IBM Storage Defender Sentinel

Installation and User's Guide

2.3.0

IBM

Contents

Note:

Before you use this information and the product it supports, read the information in "Notices" on page 65.

This edition applies to version 2, release 3, modification 0 of IBM® Storage Defender Sentinel (product number 5900-APZ) and to all subsequent releases and modifications until otherwise indicated in new editions.

About this publication

This publication provides overview, planning, installation, and user instructions for IBM® Storage Defender Sentinel anomaly scan software.

Audience and purpose

This publication is intended for administrators and users who are responsible for implementing a backup and recovery solution with IBM® Storage Defender Sentinel anomaly scan software in one of the supported environments.

System administrators can use this guide to help install, maintain, and start the application, manage users, and catalog resource information. Users can find procedures on how to search and browse for objects, generate and interpret reports, schedule jobs, and orchestrate backup and restore jobs.

What's new

New features and enhancements are available in IBM® Storage Defender Sentinel 2.3.0.

Feature	Description	Benefit
Windows™ file system scanning	IBM® Storage Defender Sentinel now supports security scanning for snapshots of Windows™ NTFS and FAT32 file systems.	Scans Windows™ NTFS and FAT32 file systems for ransomware and other latest capabilities.
Microsoft™ SQL database scanning	IBM® Storage Defender Sentinel adds support for security scanning on standalone virtual and physical Microsoft™ SQL servers databases.	Scans Microsoft™ SQL databases for ransomware and other latest capabilities.
Support for IBM® Storage Defender Copy Data Management 2.3.0	IBM® Storage Defender Sentinel 2.3.0 is now qualified with IBM® Storage Defender Copy Data Management 2.3.0.	Use IBM® Storage Defender Sentinel 2.3.0 with IBM® Storage Defender Copy Data Management 2.3.0.

Important: Review the Limitations and known issues topic before you start using the IBM® Storage Defender Sentinel application.

IBM® Storage Defender Sentinel anomaly scan software overview

IBM® Storage Defender Sentinel anomaly scan software solution facilitates an end-to-end automated cyber resilience workflow that is designed to help protect copies of data, detect malicious code attacks, and enable accelerated and automated recovery of data from clean copies with IBM FlashSystem® family and SAN Volume Controller (SVC) storage.

IBM® Storage Defender Sentinel combines an IBM® Storage Defender Copy Data Management with an anomaly scan software to coordinate file & database corruption scanning with snapshot management and recovery orchestration.

IBM® Storage Defender Copy Data Management can take application-aware, immutable snapshots, commonly known as Safeguarded Copy, in IBM® FlashSystems and SAN Volume Controller (SVC) storage starting with version 2.2.16.

The anomaly scan software with IBM® Storage Defender Copy Data Management and an anomaly scan engine provides scanning for corruption due to malicious code and cataloging for immutable snapshots in primary storage, enabling clients to automate recovery after an event.

Real-time cyber protection solutions are designed to protect from an attack. However, these solutions are not 100% effective and corporate data is corrupted daily. Anomaly scan software adds a layer of protection to these real time solutions and finds corruption that occurs when an attack has successfully penetrated the data center. Anomaly scan software enables early detection of issues so that IBM® Storage Defender Copy Data Management can coordinate fast application recovery, minimizing business interruption.

Anomaly scan software identifies files corrupted by malicious code using a set of statistics about files on the host being analyzed with a Machine Learning Model (MLM) trained using real world malicious codes to identify if a host was attacked by malicious code. In addition to identifying malicious code attacks, anomaly scan software checks the integrity of databases to detect corruption of the internal database data. The databases could be corrupted by an attacker, logical or physical data corruption or damage at the disk/volume level, or as a flaw in the process in the creation of a snapshot or backup of the database.

The anomaly scan software examines existing database pages and allocation tables if they exist to ensure that all the allocated database pages are present and located in their correct position. In cases where some type of page data signature is available and/or enabled by the database administrator, such as a checksum or CRC, anomaly scan software recalculates the signature based on the current page contents and verifies it against the value found in the page header. Other ancillary fields are also verified within each page depending upon the database application. The anomaly scan software Machine Learning Model (MLM) has been designed to tolerate a small amount of database corruption that is commonly observed in production database systems to avoid excessive false-positive alerts.

In addition to the anomaly scan software information that is available in IBM® Documentation, other information that you might find helpful can be obtained through IBM Storage Defender Sentinel Support.

Preparation

This guide provides instructions for performing an initial installation of the IBM® Storage Defender Sentinel anomaly scan software.

This document covers installations where the server that will run the anomaly scan software does not have Internet access. Anomaly scan software now provides Linux repositories containing the packages required by the application.

Pre-installation

To help ensure a smooth and successful installation of IBM® Storage Defender Sentinel anomaly scan software, complete a site survey before you plan to install the product.

- **Resources**

  Review the anomaly scan software requirements. To review, see "Server requirements and recommendations" on page 9 that follow and confirm that the environment can adequately accommodate the system. If the environment cannot meet the minimum requirements, unpredictable application behavior is possible.

- **Support portal access**
  - Confirm that you have an account that is created in the support portal prior to the installation of the product.
  - Sign in to the portal and sign the End User License Agreement (EULA). Accepting the EULA is mandatory to register the new system and activate or install the license.
- **License agreement**
  - The authorized user or license owner must sign in to the anomaly scan software and sign the End User License Agreement (EULA). Accepting the EULA is mandatory to register the new system and activate or install the license.
- **TIP:**
  - In addition to reviewing the details that follow, see the "Installation checklist" on page 52 in the guide. You can print those two pages so that you can mark off each item as you complete the steps.
  - The `CheckEngine.sh` script is available on the Passport advantage online. You need to install the script in the `/usr/local/bin` directory and make it executable. You need to run the script to confirm that the system is ready for a software installation and then to confirm the final configuration.

    > **Note:** For steps on how to use Passport advantage online website, refer to Download Information.

Server requirements and recommendations

IBM® Storage Defender Sentinel gives you the flexibility to choose your own server platform. You can deploy the IBM® Storage Defender Sentinel anomaly scan software on a virtual machine (VM) or on a physical server that meets the minimum hardware and software requirements, which are shown in the following tables.

Initiators for Fibre Channel and iSCSI must be established between physical anomaly scan software server deployments and IBM® storage such as IBM® Storage FlashSystem 9100 and IBM® Storage FlashSystem 5200. Fibre Channel is the preferred initiator option for physical anomaly scan software server deployments.

The IBM® Storage Defender Sentinel offering consists of IBM® Storage Defender Copy Data Management with anomaly scanning software. The minimum version levels of the software IBM® Storage Defender Sentinel are as follows:

- IBM® Storage Defender Sentinel anomaly scan software 8.1.0 Build 1.x and later patches

  > **Note:** Check on Fix Central for the latest IBM® Storage Defender Sentinel 2.3.0 interim fixes, refer to Download Information.

- IBM® Storage Defender Copy Data Management 2.3.0 and later interim fixes
- IBM Spectrum® Virtualize Software for IBM® Storage FlashSystem 8.5.1 and later interim fixes

For IBM® Storage Defender Copy Data Management requirements, refer to system requirements and for IBM Storage® Virtualize requirements, refer to requirements.

Scanning for ransomware by using the anomaly scan software is supported on the following applications:

- InterSystems Caché and InterSystems IRIS (collectively referred to as InterSystems Database), refer to InterSystems Database requirements.
- SAP HANA, refer to SAP HANA requirements.
- Oracle, refer to Oracle requirements.
- VMware virtual machine workloads, refer to VMware requirements.
- Microsoft™ SQL, refer to Microsoft SQL requirements.
- File System (Windows™ and Linux), refer to File System requirements.

In the IBM® Storage Defender Sentinel 2.3.0 release, support has been added for scanning Windows™ file system snapshots and standalone physical and virtual SQL databases. To use these new scanning capabilities, users must install the required NTFS and FAT32 drivers (for example, `ntfs-3g` for NTFS) on the IBM® Storage Defender Sentinel host.

The requirements apply to the anomaly scan software server component of the IBM® Storage Defender Sentinel offering only. Generally, you want to successfully install IBM® Storage Defender Copy Data Management before you deploy the anomaly scan software server. For more information, see Installation and setup.

