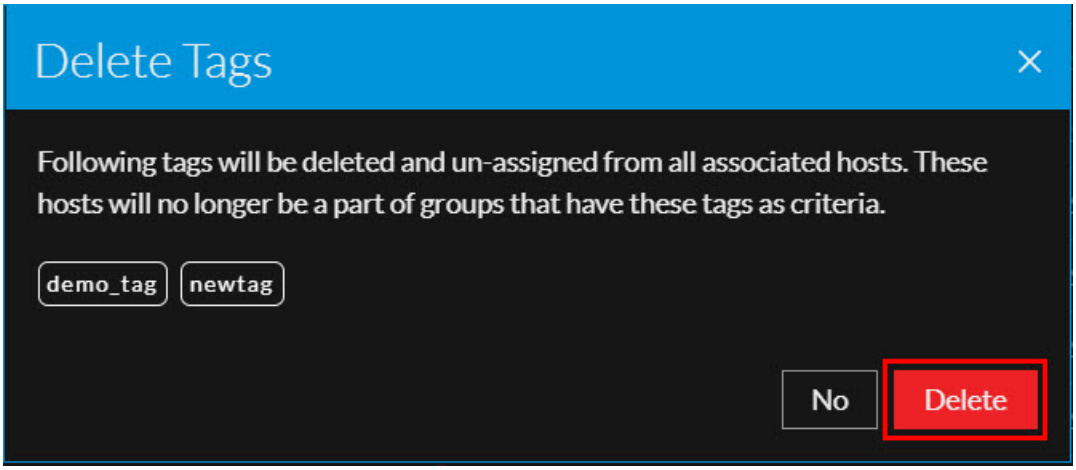
1. Click **Tags > Manage Tags** on the Hosts tab.



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



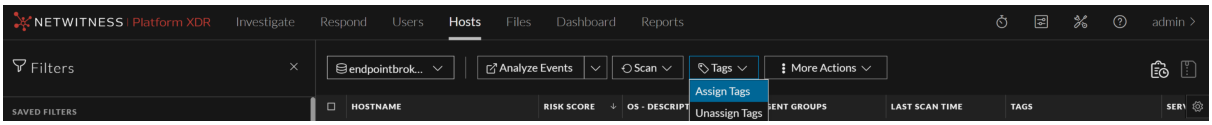
3. Click **Delete** on the **Delete Tags** confirmation pop-up.



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 What happens next after unassigning or deleting tags from hosts? for more information.

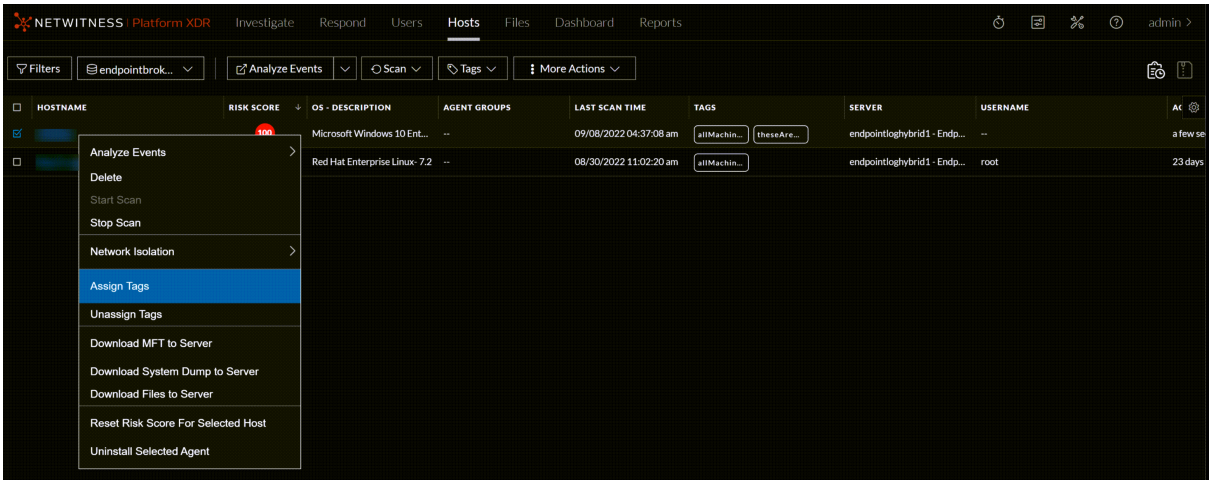
Assign tags

1. Select one or more hosts on the Hosts tab.
2. Select **Tags > Assign Tags** from the menu.



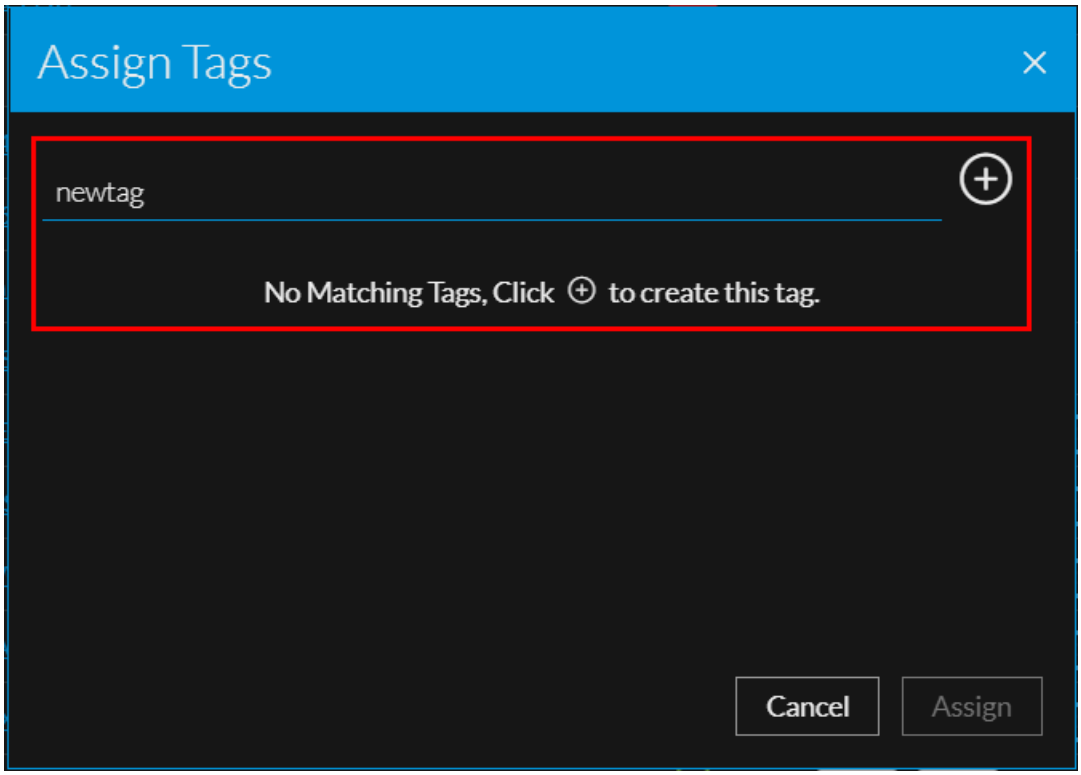
(or)

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



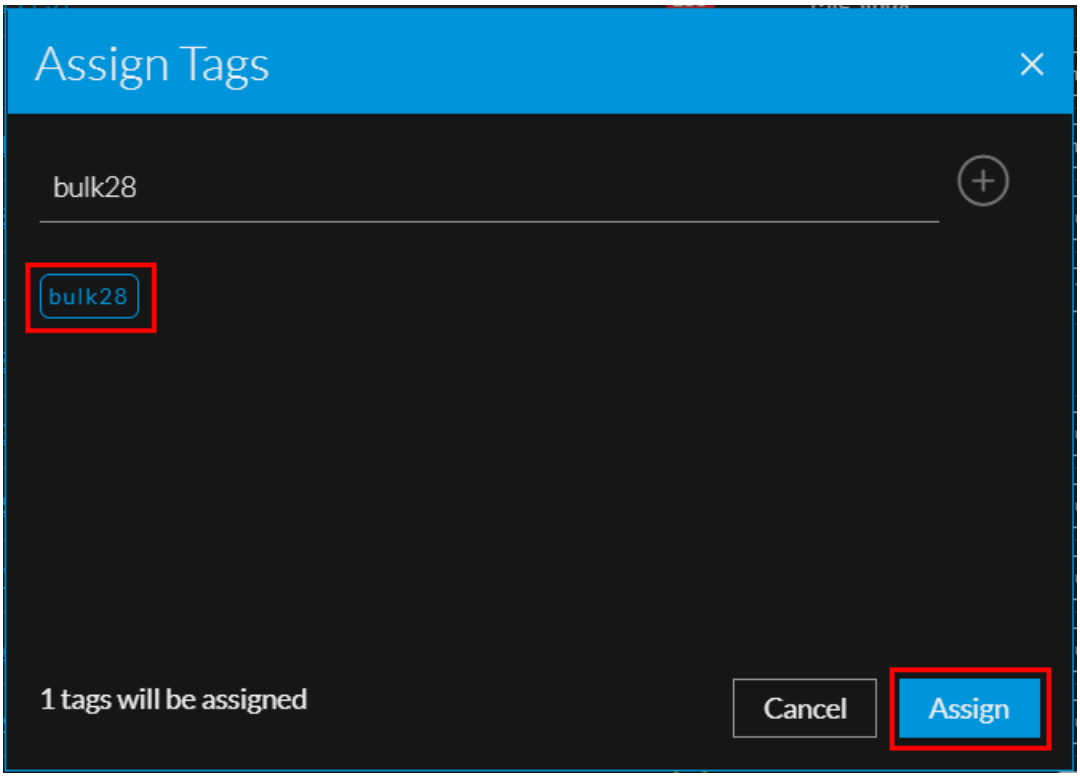
3. The Assign Tags pop-up will appear and shows all the existing tags. You can either

- Enter a valid tag and click to create it. The newly created tag is selected by default.

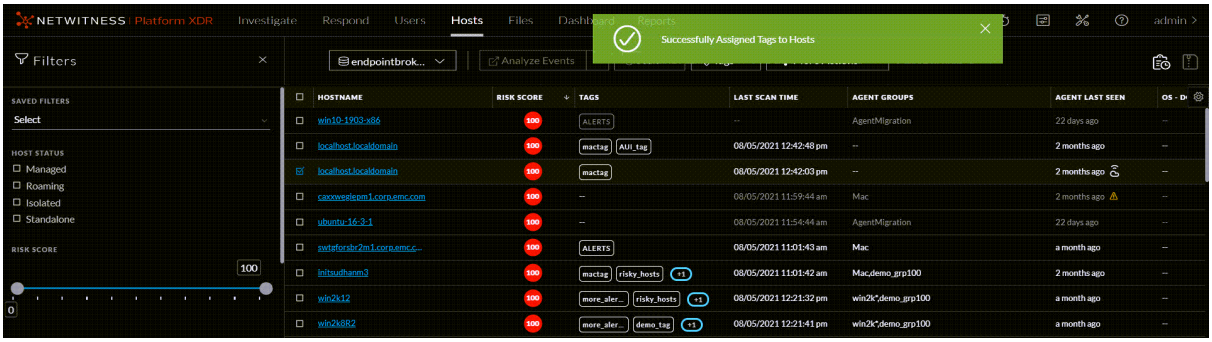


(Or)

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



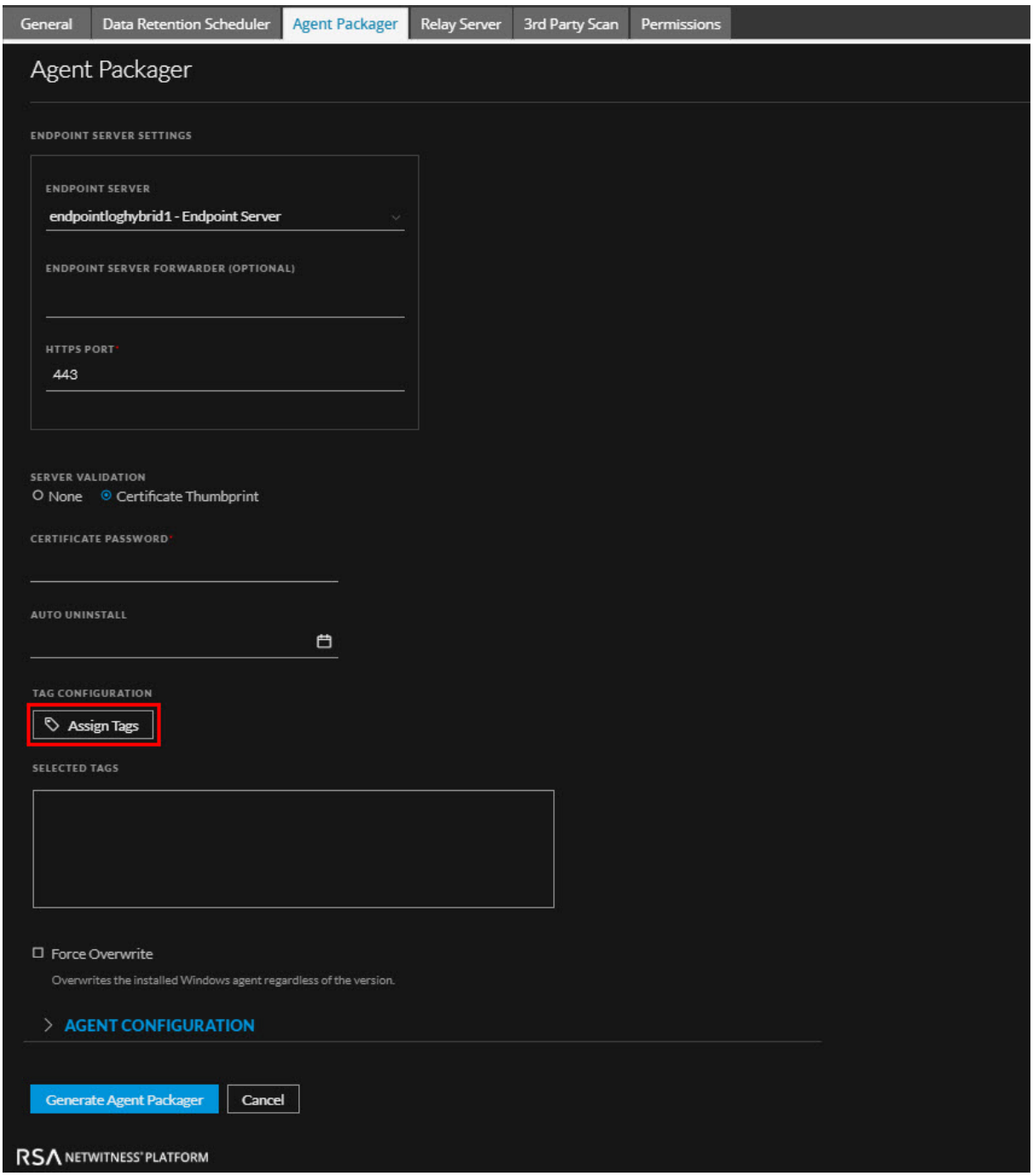
4. Click **Assign**. These tags will be assigned to the selected hosts.



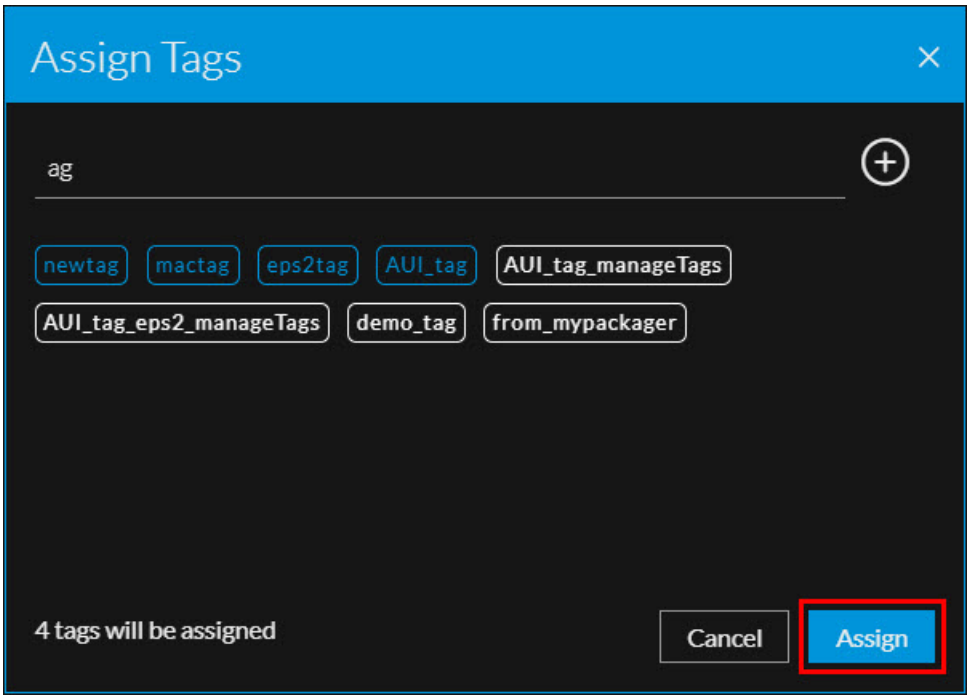
Create and Assign Tags When Generating the Agent Packager

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.



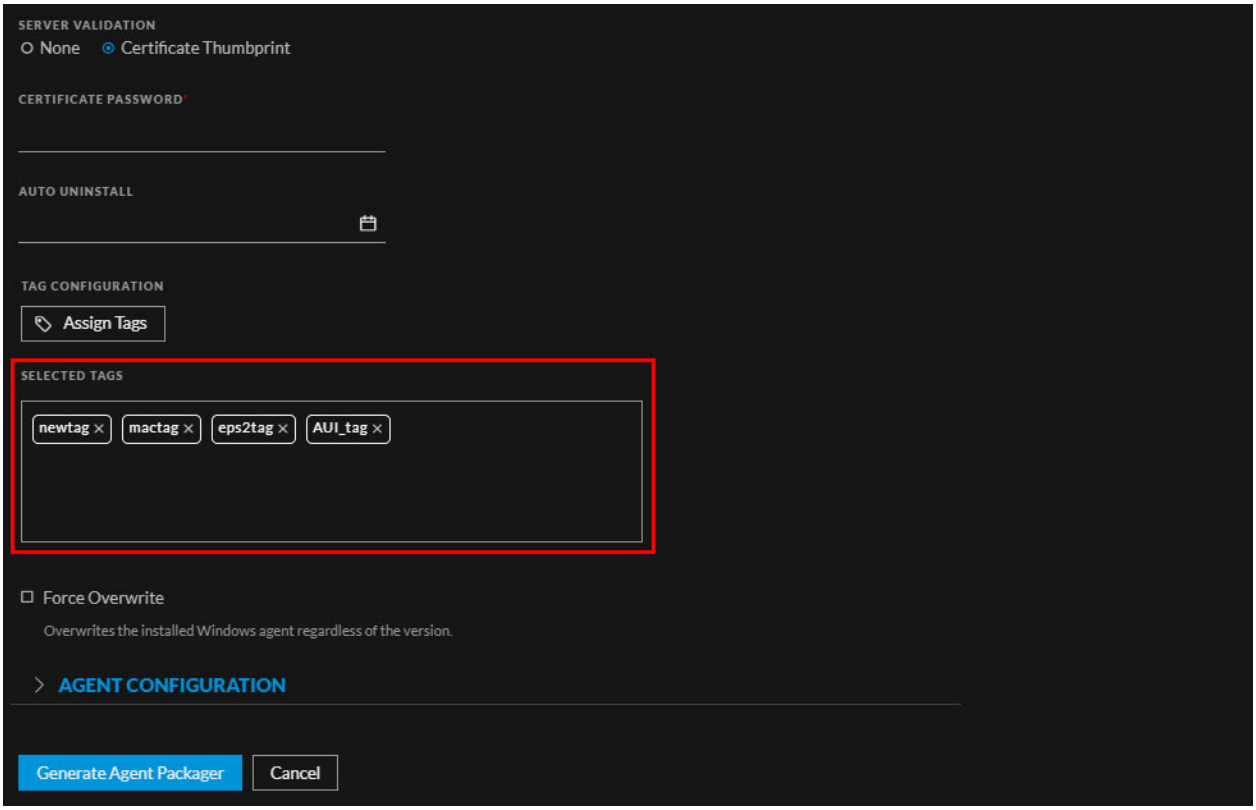
2. On the **Assign Tags** pop-up,
   - Search for an existing tag using the text field and click **Assign**.



(or)

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

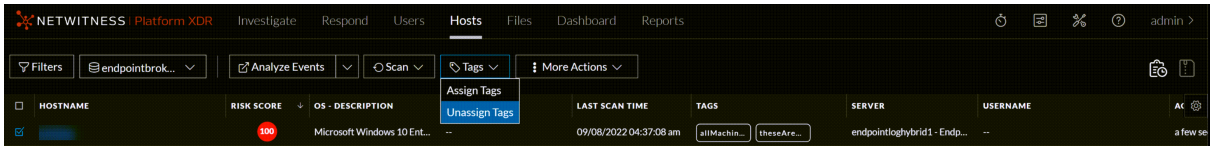
3. Assigned tags will appear under **SELECTED TAGS**.



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

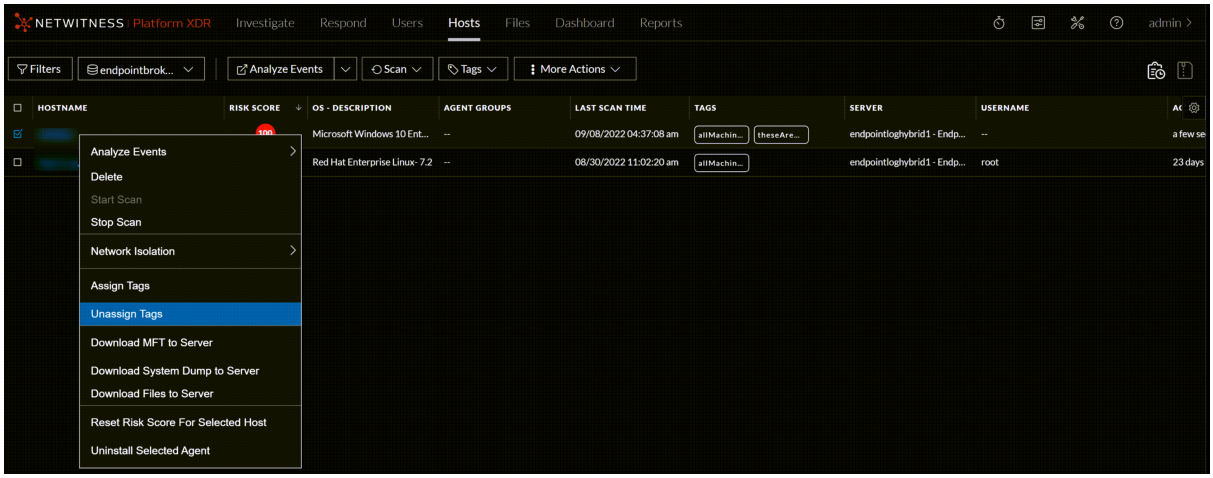
Unassign tags

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

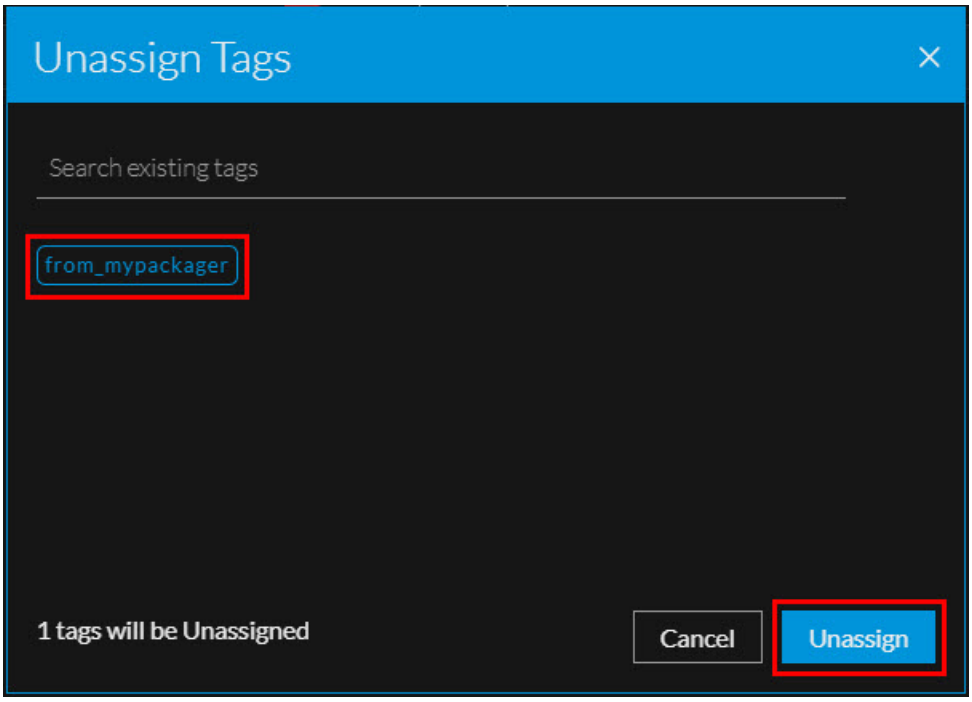


(or)

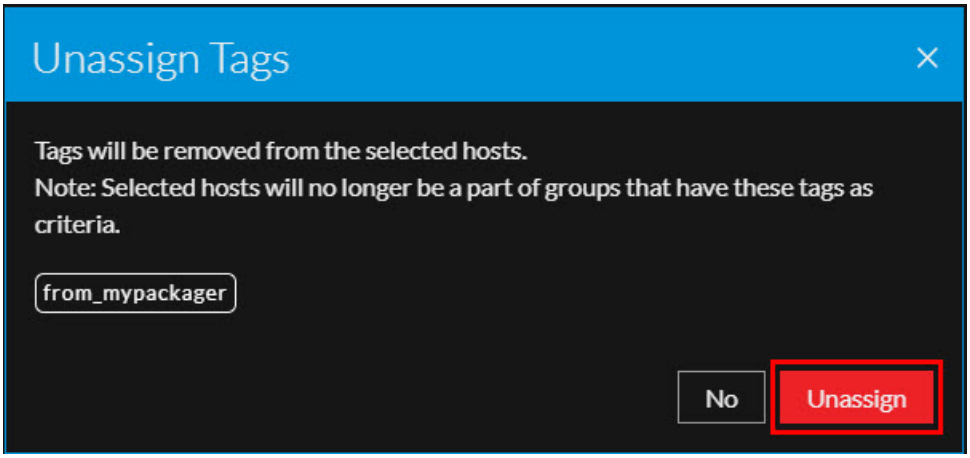
Right click on a host and select **Unassign** Tags. The **Unassign Tags** pop-up will appear and shows all the tag assigned to the selected hosts.



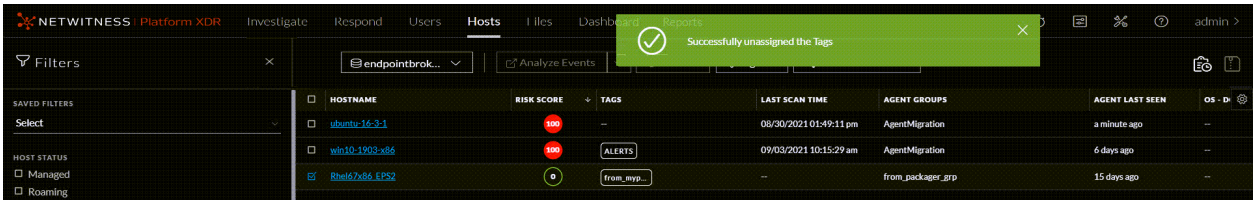
3. Search for the tags you want to unassign, select them and click **Unassign**.



4. Click **Unassign** on the confirmation pop-up.



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



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.

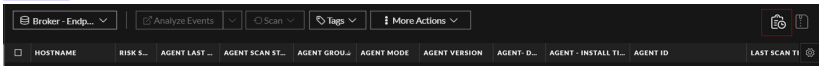
View Agent History

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:

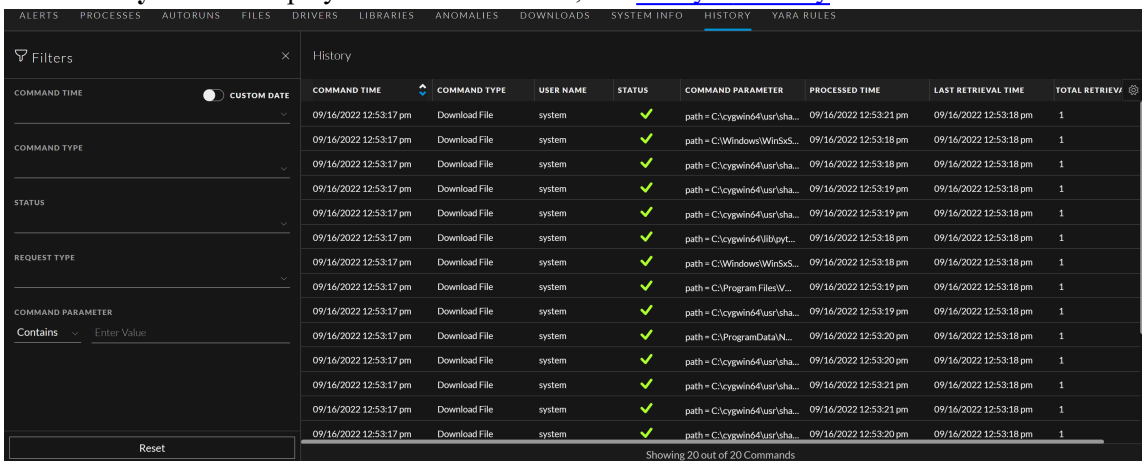
1. Go to **Hosts**.
2. Do any one of the following,

- To view all commands, click . You can also filter commands, for more information see Filter Hosts.



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.

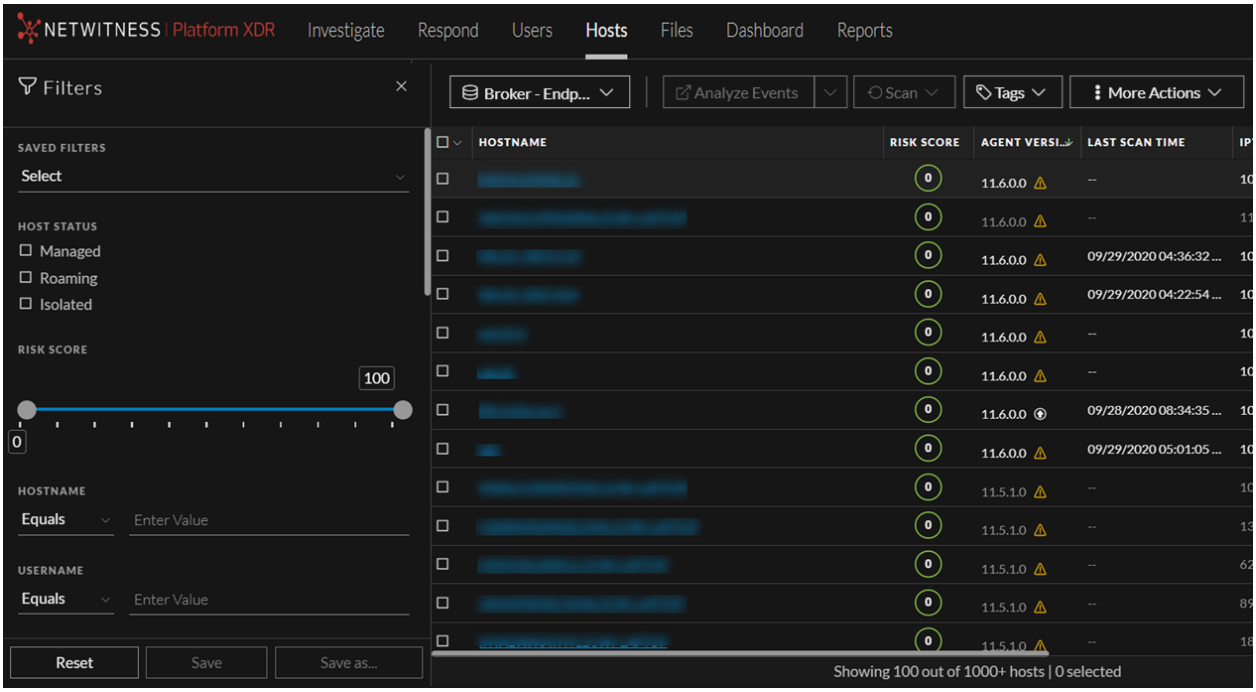


Filter Hosts

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.

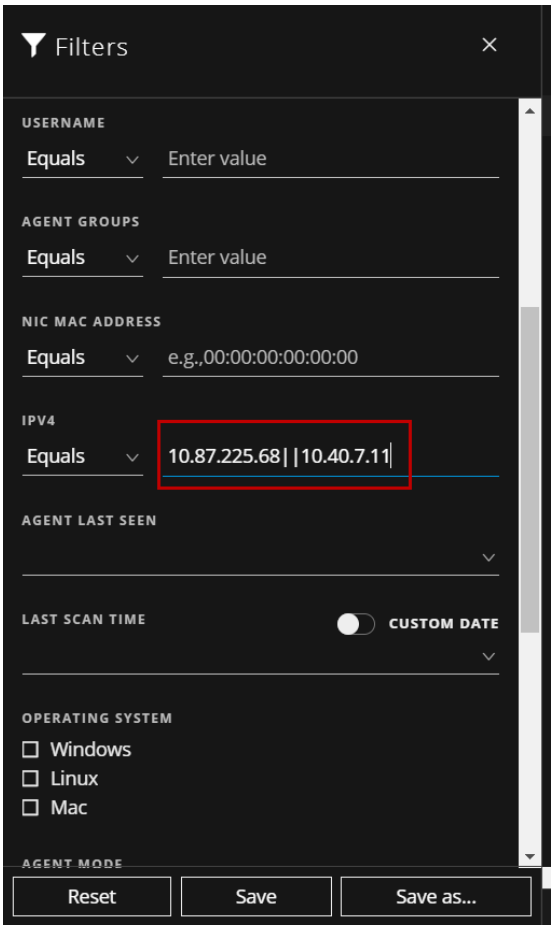
In the **Host** view > click , to filter the commands on command type, status, host name, request type, command parameter and command time. In the Command Time field, you can filter by custom date range.

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.



