

# Ransomware Detection powered by CyberSense®

v8.13.0

---

## Installation Guide

Instructions for downloading, installing, and configuring the Ransomware Detection software.

© 2023, 2025 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](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>.

CyberSense® is a registered trademark of Index Engines, Inc.

# Contents

---

<b>Chapter 1. Preparation.....</b>	<b>5</b>
Pre-installation.....	6
Server requirements and recommendations.....	7
Firewall port configuration.....	8
Special considerations.....	9
Tasks prior to installation.....	10
Set hostname.....	10
Map your local hostname to the loopback address.....	10
<b>Chapter 2. Ransomware Detection software installation.....</b>	<b>13</b>
Local repositories.....	14
Installing the .tar repository bundles.....	14
Installing the Ransomware Detection software.....	16
<b>Chapter 3. Final installation steps.....</b>	<b>19</b>
Setting the admin password.....	20
Multi-factor authentication.....	21
Enabling MFA for the admin account.....	21
Additional MFA commands.....	22
Logging into the Ransomware Detection UI.....	25
Setup view.....	26
Viewing and accepting the EULA.....	26
Setting up a license.....	26
Setting up index maintenance.....	27
Configure analysis.....	28
Logging out of the Ransomware Detection UI.....	29
<b>Appendix A. Commands to manage the Ransomware Detection services.....</b>	<b>31</b>

---

# Chapter 1. Preparation

---

This guide provides instructions for performing an initial installation of the Hitachi Vantara Ransomware Detection software.

This document covers installations where the server that will run the Hitachi Vantara Ransomware Detection User Interface (UI) does not have Internet access. Hitachi Vantara now provides repositories containing the packages required by the application. To install the Ransomware Detection UI on a system, follow the installation procedure in this manual.


## Pre-installation

To ensure a smooth and successful installation, Hitachi Vantara recommends performing a site survey prior to performing the installation. Consider the following:

- **Resources** – Review the Ransomware Detection [Server requirements and recommendations \(on page 7\)](#) that follow and confirm that the environment can adequately accommodate the system. If the environment cannot meet our minimum requirements, unpredictable application behavior may result.
- **Support Portal Access:**
  - Confirm that you have an account created at Hitachi Vantara Support Connect prior to the installation date. The support portal is found at <https://support.hitachivantara.com>.

## Server requirements and recommendations

Hitachi Vantara offers the flexibility to choose your own server platform. You can deploy the Ransomware Detection software on a Virtual Machine (VM) or on a physical server that meets the Hitachi Vantara recommended minimum hardware and software requirements shown in the following tables.

Hitachi Vantara Ransomware Detection Server Requirements and Recommendations			
Components	Use Cases		
Size of Data	Small <sup>1</sup>	Medium <sup>2</sup>	Large <sup>3</sup>
CPU (cores)	24 <sup>4</sup>	32 <sup>4</sup>	48 <sup>4</sup>
Memory	128 GB	256 GB	384 GB
OS	Red Hat Enterprise Linux (RHEL) (9.4)		
Architecture	x86_64 <b>REQUIRED</b>		
Filesystem	XFS is preferred. EXT4 is also acceptable.		
<b>Minimum Requirements and Storage</b>			
<b>Partitioning Schema</b>			
/ partition	120 GB		
	 <b>Note:</b> This partition includes the /var directory. You do not need to create a separate /var partition.		
/boot partition	500 MB		
/opt/ie partition <sup>5</sup>	11 TB	19 TB	42 TB
Swap	448 GB	448 GB	832 GB
Connectivity to Data Source (iSCSI)	2 x 25 Gbps Ethernet	2 x 25 Gbps Ethernet	2 x 100 Gbps Ethernet
Connectivity to Data Source (Fibre Channel)	2 x 32 Gbps	2 x 32 Gbps	2 x 64 Gbps

1. Amount of front-end backup data to be indexed  $\leq 75$  TB
2. Amount of front-end backup data to be indexed  $\geq 75$  TB and  $\leq 150$  TB
3. Amount of front-end backup data to be indexed  $\geq 150$  TB
4. Bare metal installations: Number of physical cores with HyperThreading (HT) or Simultaneous MultiThreading (SMT) enabled.
5. 8 x SSD or NVMe drive in an SW RAID5 7+1 configuration



**Note:** Connectivity to the data source can be iSCSI, Fiber Channel, or both.

## Firewall port configuration

Hitachi Vantara uses the ports shown below.

