

Ransomware Detection powered by CyberSense®

v8.15.2515

User Guide

Describes how to use the Ransomware Detection software to monitor data integrity, detect malicious activity, and accelerate recovery in the event of a cyberattack.

© 2023, 2026 Hitachi Vantara. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

- 1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
- 2) Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Chapter 1. The Ransomware Detection User Interface.....	7
Logging into the Ransomware Detection UI.....	8
Expired password.....	9
Help.....	10
Changing your password.....	10
UI messages.....	10
Logging out of the Ransomware Detection UI.....	11
Chapter 2. Welcome to Ransomware Detection.....	13
License Expiration.....	13
Hosts Analyzed.....	14
Policies.....	14
Total Files Analyzed.....	15
Files Analyzed	15
Chapter 3. Investigating alerts.....	17
The Alerts table.....	17
Selected alert details.....	19
Suspect files list.....	24
Clearing an alert.....	28
Analyzing Ransomware Detection alerts.....	29
Identifying the suspect files.....	29
Remediate the attack.....	29
Stop reporting the infection.....	30
Chapter 4. Working with Ransomware Detection and hosts.....	31
Selecting a host.....	32
Daily Activity graphs.....	33
Viewing Daily Activity graphs.....	34
Daily Activity Threshold Exceeded alerts.....	42
Viewing Daily Activity threshold alerts.....	42
Configuring a Daily Activity threshold.....	43
Editing a Daily Activity threshold.....	45
Chapter 5. Checking your snapshots	47
Snapshots.....	48

Filtering the Snapshots table.....	50
The Snapshots CSV file.....	51
Alerts associated with a snapshot.....	53
Chapter 6. Managing policies.....	55
The Policy Editor.....	57
Creating a VMFS-based HVSP policy.....	57
Creating a block-based HVSP policy.....	60
Editing a policy.....	62
Deleting a policy.....	62
Using filters to specify paths and files.....	63
Log.....	68
Policy job details.....	69
Associated Alert table.....	71
Policy job phases.....	72
Viewing policy information.....	73
Filtering the Policies and Log tables.....	74
Exporting a Policy or Log report.....	79
Chapter 7. Configuring Ransomware Detection settings.....	81
Storage menu.....	82
Index Storage	82
User Management menu.....	85
User accounts.....	85
Role Privileges.....	87
Alerts menu.....	95
Special Criteria.....	95
Email Notifications.....	101
Network and Security menu.....	104
Login.....	104
Password Configuration.....	105
Active Directory.....	107
Security Certificates.....	109
Diagnostics and Reporting.....	111
License Management menu.....	114
License Status.....	114
License Details.....	117
Moving to client/server licensing on existing engines.....	120
Viewing the EULA.....	125
Advanced menu	126

Custom Thresholds.....	126
Custom YARA rulesets.....	139
Trusted Files.....	145
Global Resets.....	148
Recover from Backup.....	150
Global Feature Options.....	151
Appendix A. Supported systems and limits.....	153
Block device capacity limits.....	154
File system capacity limits.....	155

Chapter 1. The Ransomware Detection User Interface

The Hitachi Vantara Ransomware Detection User Interface (UI) is used by IT professionals to analyze any possible infection alerts created by Ransomware Detection analysis jobs, review any alert activity happening on hosts in a data center, view the status of recent snapshots, run policies to index and scan data on a target host, and configure various system settings after the initial setup process. Ransomware Detection performs full content analysis on each snapshot. The analysis is then used to determine the probability that the data modifications indicate possible corruption by ransomware, which is displayed graphically and in tabular form on the **Alerts**, **Hosts**, and **Snapshots** pages.

Use the pages in the Ransomware Detection UI to monitor your data integrity, detect malicious activity, and accelerate recovery in the event of a cyberattack. The pages are:

- [Home \(on page 13\)](#) - displays statistics on your data that is being analyzed by Ransomware Detection over a 30-day period.
- [Alerts \(on page 17\)](#) - displays alerts for evidence of data corruption, matching malware signatures, and any user-configurable thresholds.
- [Hosts \(on page 31\)](#) - shows up to 30-days worth of Ransomware Detection activity for a specified host, which includes changes to files, entropy, and possible data corruption, as well as user-configured alert thresholds based on the change types, and a tabular view of all alerts for this host.
- [Snapshots \(on page 47\)](#) - monitor the status and Ransomware Detection analysis of the snapshots to quickly identify the latest clean snapshot.
- [Policies \(on page 55\)](#) - displays a list of policies that have indexed and scanned a target host.
- [Settings \(on page 81\)](#) - shows the user-configurable settings for various system components, such as index storage, license management, and user-configurable alert thresholds.

You can easily review historical metrics showing that Ransomware Detection is scanning your data and hosts for possible ransomware attacks, ensuring that your snapshots are clean, and noting if any suspicious activity has taken place in them.

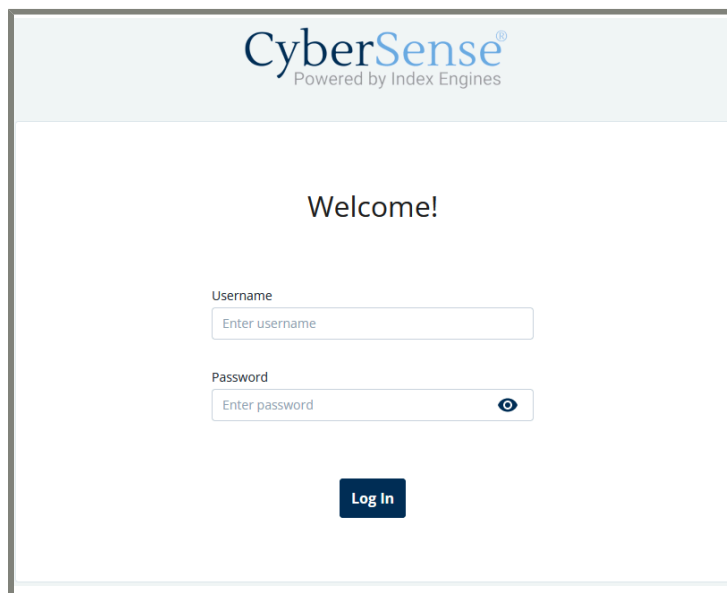
Logging into the Ransomware Detection UI

To log into the Ransomware Detection UI:

1. In a web browser, type:
`https://<hostname>`

 **Note:** The hostname is case sensitive.

Where *<hostname>* is the hostname or IP address of the server running the Ransomware Detection software.

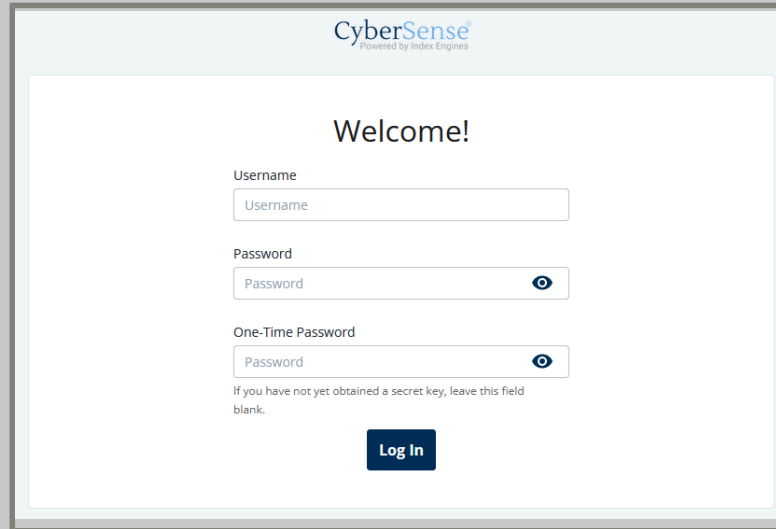


2. In **Username**, type your login, or the default administrator login of `admin`. In **Password**, enter your password. If using the default `admin` login, the password is `admin`. Select **Log In**.



Note:

If you have enabled MFA, the login screen will also display the **One-Time Password** field. Enter the OTP from your authenticator app. On your initial login, leave the field blank if your user account is not required to use MFA.



The **EULA** page of the **Setup** view appears.

Expired password

When you use an expired password to log into the Ransomware Detection UI, the **Login** page will prompt you to change your password.

To change your password:

In **New Password**, enter an updated password that conforms to company policy.


The new password must meet the following requirements:

- a minimum of 12 characters
- a maximum of 24 characters
- contain a minimum of one uppercase letter
- contain a minimum of one lowercase letter
- contain a minimum of one numerical character
- contain a minimum of one special character (!, @, #, \$, %, etc.)

Additional requirements are:

- no more than two repeating characters
- the new password cannot be the same as at least any of the previous five passwords

Help

In the Ransomware Detection UI, access the Ransomware Detection user documentation and the software version that's currently installed on the Ransomware Detection server from the **Help** icon  in the upper menu area.

The Ransomware Detection documentation is a locally hosted, browser-based documentation system, which is called WebHelp. It contains all the documentation needed to install and use the Ransomware Detection application, perform administrative functions, and source additional reference documents, such as the latest list of ransomware extensions, and is easily searchable. WebHelp also contains PDFs if you prefer that publishing format.

Changing your password

Change your password from any screen in the Ransomware Detection UI. Follow your company password guidelines when creating a new password to use to log into the Ransomware Detection UI.

1. From anywhere in the Ransomware Detection UI, select the user icon in the upper right, and then select **Change Password** from the drop-down menu.
2. In **Change Password**, type the username in **Username**.
3. In **Current Password**, type your current password.
4. In **New Password**, type a new password that follows your company password guidelines.
5. In **Confirm Password**, re-type the new password and select **Save**.

You will be logged out of the Ransomware Detection UI and need to log in using your new password.

UI messages

When using the Ransomware Detection UI, messages generated by a change confirmation or error are displayed in the upper right of the screen on any page of the UI. These messages are labeled as either:

- **Success** - indicated with a green background and are dismissed automatically in three seconds.
- **Error** - indicated with a red background and requires a user to close the message.

Logging out of the Ransomware Detection UI

To log out of the Ransomware Detection UI:

From any view, select the user icon in the upper right, and then **Log out** from the drop-down menu.

Chapter 2. Welcome to Ransomware Detection

The **Home** page, also referred to as the **Welcome to Ransomware Detection** page, is where you land when first logging into the Ransomware Detection UI after completing the installation setup. It displays what Ransomware Detection has been actively scanning and analyzing in the previous 30 days to find suspicious activity, even when none is found.

The information displayed on the **Home** page includes:

- [License Expiration \(on page 13\)](#)
- [Hosts Analyzed \(on page 14\)](#)
- [Policies \(on page 14\)](#)
- [Total Files Analyzed \(on page 15\)](#)
- [Files Analyzed \(on page 15\)](#)

See the links above for more information on each section of the **Home** page.

Download a PDF of the Data Integrity Scan report which reflects the data being displayed on the **Home** page by selecting **Download**.

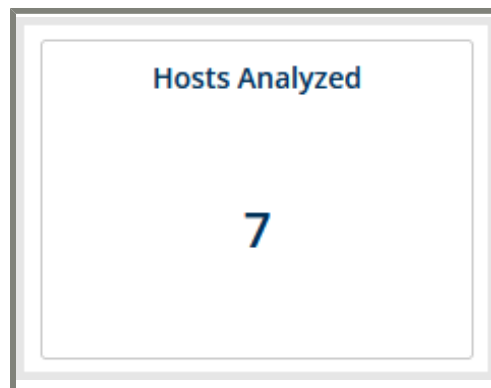
License Expiration

The **License Expiration** section of the **Home** page displayed the expiration of the installed license. The engine may be retrieving license information from a license server or a locally installed one. If you have a permanent license, the pane will state **Perpetual License**.



Hosts Analyzed

The **Hosts Analyzed** section of the **Home** page lists the number of target hosts whose files have been analyzed by Ransomware Detection per day.



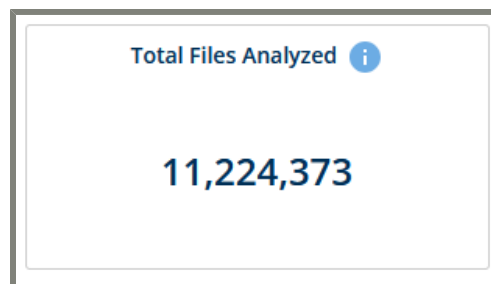
Policies

The **Policies** section on the **Home** page displays the number of all policies configured on the engine. It includes all policies whether they have been used when running a job or not.



Total Files Analyzed

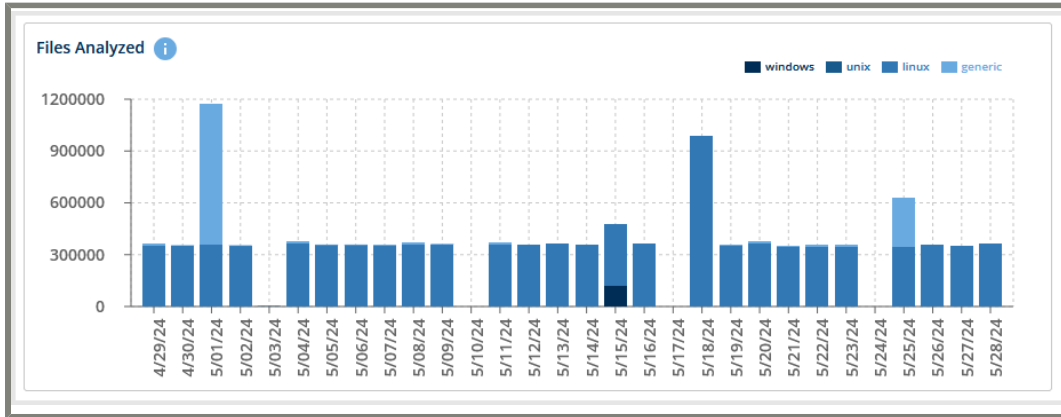
The **Files Analyzed** section of the **Home** page displays the number of all files analyzed by Ransomware Detection, including those that were created or modified.



Files Analyzed

The **Files Analyzed** section of the **Home** page graphically displays the number of files that were analyzed by Ransomware Detection, including created or modified ones, and groups them by host platform type chronologically. The different host platform types are:

- **Windows** - any Windows operating system
- **Unix** - any Unix operating system
- **Linux** - any Linux operating system
- **Generic** - any other data type



Chapter 3. Investigating alerts

The **Alerts** page lists any pending and cleared alerts that were generated when a policy was run on a target host. The alerts are found in the snapshot created by the policy. At a glance, you can quickly evaluate the state of your data by reviewing what types of alerts are listed and the alert severities. The **Alerts** tab also includes an indicator of the number of active alerts on the engine.

With this information, you can then perform company-instituted policies to remediate the suspect files and clear the infection or malware from your system. The possible suspect files are identified during the Ransomware Detection analysis phase in the post-processing of a scan. On the **Alerts** page, you can also clear the alert, which stops the reporting of the alert, and view the suspect files on a host.

The Alerts table

The **Alerts** table displays all pending and cleared alerts that have occurred on the Ransomware Detection server as well as the total number of alerts per severity. From this table, review existing alerts, clear alerts that have been dealt with, and filter the results to accommodate your needs. To see the details of an alert, select the alert in the **Alerts** table. If you want to review the suspect files, select **Show Files** associated with the selected alert to display a list of suspect files under the **Alerts** table. See [Selected alert details \(on page 19\)](#) for more information.

The alerts are grouped in two tabs, which are:

Tab Name	Description
Pending Alerts	These alerts are active and have not been cleared yet. The alert status displays as Pending on other pages, such as the Snapshots and Hosts pages.
Cleared Alerts	These alerts have been cleared and will no longer be reported. The alert status displays as Cleared on other pages, such as the Snapshots , Hosts , and Logs pages.

The table includes the following alert information:

- the **SEVERITY** of the alert. The alert severity is configurable for the user-defined alert thresholds and can be one of the following:

Alert Severity	Description
Critical	All malware and infection found alerts have a non-configurable severity of Critical . User-defined threshold alerts can be configured to have a Critical severity.
High	User-defined threshold alerts can be configured to have a High alert severity. Setting the severity level is dependent on your company's policies.
Medium	User-defined threshold alerts can be configured to have a Medium alert severity. Setting the severity level is dependent on your company's policies.
Low	User-defined threshold alerts can be configured to have a Low alert severity. Setting the severity level is dependent on your company's policies.

The alerts are also summed by severity above the **Alerts** table, which shows you the number of alerts of each severity type.



- the **TYPE** of alert, which is one of several types:

Alert Name	Description
Infection found	A possible infection was found. The alerts have a severity level of Critical which cannot be changed. See Infection found alerts (on page 21) for more information.
Malware File Detected	A possible malware file was detected. The alerts have a severity level of Critical which cannot be changed. See Malware File Detected alerts (on page 22) for more information.
YARA Ruleset Match	A possible match to a YARA ruleset was detected. YARA rulesets are user-configurable on the Settings > Advanced > Custom YARA Rulesets page. See Custom YARA rulesets (on page 139) for more information.
Threshold Exceeded	A threshold has been exceeded for the specified threshold. The alert threshold and severity is user-configurable on the Hosts page. See Threshold Exceeded alerts (on page 22) for more information.
Database Corruption	Indicates a possible corrupted database. See Database corruption alerts (on page 23) for more information.

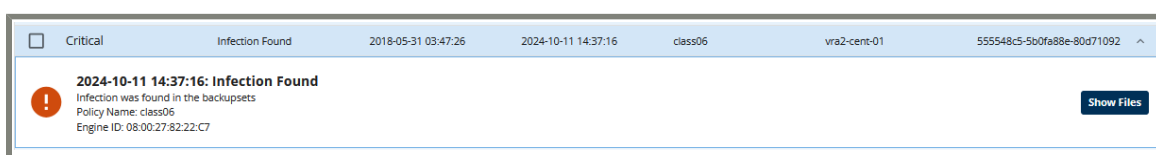
- the **SNAPSHOT TIME** is the date and time that the snapshot was created.
- the **ALERT TIME** is the date and time when the alert last occurred.

- the **POLICY NAME** is the name of the policy used in the Ransomware Detection job that generated the alert.
- the **HOST** is the target host on which the alert occurred.

Selected alert details

Select an alert to view more detailed information, which is displayed just under the selected alert. The information includes the type of alert, the policy name, and the host that was affected. You also have the option to display all files associated with the alert by selecting **Show Files**. The list appears under the **Alerts** table.

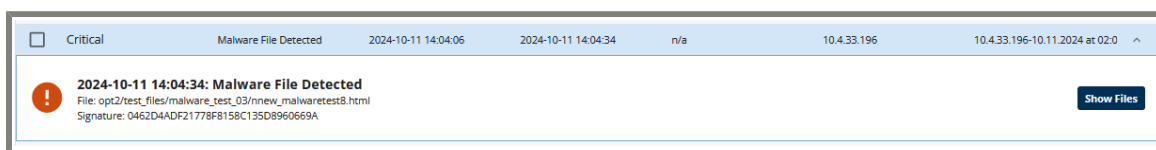
The following example illustrates the details shown for an **Infection found** alert.



The details for a **Infection found** alert include:

- the location of the infection
- what type of encryption or infection method was used by the malware
- the policy name
- the engine ID (host) of the Ransomware Detection server

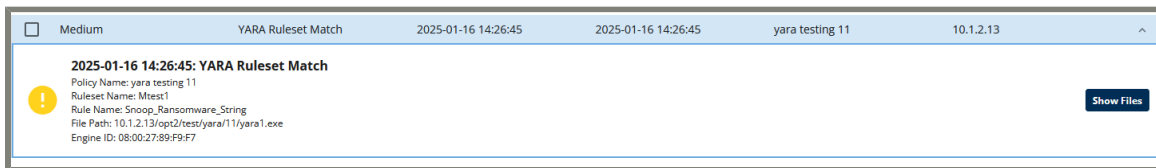
The following example illustrates the details shown for a **Malware File Detected** alert. The name of the suspected file and the malware signature that was matched is displayed.



For **Malware File Detected** alerts, the details shown are:

Field	Description
Policy Name	The name of the policy which generated the alert.
File	The path and filename of the file that triggered the alert.
Signature	The MD5 signature of the potential malware file.
Engine ID	The ID of the Ransomware Detection engine.

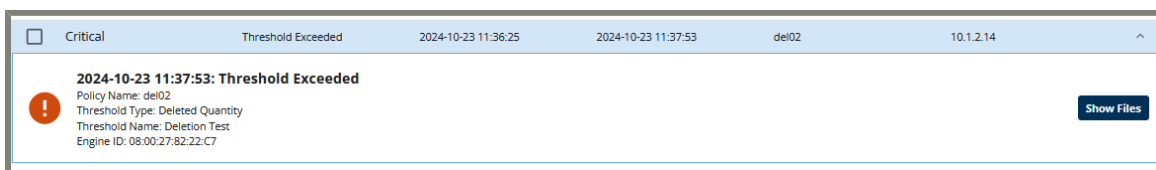
A **YARA Ruleset Match** alert is generated from user-defined YARA rulesets on **Settings > Advanced > Custom YARA Rulesets**.



The alert displays:

Field	Description
Policy Name	The name of the policy which generated the alert.
Ruleset Name	The name of the user-defined YARA ruleset
Rule Name	The name of the rule defined in the YARA ruleset.
File Path	The file name and path to the file that matched the YARA rule.
Engine ID	The ID of the Ransomware Detection engine.

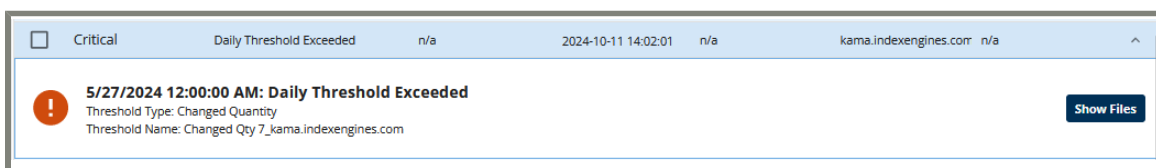
A **Threshold Exceeded** alert can be generated when a **Daily Activity** or **Custom Threshold** has been exceeded. The **Daily Activity** threshold definitions are set on the **Hosts** page, while the **Custom Threshold** definitions are set on the **Settings > Advanced > Custom Thresholds**.



For a **Custom Threshold** alert, the alert details are:

Field	Description
Threshold Format	Indicates whether the threshold that generated the alert was a Custom Threshold or a Daily Activity threshold.
Policy Name	The name of the policy which generated the alert. The threshold name is comprised of the type of change, the data format type, and the host.
Threshold Type	The type of Custom Threshold that was exceeded.
Threshold Name	The name of the Custom Threshold that was exceeded.
Engine ID	The ID of the Ransomware Detection engine.

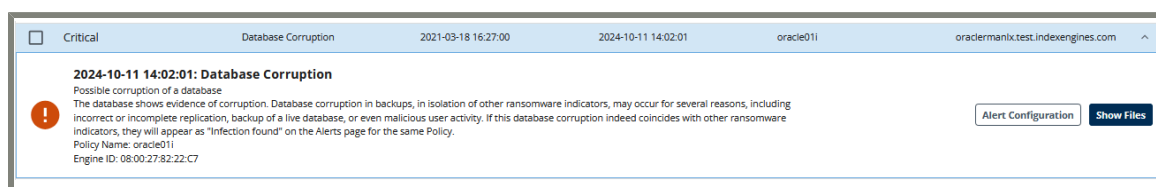
When a **Daily Activity** threshold alert occurs, no policy or snapshot is associated with this type of threshold alert.



The alert details are:

Field	Description
Threshold Format	Indicates whether the threshold that generated the alert was a Custom Threshold or a Daily Activity threshold.
Threshold Type	The type of Daily Activity threshold that was exceeded.
Threshold Name	The name of the host on which the Daily Activity threshold was exceeded.

If a **Database Corruption** alert has occurred, the details include the policy name and the engine ID.



After verifying and remediating the alert per company protocol, select **Clear** to change the status of the alert from **Pending** to **Cleared**. The alert will now appear under the **Cleared Alerts** tab in the upper section. To clear multiple alerts at once, select all the alerts you want to clear and then select **Clear** at the top of the **Alerts** table.

Infection found alerts

The Ransomware Detection post-processing phase analyzes the indexed files and will create **Infection found** alerts if it suspects files have been infected. When you select an alert in the **Alerts** table, its details are displayed in the middle pane, which include the infection type. If more than one infection type is found by Ransomware Detection analysis, then all applicable types are listed. Any found infections are associated with a policy name because the suspect files are found during the Ransomware Detection analysis post-processing.

If Ransomware Detection cannot identify a file's type, it will be labeled as **Unknown** in the **Suspect Files List** when **Show Files** is selected for an **Infection Found** alert. If the unknown file type matches a trusted filename pattern in the **Trusted Files** list, then Ransomware Detection will label the filetype as **Trusted** even though it is still an unknown filetype. See [Trusted Files \(on page 145\)](#) for more information.

The possible infection types are listed in the following table.

Type	Description
Encrypt with Original Filename	The file retains its original name and file extension, but the content has been encrypted.
Encrypt with Known Ransomware Extension	The file's contents has been encrypted and the file extension has changed to a known ransomware extension.
Encrypt with New Filename	The file's contents has been encrypted and the file name has been changed to hide the identity of the file.

Type	Description
<p>Ransomware Detection was unable to read some of the file systems from one or more disks on the host(s).</p>	<p>The disks were readable in a previous Ransomware Detection scan. There are several possible reasons for this change, including: (a) The disk may have been encrypted or erased by ransomware. (b) The disk may have been backed up improperly. (c) The disk may be defective. (d) The disk may have been out of operation during the snapshot process. (e) There may have been changes to the partition table. You should investigate each disk on the identified host(s) to determine the cause for the change in file access.</p>

Malware File Detected alerts

You can upload a more current file in the **Settings > Alerts > Special Criteria** window. See [Special Criteria \(on page 95\)](#) for more information.



Note: You cannot upload a malware signature file that is older than the currently installed one. The upload will fail.

After uploading an updated malware signature file, the detection process examines all existing segments for file signatures that match any of the known malware file signatures. For each new signature match, an alert is created. When the malware detection process runs after a policy job is finished, it will only analyze the newly created segments in the index.



Note: Updated malware signature files are available weekly.

The malware detection process works independently from ransomware analysis because it is not associated with a policy job, even though it runs during the post-processing phase of a policy job.

YARA Ruleset Match alerts

A YARA ruleset alert is generated when a file is found to match a rule in a user-defined YARA ruleset, which is set on **Settings > Advanced > Custom YARA Rulesets**. If multiple YARA rulesets match a single file, the alert with the highest severity level is displayed in the **Alerts** table. YARA rulesets contain pattern-matching rules to identify malware files and Ransomware Detection applies the rulesets when the storage is being read. See [Custom YARA rulesets \(on page 139\)](#) for more information.

Threshold Exceeded alerts

The **Threshold exceeded** alert type is generated by Ransomware Detection analysis in one of two ways:

- a **Daily Activity** threshold has been exceeded.
- a **Custom Threshold** has been exceeded.

With the **Daily Activity** and **Custom Thresholds**, you can set multiple alert thresholds with different severity levels. A Ransomware Detection policy may generate one or more threshold alerts for a particular host. When more than one threshold alert is raised, e.g., an alert for **Deleted Files** with a severity of **High** and one for **Changed Files** with a severity of **Medium**, then each alert is displayed as single line items in the **Alerts** table on the **Alerts** page. In this case, two **Threshold Exceeded** alerts will be displayed in the **Alerts** table along with the user-configured severity and the policy or snapshot that is associated with the threshold alert.



Note: When you configure a Daily Activity or custom threshold for **Changed File Type**, the threshold will consider **Trusted** and **Unknown** to be the same file type. However, a file of unknown type that matches the filename pattern under **Settings > Advanced > Trusted Files** will still appear as **Trusted** in the **Alerts > Show Files** table.

Daily Activity threshold definitions

A **Daily Activity** threshold generates alerts for a change type on a specific host and are triggered daily based on totals from the previous 24-hour period. The threshold graphs the changes per day to show the overall health of a host and its files. On the **Alerts** page, in the top table, all alerts from all hosts from a single day are grouped into a line item. Select the alert to see which thresholds were crossed per host. This threshold alert type has no policy name listed in the **Pending Alerts** table. Each kind of threshold alert has a unique list of relevant files. You can view that list in the lower section of the **Alerts** page.

Custom threshold definitions

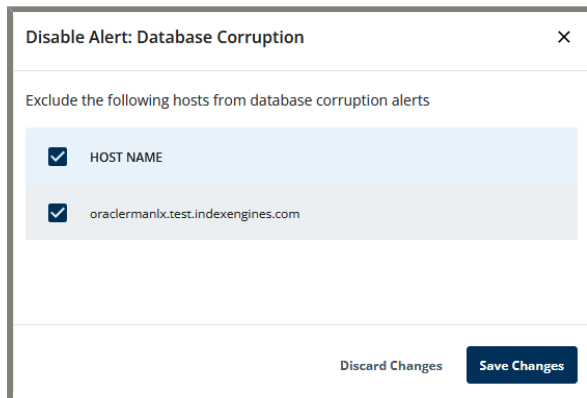
The **Custom Threshold** definition has the benefit of generating alerts for a specific host and folders or files to monitor between snapshots even when the snapshots are created on the same day. This granularity is not available when setting the **Daily Threshold Exceeded** alert thresholds. In the custom threshold definition, you can define multiple locations to be monitored as well as multiple definitions for different change types. Each alert is listed individually and is associated with a policy in the **Alerts** table. They are detected during the process of scanning snapshots.

Database corruption alerts

In certain circumstances, alerts for possible database corruption are generated for a policy that indexes and scans a snapshot volume containing a database. Sometimes this means the data in a database is corrupted but the structure is intact. If a possible infection is found, then two alerts may be generated; the first would be an **Infection Found** alert, and the second would be a **Database Corruption** alert. With Ransomware Detection, you can disable or enable the reporting of **Database Corruption** alerts when you select an alert in the **Alerts** table. This will not affect the generation of **Infection Found** alerts, which will appear regardless of whether the **Database Corruption** alerts are suppressed for a given host.

Disabling database corruption alerts

When you select **Alert Configuration** on a **Database Corruption** alert, you can disable the alerts for the suspected hosts by selecting the host name.



To enable or disable the database corruption alerts for all hosts, see [Configuring the database corruption alerting criteria \(on page 98\)](#) under **Settings** for more information.



Note: Disabling the reporting for database corruption alerts in the **Alerts** table overrides the global setting in **Settings > Alerts > Special Criteria**.

Suspect files list

When you select **Show Files** after displaying the details of an alert, the **Files** section appears under the **Alerts** table. The **Files** section displays a high-level summary of the alert details and graphical representations of the files related to the alert as well as a listing of those files. The **Files** that are listed are the suspect files and hosts, and any files that may have been added, deleted, or modified when an alert has been selected if applicable, and files that contributed to generating a user-configurable threshold. Change the view of this section with the buttons to display only the list or graphs, or use the **Search** field to find a specific set of files in the list.

Select **Show Files** on a selected alert in the **Alerts** table to list the alert statistics in various configurable ways. Using the **Filter** and **Columns** options, you can filter the files using one or several different attributes as well as remove or add columns to the table. For ease of reviewing the list of files, use the page navigation tools under the list and select the number of rows to display per page.

The information that is listed about the suspect files is:

- **HOST** - the host on which the suspect file is located.
- **PATH** - the location of the file including the hostname and directory.
- **NAME** - the name of the suspect file.
- **LAST MODIFIED** - the date and time that the file was last modified.
- **SIZE** - the size of the file.

- **LAST KNOWN SNAPSHOT ID** - the ID of the last snapshot in which Ransomware Detection found the suspect file.
- **MALWARE NAME** - *only displayed for malware alerts*; the name of the malware that was matched in the malware signature database.
- **ENTROPY** - the Shannon entropy of the file based in bytes, which is an indicator of whether a file is infected or not. The higher the value, the more likely a file is infected.
- **FILE TYPE** - during analysis, Ransomware Detection tries to identify the type of file. Besides identifying and displaying known file types, such as Windows Explorer files, the following are unknown file types that may be found by Ransomware Detection:

File Type	Description
Unknown	The file type is unknown to Ransomware Detection and cannot be identified.
Trusted	The file type is unknown to Ransomware Detection, but it matched a trusted filename pattern in the Trusted Files list. See Trusted Files (on page 145) for more information.



Note: This **Alerts > Show Files** table indicates the status of the files at the time that Ransomware Detection generated the alert. Subsequent changes to the **Trusted Files** patterns only affect future Ransomware Detection analyses.