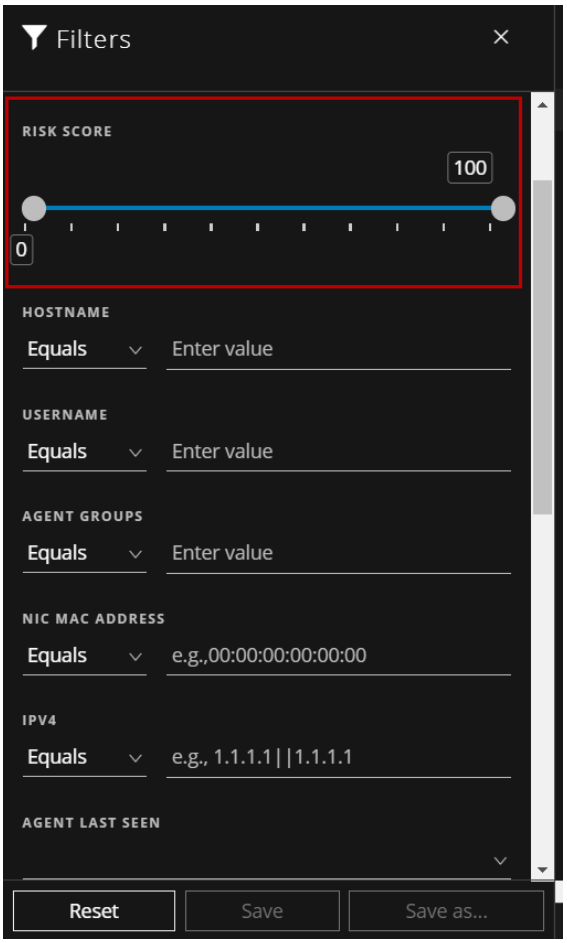
To search multiple values within a field, set the filter option to `Equals`, and use `||` as a separator.

For example, using `Equals` operator for multiple IPV4 values with a separator `||`.



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.

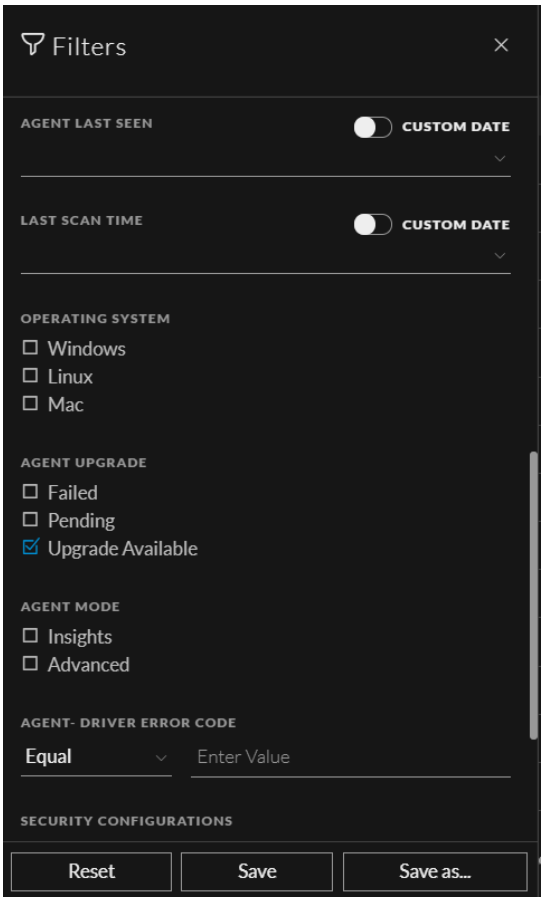
To filter on the risk score, use the slider to increase or decrease the values between 0 to 100.



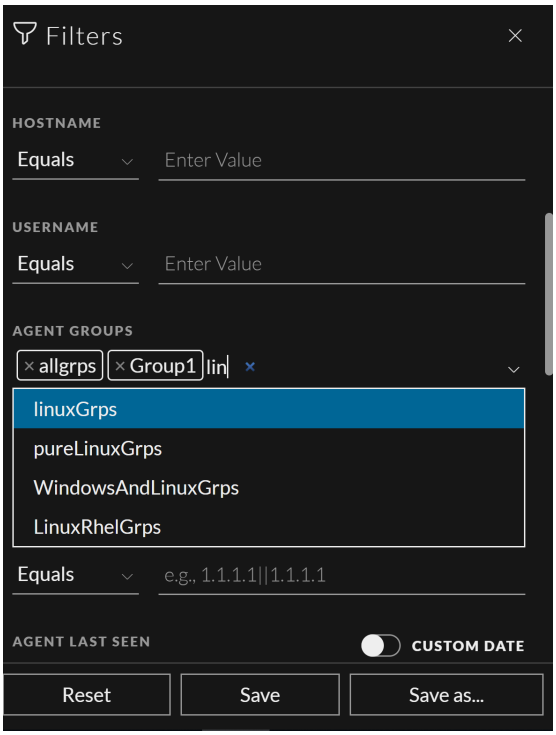
Click **Save** to save the filter and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters panel on the left. To delete a filter, hover over the filter name and click 🗑.

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

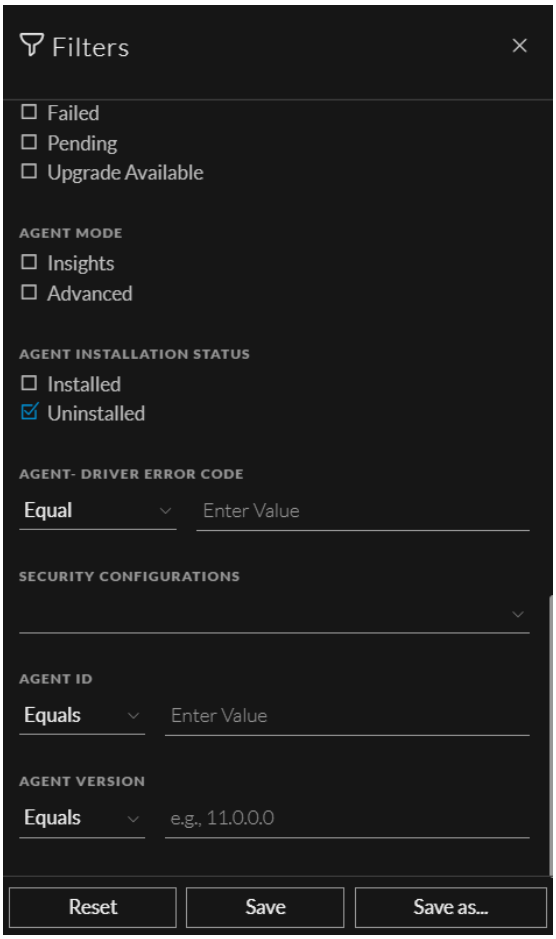
To filter the agents based on the upgrade status, select one of the upgrade statuses. For example, select the **Upgrade Available** checkbox to get the list of agents available for an upgrade.



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.



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.

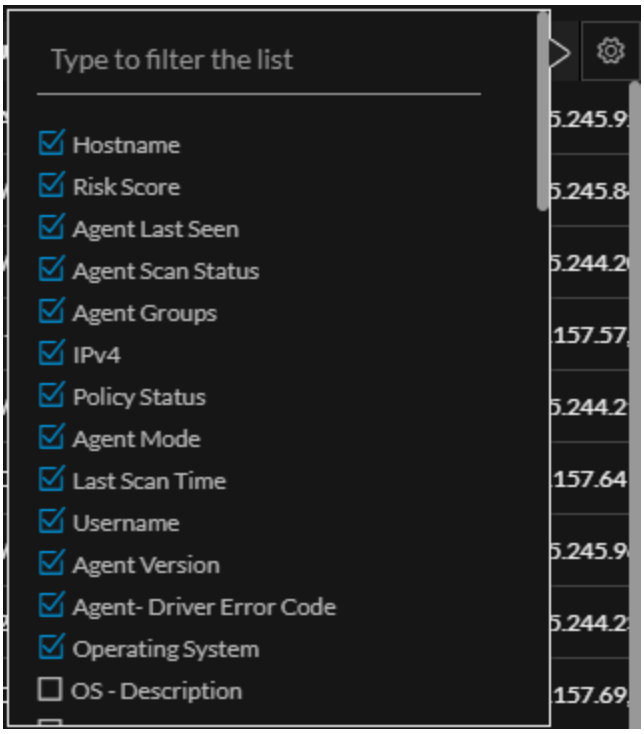


You can also filter the commands on command type, status, host name, request type, command parameter and command time (In which you can filter by custom date range), by clicking .

Adding and Sorting Columns in the Table

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

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



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

Scan Hosts

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

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.

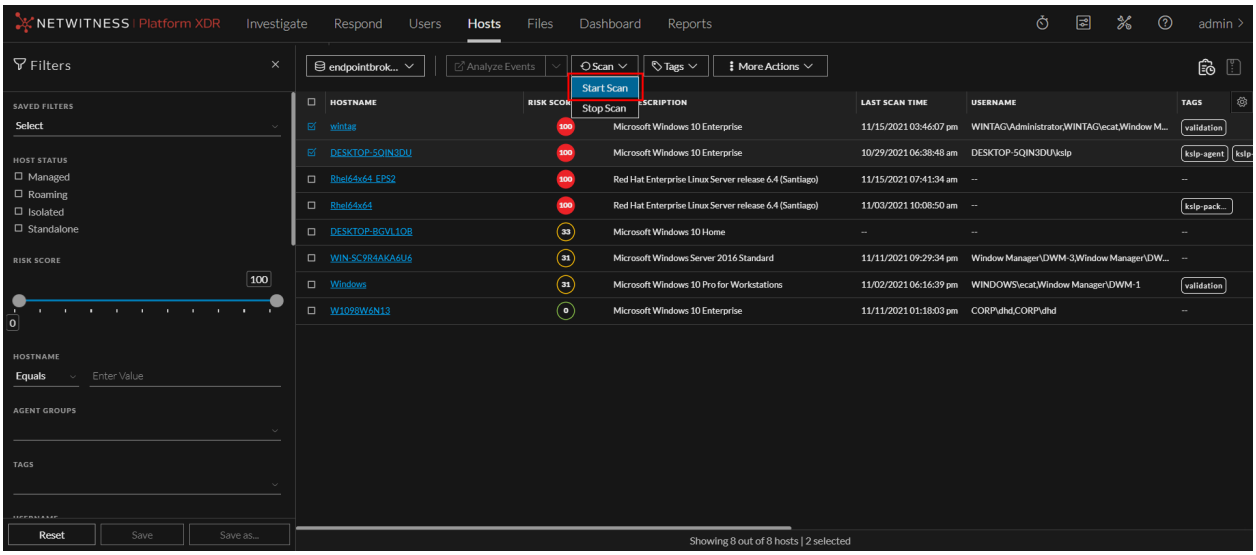
The following are the scan statuses:

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.

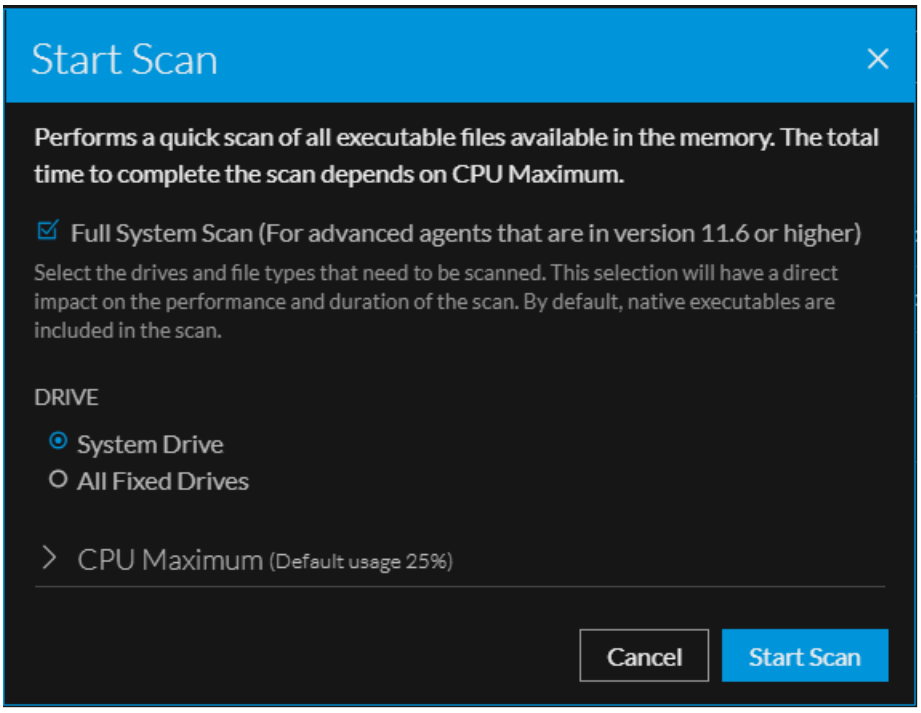
To perform a Full System Scan:

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



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.



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

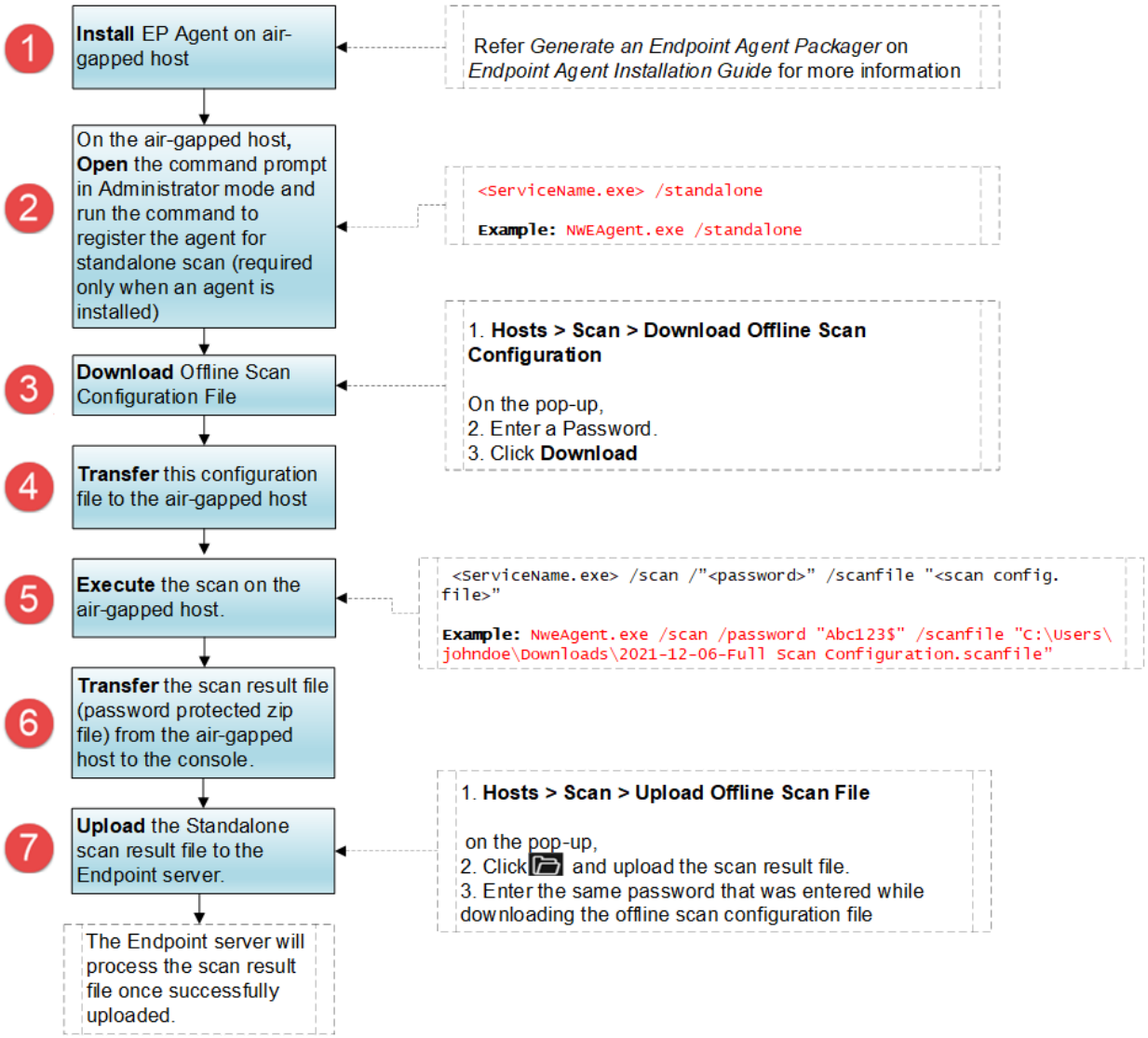
Standalone Scan on Air-gapped Windows Hosts

The Standalone scan feature allows administrators to run scans on the air-gapped Windows 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, we recommend 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.

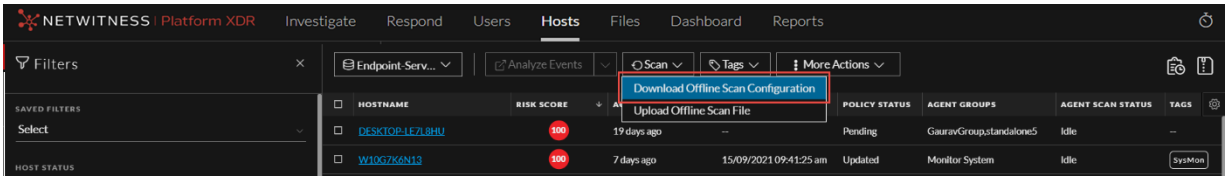
Standalone scan workflow:



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.

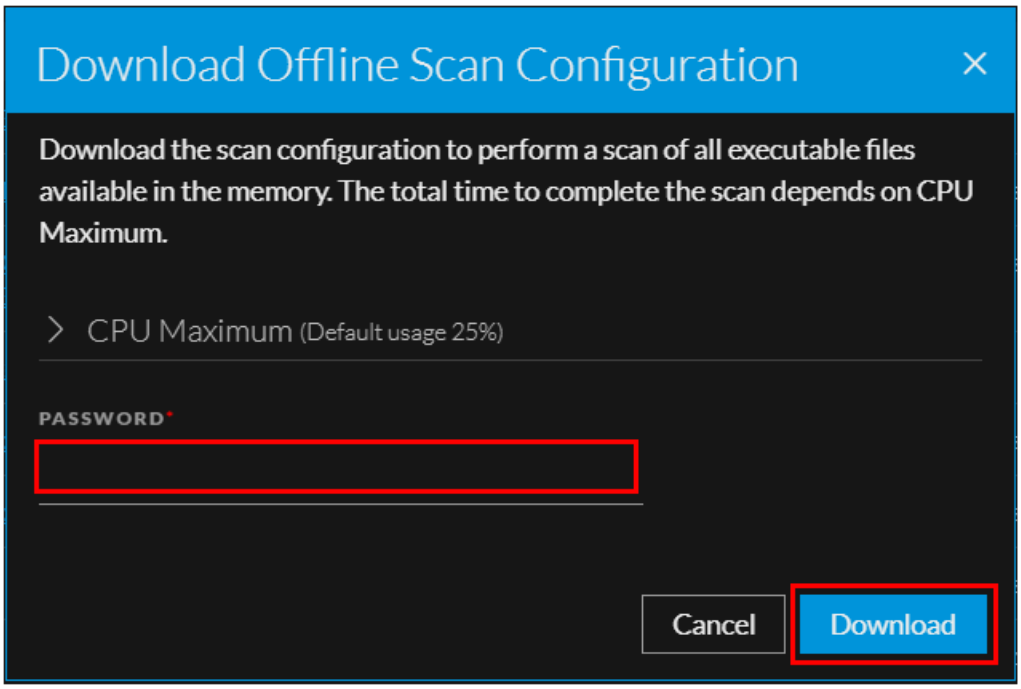


On the Download Offline Scan Configuration pop-up,

2. (Optional) **Select CPU Maximum**.

3. Enter a Password. (not more than 31 characters long)

4. Click **Download**.



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)
   - Open command prompt in administrator mode and execute the following command:

     `ServiceName.exe /standalone`

     Example: `NweAgent.exe /standalone`

Start a Standalone scan

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 "<scan config. file>”
```

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

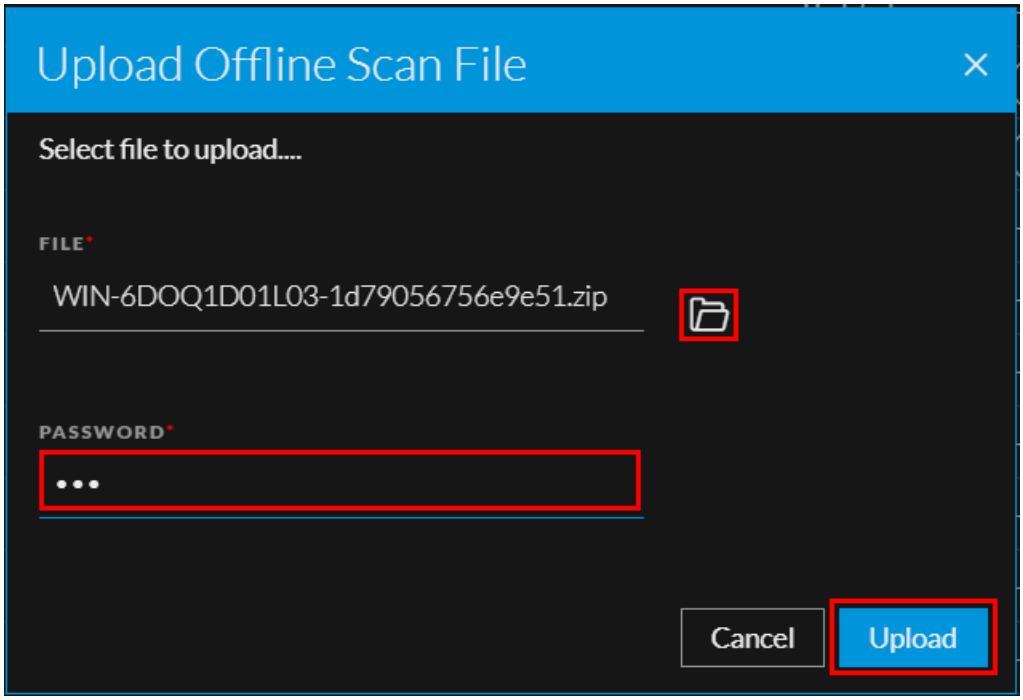
- `<password>` is the password entered while generating the Offline Scan Configuration File.

- `<scan config file>` is name of the scan configuration file with full path.

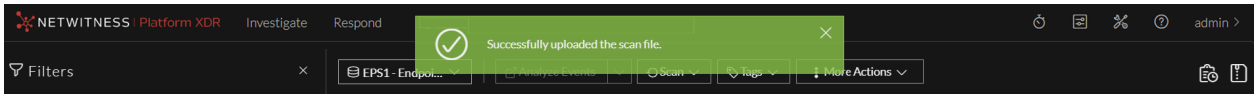
3. Wait until the scan is completed.
4. Transfer the scan result file(password protected .zip file) back to the machine to upload to the UI.

Upload the Standalone scan result file

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



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.



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.

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.

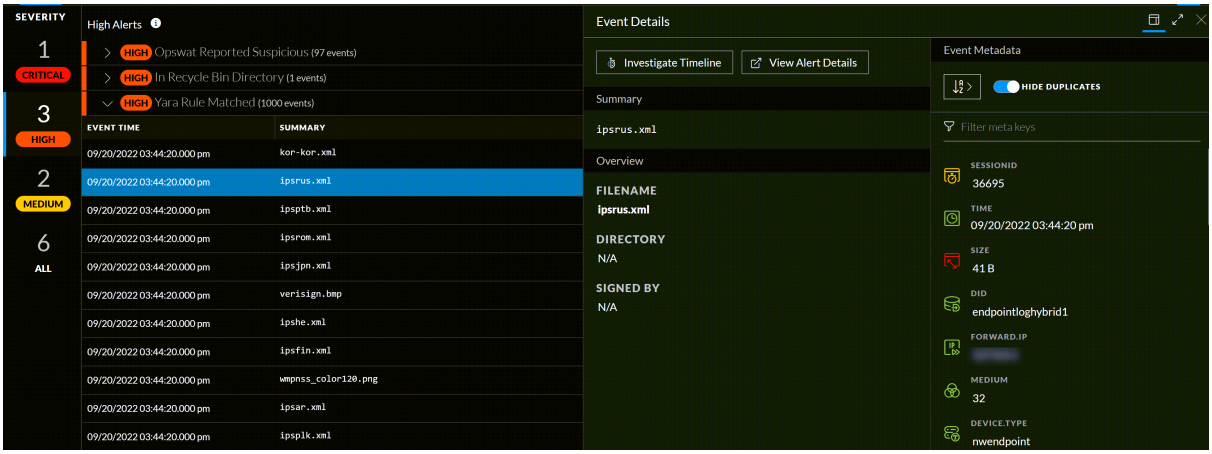
   - Click a row to view the risk associated with the host in the **Risk Details** panel.
   - Click the hostname to investigate the host.

     The **Alerts** tab is displayed.

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

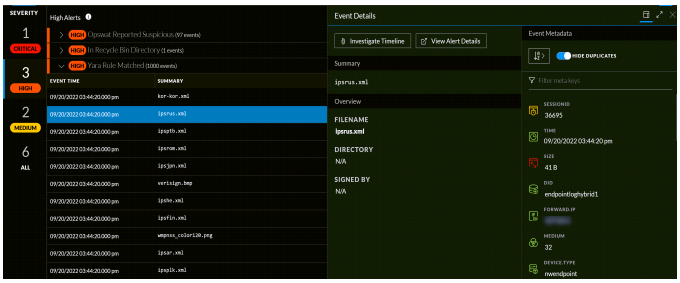
   The list of distinct alerts is displayed along with the total number of events associated with the alert.

5. Click an alert to view the associated events.

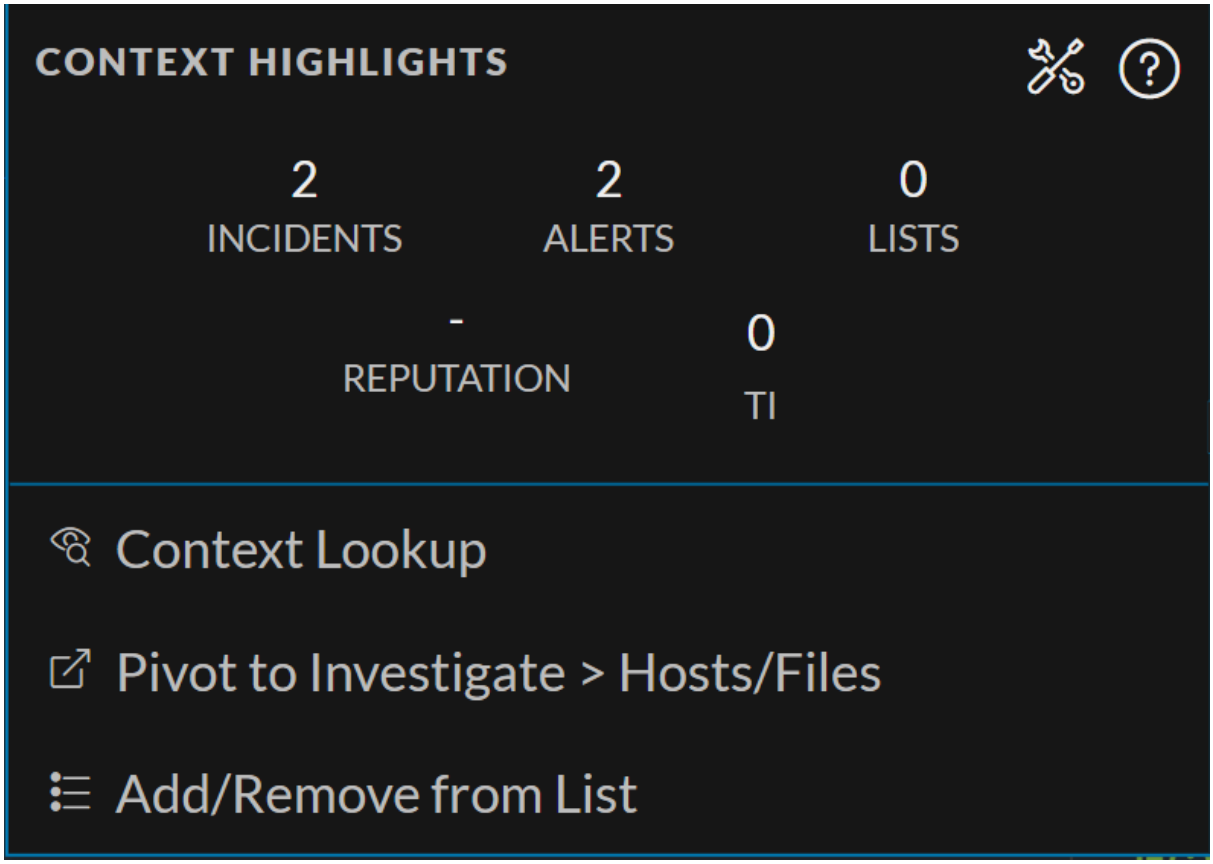


Note: For each alert, only the latest 1000 events are displayed.

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 **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.

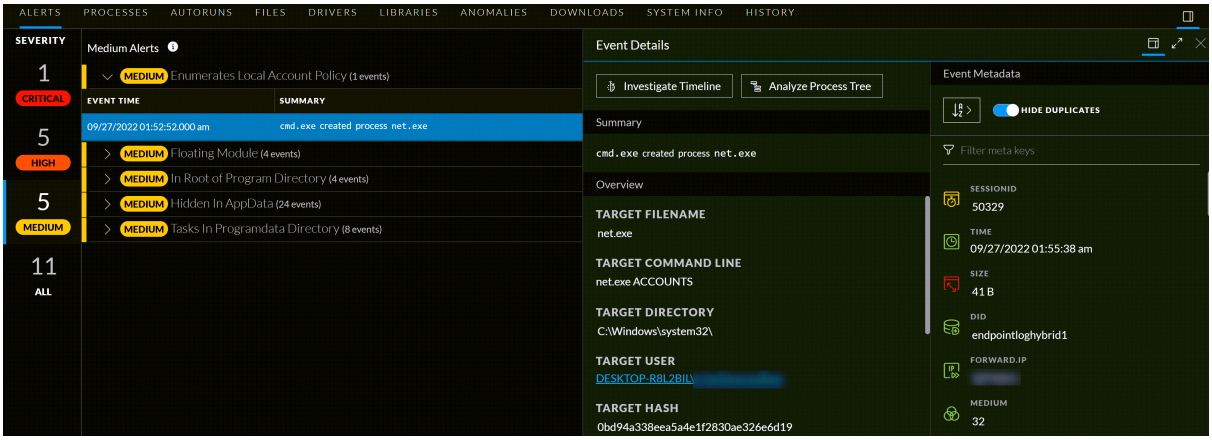
4. In the **Alerts** > **Severity** panel, click the **Medium** alert severity.

   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.

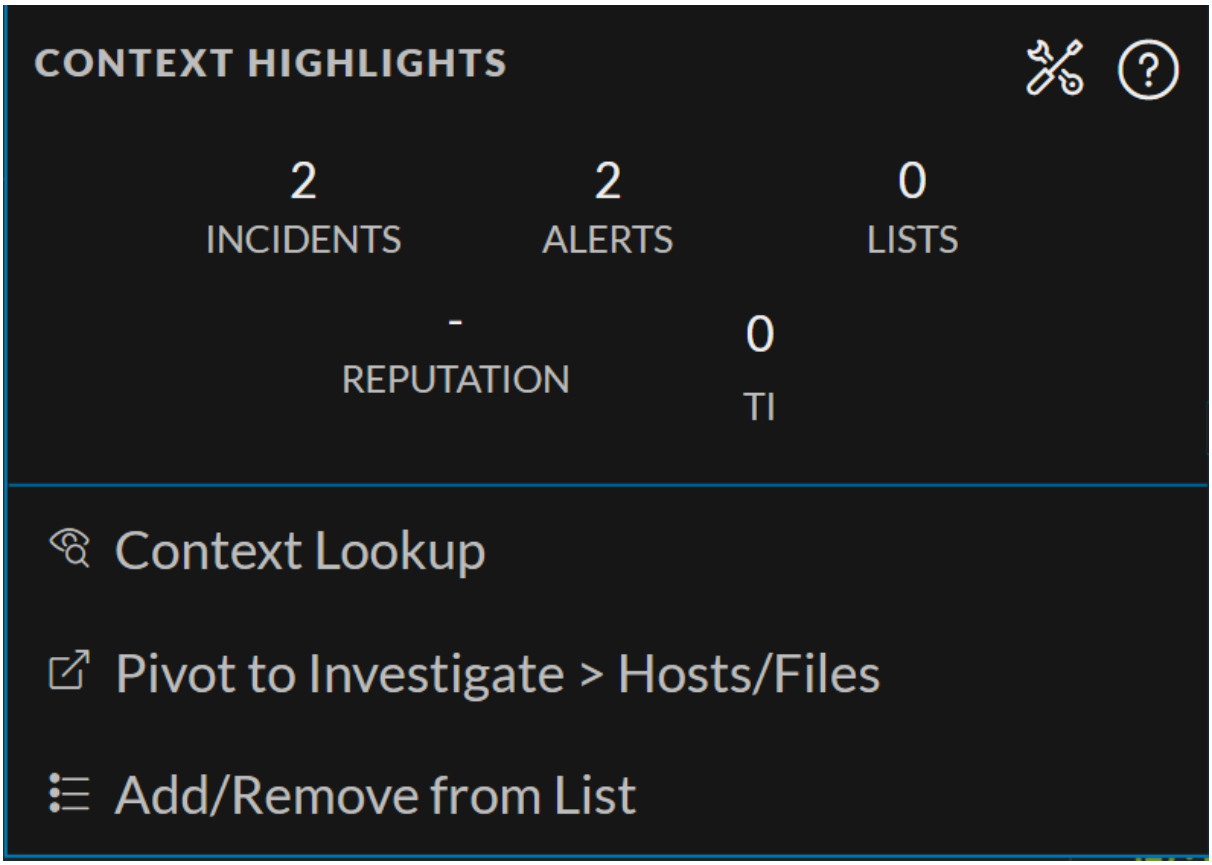
   Note: For each alert, only the latest 1000 events are displayed.

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.

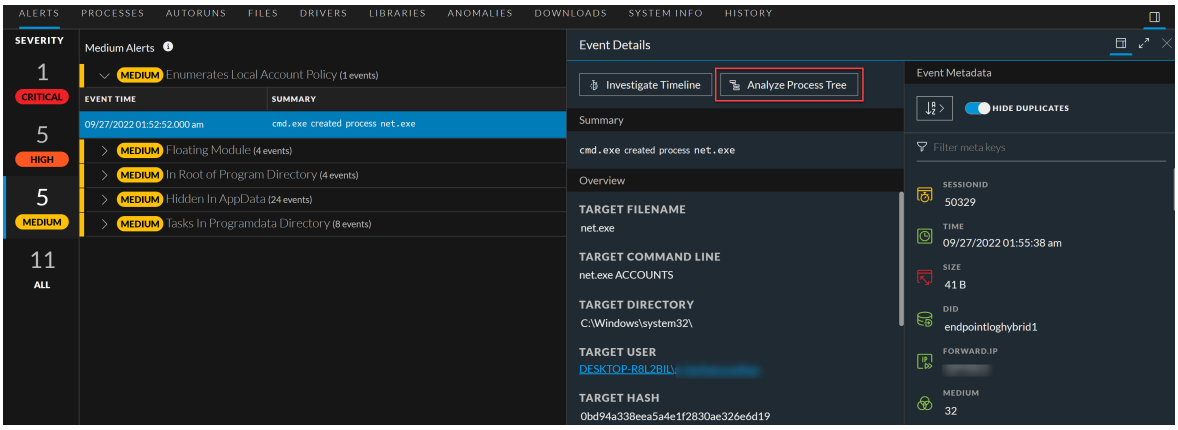


7. You can also view the Event Metadata such as IP, Filename, File hash, and Category in the **Event Details** panel.

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.

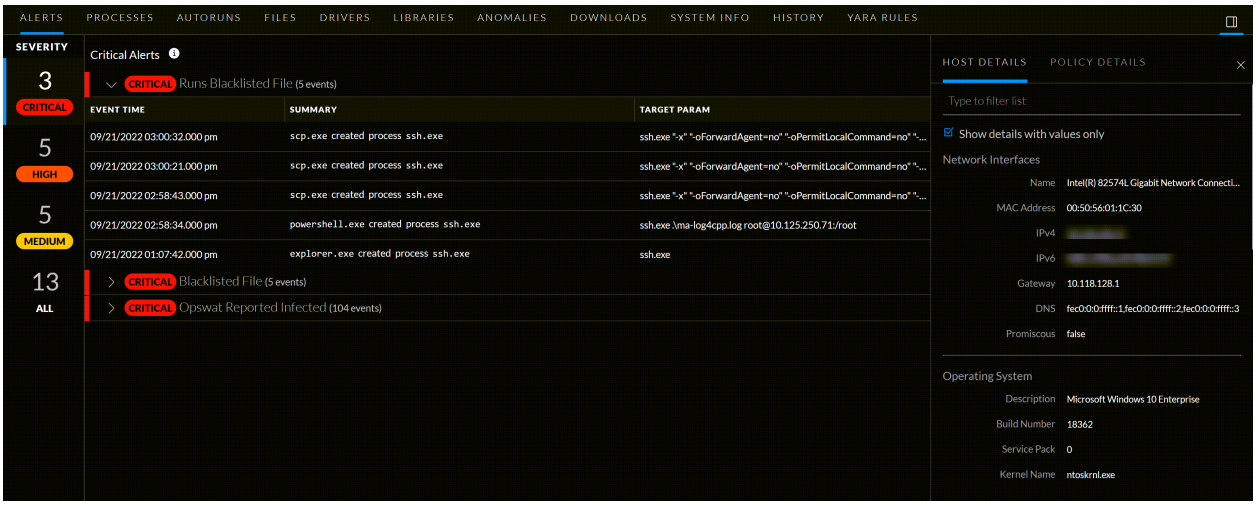


Analyze Host Details

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

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

For more details, see Hosts View - Details Tab.



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 .

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 .

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.

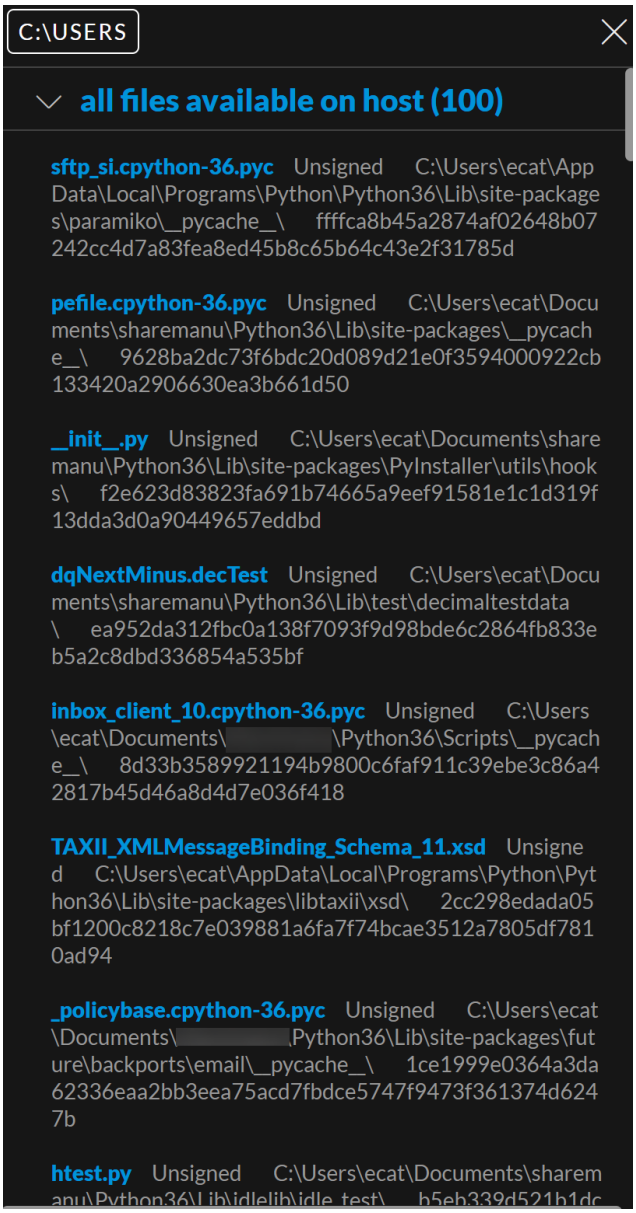
Note: To search for a SHA-256 checksum, provide the entire hash string in the search box.

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.



This file is run as a Process.

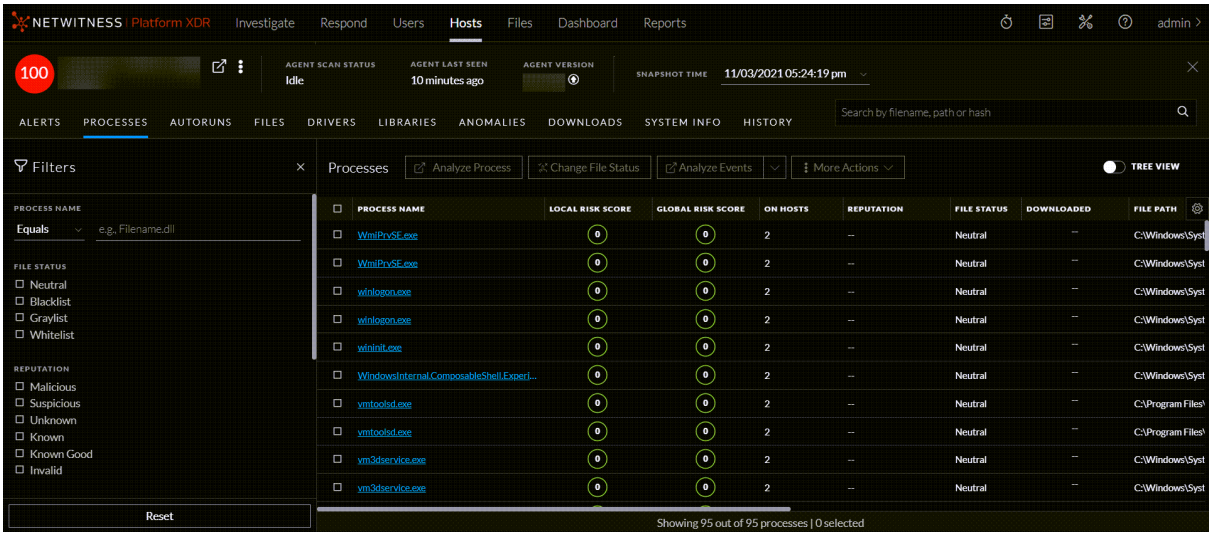
4. To view details of this file, click **Process** in the result.

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

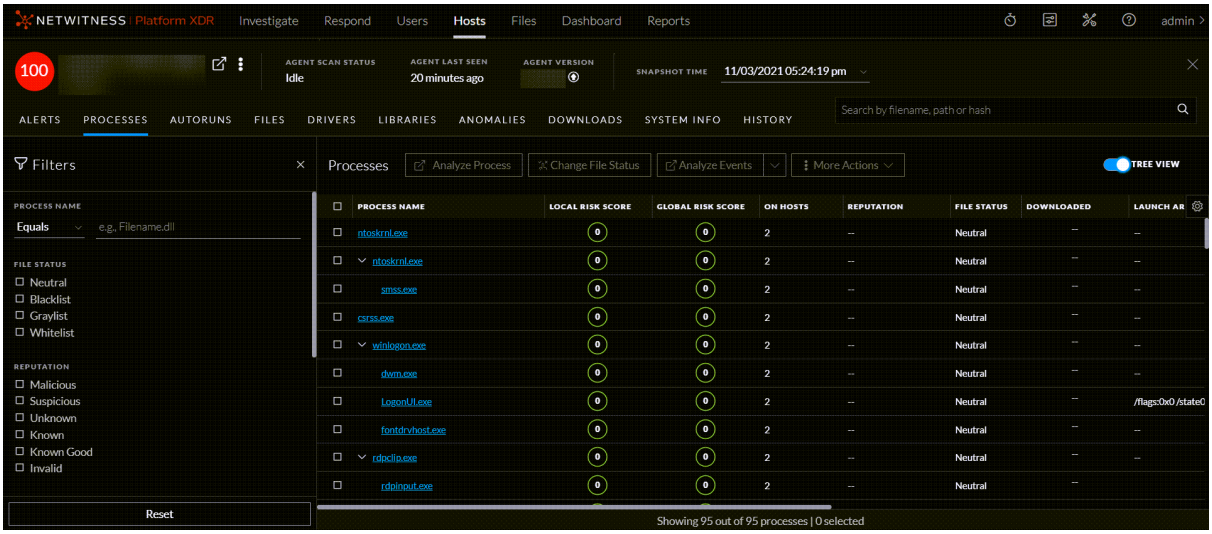
Analyze Processes

To analyze the process:

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

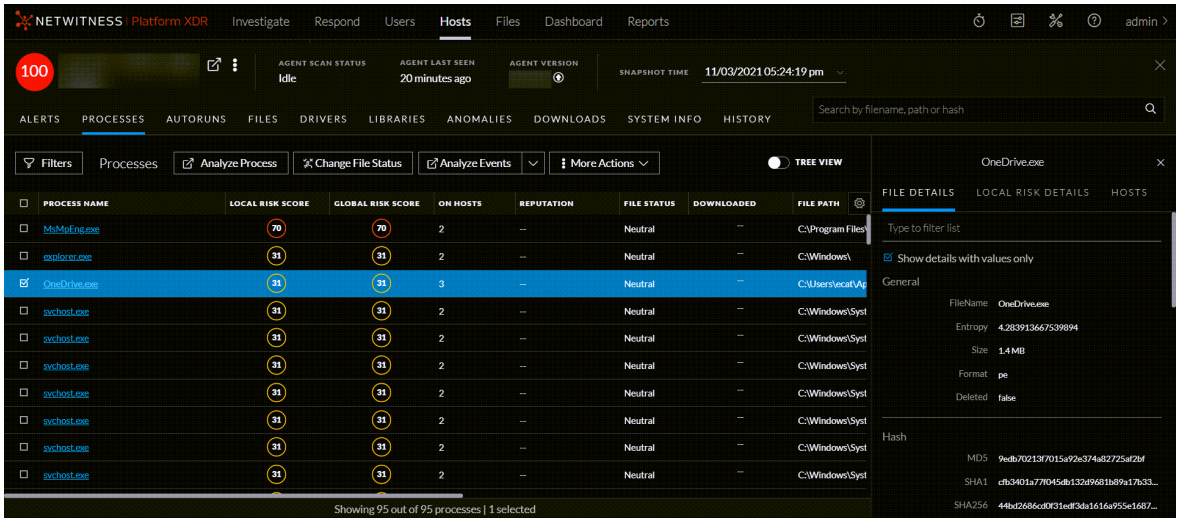


To view the process tree, click the toggle switch. The following is an example of the tree view:

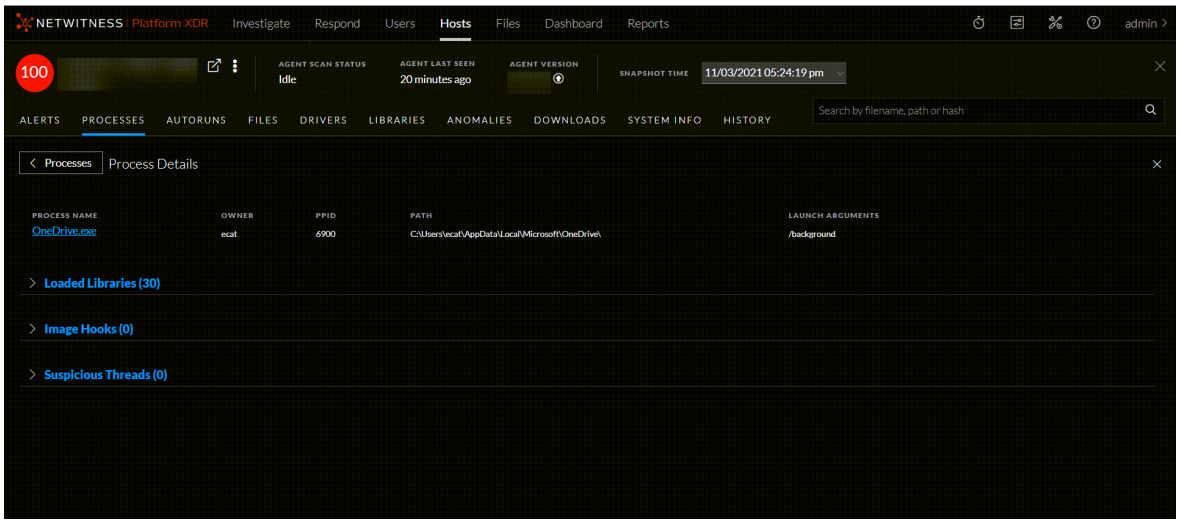


2. In the **Processes** Tab, do one of the following:

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



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



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

For example,

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

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

Analyze Autoruns

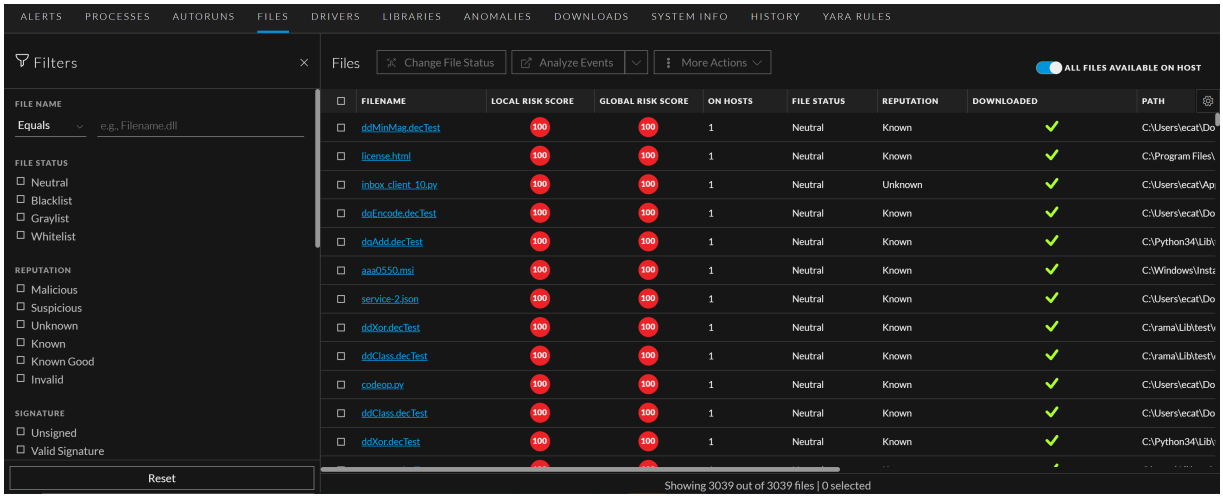
In the Hosts details, select the **Autoruns** tab. You can view the autoruns, services, tasks, and cron jobs that are running for the selected host.

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

Analyze Files

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.



- 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.

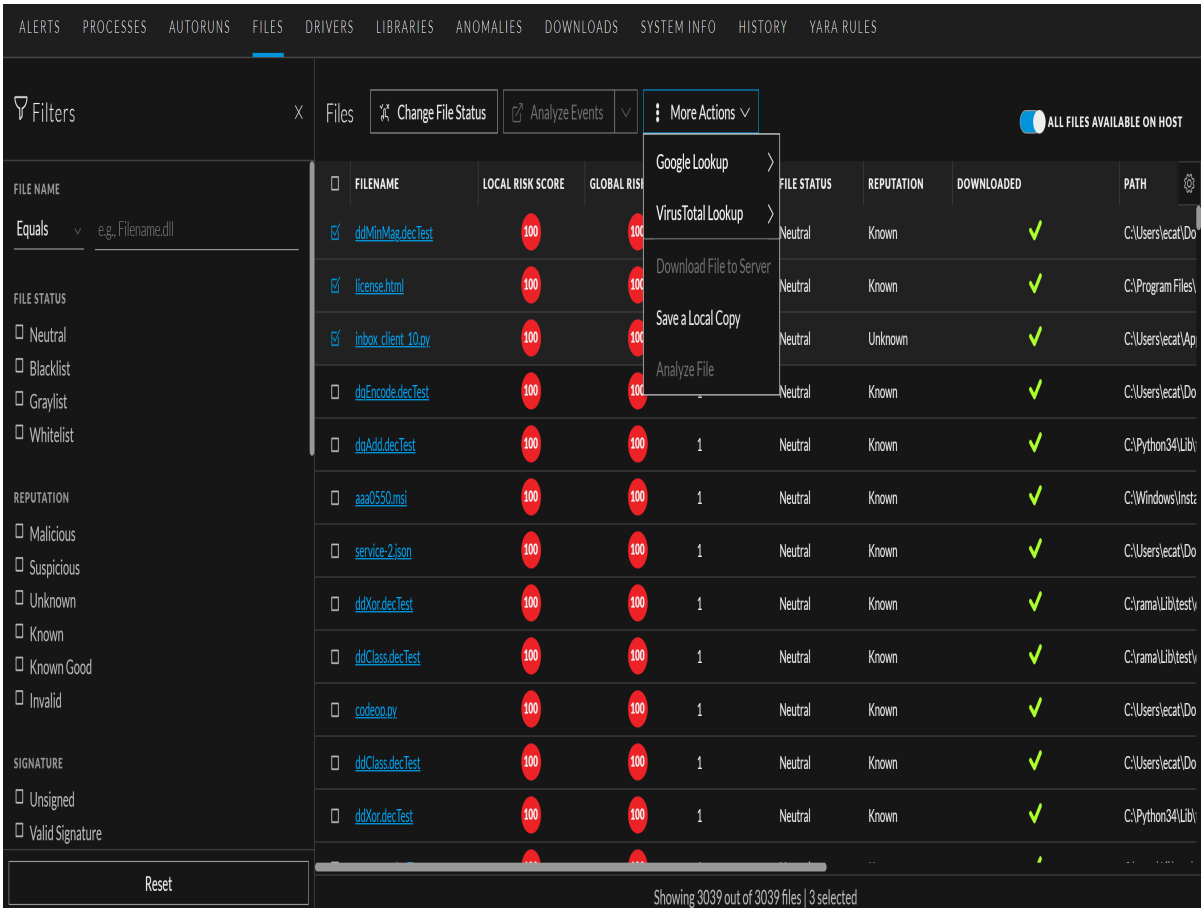
   Note: allfiles.json file is exported irrespective of the selected snapshot.

- 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:



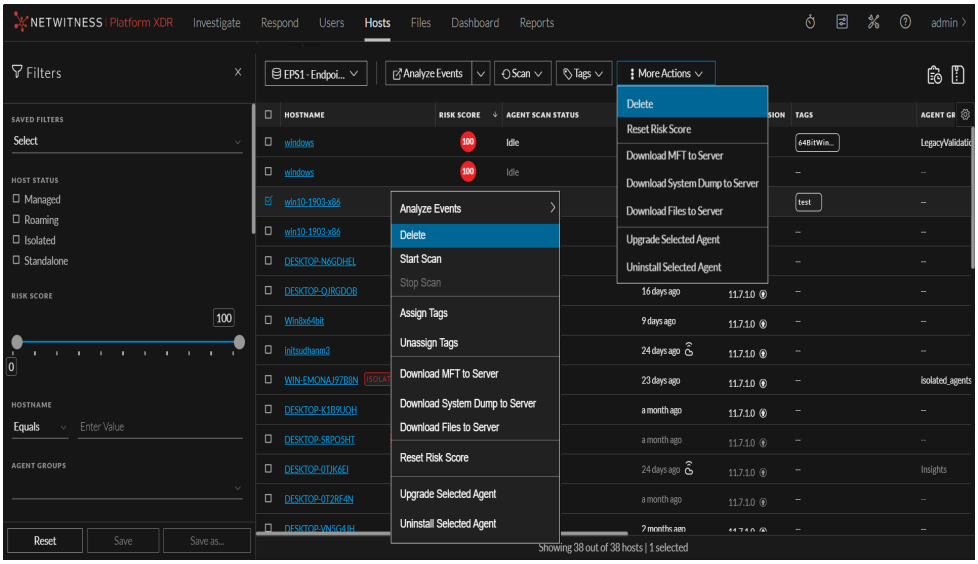
- Select **Google Lookup** to perform a search on the filename, MD5, SHA1, or SHA256.
- Select **VirusTotal Lookup** to perform a search on MD5, SHA1, or SHA256.

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:



- 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:

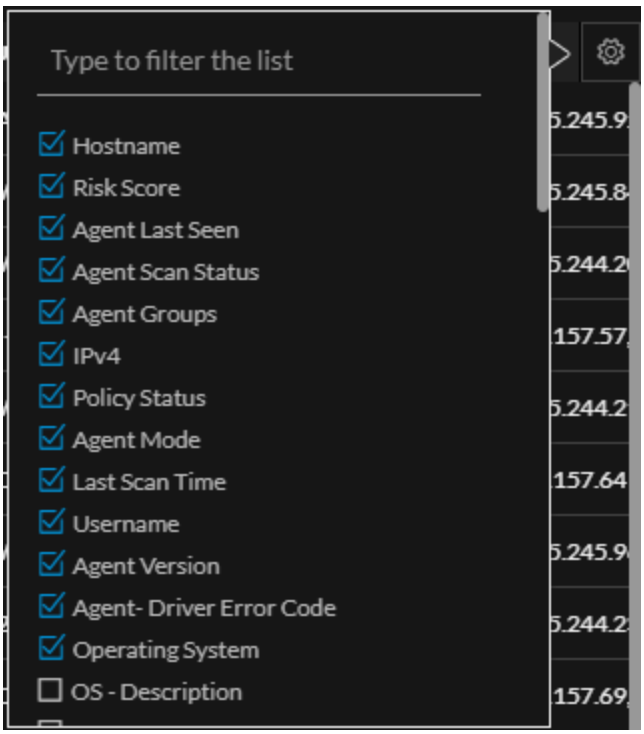
1. Go to **Hosts** view.
2. Filter the hosts based on the Agent version, and delete these hosts.

   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 drop-down list displayed while adding columns:



3. Scroll down or enter the keyword to search for the column in the displayed list.
4. Sort the data on the required column.

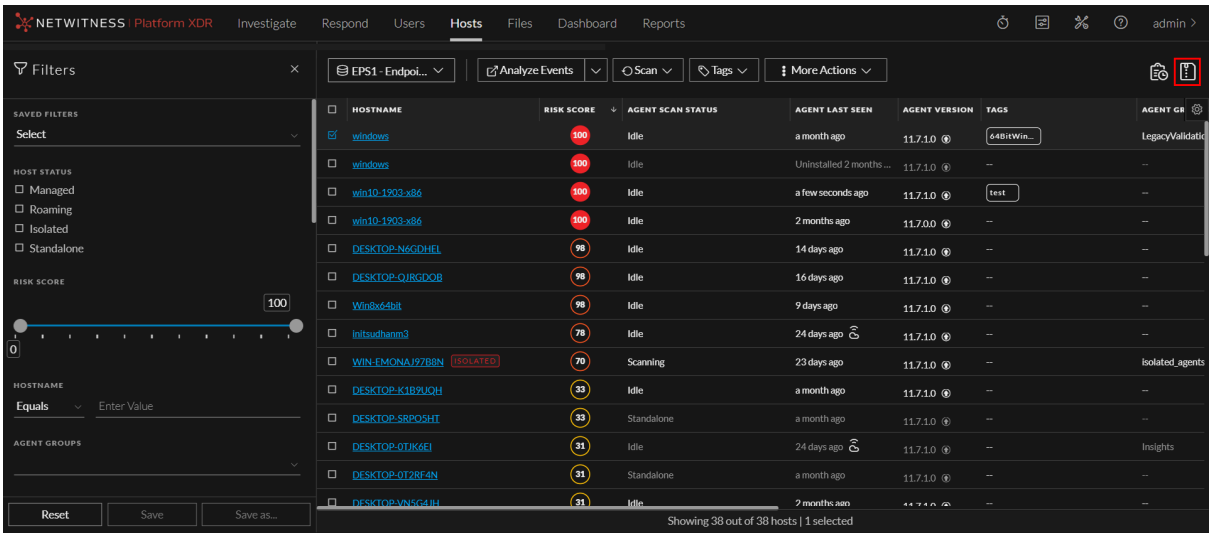
Note: The selections you make here become your default view every time you log in to the Hosts view.

Export Host Attributes

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

1. Go to **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.



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.

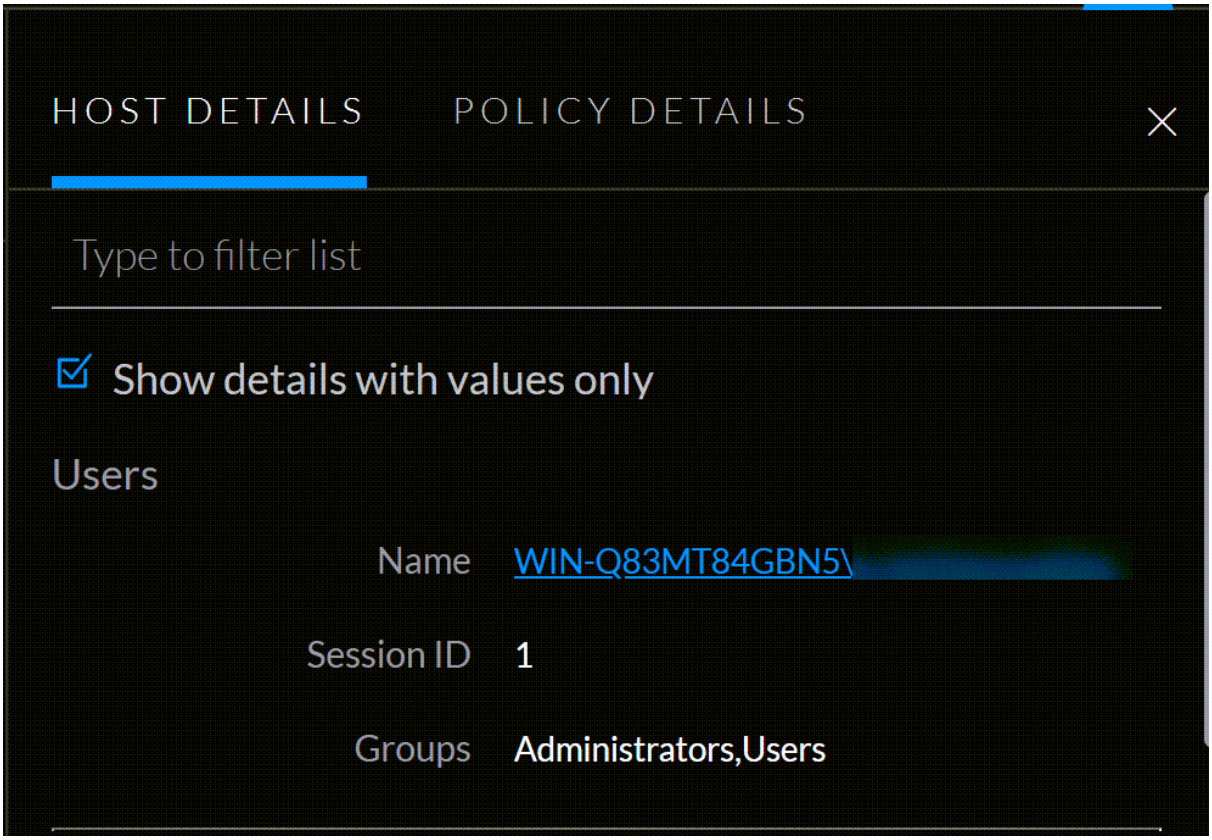
Note: To view only managed hosts, select the **Show Only Managed Agents** option in the Filters panel.

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.



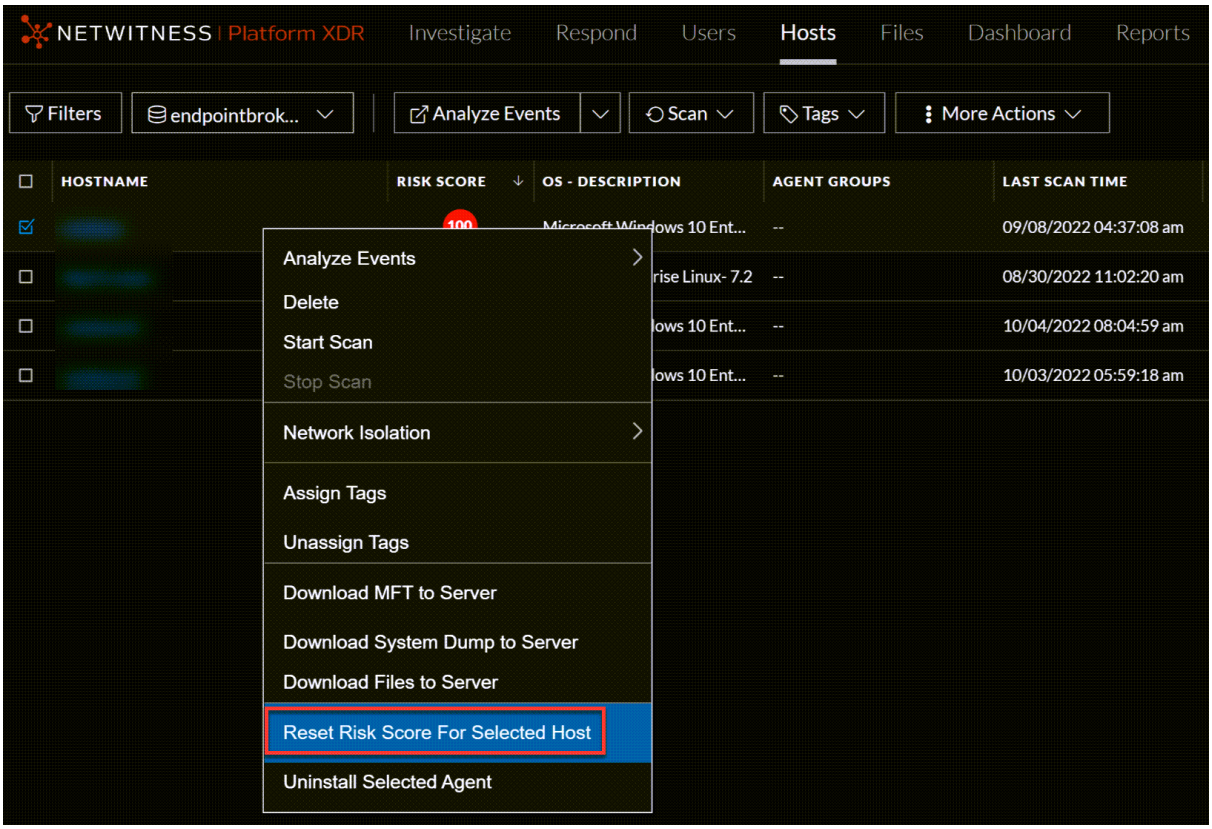
Resetting Risk Score of Hosts

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:



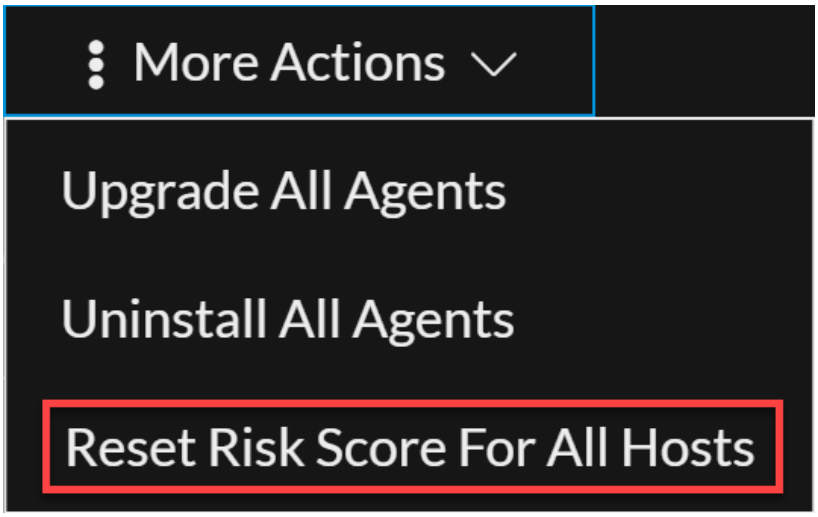
- Right-click and select **Reset Risk Score For Selected Host** from the context menu.
- Click **More Actions** > **Reset Risk Score For Selected Host** in the toolbar.

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.

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

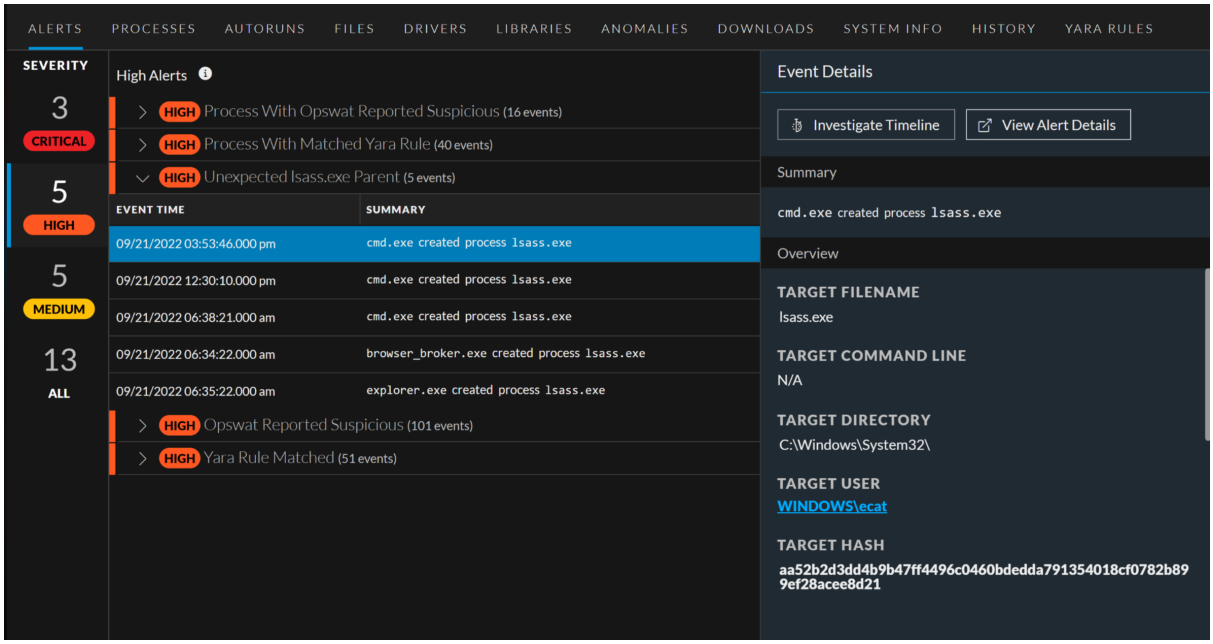
Note: Linux is not supported for analyzing a process.

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:

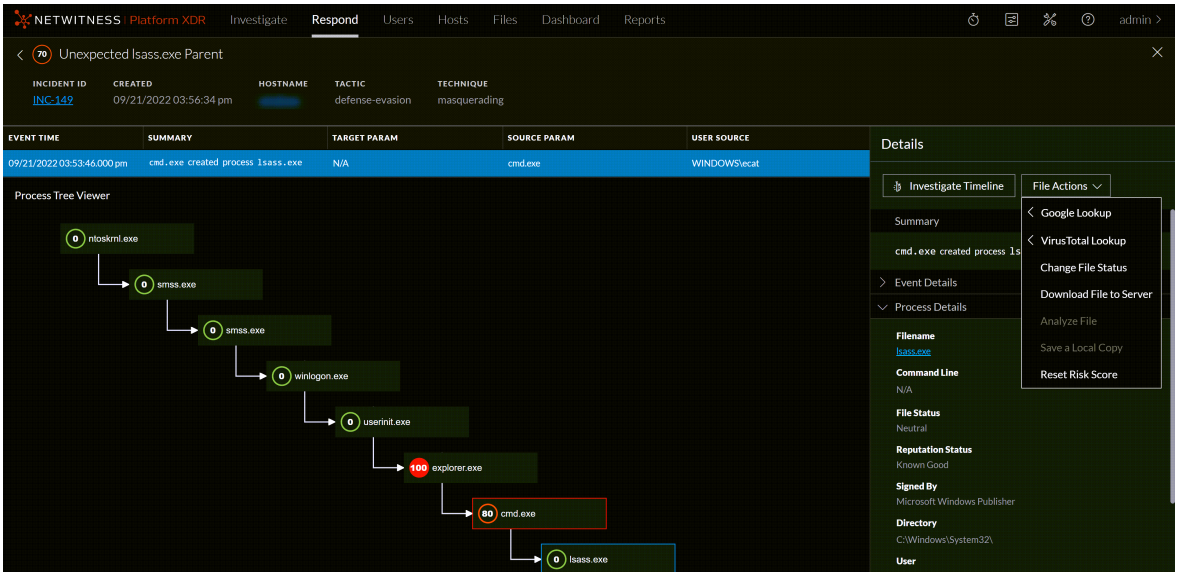
1. Go to **Hosts** and click on a host.
2. Click on an event associated with the **Critical** or **High** alert on the Host Details view. The **Event Details** panel appears.
3. Click **View Alert Details** to analyze the process activities of a file associated with the **Critical** or **High** Alerts.



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**

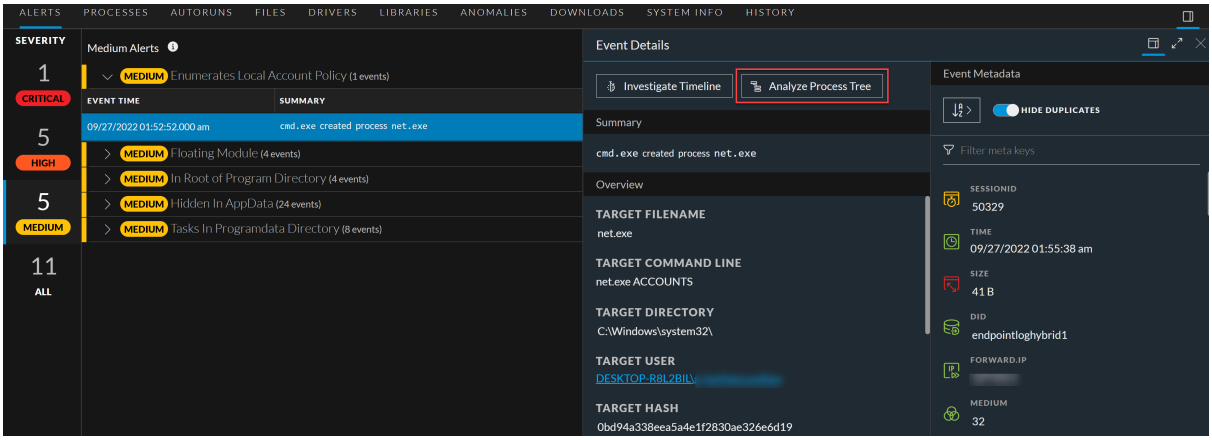
- **Reset Risk Score**



To analyze the process associated with Medium Alerts:

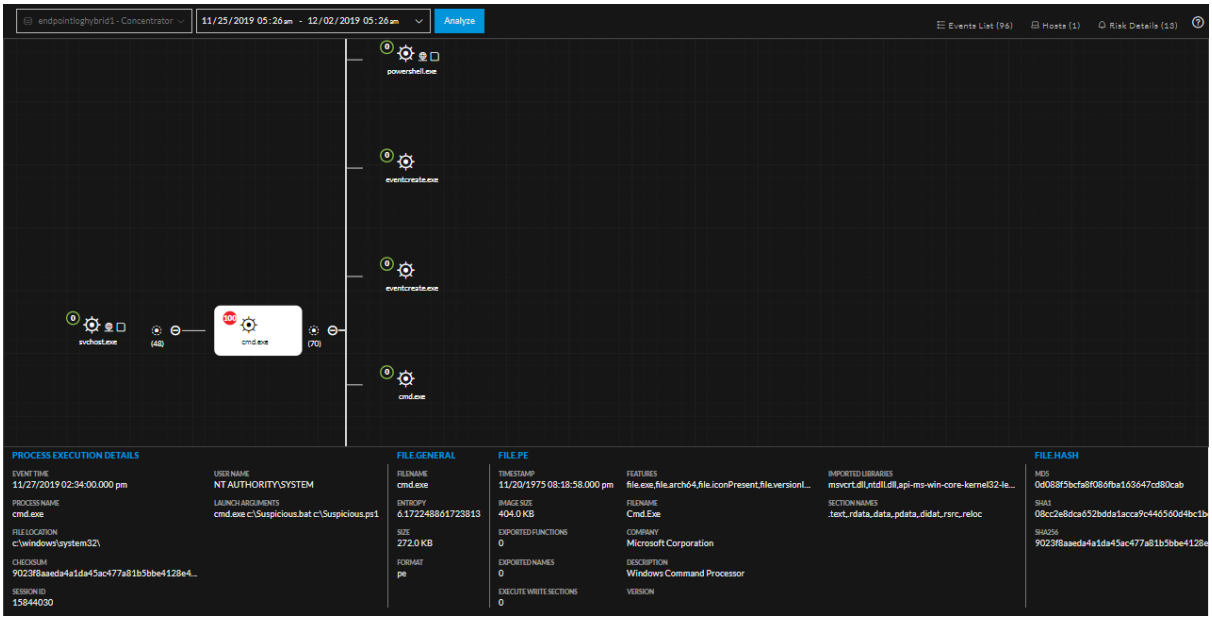
1. Go to **Hosts** and click on a host.
2. Click on an event associated with the **Medium** alert on the Host Details view. The **Event Details** panel appears.
3. To analyze the process activities of a file associated with the **Medium** Alerts, do one of the following:
   - In the **Event Details**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



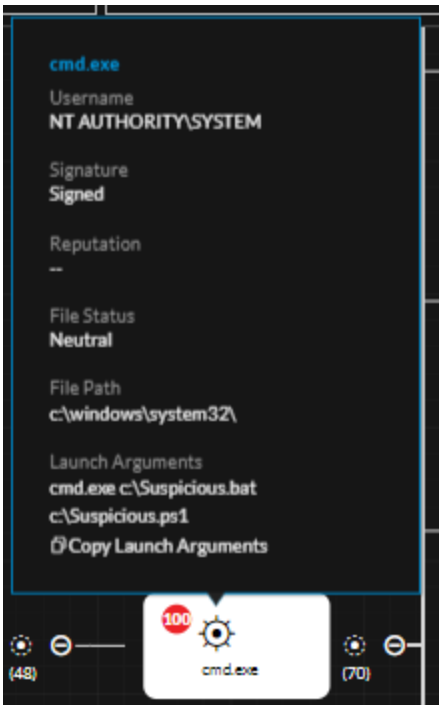
Clicking **Analyze Process** displays the process visualization. For each node, the process name, risk score, and type of activity the selected process has performed (network, file, or registry) are displayed. Optionally, you can change the time range to view data.

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



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.

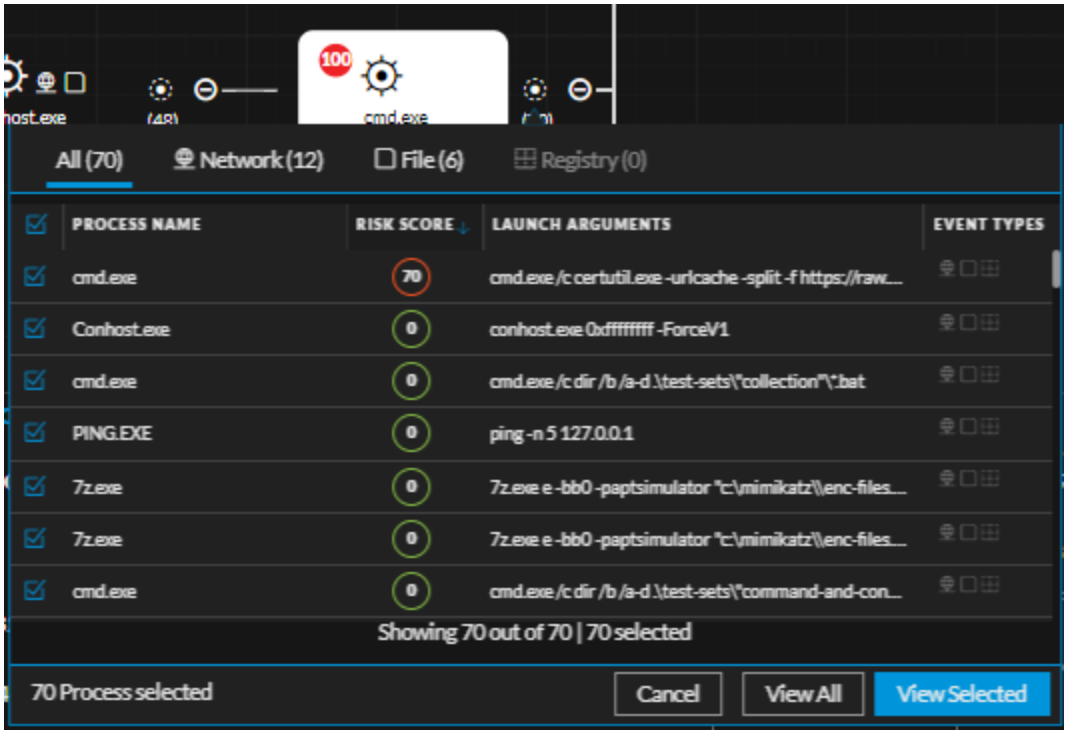


6. Click to view the child processes. The Process selection dialog is displayed with the child processes associated with the process based on the risk score. You can filter the result on the event type by clicking icons on the top panel. When no matching event types are available, these filter options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

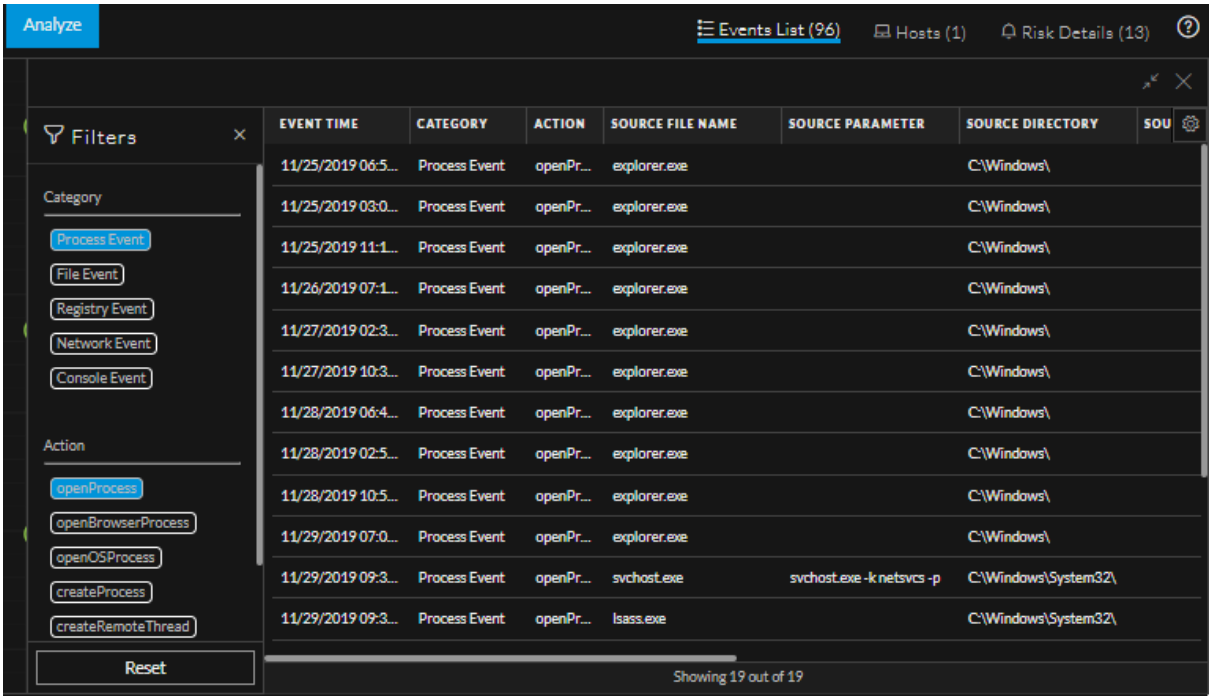


Analyze Events for a Process

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).

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



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

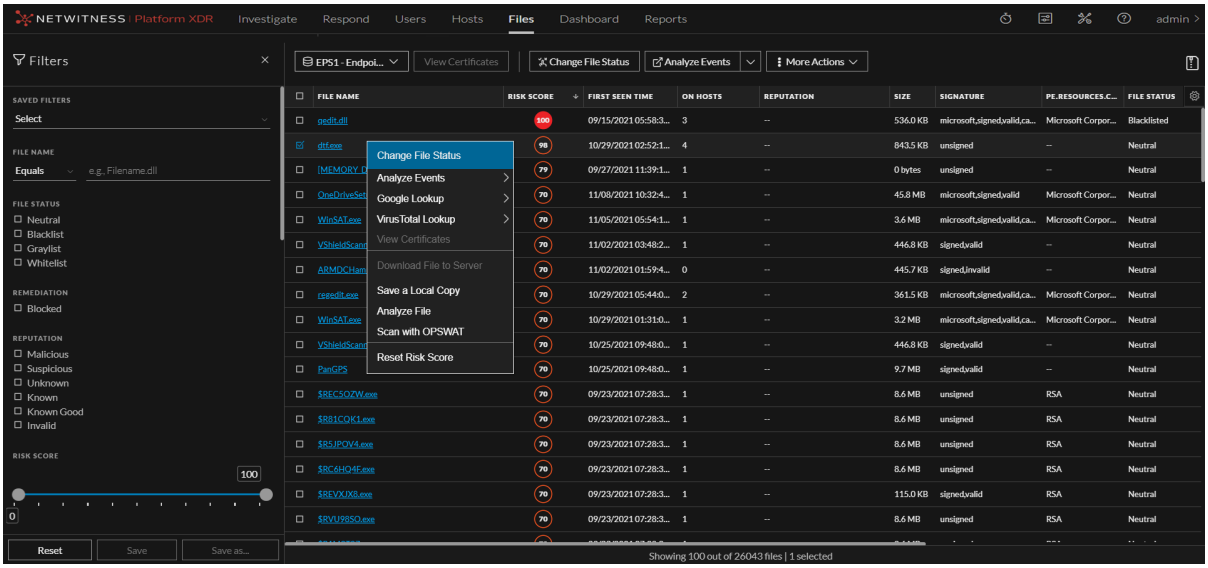
Note: For the console events, the context for local and remote are available only if the data is sent from 11.4 or later agents.

Changing File Status or Remediate

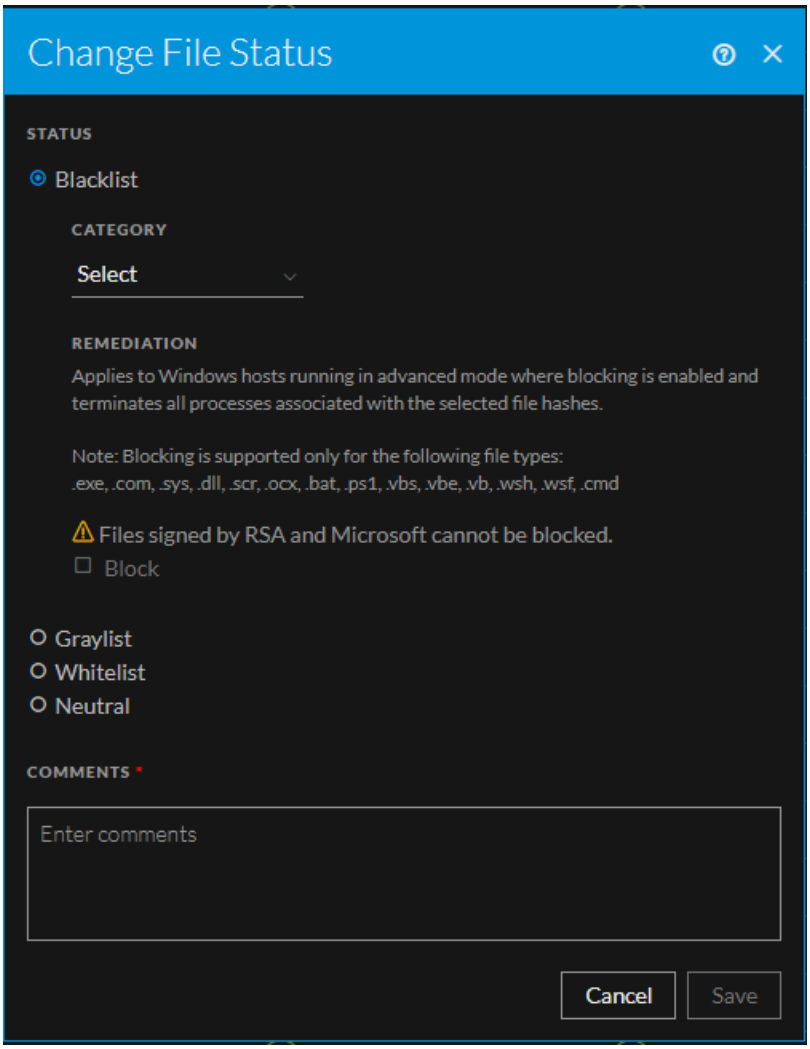
Note: By default, the blocking option is disabled in the policy. To enable blocking, in the policy configuration, change the **Blocking** option to **Enabled** under Response Action Settings. For more information, see the *NetWitness Endpoint Configuration Guide*.

To change the status of a file:

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



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



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

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

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

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

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

Note: Blocking is supported only for Windows hosts 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 Changing File Status 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":
["1b30e463ebe0131db66fce7d4aa43f3e149064d85c4c0dc5218b077886da2804","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:

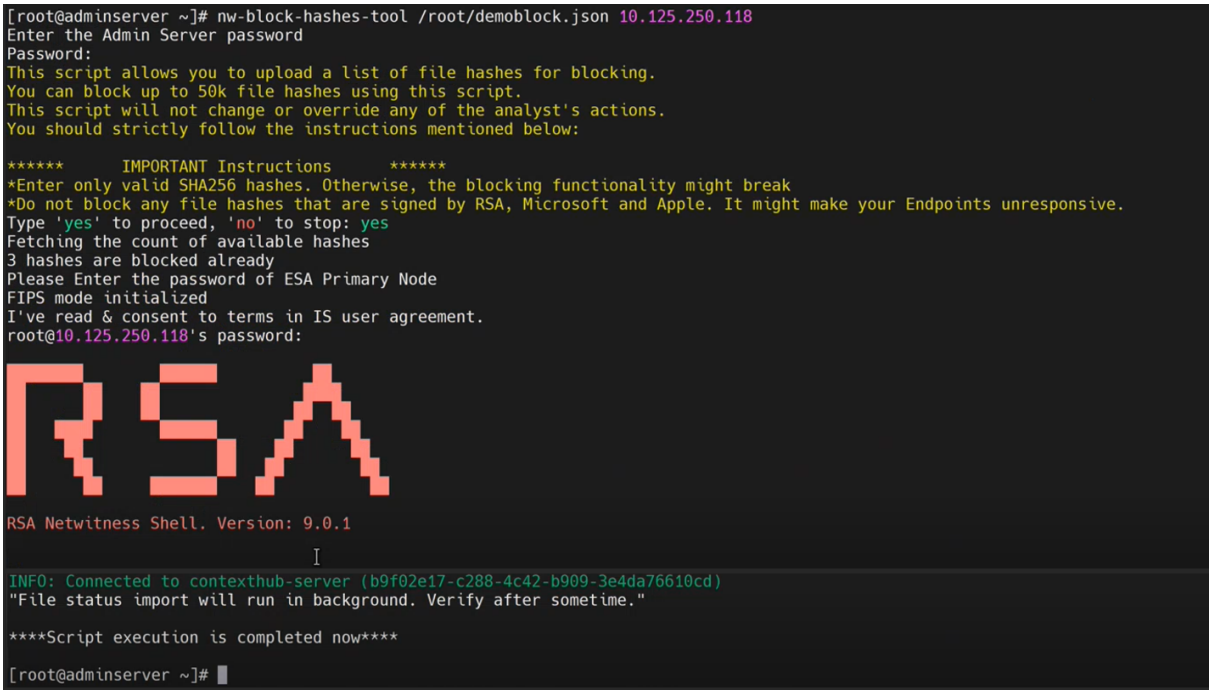
```
[{
"checksums":
["2b30e463ebe0131db66fce7d4aa43f3e149064d85c4c0dc5218b077886da2800","97fa30e4
63ebe0131db66fce7d4aa43f3e149064d85c4c0dc5218b077dsbhb500","38vbba909e463ebe0
131dsdsdb66fce7d4aa43f3e1dsdsd49064d85dsdsman68c"],
"fileStatus": "Blacklist",
"comment": "File status change set through new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