Firewall Port Configuration		
Open Ports	To Allow	When
443	Inbound connections	To access the Ransomware Detection software
53	Outbound connections	DNS
860 3260	Outbound connections	TCP iSCSI (if using iSCSI for Virtual Machine scanning)
25	Outbound connections	Optional when email is supported
7785	Inbound connections on a license server engine and outbound connections on license client engines	To share licenses between Ransomware Detection servers

## Special considerations

To avoid common mistakes during installing or upgrading procedures:

1. Ensure that your firewall is disabled or configured to open the ports specified in the port configuration table.
2. *Optional* - If you want to receive CyberSense emails, ensure that you have a Mail Transfer Agent (MTA) running to enable email notifications. Set up the MTA to accept the email that the Hitachi Vantara software generates on port 25.
3. Consistently use the hostname of your engine. For example, for host "engine1.example.com", consistently use either the Fully Qualified Domain Name (FQDN), which is the preferred usage, "engine1.example.com" or "engine1" but not both.
4. Verify that your local host maps to the loopback address. See [Map your local hostname to the loopback address \(on page 10\)](#) for more information.

## Tasks prior to installation

There are several tasks that must be performed on your Hitachi Vantara server to prepare the engine for software installation.

### Set hostname

Set your hostname on the Hitachi Vantara server. Once it has been set, you must reboot the server for the change to take effect. After the reboot, make sure that the hostname has changed by running the `hostname` command.



**Note:** Consistently use the hostname of your engine. For example, for host "engine1.example.com", consistently use either the Fully Qualified Domain Name (FQDN), which is the preferred usage, "engine1.example.com" or "engine1" but not both.

### Map your local hostname to the loopback address

Your local hostname must map to the loopback address, which is `127.0.0.1`, on your server. If not, edit the `/etc/hosts` file as in the example that follows.

The local hostname is missing in the following example and will not resolve to `127.0.0.1`:


```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost.localdomain localhost6 localhost6.localdomain6
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

To map the local hostname to the loopback address of `127.0.0.1`, modify the first line by adding the FQDN hostname ("myhost.domain"), followed by the shortened name if you want to use it ("myhost"). The changes are highlighted in bold.



**Note:** If `localhost` is mapped to `::1` in the `/etc/hosts` file, remove that entry.

```
127.0.0.1 myhost.domain myhost localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 ip6-localhost ip6-loopback localhost6 localhost6.localdomain6
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

 **Important:** Do not add a second entry for 127.0.0.1.



# Chapter 2. Ransomware Detection software installation

---


To install the Ransomware Detection software, the first steps are:

- [Installing local repository bundles \(on page 14\)](#)
- [Installing the Ransomware Detection software \(on page 16\)](#)

After installing the software, configure the Ransomware Detection server for initial use; see [Final installation steps \(on page 19\)](#) for final setup instructions.

## Local repositories

Hitachi Vantara provides a selection of repository bundles containing required software packages to install the Ransomware Detection software on a server running a given OS for environments that do not have access to the Internet.

 **Important:** This step is required if you do not have Internet access on the Ransomware Detection server.

Repository bundles are found on [Hitachi Vantara Support Connect](#). The repository bundle includes any OS dependency packages necessary for installation on a specific operating system and version. Some of the repository bundles are .tar files.

On the support portal, the repository bundles are listed on the **Software Download** tab, under **Ransomware Detection powered by CyberSense**.

The filename format is as follows:

```
repopundle-indexengines-<operating_system>-<os_rel_ver>-<date>.tar
```

where:

- *operating\_system* - This is the operating system of the server. RHEL repository bundles are available at this time.
- *os\_rel\_ver* - This indicates the operating system's release version.
- *date* - This is the date that the repository bundle was created.

As an example, the filename for the RHEL 9.4 installation repository bundle would be:

```
repopundle-indexengines-rhel-9.4-250330.tar
```

It is recommended that you download the repository to a temporary location, such as `/tmp/ie-repos` on the server.



**Note:** If you do not have Internet access on the system that requires the repository bundle, download the repository bundle on a local machine that has Internet access. Next, copy it to the system and continue with the repository installation before attempting to install the software.

---

## Installing the .tar repository bundles

---

The repository bundles for RHEL 9.4 are .tar files and are found on [Hitachi Vantara Support Connect](#).

To download and install the repository bundle:

1. Download the appropriate repository bundle onto a system with Internet access. Log into the system designated to be the Hitachi Vantara server as `root` and copy the tar file to an accessible location.
2. If the directory does not already exist, on the Hitachi Vantara server, make the following directory for extracting the repository bundle:

```
mkdir -p /opt/ie
```

3. Extract the repository bundle:

```
tar xpcf /opt/ie /<path_to_repo_bundle>/repobundle-  
indexengines-<operating_system>-<os_rel_ver>-<date>.tar
```

4. Next, install the repository bundle:

```
sh /opt/ie/repos/INSTALL
```

After installing the repository bundle, proceed with the installation or upgrade of the Hitachi Vantara software.