For infection alerts, the number of suspect files and hosts are displayed as well as the number of added, deleted, and modified files. These are the files that exhibit characteristics indicative of that particular class of ransomware infection.

When a **Threshold Exceeded** alert is generated, the custom threshold type is displayed in the alert details. Select **Show Files** to list the files on the host that generated the alert.

Displaying and filtering the affected files

Select a tab to display the associated files. Each alert type will list the files slightly differently.



Note: This list is applicable to **Infection found** alerts. The files that have been added, deleted, or modified include all files on the host, even those that are not suspect. **Malware File Detected** alerts have found a file that has a signature matching a known malware and no files will be listed. For **Threshold exceeded** alerts, there will be two different displays for the files which is dependent on the origin of the threshold alert.

- files - files suspected of an infection or malware attack.
- suspect host(s) - hosts suspected of an infection or malware attack.
- added files - files in the snapshots that were added to the file system.

- modified files - files in the snapshots that were modified .
- deleted files - files in the snapshots that were deleted from the file system.

The top section lists, if applicable, the executed policy name, and the number of: suspect files, suspect hosts, added files, deleted files, and modified files. These statistics change depending on which alert you selected in the alert table. When you select a particular alert, this panel will show a list of files that Ransomware Detection has identified as possibly corrupt. However, because identifying an infection relies on the analysis of all the files in the snapshot, it is not always possible to identify specific, individual files that exhibit corruption.



Note: If Ransomware Detection has detected a Raw Disk Attack, you will not see a list of suspect files in this pane.

To download a CSV file containing the information about the files and hosts that are suspected to be infected, select **Download**.

The lower section of the dashboard displays a list of files, which you can group by the fields listed in the column headers. You can also choose which fields and columns to display using the **Filter** and **Column** options.

Another way to filter and sort the suspect files is to select a host, file extension, or a modified time, and the filtered results are displayed below the graphic. In the example below, the results were filtered by file extension first, then host, and finally the modification time.

Viewing file metadata

The metadata of a suspect file contains several descriptive fields that can help you decide whether a file is infected or not. This information includes the following metadata fields:



Note: Depending on the alert type, some fields may not be populated because they do not pertain to that particular alert type.

Metadata Field	Description	Example
File	The name of the file, not including the directory path.	malwarefile8.html
Result ID	Identifies the current location of a particular object in an index.	8796756951243-4-9.0
Path	Path to the file. The path includes the server and does not include the filename.	192.168.192.75/opt2/ie/var/
Size	The nominal size of the file as reported by the file system or the file's container.	158 Bytes

Metadata Field	Description	Example
File Type	The type of the file based on analyzing the content of the file.	Hypertext Markup Language (HTML)
Signature	The MD5 Hash of the contents of the file.	0E9C94A76D79F1FF04A54B86769A043C
Malware Name	If the signature matches an entry in the malware signature file, the name of the malware is displayed here.	STOP-dapo Ransomware
Modified	The modification time of the file.	Tue Jan 17 20:14:59 2023
Accessed	The last time the file was accessed, if present.	Thu Mar 23 15:03:55 2023
Host	The IP address or FQDN of the host where the file is located.	192.168.192.75
Snapshot Time	The date and time that the snapshot was created.	Wed Mar 29 15:18:12 2023
Snapshot ID	The ID of the snapshot assigned by the system when available.	192.168.192.75-03.29.2023 at 03:18 PM-94-1
Indexed Owner	The SID or username of the owner of the file.	S-1-6-1-5173
File Entropy	The Shannon entropy for the file based on bytes.	59
Entropy Delta	The difference between the entropy of the new version of a file compared to the previous version.	23
Status Flags	A set of flags that provide information on the status of an index and the indexing process, especially when the policy has encountered errors. See the <i>Hitachi Vantara Metadata Field Guide</i> for more information.	Corrupted (12207 anomalies including 39 Rman corruptions: 1:[Page 2: Invalid version in block header: is 4, expecting 2, Non-zero spare block header value, Invalid block: is 4eaf79, expecting 9c656b, Bad checksum: is 0xe0c1, computed as 0x80e4, entropy=99.69], 2:[Page 3: Invalid version in block header: is 13, expecting 2, Non-zero spare block header value, Invalid block: is 1cee79, expecting 5a80e2, Bad checksum: is 0xa85d, computed as 0x5a64, entropy=99.70]

To display the metadata of a file, select a suspect file from the list in the bottom pane of the dashboard. The metadata window opens and displays all metadata associated with the malware file or the infection alert that attacked the suspect file(s). The metadata shown below is for a **Malware File Detected** alert.

Downloading a list of suspect files

When you display the suspect files for an alert, you have the option to download a CSV file. The CSV file contains various metadata fields for each file.

1. On the **Alerts** page, select an alert from the **Alerts** table to display the alert details and the **Show Files** button.
2. Select **Show Files** and then select **Download**.
3. Save the CSV file to your preferred location.

Clearing an alert

When an alert is cleared, it will no longer show on the **Pending Alerts** tab. It is moved to the **Cleared Alerts** tab and is no longer reported by Ransomware Detection. Multiple alerts can be cleared at once.



Note: Clear an alert only after you have remediated the threat or corrupt files.

1. On the **Alerts** page, select the check box next to the alert(s) to clear.
2. After selecting all of the alerts you want to clear, select **Clear**. The cleared alerts will be moved to the **Cleared Alerts** tab.

Analyzing Ransomware Detection alerts

The **Alerts** page displays alerts that indicate a possible malware signature match, data corruption, a threshold was exceeded, or an infection has corrupted files. A typical workflow to remediate the infected files after a ransomware attack is:

- view the details of the critical alert indicating the ransomware attack
- restore from a clean snapshot copy
- clear the alert in the **Alerts** page

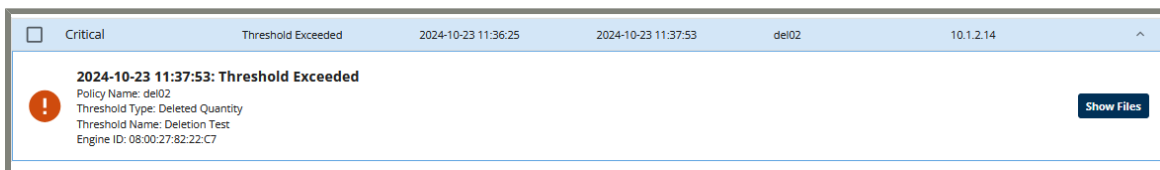
Identifying the suspect files

New alerts may appear after a policy job runs, and, during the post-processing phase of Ransomware Detection Analytics. When a new alert is listed in the **Pending Alerts** tab, it displays the number of hosts associated with the alert, the policy name used for the Ransomware Detection analysis job, the status, the type of alert, and the severity.



Note: At this time, only alerts with a status of **Pending** are displayed in the **Pending Alerts** table.

To see more detail on the alert, select it in the **Alerts** table. The details are displayed just below the selected alert.



From the alert details, you learn more information about the data corruption, infection, malware, or threshold. To see the files that are on the host that was affected by the alert, select **Show Files**. The files will be listed below the **Alerts** table.

To view the metadata of the suspect files, select a file from the bottom pane of the dashboard. The metadata pop-up opens.

The next step is remediation of the suspect files.

Remediate the attack

Once the suspect files are located, follow your company's policies to remediate the condition, which could include instructions similar to:

- remove the corrupted files
- restore from a recent snapshot
- verify that the infection has been removed

Stop reporting the infection

Clearing an alert moves it to the **Cleared Alerts** tab and stops reporting that alert in both email reports and on the **Alerts** page. Clearing an alert does not suppress subsequent analysis of that host, nor does it exclude files from subsequent analysis and alerting. In short, clearing an alert has no effect on subsequent analysis and alerting on a future alert criteria. Restoring the system from a clean snapshot after an attack significantly improves Ransomware Detection's ability to detect any subsequent ransomware attack in the future.

To stop the reporting of an alert, select the alert(s) and then select **Clear** at the top of the **Alerts** table.

Chapter 4. Working with Ransomware Detection and hosts

Use the **Hosts** page to configure **Daily Activity** threshold definitions and view graphs that plot the data focused on various change activity over a 30-day period. This will help to better understand the activity taking place on your hosts. Ransomware Detection performs content analysis on each snapshot of a host or a host group, and the threshold definitions will create alerts if they are exceeded. The alerts are displayed as **Threshold Exceeded** alerts under the **Alerts** pane as well as on the **Alerts** page under **Pending Alerts**. The graphs on the **Hosts** page are helpful for spotting activity trends in your data.



Note:

If no host is selected, the first available one in the **Hosts** list is selected. Run a policy job and the indexed host will appear in the **Hosts** list. If no hosts appear, no policy jobs have been run yet and the graphs will not display any data.

Only hosts with snapshots within the past 30 days are available for selection.

It's common to find a small percentage of hosts generate a large percentage of an organization's alerts.

To zoom in and out on a graph, use the scroll function on your pointing device when it is over a graph. By default, a maximum of 30 days of data is displayed in each graph. By scrolling in, you can view data from a smaller time interval.

Selecting a host

Select a host to display the associated Ransomware Detection monitoring information. A host will appear in the list after it has been indexed by a policy job specifying that host. The first available host in the list will be displayed by default. After you select a host, the associated graphs will be displayed.

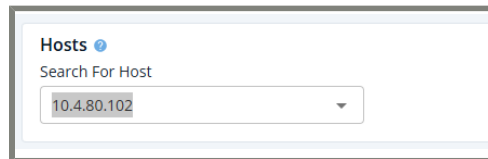
1. Go to **Hosts** and select your host from the drop-down list, or type the hostname or IP address in the field.



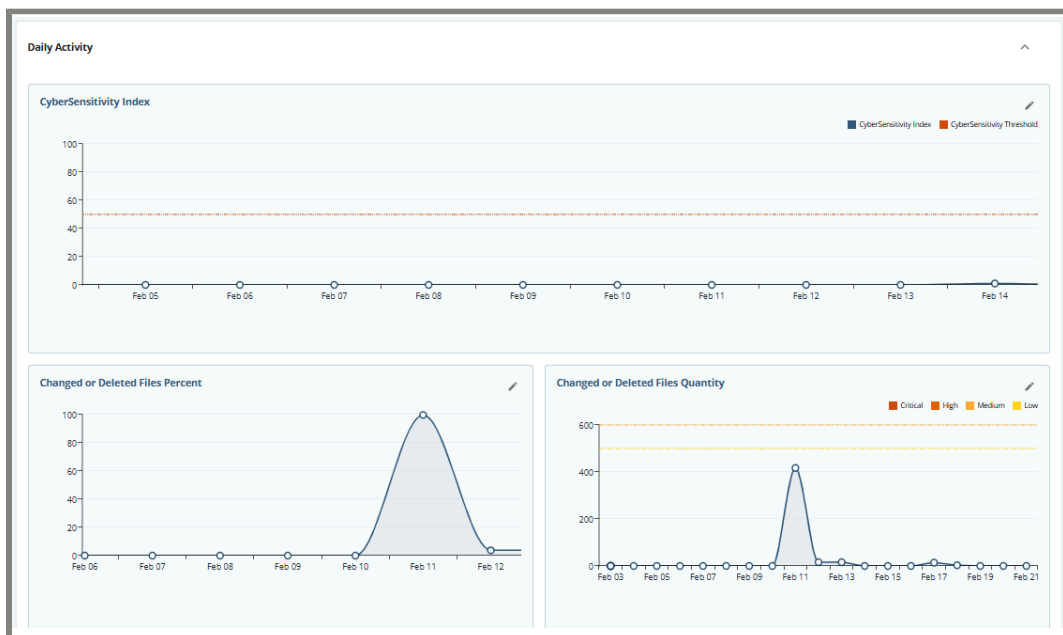
Note:

The host name may be an IP address, a DNS name or a Ransomware Detection policy name.

Only hosts with snapshots within the past 30 days are available for selection.

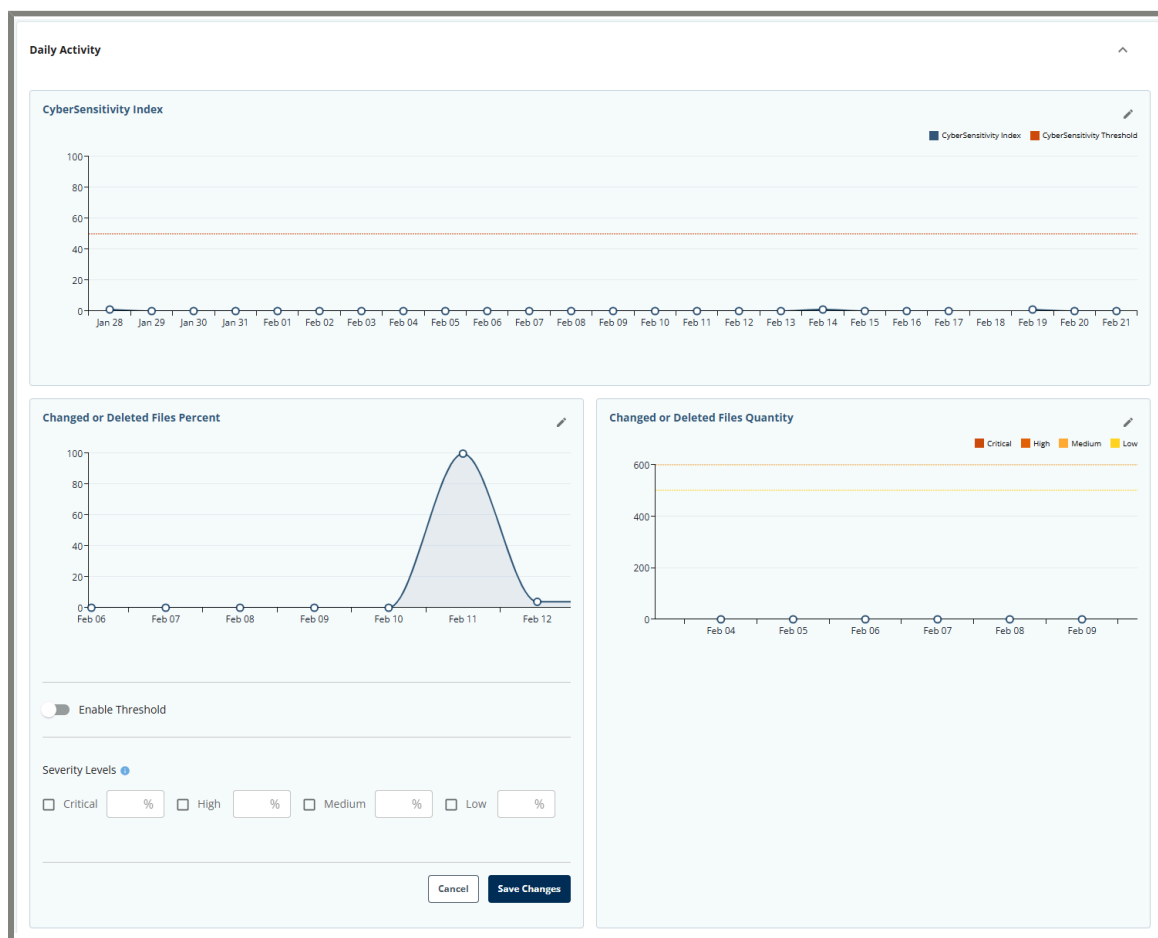


2. The **Daily Activity** graphs will be displayed.



Daily Activity graphs

Each graph displayed on the **Hosts** page is focused on a specific **Daily Activity** threshold for the selected host, and are grouped under the **Daily Activity** pane, which can be expanded and collapsed from view.



Daily Activity threshold definitions are triggered by activity on a specific host over 24 hours. **Daily Activity** threshold alerts of all types, from all hosts, on a given day, are consolidated into a single line item in **Pending Alerts** on the **Alerts** page. The highest severity of all these alerts is displayed. See [Daily Activity Threshold Exceeded alerts \(on page 42\)](#) for more information.

When you create a daily activity threshold definition, the severity levels are indicated by different colored dashed lines on the graph under **Hosts > Daily Activity**. The 30-day history of the graph can help you to choose an appropriate threshold value for the severity levels. If you change the severity level values of the daily activity threshold, the lines will move to the new value. The previous value is no longer shown.

Initially, the **CyberSensitivity Index** has a default threshold of **50** and can be changed but not deleted. The other graphs do not have default alert thresholds and you can create alert thresholds for those change types. Different threshold values for each graph is typical depending on what type of threshold alerts you are interested

in viewing. See [Changing the CyberSensitivity Index alert threshold \(on page 36\)](#) for information on setting the CyberSensitivity Index threshold.

When a policy using the selected host is run, the data is plotted on the graphs and the following change types are displayed for the previous 30 days worth of data. View these change types as a quantity or percentage.

- **CyberSensitivity Index** - the total risk score based on Ransomware Detection analysis on the selected host. This graph is only displayed for **Daily Activity** threshold definitions. You can change the threshold level on this graph; see [Changing the CyberSensitivity Index alert threshold \(on page 36\)](#) for more information.
- **Changed Files** - the amount of changed files for the selected host.
- **Changed File Type** - the amount of files whose type changed for the selected host.
- **Deleted Files** - the amount of deleted files for the selected host.
- **Entropy** - the average entropy of all the files for the selected host over time. Entropy describes the randomness of data in a file and is usually an indicator of file encryption. Encrypting a file typically increases the file's entropy. The entropy value in this graph ranges from 0 (no entropy) to 100 (maximum entropy). Ransomware typically increases a file's entropy to more than 90 on this scale.

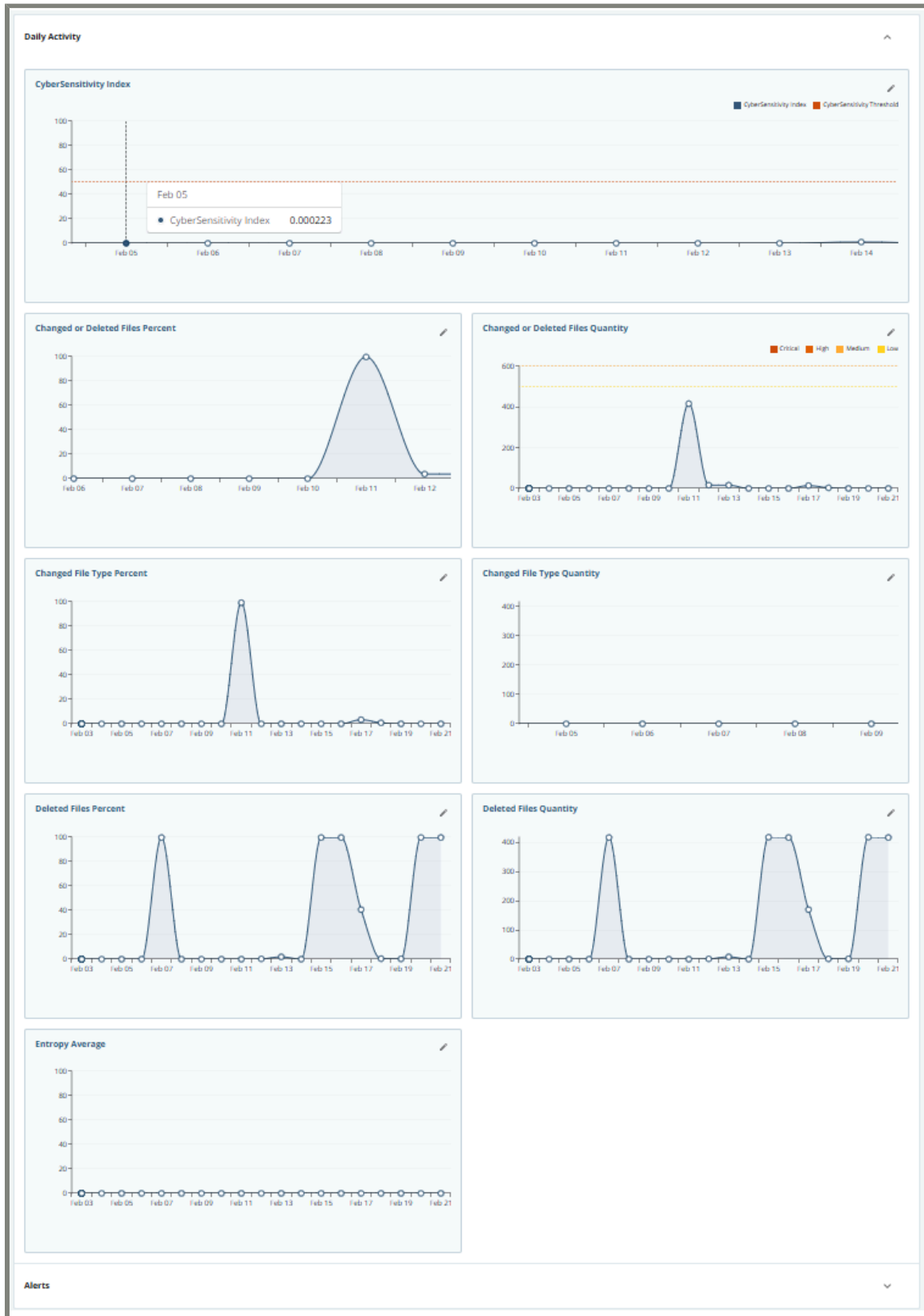
The threshold severity levels are displayed as different color lines on the graphs indicating the level at which a threshold alert will be generated if it is exceeded. Modify and enable the **Daily Activity** thresholds by selecting the **Edit** icon for a graph. See [Configuring a Daily Activity threshold \(on page 43\)](#) for more information.

Viewing Daily Activity graphs

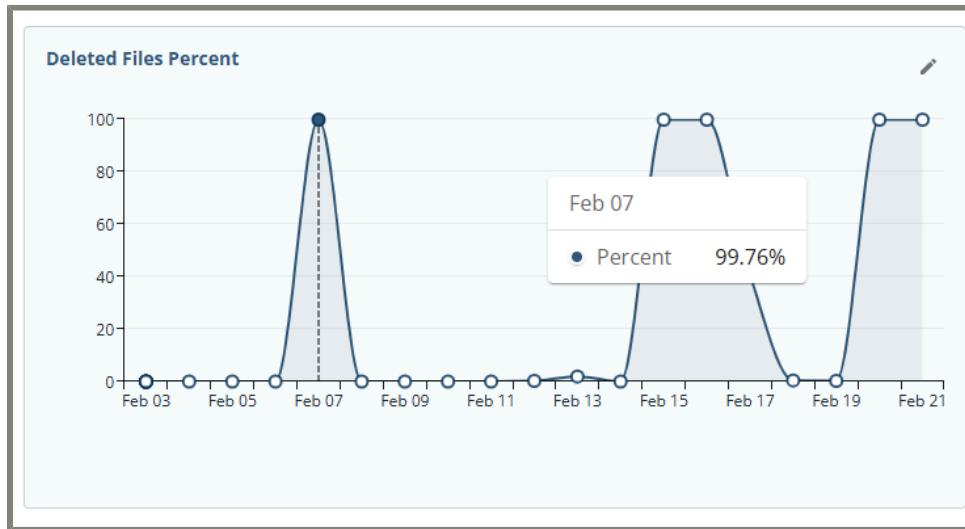
By default, the first host in the **Host** dropdown list is displayed in the **Hosts > Daily Activity** pane. If no hosts exist in the dropdown list, the panes are empty and messages are displayed to indicate that a host must be selected. Run policy jobs to display the hosts in the **Host** dropdown list.

To view the **Daily Activity** graphs for a selected host:

1. Go to **Hosts** and select a host from the drop-down list.
2. Select the **Daily Activity** pane to expand it. The graphs display data from running policies on a host and the data grouped by the type of change on the files.

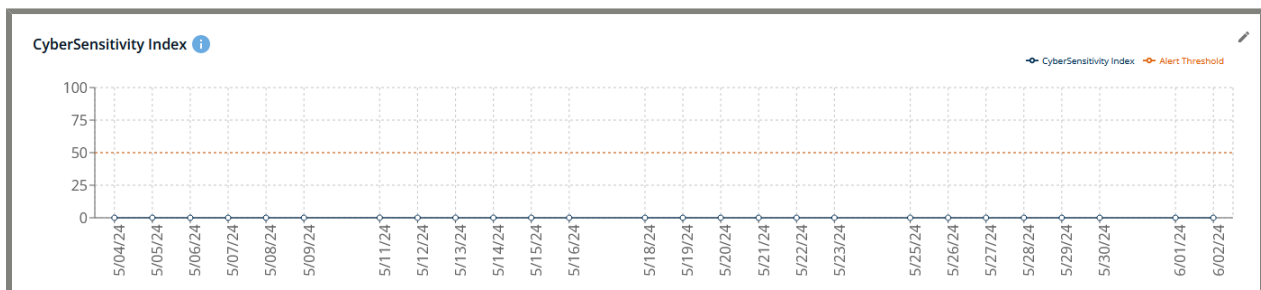


Hover over a graph to see more details for a specific date. The graph will list all severity levels that were set using different color dashed lines as well as a severity level key in the upper right corner.



CyberSensitivity Index

The **CyberSensitivity Index** graph shows the daily history of the value that Ransomware Detection assigned to potential of ransomware corruption. This tracks the Artificial Intelligence (AI) score that Ransomware Detection generates using multiple machine learning algorithms on full content analysis of the host data. This score shows the probability as a value between 0 and 100. The default value is 50 and can be modified. See [Changing the CyberSensitivity Index alert threshold \(on page 36\)](#) for details. To see the details of a particular date, hover on the data line to display the information.

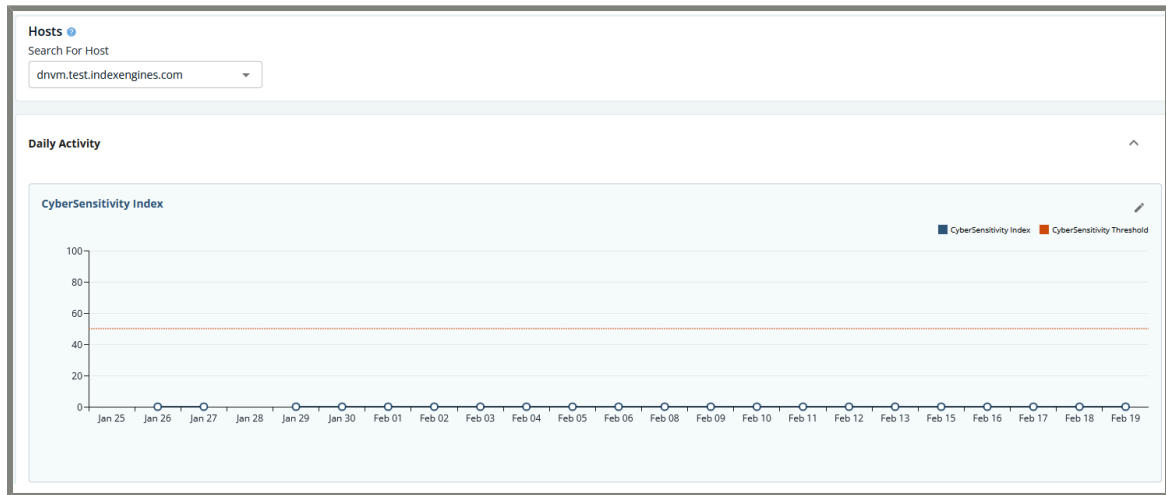


The **CyberSensitivity Index** is determined by the process where Ransomware Detection performs full content analysis on each indexed snapshot, and then feeds the analysis into its Artificial Intelligence (AI) engine to determine the probability that the data has been modified by ransomware. By default, Ransomware Detection will generate an alert if the value of the analysis is greater than 50 (default); modify this level to a lower value to increase sensitivity, or to a higher value to decrease sensitivity, between 5 and 95.

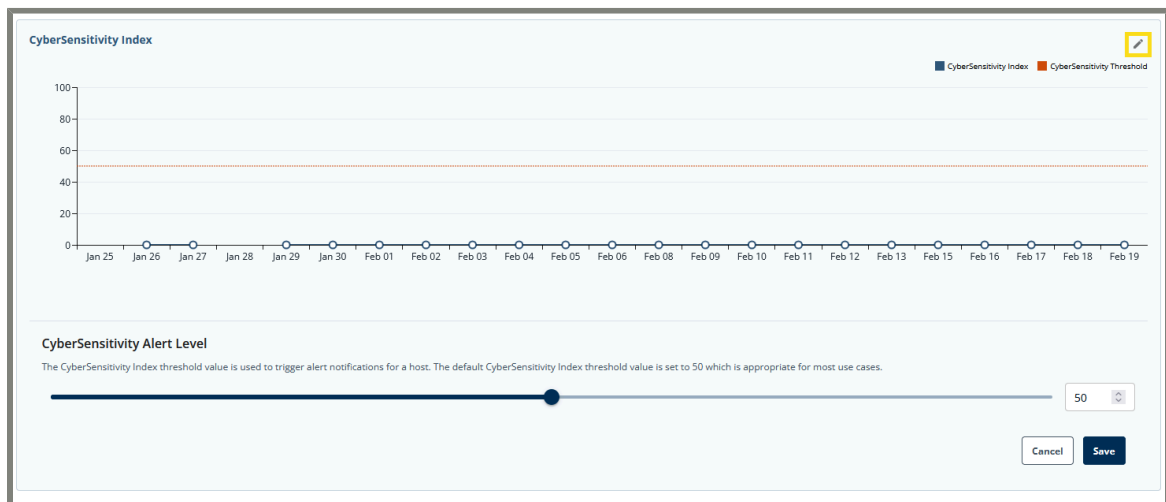
Changing the CyberSensitivity Index alert threshold

To change the alert threshold on the CyberSensitivity Index graph:

1. Go to **Hosts** and select a host from the drop-down menu.
2. The **Daily Activity** pane is expanded and the associated activity graphs are displayed.



3. Select the **Edit** icon in the upper right corner of the **CyberSensitivity Index** graph. This opens the **CyberSensitivity Alert Level** pane for editing.

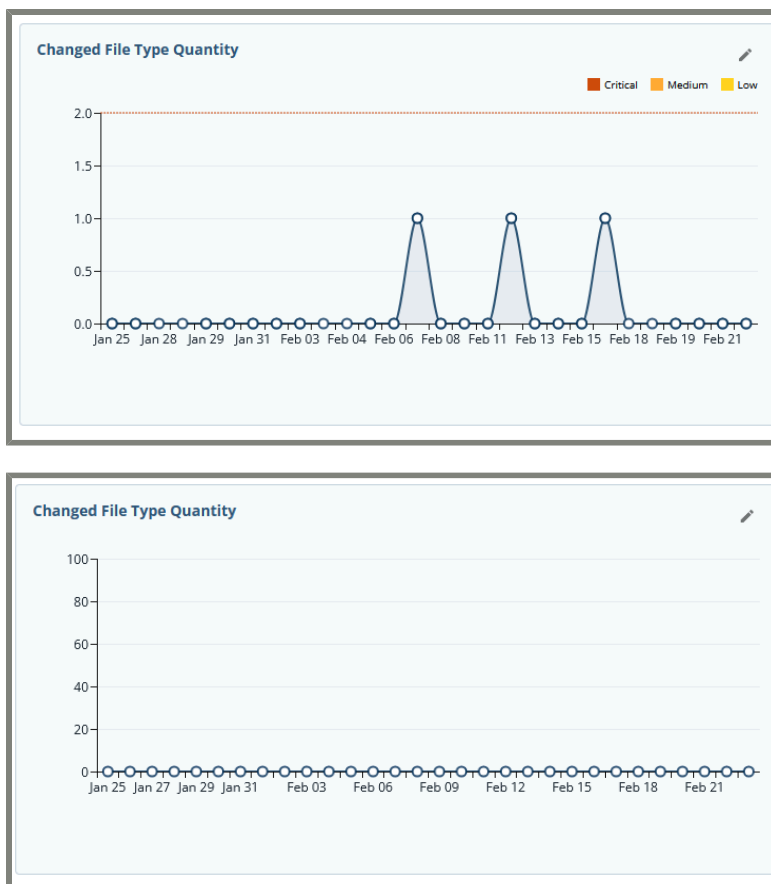


Note: A higher threshold value decreases the sensitivity of the Ransomware Detection analysis process and the results may not reflect the correct number of affected files. Lowering the threshold value increases the sensitivity and results in a larger number of files that are suspected of being affected by ransomware.