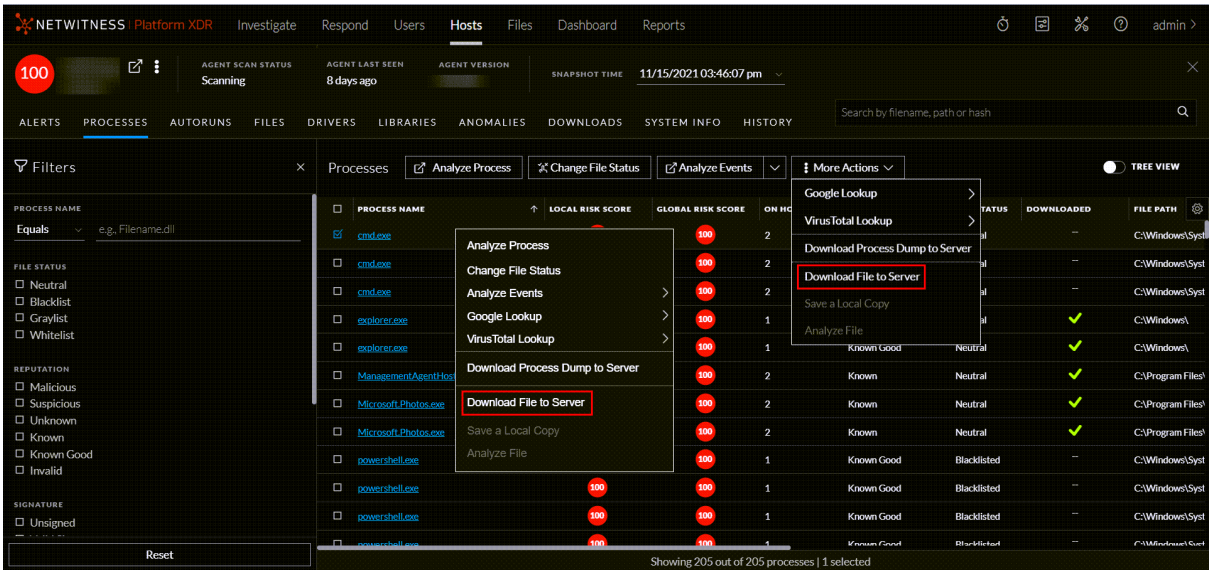
By default, the files that are unsigned and size lesser than or equal to 1 MB are downloaded automatically to the NetWitness Endpoint server. And, only single copy of each file is downloaded automatically. You can limit the volume of files to be downloaded in the **> Endpoint Sources > Policies** tab, 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:

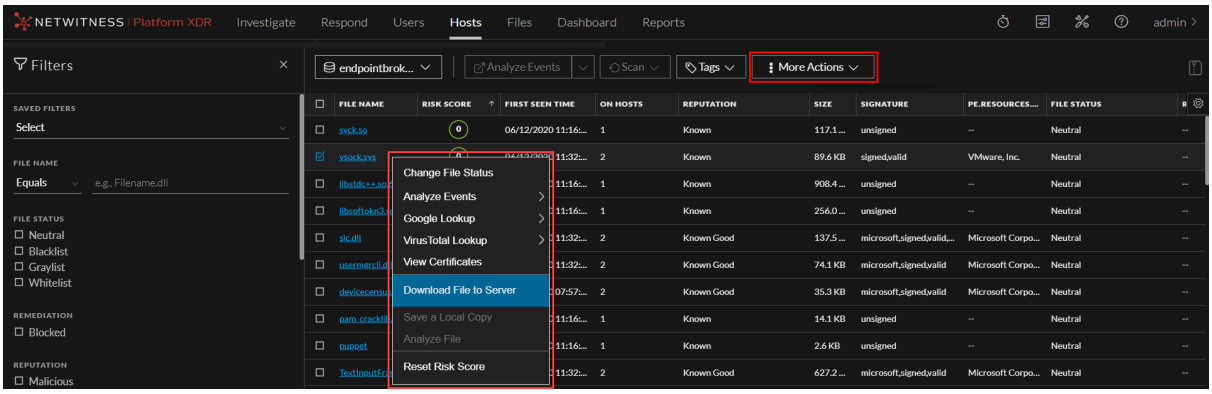
1. Go to **Hosts**.
2. Select the hostname to open the Host Details view.
3. In any of the Processes, Autoruns, Files, Drivers, Libraries, or Anomalies tabs, select the file, and do one of the following:



- 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:



- 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.

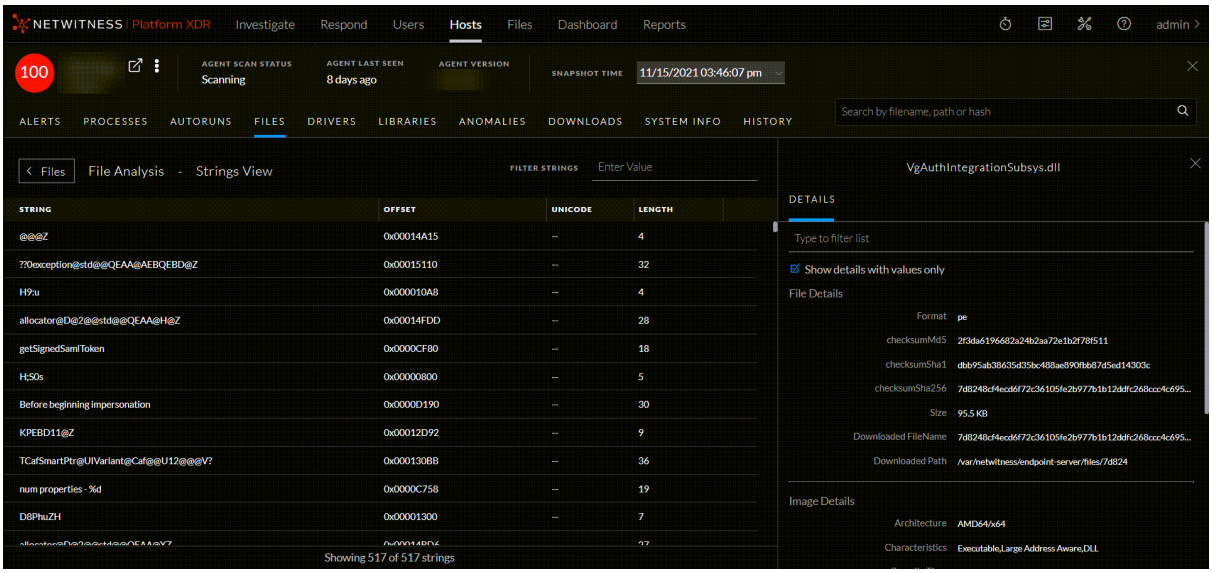
To save a file:

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

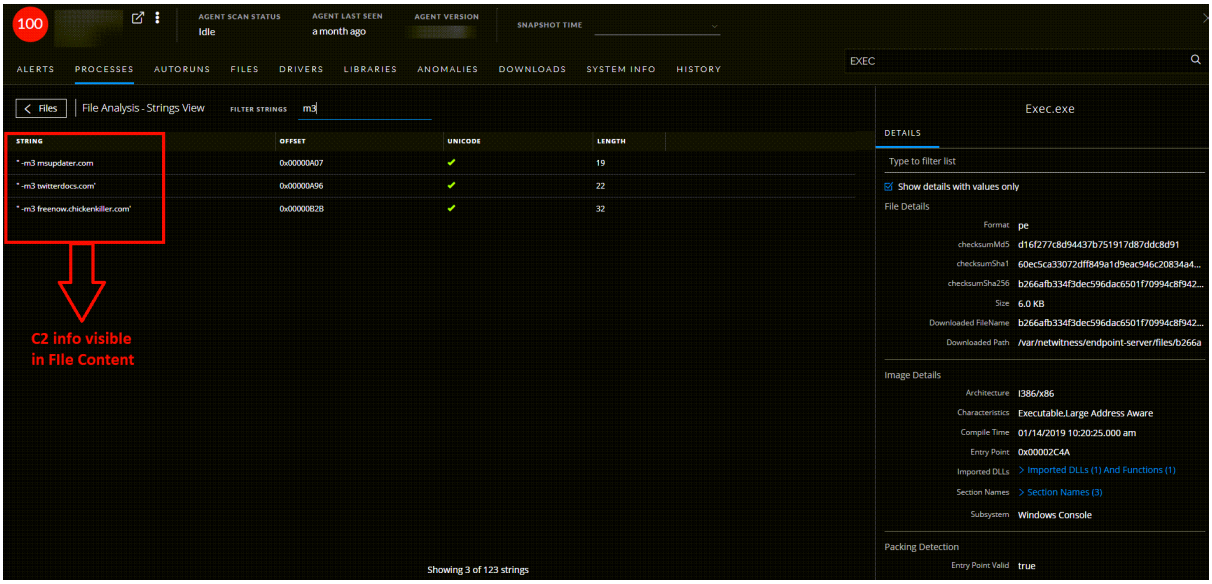
You can use the **Analyze File** option to view detailed information about a downloaded file. This option is enabled only if the file is downloaded to the server. To analyze a file:

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.