IBM® Storage Defender Sentinel anomaly scan software server requirements		
Components	**Use Cases**	
	Medium: Amount of front-end backup data to be indexed ≤ 15 TB	**Large: Amount of front-end backup data to be indexed ≥ 15 TB**
CPU (cores)	20	32
Memory	192 GB	384 GB
OS	SUSE Linux Enterprise Server (SLES) 15.4, SUSE Linux Enterprise Server (SLES) 15.6	
	Red Hat (RHEL) 9.2, Red Hat (RHEL) 9.4	
	Note: Repository bundles are not provided for the supported operating systems.	
SELinux	**REQUIRED:** **Note:** On servers that are using SUSE operating system, if SELinux is enabled and enforcing, you must switch it to permissive mode before you install or upgrade the anomaly scan software. After the installation/upgrade has finished, switch SELinux back to enforcing / enabled mode.	
Architecture	x86_64 **REQUIRED**	
File system	XFS is preferred. EXT4 is also acceptable.	

IBM® Storage Defender Sentinel anomaly scan software server requirements			
Components	**Use Cases**		
	Medium: Amount of front-end backup data to be indexed ≤ 15 TB	**Large: Amount of front-end backup data to be indexed ≥ 15 TB**	
Host OS Partitioning Schema **MINIMUM** Requirements and Storage (Direct attached, local, or SAN)	**`/ partition`**	120 GB	
	`/boot partition`	500 MB	
	`/opt/ie partition`	Your anomaly scan software support personnel can provide guidance on the size of this partition based on the details of your data.	
	***Swap**	Memory	Swap
		192 GB	384 GB Medium
		448 GB	832 GB Large
Connectivity to Storage	To be determined at the time of sizing.		

Supported applications and operating systems						
Scan type	**Application host / server type**	**Platform type**	**Supported Sentinel host / server type**	**Supported Sentinel operating systems**	**Supported storage arrays (*SGC - Safeguarded copies)**	**Description**
Database applications (Oracle, IRIS, SAP HANA)	Physical	x86, Linux on Power (LoP)	Physical	RHEL 9.2, RHEL 9.4, SLES 15.6	IBM® Storage FlashSystem (SGC1.0 and SGC2.0)	Scanning of a physical application is supported on a physical Sentinel host only.
	Virtual	x86	Virtual	RHEL 9.2, RHEL 9.4, SLES 15.6	IBM® Storage FlashSystem (SGC1.0 and SGC2.0)	Scanning of a virtual application is supported on a virtual Sentinel host only.

Supported applications and operating systems						
Scan type	**Application host / server type**	**Platform type**	**Supported Sentinel host / server type**	**Supported Sentinel operating systems**	**Supported storage arrays (*SGC - Safeguarded copies)**	**Description**
Microsoft™ SQL database	Physical, Virtual	Windows™	Physical/ Virtual machine (pRDM)*	RHEL 9.2, RHEL 9.4, SLES 15.6	IBM® Storage FlashSystem (SGC1.0 and SGC2.0)	Scanning of standalone physical and virtual Microsoft™ SQL databases is supported. Sentinel supports the NTFS and FAT32 file system types for scanning. To enable scanning, you must install the required NTFS and FAT32 drivers on the Sentinel host. (For example, `ntfs-3g` for NTFS-based file systems.) The scanning capability requires iSCSI/FC connectivity between IBM® Storage FlashSystem and the IBM Storage Defender Sentinel host. When you use FC, verify that the Sentinel host is zoned and defined in the SVC array as FC host. When you use iSCSI, verify that the iSCSI is enabled in the Sentinel host, and has network reachability over iSCSI port (3260/TCP) with IBM® Storage FlashSystem. Also verify that the Sentinel host is defined as iSCSI host.
AIX based database applications	Physical, Virtual	Power	Physical/ Virtual	RHEL 9.2, RHEL 9.4, SLES 15.6	IBM® Storage FlashSystem (SGC1.0 and SGC2.0)	Sentinel scanning is supported on physical and virtual Sentinel hosts both.

Supported applications and operating systems						
Scan type	**Application host / server type**	**Platform type**	**Supported Sentinel host / server type**	**Supported Sentinel operating systems**	**Supported storage arrays (*SGC - Safeguarded copies)**	**Description**
VMware	Virtual	x86	Physical/ Virtual machine (pRDM)*	RHEL 9.2, RHEL 9.4, SLES 15.6	IBM® Storage FlashSystem (SGC1.0 and SGC2.0)	The scanning capability requires iSCSI/FC connectivity between IBM® Storage FlashSystem and the IBM® Storage Defender Sentinel host. When you use FC, verify that the Sentinel host is zoned and defined in the SVC array as FC host. When you use iSCSI, verify that the iSCSI is enabled in the Sentinel host, and has network reachability over iSCSI port (3260/TCP) with IBM® Storage FlashSystem. Also verify that the Sentinel host is defined as iSCSI host.
File Systems (Linux and Windows™)	Physical (Linux)	x86, Linux on Power (LoP)	Physical/ Virtual machine (pRDM)*	RHEL 9.2, RHEL 9.4, SLES 15.6	IBM® Storage FlashSystem (SGC1.0 and SGC2.0)	The scanning capability requires iSCSI/FC connectivity between IBM® Storage FlashSystem and the IBM® Storage Defender Sentinel host. When you use FC, verify that the Sentinel host is zoned and defined in the SVC array as FC host. When you use iSCSI, verify that the iSCSI is enabled in the Sentinel host, and has network reachability over iSCSI port (3260/TCP) with IBM® Storage FlashSystem. Also verify that the Sentinel host is defined as iSCSI host.

Supported applications and operating systems						
Scan type	**Application host / server type**	**Platform type**	**Supported Sentinel host / server type**	**Supported Sentinel operating systems**	**Supported storage arrays (*SGC - Safeguarded copies)**	**Description**
	Physical (Windows™)	Windows™	Physical/ Virtual machine (pRDM)*	RHEL 9.2, RHEL 9.4, SLES 15.6	IBM® Storage FlashSystem (SGC1.0 and SGC2.0)	Sentinel supports the NTFS and FAT32 file system types for scanning. To enable scanning, you must install the required NTFS and FAT32 drivers on the Sentinel host. (For example, `ntfs-3g` for NTFS-based file systems.) The scanning capability requires iSCSI/FC connectivity between IBM® Storage FlashSystem and the IBM® Storage Defender Sentinel host. When you use FC, verify that the Sentinel host is zoned and defined in the SVC array as FC host. When you use iSCSI, verify that the iSCSI is enabled in the Sentinel host, and has network reachability over iSCSI port (3260/TCP) with IBM® Storage FlashSystem. Also verify that the Sentinel host is defined as iSCSI host.

*Virtual machine (pRDM): Virtual machine where a physical device is directly mapped to it by using the FC passthrough or iSCSI connectivity. Refer to the following links for additional information on FC passthrough configuration:

- VMware KB article 309986
- IBM community blog: Using IBM Storage Defender CDM for VMware - FC based Sentinel scanning

Anomaly scanning server operating systems supported by Sentinel										
Server OS	**1.1.2**	**1.1.3**	**1.1.4**	**1.1.7**	**1.1.8**	**1.1.9**	**1.1.10**	**1.1.11**	**1.1.12**	**2.3.0**
RHEL 9.2	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
RHEL 9.4	No	No	No	No	No	No	No	Yes	Yes	Yes
SLES 15.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SLES 15.6	No	No	No	No	No	No	Yes	Yes	Yes	Yes

1. RHEL 8 is an unsupported operating system on the anomaly scanning server.
2. IBM® Storage Defender Sentinel requires Storage Virtualize for IBM® Storage FlashSystem versions 8.5.1 and later interim fixes.

3. For supported versions of File System, SAP HANA, EPIC, Oracle, Microsoft™ SQL, and VMware, refer to the IBM® Storage Defender Copy Data Management support pages.

Note: The EPIC and SAP HANA applications can run on physical and virtual servers in addition to the power server.

Important: Review the Limitations and known issues topic before you start using the IBM® Storage Defender Sentinel application.