4. Change the value of the threshold and select **Save** when done. Select **Cancel** to cancel the changes.

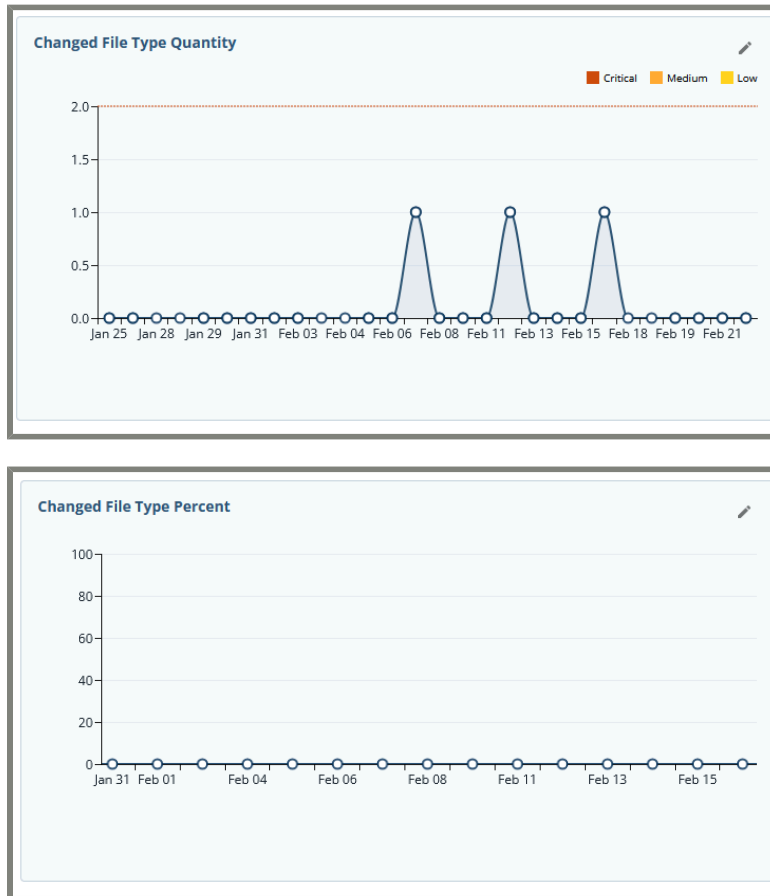
Changed Files

The **Changed Files** graph focuses on the quantity of file that changed that have occurred in the last 30 days on the selected host. This includes file content changes as well as file metadata changes. To see the details of a particular date, hover on the data line to display the information.



Changed File Type

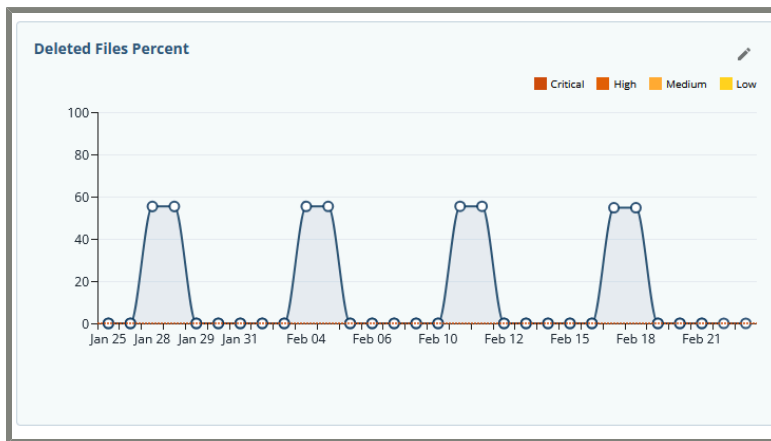
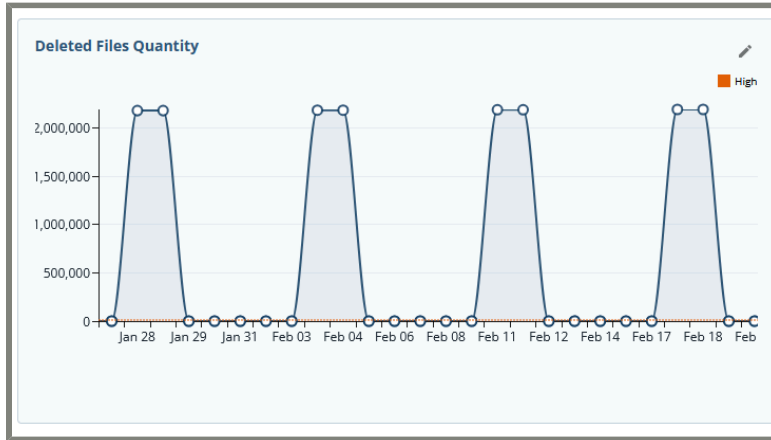
The **Changed File Type** graph focuses on the quantity of files that exhibit a different file type based upon full content analysis. The line chart represents the results of the Ransomware Detection scans over the last 30 days. To see the details of a particular date, hover on the data line to display the information.



Note: When you configure a Daily Activity or custom threshold for **Changed File Type**, the threshold will consider **Trusted** and **Unknown** to be the same file type. However, a file of unknown type that matches the filename pattern under **Settings > Advanced > Trusted Files** will still appear as **Trusted** in the **Alerts > Show Files** table.

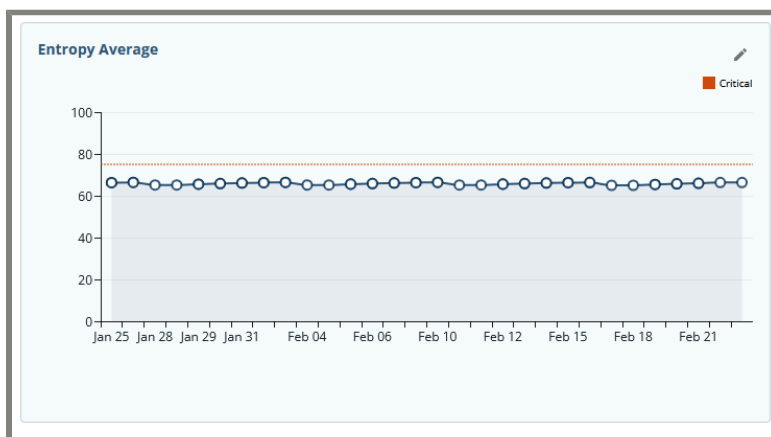
Deleted Files

The **Deleted files** graph focuses on the amount of file deletions that have occurred in the last 30 days on the selected host. To see the details of a particular date, hover on the data line to display the information.



Entropy

The **Entropy** graph focuses on the average entropy of all the files on a host and represents the results of the Ransomware Detection scans over the last 30 days. To see the details of a particular date, hover on the data line to display the information.



Entropy represents the randomness of data in a file and generally indicates file encryption. Encrypting a file typically increases the file's entropy. The entropy value in this graph ranges from 0 (no entropy) to 100 (maximum entropy).

Daily Activity Threshold Exceeded alerts

The **Alerts** table in the **Hosts > Alerts** pane displays a log of alerts that have occurred on a selected host. Select an alert to be redirected to the **Alerts** page to view more details. Using the **Filter** option, you can filter the files using one or several of the columns.

The table, which lists all alerts that have occurred for the specified host, includes information such as:

Column	Description
SEVERITY	The severity level of the alert.
TYPE	The change type of the alert.
SNAPSHOT TIME	The date and time of the snapshot which generated the alert was created.
ALERT TIME	The date and time when the alert last occurred.
STATUS	The status of the alert, which is either Pending or Cleared .
POLICY NAME	The name of the policy used in the Ransomware Detection job that generated the alert. Alerts for Daily Activity thresholds are not associated with a single policy and display n/a instead of a policy name in this column.
HOST	The target host on which the alert occurred.

Viewing Daily Activity threshold alerts

To view all Daily Activity alerts for the selected host:

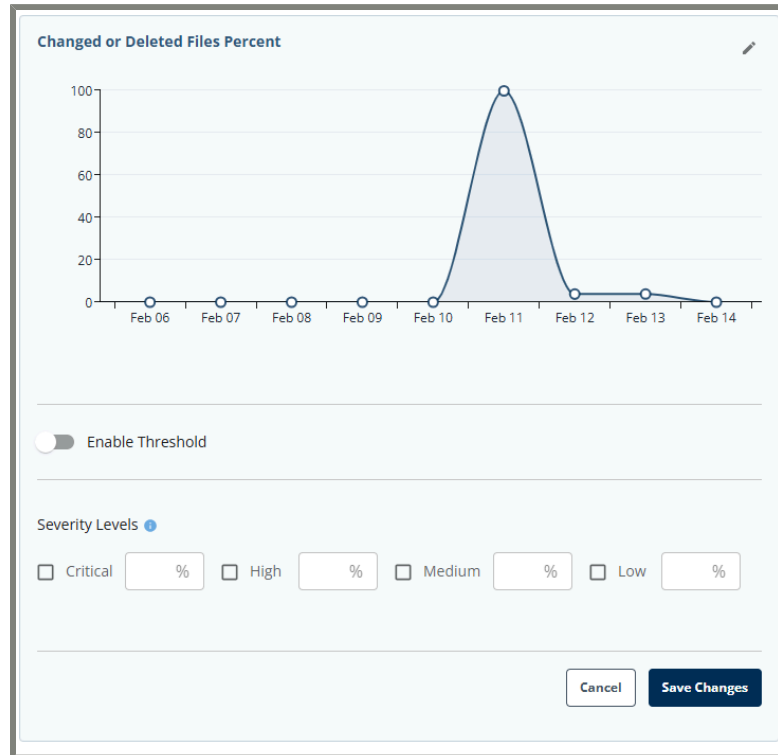
1. Go to **Hosts** and select a host from the drop-down list.
2. Select **Alerts** to expand the pane. The alerts that have occurred for the selected host are listed.

Select an alert to see more details on the **Alerts** page.


Configuring a Daily Activity threshold

To set up a **Daily Activity** threshold:


1. On the **Hosts** page, select the **Edit** icon on a **Daily Activity** graph.




2. Toggle **Enable Threshold** to enable generating alerts when the daily activity limit has been reached.

 **Note:** Once the threshold has been enabled and severity levels have been set, you can disable the **Daily Activity** threshold but you cannot remove the severity level values.

3. Configure the severity level as described below:

Field	Description
Severity Levels	<p>Set a value for each severity level that you want to use.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;">  Note: At least one severity level must be set. </div> <p>The value must decrease for each level:</p> <ul style="list-style-type: none"> ◦ Critical ◦ High

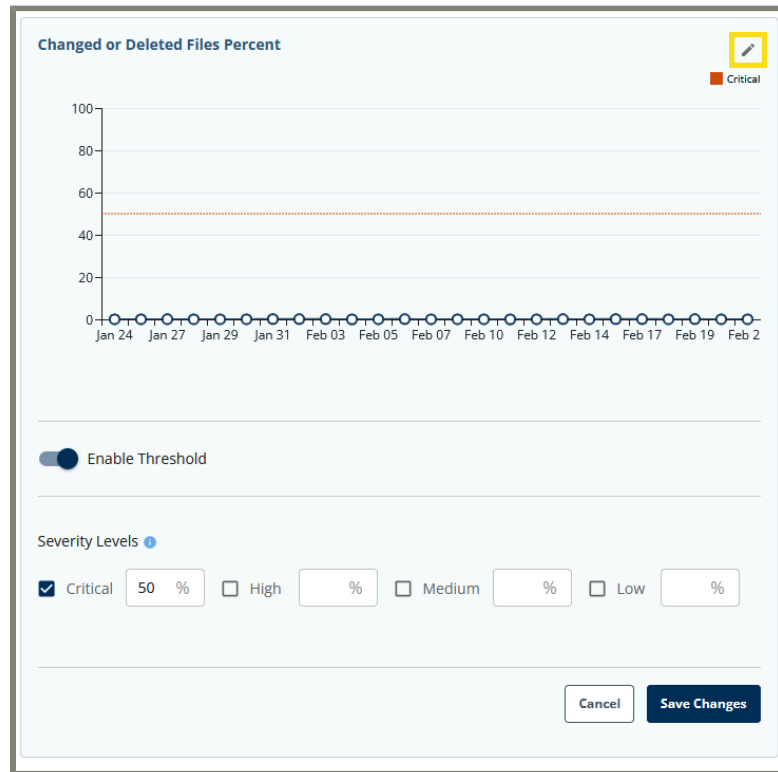
Field	Description
	<ul style="list-style-type: none"> ◦ Medium ◦ Low <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin: 10px 0;">  Note: A Threshold Exceeded alert will be triggered when the number or percentage of changed files is greater than the value set for a severity level. </div> <p>For example, you created a threshold for a percent of deleted files and want to know when more than 20%, 15%, 10%, and 5% of your files have been deleted. Set the severity levels as follows:</p> <ul style="list-style-type: none"> ◦ Critical to 20 ◦ High to 15 ◦ Medium to 10 ◦ Low to 5 <p>If more than 5% of your files are deleted, an alert with the severity level of Low is generated.</p>
Minimum	<p><i>Only available for the Entropy change type.</i> This is the minimum entropy that the configured percentage of files must be for an alert to be generated. Example: if you have set Value to 20% and Minimum to 90, then 20% of the files must have an entropy of at least 90 to generate an alert.</p>

4. Select **Save Changes** when complete.


Editing a Daily Activity threshold

To edit a **Daily Activity** threshold:

1. On the **Hosts** page, select the **Edit** icon on the graph that is associated with the **Daily Activity** threshold that you want to change.



2. Toggle **Enable Threshold** to enable/disable the threshold from generating an alert.
3. Edit the severity levels and values:

Field	Description
Severity Levels	<p>Set a value for each severity level that you want to use. At least one severity level must be set. The value must decrease for each level, which are:</p> <ul style="list-style-type: none"> ◦ Critical ◦ High ◦ Medium ◦ Low <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> Note: A Threshold Exceeded alert will be triggered when the number or percentage of changed files is greater than the value set for a severity level.</p> </div>

Field	Description
	<p>For example, you created a custom threshold for a percent of deleted files and want to be alerted when more than 20%, 15%, 10%, and 5% of your files have been deleted. Set the severity levels as follows:</p> <ul style="list-style-type: none"> ◦ Critical to 20 ◦ High to 15 ◦ Medium to 10 ◦ Low to 5 <p>If more than 5% of your files are deleted, an alert with the severity level of Low will be generated.</p>
Minimum	<p><i>Only available for the Entropy change type.</i> This is the minimum entropy that the configured percentage of files must be for an alert to be generated. Example: if you have set Value to 20% and Minimum to 90, then 20% of the files must have an entropy of at least 90 to generate an alert.</p>

4. When the changes are complete, select **Save Changes**.

Chapter 5. Checking your snapshots

In an attack scenario, use the **Snapshots** page to locate your most recent clean snapshots at a glance. The **Snapshots** page displays a list of snapshots for recently scanned host volumes, and displays the following information: the host and the snapshot group name, the volume ID, index time, creation time, and any alerts that occurred. If a snapshot has generated any alerts, select it in the table to see details about the associated alerts. When you know which snapshot is clean, you can then remove the infected files and restore them from the clean snapshot.

To find a snapshot based on the **STATUS** or another property, select the column and select the three dots for a context menu. Select **Filter** and configure the filter based on your criteria. Use the **Associated Alerts** table to quickly determine what type of alerts have been raised. Select the alert to go to the [Alerts \(on page 17\)](#) page and view the details.

Download a CSV file for a list of snapshots and detailed information. See [The Snapshots CSV file \(on page 51\)](#).

Snapshots

The **Snapshots** table lists the snapshots created during an indexing job. Navigate through the **Snapshots** table by selecting the number of rows to display and using the page number to jump to a specific page. The following snapshot information is displayed:

- **STATUS** - the status of the Ransomware Detection scan on the snapshot. If the scan raised any alerts, you will be notified here. The job status can be:

Status	Description
Alert	Ransomware Detection found potential ransomware or infections and raised at least one alert on this snapshot. Select the row to populate the Alerts table. In the Alerts table, select the row to go to the Alerts page and view more details.
In Progress	Ransomware Detection is still analyzing the snapshot.
Not analyzed	Ransomware Detection did not analyze the snapshot. This message only appears if: <ul style="list-style-type: none"> ◦ The snapshot contained zero files, no new files, or no changed files. ◦ The was not analyzed because of an error condition ◦ The job was cancelled after the snapshot was scanned and the no job was subsequently run on the policy ◦ The policy is still running and has not completed the analysis phase.
Clean	The snapshot is clean and Ransomware Detection did not raise any alerts during its scan process.
Suspect	Indicates the presence of a pending or uncleared alert generated in a at the time of analysis. If the alert is later cleared, the status of this is not affected. The following alerts generate this status: <ul style="list-style-type: none"> ◦ Malware File Detected ◦ YARA Ruleset Match ◦ Infection Found

- **HOST** - the name or IP address of the front-end host.
- **SNAPSHOT GROUP NAME** - the name of the snapshot group, which is set when a policy is run and takes a new snapshot. The naming format is a combination of an abbreviated policy name and a date/time stamp. An example of a snapshot group name is CS-vsp_policy-1753204193.
- **VOLUME ID** - the unique identifier in decimal and hexadecimal values of the primary volume for which a snapshot was taken.
- **STORAGE ARRAY** - the serial number of the storage array used by the policy.
- **MIRROR UNIT** - the unique identifier for snapshots related to a primary volume.
- **POLICY** - the name of the policy that took the snapshot.

- **CREATION TIME** - the time that the snapshot was created.
- **EXPIRATION TIME** - the time when the snapshot expires.

When dealing with a malware alert, scan the table to find the most recent snapshot with the status **Clean**. Once found, use your company policy to restore the files to a clean state.

Filtering the Snapshots table

Filter the **Snapshots** table by certain columns that are described in the table below. Select the column label to sort the column's contents in ascending or descending order.

Column	Operator	Value
STATUS	is	Select a single item from the fixed drop-down list: <ul style="list-style-type: none"> • Clean • Not analyzed • Alerts
HOST	equals	Find items that contain exactly the characters entered in the Value field.
SNAPSHOT GROUP NAME	equals	Find items that contain exactly the characters entered in the Value field.
VOLUME ID	equals	Find items that contain exactly the characters entered in the Value field.
STORAGE ARRAY	equals	Find items that contain exactly the characters entered in the Value field.
MIRROR UNIT	equals	Find items that contain exactly the characters entered in the Value field.
POLICY	equals	Find items that contain exactly the characters entered in the Value field.
CREATION TIME	between	Find snapshots based on their creation time between two dates specified with the date picker.
EXPIRATION TIME	between	Find snapshots based on their expiration time between two dates specified with the date picker.

The Snapshots CSV file

Select **Download** to download a CSV file containing detailed information about all of the snapshots that were created when a policy job was run. The following table lists the included information.



Note: The fields included in the snapshot CSV file can also be found in the *Hitachi Vantara Metadata Field Guide*.

Column Label	Description
Host	The host owns the file and the data stored on the primary volume(s) specified in the policy.
Root Path	The path of the top-most folder in the snapshot.
Status	The status of the snapshot, which can be: <ul style="list-style-type: none"> • Clean • Alerts • Not Analyzed
Dataset ID	The unique identifier of the individual snapshot.
Dataset ID Long Form	A more precise definition than the Dataset ID derived from the backup stream.
Job UUID	The unique identifier of the policy job that ran and created the snapshot.
Storage Array	The name of the storage array.
Policy	The name of the policy associated with the snapshot.
Start of Snapshot	Date and time the snapshot was created.
Creation Time	The time that the snapshot was created.
Volume ID	The unique identifier in decimal and hexadecimal values of the primary volume for which a snapshot was taken
Segment Name	The name of the segment in the index that contains the snapshot.
Indexing Start Time	The start time of the policy job's indexing phase.
Indexing End Time	The end time of the policy job's indexing phase.
Indexing Duration	The length of time that the indexing phase took to complete.
Expiration Time	The expiration time of the snapshot.
Data Size	The total number of bytes of data in the snapshot.
Total files	The total number of files in the snapshot.

Column Label	Description																		
Total Directories	The total number of directories in the snapshot.																		
Read Errors	The total number of errors reading the host's files.																		
Failed Directories	The number of directories that failed to be indexed.																		
Bytes In Level 1 Files	The total number of bytes in in indexed files.																		
License Size	The analyzed size charged in a pay-per-byte indexing counter in a license.																		
Exceptions	The number of exceptions that occurred during indexing.																		
Termination Status	The status of the data stream, which can be: <ul style="list-style-type: none"> • Closed Normally • Terminated • Aborted Externally 																		
Status Flags	The status flags of the indexing job.																		
Not Licensed	Indicates whether the index segments containing the snapshot data has a valid license. <ul style="list-style-type: none"> • 0 - indicates a valid license • 1 - indicates there is a licensing problem with the index segment and Ransomware Detection analysis is not performed on it. 																		
Client Type	The host platform or client application that was indexed. Potential values for this field include any of the following host platform or client application: <table border="1" data-bbox="456 1272 1464 1600"> <tbody> <tr> <td>Unknown</td> <td>IRIX</td> <td>SAP</td> </tr> <tr> <td>Windows</td> <td>Apollo</td> <td>Sybase</td> </tr> <tr> <td>Exchange</td> <td>UNIX</td> <td>DB2</td> </tr> <tr> <td>MS SQL</td> <td>AFS</td> <td>VMware</td> </tr> <tr> <td>Oracle</td> <td>Linux</td> <td>ADS</td> </tr> <tr> <td>Lotus</td> <td>Informix</td> <td>SharePoint</td> </tr> </tbody> </table>	Unknown	IRIX	SAP	Windows	Apollo	Sybase	Exchange	UNIX	DB2	MS SQL	AFS	VMware	Oracle	Linux	ADS	Lotus	Informix	SharePoint
Unknown	IRIX	SAP																	
Windows	Apollo	Sybase																	
Exchange	UNIX	DB2																	
MS SQL	AFS	VMware																	
Oracle	Linux	ADS																	
Lotus	Informix	SharePoint																	

Alerts associated with a snapshot

Select a snapshot in a row of the **Snapshots** table to display all alerts related to that snapshot in the **Associated Alerts** table. This list appears below the **Snapshots** table.

The details about the alerts are:

- **SEVERITY** - the severity of the alert, which is set by the user and can be:
 - **Critical**
 - **High**
 - **Medium**
 - **Low**
- **TYPE** - the type of alert. See [Investigating alerts \(on page 17\)](#) for more details.
- **SNAPSHOT TIME** - the most recent time the alert was updated.
- **ALERT TIME** - the time that the alert was generated.
- **POLICY NAME** - the name of the Ransomware Detection job from which the alert was generated. If the alert type is **Malware File Detected**, there is no policy associated with the alert.
- **HOST** - the host on which the alert was generated.

The table is sorted by date, newest to oldest, unless you select another column to sort by.

Select a row in the **Associated Alerts** table to go to the **Alerts** page and view more details.

Chapter 6. Managing policies

Use the **Policies** page to view, create, modify, and delete policies and list a log of the jobs that used these policies to index and scan the target host and files. Expand the policy job row to view more policy and workload information. See [Viewing policy information \(on page 73\)](#) for more details.

The **Policies** page displays a list of policies and additional information about each policy. The columns are:

- **STATUS** - the status of the policy job, which is:

Status	Description
Running	A Ransomware Detection job for that specific policy has been started.
Idle	The policy is not being used by any currently running Ransomware Detection job.
Done Failed Partial Canceled Canceling Alert	Indicates the final policy job status. <ul style="list-style-type: none">◦ Done - the job based on the specific policy has completed without errors.◦ Failed - the job has failed.◦ Partial - the job has partially completed. This may happen if the data source is not available.◦ Canceled Canceling - the job was canceled by the user or in the process of canceling.◦ Alert - an alert was generated from this job. See Investigating alerts (on page 17) for more information on the various types of alerts that can be generated.
Pending	The policy job is in the queue to run.

- **POLICY** - the user-defined name of the policy. If the policy was not created using the Ransomware Detection UI, you cannot modify or run it on this page. Go to the original application to modify the policy definition.
- **PENDING ALERTS** - indicates the presence of pending alerts on a policy job. To view the alerts on a policy job, select **Yes** to expand the alert in the **Alerts** table. The following alerts contribute to this status:
 - **Infection Found**
 - **YARA Ruleset Match**

- **Malware File Detected**
- **Threshold Exceeded**
- **Database Corruption**
- **POLICY TYPE** - displays the type of storage connector used when the policy was created.
- **PHASE** - the phase that a running policy job is currently in. See [Policy job phases \(on page 72\)](#) for the list of phases.
- **START TIME** - displays the time and date stamp of when the policy was last executed.
- **TOTAL DURATION** - the total time of a policy job. If the job is currently running, then it will show the time that has lapsed since the start of the job.
- **ACTIONS** - the available actions at this time are:



Note: If the policy was made before release 8.8.0 or in a third-party application, it cannot be edited or run in the Ransomware Detection UI. These icons will be grayed out and not selectable.

Action Icon	Description
	View the log of jobs for the selected policy.

Select **Log** on the **Policies** page to see the log of all completed jobs for the selected policy; see [Log \(on page 68\)](#) for more information.

The Policy Editor

Use the **Policy Editor** to create policy definitions to perform disk volume snapshot indexing on Hitachi Vantara enterprise class storage arrays. The Hitachi Vantara storage platform offers several classes of products, from small to large block storage arrays. The policy definition includes various attributes of a policy, such as a target host, and an optional schedule when the policy will be run. The policy is then used to run a job which scans snapshots of a single volume or multiple volumes in a consistency group. Create a new policy using the Hitachi Virtual Storage Platform (VSP) storage connector:

- **Hitachi VSP** - defines the storage information for a VSP. The Hitachi VSP storage connector has two options:
 - **Block** - a block device format for the storage connector.
 - **VMFS** - a VMFS option for the storage connector.

Each policy must have a unique name, specify the Hitachi VSP storage connector type, and list the volume(s) where the data is stored.

Creating a VMFS-based HVSP policy

Use VMFS policies to index and analyze VMware VMFS datastore volumes.

**Note:**

Before creating a policy, ensure that all required volumes from the Hitachi One Block (B24) or VSP 5000 series are properly mapped to the CyberSense server via either Fibre Channel (FC) or iSCSI.

For FC: Host group must be created and visible from CyberSense.

For iSCSI: iSCSI initiator must be configured and visible on the storage system.

Failure to configure volume mapping will result in errors during policy creation.

To create a new VMFS-based policy using the Hitachi VSP storage connector to scan the storage array:



Note: Required fields are indicated by *.



Note: Before creating a policy, configure the iSCSI connections.



Note: Contact your Hitachi Storage administrator for any required IDs or other information before you start this procedure.

1. On the **Policies** page, select **Create New Policy**.
2. In the **Policy Details** pane, specify the following:
 - **Policy Name** - type a unique name for the new policy.



Note: Leading and trailing spaces in a policy name are deleted when the policy is saved.

- **Email Notifications** - type the email address(es) that should receive alert notifications. Press **Enter** after each email address.

Select **Next**.

3. In the **Configure Storage Connector** pane, select **Hitachi Virtual Storage Platform** as the storage connector platform. Select **Next**.
4. In the next **Configure Storage Connector** pane, fill in the following fields:
 - In **Hitachi Virtual Storage Platform Hostname or IP address**, type the IP address or the hostname for the Hitachi Virtual Storage Platform Controller. Select **Next**.
 - Add the Hitachi administrator **Username *** and **Password ***. If the certificate is unverifiable, select whether or not to **Trust Unverifiable Certificate** by enabling or disabling the option.



Note: If you have previously accessed the Hitachi Storage Array, you will not be prompted to enter your credentials.

- In **Job Type**, select **VMFS** as the storage type that is used on the host. Select **Next**.
- In **Connection Option**, select the appropriate option for the connection between the Ransomware Detection server and the Hitachi storage array:
 - **Fiber Channel** - select if the connection is Fiber Channel.
 - **iSCSI** - select if the connection uses existing Ethernet infrastructure.



Note: When the Ransomware Detection server is deployed as a VM, **Fibre Channel** connectivity is not supported. Always use the **iSCSI** connection option.

Select **Next**.

- In **CyberSense Server Hostgroup Name**, select the name of the Ransomware Detection server hostgroup on the VSP array.
- In **Production Hostgroup Name**, select the appropriate hostgroup. Select **Next**.
- In **Primary Volume**, select at least one primary volume assigned to the selected hostgroup.
- In **SECONDARY VOLUME(S) ID *** for each primary volume in **PRIMARY VOLUME(S) ID ***, enter the secondary volume ID to be associated with the selected primary volume(s). Select **Next**.
- Set the **Safe Snap Retention Period** to a specific number of hours or days in which to make the snapshot immutable.



Important: Set the **Safe Snap Retention Period** to no less than 8 hours minimum.

- In **Extended Retention Period**, set the number of days to extend the retention of a snapshot.
- In **Datastore UUID**, enter the UUID of the datastore. The Datastore UUID is found on the ESXi host UI or vSphere UI.
- In **CCI Instance Number**, type the Ransomware Detection server's HORCM-configured Command Control Interface (CCI) instance number to communicate with the storage array. Select **Next**.

Select **Next**.

5. In the **Configure Policy** pane, specify the following:
 - **Only scan files or paths that match these patterns** - specify the folders and/or files to be included in the scan. Use glob expressions to filter the list. By default, all files are included. After typing in the files/directories or glob expression, press **Enter** to save the changes. Add more if needed. See [Using filters to specify paths and files \(on page 63\)](#) for more information.
 - **Only scan files or paths that match these patterns** - specify the folders and/or files to be excluded in the scan. Use glob expressions to filter the list. By default, all files are excluded. After typing in the files/directories or glob expression, press **Enter** to save the changes. Add more if needed. See [Using filters to specify paths and files \(on page 63\)](#) for more information.
 - In **Virtual Machines**, add rules to include or exclude specific VMs from scanning. Enter the following information:



Note: If you do not add a VM, then all the VMs will be scanned.

- In **Datastore UUID (optional)**, type the UUID of the datastore.
- In **Scan Rule**, select **Include in Scan** or **Exclude from Scan** to include or exclude the VM from the scan.
- In **Virtual Machine ID**, select **Name** or **UUID** to find the virtual machine by the name or the UUID.
- In **Virtual Machine Name/UUID**, add the name or UUID of the virtual machine.

Select **Next**.

6. In the **Schedule** pane, create a schedule to run the policy at the specified time and frequency. Enable scheduling to run the policy by toggling **Schedule Policy**. Enter the following **Frequency** information:
 - **Hourly** and set the number of minutes past the hour that the policy will run.
 - **Daily** and select on which day of the week and set the hour at which the policy will run.

Select **Next**. When finished, select **Create New Policy** to save the new policy definition.

7. In the **Review and Create** pane, review the policy configuration. When finished, select **Create New Policy** to save the new policy definition.

Creating a block-based HVSP policy

Create block-based policies to index and analyze data on a volume or volumes that are block-based and not VMware VMFS datastores.



Note:

Before creating a policy, ensure that all required volumes from the Hitachi One Block (B24) or VSP 5000 series are properly mapped to the CyberSense server via either Fibre Channel (FC) or iSCSI.

For FC: Host group must be created and visible from CyberSense.

For iSCSI: iSCSI initiator must be configured and visible on the storage system.

Failure to configure volume mapping will result in errors during policy creation.

To create a new block-based policy using the Hitachi VSP storage connector to scan the storage array:



Note: Required fields are indicated by *.



Note: Before creating a policy, configure the iSCSI connections.



Note: Contact your Hitachi Storage administrator for any required IDs or other information before you start this procedure.

1. On the **Policies** page, select **Create New Policy**.
2. In the **Policy Details** pane, specify the following:
 - **Policy Name**, type a unique name for the new policy.



Note: Leading and trailing spaces in a policy name are deleted when the policy is saved.

- **Email Notifications (optional)** - type the email address(es) that should receive alert notifications. Press **Enter** after each email address.

Select **Next**.

3. In the **Configure Storage Connector** pane, select **Hitachi Virtual Storage Platform** as the storage connector platform from the **Storage Connector** list. Select **Next**.
4. In the next **Configure Storage Connector** pane, fill in the following fields:

- In **Hitachi Virtual Storage Platform Hostname or IP address**, type the IP address or the hostname for the Hitachi Virtual Storage Platform Controller. Select **Next**.
- Add the Hitachi administrator **Username *** and **Password ***. If the certificate is unverifiable, select whether or not to **Trust Unverifiable Certificate** by enabling or disabling the option.



Note: If you have previously accessed the Hitachi Storage Array, you will not be prompted to enter your credentials.