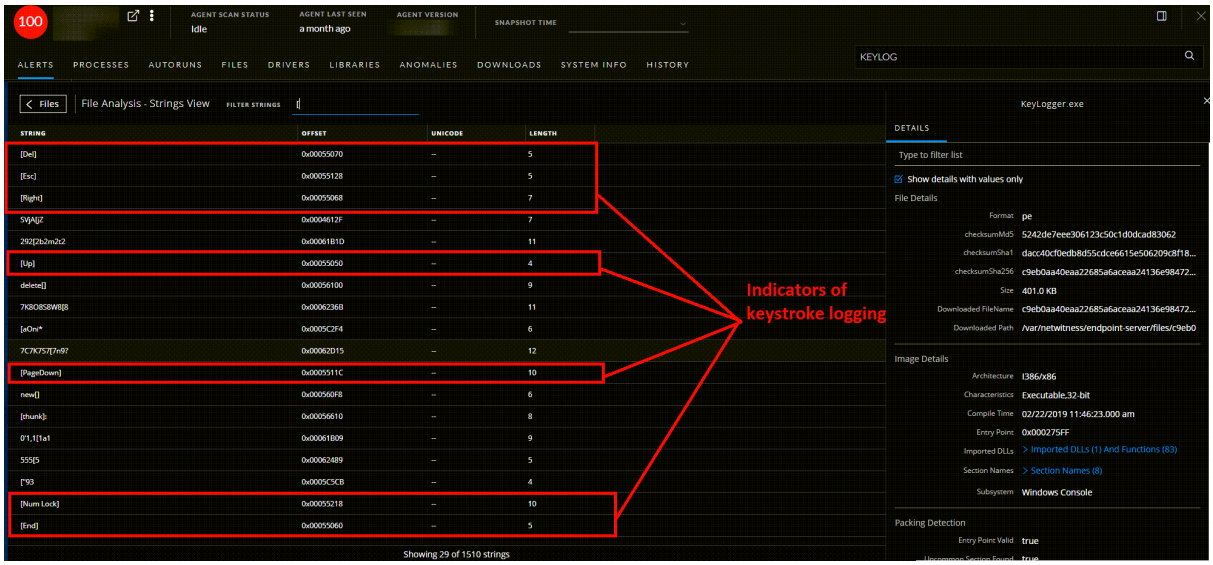


3. View strings in the file in the Strings view while analyzing an executable (such as `macho`, `pe`, `elf`). This view contains the string, offset in the binary, unicode, and the length of the string. You can search for or filter on a specific string value in the **Filter String** field.
4. View the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



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
AGENT SCAN STATUS
Idle
AGENT LAST SEEN
a month ago
AGENT VERSION
SNAPSHOT TIME
ALERTS
PROCESSES
AUTORUNS
FILES
DRIVERS
LIBRARIES
ANOMALIES
DOWNLOADS
SYSTEM INFO
HISTORY
KEYLOG
Files
File Analysis - Strings View
FILTER STRINGS
STRING
OFFSET
UNICODE
LENGTH
[Del] 0x00055070 -- 5
[Esc] 0x00055128 -- 5
[Right] 0x00055068 -- 7
5VjAJjZ 0x0004612F -- 7
292[2b2m2r2 0x00061B1D -- 11
[Up] 0x00055050 -- 4
delete[] 0x00056100 -- 9
7K8O8S8W8J8 0x00062368 -- 11
[aOn* 0x0005C2F4 -- 6
7C7K7S7[7n9? 0x00062D15 -- 12
[PageDown] 0x000551C -- 10
new[] 0x000560F8 -- 6
[chunk]: 0x00056610 -- 8
01,1[1a1 0x00061B09 -- 9
555[5 0x00062489 -- 5
[*93 0x0005C5CB -- 4
[Num Lock] 0x00055218 -- 10
[End] 0x00055060 -- 5
Showing 29 of 1510 strings
Indicators of keystroke logging
KeyLogger.exe
DETAILS
Type to filter list
Show details with values only
File Details
Format pe
checksumMd5 5242de7eee306123c50c1d0dcad83062
checksumSha1 dacc40cf0edb8d55cdce6615e506209c8f18...
checksumSha256 c9eb0aa40eaa22685a6aceaa24136e98472...
Size 401.0 KB
Downloaded FileName c9eb0aa40eaa22685a6aceaa24136e98472...
Downloaded Path /var/netwitness/endpoint-server/files/c9eb0
Image Details
Architecture I386/x86
Characteristics Executable,32-bit
Compile Time 02/22/2019 11:46:23.000 am
Entry Point 0x000275FF
Imported DLLs > Imported DLLs (1) And Functions (83)
Section Names > Section Names (8)
Subsystem Windows Console
Packing Detection
Entry Point Valid true

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.

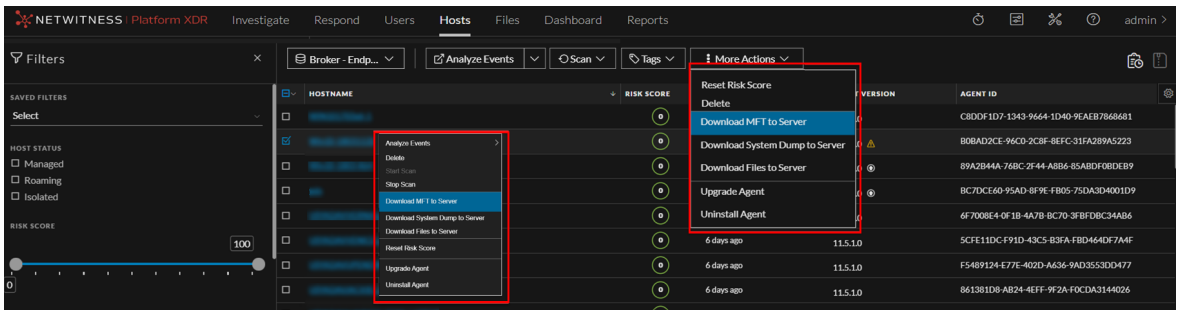
Time stomping is a technique that modifies the timestamps for a file (creation, access, update, and modification time) to mimic files that are in the same folder, making it difficult to identify suspicious files on a host. To perform forensic investigation of a suspicious file, you can download and analyze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

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

Download MFT to Server

To download MFT to the server from the Hosts view:

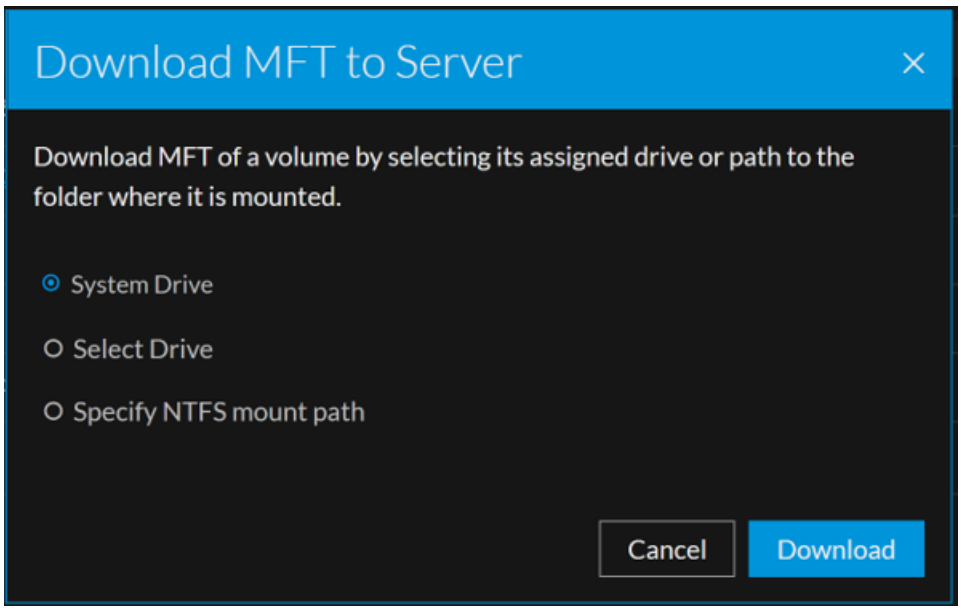
1. Go to **Hosts** and do one the following:
   - Select one or more hosts and select **Download MFT to Server** from the right-click context menu, or from the **More Actions** drop-down list in the toolbar.



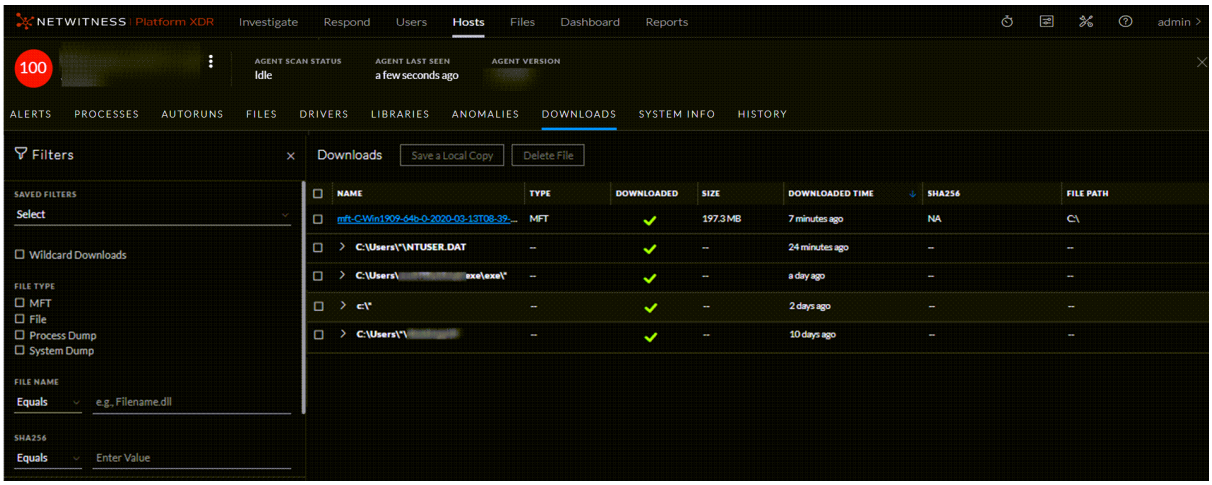
   - Select the hostname to open the host details, click ⋮ (**More**) beside the hostname, and select **Download MFT to Server**.

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 Hosts View - Downloads Tab.



Analyze Downloaded MFT

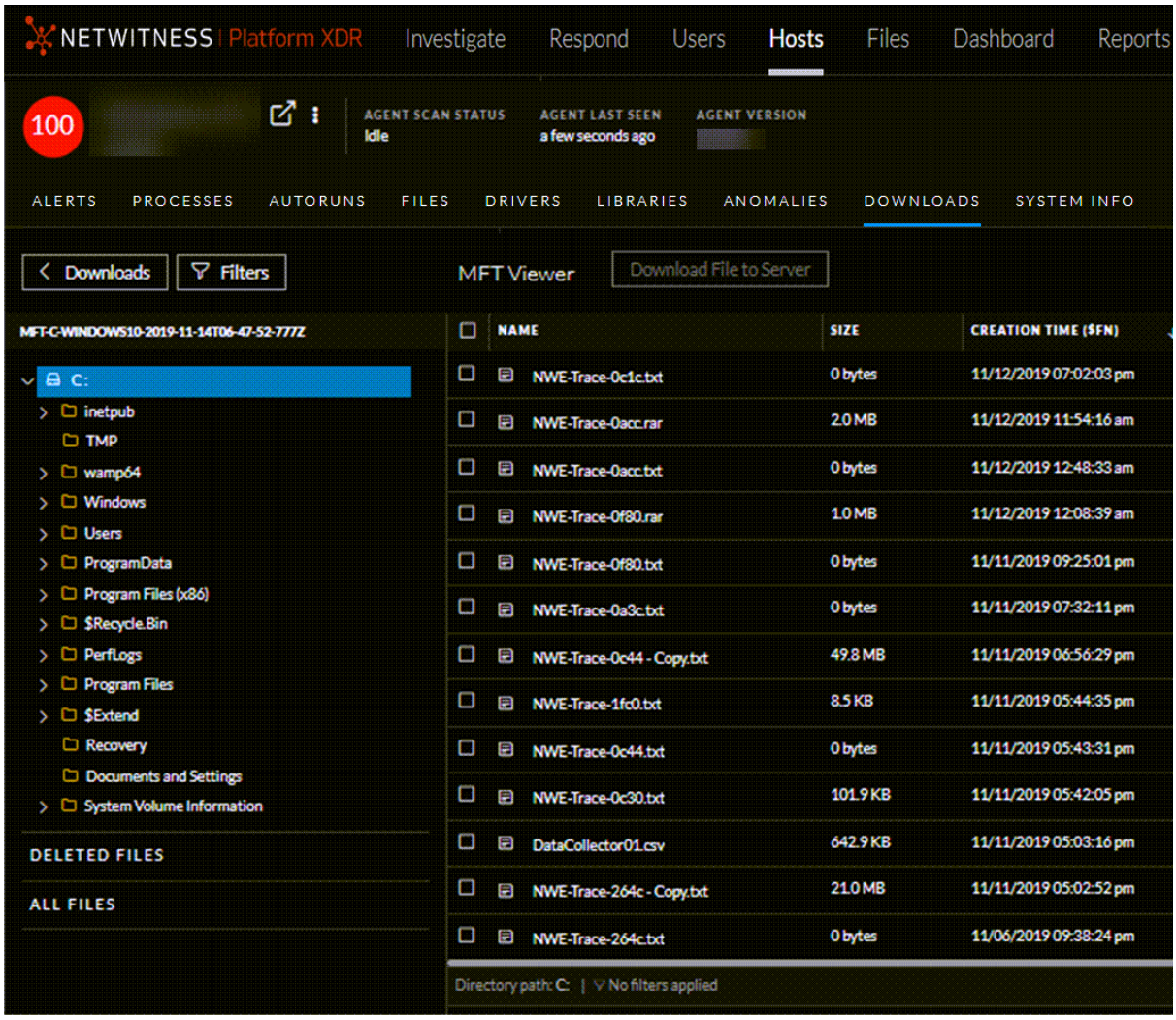
You can use the MFT viewer to begin analysis where you can search for files based on file name, time stamps, and identify files that are timestomped.

View MFT

To view the content of the downloaded MFT:

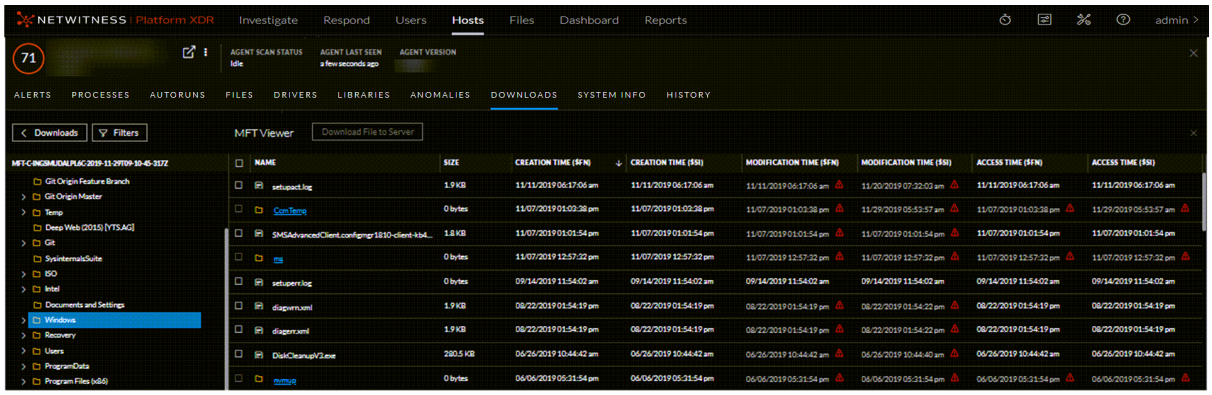
1. Go to **Hosts**.
2. Select the hostname to open the host details and select the **Downloads** tab.
3. Click the file name. The MFT viewer is displayed.

   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.



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

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

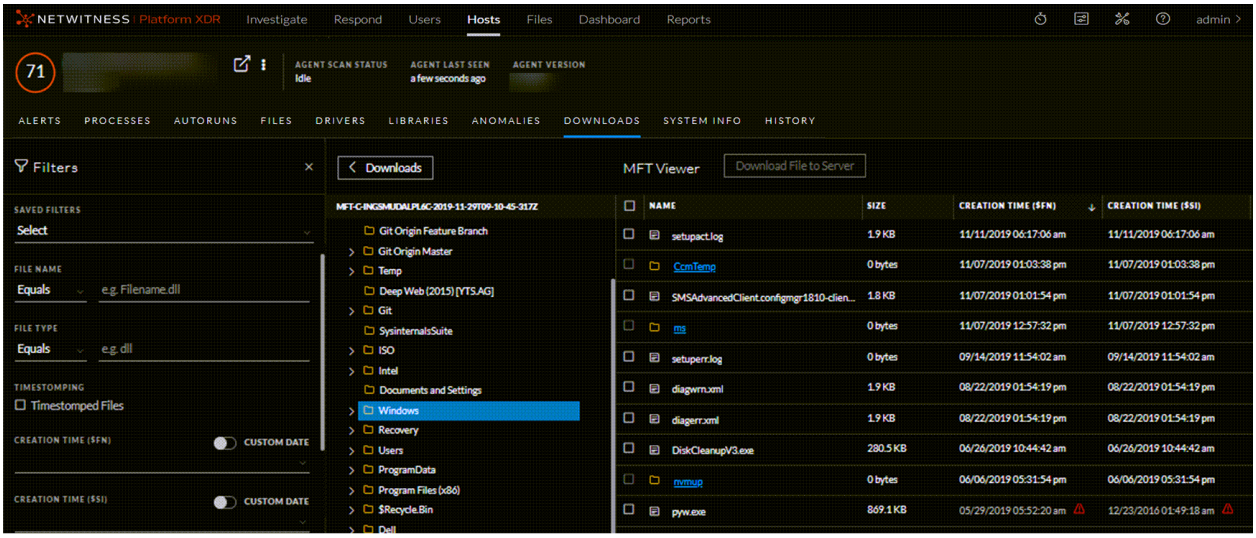


5. Select one or more files and click **Download File to Server** on the toolbar to download files to the server.

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

Filter MFT

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



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

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

To filter, save, and delete MFT, see Filter Downloaded Files, Save Downloaded File, and Delete Downloaded Files.

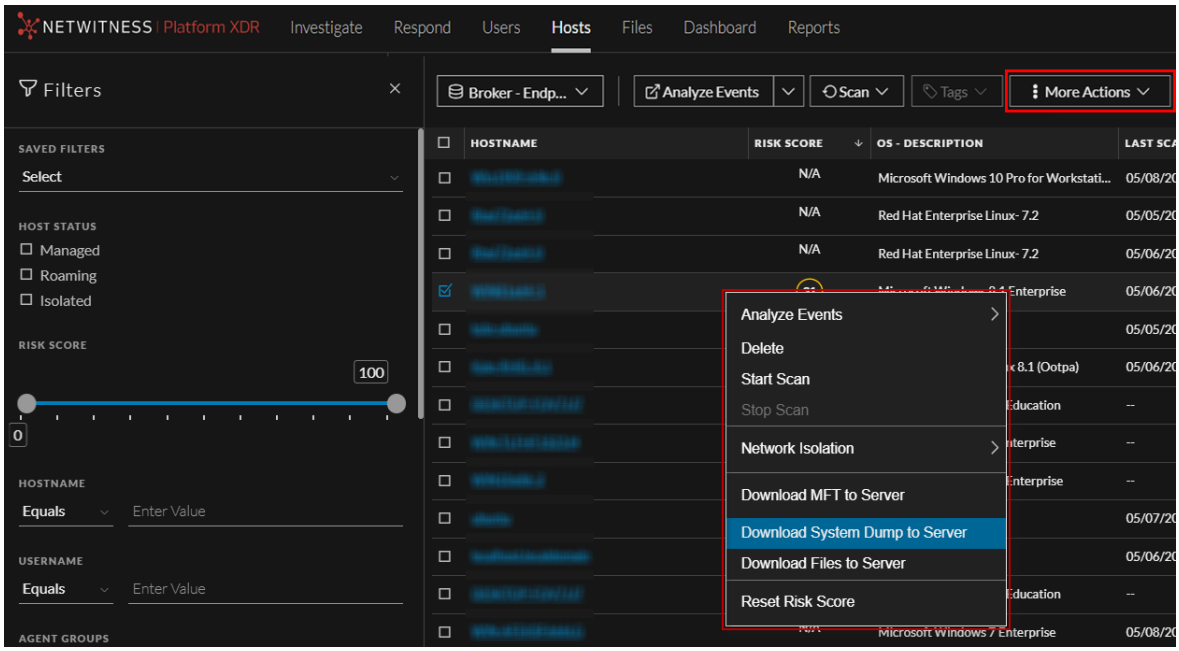
System and Process Memory Dump

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

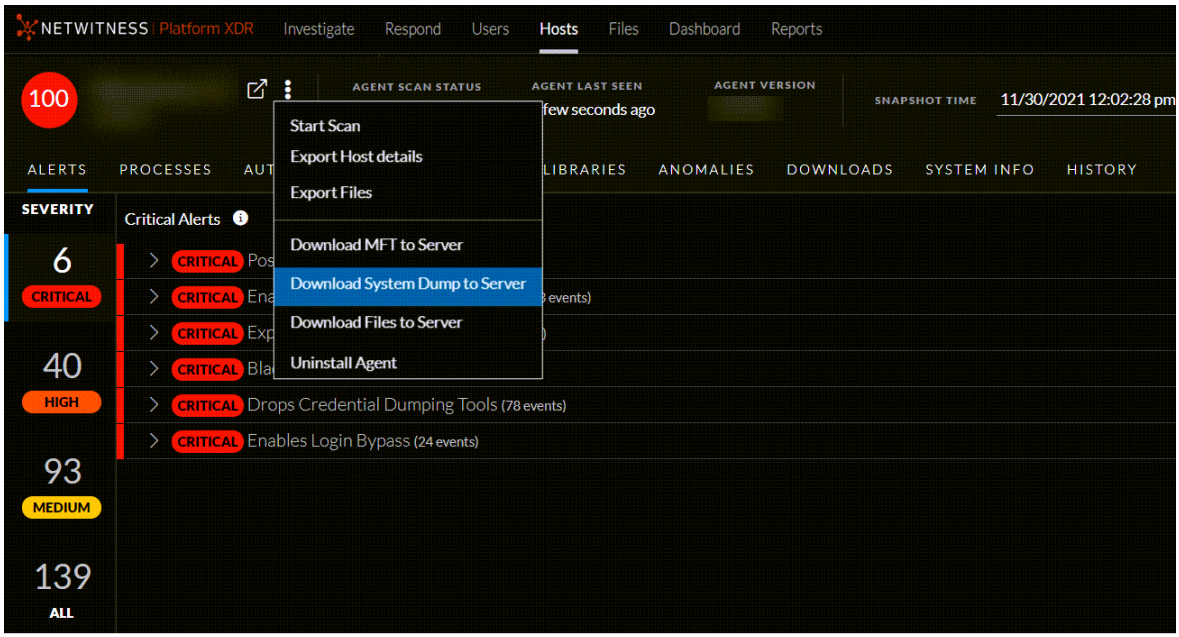
Download System Dump to Server

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

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



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

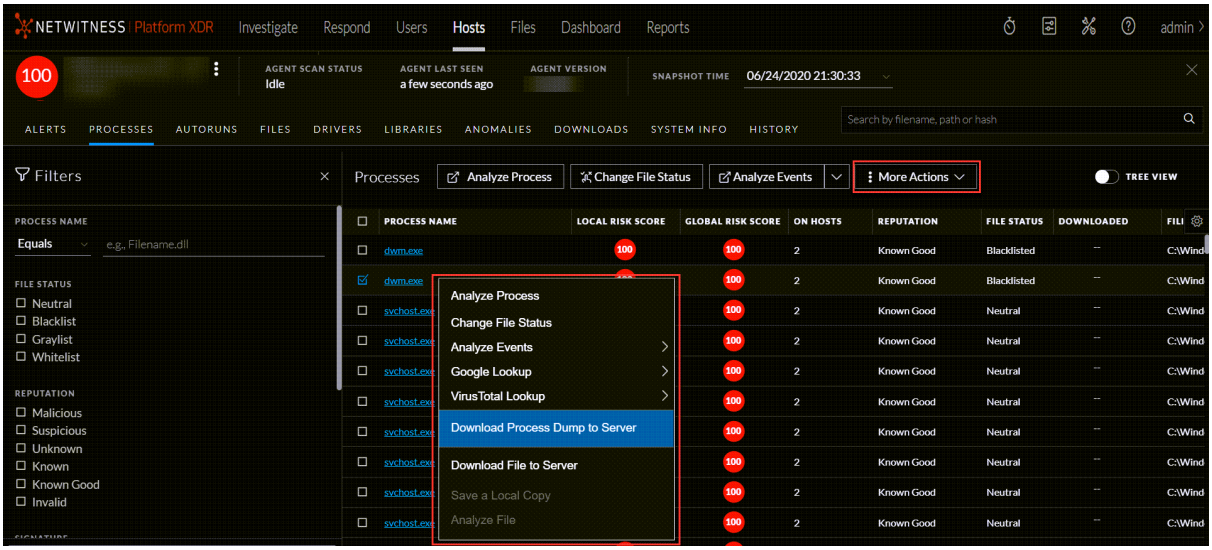


2. View the details of the downloaded system dump in the **Downloads** tab within the host details. For more information, see Hosts View - Downloads Tab.

Download Process Dump to Server

To download process dump to the server:

1. Go to **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.



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

To filter, save, and delete system dump or process dump, see Filter Downloaded Files, Save Downloaded File, and Delete Downloaded Files.

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

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

Download Files Using Full Path or Wildcard

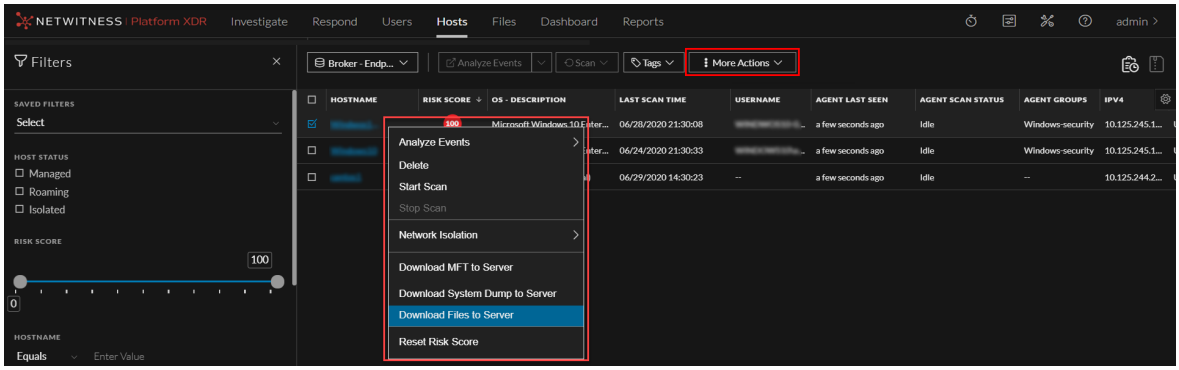
You can manually download files that help in investigations by either providing full path of the file or using wildcard.

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

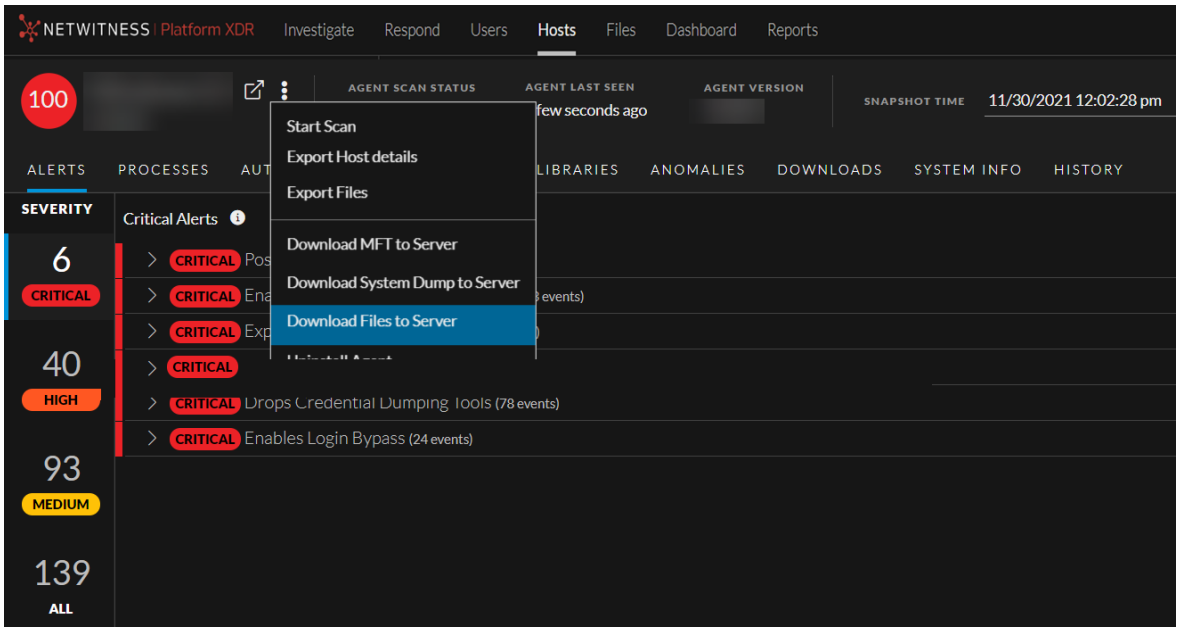
To download files to the server:

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.



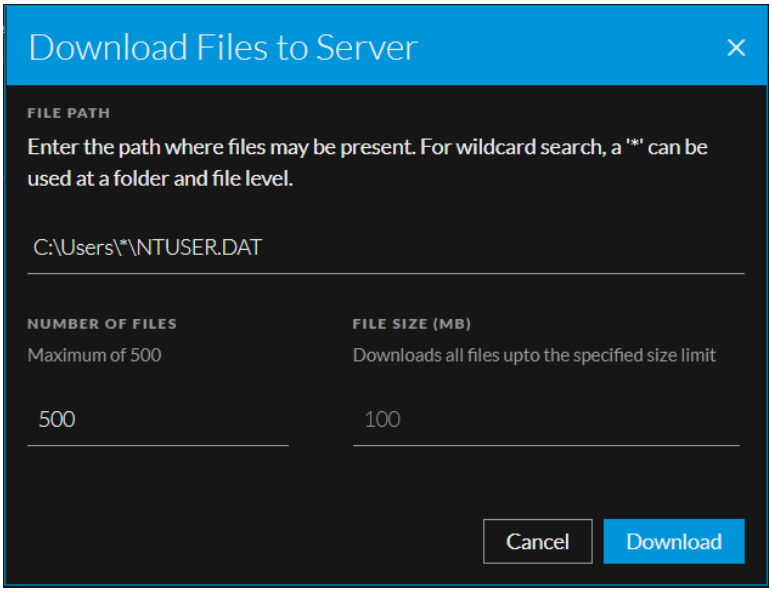
   - Select the hostname to open the host details, click ⋮ (**More**) beside the hostname, and select **Download Files to Server**.



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`.

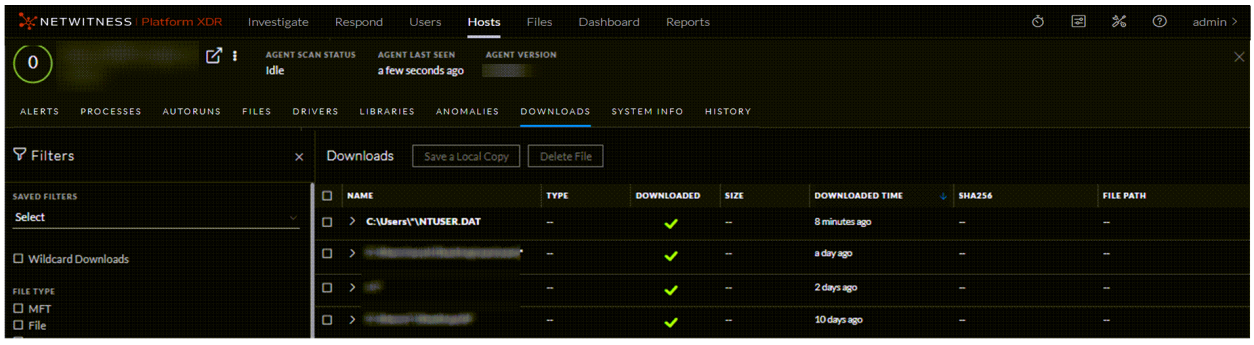


3. For wildcard search, enter the number of files to download and size of the file. By default, the number of files is set to 10 and file size is set to 100 MB. For example, if the maximum number of files is set to 10 and file size is set to 10 MB, first 10 files within 10 MB are downloaded.

> **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.

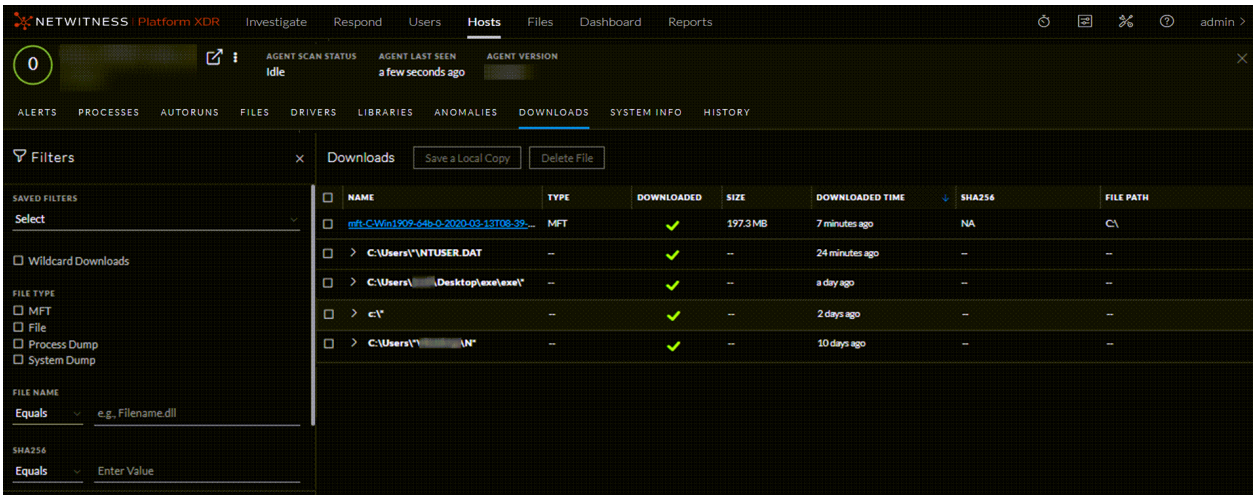
4. Click **Download**.

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.



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.



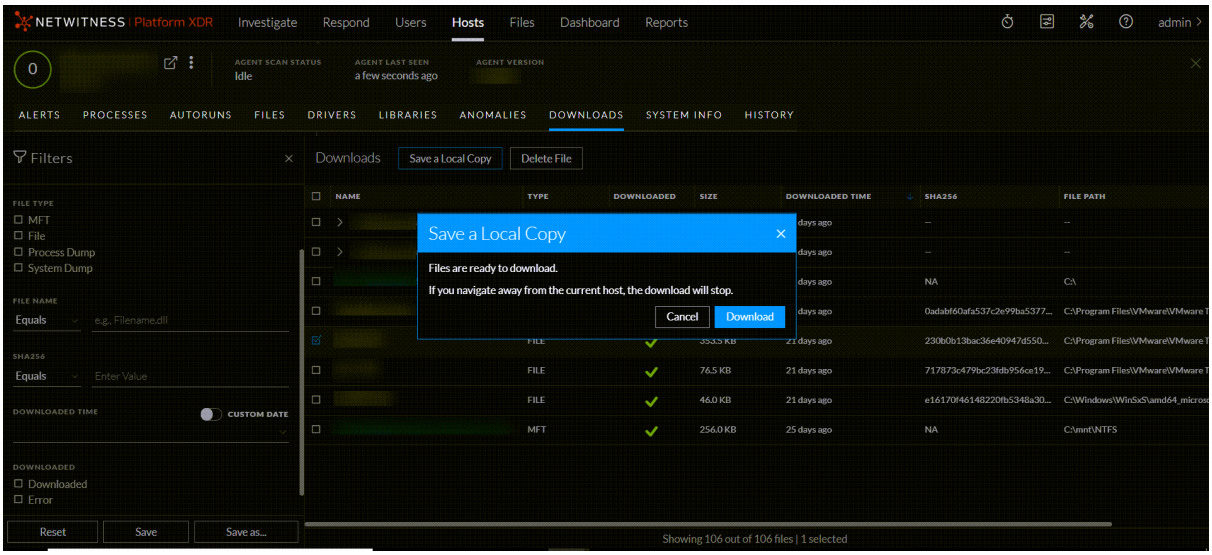
Click **Save** to save the filter and provide a name (up to 250 alphanumeric characters). The filter is added to the Saved Filters panel on the left. To delete a filter, hover over the filter name and click .