## Installing the Ransomware Detection software

The next step is to install the Ransomware Detection software from the .tar file.



**Note:** Ensure the repository bundles are locally available on your server during installation since the script will not be able to access them from the Internet.

To install the Ransomware Detection software:

1. Download the Ransomware Detection powered by CyberSense installation media.
  - a. Log on to [Hitachi Vantara Support Connect](#) using your credentials.
  - b. On the **Software Download** tab, click **Ransomware Detection powered by CyberSense**.
  - c. From the **Versions** list, select version **8.13.0**.
  - d. Locate and then download the **Ransomware Detection powered by CyberSense** installation media file.
2. When prompted, save the Ransomware Detection powered by CyberSense Installation Media file, e.g., `indexengines-8.13.0.0-0.1-e19.x86_64.tar`, to a newly created, empty directory on the Ransomware Detection server (e.g., `/tmp/ie`). This directory should be accessible to the Ransomware Detection server. Alternately, use `winscp` or a USB device to copy the downloaded file to the engine.



**Note:** The temporary directory must be empty so that you install ONLY the .rpms for this release with the command shown in the next steps.

3. On the Ransomware Detection server, go to the directory containing the downloaded .tar file and extract the files from it.

```
tar -xf indexengines-8.13.0-1.3-e17.x86_64.tar
```



**Note:** The installation will fail if the minimum disk requirements are not met. If this occurs, remediate the situation before attempting the installation again.

4. Next, go to the directory where the file is located and install the Ransomware Detection software package as root.

```
sh install_ie *.rpm 2>&1 | tee log
```

When prompted, confirm the list of rpm files to be installed.

This command runs and captures the output of the installation process to a log file. If the process fails, you can view the log to find out what the problems were and correct them before running the installation process again.

5. Once the installation is complete, reboot the system.
6. After the restart, log into the Ransomware Detection UI to continue the installation process. See [Final installation steps \(on page 19\)](#) for the next steps in the process.



# Chapter 3. Final installation steps

---

Before you can use the software, you must perform a few final installation steps that should be done before using the software for the first time. You can change these settings in the future if needed, but typically they are not changed often after the installation.

These steps are:

- [set the password for the admin user \(on page 20\)](#)
- [setting up multi-factor authentication \(on page 21\)](#)
- [logging into the CyberSense UI \(on page 25\)](#)
- [completing the initial setup steps using the Setup wizard \(on page 26\)](#)
- [logging out of the CyberSense UI \(on page 29\)](#)

## Setting the admin password

The `admin` user does not have a password set at the end of the installation process. If you do not set a password for the user, then you will not be able to log into the Ransomware Detection UI to proceed with the initial setup and configuration.

1. Log in as `root` to the Hitachi Vantara server using `ssh`.
2. On the command line, type  
`iepasswd admin`

The new password must meet the following requirements:

- a minimum of nine characters in length
- a maximum of 128 characters
- contain a minimum of one uppercase letter
- contain a minimum of one lowercase letter
- contain a minimum of one digit
- contain a minimum of one special character (!, @, #, \$, %, etc.)
- no more than one repeating character

Additional requirements are:

- passwords expire after 30 days
- passwords cannot be changed a set number of times within 24 hours (1 day) of the previous change. The number can be set to 1-3, inclusively.
- the new password cannot be the same as a set number of the previous passwords. The number can be set to 1- 24, inclusive.

You will be prompted to enter a new password and then to confirm the change.

Additionally, you can set the password to expire immediately and force a user to enter a new password when trying to log into the Ransomware Detection UI by entering:

```
iepasswd -e <user>
```

If you have attempted to enter an incorrect password too many times and are now blocked from additional attempts, enter the following to unblock the user:

```
iepasswd -u <user>
```

## Multi-factor authentication

With multi-factor authentication (MFA), the engine can act as an open authentication (OATH) server, requiring users to authenticate the login process with a combination of the username, password, and a one time passcode (OTP). Your company will determine whether to require this security feature and how to implement it. Typically, an authentication app such as Google Authenticator is used set up the MFA client-side application. This functionality is disabled by default.

If your company decides to enable MFA on the engine, each user account will get an alphanumeric key to add in the selected authentication app. The user then uses the 6-digit OTP when logging into the Hitachi Vantara UI with their username and password.