Firewall port configuration

Ideally, on the IBM® Storage Defender Sentinel anomaly scan software server, the firewall should be disabled. Disable it and turn off firewall and iptables unless you require the Linux® firewall to be enabled. In that case, anomaly scan software uses the ports shown below.

Summary for complex table

Firewall Port Configuration		
Open Ports	**To Allow**	**When**
80 or 443	Inbound connection	To access the anomaly scan software
All appropriate NDMP, CIFS, and NFS ports	Outbound connection	To access the corresponding sources
22	In bound and outbound connections on all engines	For SSH (Secure Shell) communications
25	Inbound connection	To enable remote command line access (recommended)
5432	Inbound connection on Federation Manager; outbound connection on each Federation Member	To participate in a federation
22, 7776, 7779, 7781, 7785, 7795, 7799, and 8476	Inbound and outbound connections on all engines	To participate in a federation

The configuration of your firewall may change depending on your environment. For a typical CentOS 7 or RedHat Enterprise 7 server, the commands that follow would be the minimum requirement to support the federation setup (for both the manager and member servers), and it is best to run from the Linux server system console:

```
# systemctl enable firewalld
# systemctl start firewalld
# firewall-cmd --permanent --add-service=ssh --add-service=http --add-service=https
# firewall-cmd --permanent --add-port=7776/tcp --add-port=7779/tcp --add-port=7781/tcp \
  --add-port=7785/tcp --add-port=7795/tcp --add-port=7799/tcp --add-port=8476/tcp \
  --add-port=5432/tcp
# firewall-cmd --reload
```

The adapter and zone used for anomaly scan software communication should also have the similar settings in your firewall configuration as follows:

```
# firewall-cmd --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: http https ssh
  ports: 7776/tcp 7779/tcp 7781/tcp 7785/tcp 7795/tcp 7799/tcp 8476/tcp 5432/tcp
  protocols:
  masquerade: no
  forward-ports:
```

```
source-ports:
icmp-blocks:
rich rules:
```

Special considerations

Procedure

To avoid common mistakes during installing or upgrading procedures:

1. Ensure that you have the Internet access enabled.
2. Ensure that your firewall is disabled or configured to open the ports specified in the port configuration table.
3. Ensure that you have a Mail Transfer Agent (MTA) running to enable email notifications. Set up the MTA to accept the email that the IBM® Storage Defender Sentinel anomaly scan software generates on port 25.
4. If you have multiple Network interface Cards (NIC) in your server, make sure the operating system is properly configured to use them.
5. If you are using SLES 15.6 as your operating system, ensure that the following product modules are enabled and registered:
   - SUSE Linux Enterprise Server 15 SP6 (`SLES/15.6/x86_64`)
   - Basesystem Module (`sle-module-basesystem/15.6/x86_64`)
6. If you are using SLES 15.5 as your operating system, ensure that the following product modules are enabled and registered:
   - SUSE Linux Enterprise Server 15 SP5 (`SLES/15.5/x86_64`)
   - Basesystem Module (`sle-module-basesystem/15.5/x86_64`)
7. If you are using SLES 15.4 as your operating system, ensure that the following product modules are enabled and registered:
   - SUSE Linux Enterprise Server 15 SP4 (`SLES/15.4/x86_64`)
   - Base system Module (`sle-module-basesystem/15.4/x86_64`)
8. 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.
9. Verify that your local host maps to the loopback address. If you need help, see “Map your local host to the loopback address” on page 17.
10. Ensure that the anomaly scan software server has Tomcat 7 or higher installed or enabled prior to installing the anomaly scan software. The GUI application depends on this service to run the application pages.

```
yum install tomcat
systemctl enable tomcat
```

Tasks prior to installation

There are several tasks that must be performed on your IBM® Storage Defender Sentinel anomaly scan software server to prepare the engine for software installation.

Hostname setting

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

Note: Consistently use the hostname of your engine (and that of other engines in a federation). 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 host to the loopback address

Your local host must map to the loopback address on your engine. If not, edit the `/etc/hosts` file as in the example that follows.

To specify the hostname, modify the first line by adding the FQDN hostname ("myhost.domain" in this example), followed by the shortened name if you wish to use it (“myhost” in this example):

```
127.0.0.1   myhost myhost.domain localhost localhost.localdomain localhost4
localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
```

Important:
Do not remove the existing localhost entries.

Do not add a second entry for 127.0.0.1

Alerts

From the **Alerts** menu, you can configure email notifications for security alerts and operation notifications, upload an updated malware signature file, manage custom malware signatures, and configure database corruption alerts.

IBM® Storage Defender Sentinel anomaly scan software installation

A new installation of the IBM® Storage Defender Sentinel anomaly scan software comprises of:

- installing the anomaly scan software
- registering your engine
- installing the license

After the software is installed, see “Final engine setup” on page 21.

Local repositories

IBM® Storage Defender Sentinel anomaly scan software provides repository bundles that are needed to install the software on a server that does not have access to the internet.

Repository bundles for RHEL are found on the support portal. The repository bundle includes any operating system dependency packages necessary for installation on a specific operating system and version. Some of the repository bundles are in the form of `.tar` files.

On the support portal, the repository bundles are listed under the **Repositories** section of the **Resources** page. They are ordered by operating system name and operating system version.

The file name format is as follows:

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

where:

- `operating_system`: Refers to the operating system of the server. CentOS and RHEL repository bundles are available as of now.
- `os_rel_ver`: Refers to the release version of the operating system.
- `date`: Refers to the creation date of the repository bundle.

For example, the file name for the RHEL 9.2 installation repository bundle:

```
repobundle-indexengines-rhel-9.2-230830.tar
```

You can download the repository to a temporary location, such as `/tmp/ie-repos` on the server.

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

Installing the repository bundle

Use the repository bundles to install operating system dependency packages required for installation of IBM® Storage Defender Sentinel anomaly scan software when you do not have access to the internet.

About this task

You can download the repository bundle from the IBM repository. The repository bundle includes any operating system dependency packages necessary for installation.

Procedure

Complete the following steps to install the repository bundle on an application server that does not have access to the internet:

1. Download the repository bundle from the IBM repository to a system that has access to the internet.
2. Copy the `.tar` file to the application server where you want to install the application to an accessible location.
3. On the application server, make a directory for the repository bundle by using the following command:

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

4. Extract the repository bundle by using the following command:

```
tar xpCf /opt/ie /<path_to_repo_bundle>/repobundle-indexenginessles-12.5-<date>.tar
```

5. Install the repository bundle by using the following command:

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

What to do next

Proceed with installing or upgrading the IBM® Storage Defender Sentinel anomaly scan software after you complete the installation of the repository bundle.

Downloading the software

Procedure

The next step is to download the engine software onto the system that it will be installed.

1. Use the Passport advantage online to download the IBM® Storage Defender Sentinel anomaly scan software.

> **Note:** For steps on how to use Passport advantage online website, refer to Download Information.

2. When prompted, save the anomaly scan software installation file, e.g., `indexengines-ibm-cyberv-8.9.0-1.3-suse15.x86_64.tar`, to a newly created, empty directory on the new anomaly scan software system (e.g., `/tmp/ie`). This directory should be accessible to the anomaly scan software system. Alternately, use winscp or a USB device to copy the downloaded file to the engine.

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

3. Use the Fix Central to download the anomaly scan software updates.

Installing the software

Procedure

The next step is to install the IBM® Storage Defender Sentinel anomaly scan software .tar file.

> **Important:**
> The `install_ie` script will configure the following additional repositories during execution:
>
> - For all operating systems - IBM® Storage Defender Sentinel packages for Enterprise Linux® Leap 15.4 - x86_64
> - For SLES 15.4 and OpenSUSE Leap 15.4:
> - SELinux (15.4) (security_SELinux)

- Crypto applications and utilities (15.4) (security_privacy)

- For SLES 15.4 only:
  - OpenSUSE-Leap-15.4-1
  - Online updates for OpenSUSE Leap 15.4 (standard)
- For Red Hat® 9.2

1. On the anomaly scan software system, login using root credentials.
2. Go to the directory containing the downloaded .tar file and unpack the .tar file.