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

Save Downloaded File

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

1. Go to **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.



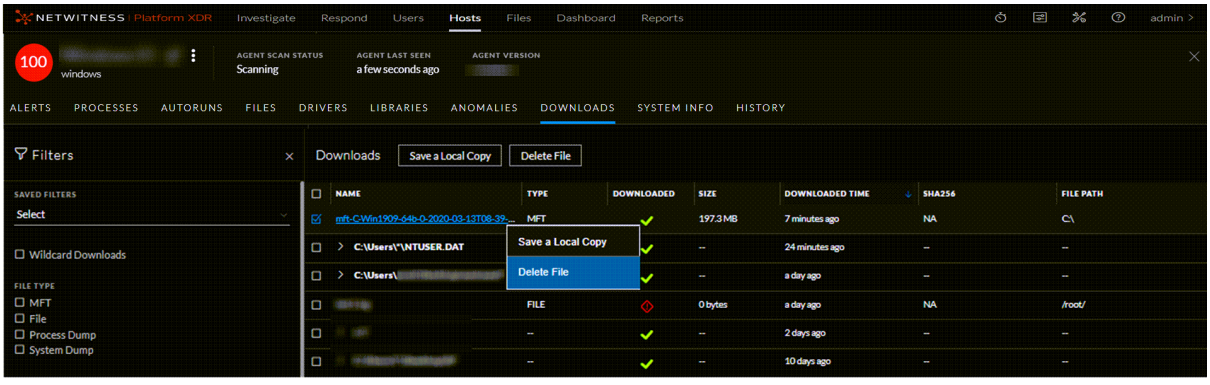
4. In the **Save a Local Copy** dialog, click **Download**.

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.



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

Analyzing Events

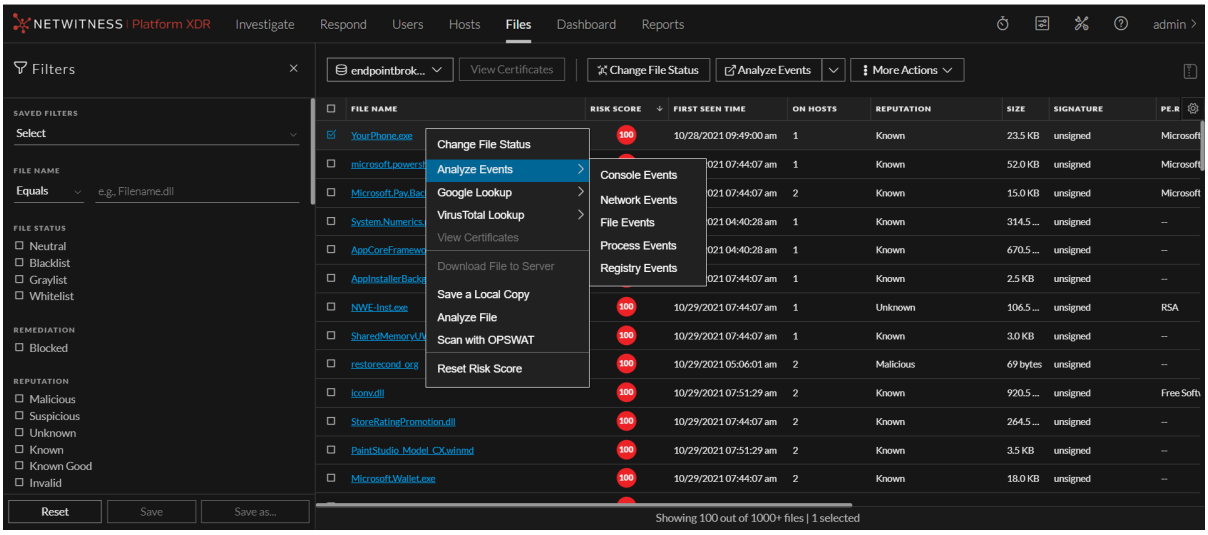
If you need to investigate a particular host, IP address, username, filename, or hash to look for related activity across a time range, you can pivot to Navigate view to get the entire context of the activity. By default, the time range is set to 7 days. You can change the time range.

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.



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

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

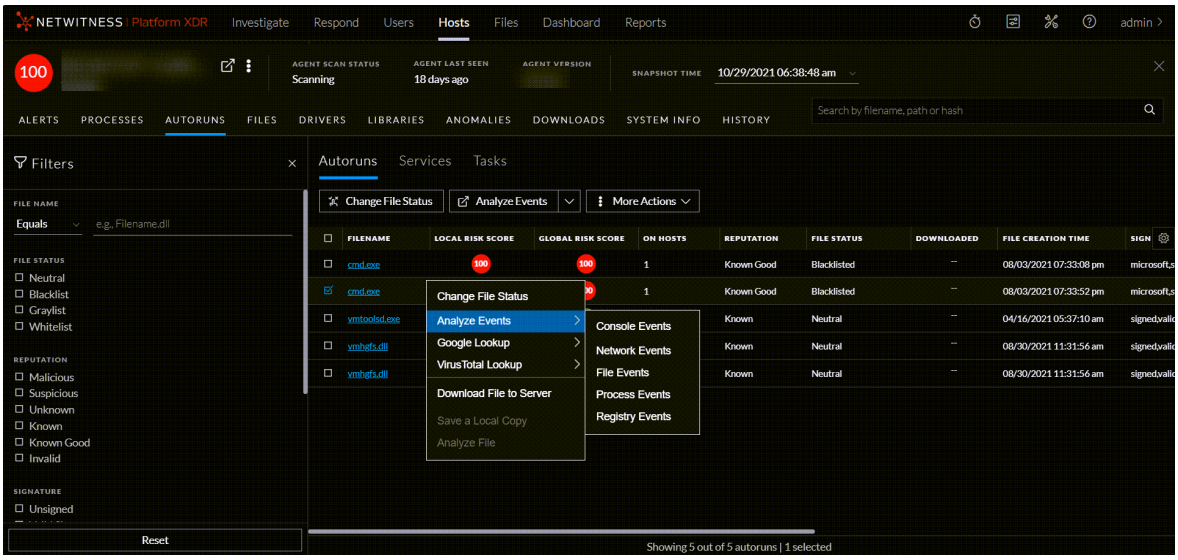
Analyze Events from Hosts View

To investigate a particular host, IP address (IPV4), or username:

1. Go to **Hosts**.
2. Do one of the following:

- Right-click a host, select **Analyze Events** from the right-click context menu or in the toolbar, and select a specific event type (such as network events, file events) that you want to view.
- Select the hostname to open the host details. Right-click a file or in the toolbar, select **Analyze Events**, and select a specific event type that you want to view.

  The following figure is an example of the Autoruns tab.



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

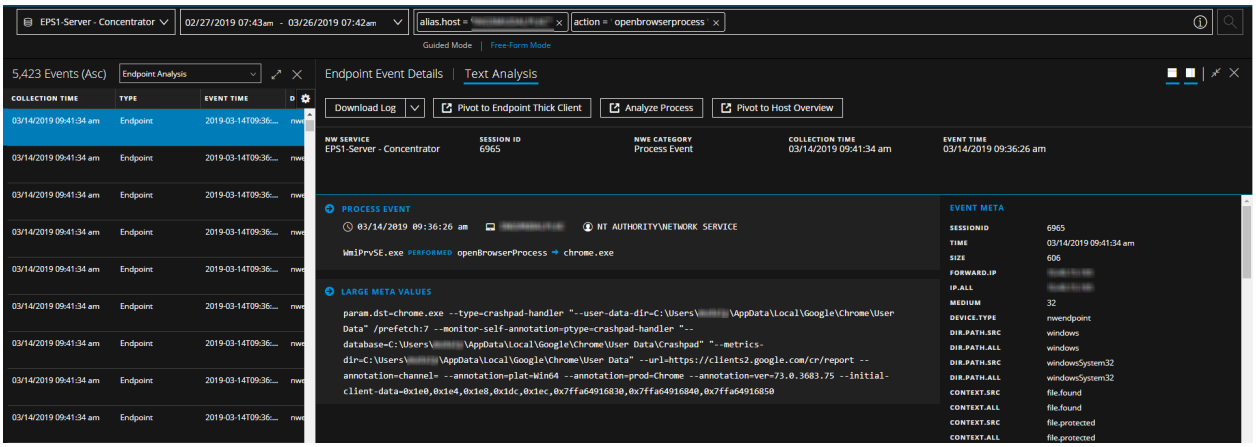
For more information on analyzing events in the Navigate and Events views, see the *NetWitness Investigate User Guide*.

Text Analysis for an Endpoint Event

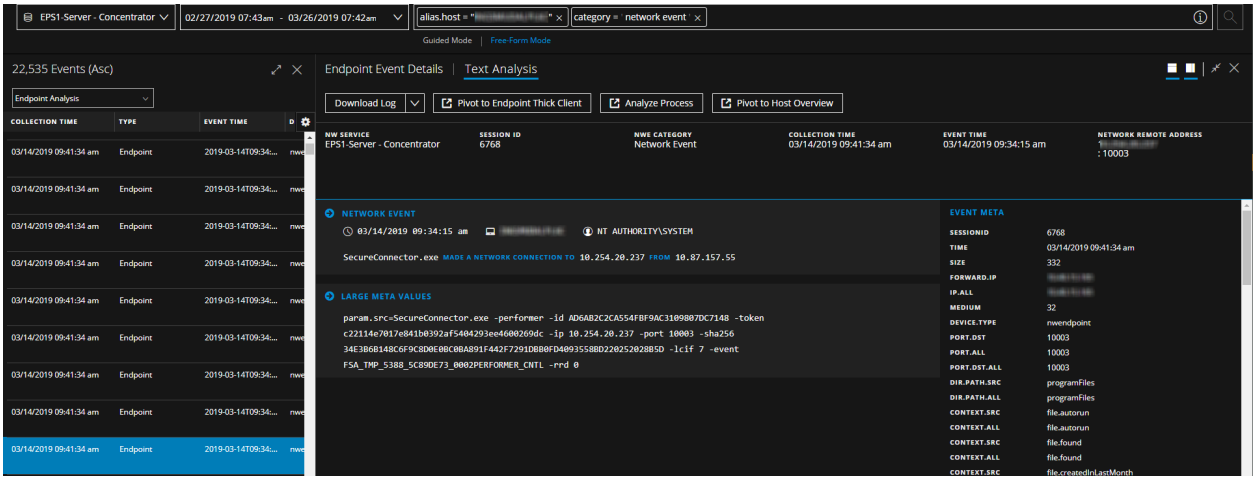
You can view all Endpoint events in their original text format in the Events view Event List panel. When you click an event in the Event list panel, the adjacent panel shows the Text Analysis. Pagination controls add flexibility when paging through the reconstructed text of an event. The Text Analysis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



Below is an example of the Network event:



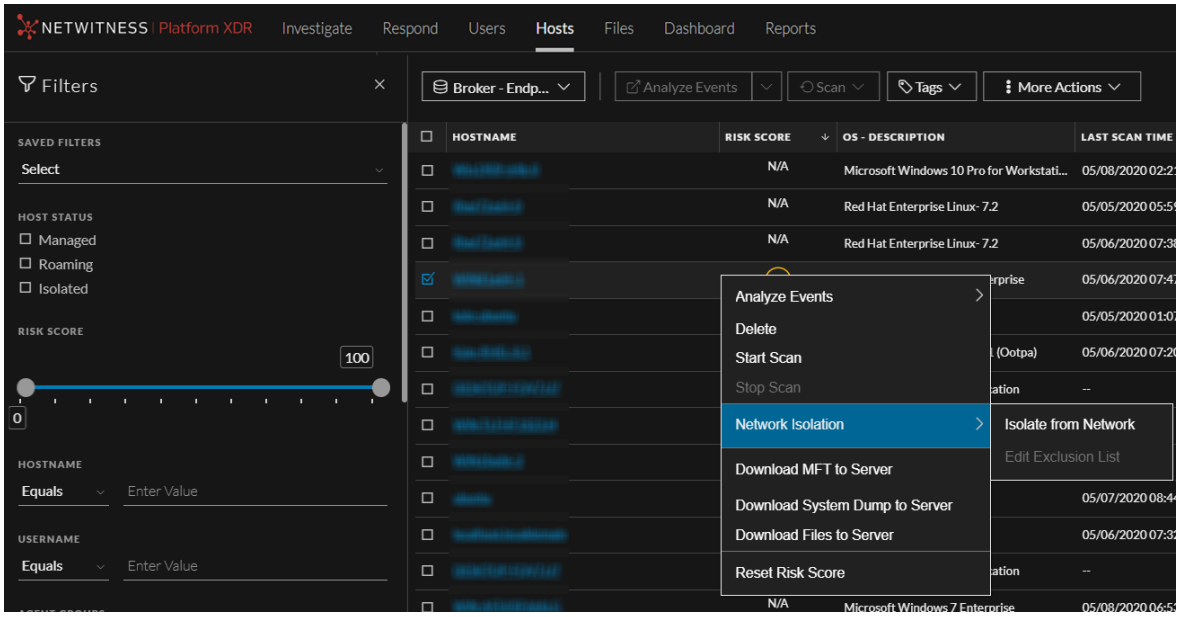
For more information on Events view, see the *NetWitness Investigate User Guide*.

Isolating Hosts from Network

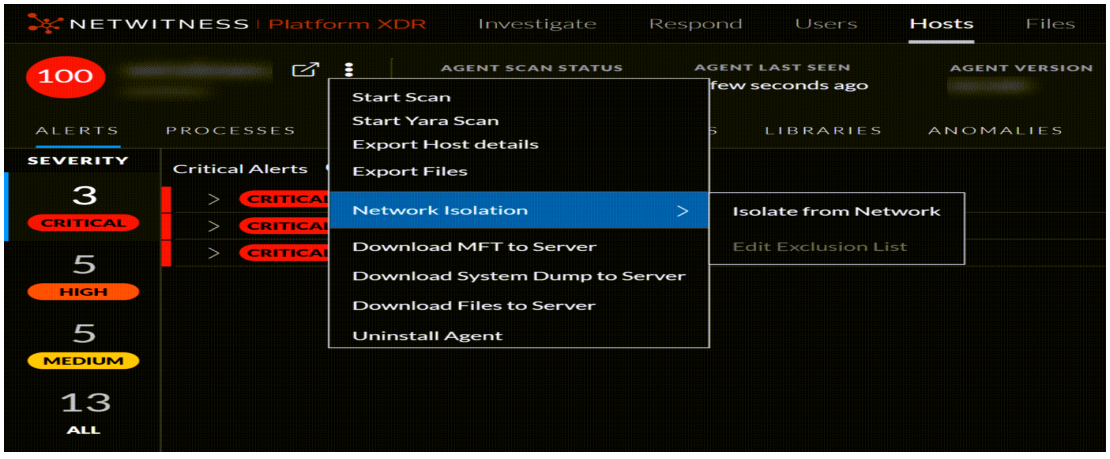
Note: By default, the network isolation option is disabled in the policy, and you cannot view options mentioned in this section. To enable network isolation, in the policy configuration, select **Enabled** in the **Network Isolation** option under Response Action Settings. For more information, see the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

To isolate a host from the network:

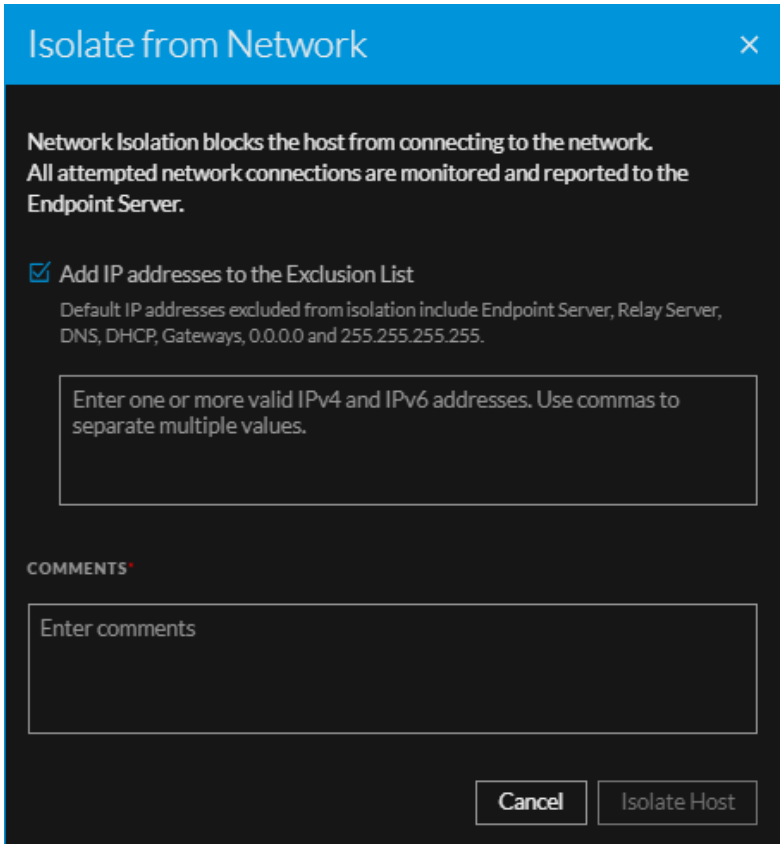
1. Go to **Hosts** and do one of the following:
   - Select a host and select **Network Isolation > Isolate from Network** from the right-click context menu, or from the **More** drop-down list in the toolbar.



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



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

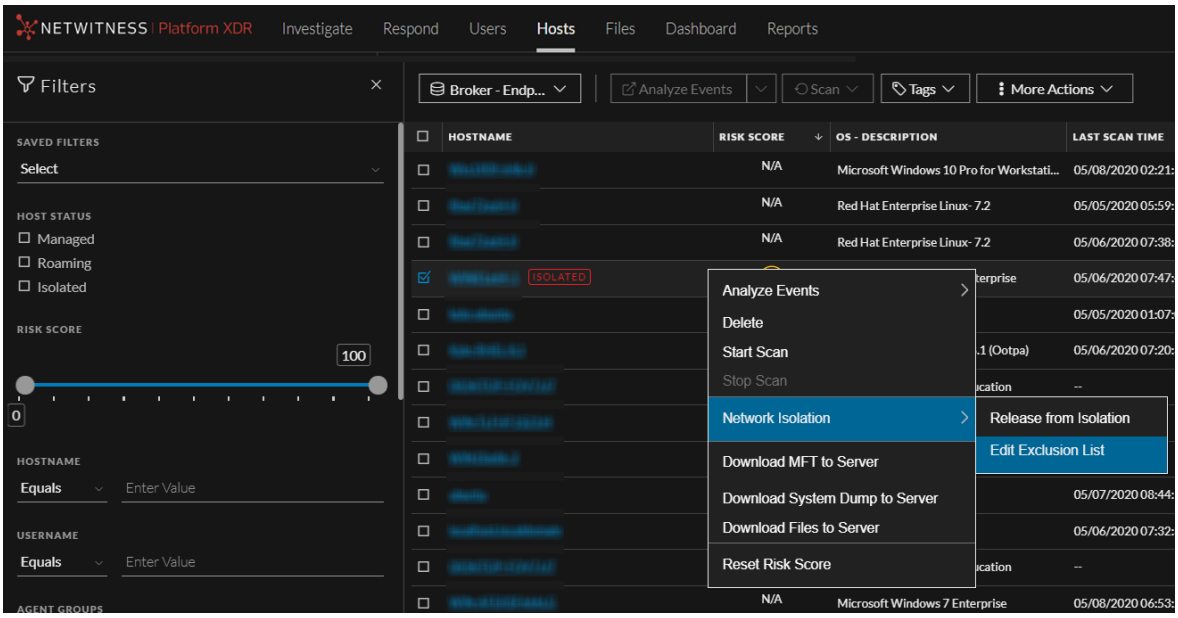


3. Enter comments.
4. Click **Isolate Host**.

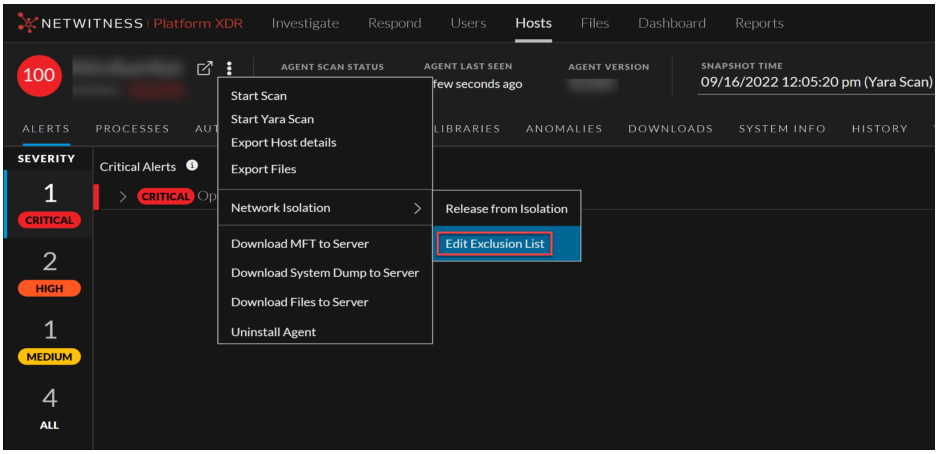
Edit Exclusion List

To edit the exclusion list:

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



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

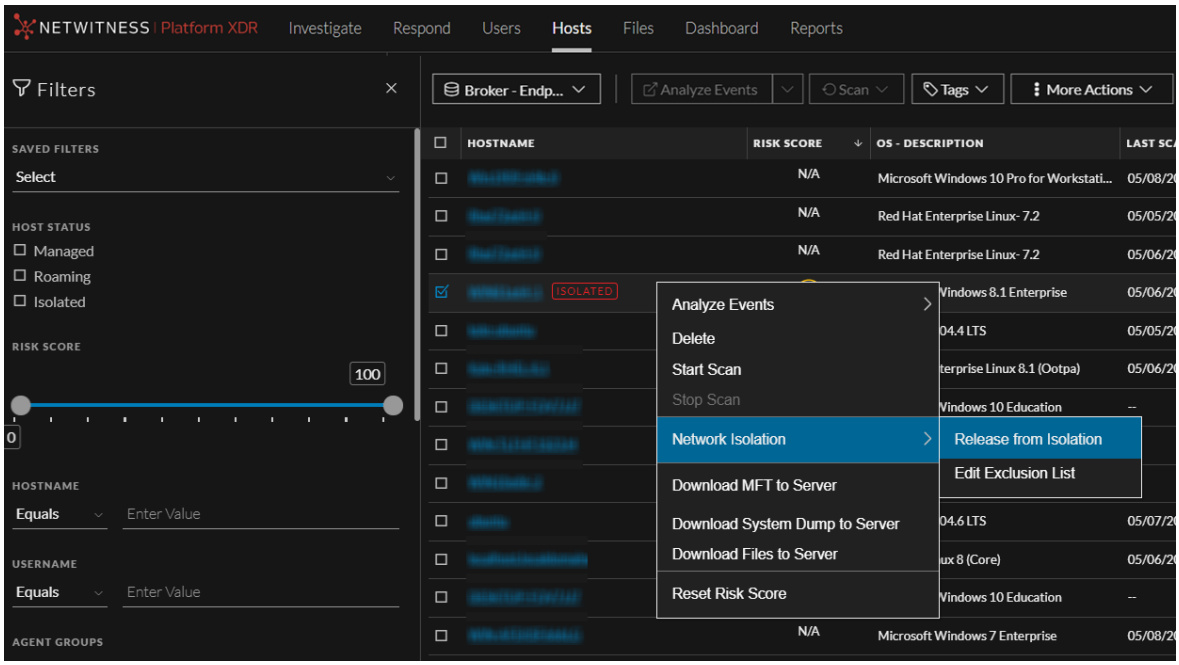


2. Add or modify the IP addresses in the list.
3. Enter comments and click **Save**.

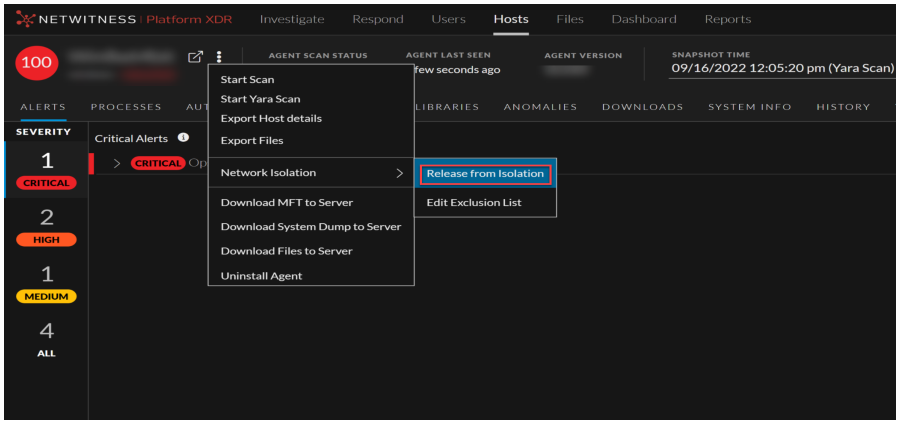
Release Isolated Hosts

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.



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



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

NetWitness Endpoint with Third-Party Antivirus Products

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

Troubleshooting NetWitness Endpoint

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

General Issues

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

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

Solution	• To verify the UDP or HTTPS connection, you must verify the connection between Windows Endpoint Agent and Endpoint Server:
	1. Go to System32 folder using the following command:
	`cd C:\Windows\System32`
	2. Execute the following command:
	`<Agent Service name>.exe /testnet`
	For example, `NWEAgent.exe /testnet`
	• If the issue is with the firewall, check the incoming and outgoing firewall rules.

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

Solution	• Firewall

	• To verify the UDP, TCP, and TLS connection, you must verify the connection between Windows Endpoint Agent and the Log Decoder:
	1. Go to System32 folder using the following command:
	`cd C:\Windows\System32`
	2. Execute the following command:
	`<Agent Service name>.exe /testlognet`
	For example, `NWEAgent.exe /testlognet`
	• If the issue is with the firewall, check the incoming and outgoing firewall rules.

Multi-server Issue

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

Hosts View Issues

Message	`An error has occurred. The Endpoint Server may be offline or inaccessible.`
Issue	When attempting to access the Hosts or Files view, the view opens with the message.
Explanation	Endpoint Server or Nginx Server is not running. Check the status of the Endpoint Server under **(Admin) > Services** or check if the Endpoint Server host IP address is registered with the Admin Server. For more information, see the *Physical Host Installation Guide* or *Virtual Host Installation Guide*. 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 **[*Host Name*] > Actions > Pivot to Investigate**

	> 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.

Issue	For MFT download: 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	Unable to analyze events from **Hosts** and **Files** view.
Explanation	Other than Broker or Concentrator, if any aggregation service, such as Archiver, is aggregating data from the Log Decoder that is configured for metadata forwarding from any Endpoint server, clicking **Analyze Events** from **Hosts** and **Files** view for this Endpoint server may not work. To resolve this issue: **Note:** To get the investigate-service-id: 1) Go to **(Admin) > Services > Concentrator** service. 2) Click > **View** > **Explore** tab. 3) Expand the **sys/stats** node list. 4) In the UUID filed, copy the value. 1. Go to **(Admin) > Services > Endpoint Server** service. 2. Click > **View** > **Explore** tab. 3. In the **endpoint/investigate** field, specify the **investigate-service-id**.

Policy Issue

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

	Permission Required - If you do not have permissions, see the "Role Permissions" topic in the *System Security and User Management Guide*.

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

Driver Issue

Issue	While loading the driver on the host, an error is encountered.
Explanation	Check the driver error code in the **Agent-Driver Error Code** column under **Hosts** view. Contact your system administrator with the error code.

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.
Solution	You must manually enable the File Reputation service. To enable the File Reputation service: 1. Go to **(Admin) > System > Live Services**. 2. In the **Additional Live Services** section, select the enable File Reputation check box. 3. Click **Apply**.

Risk Scoring for Hosts or Files Issue

Issue	NetWitness Endpoint takes a long time to process risk scoring for Hosts or Files.

Solution	Check the backlog of alerts for risk scoring. 1. SSH to the ESA Primary appliance. 2. Execute the following command: `mongo respond-server --authenticationDatabase admin -u deploy_admin -p <deploy_admin_password> --eval 'db.staging.find({"$or":[{state:"STAGED"},{state :"WORKING"}]}).count()' --quiet` The backlog count is displayed. If the backlog count is 1 million or greater, you must disable the risk scoring and Endpoint ESA alerts. 3. To disable risk scoring: a. Go to **(Admin) > Services > Respond** service. b. Click > **View** > **Explore**. c. Expand the **respond/scheduled/jobs** node list. d. In the **risk-scoring-enabled** field, set the value to **false**. 4. To disable Endpoint ESA alerts: a. To disable NetWitness Endpoint ESA alerts generation for severity; Critical, High and Medium. i. Go to **(Configure) > ESA Rules**. The Configure view is displayed with the Rules tab open. ii. In the **Options** panel, under Deployments, select the Endpoint deployment to delete. A confirmation dialog is displayed. iii. Click **Yes**. b. To disable only Medium severity NetWitness Endpoint ESA alerts: i. Go to **(Admin) > ESA Correlation** service (on which Endpoint deployment is added). ii. Click > **View** > **Explore**. iii. Expand the **correction/alert** node list. iv. In the **transient-enabled** field, set the value to **false**.

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

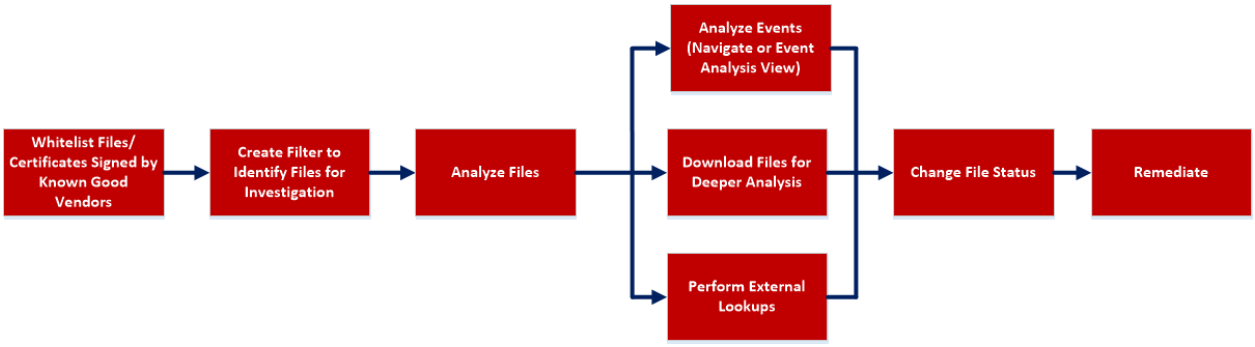
Files View

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

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

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

Workflow



What do you want to do?

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

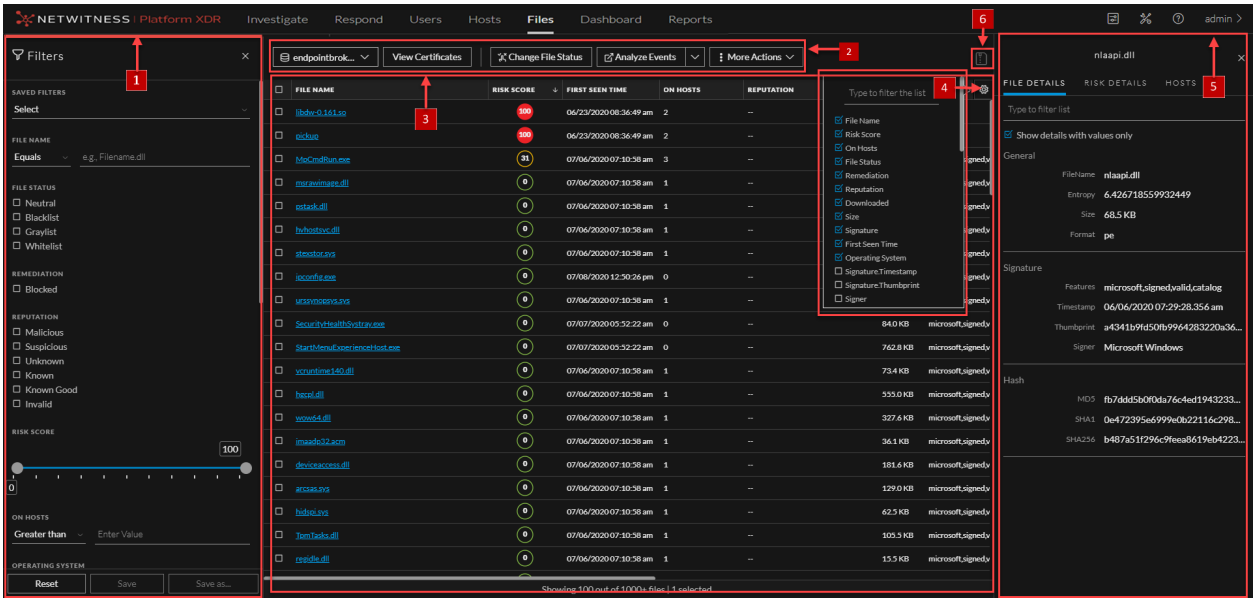
*You can perform this task in the current view

Related Topics

- Focusing on Endpoint Analysis
- Investigating Hosts
- Analyzing Downloaded Files
- Analyzing Events
- Analyze Certificates
- Changing File Status or Remediate

Quick Look

Below is an example of the Files view:

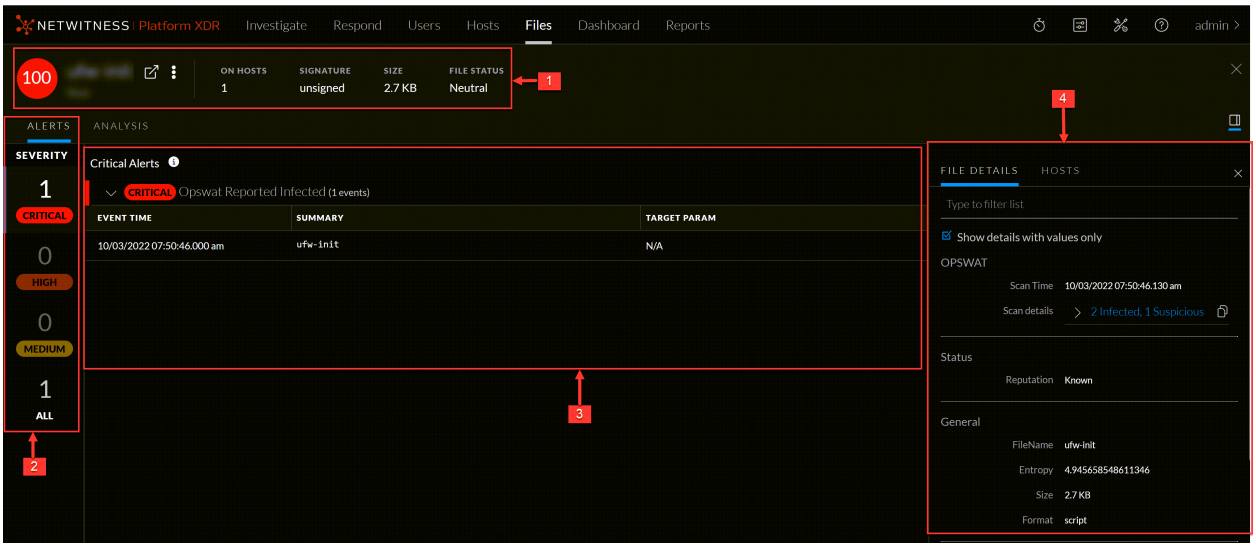


1 **Filter Files**. You can filter the files by selecting the options in the Filters panel and create filters. For more information, see Filter Files.