- In **Job Type**, select **Block** as the type of storage used on the host. Select **Next**.
- In **Connection Option**, select the appropriate option for the connection between the Ransomware Detection server and the Hitachi storage array:
 - **Fiber Channel** - select if the connection is Fiber Channel.
 - **iSCSI** - select if the connection uses existing Ethernet infrastructure.



Note: When the Ransomware Detection server is deployed as a VM, **Fibre Channel** connectivity is not supported. Always use the **iSCSI** connection option.

Select **Next**.

- In **Ransomware Detection Server Hostgroup Name**, select the name of the Ransomware Detection server hostgroup on the VSP array.
- In **Production Hostgroup Name**, select the appropriate hostgroup(s). Select **Next**.
- In **Primary Volume**, select at least one primary volume assigned to the selected hostgroup.
- For each primary volume in **PRIMARY VOLUME(S) ID**, enter the secondary volume ID to be associated with the selected primary volume in **SECONDARY VOLUME(S) ID**. Select **Next**.
- Set the **Safe Snap Retention Period** to a specific number of hours or days in which to make the snapshot immutable.



Important: Set the **Safe Snap Retention Period** to no less than 8 hours minimum.

- In **Extended Retention Period**, set the number of days to extend the retention of a snapshot.

Select **Next**.

5. In the **Configure Policy** pane, specify the following:

- **Only scan files or paths that match these patterns (optional)** - specify the folders and/or files to be included in the scan. Use glob expressions to filter the list. By default, all files are included. After typing in the files/directories or glob expression, press **Enter** to save the changes. Add more if needed. See [Using filters to specify paths and files \(on page 63\)](#) for more information.
- **Only scan files or paths that match these patterns (optional)** - specify the folders and/or files to be excluded in the scan. Use glob expressions to filter the list. By default, all files are excluded.

After typing in the files/directories or glob expression, press **Enter** to save the changes. Add more if needed. See [Using filters to specify paths and files \(on page 63\)](#) for more information.

- **Original Data Location** - specify the `hostname/path` to the source data location. The `hostname` is the original server hostname on which the data is found and `path` is the original directory where the data is located on the host.

Select **Next**.

6. In the **Schedule** pane, create a schedule to run the policy at the specified time and frequency. Enable scheduling to run the policy by toggling **Schedule Policy**. Enter the following **Frequency** information:
 - **Hourly** and set the number of minutes past the hour that the policy will run.
 - **Daily** and select on which day of the week and set the hour at which the policy will run.

Select **Next**. When finished, select **Create New Policy** to save the new policy definition.

7. In the **Review and Create** pane, review the policy configuration. When finished, select **Create New Policy** to save the new policy definition.

Editing a policy

To edit a policy:


1. On the **Policies** page, select the **Edit** icon under **ACTIONS**.
2. On the **Policy** editing page, change the following:
 - **Policy Name** - the policy name must be unique.
 - **Email Notifications** - add or remove email addresses that will receive notifications when a policy job is run.
 - **Only scan files or paths that match these patterns** - add or remove files and/or directories to include when a policy is run. Type the file/directory names or the glob expressions and press **Enter** to save the entry. Add multiple entries if needed. See [Using filters to specify paths and files \(on page 63\)](#) for more information.
 - **Do not scan files or paths that match these patterns** - add or remove files and/or directories to include when a policy is run. Type the file/directory names or the glob expressions and press **Enter** to save the entry. Add multiple entries if needed. See [Using filters to specify paths and files \(on page 63\)](#) for more information.
 - **Storage Connector information** - select the **Edit** icon to change the parameters specific to the storage connector.
 - **Schedule** - modify the schedule for running the policy.
3. When finished, select **Save Changes**.

Deleting a policy

When you delete a policy, you can no longer access or review it. If an alert has generated when you ran the deleted policy, the policy name is changed to reflect when the policy was deleted.

To delete a policy:

1. On the **Policies** page, select a policy and then select the **Edit** icon under **ACTIONS**.
2. On the **Policies > Edit** page, select **Delete** and when prompted, select **Yes, Permanently Delete This Policy** to permanently delete the policy.

 **Important:** This action will permanently delete the policy and you can no longer view or restore the policy.

Using filters to specify paths and files

When creating or editing a policy, you have the option to specify paths and/or files that you wish to include or exclude from being scanned during an indexing job. The include filter is specified by the **Only scan files or paths that match these patterns** field in the policy. The exclude filter is specified by the **Do not scan files or paths that match these patterns** field in the policy. By default, all files and folders are scanned unless otherwise excluded by a filter.

You can specify **Only scan...** and **Do not scan...** filters (relative to the directory source) when you create or edit a policy. For example, if you do not want to include a folder named **Old-Users** in the directory source to be scanned, you can list the folder name in the **Do not scan...** field as follows.

As a result, everything in the parent folder is included when the policy is run except the **Old-Users** folder. To exclude multiple folders, press **Enter** after each specific exclusion.

On the other hand, to index only the **Old-Users** folder and nothing else, list it in the **Only scan...** field.

Tips to keep in mind

When specifying filters, note:

- Use wildcard patterns to specify files and subfolders for inclusion or exclusion during indexing. As mentioned above, pattern matching starts at the beginning of a path that is relative to the root directory of the volume(s) used for indexing and continues to the end of the path. Therefore, leading and trailing wildcards are significant. A pattern that matches a folder implicitly matches all of the folder's content.
- If only **Only scan...** filters are specified, every file is included except those items that match the include patterns. Any number of filters can be added to the field.
- If only **Do not scan...** filters are specified, every file is included except those items that match the exclude patterns. Any number of filters can be added to the field.
- If both **Only scan...** and **Do not scan...** filters are supplied, then **Only scan...** filters are applied first, and then the **Do not scan...** patterns are applied to the resulting included content.

- Do not specify the same paths and/or files in the **Only scan...** and **Do not scan...** filter fields. If a file matches both the **Only scan...** and **Do not scan...** patterns, it will be excluded.
- If either pattern matches a folder, it applies to all contents of the folder. When matching a folder, it does not matter if the pattern ends with a path separator or not; a folder can match either way.
- Multiple patterns can be entered by pressing **Enter** and then adding the additional patterns. Simple wildcards are supported:
 - * matches none or any number of characters (including path separators)
 - ? matches any single character (including path separators)
- All other characters match themselves, including white space, punctuation, and path separators.
- Alphabetic characters are case-sensitive.
- Leading path separators are not required and are ignored.
- A sequence of multiple path separators is the same as a single separator.
- Patterns consisting of nothing but a single * or a single path separator are equivalent, and match everything.
- If a pattern must include wildcards as a character in a folder component or filename, they must be escaped by backslash, for example: \`*` and \`?`.

Usage

To use the **Only scan...** and **Do not scan...** filters effectively, be sure that you understand the terminology used in all of the examples that follow. The key terms are listed below.

Root Directory

The root directory of the volume(s) defined in the policy.

Top-level Folder

A first-level folder under the **Root Directory**.

Subfolder

A folder at any level under the **Top-level Folder**.

Important:

The examples that follow include two patterns under each heading. The first pattern ends with a forward slash ("/") delimiter; the second does not.

- Use the trailing forward slash when you want to include or exclude only the folders that you specify and their contents.
- Omit the trailing delimiter when you want to include or exclude both folders and files of the given name.

Examples

The examples that follow demonstrate proper syntax usage when specifying folders and/or files for inclusion in or exclusion from an indexing job.

Matching top-level folders (or top-level folders and files) with a given name in the directory source

To match a top-level folder named `FolderName` in the root directory folder, specify the folder name followed by a trailing `/`:

```
FolderName/
```

To match a top-level folder or files named `Entry1` in the root directory, specify only the file/folder name:

```
Entry1
```

Matching subfolders (or files and folders) with a given name under a top-level folder

To match a subfolder `Subfolder1` of a top-level folder named `FolderName`, specify the folder names separated by `/` and end with a trailing `/`:

```
FolderName/Subfolder1/
```

To match a file or subfolder named `Entry1` of a top-level folder named `FolderName`, do not use a trailing `/`:

```
FolderName/Entry1
```

Matching folders (or files and folders) with a given name in a subfolder on any level under a top-level folder

To match subfolder `FolderName` on any level under a top-level folder:

```
*/FolderName/
```

To match files and subfolders named `Entry1` on any level under a top-level folder:

```
*/Entry1
```

Matching both top-level folders and subfolders (or files and folders) on any level

To match folders named `FolderName` on any level, you must define two patterns. The first line matches a top-level folder named `FolderName`; the second line matches all subfolders named `SubFolderName` on any level under any top-level folder:

```
FolderName/
```

`*/SubFolderName/`

Likewise, to match all files and folders named `Entry1` on any level, you must define two patterns:

`Entry1`

`*/Entry1`

Matching folders and files with a given substring in a name on any level

To match files or folders on any level containing the substring `Substring1` anywhere in the name:

`*Substring1*`

To match folders on any level whose names begin with the substring `Substring1`, define two patterns:

`Substring1*/`

`*/Substring1*/`

To match files and folders on any level whose names begin with the substring `Substring1`, define two patterns:

`Substring1*`

`*/Substring1*`

To match folders on any level whose names end with the substring "Substring1":

```
*Substring1/
```

To match files and folders on any level whose names end with the substring `Substring1`:

`*Substring1`

To match file and folder paths on any level containing the substrings `Substring1` and `Substring2`:

`*Substring1*Substring2*`

For example, listing `*finance*budget*` in the **Exclude** filter prevents indexing files such as `finance dept \january budget.xls`.

Matching with both *Only scan* and *Do not scan* filters

When using both the **Only scan...** and **Do not scan...** filters for scanning paths and files, keep in mind that the **Do not scan...** filter takes precedence over the **Only scan...** filter results. Take a look at the following examples:

To match a file or folder named `/abc` and `/def` except for a file or subfolder named `/abc/123`, specify:

- **Only scan...:** `/abc /def`
- **Do not scan...:** `/abc/123`

If you specify the following :

- **Only scan...**: /abc /def
- **Do not scan...**: /def

All files and subfolders in /abc are included but the file and subfolders in /def will be excluded. The files and subfolders in /def match both the **Only scan...** pattern and the **Do not scan...** pattern and so will be excluded.

To match a file or folder named /abc and exclude a file or folder named /def, specify:

- **Only scan...**: /abc
- **Do not scan...**: /def

If you specify:

- **Only scan...** is set to: /abc
- **Do not scan...** is set to: /abc/*

This matches to a file named /abc but excludes all files and subfolders under the folder named /abc.

Log

The **Policies > Log** page displays a history of completed jobs. If you select a job that has generated an alert, you will see them listed in the **Associated Alerts** table below. Expand a policy job in the **Log** table to review the phase information of the policy job and workload details; see [Viewing policy information \(on page 73\)](#) for more details.

Log
Policies > Log

Filters Export

STATUS	JOB ID	START TIME	TOTAL DURATION	POLICY	POLICY TYPE
Done	27	2025-07-18 09:21:27	00:01:27	cs_policy_local	Local
Done	26	2025-07-18 09:19:02	00:01:34	cs_policy_local	Local
Done	25	2025-07-18 08:23:26	00:01:33	cs_policy_local	Local
Done	24	2025-07-17 16:46:24	00:01:51	cs_policy_local	Local
Alert	23	2025-07-17 16:41:29	00:02:08	cs_policy_local	Local

Expanded Job 23 Details:

PHASE	DURATION	WORKLOAD COMPLETED	COUNT
Initializing	00:00:05	IEAPI Unix FS	1
Scanning	00:00:01		
Indexing	00:00:44		
Postprocessing	00:01:02		
Generating Statistics	00:00:01		
Analyzing Statistics	00:00:03		

Rows per page: 10 | Page 1 of 3 | 1

Associated Alerts Selected Job: 23
Select an alert to see more details in the Alerts page.

SEVERITY	TYPE	BACKUP TIME	ALERT TIME	STATUS	HOST
Critical	Database Corruption	2025-07-17 16:41:34	2025-07-17 16:43:25	Pending	nj-colo-jovalle-rhel92-vm2.test.indexengines.com

The **Log** table lists the following details:

- the **STATUS** of a job, which can be:

Status	Description
Alert	An alert has been generated when the policy was run.
Partial	The Ransomware Detection job has completed with errors. The job completed with errors and could not scan some files. This usually relates to access denial errors such as limited permissions.
Done	The Ransomware Detection job has finished successfully and did not encounter any errors, such as access or security errors.
Failed	The Ransomware Detection job has failed. Job failure may be due to configuration errors or connectivity problems between Ransomware Detection and the source

Status	Description
	of the data being indexed, or if the system reaches the retry limit of five retries. An indexing job may also fail if the credentials used to mount the share do not have adequate permissions. A subsequent run of a Failed job may change to Done or Partial status if you re-run the job after the issue is resolved.
Canceled	The Ransomware Detection job was canceled by the user after it started.
Suspended	The Ransomware Detection job was suspended.

- the **JOB ID**



Note: When a malware alert is generated from a custom signature, the **Job ID** is the job during which the file was first indexed. When a change is made in the malware signature database, all future indexing jobs and previously indexed files are checked against the updated malware signature database.

- the **START TIME** of the job
- the **TOTAL DURATION** of the job
- the **POLICY** name

Select a policy job in the **Log** table to display the job details in a pop-out window and any associated alerts are listed in a table below the **Log** table. Use the **Filters** to return more relevant results. The filter can be based on any of the column headings.

Policy job details

When you select a job in the **Log** table, the details for the selected job are displayed in a side bar.

The details vary depending on the type of storage connector used to create a policy. In general, the detail groupings are similar to those listed below. Only properties used by the policy job are displayed.

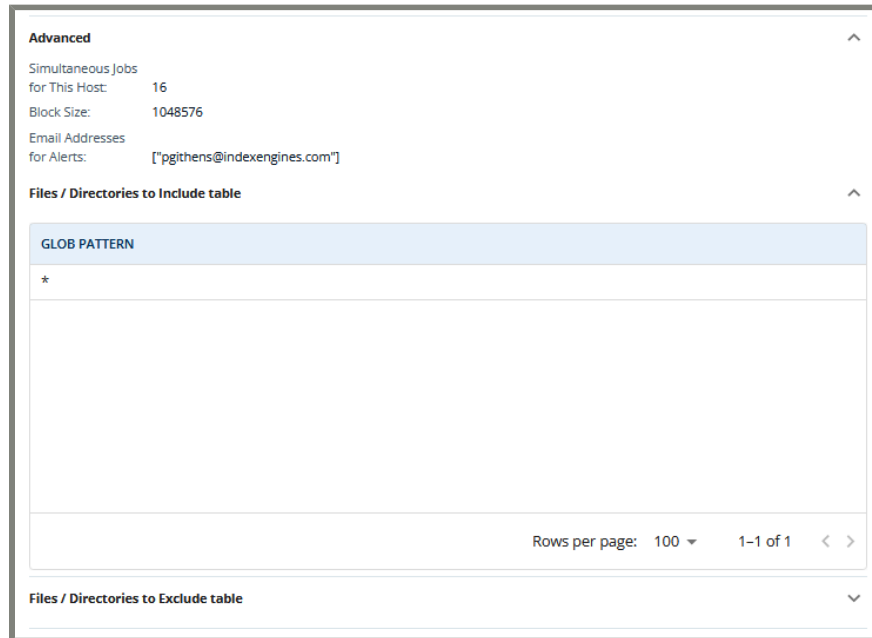
Job Definition

This section lists details about the job type and data location

- **Job Type** - lists the type of job which is always incremental for snapshots of primary storage.

Advanced

This section lists advanced settings for the job:



- **Simultaneous Jobs for This Host** - The number of simultaneous jobs that can run on this host.
- **Email Addresses for Alerts**: The email addresses that will receive the Ransomware Detection Analytics report emails.
- **Files/Directories to Include table** - Lists the files or directories that were included in the job.
- **Files/Directories to Exclude table** - Lists the files or directories that were excluded from the job.

Indexing Service Options

This section lists the options for indexing set at the time the job was run.

- **Indexing Mode** - Indicates which mode the indexing process uses.
 - **Full Content** - indexes all metadata plus the content of supported file types.
 - **Metadata with MD5 Hash** - indexes metadata only but captures the MD5 Hash file signature and file type.
 - **Metadata** - The same as the above mode except for CIFS and NFS file server data where MD5 hash values are not computed.
- **Case Handling** - Indicates how the case of keywords within documents and their metadata are handled in any indexing mode.
 - **Preserve Case** - Preserve the original case of the keywords.
 - **Map to Lowercase** - Map all upper case letters to lower case.
- **OCR** - The Optical Character Recognition (OCR) setting is disabled by default and requires an OCR license.

-
- **Ransomware Detection Data Collection** - Enables Ransomware Detection analysis processing. This requires a Ransomware Detection license.
 - **User Change Time for Incremental Indexing** - Controls whether modifications to a file's **Change Time** results in the file being indexed during the execution of the job

Job Properties

This section lists additional job properties when the job has completed.

- **Status Message**: Indicates whether or not the job completed and if an infection was found.
- **New Snapshot Groups Analyzed**: The number of new snapshot groups analyzed during the Ransomware Detection Analysis process.
- **New Snapshots Analyzed**: The number of new snapshots analyzed during the Ransomware Detection Analysis process.
- **New Infections Found**: The number of new malware infections were found during the Ransomware Detection Analysis process.
- **Total Bytes**: The total number of bytes analyzed during the Ransomware Detection Analysis.

Job Exceptions

This section will display any exceptions that occurred during the policy job.

Associated Alert table

When you select the **Alert** status chip in the policy's **Log** table, the **Associated Alerts** table is displayed below the **Log** table. Select an alert to go to the **Alerts** page for more information about the alert.

The **Associated Alerts** table lists the following information:

- the **SEVERITY** of the alert. See the [Alert severity \(on page 18\)](#) description for more details.
- the **TYPE** of alert. See the [Alert types \(on page 18\)](#) table
- the **SNAPSHOT TIME** is the date and time that the snapshot was created.
- the **ALERT TIME** is the date and time when the alert last occurred.
- the **STATUS** of the alert, which is either **Pending** or **Cleared**, which indicates that the alert was cleared.
- the **HOST** is the target host on which the alert occurred.
- the **SNAPSHOT ID** is the snapshot ID in which the alert was generated.

Policy job phases

The different phases that a policy job can be in are listed below.

Status	Description
Initializing	The policy job has successfully mounted the volume or checked the local file system and is ready to scan the content.
Scanning	The policy job has begun scanning the specified location for files and directory content that should be indexed. This includes finding files that have not be scanned yet. The duration depends on the number of files to be scanned.
Scanning & Indexing	The Scanning and Indexing job phases may overlap when the scanning process is still in process and the indexing process begins.
Indexing	The eligible data in the specified location are processed and indexed. Ransomware Detection adds file metadata needed for analysis to the index segment. The duration depends on the number of files that are to be scanned.
Post-Processing	The policy job is optimizing the index segments. The duration depends on the number and size of the index segments.
Generating Statistics	This phase indicates that Ransomware Detection has begun generating statistics for analysis. The duration depends on the number of new directories and files in those snapshots.
Analyzing Statistics	Ransomware Detection has begun to analyze the content and compare it to previous snapshots. This process determines if a potential malware attack has taken place.
Canceling	Indicates that the policy job has been canceled before it was completed.

Viewing policy information

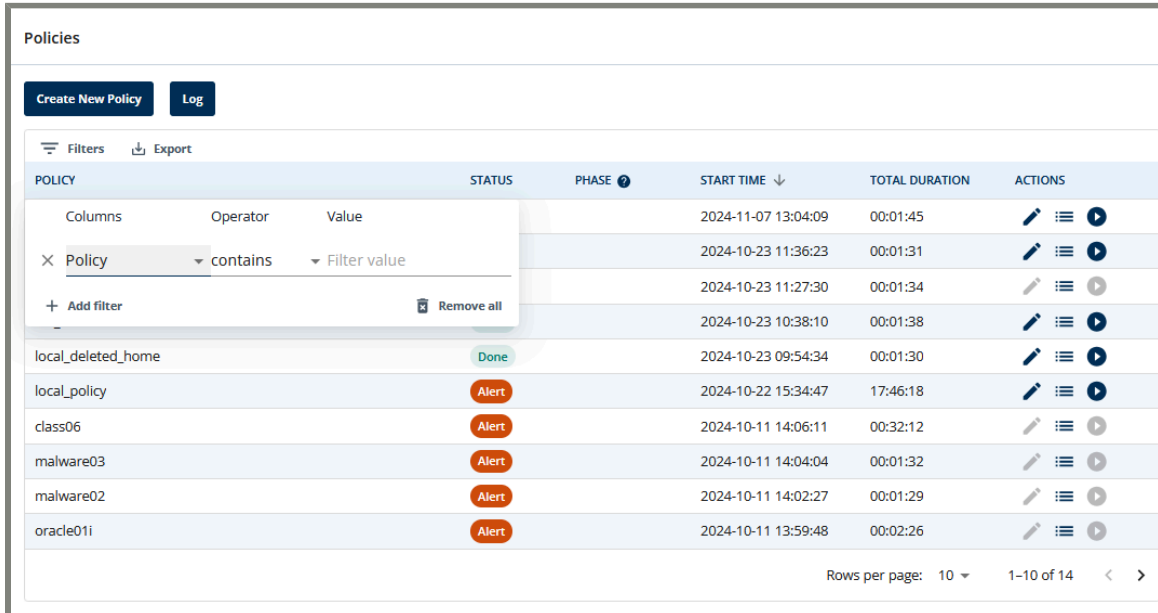
When a policy is running and indexing the specified files, view the phases and time duration as well as additional statistics by expanding a selected policy row. The row can be left open to watch the indexing phases as they are completed.

The displayed information is as follows:

Column	Description
PHASE	<p>The policy phase, which can be:</p> <ul style="list-style-type: none"> • Initializing • Scanning • Scanning & Indexing • Indexing • Post-processing • Generating Statistics • Analyzing Statistics • Canceling <p>See Policy job phases (on page 72) for more details.</p>
DURATION	The length of time that each completed phase took to complete.
WORKLOAD COMPLETED	Indicates the data type that is being scanned.
COUNT	Displays the count of items that have been scanned.
HOST IN PROGRESS	Indicates the host that is currently being scanned. This data is displayed only when a policy is scanning or indexing.
DATASET IN PROGRESS	Indicates the dataset that is currently being scanned. This data is displayed only when a policy is scanning or indexing.
TYPE	Lists the data type as a description of the dataset currently being scanned. This data is displayed only when a policy is scanning or indexing.
DURATION	Displays the duration of the scanning/indexing process on a dataset in HH:MM:SS. This data is displayed only when a policy is scanning or indexing.
ID	The policy job ID.

Filtering the Policies and Log tables

Filter the **Policies** and **Log** tables by the columns using the operators that are described below. Select the column label to sort the column's contents in ascending or descending order.



The following columns use filters and filter operators::

Column	Available operators	Values
STATUS	<ul style="list-style-type: none"> • is • is any of 	<p>Some values are only valid for the Policies table and are marked with *.</p> <ul style="list-style-type: none"> • Idle * • Pending * • Running * • Done • Failed • Partial • Canceling * • Canceled • Alert • Suspended • Suspending *

Column	Available operators	Values
POLICY	<ul style="list-style-type: none"> • contains • equals • starts with • ends with • is any of 	Type the value to use as a pattern to match in the name of a policy.
POLICY TYPE	<ul style="list-style-type: none"> • is • is any of 	Select the storage connector used when creating a policy.
PHASE <i>Only valid for the Policies table.</i>	<ul style="list-style-type: none"> • is • is any of 	<ul style="list-style-type: none"> • Initializing • Scanning • Scanning & Indexing • Indexing • Postprocessing • Generating Statistics • Analyzing Statistics • Canceling • Suspending
START TIME	<ul style="list-style-type: none"> • is • is after • is before • between 	Type or select the date on which the policy job started.
TOTAL DURATION	<ul style="list-style-type: none"> • = • > • < 	Type the length of time for the total duration of the policy job.
JOB ID <i>Only in Log table.</i>	<ul style="list-style-type: none"> • = • != • > • => • < 	Type the job ID on which to filter the Log table.

Column	Available operators	Values
	<ul style="list-style-type: none"> • <= • is any of 	

Each column has a list of operators that can be used on the contents of the table. Use the formats as specified in the examples.

Operator	Description	Example
contains	Find items that contain at least the characters entered in the Value field. Use with POLICY .	<p>Column: POLICY</p> <p>Value: policy</p> <p>Results: any Policy name that contains "policy"</p> <ul style="list-style-type: none"> • 06policy • policy06 • nfs-policy-54
equals	Find items that contain exactly the characters entered in the Value field. Use with: <ul style="list-style-type: none"> • POLICY • TOTAL DURATION 	<p>Column: POLICY</p> <p>Value: policy06</p> <p>Results: any Policy name that equals exactly "policy06"</p> <ul style="list-style-type: none"> • 06policy is not found • policy06 is found
starts with	Find items that start with the characters specified in the Value field. Use with POLICY .	<p>Column: POLICY</p> <p>Value: policy</p> <p>Results: any Policy name that starts with "policy"</p> <ul style="list-style-type: none"> • 06policy is not found • policy06 is found • nfs-policy-54 is not found
ends with	Find items that end with the characters specified in the Value field. Use with POLICY .	<p>Column: POLICY</p> <p>Value: policy</p>

Operator	Description	Example
		<p>Results: any Policy name that ends with "policy"</p> <ul style="list-style-type: none"> • 06policy is found • policy06 is not found • nfs-policy-54 is not found
is	<p>Select a single item from the fixed drop-down list. Use with:</p> <ul style="list-style-type: none"> • STATUS • PHASE • POLICY TYPE 	<p>Column: STATUS</p> <p>Value: Idle</p> <p>Results: any Policy job with the status of Idle</p>
is any of	<p>Select one or more items from a drop-down list or type the exact name of a policy. Use with:</p> <ul style="list-style-type: none"> • POLICY • STATUS • PHASE • POLICY TYPE 	<p>Column: STATUS</p> <p>Value: Idle, Done</p> <p>Results: any policy job with the status of Idle or Done.</p>
is after	<p>Find policy jobs with a start time after the date specified in the Value field. Select a date using the date picker. Use with START TIME.</p>	<p>Column: START TIME</p> <p>Value: 01/01/2025</p> <p>Results: any policy job with a start time after January 1, 2025.</p>
is before	<p>Find policy jobs with a start time before the date specified in the Value field. Select a date using the date picker. Use with START TIME.</p>	<p>Column: START TIME</p> <p>Value: 01/01/2025</p> <p>Results: any policy job with a start time before January 1, 2025.</p>
between	<p>Find policy jobs with a start time between the dates specified in the Value field. Select both dates using the date picker. Use with START TIME.</p>	<p>Column: START TIME</p> <p>Value: 01/01/2024-01/01/2025</p>

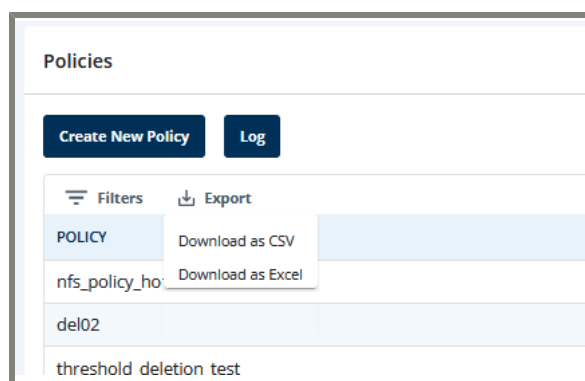
Operator	Description	Example
		<p>Results: any policy job with a start time between the dates January 1, 2024 and January 1, 2025, exclusively.</p>
>	<p>Find policy jobs with a duration time greater than the value specified in the Value field. Use with TOTAL DURATION.</p>	<p>Column: TOTAL DURATION</p> <p>Value: 00:02:30</p> <p>Results: any policy job with a duration time greater than 0 hours, 2 minutes, and 30 seconds.</p>
<	<p>Find policy jobs with a duration time less than the value specified in the Value field. Use with TOTAL DURATION.</p>	<p>Column: TOTAL DURATION</p> <p>Value: 14:02:30</p> <p>Results: any policy job with a duration time less than 14 hours, 2 minutes, and 30 seconds.</p>
=	<p>Find policy jobs with a duration time equal to the value specified in the Value field. Use with TOTAL DURATION.</p>	<p>Column: TOTAL DURATION</p> <p>Value: 14:02:30</p> <p>Results: any policy job with a duration time equal to 14 hours, 2 minutes, and 30 seconds.</p>

Exporting a Policy or Log report

Export the list of policies to a CSV file, Excel spreadsheet, or a PDF printout. The Policies report is useful to review what policies have been created, as well as the status, the start time, and total duration of the last job run using a policy.

On the **Policies** page, select **Export** and then select one of the following:

- **Download as CSV** - downloads a CSV file of the policies.
- **Download as Excel** - downloads an Excel spreadsheet of the policies.



Access the downloaded file from the browser **Downloads** option.

The **Policy** report contains the following information:

Column	Description
Status	The status of the last job that used the policy.
Policy	The name of the policy.
Policy Type	The type of storage connector on which the policy was based.
Phase	The phase of the last job that used the policy.
Start Time	The start time of the last job that used the policy.
Total Duration	The total time of the last job that used the policy.

The **Log** report contains the following information:

Column	Description
Status	The status of the last job that used the policy.
Job ID	The ID of the policy job.
Start Time	The start time of the last job that used the policy.

Column	Description
Total Duration	The total time of the last job that used the policy.
Policy	The name of the policy.
Policy Type	The type of storage connector on which the policy was based.

Chapter 7. Configuring Ransomware Detection settings

The **Settings** page displays the index storage settings and the **Settings** navigation menu, from which various system and administration settings can be configured.

Configure system settings using the **Settings** navigation menu. From this menu, you can configure user accounts, set alert email notifications and upload a new malware signature file, modify login and network security options, and define advanced settings such as alert thresholds.

The **Settings** page is persistent; if you go to the **Alerts** page and then back to the **Settings** page, you will land on the last menu item you visited on the **Settings** page.

From the **Settings** navigation menu, access the following:

- [Storage menu \(on page 82\)](#) - configure settings related to index storage.
- [User Management menu \(on page 85\)](#) - add or edit user accounts and configure role privileges.
- [Alerts menu \(on page 95\)](#) - upload a new malware signature database or set emails for alert notifications.
- [Network and Security menu \(on page 104\)](#) - configure system settings related to security and analytics reporting.
- [License Management menu \(on page 114\)](#) - view the license status, license details, and the EULA that was signed during the installation process.
- [Advanced menu \(on page 126\)](#) - add custom alert thresholds, configure custom YARA rulesets, and recover files from a restored snapshot.

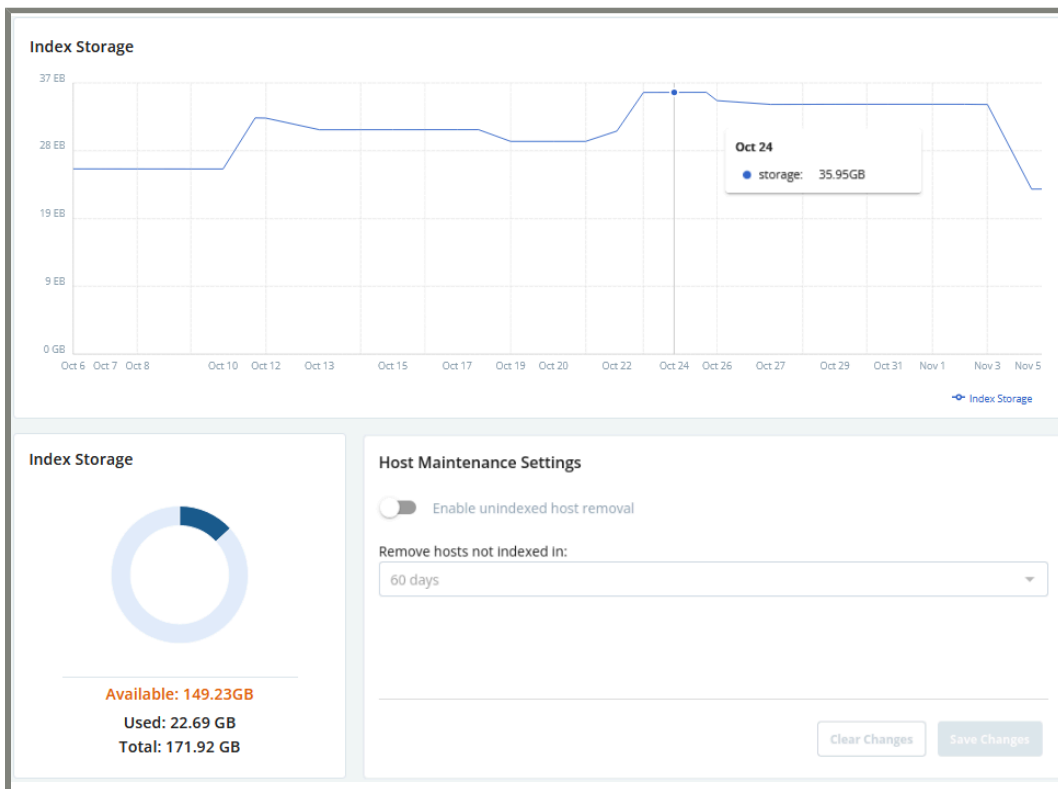
Storage menu

The following settings can be viewed and modified from the **Storage** page:

- [Index Storage \(on page 82\)](#) - shows the amount of storage that has been used and total storage allocated to the index created from Ransomware Detection jobs over time as well as current index configuration settings.