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

3. Run the command that enables the permissions to execute the installation of `install_ie` script.

   ```
   chmod 755 install_ie.sh
   ```

4. Next, install the anomaly scan software package.

   ```
   ./install_ie *.rpm
   ```

   Important: The temporary directory must contain ONLY the downloaded .tar file so that you install ONLY the .rpms that were delivered with this release with the `zypper install *.rpm` command.

5. After you completed the installation on the command line, run the command to enable the `iepasswd` command. User can use the `iepasswd` command to set the admin the password, for more information refer to "Setting the admin password" on page 21.

   ```
   source /etc/profile.d/indexengines.sh
   ```

6. For the next steps in the process, refer to "Final engine setup" on page 21.

Final engine setup

Before you can use the software, you must set the password for the `admin` user, accept the EULA, share your server MAC address or anomaly scan software ID to your IBM® account or Business Partner representative, receive your anomaly scan software license file, and upload your license file to the anomaly scan software manager interface.

Important:

1. Make sure that the contact email address is provided to your IBM® account or Business Partner representative who is placing the order for anomaly scan software.
2. The MAC address of the server (also considered as the engine ID) where you intend to install the software is required to generate and provide you with the software license file. Make a note of the MAC address of the server, refer to "Finding your engine ID" on page 22.
3. Upon order, you will receive an order confirmation or proof of entitlement email from IBM®. This proof of entitlement email contains your order number and can be used to claim your software license file for the anomaly scan software.
4. To claim your license file, reply to the order confirmation email received from IBM® with your order number and the MAC address of the server where you intend to install the anomaly scan software.
5. After you complete the steps above, you will receive an email message from IBM® with the software license file and corresponding instructions for license registration and activation.

Modifying `tmpfs` partition size

You can change the size of the `tmpfs` partition as per your requirement.

If needed, change the size of the `tmpfs` partition to ensure that the size is adequate. For example, if you expect to run queries that match large numbers of documents (more than 100 million), you need to increase the size of the `tmpfs` partition. You can modify the `tmpfs` partition size after IBM® Storage Defender Sentinel anomaly scan software is installed successfully. To modify the `tmpfs` partition size to issue the following command:

```
echo '{"params":{"size":256}}' | setconfig qcache
```

Where 256 is the `tmpfs` partition size in GB. If not adequate, change to an appropriate size for your needs.

Setting the admin password

About this task

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 IBM® Storage Defender Sentinel anomaly scan software GUI to proceed with the initial setup and configuration.

Procedure

1. Log in as `root` to the IBM® Storage Defender Sentinel anomaly scan software server using ssh.
2. On the command line, enter

   ```
   iepasswd admin
   ```

   The new password must meet the following requirements:

   - must be at least 15 characters in length
   - must contain at least one uppercase letter
   - must contain at least one lowercase letter

- must contain at least one number
- must contain at least one special character
- must contain at least three characters that are not in the previous password.

> **Note:** These settings are also available in the anomaly scan software GUI. After setting the password so you can log into the GUI, access them by going to **Setup › Configuration › Login Settings**.