### Enabling MFA for the admin account

To enable MFA on your engine:

1. In a CLI window on the engine, as `root`, type:

```
setimconfig login totp [always | ifset | never]
```

Where:

Mode	Description
<code>always</code>	MFA is enabled for all users and the OTP is required to log in.
<code>ifset</code>	MFA is set for specific users and the OTP is required for those users to log in.
<code>never</code>	MFA is not set and will not be used for logging in to the UI.

2. Create a key for the `admin` account:

```
iepasswd -k admin
```

The command returns a secret string that your system administrator `admin` user can add to an authentication app, such as Google Authenticator. See below for an example of the returned string:

```
otpauth://totp/admin?secret=C8AOWII6PYVMLMD1OSD2YCGILM&issuer=engine.example.com
```

Use the string that's located between the `=` and `&` characters.

The 6-digit code that's displayed in the authentication app is the OTP to be used when logging in.

For additional MFA commands, see [Additional MFA commands \(on page 22\)](#).

## Additional MFA commands

---

Besides enabling MFA for the `admin` account, you can enable MFA on individual user accounts, generate QR codes for the users, or disable MFA functionality.

### Enabling MFA for select users

To enable MFA on select user accounts:

1. Create a key for a specific user account using the following command:

```
iepasswd -k <username>
```

Where `<username>` is the user account to set the key for.

2. When the string is returned, send the string to the user of the account.

### Generating a QR code for a user

An alternative to using the secret string in an authentication app is to generate a QR code that is sent to the user.

To generate a QR code for a user:

1. Create a QR code for a specific user account using the following command:

```
iepasswd [-k | -g] <username> | qrcode -t <image_type>
```

Where:

Parameter	Description	Example
<code>-k</code> <code>-g</code>	Use the <code>-k</code> parameter if you do not have a secret key for the specified username.  Use the <code>-g</code> option if you already have a secret key for the specified username.	<code>iepasswd -k janedoe</code>
<code>&lt;username&gt;</code>	The user account to set the URL key for	<code>admin</code>
<code>&lt;image_type&gt;</code>	The generated image type.	<code>UTF8</code>

In this example, the returned QR code is a UTF-8 image type.



2. Send the QR code image to the user.

## Generating a URL for a user

Another alternative is to generate a URL that is sent to the user.

To generate a URL for a user:

1. Create a URL for a specific user account using the following command:

```
iepasswd [-k | -g] <username>
```

Where:

Parameter	Description	Example
-k -g	Use the <code>-k</code> parameter if you do not have a secret key for the specified username.  Use the <code>-g</code> option if you already have a secret key for the specified username.	<code>iepasswd -k janedoe</code>
<username>	The user account to set the URL key for	<code>admin</code>

2. Send the resulting URL to the user.

## Disabling MFA

To disable MFA on the engine:

1. In the CLI window, type:

```
setimconfig login totp never
```

## Retrieving a user's key

To retrieve a user's key:

1. In the CLI window, type:

```
iepasswd -g <user_name>
```

## Resetting MFA to the default setting - disabled

To reset MFA to the default setting of being disabled:

1. In the CLI window, type:

```
clearimconfig login totp
```

## Logging into the Ransomware Detection UI

To log into the Ransomware Detection UI:

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



**Note:** The URL is case sensitive and should be entered as shown.

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

2. In **Username**, enter 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 Ransomware Detection **Home** page is displayed if you have already completed the initial setup process.

# Setup view

When you log into Hitachi Vantara Ransomware Detection UI for the first time, you will be redirected to the **Setup** view. The **Setup** view appears only after an installation or upgrade of the Ransomware Detection software.

In the **Setup** view of the Ransomware Detection UI, configure the following system settings:

- [accepting the EULA \(on page 26\)](#)
- [the system license \(on page 26\)](#)
- [the index maintenance schedule \(on page 27\)](#)
- [malware alerts \(on page 28\)](#)

---

## Viewing and accepting the EULA

---

As the first step of using the Ransomware Detection UI, you must read and accept the EULA.

1. After logging in, the EULA is displayed. Read through the EULA and then select the agreement statement.



**Note:** When you log into the Ransomware Detection UI for the first time, you will automatically be redirected to the **Setup** view.

2. Select **Save and Continue**.

---

## Setting up a license

---

In the latest release of the software, Ransomware Detection licenses are no longer constrained to the confines of an engine. In the new client/server licensing model, one engine can act as a license server for several other 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 a license client, which can continue to use the license on the licensor server or not in the future.

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

## Installing the license on the license server



**Note:** Choose a Ransomware Detection engine to function as the license server and install the license on that engine first.