Index Storage

Select **Settings > Storage > Index Storage** to view the graphical representation of the storage used by the indexing jobs, review available storage, and configure host maintenance settings.



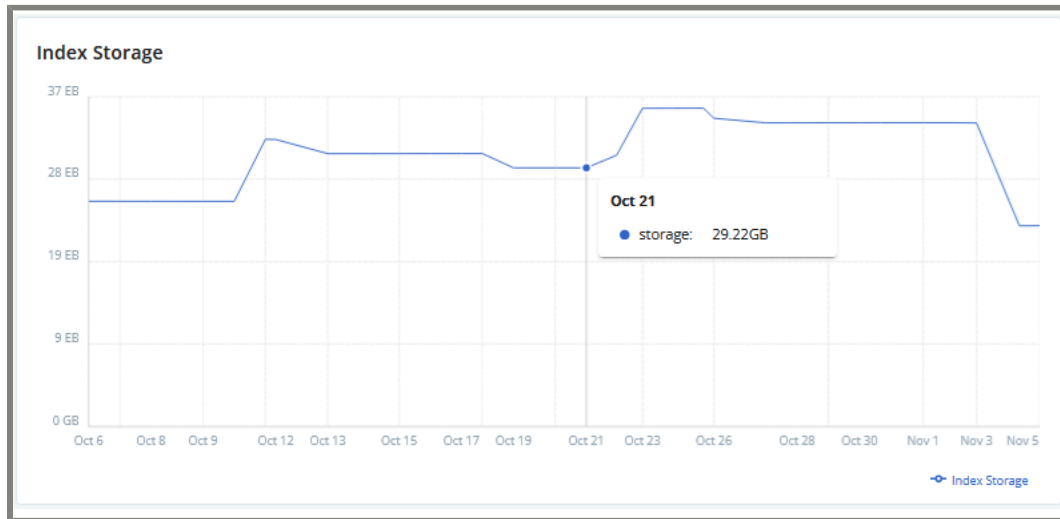
When a host is scanned by a policy, Ransomware Detection organizes the data in the index into segments. Each segment contains information about the host and the files that were scanned. An index can contain a large number of segments, which after a period of time, may no longer be needed. The following is used by the **Host Maintenance Settings** to reduce the amount of storage used by an index:

- **Enable unindexed hosts removal** - When enabled, this process performs a daily check for any new snapshots within the specified number of days for a known host, which has had previous snapshots analyzed, and, if newer snapshots do not exist, removes that host and all related data from the index. This

may happen if a host was scanned but later decommissioned, eliminating the need for further scans. In this case, the host data is still in the index but is old and no longer relevant and should be removed. Set this process to remove unindexed hosts every 30 - 90 days.

Index storage details

The graph displays the index storage usage. Hover over the usage line to see how much storage is used for a particular date.



Configuring the host maintenance settings

Configure the host maintenance settings from the original values in the **Host Maintenance** pane. Enable or disable unindexed host removal, and when enabled, set how long to retain unindexed hosts in an index

To edit the index maintenance settings:

1. Go to **Host Maintenance Settings** on the **Index Storage** page.

The screenshot shows the 'Host Maintenance Settings' configuration panel. It includes a toggle for 'Enable unindexed host removal' (currently disabled), a dropdown menu for 'Remove hosts not indexed in:' set to '60 days', and 'Clear Changes' and 'Save Changes' buttons.

2. To enable/disable unindexed host removal, select **Enable unindexed host removal**. The default is **Disabled**.
3. To change how long to retain unindexed hosts in an index, select a new value from the **Remove Hosts not indexed in** field. This can be set between **30** and **90** days. The default is **60**.
4. Select **Save Changes** to save any changes that you made. Select **Clear Changes** to discard any modifications you made.

User Management menu

Select **Settings > User Management** to manage user accounts and configure role privileges. The Ransomware Detection UI uses Role Based Access Control (RBAC) to assign a specific set of permissions in the Ransomware Detection UI for each role. Users can be assigned one of three system roles, which are described in [Role Privileges \(on page 87\)](#), or to user configured roles to control which pages and features are available to a set of users.

User accounts

Select **Settings > User Management > User Accounts** to manage user accounts. The page displays the following user options.

Column	Description
USER NAME	The user name for the account. This is set by the user who is creating the account.
SYSTEM ROLE	The assigned role and privileges to the user account. See Role Privileges (on page 87) for more information.
AD AUTHENTICATION	Indicates whether Active Directory (AD) authentication is enabled or not for the account. If disabled, the account uses local authentication.
AD USER NAME	The AD user name if AD authentication is used for the account.
DOMAIN	The domain name if AD authentication is used for the account.
USER STATUS	Indicates the user status, which can be active or inactive.



Note: You cannot delete or disable the **admin** account. Only local authentication for the **admin** account can be used.

From this page, manage the user accounts by adding, editing, or deleting user accounts as needed. See [Role Privileges \(on page 87\)](#) for the various roles that can be assigned to a user.

Adding a user account

To add a user account:

1. Go to **Settings > User Management > User Accounts**.
2. Select **Add**. The **Adding User** pop-up appears.
3. Select whether to use **Local Authentication** or **Active Directory Authentication** for the new user. The options change depending on the selected type of account authentication.



Note: AD must be enabled and a domain added in **Settings > Network and Security > Active Directory** before you will be able to use AD to authenticate the user account.

4. For **Local Authentication**, enter the following:

- the **Username**
- the **Password**, and confirm the **Password**.
- select a role to assign the user.
- select to enable or disable the **Force Password Change** option. When enabled, it forces the user to change their password on the next login to the system. By default, it is disabled.



Note: If you enable this option and change the user's password at the same time, then the user will not be forced to change their password at their next login.

- select whether the new user should be **Active** or **Inactive**.

5. If you select **Active Directory Authentication**, enter the following:



Note: You must enable AD in the **Settings > Network and Security > Active Directory** page before using AD authentication.

- **Username**
- **AD Username**
- **AD Domain**
- **Role**
- select whether the new user should be **Active** or **Inactive**.

6. Select **Add** to create the user account, or **Close** to cancel the changes.

Editing a user account

To edit a user account:

1. Go to **Settings > User Management > User Accounts**.
2. From the **User Accounts** table, select the user account you want to edit and then select **Edit**.
3. In **Editing User**, change any of the existing fields, such as:
 - **Username**
 - **Password**; if you change the password, you will be prompted to confirm the new password.
 - **Role**
 - **Force Password Change**

**Note:**

If this option is selected for an existing user, it will force the user to change their password on the next login, ignoring any password aging rules that may be in effect.

If you select this option and change the user's password at the same time, then the user will not be forced to change their password at their next login.

- **Active or Inactive**

4. Select **Save** to submit the changes to the account, or **Close** to cancel the changes.

Deleting a user account

To delete a user account:

1. Go to **Settings > User Management > User Accounts**.
2. From the **User Accounts** table, select the user account you want to edit and then select **Delete**.



Note: You cannot delete the pre-defined **admin** user account.

3. Verify that this is the user account you want to delete and select **OK**.





Role Privileges

Select **Settings > User Management > Role Privileges** to create user configured roles and manage the privileges for those roles.


ROLE NAME	ROLE TYPE	USERS	ACTIONS
admin	System	1	[Edit] [Delete]
alert editor	System	0	[Edit] [Delete]
viewer	System	0	[Edit] [Delete]
manager	User Configured	0	[Edit] [Delete]

The information shown in the **Role Privileges** table is listed below.

Column	Description
ROLE NAME	The name of the existing roles, which includes system roles and user configured roles.

Column	Description
ROLE TYPE	<p>Indicates if the role is a System role that cannot be deleted or modified or a User Configured role, which can be modified or deleted.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: A User Configured role cannot be deleted if any users are assigned that role. </div>
USERS	Indicates the number of users that have been assigned that role.
ACTIONS	Indicates if the role can be modified or deleted. If an icon cannot be selected, you cannot perform that action on the role.
	 Edit the user configured role name. See Editing a user configured role (on page 90) for more information.
	 Delete the user configured role. See Deleting a user configured role (on page 91) for more information. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: You can only delete a user configured role if no users are assigned to it. </div>

The table below lists the system roles on a Ransomware Detection system. These system roles have a set of privileges that cannot be modified.

 **Note:** The system roles cannot be modified or deleted.

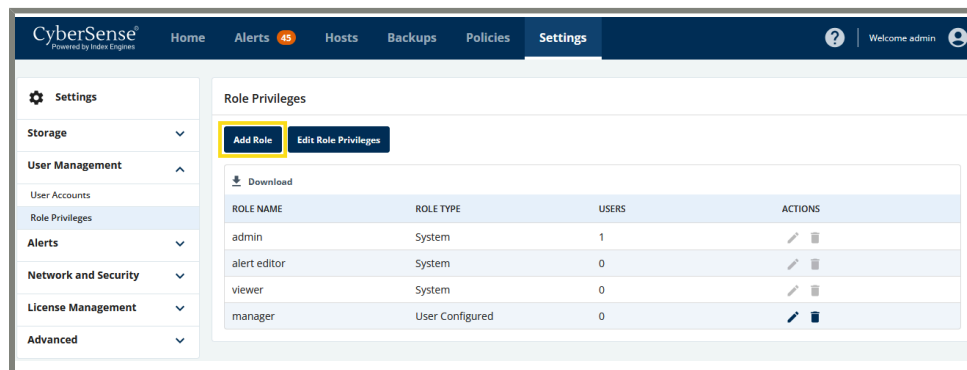
Role	Description
admin	The admin role is the system administrator of the Ransomware Detection system. The admin role can access all pages and modify any settings in the Settings menu.
viewer	<p>The viewer role has no other permissions than to view the following pages:</p> <ul style="list-style-type: none"> • Alerts • Hosts • Snapshots - view the Snapshots page. • Settings - view the Index Storage and License Status information as well as the EULA and threshold configurations. <p>This role has the most restrictive permissions and is useful for users that do not need to modify settings.</p>
alert editor	The alert editor role has the following permissions:

Role	Description
	<ul style="list-style-type: none"> • Alerts - clear alerts and select the alert configuration. • Hosts - modify the CyberSensitivity Index and the daily thresholds. • Snapshots - view the Snapshots page. • Settings - view the Index Storage and License Status information as well as the EULA and threshold configurations. In addition, this role can configure, view, modify, and delete thresholds.
user-configured role	User defined roles are assigned a custom set of privileges needed to perform a custom set of actions. There can be up to four user-configured roles on a Ransomware Detection system.

Adding a user configured role

To add a role to the Ransomware Detection system:

1. Go to **Settings > User Management > Role Privileges**.
2. Select **Add Role**.



3. In **Role Privileges**, add a name for the role in **Role Name**.
4. From the list of privileges, select the appropriate privileges group for the new role. See [Privileges \(on page 93\)](#) for more information about the privileges groups.















Note: If you do not select any privileges at this time, the new role will have the same privileges as the **viewer** system role. Any users assigned to the new role will be able to view various screens but not perform any actions.

5. Select **Save Changes** when done. The newly created role is displayed in the list of roles.

Role Privileges

[Add Role](#) [Edit Role Privileges](#)

Download

ROLE NAME	ROLE TYPE	USERS	ACTIONS
admin	System	1	 
viewer	System	0	 
alert editor	System	0	 
user_admin	User Configured	1	 
system-admin	User Configured	0	 
new_role	User Configured	0	 

Total Rows: 6

Editing a user configured role













To modify the name of a user configured role:

1. Go to **Settings > User Management > Role Privileges**.
2. Select **Edit** for the role that you want to modify.

Role Privileges

[Add Role](#) [Edit Role Privileges](#)

Download

ROLE NAME	ROLE TYPE	USERS	ACTIONS
admin	System	1	 
viewer	System	0	 
alert editor	System	0	 
user_admin	User Configured	1	 
system-admin	User Configured	0	 
new_role	User Configured	0	 

Total Rows: 6

3. Edit the name in **Role Name** and select **Save Changes** to save the new name.

Role Privileges
Roles Privileges > Edit Role Name

Role Name

Users List

USER	STATUS
No user.	

Deleting a user configured role

To delete a user configured role:



Note: You can only delete a user configured role if it does not have any users assigned to it. If the role has been assigned to a user account, reassign the user accounts to a different role and then delete the role.

1. Go to **Settings > User Management > Role Privileges**.
2. Select **Delete** associated with the role to remove.

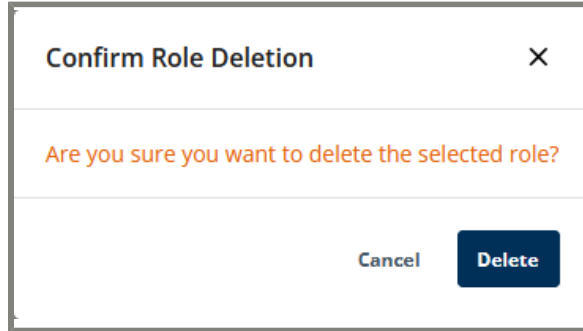
Role Privileges

Download

ROLE NAME	ROLE TYPE	USERS	ACTIONS
admin	System	1	
viewer	System	0	
alert editor	System	0	
user_admin	User Configured	1	
system-admin	User Configured	0	
new_role	User Configured	0	

1 row selected Total Rows: 6

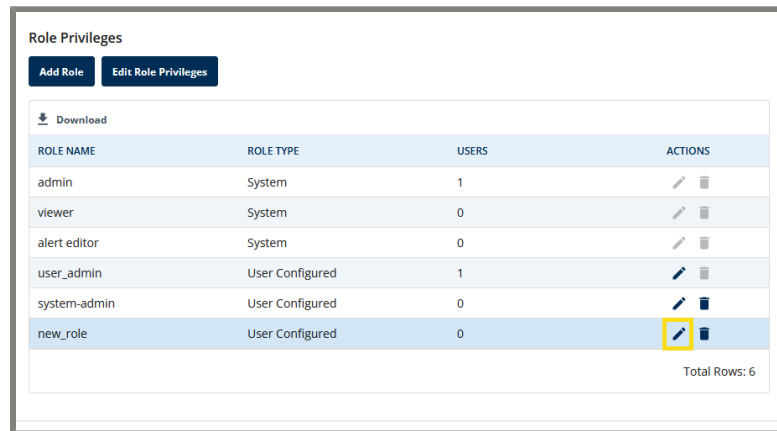
3. When prompted to confirm the deletion, select **Delete**. The role is removed from the **Roles** list.



Editing role privileges

To add or remove privileges from user configured roles:

1. Go to **Settings > User Management > Role Privileges**.



2. Select **Edit Role Privileges**. The list of privileges and roles are listed.

Each role has a list of assigned privileges. Modify the privileges of user configured roles by selecting or deselecting checkboxes under the specific role. See [Privileges \(on page 93\)](#) for more information and descriptions for each privilege.



Note: The privileges for the system roles of **admin**, **alert editor**, and **viewer** cannot be modified.

3. Select **Save Changes** when done, or **Cancel** to cancel the changes.

Privileges

Each system and user configured role is assigned a set of privileges. A user that is assigned a specific role can access various parts of the Ransomware Detection UI and may be restricted from other parts. The table below lists the different role privileges that may be assigned to a role.

Select **Edit Role Privileges** to view the privileges assigned to the system and user-configured roles. See [Editing role privileges \(on page 92\)](#) to learn how to change the privileges on user-configured roles.

Privileges Group	Description
Feature Visibility	
View all	The ability to view all pages and screens in Ransomware Detection UI.
Alert Management	
Clear alerts Manage alerts Manage special criteria alerts Manage email notifications Manage YARA rulesets	Manage alerts that occur on the Ransomware Detection server. This includes configuring the special criteria alerts, email notifications, viewing and clearing alerts, and setting up YARA rulesets.
Policy Management	
Manage policies Run policy	Create, modify, and delete policies and run policy jobs.
Account Management	
Managerole privileges Manage user accounts	Gives access to managing user accounts and role privileges.
Manage Active Directory configuration Manage diagnostics and reporting Manage login configuration Manage password configuration Manage security certificates	Manages security features, which include setting up Active Directory authorization, enabling diagnostics and reporting them back to Hitachi Vantara, login preferences, configuring password requirements, and uploading SSL/TLS certificates for secure connections.

Privileges Group	Description
Advanced Feature Management	
Manage license	Manage the licensing on your Ransomware Detection server, which includes adding a license, using a license server/license client configuration, and removing a Ransomware Detection server from a license server.
Manage trusted files	Manage the configuration of filename patterns, which label unknown file types as trusted files.
Manage thresholds	Create, modify, and delete threshold definitions, which can generate Threshold Exceeded alerts.
Recover from backup	Recover the Ransomware Detection files from a backup file that has been restored in a temporary location on the Ransomware Detection server. The backup includes the index, index segments, and license files as well as other Ransomware Detection-specific files.
Manage index settings	Access to manage index maintenance settings.

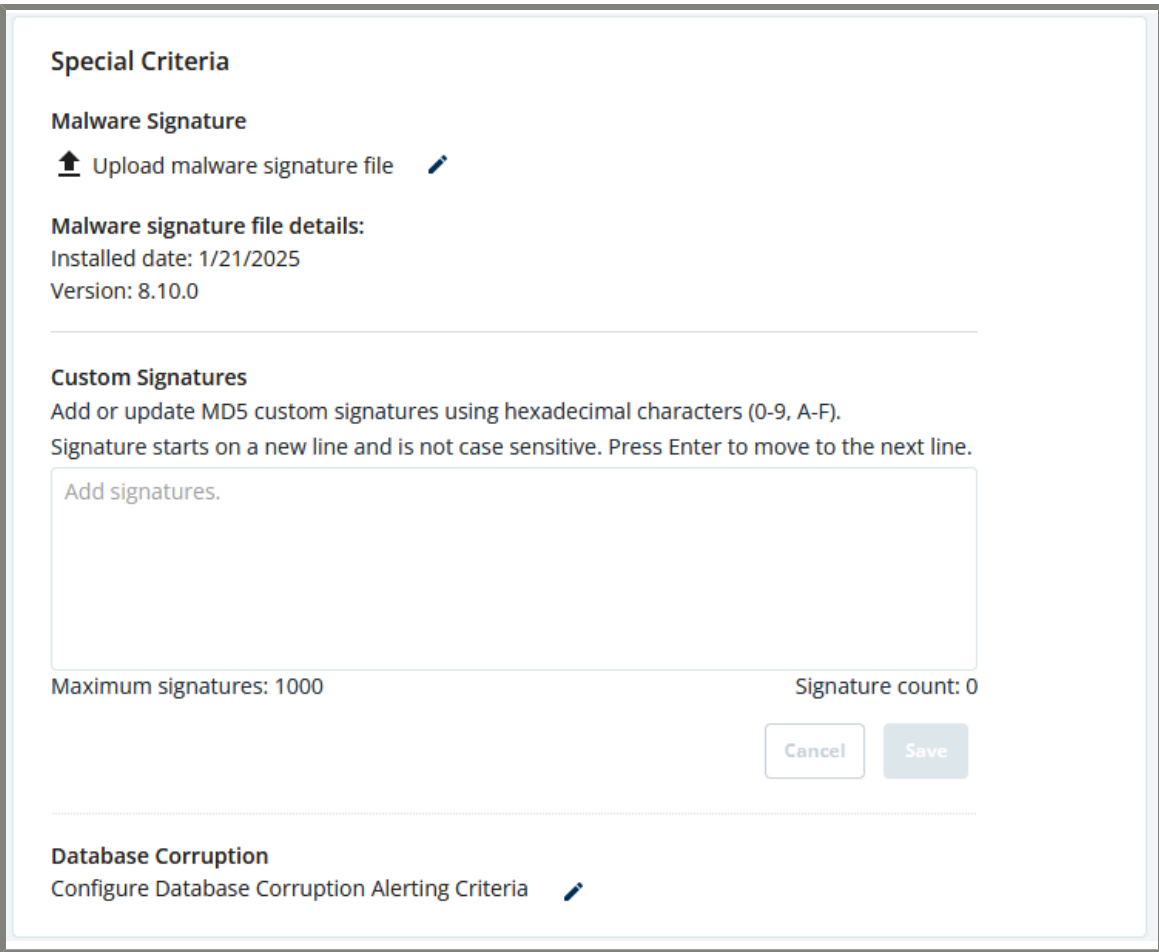
Alerts menu

To configure email notifications for security alerts and operation notifications, upload an updated malware signature file, manage custom malware signatures, or configure database corruption alerts, go to **Settings > Alerts**.

Special Criteria

The **Settings > Alerts > Special Criteria** page displays:

- an option to upload a newer malware signature file.
- the installation date and version of the currently installed malware signature file.
- the option to add or update custom malware signatures.
- the option to configure the reporting of database corruption alerts.

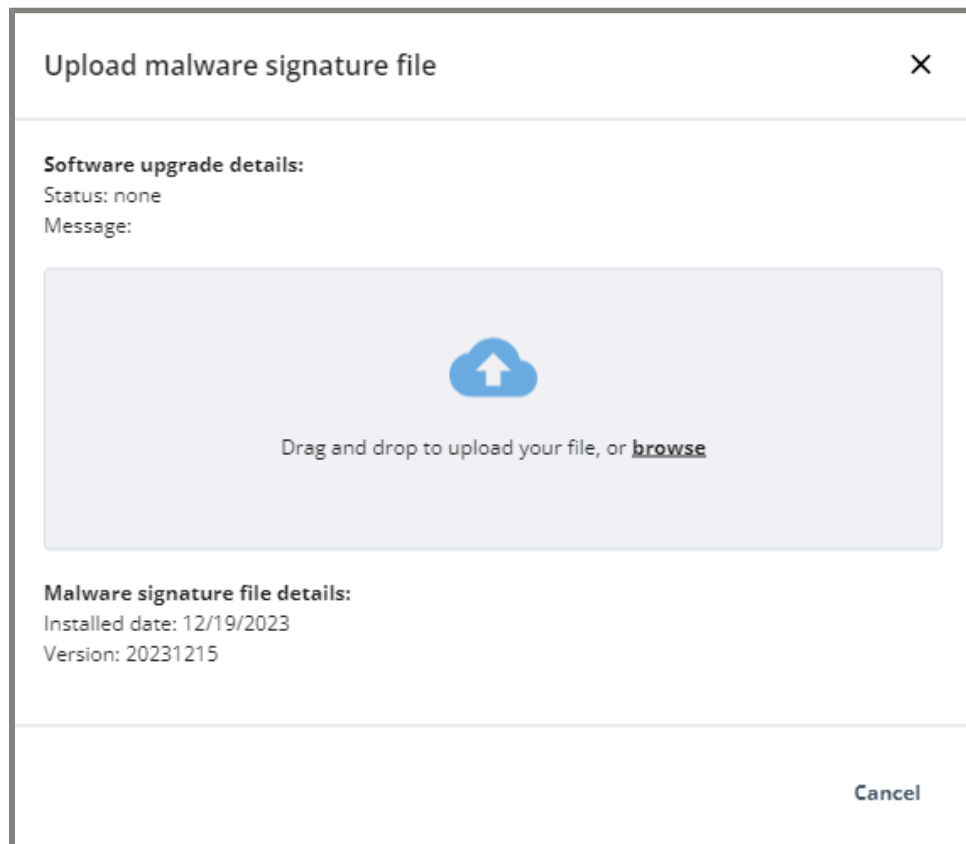


Uploading a malware signature file

If you have collected a file of malware signatures, or received the malware signature file RPM from Hitachi Vantara, upload it to the Ransomware Detection system to be used by Ransomware Detection Analytics for additional malware to look for. After uploading a new malware signature file, the detection process runs on all existing index segments. If any file signatures match malware file signatures, alerts are created.

To upload a malware signature file:

1. On the **Settings > Alerts > Special Criteria** page, select the **Edit** icon to open **Upload malware signature file**.



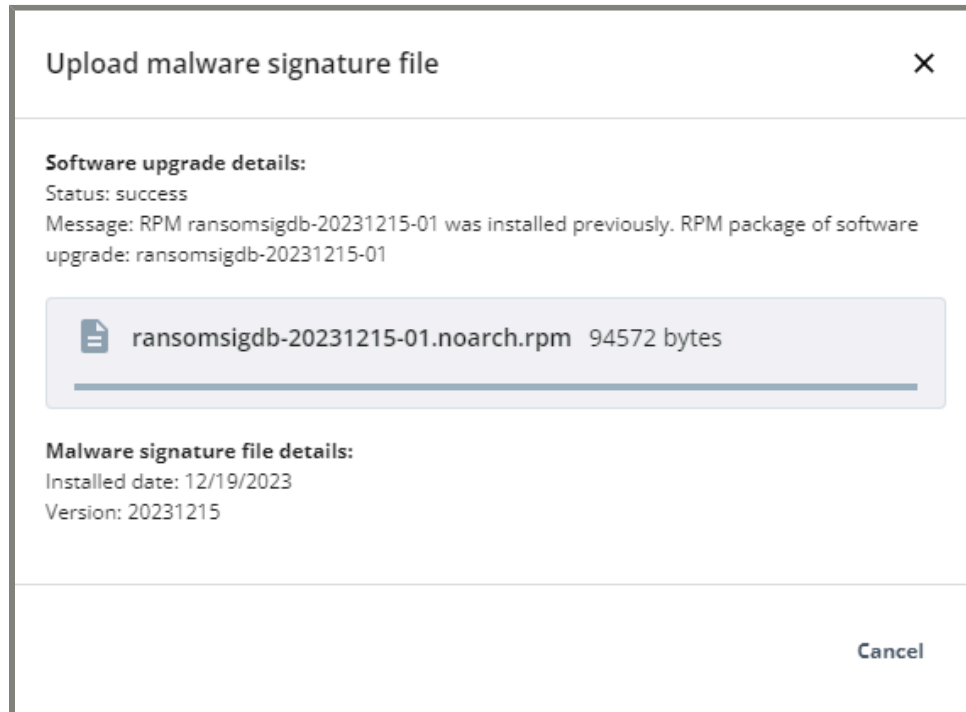
The screenshot shows a dialog box titled "Upload malware signature file" with a close button (X) in the top right corner. The dialog is divided into three main sections:

- Software upgrade details:**
 - Status: none
 - Message:
- File upload area:** A large light blue box containing a cloud icon with an upward arrow and the text "Drag and drop to upload your file, or **browse**".
- Malware signature file details:**
 - Installed date: 12/19/2023
 - Version: 20231215

A "Cancel" button is located in the bottom right corner of the dialog box.

2. Drag and drop your file into the **Upload malware signature file** box or browse to its location.

- Once the file is selected, the progress status changes to **inprogress** and then **success** when finished. Select **Close**.



Managing custom malware signatures

Malware signatures that you have encountered can be added to a custom malware signature database using the **Custom Signatures** feature. In addition to the Ransomware Detection-provided malware database, Ransomware Detection Analytics searches the signatures in the customer malware signature database. Signatures that are added or updated through the **Custom Signatures** feature are retained as the latest list of Custom Signatures. If a malware signature appears in both the malware signature database and has been added in the custom field, it is only processed once as a single alert. When the custom malware signature database is updated with a new signature that matches a file in the current index, Ransomware Detection generates a new alert for that signature and also changes the status of the corresponding policy job in the **Log** table to **Alert**.

Currently, a 32 hexadecimal character MD5 signature is the only type of custom signature accepted by Ransomware Detection.



Note:

When a malware alert is generated from a custom signature, the **Job ID** is the job during which the file was first indexed. When a change is made in the malware signature database, all future indexing jobs and previously indexed files are checked against the updated malware signature database.

When you modify the malware signature database by adding, deleting, or changing a custom malware signature, it will take up to five minutes for the change to take effect. If you are running a policy immediately after deleting a custom malware signature, you may see a false match to that custom malware signature.

To add or update a custom signature:

1. On the **Settings > Alerts > Special Criteria** page, type the malware signature in the **Custom Signatures** field, and press **Enter** to separate each signature on a new line.



Note: The custom signature is comprised of a 32 hexadecimal character MD5 signature and is the only type of custom signature accepted by Ransomware Detection.

Custom Signatures
Add or update MD5 custom signatures using hexadecimal characters (0-9, A-F).
Signature starts on a new line and is not case sensitive. Press Enter to move to the next line.

Add signatures.

Maximum signatures: 1000 Signature count: 0

Cancel Save

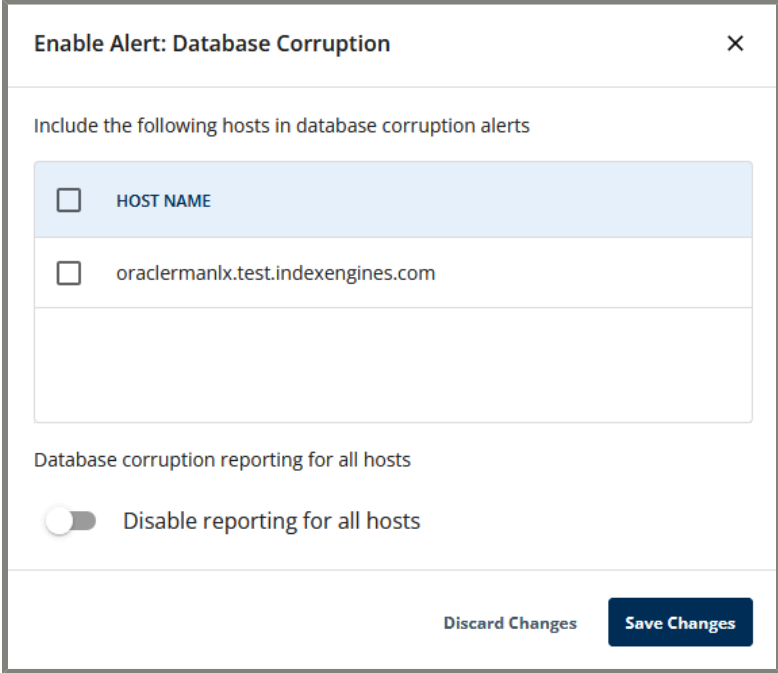
2. To delete a signature, delete the malware signature from the **Custom Signatures** field to remove it from the custom list.
3. Select **Save** to save your changes.

Configuring the database corruption alerting criteria

From the **Settings > Alerts > Special Criteria** page, disable the reporting of database corruption alerts for all hosts or re-enable the reporting for a specific host for which reporting of database corruption alerts has been disabled. After you disable the reporting of a database corruption alert for a specific host, which is done on the **Alerts** page, the hostname is listed in the **Database Corruption** section. You can re-enable reporting the database corruption alert for that host by selecting the hostname listed in this section. When you want to disable the reporting of database corruption alerts on all hosts, you can also configure that option in the **Database Corruption** section.

To configure database corruption alert reporting:

1. On the **Settings > Alerts > Special Criteria** page, select the **Edit** icon in the **Database Corruption** section.



Enable Alert: Database Corruption

Include the following hosts in database corruption alerts

- HOST NAME
- oraclermanlx.test.indexengines.com

Database corruption reporting for all hosts

Disable reporting for all hosts

Discard Changes Save Changes

2. Select the host(s) for which you want to re-enable the reporting of database corruption alerts.



Note: In this section, you will only see the list of hosts for which database corruption alert reporting has been disabled on the **Alerts** page. See [Disabling database corruption alerts \(on page 24\)](#) for more information.

3. To disable database corruption alert reporting for all hosts, select **Disable corruption reporting for all hosts**.
4. Select **Save Changes** to save your changes.