What to do next

You can set the password to expire immediately and force a user to enter a new password when trying to log into the GUI 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>
```

Finding your engine ID

Procedure

The IBM® Storage Defender Sentinel anomaly scan software GUI is accessed via a web browser from the engine server.

1. Open a web browser and sign in to the anomaly scan software. In the **URL** bar, enter `https://<hostname>/admin`. You can use hostname (preferred) or IP address of the host where the anomaly scan software system is installed. The **Sign In** page opens.

   > **Note:** If you are unable to access this page, verify that ports 80 and 443 are open on the firewall.

2. In **Username**, type the default administrator login of `admin`. In the **Password** field, type the default password of `admin`. Select **Sign In** button. Since this is the first time you have logged in to the engine, the **Upload License** page opens.
3. The license upload screen should appear once you login to the GUI for the first time. If not, you can find the license upload screen at **Administration › System › Licenses › Upload License** page. On the **Upload License** screen, you will see the engine ID listed which appears in the title bar above the **Browse** button.

Multi-factor authentication

Starting with IBM® Storage Defender Sentinel 1.1.6, you can set up multifactor authentication (MFA) on IBM® Storage Defender Sentinel new and existing user accounts. With multifactor authentication, 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). You will determine if you require this security feature and learn to implement it. Typically, an authentication app such as Google Authenticator is used to set up the MFA client-side application. This functionality is disabled by default.

If you decide to enable MFA on the engine, each user account will get an alphanumeric key to add in the selected authentication app. The user can use the 6-digit OTP when logging into the IBM® Storage Defender Sentinel user interface with their username and password.

Enabling MFA for the admin account

You can enable time-based one-time (TOTP) multifactor authentication (MFA) on the IBM® Storage Defender Sentinel `ADMIN` account.

Procedure

To enable time-based one-time (TOTP) multifactor authentication on the IBM® Storage Defender Sentinel ADMIN account, complete the following steps:

:

1. Enter the following command as a `root` user on the command-line interface (CLI):
`setimconfig login totp [always, ifset, never]`, where:

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

2. Create a key for the *admin* account by entering the following command:
`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 that you must use to log in. For additional MFA commands, see “Additional MFA commands” on page 23

Additional MFA commands

You can enable multifactor authentication (MFA) on IBM® Storage Defender Sentinel individual user accounts. You can also generate QR codes for the users, and disable the MFA functionality.

Enabling MFA for selected users

You can enable multifactor authentication (MFA) on IBM® Storage Defender Sentinel selected user accounts.

Procedure

To enable MFA on select user accounts, complete the following steps:

1. Create a key for a specific user account using the following command:
`iepasswd -k <username>`
where **<username>** is the user account for which you will set the key.
2. When the string is returned, send the string to the user of the account.

Generating a QR code for a user

About this task

You can also use an alternative way to use the secret string in an authentication app by generating a QR code that is sent to the user.

Procedure

To generate a QR code for a user, complete the following steps:

1. Create a URL key for a specific user account using the following command:
   `iepasswd -k <username> | qrencode -t <image_type> <url_key>`
   where:

Parameter	Description	Example
<username>	The user account to set the URL key for	admin
<image_type>	The generated image type.	UTF8
<url_key>	The URL string from the **iepasswd** command.	otpauth://totp/admin?secret=C8AOWII6PYVMLMD1OSD2YCGILM&issuer=engine.example.com

2. Send the QR code image to the user.

Disabling MFA

You can disable multifactor authentication (MFA) on IBM® Storage Defender Sentinel.

About this task

Procedure

To disable MFA on IBM® Storage Defender Sentinel, complete the following steps:

1. Enter the following command on the command-line interface (CLI):
   `setimconfig login totp never`

Retrieving a user's key

You can retrieve a user's key on IBM® Storage Defender Sentinel.

Procedure

To retrieve a user's key, complete the following steps:

1. Enter the following command on the command-line interface (CLI):
   `iepasswd -g <user_name>`

Resetting MFA to the default setting - disabled

About this task

You can reset multifactor authentication (MFA) on the IBM® Storage Defender Sentinel to its the default setting. The default setting of MFA on IBM® Storage Defender Sentinel is **disabled**.

Procedure

To reset MFA to the default setting **disabled**, complete the following steps:

1. Enter the following command on the command-line interface (CLI):
   `clearimconfig login totp`

Completing the application licensing

Procedure

Once you have received the software license file, follow the steps below to install the license on your system.

> **Attention:** If you are in a federation, upload a license only to the manager machines. Member machines share the license from the manager.

1. Save the email attachment that contains the license file to the system that will be used to access the IBM® Storage Defender Sentinel anomaly scan software web browser interface.
2. Open a web browser and sign in to the anomaly scan software. In the **URL** bar, enter `https://<hostname>/admin`. You can use hostname (preferred) or IP address of the host where the anomaly scan software system is installed. The **Sign In** page opens.

   > **Note:** If you are unable to access this page, verify that ports 80 and 443 are open on the firewall.

3. In **Username**, type the default administrator login of `admin`. In **Password**, type the default password of `admin`. Select **Sign In**.
4. After you sign in, the **Upload License** page opens. If not go to **Administration › System › Licenses › Upload License** page.
5. Use the **Browse** button to locate the license file you saved on the system. Then select **Upload**.
   If you have any questions or need support, contact through IBM Storage Defender Sentinel Support.

Result

License installation in the manager engine is now complete.

Setup view

When you log in to the IBM® Storage Defender Sentinel anomaly scan software GUI for the first time, you are redirected to the **Setup view**. The **Setup view** appears only after an installation or upgrade of IBM® Storage Defender Sentinel anomaly scan software.

In the **Setup view** of IBM® Storage Defender Sentinel anomaly scan software GUI, configure the following system settings:

- “Viewing and accepting the EULA” on page 25
- “Setting up a license” on page 26

Viewing and accepting the EULA

The topic provides information about viewing and accepting the EULA.

As the first step of using the IBM® Storage Defender Sentinel anomaly scan software, you must read and accept the EULA.

Complete the following steps to read and accept the EULA.

1. Open a web browser and sign in to the anomaly scan software. In the **URL** bar, enter `https://<hostname>/admin`. You can use hostname (preferred) or IP address of the host where the anomaly scan software system is installed. The **Sign In** page opens.

   > **Note:** If you are unable to access this page, verify that ports 80 and 443 are open on the firewall.

   > **Note:** When you log in to IBM® Storage Defender Sentinel anomaly scan software GUI for the first time, you are automatically redirected to the **Setup view**.

2. Go to **Administration › System › EULA**.
3. The EULA is displayed. Read through the EULA, then check the agreement and accept terms check-box.

4. Click **Save and Continue**. The **Set up License** page appears.

Setting up a license

The topic provides information about setting up a license.

In the latest release of the software, 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 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, helping ensure the most efficient distribution of the licenses among all the engines that are registered with the engine that acts as the license server. The license server issues a perpetual certificate to a license client, which can continue to use the license on the license server or not in the future.

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

Installing the license on the license server

The topic provides information about installing the license on the license server.

> **Note:** Choose an engine to function as the license server and install the license on that engine first.

To install a license locally on the IBM® Storage Defender Sentinel anomaly scan software, complete the following tasks:

1. On the **Set up License** page, copy the `Engine ID` and log in to the support portal at `http://www.indexengines.com/support`.
2. On the support portal, register your engine. After registration, you receive an email that contains the license file to download.
3. Select **Obtain and Upload License** as the licensing option to upload a license for that specific engine, whether it becomes a license server or a standalone engine. The option is the default selection.
4. Click the **Browse** link to locate and choose the license file that you received in email after you registered the engine on the support portal. Select **Open** to upload. The file name of the license includes the engine ID to which the license applies. You need to make sure that it matches the engine ID shown on the **Setup License** page of your system. If not, contact to the support team.
5. Click **Save and Continue**. When the file upload completes, the license details are displayed. Verify the license information.

Registering an engine with a license server

The topic provides information about registering an engine with a license server.

To register an engine with a license server, complete the following steps:

1. On the **Settings › License Management** page, select radio button with option as **Register with License Server** for the licensing option. The option registers the engine as a license client with the engine that is functioning as the license server.
2. Add the license server information to the following fields:
   - **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 Multi-Factor Authentication (MFA) is enabled on the license server engine or for the admin user of the license server, then enter the OTP in this field, otherwise keep it blank.

> **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.

3. When complete, click **Register** and then **Save and Continue**. The **Set up Index Maintenance** page appears.

Settings menu

From the **Settings** navigation menu, you can configure various system and administration settings.

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

Storage

From the **Storage** menu, you can view and modify index storage settings.

Go to **Settings › Storage › Index Storage** to view the amount of storage that is used, and the total storage that is allocated to the index. You can also view and modify the index storage settings on the page.

Index Storage

The **Index Storage** graph displays the index storage usage.

When a host is scanned by a policy, the anomaly scan software organizes the data in the index into segments. Each segment contains information about the host and the files that are scanned. An index can contain many segments, which can no longer be needed later. You can use two options to reclaim index storage space and remove hosts that you do not want to index.

- **Reclaim index storage**: The weekly process that manages older segments and removes versions of files that are no longer needed from the segments. You can set the weekly schedule for the process to run.
- **Enable unindexed hosts removal**: When enabled, the daily process checks for any new backups within the specified number of days for a known host, which has had previous backups analyzed, and if newer backups do not exist, removes that host and all related data from the index. If a host is scanned but later decommissioned, eliminating the need for further scans, the host is removed from the index. In this case, the host data is still in the index but is old and no longer relevant and can be removed. You can set the schedule for the process to run every 30 to 90 days.

Go to **Settings › Storage › Index Storage** to view the graphical representation of the storage used by the indexing jobs, storage availability, and reset the index. Hover over the usage line to see how much storage is being used for a particular date.

Editing the index maintenance settings

You can modify the index maintenance settings from the **Index Maintenance Settings** section. The following settings can be modified:

- When index storage is reclaimed
- Enable or disable unindexed host removal
- Modify how long to retain unindexed hosts in an index

To edit the index maintenance settings, complete the following steps:

1. Go to the **Settings › Storage › Index Storage** page.
2. Select **Index Maintenance Settings**.
3. To change the time and day of reclaiming index storage space, select a new value from the **Reclaim index storage** field calendar.
4. To enable or disable unindexed host removal, enable or disable **Enable unindexed host removal** toggle option. By default, the option is not enabled.
5. To change how long to retain unindexed hosts in an index, select a new value from the **Remove Hosts not indexed** in field. The value can be set between 30 to 90 days. The default value is 60.
6. Click **Save Changes** to save any changes that you made. Click **Discard Changes** to discard any modifications you made.

Resetting the index

To reset the index, complete the following steps:

1. Go to the **Settings › Storage › Index Storage** page.
2. To delete the current index and create a new one, click **Reset Index**.
3. To confirm the reset of your index, type **Reset Index** and then click **Confirm Index Reset**.

> **Note:** Resetting the index deletes all data. You cannot reverse the action.

User management

From the **User Management** menu, you can add, edit, and delete users and manage user roles.

Select **Settings User › Management › User Accounts** to manage user accounts.

The **User Accounts** page displays the following options:

- The username for the account that the user provides.
- The system role of the account. The admin, viewer, and alert editor are the roles.
- The type of authentication, local or Active Directory (AD) authentication.
- If AD authentication is used for the account, the AD username.
- If AD authentication is used for the account, the AD domain name.
- The status of the user, which can be active or inactive.

Users can be assigned one of the following three roles to control which pages and features are available to a user.

Table 8: Roles and description

Role	Description
admin	The admin role is the system administrator of the IBM® Storage Defender Sentinel anomaly scan software. The admin role can access all pages and modify any settings in the **Settings** menu.