To install a license locally on the Ransomware Detection engine:

30 In **Set up License**, copy the **Engine ID** and log onto [pa@ca.com](mailto:pa@ca.com) or [Support Connect](#).

40 On the Hitachi Vantara portal, register your engine. You will receive an email containing the license file to download.

50 In **Set up License** in the Ransomware Detection UI, select **Upload License** as the licensing option. This will upload a license for that specific engine, whether it becomes a license server or a stand-alone engine. This is the default selection.

60 Select **Browse** to locate and choose the license file that Hitachi Vantara sent via email after you registered the engine on the support portal. The filename of the license includes the engine ID to which the license applies; be sure that it matches the engine ID shown on the **Setup License** page of your system. If not, contact the Hitachi Vantara support team. Then select **Open**.

70 Next, select **Save and Continue**. Once the file uploads, the license details are displayed. Verify that the license information is as you expected.

## Registering an engine with a license server

To register an engine with a license server:

1. In **Set up License**, select **Register with License Server** for the licensing option. This will register the engine as a license client with the engine that is functioning as the license server.
2. The following fields are displayed.
3. Add the license server information to:
  - **Host Name** - the hostname of the License Server
  - **Username** - the `admin` account of the license server is always used and cannot be changed.
  - **Password** - the password of the `admin` account.
  - **One-Time Password** - if MFA has been enabled on the license server engine or for the `admin` user of the license server, then enter the OTP in this field.



**Note:** Contact the system administrator of the license server to receive a QR code or secret key with which you can use in an authenticator app.

4. When complete, select **Register** and then **Save and Continue**.

## Setting up index maintenance

On this screen, set up the index maintenance schedule, which will merge segments and remove hosts whose data is no longer being indexed. These hosts are considered "stale". This saves space on the system that stores the indexing data by no longer indexing stale hosts and merging segments to remove duplicate data.

1. In **Set up Index Maintenance**, there are three fields to configure. First, in the **Reclaim index storage every** field, set the day of the week and hour when segments will be merged to reclaim indexing storage space.
2. For the **Enable unindexed host removal** field, enable or disable to remove hosts that have not been indexed in a set period of time. The default is **Disabled**.
3. In the **Remove hosts not indexed in** field, select the period of time to retain the unindexed hosts in the database. This can be set between **30** and **90** days, with the default of **60**.
4. Select **Save and Continue**. The next window will open.

---

## Configure analysis

---

When a **Malware File Detected** alert is created, an email including alert details will be sent to specified recipients. Configure the email addresses, upload a malware signature file for signature matching, or enable **Diagnostic log file reporting**.

1. On the **Set up Alerts** page, add the emails of the recipients in the **Alerts will be sent to** field. When adding the email addresses, press **Enter** after each entry to save it. These email addresses will receive all Ransomware Detection emails for alerts and when jobs have completed.
2. *Optional* - If you have a malware signature file more recent than the currently installed one, upload it here. The version and date of the currently installed malware signature file is displayed on this page. The file will be used to match any malware files and create alerts if detected. You will be notified of the upload status and whether it was successful or not. The upload process will fail if you attempt to use a malware signature file older than the currently installed one.



**Note:** Updated malware signature database files are available weekly. Contact your support personnel for more information.

3. Select to enable **Diagnostic log file reporting**, which is disabled initially.
4. Select **Save and Continue**.

When the setup steps are complete, you will be redirected to the **Alerts** page.

## **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.



# Appendix A. Commands to manage the Ransomware Detection services

---

The Ransomware Detection `dservice` command is found in the `/opt/ie/bin` directory. The Ransomware Detection software installation adds this directory to your path so that this command can be easily executed, however, it does not take effect after the initial installation until you log out and back in again.

Action	Command
Get status of Ransomware Detection Services	<code>dservice status all</code> or <code>dservice status &lt;service name&gt;</code>
Restart Ransomware Detection Services	<code>dservice restart all</code> or <code>dservice restart &lt;service name&gt;</code>
Stop Ransomware Detection Services	<code>dservice stop all</code> or <code>dservice stop &lt;service name&gt;</code>
Start Ransomware Detection Services	<code>dservice start all</code> or <code>dservice start &lt;service name&gt;</code>

## Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive  
Santa Clara, CA 95054 USA [www.HitachiVantara.com](http://www.HitachiVantara.com) [community.HitachiVantara.com](http://community.HitachiVantara.com)

### Regional Contact Information

Americas: +1 866 374 5822 or [info@hitachivantara.com](mailto:info@hitachivantara.com)

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

Asia Pacific: +852 3189 7900 or [info.marketing.apac@hitachivantara.com](mailto:info.marketing.apac@hitachivantara.com)