Enabling the alert reporting for a specific host

To enable database corruption alerts:

1. On the **Settings > Alerts > Special Criteria** page, select the **Edit** icon.

Enable Alert: Database Corruption

Include the following hosts in database corruption alerts

- HOST NAME
- sqllee.test.indexengines.com
- oraclermanlx.test.indexengines.com

Database corruption reporting for all hosts

Disable reporting for all hosts

Discard Changes Save Changes

2. Select the host(s) for which you want to enable the reporting of database corruption alerts.



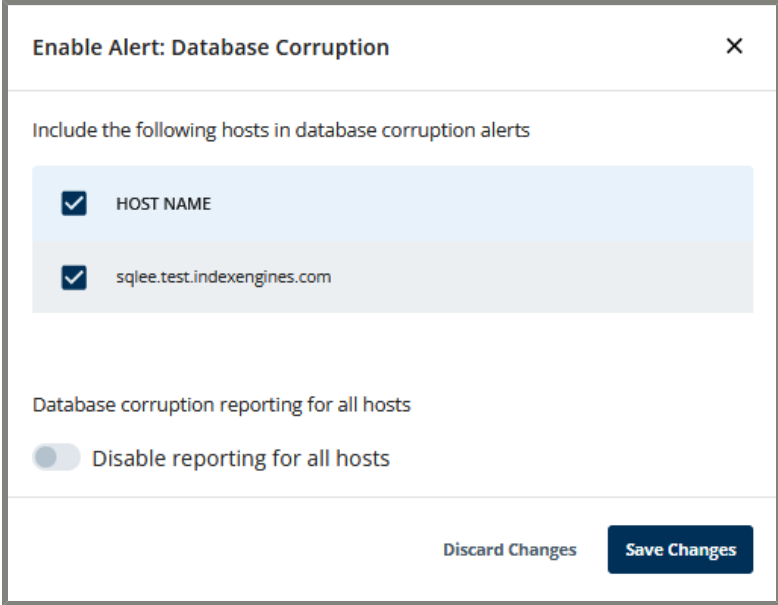
Note: In this pane, you will only see the list of hosts for which database corruption alert reporting has been disabled in the **Alerts** page.

3. Select **Save Changes** to save your changes to the alert reporting.

Globally enabling/disabling the alert reporting for all hosts

To globally enable or disable database corruption alerts:

1. On the **Settings > Alerts > Special Criteria** page, select the **Edit** icon.



Enable Alert: Database Corruption

Include the following hosts in database corruption alerts

- HOST NAME
- sqllee.test.indexengines.com

Database corruption reporting for all hosts

Disable reporting for all hosts

Discard Changes Save Changes

2. Set the slide control to **Disable**, which disables database corruption alert reporting for all hosts.
3. If the alert reporting has been previously disabled, select the host name to enable the reporting.
4. Select **Save Changes** to save your changes to the alert reporting.

Email Notifications

Configure email notifications for security alerts and job-related operation notifications on the **Alerts > Email Notifications** page.

The security alerts that trigger an email to the listed addresses are those that appear on the **Alerts** table on the **Alerts** page, which include:

- **Threshold Exceeded**
- **Infection Found**
- **Database Corruption**
- **Malware Detected**

In addition to sending emails that indicate a security alert found during Ransomware Detection analysis, an email is sent when a policy job finishes successfully and Ransomware Detection analysis does not find any security alerts.

For operations notifications, the following processes can be selected to trigger an email to be sent to the entered addresses:

- **Job Failed** - includes any indexing or post-processing job that has failed and cannot finish.
- **Job Start and Job Done** - includes when an indexing job or a post-processing job starts and finishes.

System update notifications send an email for the following events:

- a system update has become available.
- a system update has finished.
- a system update has failed.

Setting the email addresses for security alerts

To add or delete an email address from the list that receives email notifications for security alerts:

1. On the **Settings > Alerts > Email Notifications** page, enter an email address in the **Security Alerts** text box and press **Enter**. The email address is added to the list.

The screenshot shows the 'Email Notifications' configuration page. It is divided into three sections: 'Security Alerts', 'Operations Notifications', and 'Update Notifications'. Each section has an 'Email' input field. The 'Security Alerts' section has a single empty input field. The 'Operations Notifications' section has an input field containing two email addresses: 'jovalle@indexengines.com' and 'vpatel@indexengines.com', each with a small 'X' icon to its right. Below the input field is the text 'Add email and press Enter.' and two checkboxes: 'Job Failed' (checked) and 'Job Started and Job Done' (checked). The 'Update Notifications' section has a single empty input field. At the bottom right of the form are two buttons: 'Clear Changes' and 'Save Changes'.

2. To delete an email address, select the **X** associated with the email address.
3. Select **Save changes** to save your changes.

Setting the email addresses for operations notifications

To add or delete an email address from the list that receives email notifications for LAN Indexer and post-processing jobs:

1. On the **Settings > Alerts > Email Notifications** page, type an email address in the **Operations Notifications** text box and press **Enter**. The email address is added to the list. Add more emails if needed.

Email Notifications

Security Alerts
Send an email notification for security alerts.

Email

Add email and press Enter.

Operations Notifications
Send an email notification for LAN Indexer and post-processing jobs.

jovalle@indexengines.com vpatel@indexengines.com Email

Add email and press Enter.

Job Failed
 Job Started and Job Done

Update Notifications
Send an email for system update notifications.

Email

Add email and press Enter.

Clear Changes Save Changes

2. Select which job status that you want to be notified about. The options are:
 - **Job Failed** - includes any indexing or post-processing job that has failed and cannot finish.
 - **Job Started and Job Done** - includes when an indexing job or a post-processing job starts and finishes.
3. To delete an email address, select the **X** associated with the email address.
4. Select **Save changes** to save your changes.

Network and Security menu

Go to the **Settings > Network and Security** menu to find network and security system setting options. The options can be found in the menus listed below:

- [Login \(on page 104\)](#) - change login options to increase security for account logins.
- [Password Configuration \(on page 105\)](#) - configure the password complexity and rules for user account passwords.
- [Active Directory \(on page 107\)](#) - set up your Active Directory (AD) domain for user management.
- [Security Certificates \(on page 109\)](#) - configure security certificates, such as SSL/TLS.
- [Diagnostics and Reporting \(on page 111\)](#) - set up the audit trail heartbeat and the sending of information to Hitachi Vantara.

Login

The **Settings > Network and Security > Login** page displays settings for various login options, which include:

- logging out the user after a configured period of inactivity.
- set the number of failed login attempts before a user account is locked out.

Configuring the inactivity timeout

The **Allow Timeout** option is disabled by default. When enabled, the user account will be logged out after the set number of minutes of inactivity.

To enable or disable the login timeout:

1. On the **Settings > Network and Security > Login** page, to enable the timeout option, toggle **Allow Timeout** and set the **Timeout** in minutes.
2. Select **Save Changes** to save the configured values.

Setting failed login attempts limits

The **Failed Login Attempts Limits** option sets the number of failed login attempts within a configured time period, which can be set in seconds, minutes, or hours. If a account exceeds the configured number of attempts within the set time, then the account is locked. Set the limit for the number of attempts within a configured number of seconds, minutes, or hours.

To set the failed login attempts limits:

1. On the **Settings > Network and Security > Login** page, set the number of login attempts and the time period as needed by company policy. The maximum number of failed attempts has a default of **10**.
2. Select **Save Changes** to save the configured values.

Password Configuration

Select **Settings > Network and Security > Password Configuration** to globally configure and manage password complexity for user accounts. Any changes that you make to the password complexity does not apply to existing passwords. You can force the user to reset their password on their next login. See [Editing a user account \(on page 86\)](#) for details.

Enable and modify the following fields:

Field	Description
Password Length	
Minimum Characters	The minimum length of the password. This can be set between 12 and 24 characters, inclusive.
Maximum Characters	The maximum length of the password. The default is 24 characters, inclusive.
Password Complexity	
Lowercase Letter(s)	The minimum number of lowercase letters, inclusive. The default is at least 1 lowercase letter.
Uppercase Letter(s)	The minimum number of uppercase letters, inclusive. The default is at least 1 uppercase letter.
Numerical Character(s)	The minimum number of numerical characters, inclusive. The default is at least 1 .
Special Characters	The minimum number of special characters, inclusive. The special characters list includes characters such as ~! @ # \$ % ^ & * () _ + = - ' [] / ? > <) and any unicode character that is not a letter, number, or white space. The default is at least 1 special character.
Maximum Number of Consecutive Repeated Characters	The maximum number of a consecutive identical character in a password. For example, if the value is set to 2 , then a password containing "abbbcd" is not valid because it contains three consecutive identical characters. The default is disabled.
Password Uniqueness	
New password must be different from X previous passwords	The number of unique passwords associated with a user account that cannot be reused when creating a new password. The default is 5 with a maximum of 10 , inclusively.
Password must not include username	Restricts the password from containing the username. The default is disabled.
Password Change Policy	

Field	Description
Expiry (Days)	The maximum number of days before the password will expire and the user is forced to change their password. The default is 60 days with a maximum of 90 days, inclusively.
Changes allowed within 24 hours	The maximum number of times a user can change their password in a 24 hour period. The default is 3 and can be modified.
Password expiry warning (days)	The number of days before the password expiration that a warning message appears. The warning notifies the user how many days remain before they are forced to change their password. The default is disabled.

Configuring the password complexity

To configure the password complexity for the Ransomware Detection server:

1. On the **Settings > Network and Security > Password Configuration** page, select the password complexity fields to enable. You can't enter text into a field unless you have selected it.



Note: If you no longer want to use a field, select the checkbox associated with the field to disable it and any values will be ignored.

2. After selecting the fields to use, enter values that follow company password requirements:

Field	Description
Password Length	
Minimum Characters	The minimum length of the password. This can be set between 12 and 24 characters, inclusive.
Maximum Characters	The maximum length of the password. The default is 24 characters, inclusive.
Password Complexity	
Lowercase Letter(s)	The minimum number of lowercase letters, inclusive. The default is at least 1 lowercase letter.
Uppercase Letter(s)	The minimum number of uppercase letters, inclusive. The default is at least 1 uppercase letter.
Numerical Character(s)	The minimum number of numerical characters, inclusive. The default is at least 1 .
Special Characters	The minimum number of special characters, inclusive. The special characters list includes characters such as ~! @ # \$ % ^ & * () _ + = - ' [] / ? > <) and any unicode character that is not a

Field	Description
	letter, number, or white space. The default is at least 1 special character.
Maximum Number of Consecutive Repeated Characters	The maximum number of a consecutive identical character in a password. For example, if the value is set to 2 , then a password containing "abbbcd" is not valid because it contains three consecutive identical characters. The default is disabled.
Password Uniqueness	
New password must be different from X previous passwords	The number of unique passwords associated with a user account that cannot be reused when creating a new password. The default is 5 with a maximum of 10 , inclusively.
Password must not include username	Restricts the password from containing the username. The default is disabled.
Password Change Policy	
Expiry (Days)	The maximum number of days before the password will expire and the user is forced to change their password. The default is 60 days with a maximum of 90 days, inclusively.
Changes allowed within 24 hours	The maximum number of times a user can change their password in a 24 hour period. The default is 3 and can be modified.
Password expiry warning (days)	The number of days before the password expiration that a warning message appears. The warning notifies the user how many days remain before they are forced to change their password. The default is disabled.

3. When finished, select **Save Changes**.

Active Directory

Ransomware Detection integrates Active Directory (AD) to authenticate user accounts. Make sure that the users for which you enable AD have AD user accounts.

Each engine using the client/server licensing model handle the AD queries. If you want to integrate AD, you should set up AD on each engine.

Active Directory

Domain

Domain Name
INDEXENGINES.COM

Account

Login Username
pglthens

Password

QUERY DOMAIN	DOMAIN NAME	DNS NAME	QUERY STATUS
<input type="checkbox"/>	IEMAILMEN	iemailmen.com	Not Queryable
<input checked="" type="checkbox"/>	INDEXENGINES	indexengines.com	Successful
<input type="checkbox"/>	EMAIL	email.indexengines.com	Not Queryable
<input type="checkbox"/>	TEST	test.indexengines.com	Not Queryable
<input type="checkbox"/>	DEVEL	devel.indexengines.com	Not Queryable

Once AD is enabled and you have added a domain name with proper user account credentials, a table listing all the domains that were probed when you enabled AD. The following information is displayed in the table:

- **QUERY DOMAIN** - the user's AD account has been configured with no query restrictions. Certain accounts may limit the number of times the account can query the AD domain before being locked out.
- **DOMAIN NAME** - the domain name of the AD domain.
- **DNS NAME** - the Domain Name System name of the AD domain, which contains the domain name and the domain extension.
- **QUERY STATUS** - shows the status of the probe operation that took place when you enabled AD. The process is either **Successful** or **Not Queryable**.

Enabling Active Directory

When you enable AD on your engine, you must also add the domain name and AD account credentials.



Note: You must enable AD and add an AD domain before you can add AD credential authentication to a user account.

**Note:**

If you receive an error regarding an incorrect domain name or user credentials, make sure that the `/etc/resolv.conf` file is configured correctly and includes a search line. The following is an example:

```
search [domain-name].com
nameserver 192.256.256.213
nameserver 10.192.256.2
```

To enable AD on your engine:

1. On the **Settings > Network and Security > Active Directory** page, toggle the **Domain** option to enable AD integration.

Active Directory

Domain

Domain Name

example.com

Account

Login Username

jsmythe

Password

.....

Clear Changes Save Changes

2. In the **Account** section, add the AD username and password.



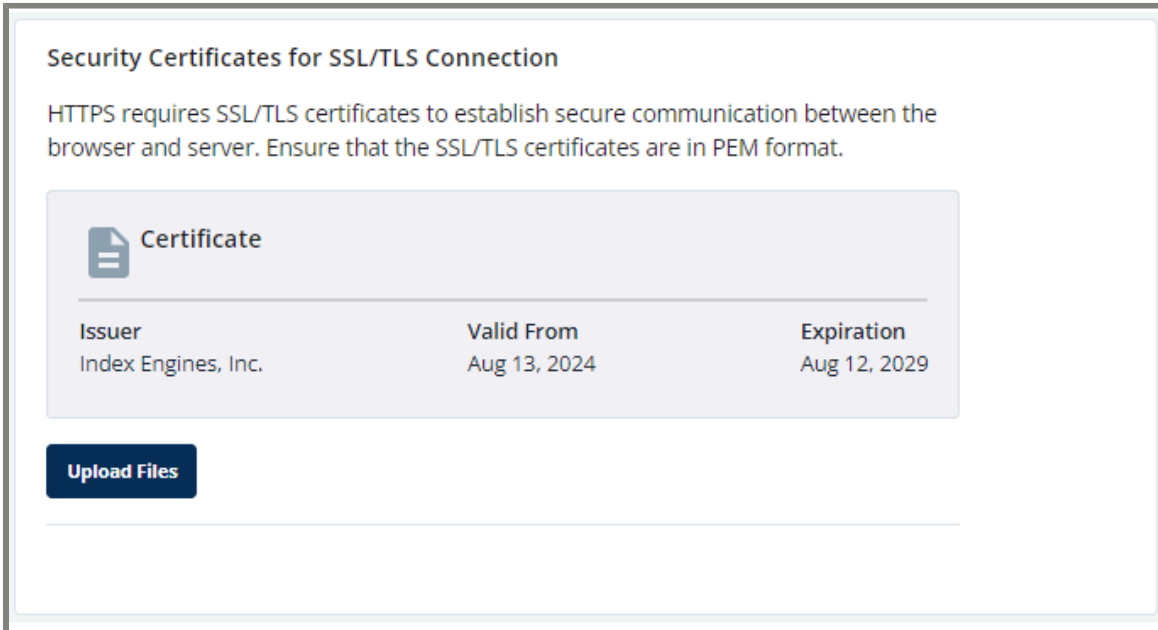
Important: When enabling AD integration, ensure the credentials you are using are not restricted in any way.

3. Select **Save Changes** when finished. The newly added AD account will be added to the AD accounts table.

Security Certificates

Control SSL/TLS connections and security certificates for the Ransomware Detection engine on the **Settings > Network and Security > Security Certificates** page. HTTPS requires SSL/TLS certificates to establish secure

communication between the browser and server. From this page, you can also upload new security certificates if needed.



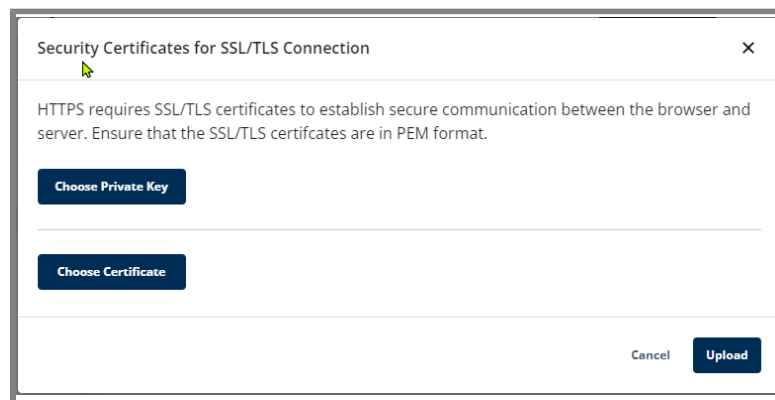
Configuring HTTPS for SSL/TLS connections

To configure SSL/TLS connections to use HTTPS:

1. On the **Settings > Network and Security > Security Certificates** page, select **Upload Files** to upload private key and certificate files.



Note: SSL/TLS certificates must be in PEM format.



2. Select **Upload** to upload the files. Once uploaded, the certificate details will be displayed in the **Certificates** table on this page.

Diagnostics and Reporting

Select the **Settings > Network and Security > Diagnostics and Reporting** menu to enable the audit trail heartbeat, which sends an event every hour to the Audit Trail log to indicate that the engine is operational, and send status reports and crash reports to Hitachi Vantara.



Note: You must enable audit trail logging prior to enabling the audit trail heartbeat feature.

Enabling audit trail logging

The Audit Trail feature logs all user actions and alerts. Audit trail information includes the user who performed an action, the action taken, the Ransomware Detection engine on which the action happened, and the date and time of the action. The alerts cover the services that run during different processes, such as indexing jobs, starting and stopping services. After enabling the audit trail logging, enable the audit trail heartbeat in **Settings > Network and Security > Diagnostics and Reporting**.

To enable audit trail logging, update the system logging configuration as follows:

1. Save a copy of the `/etc/rsyslog.conf` file.
2. Update the `/etc/rsyslog.conf` file as follows:
 - a. Add the following lines to the end of the script if they don't exist. If they do exist and are commented out, uncomment them by removing the `#` in front of the line.

```
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514
LOCAL1.* /var/log/iesyslog.log
```



Note: The last line above determines where the logs will be stored. Store the logs in the `/opt/ie/var/` directory. For example: `/opt/ie/var/log/iesyslog.log`

- b. In `/etc/rsyslog.conf`, add `local1.none` to the line for `/var/log/messages` as shown below:

```
*.info;mail.none;authpriv.none;cron.none;local1.none; /var/log/messages
```



Note: The line in the `/etc/rsyslog.conf` file may look different than the example above depending on your OS and should be located at the end of the file.

3. Restart the `rsyslog` service by executing this command:

```
systemctl restart rsyslog.service
```

The `/var/log/iesyslog.log` file will now record all user actions. Your system administrator should manage this file using `logrotate` — or a similar command — to rotate and purge logs as desired.

Once the setup completes, activity messages start appearing in `/var/log/iesyslog.log`. These messages will be similar to those in the following example:

```
Feb 4 09:16:03 farset local1: {"engine":["farset.test.indexengines.com"],"description":["Index trunk_r98672 (ID 110) has been deselected."],"date":["Feb-04-2024 09:16:03"],"user":["admin"],"function":["DeselectIndex"]}
```

```
Feb 4 09:16:39 farset local1: {"engine":["farset.test.indexengines.com"],"description":["Index trunk_R98712 (ID 111) has been selected."],"date":["Feb-04-2024 09:16:39"],"user":["admin"],"function":["SelectIndex"]}
```

```
Feb 4 09:40:06 farset local1: {"engine":["farset.test.indexengines.com"],"description":["admin logging in..."],"date":["Feb-04-2024 09:40:06"],"user":["admin"],"function":["LogIn"]}
```

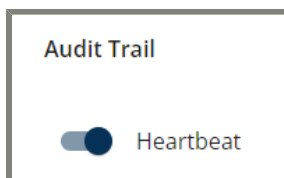
```
Feb 4 09:41:31 farset local1: {"engine":["farset.test.indexengines.com"],"description":["Catalog Ingestion Save Server"],"date":["Feb-04-2024 09:41:31"],"user":["admin"],"function":["CatalogIngestionSaveServer"]}
```

Enabling the Audit Trail heartbeat

Before enabling the audit trail heartbeat, make sure to enable audit trail logging. See [Enabling audit trail logging \(on page 111\)](#) for instructions.

To enable or disable the Audit Trail heartbeat:

1. On the **Settings > Network and Security > Diagnostics and Reporting** page, toggle the **Audit Trail > Heartbeat** option to enable or disable the audit trail heartbeat feature. This will send an event hourly to the audit trail log to indicate that the system is operational.



2. Select **Save Changes**.

Configuring analytics reporting

Enable or disable analytics reporting of diagnostics to enhance Ransomware Detection, which sends data from Ransomware Detection to Hitachi Vantara for algorithm enhancement.

To configure analytics reporting:

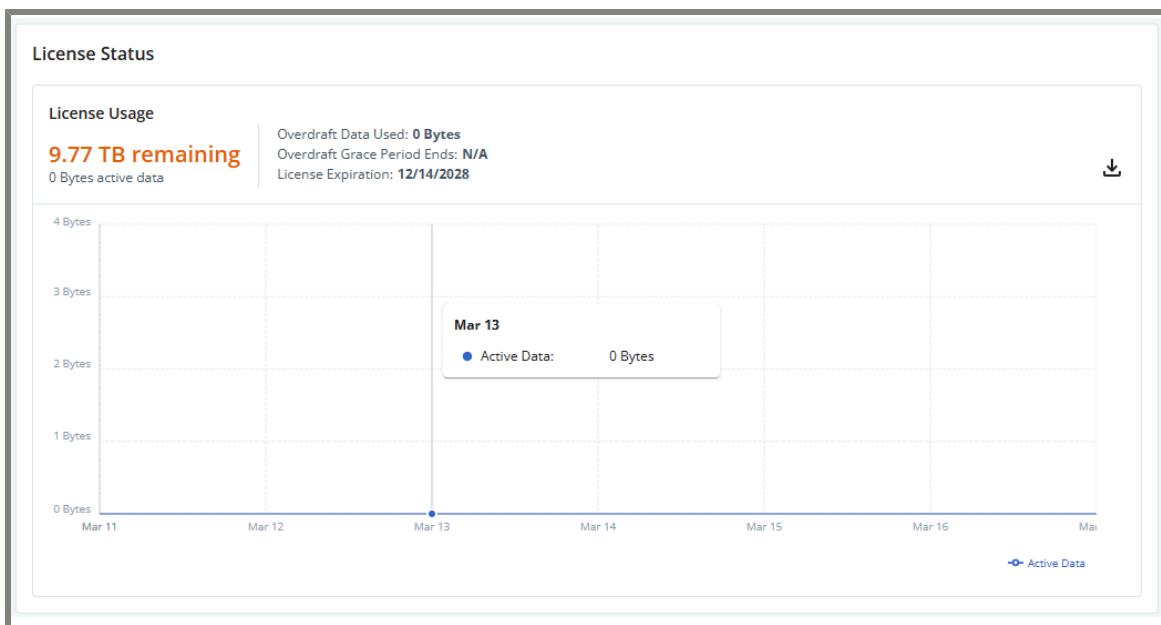
1. On the **Diagnostics and Reporting** page, select the **Enhance Analytics** checkbox to enable sending data from Ransomware Detection to Hitachi Vantara.
2. Select **Save Changes** to save your choice.

License Management menu

Under the **License Management** menu, view the license status and details, upload an additional license, and view the EULA that was signed in the **Setup** process during installation.

License Status

Select **License Management > License Status** to view the license usage graph that shows the amount of Active Data in the current index on an engine over time and the total amount of Active Data remaining in the license. Additionally, any overdraft amount of Active Data is displayed in **Overdraft Data Used** and the remaining grace period is displayed in **Overdraft Grace Period Ends**; these are displayed whether an overdraft of Active Data is present or not. Select the varied line to view the amount of Active Data used on different days. You can also download a CSV file of licensing information starting with when the license was installed. See [Downloading a license capacity CSV report \(on page 115\)](#) for details.



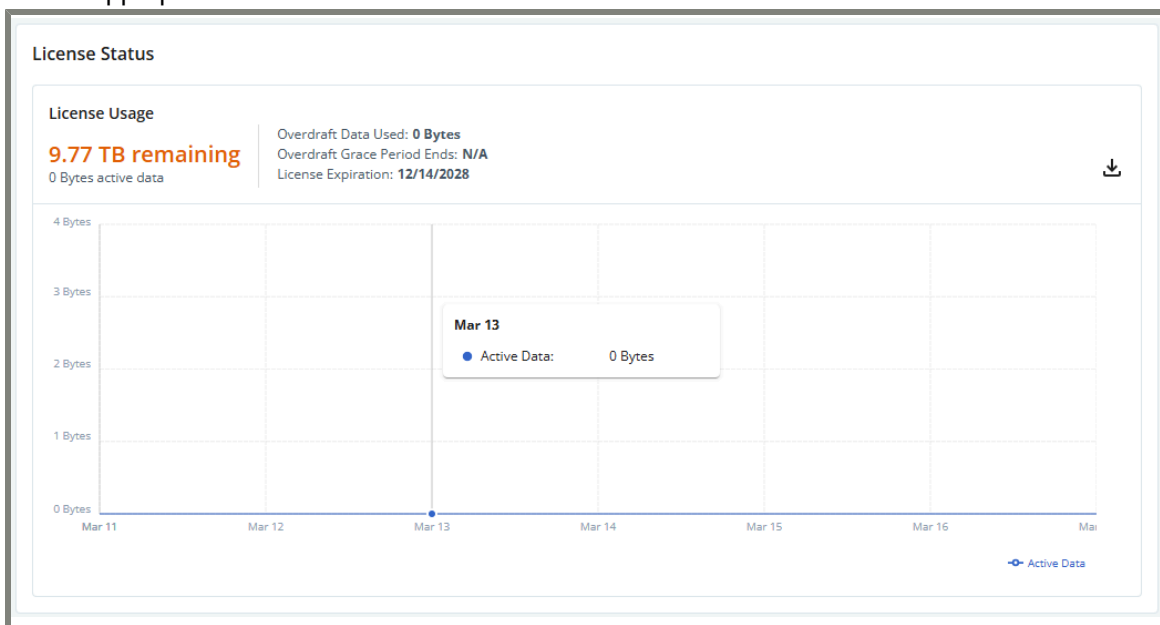
In the latest release of the software, Ransomware Detection licenses can be shared between more than one engine. With the client/server licensing model, one engine can act as a license server for several engines — license clients — by dynamically distributing its license among all engines at the site to meet usage needs. Engines can automatically request and return license counters as their Active Data changes over time, ensuring the most efficient distribution of the licenses among all the engines registered with the engine acting as the license server. The license server issues a perpetual certificate to the license clients, whether or not the license client uses the license server in the future.

To enable license server functionality, you first install one or more licenses on the engine that will act as the license server. Next, you will register other engines with the license server. All other engines will then have access to the shared license pool.

Downloading a license capacity CSV report

The license CSV report contains a list of hosts that have Active Data in the current index as well as the amount of Active Data from that host at various points in time. The **License Status** graph displays the total amount of Active Data used by all host(s) listed in the license CSV report for a specific date. This capacity report is a good place to start looking if your system is in overdraft of your license since you can easily determine which hosts are the largest consumers of Active Data in a license and which ones haven't been indexed in a long time. If a host has not been indexed in a long time, it may indicate that the host is no longer active, e.g., it may have been decommissioned. To automatically remove inactive hosts from the index and avoid consuming Active Data for them, enable **Remove Unindexed Hosts** on the **Settings > Storage > Index Storage** page.

On the **License Management > License Status** page, select the **Download** icon and when prompted, save the CSV file in the appropriate location.



A sample CSV is shown below.

	A	B	C
1	Client hostname	Date	Active Data
2	vra2-cent-01	Mon Jan 15 05:32:43 2024	3156777484
3	vra2-cent-01	Mon Jan 15 08:13:27 2024	3156777484
4	vra2-cent-01	Mon Jan 15 15:12:48 2024	3156777484
5	vra2-cent-01	Mon Jan 15 15:27:48 2024	3156777484
6	vra2-cent-01	Mon Jan 15 17:24:48 2024	3156777484
7	vra2-cent-01	Mon Jan 15 20:12:20 2024	6313554968
8	oraclermanlx.example.com	Sun Jan 14 01:18:32 2024	6289040384
9	oraclermanlx.example.com	Sun Jan 14 06:42:27 2024	12578080768
10	oraclermanlx.example.com	Sun Jan 14 21:14:01 2024	6289040384
11	oraclermanlx.example.com	Mon Jan 15 00:28:17 2024	6289040384
12	oraclermanlx.example.com	Mon Jan 15 00:40:17 2024	6289040384
13	oraclermanlx.example.com	Mon Jan 15 05:32:43 2024	6289040384
14	mssqldem2	Sun Jan 14 06:42:27 2024	2302681088
15	mssqldem2	Sun Jan 14 21:14:01 2024	2302681088
16	mssqldem2	Mon Jan 15 00:28:17 2024	2302681088

The columns in the CSV files list:

- the client hostname.
- the date on which the Active Data amount used by a host was evaluated.
- the amount of Active Data used in the index for that host.

Sort the CSV by date and add the Active Data amounts for all hosts listed for that date. The total amount of Active Data is the amount displayed on the **License Status** graph for a specific date.

License overdraft

When the amount of licensed Active Data has been exceeded, you will receive a notification in the Ransomware Detection email informing you of an overdraft of your license. There is a 90-day grace period until Ransomware Detection stops analyzing data. If the amount of Active Data decreases under the license capacity, then the 90-day grace period resets. To calculate how much remaining Active Data you have on your license, see [Moving to client/server licensing on existing engines \(on page 120\)](#) for details.

One method to find out how much Active Data your hosts are consuming is to download the license capacity CSV report from the **Settings > License Status** pop-up. See [Downloading a license capacity CSV report \(on page 115\)](#) for instructions. This report lists the client hosts, the date on which Ransomware Detection last indexed the host's files, and how much Active Data is allocated to each host.

Review the last date that a host's files were indexed by Ransomware Detection along with the amount of Active Data used by that particular host. If a host is no longer active, Ransomware Detection will still attribute Active Data to that host until you remove the host from the index. You can configure the **Host Maintenance Settings** to remove those hosts that have not been indexed a long time. By removing the hosts from the list to be indexed, you will free up Active Data, which will then be available to other hosts. See [Configuring the host maintenance settings \(on page 83\)](#) for more details.

License Details

Select **Settings > License Management > License Details** to view information about installed licenses and all license client engines that have received a certificate from the license server that you are currently accessing in the Ransomware Detection UI. This list includes license client engines that are no longer active, cannot establish connection to the license server, or no longer configured to use the license server. Use the **LAST CONTACT** entries to determine which license clients are still active and recently established a connection to the license server. The license clients that have most recently established a connection to the license server are listed towards the top of the column.

License Details

License Server

Host:

This CyberSense Server

Host: server1-blade10

Engine ID: 3C:EC:EF:D9:70:74

License Clients

IP ADDRESS	HOST	LAST CONTACT	ROLE
No rows			

Create a License Server Connect to a License Server

[Upload License](#)

In the **License Server** section, the **Host** displays the server details for **This Ransomware Detection Server** if it is registered with the license server. If **This Ransomware Detection Server** is not registered with a license server, then either register it with a license server or use its local license.

In the **License Clients** section, the table lists the license clients that have registered this Ransomware Detection node as a license server.

When you upload an additional license, the Active Data amount is added to the existing amount for additional capacity. The new license does not overwrite the original one.

From the **License Details** page, do the following:

- review the host information.
- review the engine ID.

- review the expiration date of the current license.
- change how the Ransomware Detection host has been licensed or upload an additional license.

Creating a license server

During the Ransomware Detection installation process, you selected to use a license server for your licensing requirements or create a license server for license clients to connect to. When you create a license server, the license is installed locally on the Ransomware Detection system. Additional licenses can be uploaded to increase the licensing capacity of the Ransomware Detection system. The new locally installed license increases the amount of Active Data capacity and does not overwrite other licenses.