2	**Actions in the toolbar:** **Server drop-down list** - You can select the Endpoint server or Endpoint Broker server to view the hosts. **View Certificates** - Provides a list of code-signing certificates reported by hosts found in your deployment and their associated properties. For more information, see Analyze Certificates. **Change File Status** - Provides capabilities to manage suspect and legitimate files and block malicious or infected files to prevent future execution of the file on any host. For more information, see Changing File Status or Remediate. **Analyze Events** - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see Analyzing Events. **More 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 Analyze Hosts with File Activity.
6	**Export to CSV** - Extracts global files to a CSV file. For more information, see Export Global Files.

File Details View

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



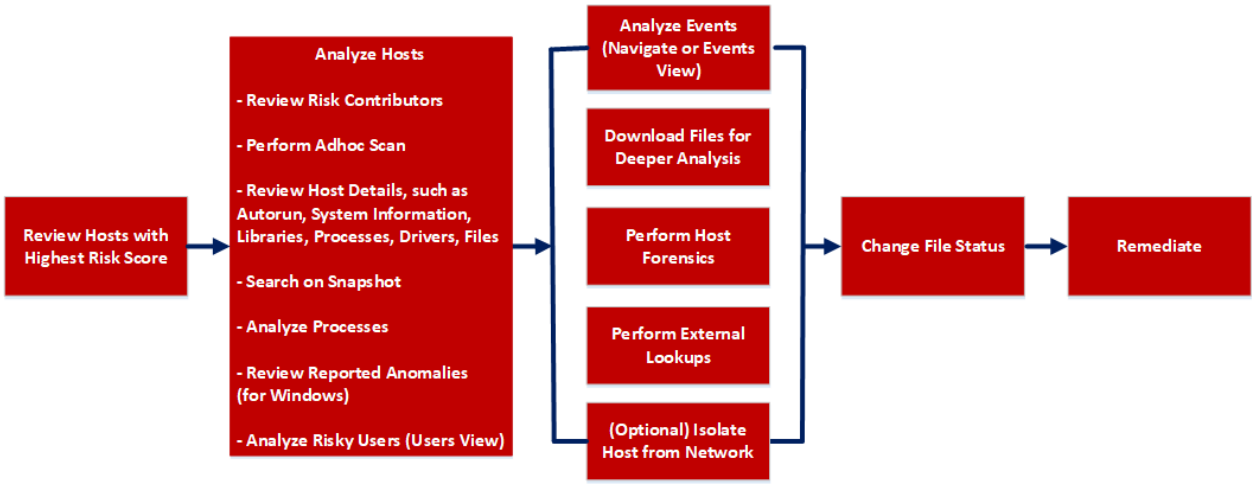
1	**Agent and Scan Details**. You can view the following agent and scan details of the selected host: **Host name** - Name of the host. For example, `WIN-ABC`. **Risk score** - Risk score of the host. **Operating System** - Operating system on which the agent is running (Linux, Windows, or Mac). **Analyze Events** - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see Analyzing Events. **More** - Provides options to perform external lookups. **On Hosts** - Indicates the number of hosts on which a file exist. **Signature** - Provides signatory information. **Size** - Size of the file. **File Status** - Status of the file. For example, `Neutral`.
2	**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 Analyzing Downloaded Files.
3	Displays events for an alert and metadata associated with a specific event.
4	**Show/Hide File Properties Panel.** Click a row to show or hide the File Properties panel. It displays the following tabs: **File Details** - Displays the file information. **Hosts** - Displays the hosts on which file activities are present. For more information, see Analyze Hosts with File Activity.

Hosts View

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

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

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details*	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
Threat Hunter	analyze processes*	Investigating a Process
Threat Hunter	review reported anomalies*	Analyze Anomalies

User Role	I want to ...	Show me how
Threat Hunter	analyze risky users*	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files*	Filter Host Details
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT*, system dump*, or process dump	Performing Host Forensics

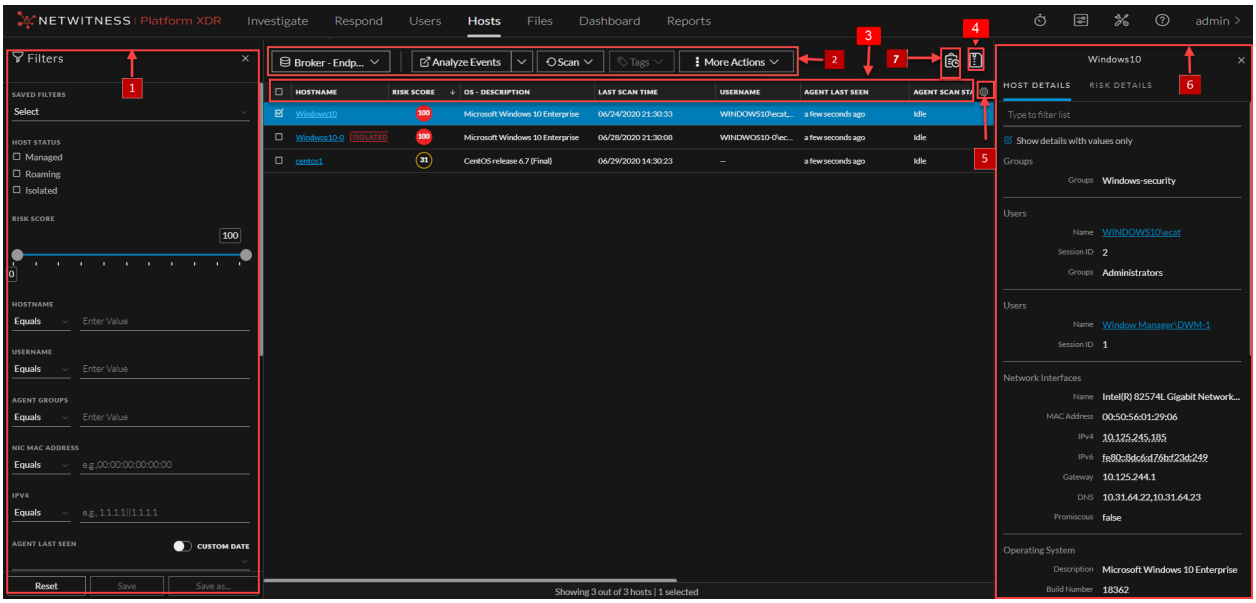
*You can perform this task in the current view.

Related Topics

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

Quick Look

Below is an example of the Hosts view:



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

2 **Actions in the toolbar:**

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

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

Start Scan - Starts a scan for the selected hosts.

Stop Scan - Stops a scan for the selected hosts.

More 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 System and Process Memory Dump.
- Isolation host from the network. For more information, see Isolating Hosts from Network.

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

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

4 **Export to CSV** - Extracts host attributes to a CSV file. For more information, see Export Host Attributes.

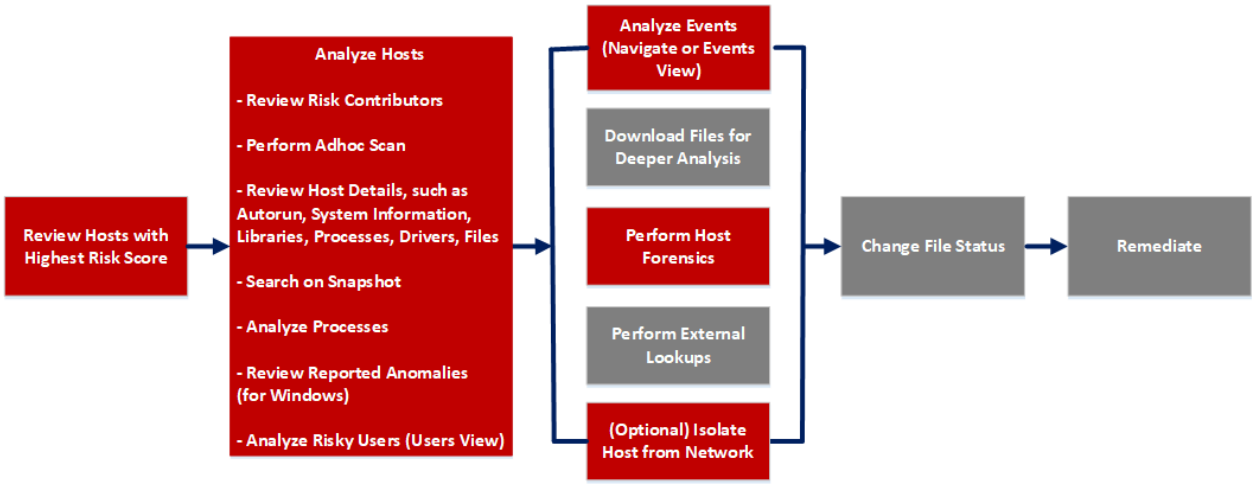
5	**Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.
6	**Show/Hide Host Properties Panel.** Click a row to show or hide the Host Properties panel. It displays the following tabs: **Host details** - Displays the host information such as Network Interfaces, operating system, hardware and others. **Risk details** - Displays the distinct alerts associated with the risk score.
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 Version 11.1 and later.

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

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details*	Analyze Host Details
Threat Hunter	search files on host*	Search Files on Host
Threat Hunter	analyze processes*	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies

User Role	I want to ...	Show me how
Threat Hunter	analyze risky users*	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis	Analyzing Downloaded Files
Threat Hunter	perform external lookups	Launch an External Lookup for a File
Threat Hunter	change file status or remediate	Changing File Status or Remediate
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT*, system dump, or process dump*	Performing Host Forensics

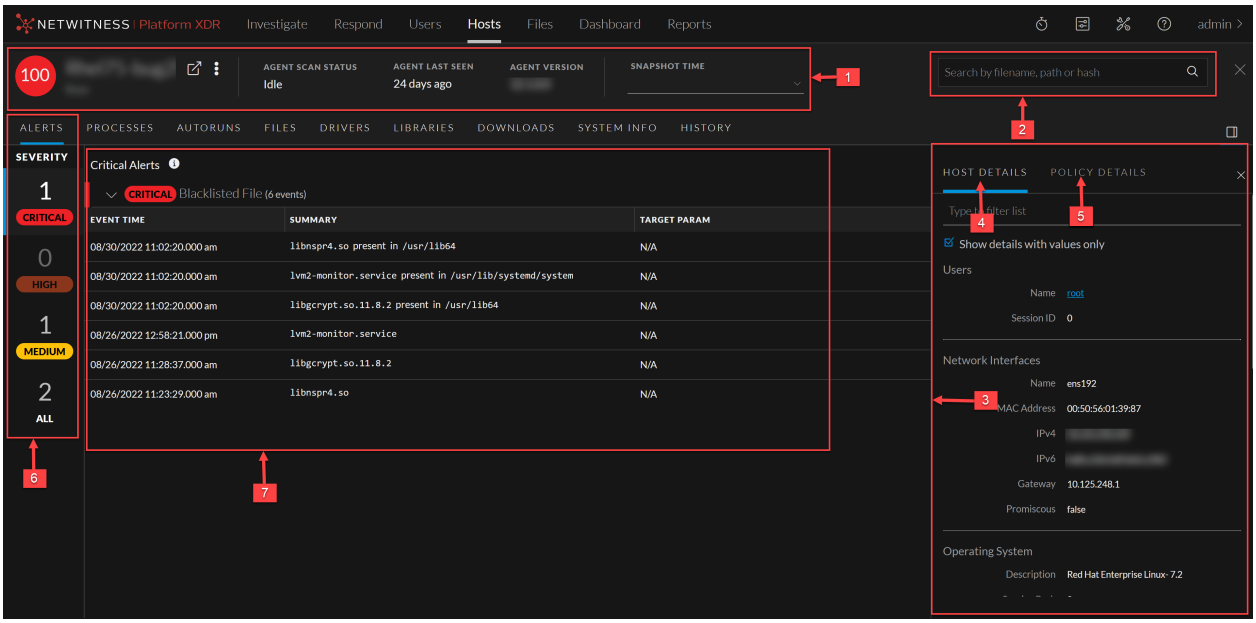
*You can perform this task in the current view.

Related Topics

- Focusing on Endpoint Analysis
- Investigating Hosts
- Analyzing Events
- Performing Host Forensics
- Isolating Hosts from Network

Quick Look

Below is an example of the Details tab:



1	**Agent and Scan Details**. You can view the following agent and scan details of the selected host: **Host name** - Name of the host. For example, `WIN-ABC`. **Risk score** - Risk score of the host. **Operating System** - Operating system on which the agent is running (Linux, Windows, or Mac). **Agent Scan Status** - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see Scan Hosts. **Agent Last Seen** - Time when the agent last communicated with the Endpoint server. **Agent Version** - Version of the agent. For example, `11.3.0.0`. **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 System and Process Memory Dump. **Snapshot Time** - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.
2	Search 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.

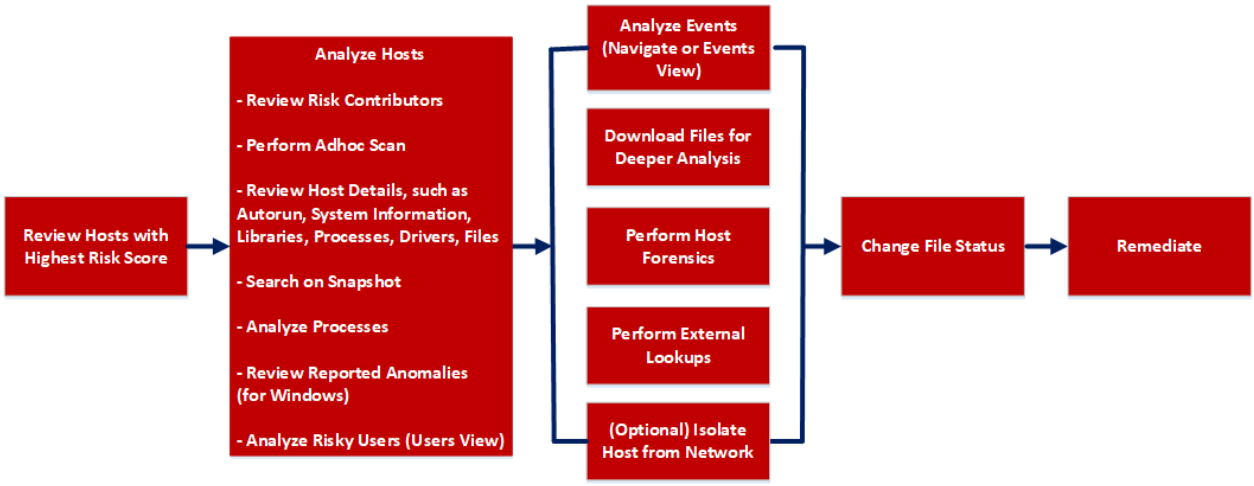
7	Displays events for an alert and metadata associated with a specific event. For more information, see Analyze Hosts Using the Risk Score.

Hosts View - Process Tab

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

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

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
Threat Hunter	analyze processes*	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies

User Role	I want to ...	Show me how
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files*	Filter Host Details
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

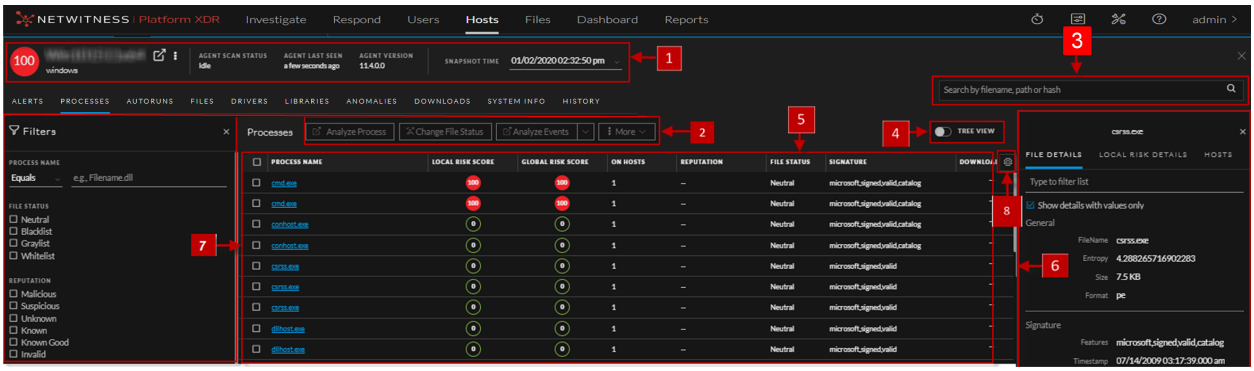
*You can perform this task in the current view.

Related Topics

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

Quick Look

Below is an example of the Process tab:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

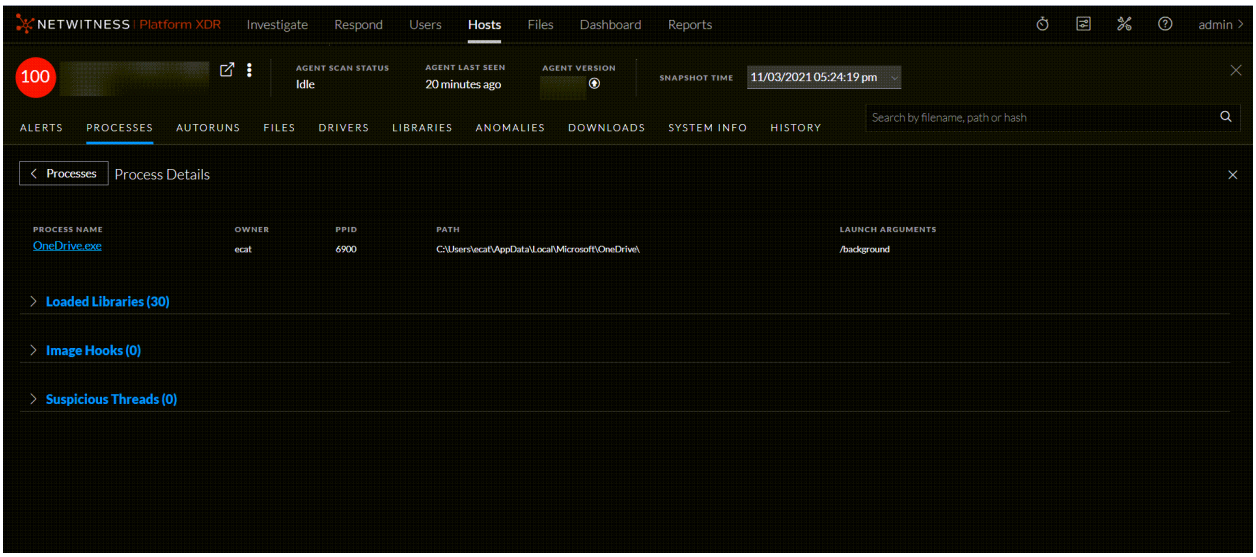
- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host Attributes.
- Isolation host from the network. For more information, see Isolating Hosts from Network.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

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

2	**Actions in the toolbar:** **Analyze Process** - Lets you perform process analysis to investigate a particular process behavior, and understand the entire process event chain, process parent-child relationships, and all associated events. For more information, see Investigating a Process. **Change File Status** - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see Changing File Status or Remediate. **Analyze Events** - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see Analyzing Events. **More** - Provides options to: • Perform external lookups. • Download files to server, save a local copy, and analyze files for deeper analysis. • Download process dump to server. **Note:** You can perform some of the above actions from the right-click context menu.
3	**Search on Snapshots**. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see Search Files on Host.
4	**Toggle.** Lets you toggle between List view and Tree view.
5	**Process panel** - Displays process information, such as process name, local risk score, global risk score, On Hosts, reputation status, file status, and others.
6	**Show/Hide Right Panel** - Displays the following properties of a process in the right panel: • **File Details** - Displays all properties of the selected process. It is grouped as follows: **General** - General information about the file, such as file name, entropy, size, and format. **Signature** - Provides signatory information. **Hash** - Hash type of the file (MD5, SHA1, and SHA256). **Time** - Time when the file was created, modified, or accessed. **Location** - Location of the file. **Process** - Details of the process, such as image size and PID. **Image** - Image details loaded by the process. • **Local Risk Details** - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All. • **Hosts** - Displays the top 100 hosts based on the risk score on which the file is present.
7	**Filter Files**. You can filter processes by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details.
8	**Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.

Process Details

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



Field	Description
Process Name	Name of the process. For example, `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`.

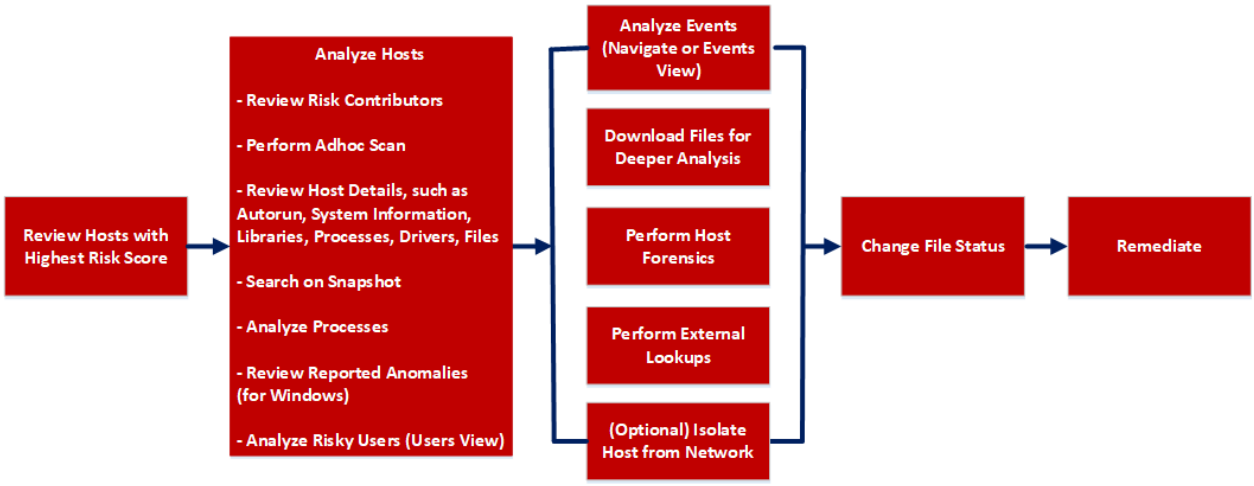
- List of loaded libraries for the selected process, such as DLLs (for Windows), Dylibs (for Mac), or .SO (for Linux).
- List of autoruns (if configured).
- List of image hooks and suspicious threads (for Windows).

Hosts View - Autoruns Tab

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

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

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies

User Role	I want to ...	Show me how
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files	Filter Host Details
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

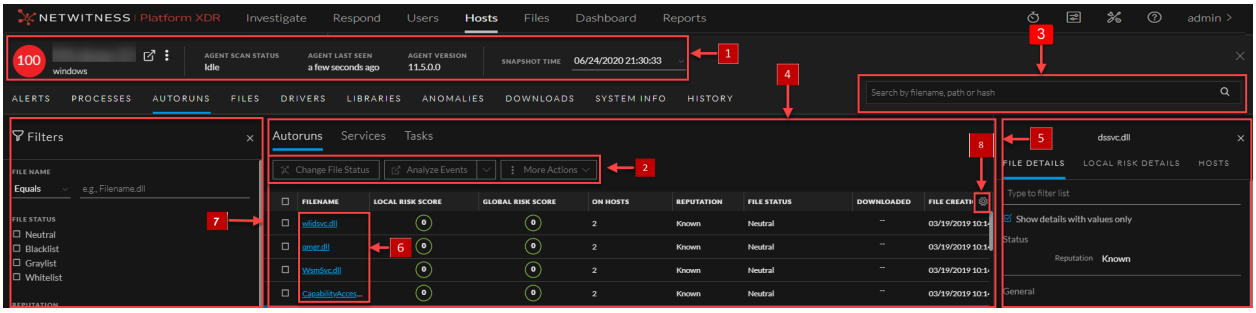
*You can perform this task in the current view.

Related Topics

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

Quick Look

Below is an example of the Autoruns tab:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 System and Process Memory Dump.

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

2 **Actions in the toolbar:**

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

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

More 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.

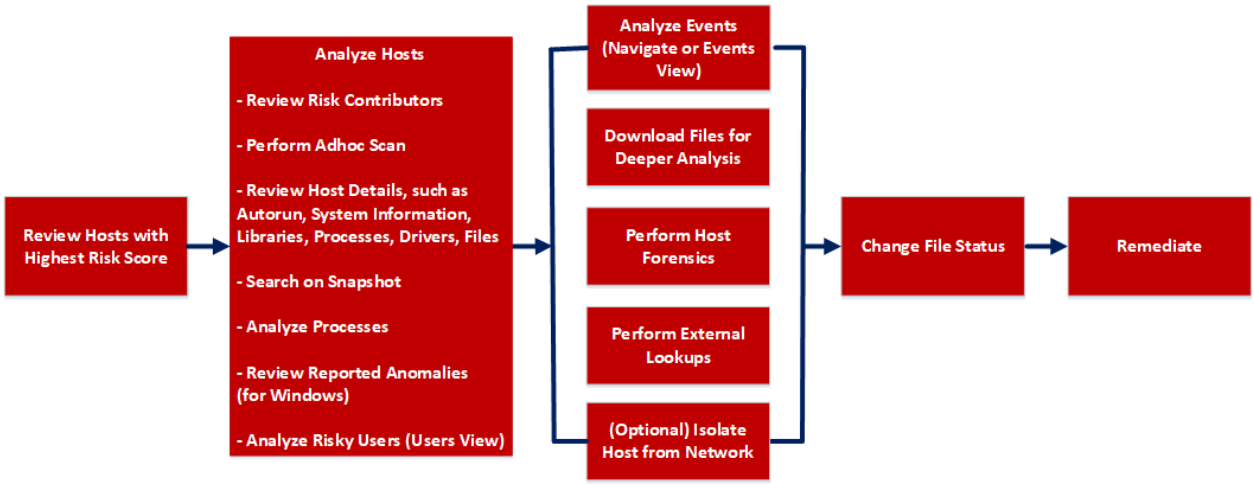
4	**Details Panel** - Displays the following tabs: • **Autoruns** - Files that are executed at start-up. • **Services** - Files that are running as a service for the selected host. • **Tasks/Cron jobs** - Files that are configured to run as scheduled tasks along with the trigger.
5	**Show/Hide Right Panel** - Displays the following properties in the right panel: • **File Details** - Displays all properties of the selected process. It is grouped as follows: **General** - General information about the file, such as file name, entropy, size, and format. **Signature** - Provides signatory information. **Hash** - Hash type of the file (MD5, SHA1, and SHA256). **Time** - Time when the file was created, modified, or accessed. **Location** - Location of the file. **Autoruns/Services/Tasks** - Details related to autrouns, services, or tasks. • **Local Risk Details** - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All. • **Hosts** -Displays the top 100 hosts based on the risk score on which the file is present.
6	Clicking a filename lets you navigate to the Files view for further analysis.
7	**Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details.
8	**Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.

Hosts View - Files Tab

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

The Files tab displays all files on the host including the files deleted within last 30 days. To access this tab, select a host from the **Hosts** view and click the **Files** tab. By default, it displays 100 files. To display more files, click **Load More** at the bottom of the page.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	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 File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files*	Filter Host Details
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT*, system dump, or process dump*	Performing Host Forensics

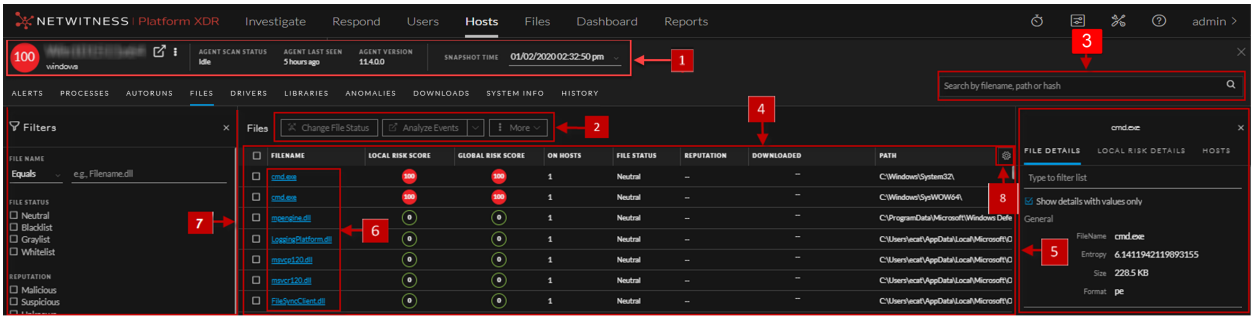
*You can perform this task in the current view.

Related Topics

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

Quick Look

Below is an example of the Files tab:



1	**Agent and Scan Details**. You can view the following agent and scan details of the selected host: **Host name** - Name of the host. For example, `WIN-ABC`. **Risk score** - Risk score of the host. **Operating System** - Operating system on which the agent is running (Linux, Windows, or Mac). **Agent Scan Status** - Current status of the scan - Idle, Scanning, Starting Scan, or Stopping Scan. For more information, see Scan Hosts. **Agent Last Seen** - Time when the agent last communicated with the Endpoint server. **Agent Version** - Version of the agent. For example, `11.3.0.0`. **More** - Provides options to: • Start a scan for the selected hosts. For more information, see Scan Hosts. • Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 System and Process Memory Dump. **Snapshot Time** - Lists scanned time stamps. To view the scan history, you can select the snapshot time from the drop-down menu.
2	**Actions in the toolbar:** **Change File Status** - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see Changing File Status or Remediate. **Analyze Events** - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see Analyzing Events. **More Actions** - Provides options to: • Perform external lookups. • Download files to server, save a local copy, and analyze files for deeper analysis. **Note:** You can perform some of the above actions from the right-click context menu.
3	Search files on host. Lets you search the files on the host (file name, file path, and SHA-256 checksum). For more information, see Search Files on Host.
4	**All Files Available on Host** - Lists all files (reported as part of scan and tracking) on the host. By default, **All Files Available on Host** toggle is enabled for Windows and Mac.
5	**Details Panel** - Displays information, such as filename, local risk score, global risk score, on hosts, reputation status, file status, package details and others.

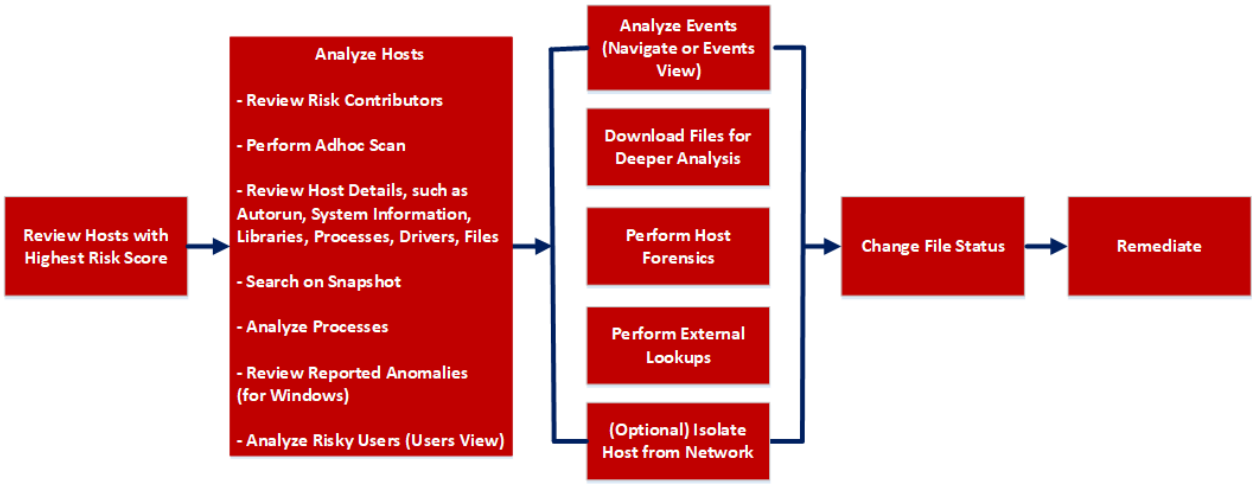
6	**Show/Hide Right Panel** - Displays the following properties in the right panel: • File Details - Displays all properties of the selected process. It is grouped as follows: **General** - General information about the file, such as file name, entropy, size, and format. **Signature** - Provides signatory information. **Hash** - Hash type of the file (MD5, SHA1, and SHA256). **Time** - Time when the file was created, modified, or accessed. **Location** - Location of the file. • Local Risk Details - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All. • Hosts - Displays the top 100 hosts based on the risk score on which the file is present.
7	Clicking a filename lets you navigate to the Files view for further analysis.
8	**Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. **Note:** In the **Deleted** column, a trash icon appears next to the deleted file. The **Deleted** column is not displayed if you disable **All Files Available On Host**. For more information, see Filter Host Details.
9	**Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.