viewer	The viewer role can only view the following pages: • **Alerts** • **Hosts** • **Backups** • **Settings**: View the **Index Storage** and **License Status** This role has the most restrictive permissions and is useful for users that do not need to modify settings.

Role	Description
alert editor	The alert editor role has the following permissions: • **Alerts**: Clear the alerts and select the alert configuration. • **Hosts**: Modify the index and the daily thresholds. • **Backups**: View the **Backups** page. • **Settings**: View the **Index Storage** and **License Status** information and the EULA and threshold configurations. In addition, users with the alert editor role can configure, view, modify, and delete thresholds.

User Accounts

From the **User Accounts** page, manage the user accounts by adding, editing, or deleting user accounts as needed.

Adding a user account

Complete the following steps 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:** Active Directory (AD) authentication must be enabled and a domain added in **Settings › Network and Security › Active Directory** before you use AD to authenticate the user account.

4. If you select the **Local Authentication** option, enter the following information:
   - Enter a username in the **Username** field.
   - Enter a password in the **Password** field.
   - Retype the password in the **Confirm Password** field.
   - Select a role to assign the user from the **Role** drop-down.
   - Select the toggle **Force Password Change on Next Login** option to enable it. When enabled, the user is forced to change the password on the next login to the system. By default, the option is not enabled.

     > **Note:** If you enable the option and change the password of the user at the same time, then the user is not forced to change the password at their next login.

   - Select or de-select the **Active** toggle button to specify whether the user is active.
5. If you select the **Active Directory Authentication** option, enter the following information:
   - Enter a username in the **Username** field.
   - Enter an AD username in the **AD Username** field.
   - Enter AD domain in the **AD Domain** field.
   - Select a role to assign the user from the **Role** drop-down.

- Select or de-select the **Active** toggle button to specify whether the user is active.

Editing a user account

Complete the following steps to edit a user account:

1. Go to **Settings › User Management › User Accounts**.
2. Select the account that you want to edit from the available accounts, then click **Edit**.
3. Edit the details that you want to edit, such as authentication method, password, role, force password change, and active status as needed.

   > **Note:** If you enable the **Force Password Change on Next Login** option, the user is forced to change the password on the next login, ignoring any password aging policy.
   > If you change the password of the user at the same time, the user is not forced to change the password on the next login.

4. Click **Save** to save the changes.

Deleting a user account

Complete the following steps to delete a user account:

1. Go to **Settings › User Management › User Accounts**.
2. Select the account that you want to delete from the available accounts, then click **Delete**.
   A confirmation dialog appears to confirm the deletion of the user.
3. Click **Delete** to delete the user account.

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

Alerts

From the **Alerts** menu, you can configure email notifications for security alerts and operation notifications, upload an updated malware signature file, manage custom malware signatures, and configure database corruption alerts.

Special Criteria

The **Special Criteria** page allows users to upload a newer malware signature file, view the installation date and version of the currently installed malware signature file, and configure the reporting of database corruption alerts.

On the **Special Criteria** page, you can:

- Upload a newer malware signature file
- View the installation date and version of the currently installed malware signature file
- Add or update custom malware signatures
- Configure the reporting of database corruption alerts

Uploading a malware signature file

If you have a file of malware signatures, or received the malware signature file RPM, you can upload it to the system to be used for checking other malware. After you upload 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.

You can download the latest malware signature file from the IBM repository.

Note: If you upload a more current malware signature file and a malware signature was removed from the database, then any alerts that are created by that malware signature are discarded.

Complete the following steps to upload a malware signature file:

1. On the **Settings › Alerts › Special Criteria** page, click the edit icon for the **Upload malware signature file** option.
   The **Upload malware signature file** dialog appears.
2. Drag the signature file into the **Upload malware signature file** box or click **browse** and select the file.
3. Once the file is selected, the progress status changes to in-progress and then success when finished.
4. Click **Close** to close the dialog.

Managing custom malware signatures

You can add encountered malware signatures to a custom malware signature database using the **Custom Signatures** option. In addition to the Index Engines malware database, Anomaly scan software searches the signatures in the customer malware signature database. Signatures that are added or updated through the **Custom Signatures** option 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.

Note: Only a 32-character hexadecimal MD5 signature is supported as custom signature.

Note: When a malware alert is generated from a custom signature, the Job ID is the job during which the file is 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, changes may take up to five minutes 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, complete the following steps:

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

Complete the following steps to configure the database corruption alert criteria:

1. On the **Settings › Alerts › Special Criteria** page, click the edit icon for the **Configure Database Corruption Alerting Criteria** option.
   The **Enable Alert: Database Corruption** dialog appears.
2. Select the hosts for which you want to enable the reporting of database corruption alerts.
3. To disable database corruption alert reporting for all hosts, enable the **Disable reporting for all hosts** toggle option.

4. Click **Save Changes** to save your changes.

Email Notifications

The **Email Notifications** page allows users to configure email addresses for security alerts and operation notifications.

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

- Threshold exceeded
- Infection found
- Database corruption
- Malware detected

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

- Job failed: Any indexing or post-processing job that fails.
- Job start and job done: Any indexing job or post-processing job that starts and finishes.

Complete the following steps to configure email addresses for security alerts and operator notifications:

1. Go to the **Settings › Alerts › Email Notifications** page.
2. Under **Security Alerts**, type an email address in the text box and press Enter. The email address is added to the list. Add more emails if needed.
3. To delete an email address, click the delete icon that is associated with the email address.
4. Under **Operations Notifications**, type an email address in the text box and press Enter. The email address is added to the list. Add more emails if needed.
5. Select the options for operation notifications as needed:
    - **Job Failed**: When an indexing or a post-processing job fails.
    - **Job Started and Job Done**: When an indexing job or a post-processing job starts and finishes.
6. To delete an email address, click the delete icon that is associated with the email address.
7. Click **Save Changes** to save your changes.

Network and Security

From the **Network and Security** menu, can configure security and network settings for login, password, Active Directory (AD), security certificates, and diagnostics and reporting.

Login

From the **Login** page, you can configure inactive timeout and failed login attempt for a user.

You can configure the following options:

- **Allow Inactivity Timeout**: When enabled, the user account is logged out after the specified time of inactivity, which is set in minutes.
- **Failed Login Attempts Limits**: The option sets the number of failed login attempts within a configured time period, which can be set in seconds, minutes, or hours. If a user account exceeds the configured number of attempts within the set time, then the account is locked. You can set the limit for the number of attempts within a configured number of seconds, minutes, or hours.

Complete the following steps to configure login settings:

1. Go the **Settings › Network and Security › Login** page.

2. Toggle the **Allow Inactive Timeout** option. Specify the timeout option in minutes. The option is not enabled by default.
3. Under **Failed Login Attempts Limits**, set the number of attempts within seconds, minutes, or hours. The option is not enabled by default.
4. Click **Save** to save changes.

Password

From the **Password** page, you can configure complexity of password for user accounts.

Complete the following steps to configure password complexity:

1. Go the **Settings › Network and Security › Password** page.
2. Select the password complexity sections that you want to enable. You can configure the following options:
    - **Password Length**: Set the minimum and maximum password length.
        - **Minimum Characters**: The minimum length of the password, inclusive
        - **Maximum Characters**: The maximum length of the password, inclusive.
    - **Password Complexity**: Configure the minimum number of uppercase letters, lowercase letters, numerical characters, and special characters.
        - **Lowercase Letter(s)**: The minimum number of lowercase letters, inclusive.
        - **Uppercase Letter(s)**: The minimum number of uppercase letters, inclusive.
        - **Numerical Character(s)**: The minimum number of numerical characters, inclusive
        - **Special Characters**: The minimum number of special characters, inclusive. The special characters list includes !, @, #, $, %, (,), and other non-alphanumeric characters.
        - **Maximum Number of Consecutive Repeated Characters**: The maximum number of a consecutive identical character in a password.
    - **Password Uniqueness**: Set the uniqueness of password.
        - **Password must not include username**: Restricts the password from containing the username.
        - **New password must be different from X previous passwords**: The number of previous passwords that cannot be used.
    - **Password Change Policy**: Set the password expiration period and limit the number of password changes allowed within a 24-hour period.
        - **Password Expiry (Days)**: The maximum number of days before the password expires and the user is forced to change the password.
        - **Password changes allowed within 24 hours**: The maximum number of times a user can change password in a 24-hour period.
3. Click **Save Changes** to save the configuration.

Active Directory

From the **Active Directory** page, you can enable Active Directory (AD) for your engine.

You can integrate Active Directory (AD) to authenticate user accounts. Make sure that the users for which you enable AD option must have AD user accounts. Each engine handles the AD queries by using the client/server licensing model. If you want to integrate AD, you need to set up AD on each engine.

When you enable AD and add a domain name with proper user account credentials, the following information is displayed in a tabular format:

- **QUERY DOMAIN**: The user's AD account is configured with no query restrictions. Certain accounts can limit the number of times the account can query the AD domain before the user locked out.
- **DOMAIN NAME**: The domain name of the AD domain.

- **DNS NAME**: The Domain Name System (DNS) name of the AD domain, which contains the domain name and the domain extension.
- **QUERY STATUS**: The status of the probe operation that occurs when you enabled AD. The status is either **Successful** or **Not Queryable**.

Complete the following steps to enable AD for your engine:

1. Go the **Settings › Network and Security › Active Directory** page.
2. Toggle the **Domain** option to enable AD integration.
3. Add an AD username and password in the **Account** section.
4. Select **Save Changes**. The newly added AD account is added to the AD accounts table.

Security Certificates

From the **Security Certificates** page, you can upload security certificates for SSL/TLS connections.

You can configure SSL/TLS connections and security certificates on the **Settings › Network and Security › Security Certificates** page. An HTTPS request requires SSL/TLS certificates to establish secure communication between the browser and server.

Complete the following steps to upload security certificates for SSL/TLS connections:

1. Go the **Settings › Network and Security › Security Certificate** page.
2. Click **Upload Files**. A pop-up appears to upload private key and certificate.
3. Click **Choose Private Key** and select the private key file.
4. Click **Choose Certificate** and select the certificate file.
5. Click **Upload** to upload to files.
   After upload, the certificate details are displayed in the **Certificates** table on the page.

Diagnostics and Reporting

From the **Diagnostics and Reporting** page, you can enable the audit trail heartbeat, which sends an event every hour to the audit trail log. The audit trail heartbeat checks that the engine is operational. You can also enable the diagnostics log reporting that sends status report and crash reports to the scan engine.

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 that is taken, the 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, scheduling an action query, and starting and stopping services. After enabling the audit trail logging, enable the audit trail heartbeat in **Settings › Network and Security › Diagnostics and Reporting**.

Complete the following steps to enable audit trail logging:

1. Save a copy of the `/etc/rsyslog.conf` file.
2. Update the `/etc/rsyslog.conf` file as follows:
   a. Verify that the following four entries are not commented. If a # sign appears in front of any of these entries, then remove the # sign:

   ```
   $ModLoad imudp
   $UDPServerRun 514
   $ModLoad imtcp
   $InputTCPServerRun 514
   ```

   b. Add the following line to the `/etc/rsyslog.conf` file before the `$IncludeConfig` entry:

   ```
   LOCAL1.* /var/log/iesyslog.log
   ```

> **Note:** If you use the backup feature to return your logs, store the logs in the `/opt/ie/var/` directory. For example: `/opt/ie/var/log/iesyslog.log`.

c. In the `/etc/rsyslog.conf` file, add `local1.none` to the line for `/var/log/messages` as follows:

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

> **Note:** The line in the `/etc/rsyslog.conf` file can look different than the example because of your operating system.

3. Restart the `rsyslog` service by issuing the following command:

```
systemctl restart rsyslog.service
```

The `/var/log/iesyslog.log` file now records all user actions. Your system administrator can manage the file by using **`logrotate`** or a similar command to rotate and purge logs as needed.

When the setup completes, activity messages start appearing in the `/var/log/iesyslog.log` file.

Enabling the Audit Trail heartbeat

To enable audit trail heartbeat, verify that audit trail logging is enabled. To enable the audit trail heartbeat, complete the following steps:

1. Go the **Settings › Network and Security › Diagnostics and Reporting** page.
2. Toggle the **Heartbeat** option under the **Audit Trail** to enable it.
3. Click **Save Changes**.

Setting the diagnostic log file reporting

1. Go the **Settings › Network and Security › Diagnostics and Reporting** page.
2. Select the checkbox under **Diagnostic Log File Reporting** to enable it.
3. Click **Save Changes**.

License management

From the **License Management** menu, you can view the license status, license details, and the EULA.

License Status

The **License Status** page displays the license usage graph. The graph shows the amount of active data in the current index on an engine over time and the total amount of active data that is available in the license.

Select the varied line to view the amount of active data used on different days. You can also download a CSV file that contains license information from the time when you installed the license.

Now, you can share licenses between multiple engines with the client/server licensing model. One engine can act as a license server for several engines by dynamically distributing its license to engines at the site. Engines automatically request and return license counters as their active data changes over time to make most efficient distribution of the licenses among all the engines that are registered with the engine that acts as the license server. The license server issues a perpetual certificate to the license clients, whether 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 acts as the license server. Next, you can register other engines with the license server. All the registered engines 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 and also the amount of active data from that host at various points in time. The **License Status** graph displays the total amount of active data that is used by all hosts that are listed in the license CSV report for a specific date. The 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 have not been indexed for a long time. If a host has not been indexed in a long time, it indicates that the host is no longer active, and the host may be decommissioned. To automatically remove non-active hosts from the index and avoid using active data, enable **Remove Unindexed Hosts** on the **Settings › Storage › Index Storage** page.

To download the license capacity CSV report, go to **License Management › License Status** page. Select the download icon and when prompted, save the CSV file.

The CSV file includes the following columns:

- **Client hostname**: The hostname of the client.
- **Date**: The date and time when the active data amount that is used by the host is evaluated.
- **Active Data**: The amount of active data used in the index for that host.

License Details

The **License Details** page displays all license client engines that have received a certificate from the license server that you are accessing.

The list on the **License Details** page includes license client engines that are not active, cannot establish connection to the license server, or not 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 are listed in the order of most recently established a connection to the license server.

In the **License Server** section, **Host** displays the server details if it is registered with the license server. If the server is not registered with a license server, then either register it with a license server or use it as local license. In the **License Clients** section, the table lists the license clients that have registered the server as a license server.

Editing the license

To edit the license, complete the following steps:

1. Go to the **Settings › License Management › License Details** page.
2. If you currently use a local license installed on an engine, but want to add a license by registering with a license server, select **Register with License Server**. Enter information for the following fields and click **Register**:
    - **Hostname**: The name of the license server host. The license can be accessed by one or more engines.
    - **Username**: The only permissible username is the `admin` account of the license server and cannot be changed.
    - **Password**: The password for the admin account of the license server.

      > **Note:** If the password of the admin accounts is changed later, you do not have to update the password on the page.

    - **One-Time Password**: If MFA has been enabled on the license server engine or for the admin account on the license server, then enter the OTP.

      > **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 authentication app.

3. Select **Register**. When the license client is successfully registered with the license server, the license server is displayed as host.

4. If you previously registered with a license server and now want to use a locally installed license on your engine, complete the following steps:
    a. Select **Deregister**, and then select the **Upload License** option.
    b. Select **Upload License**. When prompted, select your license file to upload.
    c. Select the **Upload License** button to complete the process. With a locally installed license, the engine can now function as a license server if needed.

Moving to client/server licensing on existing engines

Now, you have the option to use a new licensing model, which is a client/server model to share licenses. 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. The 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.

You can install licenses locally on each engine or choose to add Active Data by 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 locally installed license and the remaining Active Data on the license server engine.

To calculate the amount of Active Data for the indexes of your engines, note the Active Data amount displayed in the **Settings › License Status** page 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 and multiply by the number of license clients.

License overdraft

When the amount of licensed Active Data has been exceeded, you receive a notification in the email informing you of an overdraft of your license. There is a 90-day grace period until IBM® Storage Defender Sentinel stops analyzing data. If the amount of Active Data decreases under the license capacity, then the 90-days grace period resets.

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** page. The report lists the client hosts, the date on which last indexed the host's files, and how much Active Data is allocated to each host.

Review the last date when host files were indexed along with the amount of Active Data that are used by that particular host. If a host is no longer active, IBM® Storage Defender Sentinel still attributes Active Data to that host until you remove the host from the index. You can configure the **Index Maintenance Settings** to remove those hosts that have not been indexed for a long time. By removing the hosts from the index list, you can make Active Data available, which will then be available to other hosts.

EULA

From the **EULA** page, you can view the EULA that you signed during the installation process.

To view the EULA that you signed at the time of installation, go to the **Settings › License Management › EULA** page.

Advanced

The **Advanced** menu provides options to configure threshold monitoring, manage YARA rulesets and trusted files, recover files from a restored backup, and set the custom YARA ruleset in the global control.

Custom thresholds

The **Custom Thresholds** page displays the threshold definitions and provides the option to create new threshold definitions. Only the threshold definitions for the selected host are displayed on the page.

To view a threshold's configuration from the **Custom Thresholds** page, select the **+** icon for a specific threshold. You can expand multiple threshold at a time.

The **Custom Thresholds** page displays the following information:

- **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 IBM® Storage Defender Sentinel anomaly scan software.
- **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**: The actions that can be taken on the threshold definition, which are edit and delete.

A custom threshold defines a threshold at a 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. In addition, you can 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 when a custom threshold is reached with every scan of a host.

You can view the graphs for custom threshold definitions for a host by navigating to**Hosts › View › Custom Thresholds**. Each configured severity level is indicated on the graphs with by using a specific color dashed line. If you change the severity level values of the daily activity threshold, the lines move based on the new values you provided.

Alerts are generated when a custom threshold is exceeded with every scan of that host. This is different than the hosts threshold alerts, which only occur once in a 24-hour period.

> **Note:** Custom thresholds work with Full, Incremental, and Differential backups, but not with virtual machines by using Delta Block Analysis.

The following options are available to configure threshold:

Creating a custom threshold

Complete the following steps to configure threshold:

1. On the **Settings › Advanced › Customer Threshold** page, click **Create Threshold**.
2. The **New Custom Threshold** page appears. Toggle the **Enable Alert Threshold** to enable generating alerts when the daily activity limit has been reached. By default, the option is enabled.
3. Add the following information on the **New Custom Threshold** page:
    - **Name**: A user-defined name of the threshold configuration. You can use a name that describes the threshold type, such as "Deleted Files - 10 Percent - Finance Servers". It helps you to easily identify the exceeding threshold and the associated host.
    - **Type**: Select one of the following options from the drop-down:
        - **Added Files**: The number of added files that has occurred between the last two backups analyzed.
        - **Changed or Deleted**: The number of files that have changed content or the files have been deleted since the last backup analyzed. This monitors a comprehensive change to the files or folders, combining deletions and file content changes.
        - **Changed File Type**: The number of files in a previous backup that have a different file type in the current backup.

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

    - **Deleted Files**: The number of deleted files that has occurred between the last two backups analyzed.
    - **Entropy**: The randomness of data in a file and generally indicates file encryption. Encrypting a file typically increases the entropy of the file. The entropy value ranges from 0 (no entropy) to 100 (maximum entropy).
- **Data Format**: The number of files affected by the change type as a percentage or quantity. Select Quantity or Percentage. For **Entropy**, only the **Percentage** option is available.
- **Severity**: 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:
    - **Critical**
    - **High**
    - **Medium**
    - **Low**

  A threshold exceeded alert is triggered when the number or percentage of changed files is greater than the value set for a severity level. 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:
    - **Critical** to **20**
    - **High** to **15**
    - **Medium** to **10**
    - **Low** to **5**
- **Minimum**: The option is only available for the **Entropy** change type. It configures the minimum entropy that the configured percentage of files must be for an alert to be generated. For 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.

4. For the **Add Location** field, provide the following inform
    - **Host**: The name or IP address of the host that you want to monitor for changes.
    - **Path**: The path can be a directory or a path to a file. This is defined relative to the snapshot.
    - **Include Subdirectories**: The threshold is applied to the host and path and any existing subdirectories to analyze the files for changes.

    > **Note:** For more information, see Hosts and paths.

5. Click **Save Changes** to save the configuration.

Editing a custom threshold

To edit a custom threshold, complete the following steps:

1. On the **Settings › Advanced › Custom Threshold**, select the **Edit** icon under the **ACTIONS** column.
2. The **Edit Custom Threshold** page appears. Toggle the **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 information for the following fields:

- **Name**
- **Type**
- **Data Format**
- **Severity**
- **Minimum**

4. . For a location , edit the following information:
   - **Host**
   - **Path**
   - **Include Subdirectories**
5. Select **Add Location +** to add more locations to the threshold.
6. Click **Save Changes** to save the configuration.

Hosts and paths

For threshold definitions, you need information about the front-end host and the path that you want to monitor.

Hosts and Paths

The front-end host can be defined with either the name or IP address. A path is a text string that starts with a slash (/) and specifies a path and a file name or just a path to a folder. When you are specifying a path to a folder, you must end the text string with a (/) slash. The section describes how the text string in the **Host** and **Path** fields breaks down into its various components, how to escape special characters in the text string, and how to indicate system folders in the path.

> **Note:** The examples are Linux-based path syntax unless otherwise specified.

Hosts

In the following example, the threshold definition specifies the host that was indexed in the backupset. 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`. If you configured your backup software to use the IP address of a host, use the IP address. If you configured your backup software to use the hostname, use the hostname.

> **Note:** Some backup software or indexing methods do not use the IP address or hostname. If you are using Avamar, you need to use the Avamar Client ID as the host. For virtual machine backups, the hostname can be a virtual machine name that is given by the virtual machine host and can be different from the virtual machine DNS name. In other cases, the hostname can be the IBM® Storage Defender Sentinel policy name.

Path to a folder

The following example is an Linux-based path to a folder:

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

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 example is an Linux-based path to a file:

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

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

Table 9: Components of a file path

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 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 backup software or indexing methods do not use the drive letter designation. For VM backups, the drive letter can 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 that is named `Marketing`.

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