Note: At any time, you can change from being a license server to a license client.

To create a license server or upload additional licenses:

1. On **Settings > License Management > License Details**, select **Create a License Server**.

IP ADDRESS	HOST	LAST CONTACT	ROLE
No rows			

Select **Upload License**.



2. When prompted, select your license file to upload. Select **Open** to finish the process.

With a locally installed license, this engine can now function as a license server if needed.

Connecting to a license server

If you currently have a local license installed on the Ransomware Detection server, you can change your licensing method to use a license server instead. A license server holds a license which has a certain amount of allocated Active Data. With a locally installed license and connecting to a license server, the capacity of the licenses are combined and do not overwrite any previously installed licenses.


1. On **Settings > License Management > License Details**, select **Connect to a License Server**. Fill in the following fields:

Field	Description
License Server Host	The name of license server host. This license can be accessed by one or more engines.
Username	Currently, the only permissible user name is the <code>admin</code> account of the license server and cannot be changed.
Password	The password for the <code>admin</code> account of the license server. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px;"> <p> Note: If the <code>admin</code> account's password changes later, you do not have to update the password in this pane.</p> </div>
One-Time Password	If MFA has been enabled on the license server engine or on the <code>admin</code> account on the license server, then enter the OTP in this field. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px;"> <p> Note: Contact the system administrator of the license server engine to receive a QR code or secret key with which you can use in an authenticator app.</p> </div>

Upload License
 Register with License Server

License Server Host:

Username:

Password: 

One-Time Password:

2. Select **Register**. When the license client is successfully registered with the license server, the license server is displayed as the **Host** in the **License Server** section and the license client that was just registered is the **Host** in the **This Ransomware Detection Server** section.

The screenshot displays the 'License Management' interface. It is divided into several sections:

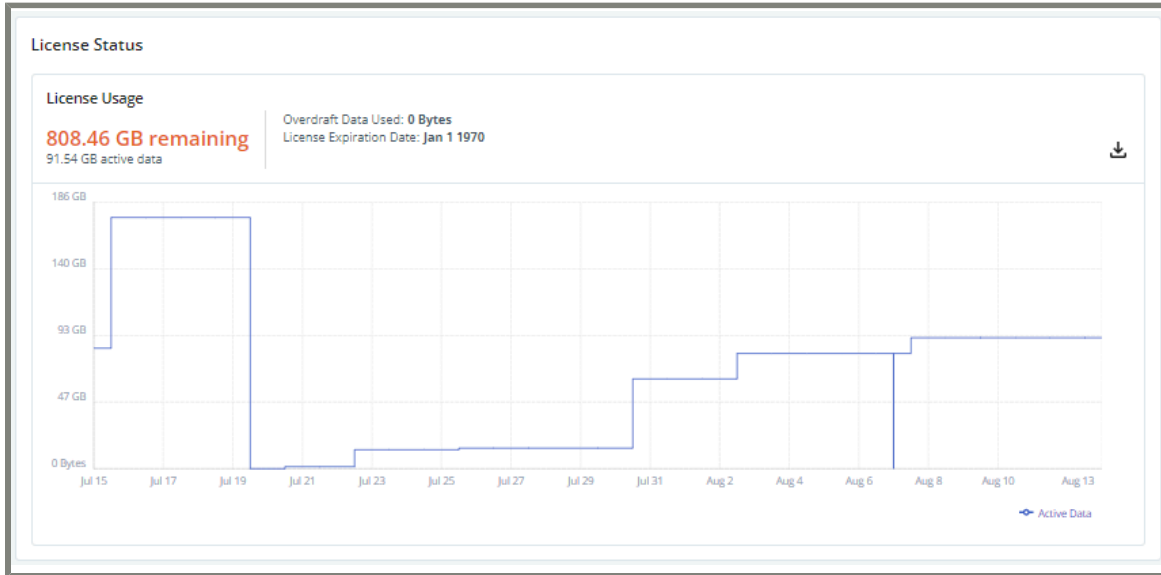
- License Details:** Shows 'License Server' as 'license-host.company.com' and 'This CyberSense Server' with 'Host: server1-blade10' and 'Engine ID: 3C:EC:EF:D9:70:74'.
- License Clients:** A table with columns 'IP ADDRESS', 'HOST', 'LAST CONTACT', and 'ROLE'. The table is currently empty, showing 'No rows'.
- Registration Options:** Two radio buttons are present: 'Create a License Server' (unselected) and 'Connect to a License Server' (selected).
- Registration Fields:** Includes 'License Server Host' (license-host.company.com), 'Username' (admin), 'Password' (masked with dots), and 'One-Time Password' (Enter One-Time Password).
- Buttons:** 'Cancel' and 'Register' buttons are located at the bottom right.

Moving to client/server licensing on existing engines

The purchased license is typically split on the Hitachi Vantara support portal across multiple engines and the split licenses are then installed locally on each engine.

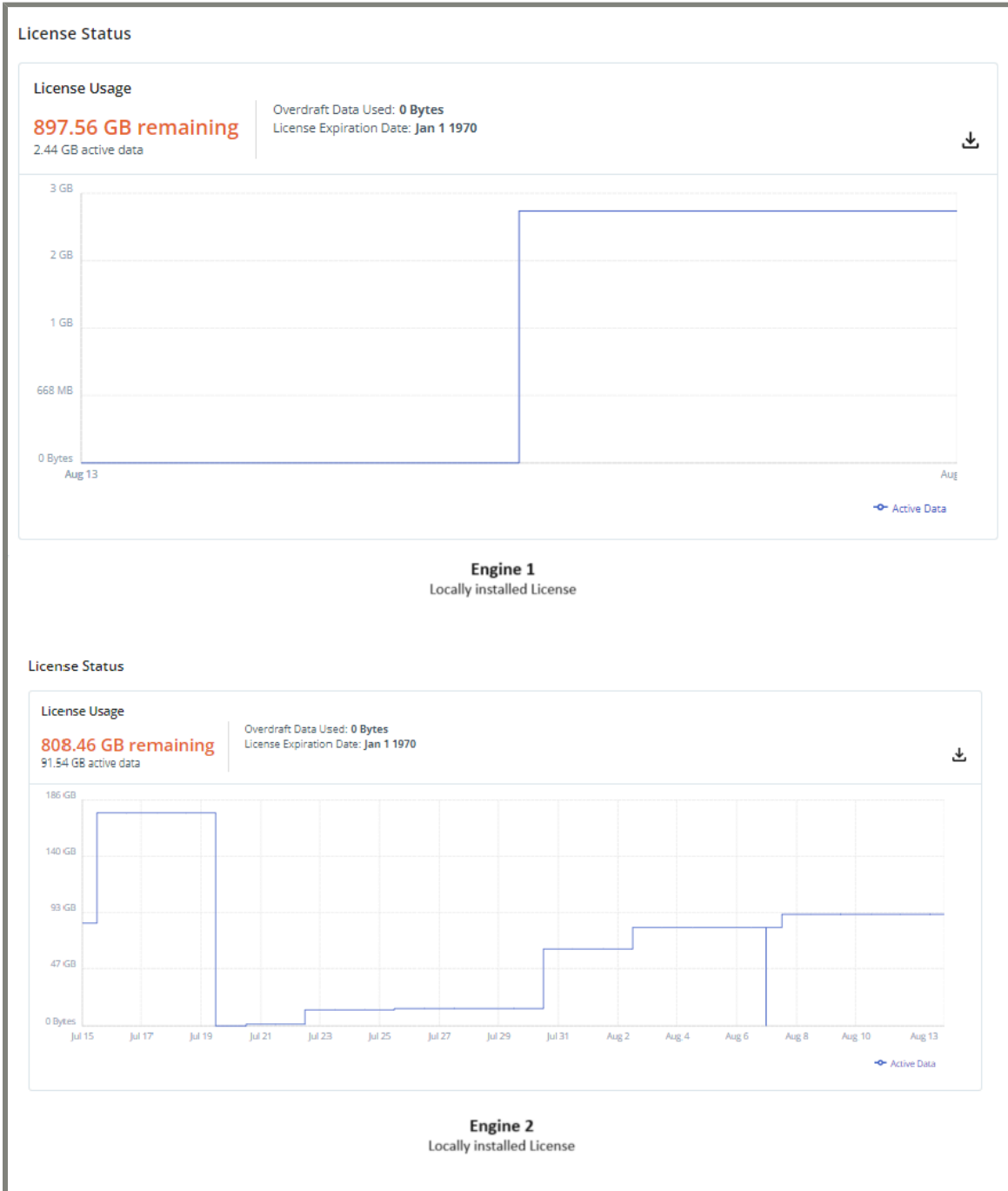
You also have the option to use a licensing model, which is a client/server approach to share licensing. An engine can function as a license server when it has a locally installed license. Other engines can register with the license server as clients for the licensing information, even if they have a locally installed license. The license sets the amount of data that can be active at any time. This concept is called Active Data. The amount of Active Data from the license server is fungible across all the license clients and the license server.

To review the Active Data amount on an engine, open the **License Management > License Status** page. In the simple example below, the engine is a standalone engine with a locally installed license. The license allocates 900GB of Active Data to this engine from the total purchased. The index on the engine has 91.54GB of Active Data and 808.46GB remaining Active Data in its license.

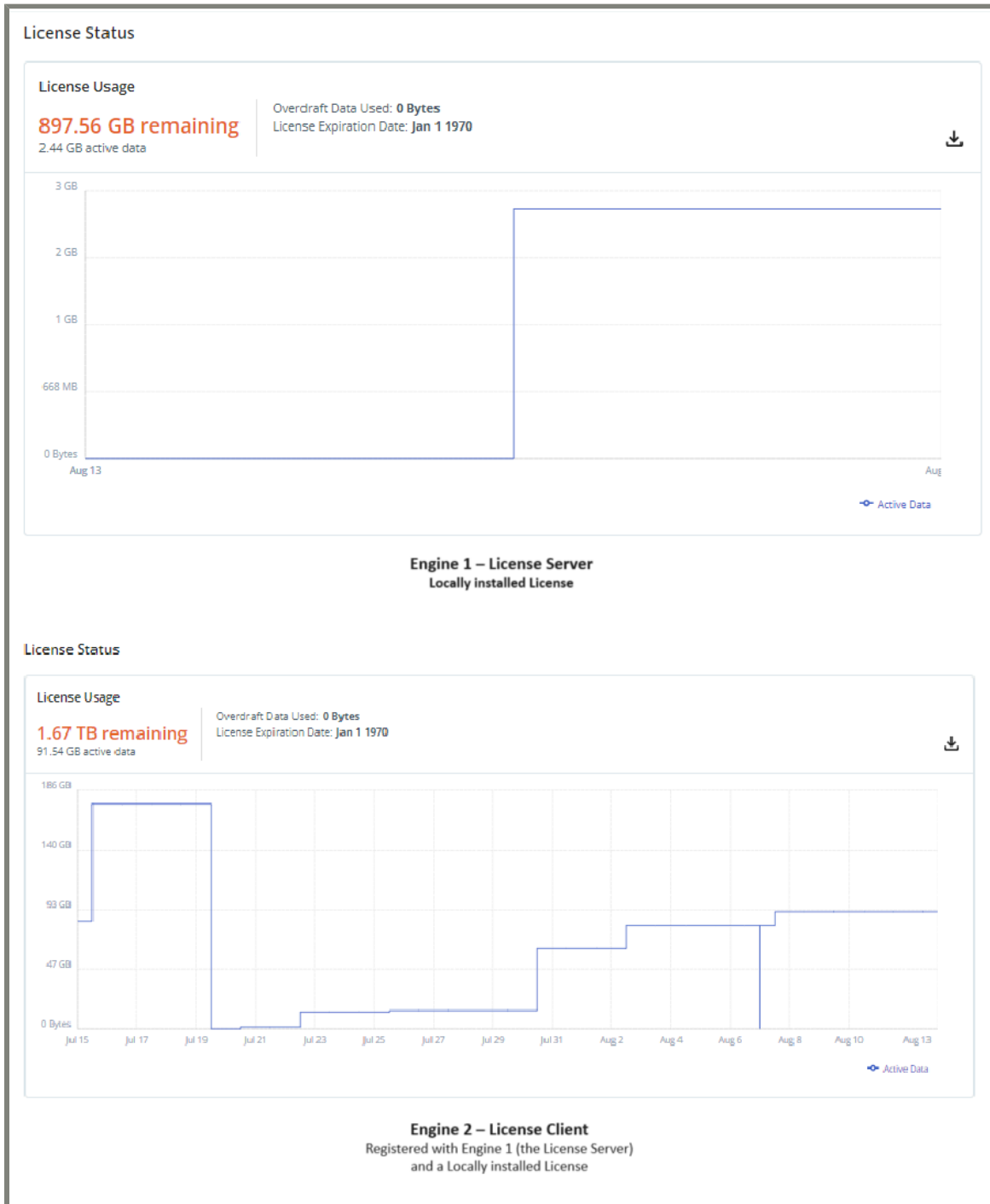


You can install licenses locally on each engine or choose to add Active Data using the client/server licensing model by designating an engine to function as the license server. When using the client/server licensing with engines that have locally installed licenses, the value for the remaining Active Data on the license client engines is the sum of the remaining Active Data on the engine's existing locally installed license and the remaining Active Data on the license server engine.

The first image shows the **License Status** panes for two engines each using a locally installed license. The remaining Active Data is displayed in the orange text.



The second image shows the **License Status** panes for two engines that share the license on the license server. Engine 1 is functioning as the license server and Engine 2 has a locally installed license and is registered as a license client with Engine 1. Note that the remaining Active Data for Engine 2 is the sum of the remaining Active Data values show above from both engines' licenses (1.67TB = 897.56GB + 808.46GB).



To calculate the amount of Active Data for the indexes of your engines, note the Active Data amount displayed in the **Settings > License Status** pane for each license server and client, and add them up for the total Active Data.

To calculate the amount of remaining Active Data for the license server and license clients, note the amount of remaining Active Data on each engine and add them up. Take the sum and subtract the remaining Active Data from the license server multiplied by the number of license clients.

For example, you have four engines with licenses locally installed on them as follows:

- a 6TB license for Engine 1 (E-1)
- a 5TB license for Engine 2 (E-2)
- a 5TB license for Engine 3 (E-3)
- a 4TB license for Engine 4 (E-4)

Each engine has the following amount of ActD and RAD:

Engine	Active Data in License	Active Data in Index	Remaining Active Data Shown
E-1	6TB	1TB	5TB
E-2	5TB	4TB	1TB
E-3	5TB	3TB	2TB
E-4	4TB	2TB	2TB

When you choose an engine to function as a license server, the remaining three engines can function as license clients. The license clients also have the locally installed licenses. The remaining Active Data displayed on each license client is a total of the remaining Active Data on the license server plus the remaining Active Data on the license client. This remaining Active Data is a pool that can be used by the license client.

For our example, we've designated E-1 as the license server and E-2 through E-4 are now license clients. They register with E-1 license server. The remaining Active Data shown on E-2 is 6TB, which is the sum of 5TB on E-1 and 1TB on E-2.

Engine	License Server or Client	Active Data in License	Active Data in Index	Remaining Active Data Shown	Remaining Active Data Label
E-1	Server	6TB	1TB	5TB	R ₁
E-2	Client	5TB	4TB	6TB (1TB + 5TB)	R ₂
E-3	Client	5TB	3TB	7TB (2TB + 5TB)	R ₃
E-4	Client	4TB	2TB	7TB (2TB + 5TB)	R ₄

To calculate the remaining Active Data for the license on E-1:

1. Add the remaining Active Data amounts from all the engines:

$$R_{\text{Total}} = R_1 + R_2 + R_3 + R_4$$

Example: 25TB = 5TB + 6TB + 7TB + 7TB

2. Multiply the remaining Active Data amount on the license server by the number of license clients:

$$R_{1 \times N} = R_1 \times N$$

Example: 15TB = 5TB x 3

3. Subtract the value found in step 2 from the total found in step 1:

$$R_{\text{Real}} = R_{\text{Total}} - R_{1 \times N}$$

Example: 10TB = 25TB - 15TB;

There is 10TB of remaining Active Data available from all licenses installed on the engines; 5TB from the license server is shared between all the engines.

Viewing the EULA

To view the EULA:

On the **Settings > License Management** page, select **EULA** to view the Hitachi Vantara EULA that was signed during the installation process. Scroll down the page to read all of the EULA.

End User License Agreement (EULA)

Please read this agreement (the "Agreement") carefully. It is a contract between your employer ("Licensee") and Index Engines ("Licensor") that governs the use of Licensor's software (the "Software"). It contains important terms that affect Licensee and its use of the Software, except to the extent all or any portion of the Software is the subject of a currently enforceable, written and separately signed agreement between Licensor, or resellers authorized by Licensor to enter into such agreements, and Licensee.

By clicking, "Accept" you agree to these terms, including the disclaimers herein, on behalf of Licensee, and represent that you have the authority to bind Licensee to these terms.

IF YOU DO NOT HAVE SUCH AUTHORITY, OR DO NOT AGREE TO THESE TERMS, YOU MAY NOT USE THIS SOFTWARE.

1. License Grant.
Licensor grants Licensee a personal, non-exclusive, non-transferable license to the Software, subject to the terms and conditions in this Agreement, and only for the uses enabled by any Licensor-supplied license keys.

2. Permitted Uses.
2.1. Installation. Licensee may install and use the number of copies of the Software for which Licensee has been granted a license.

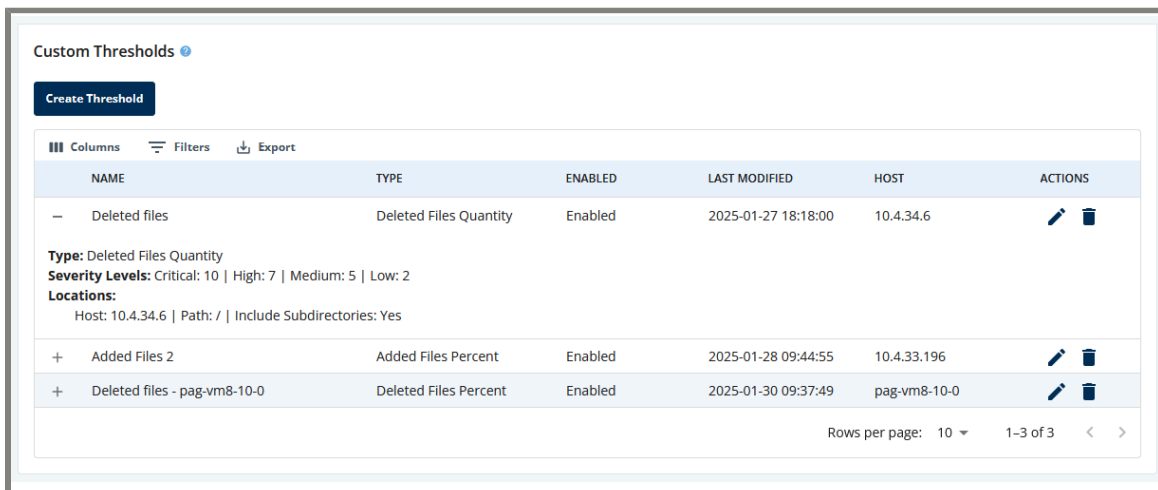
Advanced menu

The **Settings > Advanced** menu offers the following options:



- [Custom Thresholds \(on page 126\)](#) - configure threshold monitoring options.
- [Custom YARA rulesets \(on page 139\)](#) - manage YARA rulesets
- [Trusted Files \(on page 145\)](#) - add filename patterns to create a list of trusted files.
- [Recover from Backup \(on page 150\)](#) - recover files from a restored backup.
- [Global Feature Options \(on page 151\)](#) - set the custom YARA ruleset global control.

Custom Thresholds

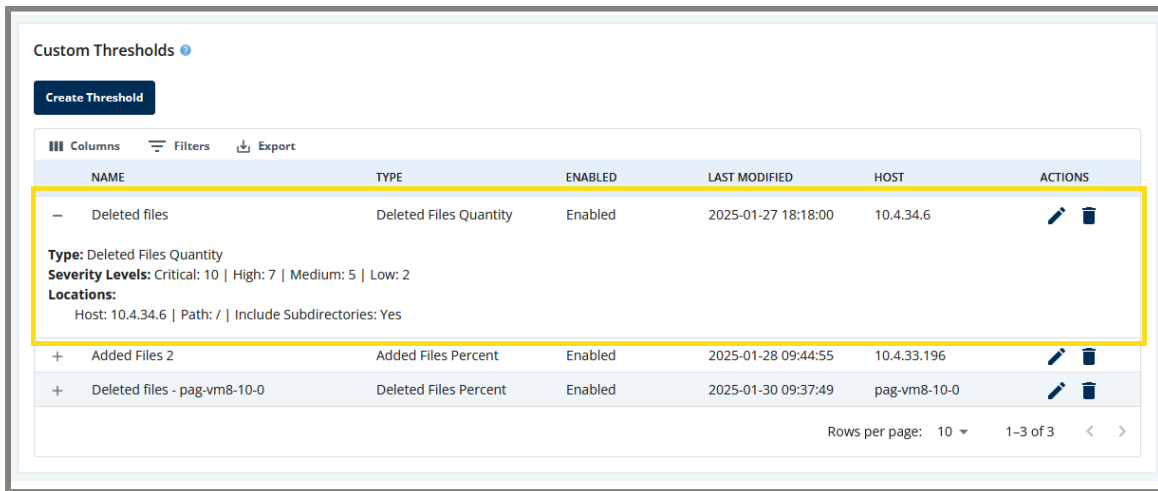
The **Settings > Advanced > Custom Thresholds** page displays the following information about the threshold definitions as well as the option to create new threshold definitions. Only the threshold definitions for the selected host will be displayed.



Column	Description
NAME	The name of the threshold definition.
TYPE	The type of change that the threshold definition monitors.
ENABLED	Indicates whether the threshold definition is enabled and be used by Ransomware Detection or not.
LAST MODIFIED	Indicates the last time the threshold definition was modified.
HOST	The host IP address or name that is monitored by the threshold definition.
ACTIONS	Indicates the actions that can be taken on the threshold definition, which are:

Column	Description
	Edit the threshold definition. See Editing a Custom Threshold (on page 131) for more information.
	Delete the threshold definition.

To view a threshold's configuration from the **Custom Threshold** page, select the **+** for a specific threshold. Multiple threshold definitions can be expanded at once. The threshold details are displayed below the threshold definition.




The screenshot shows the 'Custom Thresholds' interface. At the top, there is a 'Create Threshold' button and a table with columns: NAME, TYPE, ENABLED, LAST MODIFIED, HOST, and ACTIONS. The first row is 'Deleted files' with a yellow highlight around it. Below this row, the details for 'Deleted files' are expanded, showing 'Type: Deleted Files Quantity', 'Severity Levels: Critical: 10 | High: 7 | Medium: 5 | Low: 2', and 'Locations: Host: 10.4.34.6 | Path: / | Include Subdirectories: Yes'. Other rows include 'Added Files 2' and 'Deleted files - pag-vm8-10-0'.

Create custom threshold definitions to monitor activity on your hosts, which are defined as:

- **Custom Threshold** - defines a threshold at the granular level, which gives you the maximum flexibility for configuring alert thresholds.

You can create a **Custom Threshold** definition for the files and paths to monitor as well as define the type of changes to the files and set severity levels of the alerts. The files and directories typically monitored are important system files and folders that infrequently or never change. If the **Custom Threshold** definition for a change is exceeded between two snapshots, then an alert at the user-configured severity level is created immediately. The alerts are generated any time a **Custom Threshold** is reached with every scan of a host. View the graphs for a host's **Custom Threshold** definitions on **Hosts > View > Custom Thresholds**. Each configured severity level is indicated on the graphs with different color dashed lines. If you change the severity level values of the daily activity threshold, the lines will move to the new value. The previous value is no longer shown.

The change types that can be monitored are:

Change Type	Description
Added Files	The number of added files that has occurred between the last two snapshots analyzed by Ransomware Detection.
Changed or Deleted	The number of files that have content changed and/or the files have been deleted since the last snapshot analyzed by Ransomware Detection. This monitors a comprehensive change to the files or folders, combining deletions and file content changes.
Changed File Type	<p>The amount of files in a previous snapshot that have a different file type in the current snapshot.</p> <div data-bbox="472 751 1464 982" style="border: 1px solid gray; padding: 5px;">  Note: When you configure a Daily Activity or custom threshold for Changed File Type, the threshold will consider Trusted and Unknown to be the same file type. However, a file of unknown type that matches the filename pattern under Settings > Advanced > Trusted Files will still appear as Trusted in the Alerts > Show Files table. </div>
Deleted Files	The number of deleted files that has occurred between the last two snapshots analyzed by Ransomware Detection.
Entropy	Entropy represents the randomness of data in a file and generally indicates file encryption, Encrypting a file typically increases the file's entropy. The entropy value in this graph ranges from 0 (no entropy) to 100 (maximum entropy).

Set a threshold definition of each kind per host - **Added Files**, **Changed or Deleted** files, **Changed File Type**, **Deleted Files**, and Entropy - and the severity levels for each threshold alert. A Ransomware Detection job may generate one or more threshold alerts for a particular host.

Creating a Custom Threshold

To configure a custom threshold:

1. On the **Settings > Advanced > Custom Thresholds** page, select **Create Threshold**.

Custom Thresholds

Create Threshold

Columns Filters Export

NAME	TYPE	ENABLED	LAST MODIFIED	HOST	ACTIONS
- ENT-torphy	Entropy	Enabled	2024-10-25 12:33:34		
Type: Entropy Severity Levels: Critical: 10 Locations: Host: Path: /download Include Subdirectories: No Host: Path: /main Include Subdirectories: No Host: Path: /* Include Subdirectories: No					
+ Changed quantity	Changed Or Deleted Files ...	Enabled	2024-10-30 19:30:42	kama.indexengines.c...	
+ abcdef	Added Files Quantity	Enabled	2024-11-18 10:53:08	kama	
+ let me go homes	Added Files Quantity	Enabled	2025-01-28 13:19:00	bern.index	
+ let me go homeee	Changed File Type Percent	Enabled	2025-01-28 13:20:00	bern.index	
+ jeff's threshold	Changed Or Deleted Files ...	Enabled	2025-01-28 17:02:14	kama.indexengines.c...	
+ jeff_dnm	Changed Or Deleted Files ...	Enabled	2025-02-08 13:51:41	*	
+ jeff_dnm_w_hostname	Changed File Type Quantity	Enabled	2025-02-08 13:59:50	dnvm.test.indexengin...	
+ jeff_test	Added Files Quantity	Enabled	2025-02-09 18:36:54	*	
+ dnmv_test20	Changed Or Deleted Files ...	Disabled	2025-02-13 15:46:29	*	

Rows per page: 10 1-10 of 10

2. The **New Custom Threshold** page appears. Toggle **Enable Alert Threshold** to enable generating alerts when the daily activity limit has been reached. By default, this option is enabled.

Custom Thresholds

Custom Thresholds > New Custom Threshold

Enable Threshold

Name: Type: Data Format:

Severity Levels



Critical High Medium Low

Locations

Host: Path: Include Subdirectories

Add Location +

3. Configure the following information:

Field	Description
Threshold Name	<i>Required.</i> The name for the threshold definition. It is helpful to use a name that will describe the threshold type, such as "Deleted Files - 10 Percent - Finance Servers". This way, you can see at a glance which threshold has been exceeded and on what host.
Type	The change type to be monitored by the threshold: <ul style="list-style-type: none"> ◦ Added Files ◦ Changed or Deleted ◦ Changed File Type ◦ Deleted Files ◦ Entropy
Data Format	The number of files affected by the change type as a percentage or quantity. Select Quantity or Percentage . <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Note: For Entropy, the only option is Percentage. </div>
Severity Levels	Set a value for each severity level that you want to use. At least one severity level must be set. The value must decrease for each level, which are: <ul style="list-style-type: none"> ◦ Critical ◦ High ◦ Medium ◦ Low <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Note: A Threshold Exceeded alert will be triggered when the number or percentage of changed files is greater than the value set for a severity level. </div> <p>For example, you created a custom threshold for a percent of deleted files and want to be alerted when more than 20%, 15%, 10%, and 5% of your files have been deleted. Set the severity levels as follows:</p> <ul style="list-style-type: none"> ◦ Critical to 20 ◦ High to 15 ◦ Medium to 10 ◦ Low to 5 <p>If more than 5% of your files are deleted, an alert with the severity level of Low will be generated.</p>

Field	Description
Minimum	Only available for the Entropy change type. This is the minimum entropy that the configured percentage of files must be for an alert to be generated. Example: if you have set Value to 20% and Minimum to 90 , then more than 20% of the files must have an entropy of more than 90 to generate an alert.

4. To add a specific host, select **Add Location**. Add the following information:

Field	Description
Host	The name or IP address of the host that you want to monitor for changes. See Hosts and Paths (on page 134) for more information.
Path	The path can be a directory or a path to a file. This is defined relative to the snapshot. See Hosts and Paths (on page 134) for more information.
Include Subdirectories	The threshold is applied to the host and path and any exiting subdirectories to analyze the files for changes.

Select **Add Location +** to add more locations to the threshold.

5. Select **Save Changes** when complete.


Editing a Custom Threshold


To edit a **Custom Threshold**:

1. On the **Settings > Advanced > Custom Threshold** page, select the **Edit** icon.

2. The **Edit Custom Threshold** page appears. Toggle **Enable Alert Threshold** to enable/disable generating alerts when the daily activity limit has been reached. If you want to delete the **Custom Threshold**, select **Delete**.

3. Edit the following information:

Field	Description
Threshold Name	<i>Required.</i> The name for the threshold definition. It is helpful to use a name that will describe the threshold type, such as "Deleted Files - 10 Percent - Finance Servers". This way, you can see at a glance which threshold has been exceeded and on what host.
Type	The change type to be monitored by the threshold: <ul style="list-style-type: none"> ◦ Added Files ◦ Changed or Deleted ◦ Changed File Type ◦ Deleted Files ◦ Entropy
Data Format	The number of files affected by the change type as a percentage or quantity. Select Quantity or Percentage . <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Note: For Entropy, the only option is Percentage. </div>

Field	Description
Severity Levels	<p>Set a value for each severity level that you want to use. At least one severity level must be set. The value must decrease for each level, which are:</p> <ul style="list-style-type: none"> ◦ Critical ◦ High ◦ Medium ◦ Low <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  Note: A Threshold Exceeded alert will be triggered when the number or percentage of changed files is greater than the value set for a severity level. </div> <p>For example, you created a custom threshold for a percent of deleted files and want to be alerted when more than 20%, 15%, 10%, and 5% of your files have been deleted. Set the severity levels as follows:</p> <ul style="list-style-type: none"> ◦ Critical to 20 ◦ High to 15 ◦ Medium to 10 ◦ Low to 5 <p>If more than 5% of your files are deleted, an alert with the severity level of Low will be generated.</p>
Minimum	<p><i>Only available for the Entropy change type.</i> This is the minimum entropy that the configured percentage of files must be for an alert to be generated. Example: if you have set Value to 20% and Minimum to 90, then more than 20% of the files must have an entropy of at least 90 to generate an alert.</p>

4. For a location , edit the following information:

Field	Description
Host	The name or IP address of the host that you want to monitor for changes. See Hosts and Paths (on page 134) for more information.
Path	The path can be a directory or a path to a file. This is defined relative to the snapshot. See Hosts and Paths (on page 134) for more information.
Include Subdirectories	The threshold is applied to the host and path and any exiting subdirectories to analyze the files for changes.

Select **Add Location +** to add more locations to the threshold.

5. Select **Save Changes** when complete.

Hosts and Paths

To define a location in the Ransomware Detection UI, you need a few pieces of information, two of which are the front-end host and the path where the directory or files are located. This information is used in the **Host** and **Path** field when creating a custom threshold definition. The front-end host is defined with either the name or IP address. A path is a text string that typically starts with a slash / and specifies a path and a file name or just a path to a folder. The leading slash is not required in the **Path** field.

This section describes how to:

- break down the text string into its various components
- escape special characters in the text string for a path or special files
- use wildcard characters to match one or more hosts or paths
- indicate system folders in the path
- describe additional special situations



Note: Many of the examples that follow are Linux-based path syntax unless otherwise specified. Forward and backward slashes can be used interchangeably in a path. They are interpreted correctly by the Ransomware Detection software as a Windows or Linux path.