Hosts View - Drivers Tab

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

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

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies

User Role	I want to ...	Show me how
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files*	Filter Host Details
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT*, system dump, or process dump*	Performing Host Forensics

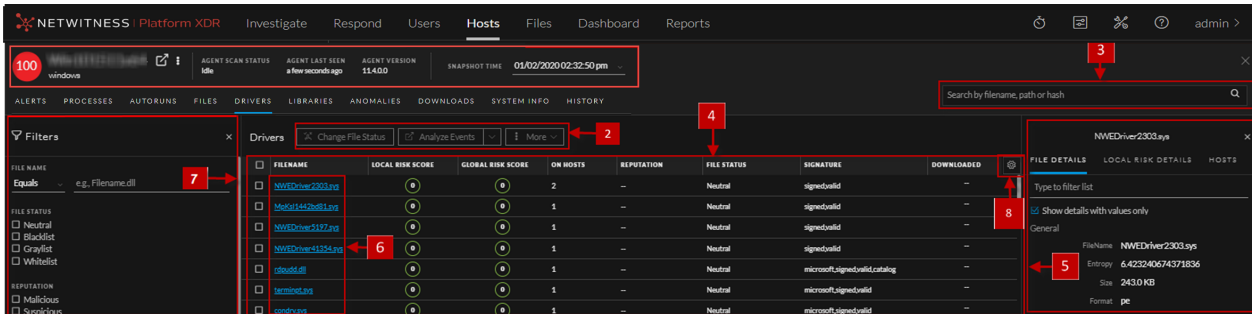
*You can perform this task in the current view.

Related Topics

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

Quick Look

Below is an example of the Drivers tab:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 System and Process Memory Dump.

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

2 **Actions in the toolbar:**

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

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

More - Provides options to:

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

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

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

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

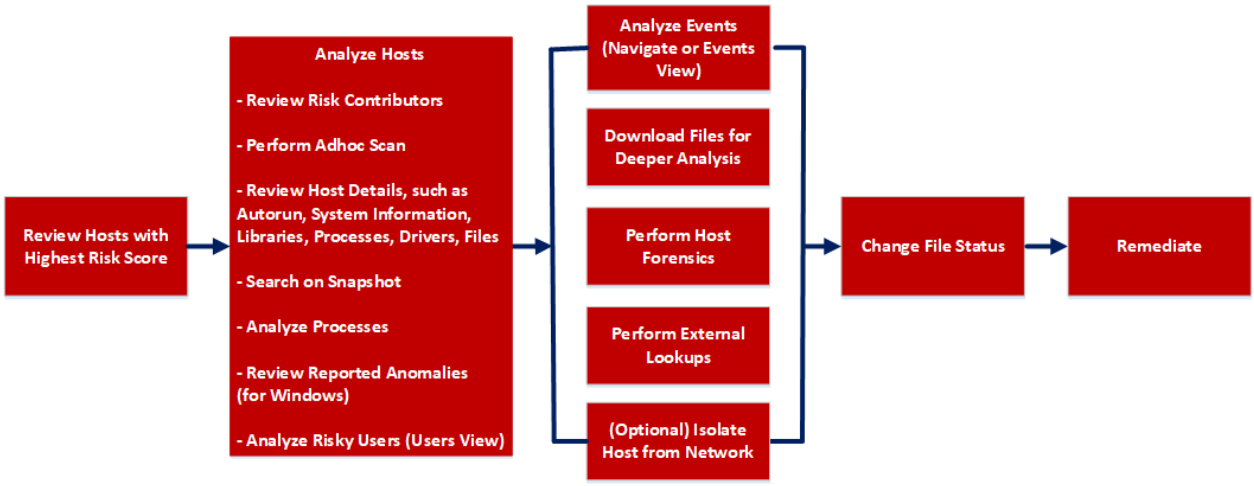
5	**Show/Hide Right Panel** - Displays the following properties in the right panel: • **File Details** - Displays all properties of the selected process. It is grouped as follows: **General** - General information about the file, such as file name, entropy, size, and format. **Signature** - Provides signatory information. **Hash** - Hash type of the file (MD5, SHA1, and SHA256). **Time** - Time when the file was created, modified, or accessed. **Location** - Location of the file. **Image** - Loaded image. • **Local Risk Details** - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All. • **Hosts** - Displays the top 100 hosts based on the risk score on which the file is present.
6	Clicking a filename lets you navigate to the Files view for further analysis.
7	**Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details.
8	**Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.

Hosts View - Libraries Tab

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

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

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score*	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies

User Role	I want to ...	Show me how
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events*	Analyzing Events
Threat Hunter	download files for deeper analysis*	Analyzing Downloaded Files
Threat Hunter	perform external lookups*	Launch an External Lookup for a File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files*	Filter Host Details
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

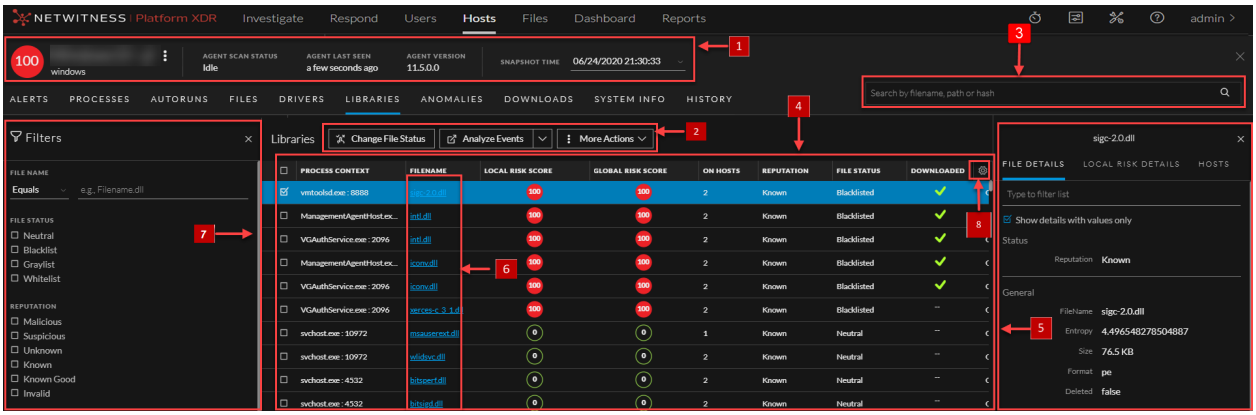
*You can perform this task in the current view.

Related Topics

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

Quick Look

Below is an example of the Libraries tab:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 System and Process Memory Dump.

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

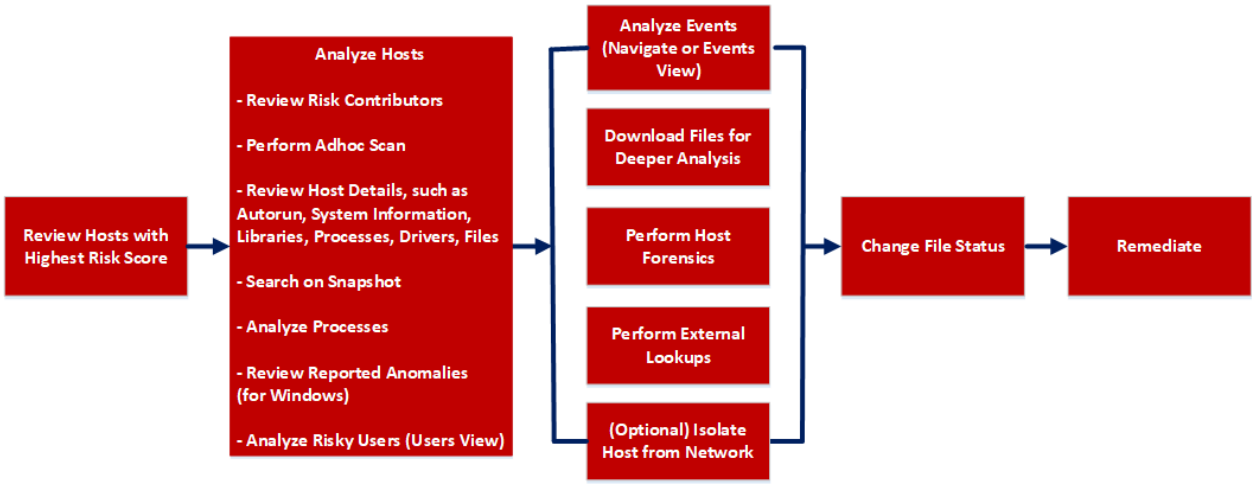
2	**Actions in the toolbar:** **Change File Status** - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see Changing File Status or Remediate. **Analyze Events** - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see Analyzing Events. **More Actions** - Provides options to: • Perform external lookups. • Download process dump to server. • Download files to server, save a local copy, and analyze files for deeper analysis. **Note:** You can perform some of the above actions from the right-click context menu.
3	**Search on Snapshots**. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see Search Files on Host.
4	**Details Panel** - Displays information, such as process context, filename, local risk score, global risk score, on hosts, reputation status, file status, and others.
5	**Show/Hide Right Panel** - Displays the following properties in the right panel: • **File Details** - Displays all properties of the selected process. It is grouped as follows: **General** - General information about the file, such as file name, entropy, size, and format. **Signature** - Provides signatory information. **Hash** - Hash type of the file (MD5, SHA1, and SHA256). **Time** - Time when the file was created, modified, or accessed. **Location** - Location of the file. **Process** - Details of the process, such as image size and PID. • **Local Risk Details** - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All. • **Hosts** - Displays the top 100 hosts based on the risk score on which the file is present.
6	Clicking a filename lets you navigate to the Files view for further analysis.
7	**Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details.
8	**Settings Menu.** You can set Hosts view preferences by selecting columns from the Settings menu. For more information, see Set Hosts Preference.

Hosts View - Anomalies Tab

Note: The information in this topic applies to 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 File
Threat Hunter	change file status or remediate*	Changing File Status or Remediate
Threat Hunter	filter files	Filter Host Details
Threat Hunter	isolate host from network*	Isolating Hosts from Network
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

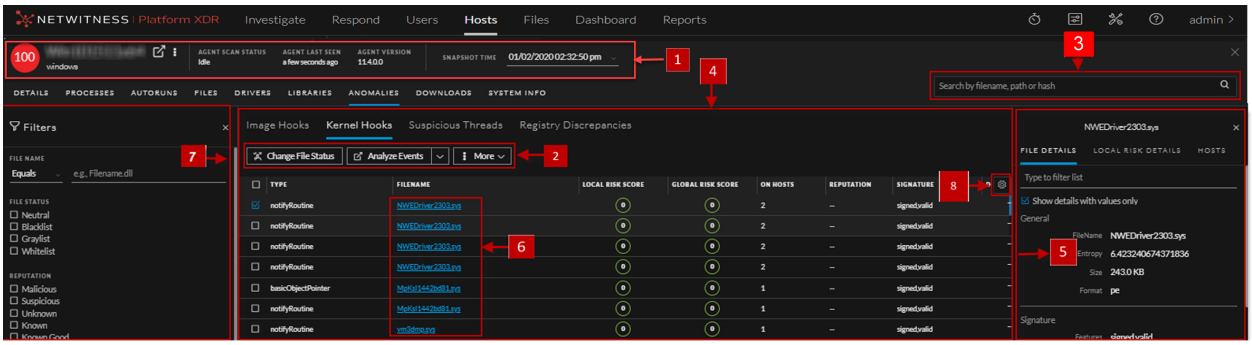
*You can perform this task in the current view.

Related Topics

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

Quick Look

Below is an example of the Anomalies tab:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 System and Process Memory Dump.

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

2	**Actions in the toolbar:** **Change File Status** - Provides capabilities to manage suspect and legitimate files and block malicious or infected file to prevent future execution of the file on any host. For more information, see Changing File Status or Remediate. **Analyze Events** - Lets you investigate a particular host, IP address, username, filename, or hash to get the entire context of the activity. For more information, see Analyzing Events. **More** - Provides options to: • Perform external lookups. • Download process dump to server. • Download files to server, save a local copy, and analyze files for deeper analysis. **Note:** You can perform some of the above actions from the right-click context menu.
3	**Search on Snapshots**. Lets you search on all snapshots (file name, file path, and SHA-256 checksum). For more information, see Search Files on Host.
4	**Details Panel** - Displays the following tabs: • Image Hooks • Kernel Hooks • Suspicious Threads • Registry Discrepancies
5	**Show/Hide Right Panel** - Displays the following properties in the right panel: • **File Details** - Displays all properties of the selected process. It is grouped as follows: **General** - General information about the file, such as file name, entropy, size, and format. **Signature** - Provides signatory information. **Hash** - Hash type of the file (MD5, SHA1, and SHA256). **Time** - Time when the file was created, modified, or accessed. **Location** - Location of the file. **Image Hooks/Kernel Hooks/Suspicious Threads/Registry Discrepancies** - Details related to image hooks, kernel hooks, suspicious threads, or registry discrepancies. • **Local Risk Details** - Displays the alerts associated with the local risk score, such as Critical, High, Medium and All. • **Hosts** - Displays the top 100 hosts based on the risk score on which the file is present.
6	Clicking a filename lets you navigate to the Files view for further analysis.
7	**Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter Host Details.

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

Image Hooks

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

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

Kernel Hooks

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

Category	Description
Type	Type of kernel object which was modified. Possible values are: objectInitializer,basicObjectPointer, majorFunction, invalidObject, fastIO, notifyRoutine, attachedDevice, device, miniPort, sdt, sysEnter, or type.idt.
Driver name	Name of the driver which placed the hooks.
Local Risk Score	Risk score of suspicious or malicious activities performed by the file on a specific host.
Global Risk Score	Aggregated score of all suspicious and malicious activities performed by the file across all hosts.

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.

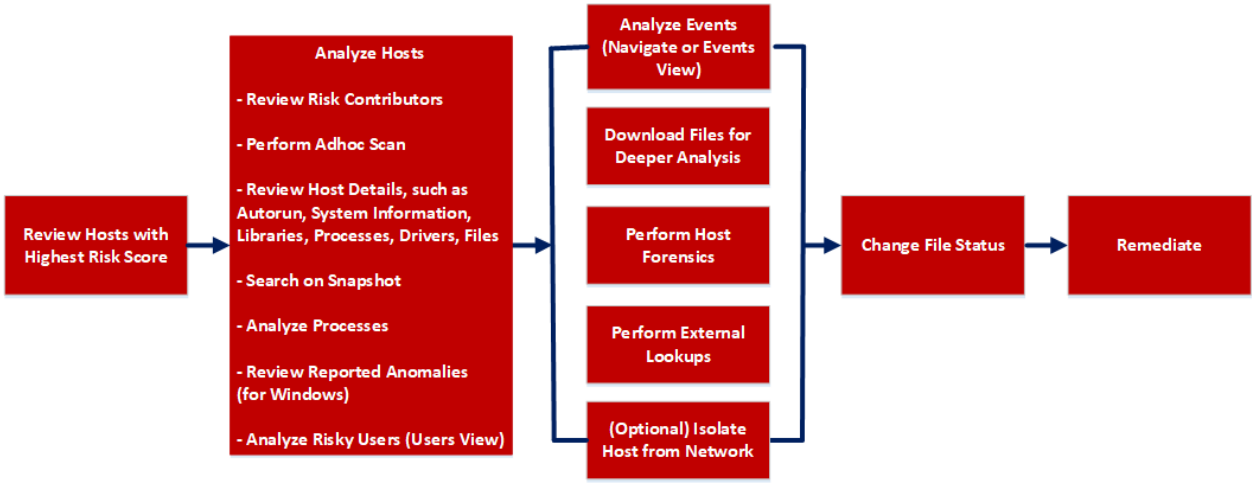
Category	Description
Hive	Name of the registry hive when possible, otherwise it displays the hive ID. Possible values are: `hkeyClassesRoot`, `hkeyCurrentUser`, `hkeyLocalMachine`, `hkeyUsers`, or `hkeyPerformanceData`.
Reason	Type of registry discrepancy. Possible values are: notFound, embeddedNull, 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.

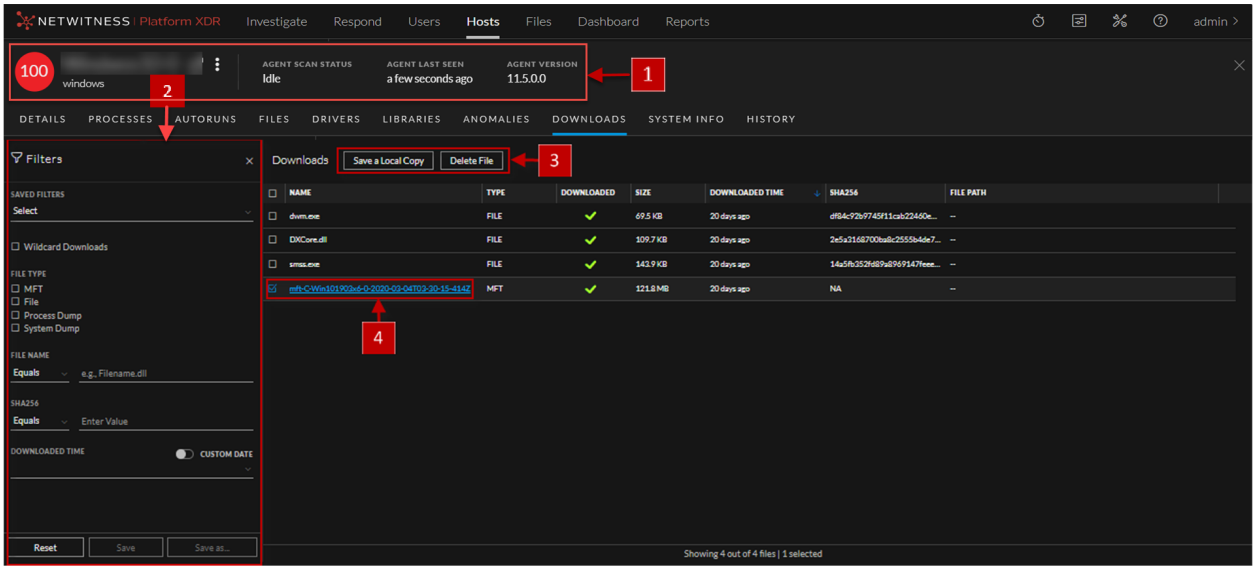
Related Topics

- Focusing on Endpoint Analysis
- Investigating Hosts

- Performing Host Forensics
- Isolating Hosts from Network

Quick Look

Below is an example of the Downloads tab:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 Download Files Using Full Path or Wildcard.
- Download System Dump to the server. For more information, see System and Process Memory Dump.

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

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

Delete File - Deletes the downloaded MFT from the server.

For more information, see Performing Host Forensics.

4 **View MFT Details**. Click the filename to view the MFT details. For more information, see MFT Viewer.

The table displays the following information:

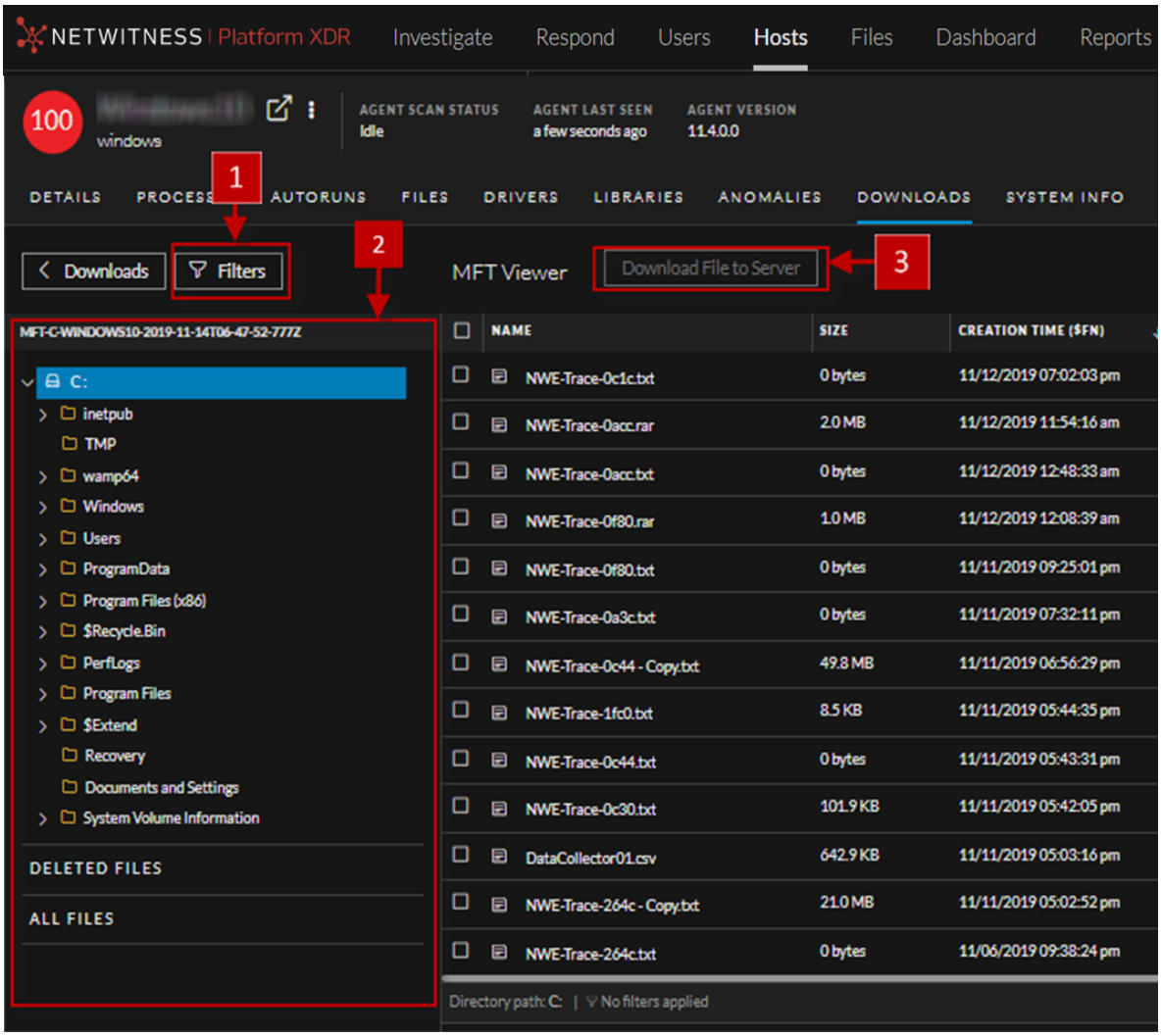
Column	Description
File Name	Name of the file that is downloaded. For example, `VGAuthService.exe`.
Type	Type of file downloaded - MFT, file, memory dump.

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 Analyze Downloaded MFT.

Below is an example of the MFT Viewer:



1. **Filter Files**. You can filter files by selecting the options in the Filters panel and create filters. For more information, see Filter MFT.
2. **Folder Details**. Lets you view the content of the MFT.
3. **Download File to Server**. Downloads files to the server.

The table displays the following information:

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

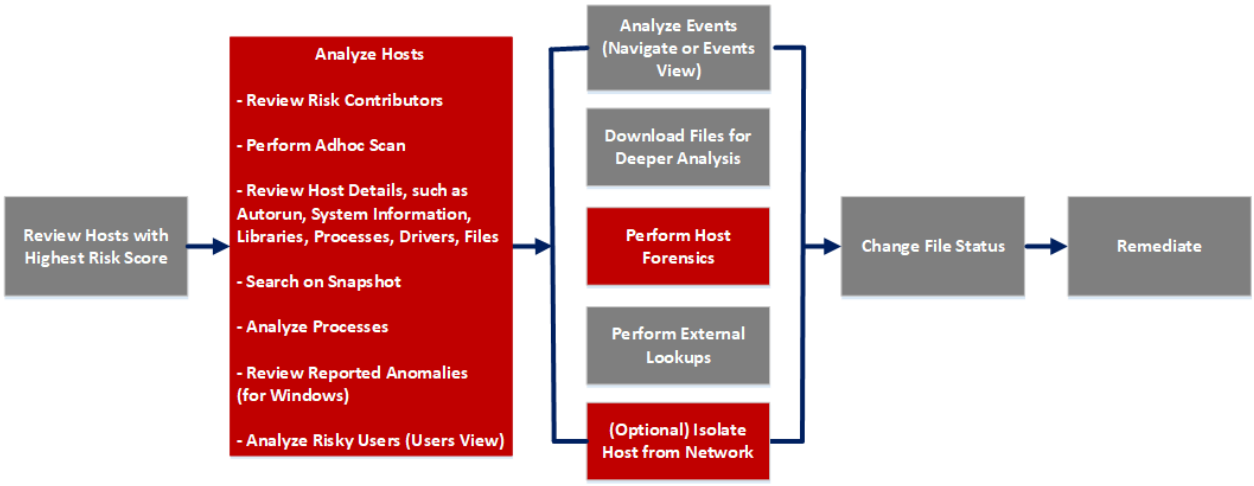
Column	Description
Modification time ($FN)	$FN modified time.
Modification time ($SI)	$SI modified time.
Access time ($FN)	$FN access time.
Access time ($SI)	$SI access time.
Update time ($FN)	$FN updated time.
Update time ($SI)	$SI updated time.
Full Path	Path of the file.
Allocated Size	File size on 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 Version 11.1 and later.

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

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Threat Hunter	review hosts with highest risk score	Analyze Hosts Using the Risk Score
Threat Hunter	analyze hosts*	Investigating Hosts
Threat Hunter	perform adhoc scan*	Scan Hosts
Threat Hunter	review host details	Analyze Host Details
Threat Hunter	search on snapshot*	Search Files on Host
Threat Hunter	analyze processes	Investigating a Process
Threat Hunter	review reported anomalies	Analyze Anomalies
Threat Hunter	analyze risky users	Analyzing Risky Users
Threat Hunter	analyze events	Analyzing Events
Threat Hunter	download files for deeper analysis	Analyzing Downloaded Files

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

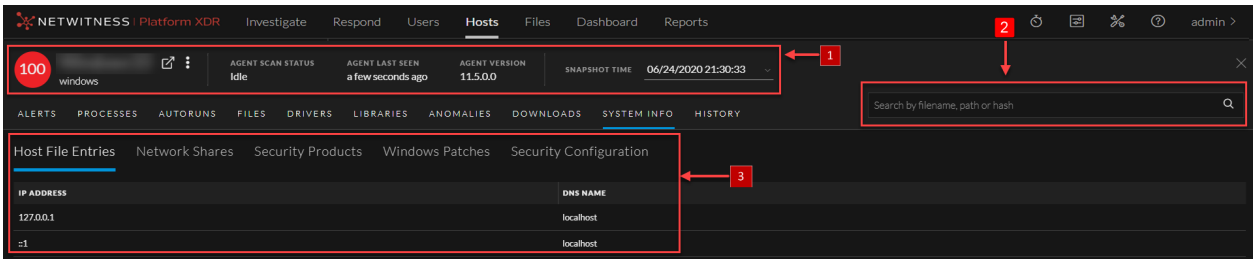
*You can perform this task in the current view.

Related Topics

- Focusing on Endpoint Analysis
- Investigating Hosts

Quick Look

Below is an example of the System Information tab:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 System and Process Memory Dump.

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

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

3 **System Information Panel** - See System Information Panel.

System Information Panel

The System Information panel displays the following tabs:

Tabs	Description
Host File Entries	All network redirections written in the host file. For example, IP Address - `10.10.10.3` and DNS Name - `localhost,localhost.localdomain,localhost4,localhost4.localdomain4`
Network Shares	Network name of the shared resource (for Windows only). For example, Name - `Admin$`, Description - `Remote Admin`, Path - `C:\`, Permissions - `None`, Type - `disk, special`, Max Users - `4294967295`, Current Users - `0`.
Security Products	Installed security products (for Windows only). For example, Display Name - `Windows Defender`, Instance - `D68DDC3A-831F-4FAE-9E44-DA132C1ACF46`, Features - `Enabled`, Type - `antiVirus`.

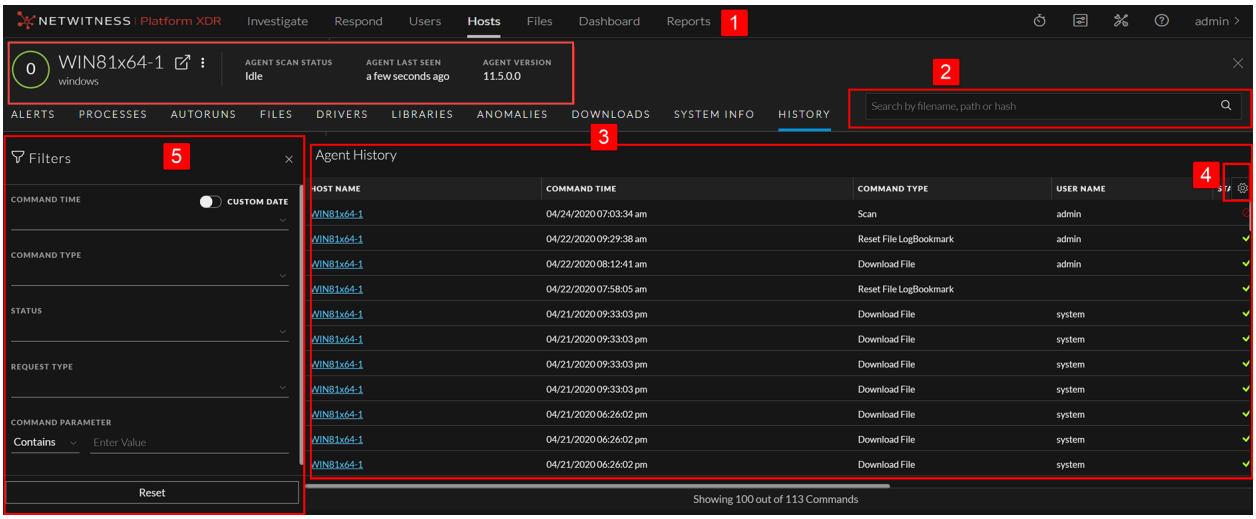
Tabs	Description
Windows Patches	List of patches applied by Windows update (for Windows only). For example, `KB2959936`.
Security Configuration	Security configuration details on the host. For example, firewall disabled or enabled, smart screen filter disabled or enabled. This field is only applicable for Windows and Mac.

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:



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

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

Risk score - Risk score of the host.

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

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

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

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

More - Provides options to:

- Start a scan for the selected hosts. For more information, see Scan Hosts.
- Extracts host attributes and endpoint data to a JSON file of the selected snapshot. For more information, see Export Host 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 System and Process Memory Dump.

2 **Search files on host**. Lets you search the files on the host (file name, file path, and SHA-256 checksum).

3 **Details Panel**- Displays information, such as:

- **Command Time** - Command issued time.
- **Command Type** - Type of the command (Identity, scan, stop scan, download file, MFT, process dump, system dump, start isolation, update isolation exclusion list, stop isolation, reset file logbookmark, and download multiple files, 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.

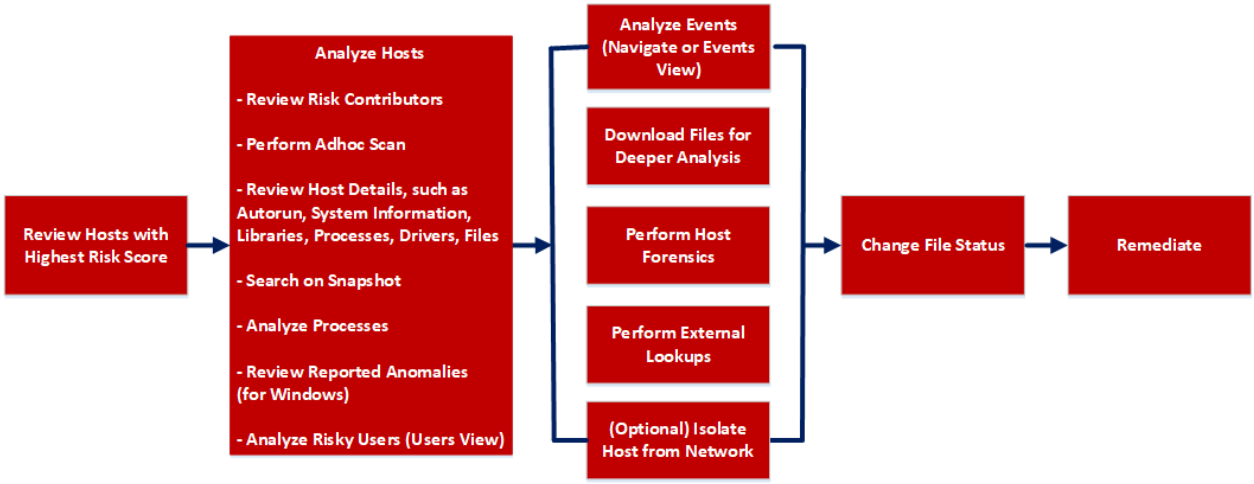
5 **Settings Menu.** You can set History view preferences by selecting columns from the Settings menu.

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

User Role	I want to ...	Show me how
Threat Hunter	download MFT, system dump, or process dump*	Performing Host Forensics

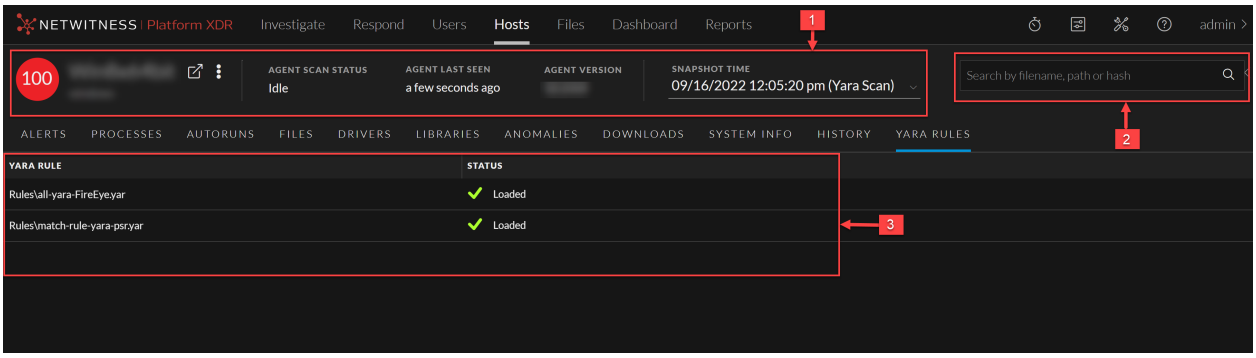
*You can perform this task in the current view.

Related Topics

- Focusing on Endpoint Analysis
- Investigating Hosts

Quick Look

Below is an example of the **YARA Rules** tab:



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

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

Risk score - Risk score of the host.

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

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

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

Agent Version - Version of the agent. For example, `12.0.0.0`.

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 System and Process Memory Dump.

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

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

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.