Host

The **Host** field is specified in the threshold definition when you are creating alert thresholds on the **Hosts** page. In this example, the threshold definition specifies the host that was indexed in the snapshot. The **Host** can be entered in the **Host** field as:

```
exch1.example.com
```

The host can be entered as `exch1.example.com` or the IP address of the host, such as `192.168.192.192`. The host must match what was indexed in the snapshots.



Note: For VMFS datastore snapshots, the hostname may be a VM name given by the VM host and could be different from the VM's DNS name. In other cases, the hostname may be the Ransomware Detection policy name.

Path to a folder

A **Path** specifies where a directory or file is located. This example is a Linux-based path to a folder. The **Path** text string is:

```
/Documents/BobSmith/marketing/Jan2024
```

This example path ends at a folder because a file with that name was not found.

Component	Description
Documents/	A folder name.
BobSmith/	A folder name under the Documents folder.
marketing/	A folder name under the BobSmith folder.
Jan2024	A folder name.

Path to a file

Specifying a path to a file is done by ending the path text string with the file name and extension. The following is a Linux-based path to a file.

```
/Dave_Smith/Documents/file01.txt
```

The **Path** string can be broken down into the following components:

Component	Description
Dave_Smith/	A folder name.
Documents/	A folder name under the Dave_Smith folder.
file01.txt	The file name that you want to monitor for any activity.

Path to a Windows drive

When accessing a specific drive on a Windows system, in the **Path** field, use the following syntax followed by the remaining path:

```
/<drive_letter>:/
```

Where *<drive_letter>* is the specific drive on the Windows system. An example of specifying the Windows drive letter and a path is:

```
/C:/Users/JSmith
```



Note: Some indexing methods do not use the drive letter designation. For VMFS datastore snapshots, the drive letter may be replaced by a drive UUID and a partition or file system UUID.

Escaping special characters in the path

File and folder names can contain special characters but these characters must be handled correctly for the path to be interpreted properly. When a special character is in a folder name, use the pipe | character before it. For example, a folder is named **Sales/Marketing**. If the slash / is not escaped by adding the pipe | in front of it, the folder is seen as a **Sales** folder that contains a subfolder named **Marketing**. Escape slashes, when the character is not used as a folder separator, such as when the character is part of a folder name and not the delimiter between folders.

To interpret **Sales/Marketing** as the name of a folder, enter it in the **Path** field as:

```
Sales|/Marketing
```

The folder is now interpreted as a single folder named **Sales/Marketing**.

The special characters that must be escaped are:

Field	Special Characters
Host	<ul style="list-style-type: none">• /• \• • :
Path	<ul style="list-style-type: none">• /• \• • >

Another example is when a file or folder name contains the pipe | character, `folder|name`. To correctly format this folder name in the **Path** field, use a preceding pipe to escape the pipe | character in the folder name:

```
folder||name
```

Using wildcards

Wildcard characters can be used in the **Path** field for **Custom Threshold** definitions. The valid wildcard characters are:

- * - the asterisk; use it to match one or more characters.
- ? - the question mark; use it to match a single character.



Note: Using wildcards are more computationally expensive than specifying a slash / and selecting the **Include Subdirectories** option, which specifies to monitor all paths on the host.

The following are valid paths to specify a threshold definition, which will monitor all the paths found on a host:

- *
- /*
- / and select **Include Subdirectories**. This is the best option for performance.

Using a system folder in the path

Specifying a path to a system folder is handled differently than other folder types. The system folder is indicated by the pipe | and then **S**. This character combination is interpreted as a system folder.

```
/RMAN:|S/18/XE
```

The **Path** string is broken down into the following components:

Component	Description
RMAN: S/	A system folder name for an Oracle database, which is indicated by the s terminator.
18	A folder under the system folder.
XE	A folder under the 18 folder.

Specifying a path in a VMFS datastore snapshots

To specify a path for a VMDK, use the disk UUID, the partition UUID and the specific path to specify the VMDK and path in the **Path** field:

```
/By Device|S/<disk_uuid>/<partition_uuid>/<path_to_files>/<file_name>
```

You can specify either a path to a folder or a specific file name. Contact your IT professional or system administrator to obtain the disk and partition UUIDs.

For example, the file `/bin/file01.txt` on the host `examplehost.com` is listed in a in a VMFS datastore snapshot and indexed by Ransomware Detection. The disk has a UUID of `6000C29f-aa7a-0d31-ec39-f702758` and the partition that the file is located in has a UUID of `7EB48F74B4DF2D81`. To specify the path correctly, type:

```
/By Device|S/6000C29f-aa7a-0d31-ec39-f702758/7EB48F74B4DF2D81/bin/file01.txt
```

If you want to define the threshold at the host level, specify the host in the **Host** field and type `/` in the **Path** field. This will monitor all the folders and files on the host.

Specifying a path for a block device

To specify a threshold definition to monitor a path to a directory on a block device, use the following in the **Path** field:

```
*/<path-to-directory>
```

Additionally, to specify the threshold definition to monitor all paths on a block device, use the following in the **Path** field:

```
*
```

Specifying a location

At times, you need to specify a location of a filename of an attachment or This example describes the text string in a **Location** field when you need to specify a service root and the filename of an attachment. The string is:

```
exch1.example.com:exchange/DSmith/Recoverable Items|S/08294367ac73b35f|
>documents.zip|:1|>My Documents/
```

The path can be broken down to the following components and component separators as shown in the following table.

Component	Description
exch1.example.com	The hostname . Every path begins with the hostname and ends with a colon : or forward slash /.
exchange	The service root . If the hostname was terminated by a colon, then the next path component is the name of an application service hosting the data. If the hostname was terminated by a slash, then the rest of the path indicates files in the filesystem of that server.
DSmith	A folder name . In this case, it represents an Exchange mailbox.
Recoverable Items	A folder name . The “ S” terminator indicates that this folder is a hidden, system folder. In this case, it is a folder managed by Exchange and is in a distinct name space from other folders “Dave Smith” may have created in his mailbox. It is not visible to the user.
08294367ac73b35f	The filename of an Exchange email message. If this path component is terminated with >, then it is a filename, as in this case. If it is terminated by a forward slash /, then it is a folder name.
documents.zip	The filename of the attachment. This example has a suffix of :1 which is the attachment disambiguation number. In this case, it indicates that this is the second attachment with the name documents.zip. The two files may contain different content, but happen to have the same filename. The > terminator indicates that it is a filename, not a folder.
My Documents	A folder name , which, in this case, is contained inside documents.zip

Specifying a location on a Windows drive

This example describes a text string to specify a location on a Windows drive:

```
exch1.example.com/C:\exchange\First Storage Group\Mailbox Store\priv1.edb|>Dave
Smith/Sales|/Marketing/
```

The above example breaks down the components similar to the previous example, but ultimately points to a folder located on a file system instead of a path to a folder originating from an application, such as Exchange.

Component	Description
exch1.example.com	The hostname . This example ends with a slash.
C:	A drive name .
exchange	A folder name under C: drive.
First Storage Group	A folder name under the exchange folder.
Mailbox Store	A folder name under the First Storage Group folder.
priv1.edb	The filename . The path component terminator > indicates that it is a filename.
Dave Smith	A folder name , which is a mailbox in this case.
Sales/Marketing	A folder name under Dave Smith. This folder has a slash in its name and that is escaped by the pipe followed by a slash /.

Custom YARA rulesets

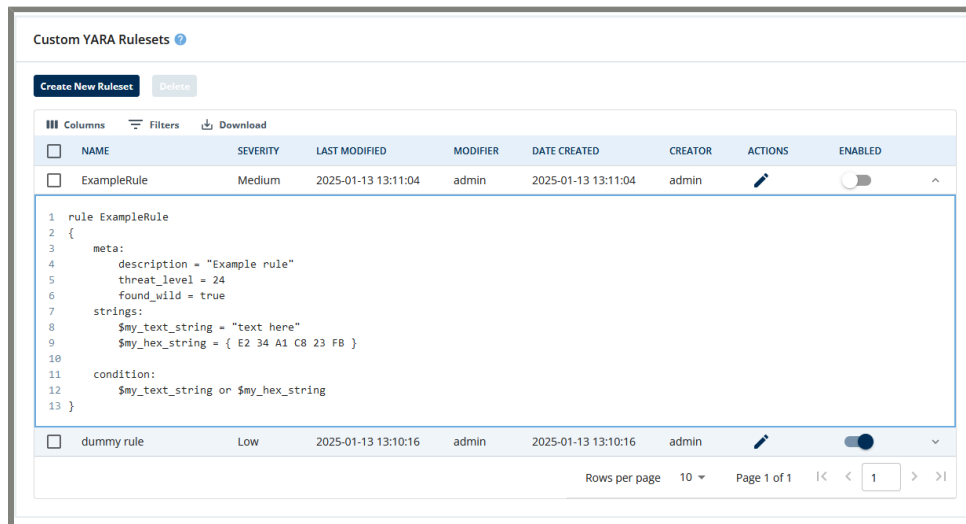
Add custom YARA rulesets to detect possible malware on your front end hosts' PE32 files using a set of pattern-matching rules. A YARA rule is a single entity, while a YARA ruleset is a set of rules in a YARA definition file, which can contain one or more YARA rules. YARA rules are customizable specifications that look for patterns in files and file content to identify and classify malware before a cyber attack. The rule is typically comprised of two sections: a `strings` definition and `condition` logic. They can be very simple, as seen in the included examples, or very complex depending on your requirements, and include a `metadata` section describing the custom rule. Use regular expressions, hexadecimal or text strings, XOR strings, etc., when defining the strings in a rule. Conditions are essentially Boolean expressions and if true, a match was found to the pattern defined in the `strings` section. For more information on YARA rules and usage, go to the official YARA online documentation at <https://yara.readthedocs.io/en/stable/index.html>.



Note: YARA rulesets only apply to PE32 files at this time.

Ransomware Detection applies the custom YARA ruleset while reading the file content on the host during indexing when a policy job is run.

Select **Settings > Advanced > Custom YARA Rulesets** to manage existing rules and create new ones.



Example – Simple text YARA ruleset

This example shows a simple YARA ruleset that will return true if the text defined in `$my_text_string` or the hexadecimal characters in `$my_hex_string` are found.

```
rule ExampleRule
{
  meta:
    description = "Example rule"
    threat_level = 24
    found_wild = true
  strings:
    $my_text_string = "text here"
    $my_hex_string = { E2 34 A1 C8 23 FB }

  condition:
    $my_text_string or $my_hex_string
}
```

Example – Counting the number of occurrences of a string

This second example shows a ruleset that counts the number of times a string occurs in a file.

```
rule CountExample
{
  strings:
    $a = "dummy1"
    $b = "dummy2"

  condition:
    #a == 6 and #b > 10
}
```

In this example, the condition is met if `dummy1` occurs exactly six times and `dummy2` occurs more than 10 times.

Creating a YARA ruleset

To create a custom YARA ruleset:

1. On the **Settings > Advanced > Custom YARA Rulesets** page, select **Create New Ruleset**.

This opens the **YARA Ruleset Creator**. Do the following:

- **Enable Ruleset** - select to enable/disable the ruleset after it's been created. When disabled, it will not be used by Ransomware Detection during indexing.
- **Select Ruleset** - open a ruleset definition file, which can contain one or more rules. The supported file types are `.yar` and `.yara`. The YARA ruleset from the file will be displayed in the editor pane for further editing if needed.
- **Ruleset Name** - type a user-friendly name for the ruleset. The ruleset name guidelines are:
 - Restricted name length - between 3 and 128 characters inclusively.
 - There are no character limitations; all special characters can be used and the name can start with a digit.



Note: The guidelines for the YARA rule name in the ruleset are slightly different. See <https://yara.readthedocs.io/en/stable/index.html> for more information on the restrictions for YARA rule names.

- **Alert Severity** - select an alert severity from the dropdown list. The available options are:

- **Critical**
- **High**
- **Medium**
- **Low**

See [The Alerts table \(on page 17\)](#) for more information on alert severity in the **Alerts** table.

- Alternatively, add the YARA ruleset text in the editor pane.
2. After adding a YARA ruleset, select **Verify**. If the ruleset cannot be verified, you will receive an error. Fix the error and verify the ruleset again. **Verify** is useful when you are developing the ruleset in the editor pane and want to verify your progress. You can also verify the ruleset when you select **Submit Ruleset**.
 3. When the ruleset has been verified, select **Submit Ruleset**. If you selected a YARA ruleset from a file, the file will now be uploaded.

When you create at least one ruleset, Ransomware Detection will index all PE32 file during the next indexing operation. Ransomware Detection checks the PE32 files against the newly added YARA ruleset.

Editing a YARA ruleset

To edit a custom YARA ruleset:

1. On the **Settings > Advanced > Custom YARA Rulesets** page, select the **Edit** icon for an existing YARA ruleset.

This opens the **YARA Ruleset Editor**. Edit any of the following:

- **Enable Ruleset** - select to enable/disable the ruleset for indexing.
 - **Replace Ruleset** - select a ruleset file. The supported file types are `.yar` and `.yara`. The uploaded YARA ruleset will be displayed in the editor pane for further editing if needed.
 - **Ruleset Name** - the name for the ruleset.
 - **Alert Severity** - the alert severity from the available options.
 - Edit the YARA ruleset text in the editor pane.
2. After editing a YARA ruleset, select **Verify**. If the ruleset cannot be verified, you will receive an error. Fix the error and verify the ruleset again. **Verify** is useful when you are developing the ruleset in the editor pane and want to verify your progress. You can also verify the ruleset when you select **Submit Ruleset**.
 3. When the ruleset has been verified, select **Submit Ruleset**. If you selected a YARA ruleset to upload, the file will now be uploaded.

When you modify at least one ruleset, Ransomware Detection will index every PE32 file during the next indexing operation, regardless of whether the files have changed or not. Ransomware Detection checks the PE32 files against the newly updated YARA rulesets.

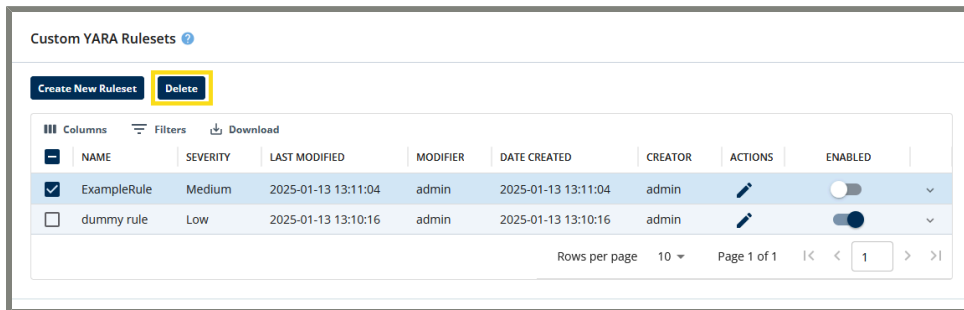
Deleting a YARA ruleset

There are two places from which you can delete a YARA ruleset:

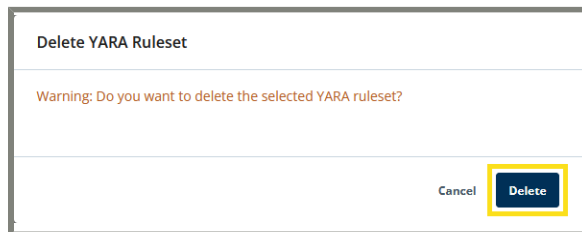
- the **Custom YARA Rulesets** page
- in the **YARA Ruleset Editor** page

Deleting a YARA ruleset on the Custom YARA Rulesets page

1. On the **Settings > Advanced > Custom YARA Rulesets** page, select a single or multiple existing YARA ruleset(s).



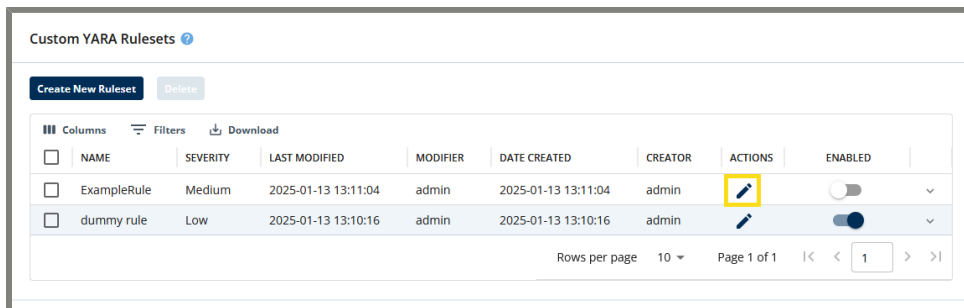
2. Select **Delete**. When prompted to confirm the deletion, select **Delete** in the confirmation window.



Deleting a YARA ruleset in the editor

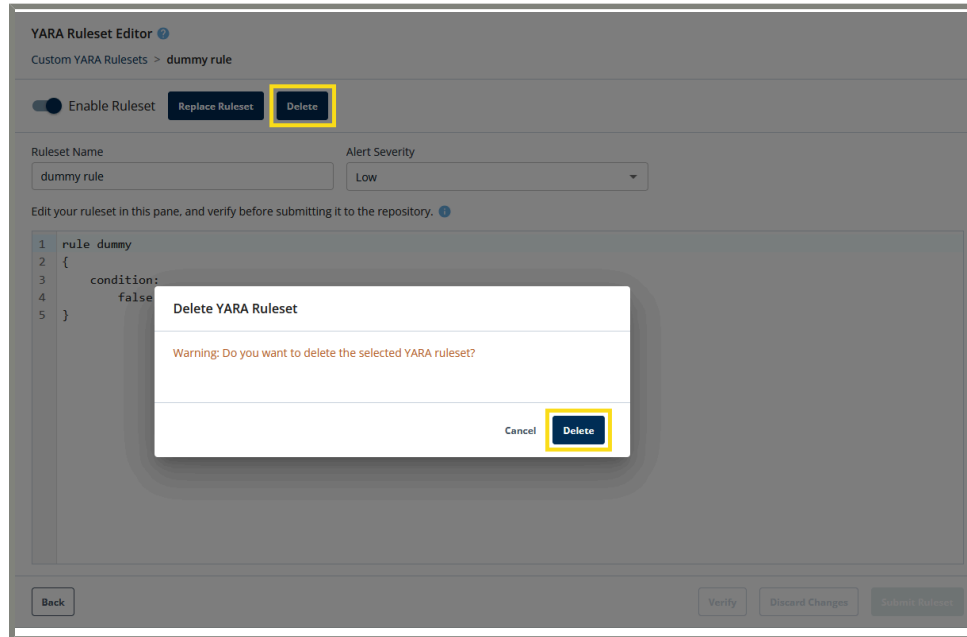
To delete a custom YARA ruleset from the **YARA Ruleset Editor** page:

1. On the **Settings > Advanced > Custom YARA Rulesets** page, select the **Edit** icon for an existing YARA ruleset.



This opens the **YARA Ruleset Editor**.

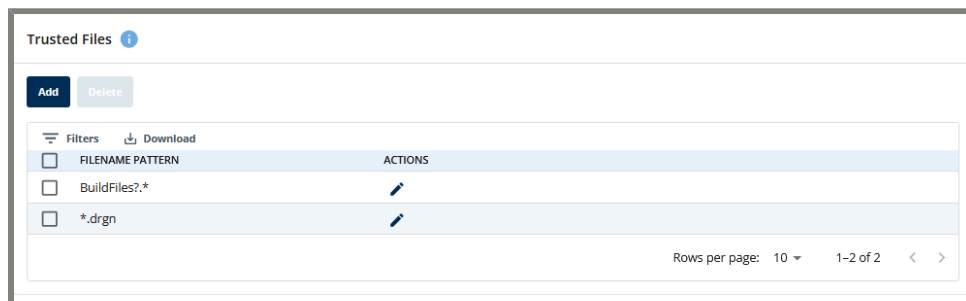
2. Select **Delete**. When prompted to confirm the deletion, select **Delete** in the confirmation window.



Trusted Files

The **Trusted Files** feature uses user-configurable filename patterns to categorize files that are unknown to Ransomware Detection as trusted files. During analysis, Ransomware Detection identifies the type of each file based on its content. If Ransomware Detection cannot identify the file type — e.g., a proprietary file format for an internally developed application — then it considers the file may be corrupted, which is one of many factors that can contribute to an **Infection Found** alert.

If Ransomware Detection is generating **Infection Found** alerts when there is no data corruption, use the **Trusted Files** feature to change the type of files that match a filename pattern. The filename patterns are filters that use alphanumeric characters and two wildcard characters, which are the asterisk * and the question mark ?. When Ransomware Detection encounters a file of an unknown type and it matches a filename pattern, Ransomware Detection will consider the file type as known and trusted. This reduces the possibility of incorrect **Infection Found** alerts.



File types are displayed when **Show Files** is selected on an alert in the **Alerts** table on the **Alerts** page. See [Suspect files list \(on page 24\)](#) for more information. File types that Ransomware Detection identifies as unknown but they match to a trusted filename pattern in the **Trusted Files** list are labeled **Trusted**. File types that Ransomware Detection identifies as unknown are labeled as **Unknown**.

The **Alerts > Show Files** table indicates the status of the files at the time that Ransomware Detection generated the alert. Subsequent changes to the **Trusted Files** patterns only affect future Ransomware Detection analyses.

Creating a trusted filename pattern

To create a filename pattern for a list of trusted files:

1. Go to **Settings > Advanced > Trusted Files**.
2. Select **Add**. In the displayed pane, type the filename patterns, separating them with **Enter**.



Note: Filename patterns are case-sensitive.

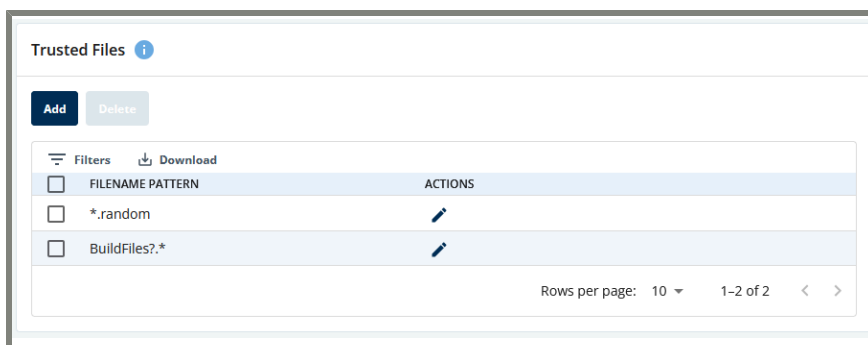
Select **Save** when done.

The filename patterns are displayed. Any files matching those patterns are recognized as trusted files by Ransomware Detection.

Editing a trusted filename pattern

To edit a trusted filename pattern:

1. Go to **Settings > Advanced > Trusted Files**.



2. Select the **Edit** icon for the filename pattern to edit. In the displayed pane, edit the pattern. When done, select **Save**. The edited pattern is displayed in the list.

Dialog box titled "Edit Filename Pattern" with a close button (X). The text "Edit the filename pattern." is displayed above a text input field containing "*.random?". At the bottom right, there are "Cancel" and "Save" buttons.

Deleting a trusted filename pattern

To delete a trusted filename pattern:

1. Go to **Settings > Advanced > Trusted Files**.

Trusted Files settings page showing a table of filename patterns. The table has columns "FILENAME PATTERN" and "ACTIONS". Two rows are listed: "BuildFiles?*" and "*.drgn". The "ACTIONS" column contains edit icons for both rows. Below the table, it says "Rows per page: 10" and "1-2 of 2".

2. Select the pattern to delete and then select **Delete**.
3. In **Delete Filename Pattern(s)**, select **Delete** to confirm.

Dialog box titled "Delete Filename Pattern(s)" with a close button (X). The text "Warning: Do you want to delete the selected filename pattern(s)?" is displayed in orange. At the bottom right, there are "Cancel" and "Delete" buttons.


The pattern is removed from the list.

Trusted Files settings page showing the table after deletion. The table has columns "FILENAME PATTERN" and "ACTIONS". One row is listed: "BuildFiles?*" with an edit icon in the "ACTIONS" column. Below the table, it says "Rows per page: 10" and "1-1 of 1".

Global Resets


Select **Settings > Advanced > Global Resets** to reset several system-level features, which includes:

- resetting existing YARA rulesets
- resetting existing thresholds

 **Warning:** Resetting any of these features cannot be reversed.

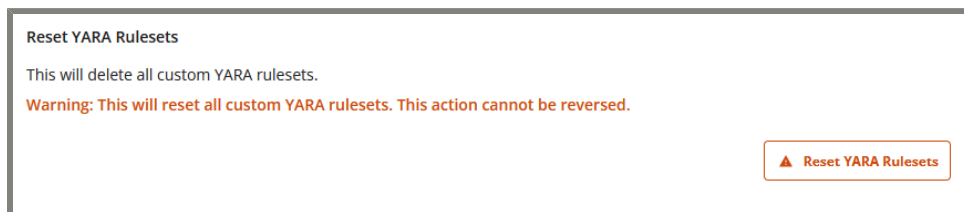
Resetting YARA rulesets


Reset the YARA rulesets to delete any existing YARA rulesets.

 **Warning:** Resetting the YARA rulesets will delete all existing YARA rulesets. This action cannot be reversed.

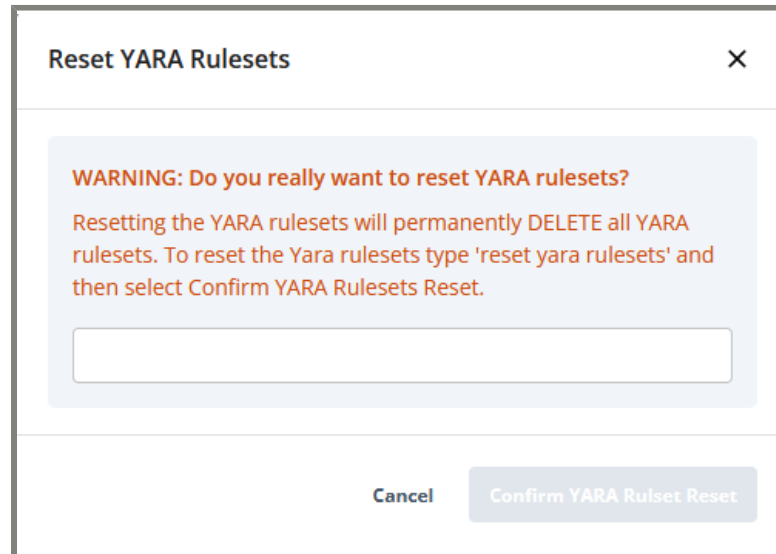
To delete the YARA rulesets:

1. Go to **Settings > Advanced > Global Resets**.
2. To delete existing YARA rulesets, select **Reset YARA Rulesets**.



 **Warning:** This action cannot be reversed.

- To confirm the deletion of the existing YARA rulesets, type **reset yara rulesets** and then select **Confirm YARA Ruleset Reset**.



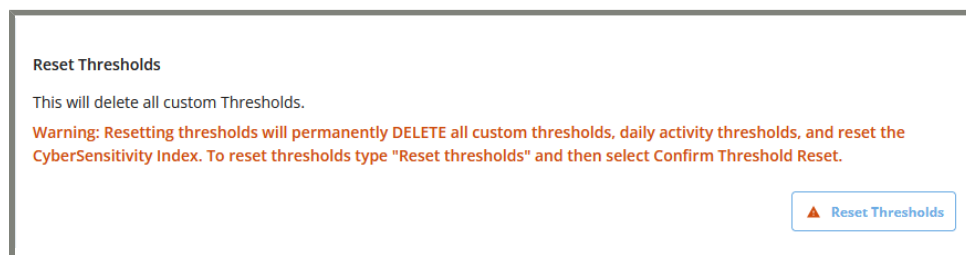
Resetting custom and daily activity thresholds

Reset the thresholds to delete any existing **Custom Thresholds** and **Daily Activity** thresholds.

Warning: Resetting the thresholds will delete all existing thresholds. This action cannot be reversed.

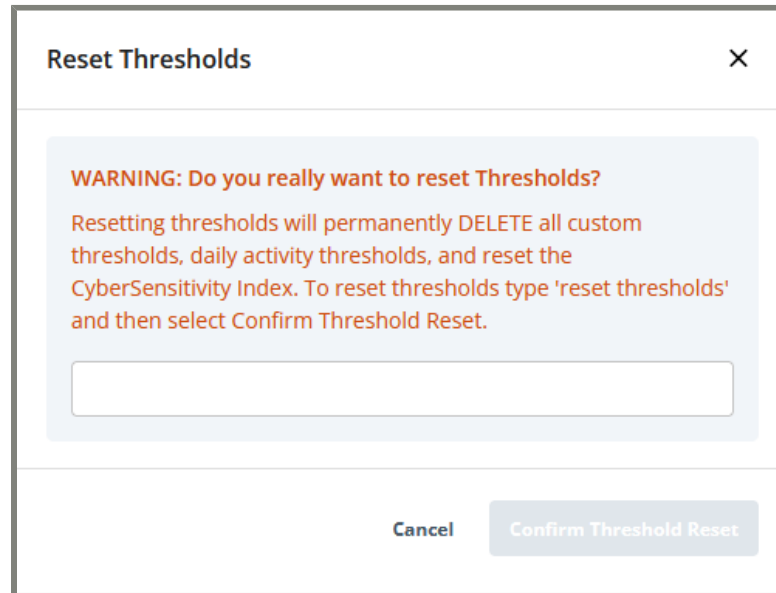
To delete the thresholds:

- Go to **Settings > Advanced > Global Resets**.
- To delete existing thresholds, select **Reset Thresholds**.



Warning: This action cannot be reversed.

3. To confirm the deletion of the existing thresholds, type **reset thresholds** and then select **Confirm Threshold Reset**.



Recover from Backup

Use the **Recover from Backup** page to recover the restored files from a backup. The process is:

- take a backup of your Ransomware Detection server using a third-party application. This is usually done as a scheduled procedure or prior to higher risk maintenance of the server.
- restore the backup file to a temporary location, `/opt/ie/backup` on your Ransomware Detection server. This step is performed using the same third-party application that created the backup.



Note: The default location of `/opt/ie/backup` must be used to restore and recover the files.

- recover the files using the Ransomware Detection UI to make the files active again.

Follow the procedures in the *Hitachi Vantara Ransomware Detection powered by CyberSense® Backup, Restore, and Recovery Guide* to back up the Ransomware Detection configuration files, indexes, databases, log files, and license files and then restore the files into a temporary location. After the files are restored, use the [Recovering files from a restored backup \(on page 150\)](#) procedure to recover the files into the proper location.

Recovering files from a restored backup

To recover the files in the restored backup:



Note: Your user account must be assigned the `admin` role to complete this process.

1. On the **Settings > Advanced > Recover from Backup** page, type the path where the backup file was restored to. See [Hosts and Paths \(on page 134\)](#) for more information.



Note: The default location of `/opt/ie/backup` must be used to recover the files.

2. Select **Recover**.
3. When the files have been recovered, log out, reboot the Ransomware Detection server, and log back into the Ransomware Detection UI to complete the recover process. The files in the temporary location are removed automatically at the end of the recover process.

Global Feature Options

Select **Settings > Advanced > Global Feature Options** to globally enable/disable all custom YARA rulesets.



Note: Only a user assigned the admin role can access this page.

Globally setting YARA rulesets

To globally enable/disable YARA rulesets:

1. Go to **Settings > Advanced > Global Feature Options**.

2. From the **Custom YARA Ruleset Global Control** options, select:

- **Enable** to enable all custom YARA rulesets.
- **Disable** to disable all custom YARA rulesets.

Then select the **Enable** or **Disable** button.



Note: When you globally enable or disable YARA rulesets, the selected option is reset to the default of **Enable**, which you can see by navigating away from and back to the page. Once the option is set, the state of the option is no longer needed. You can enable or disable individual YARA rulesets on the **Custom YARA Rulesets** page and that setting will override the global setting.

Appendix A. Supported systems and limits

This section lists the currently supported block devices, file systems, and capacity limits.

- [Block device capacity limits \(on page 154\)](#)
- [File system capacity limits \(on page 155\)](#)

Block device capacity limits

The following table lists currently supported block devices and capacity limits.

System Architecture	Maximum Block Device Size	Notes
64-bit systems	~8 exabytes (EB)	
32-bit systems	16 TB	

File system capacity limits

The following table lists the currently supported file system types and capacity limits.

File System	Maximum Size	Maximum File Size	Notes
ext4	1 exabyte (EB)	16 TB	
ext3	32 TB	2 TB	Legacy; currently supported
XFS	8 EB	8 EB	
NTFS	8 PB	16 TB	

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com

Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com