```
Sales|/Marketing
```

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

Table 10: Escaping special characters

Field	Special characters
Host	• / • \ • | • :
Path	• / • \ • |

Specifying 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`). The character combination is interpreted as a system folder, such as:

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

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

Table 11: System folder path

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

Some backup agents, such as NBU and IBM Storage Protect, create disk image backups of a virtual machine (VMDK) instead of at the file level. With these types of VMDK backups, IBM® Storage Defender Sentinel extracts the file information, but not the complete path name of the file locations. This information indicates the disk and partition information where the file is stored on. 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 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 IBM Storage Protect VM disk backup and indexed by IBM® Storage Defender Sentinel. 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 to monitor all the folders and files on the host.

Specifying a location

You can specify a location of a file name of an attachment. The following example describes the text string in the **Location** field where you need to specify a service root and the file name of an attachment.

```
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.

Table 12: Specifying a location

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 is terminated by a colon (`:`), then the next path component is the name of an application service hosting the data. If the hostname is terminated by a slash (`/`), then the rest of the path indicates files in the file system 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.

Component	Description
`08294367ac73b35f`	The filename of an Exchange email message. If this path component is terminated with `|>` , then it is a file name, 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

The following example describes a text string that specifies a location on a Windows drive:

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

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

Table 13: Specifying a location on a Windows drive

Component	Description
`exch1.example .com`	The hostname. This example ends with a slash.
`C:`	The name of the drive.
`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 file name. The path component terminator `|>` indicates that it is a file name.
`Dave Smith`	A folder name, which is a mailbox in this case.
`Sales/Marketing`	A folder name under `Dave Smith`. The folder has a slash in its name and that is escaped by the pipe `|` and followed by a slash `/`.

Custom YARA rulesets

YARA rules are customizable specifications that look for patterns in files and file content to identify and classify malware before a cyberattack.

You can add custom YARA rulesets to detect possible malware in the PE32 files of your front-end hosts by 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.

A rule is typically comprised of the following two sections:

- `strings`: The section contains regular expressions, hexadecimal or text strings, and XOR strings.
- `conditions`: The section contains Boolean expressions and if the match is found to the pattern defined in the `strings` section, the expression returns `true`.

Some complex YARA rules can include an additional `metadata` section, which defines custom rules.

For more information on YARA rules and usage, see official YARA documentation .

Note: YARA rulesets only apply to PE32 files.

IBM® Storage Defender Sentinel anomaly scan software applies the custom YARA ruleset while reading the file content on the host during indexing when a policy job runs.

Example - Simple text YARA ruleset

The following example shows a simple YARA ruleset that returns `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

The following 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

You can create a custom YARA ruleset to detect possible malware in the PE32 files of your front-end hosts.

To create a custom YARA ruleset, complete the following steps:

1. Go to **Settings › Advanced › Custom YARA Rulesets** page, select **Create New Ruleset**. The **YARA Ruleset Creator** page opens.
2. In the **YARA Ruleset Creator** page, add the following information:
   - **Enable Ruleset:** Select to enable or disable the ruleset after you have created a rule. When disabled, the rule is not used during indexing.
   - **Select Ruleset**: When you click the option, it opens a ruleset definition file, which can contain one or more rules. The supported file types are `.yar` and `.yara`. The YARA ruleset file is displayed in the editor pane for further editing if needed.
   - **Ruleset Name**: Name of the ruleset. Name length must be between 3 and 128 characters inclusively. Special characters and numbers can be used in the ruleset name. For more information about rule name restrictions, see official YARA documentation.
   - **Alert Severity**: select an alert severity from the dropdown list. The available options are:
     - **Critical**
     - **High**
     - **Medium**
     - **Low**

   Alternatively, you can add the YARA ruleset text in the editor pane.

3. After adding a YARA ruleset, click **Verify** to verify the correctness of the rule you have created. If you receive errors, fix errors and verify the ruleset again. When you are developing the ruleset in the editor, you must verify your rule to avoid errors.
4. When the ruleset has been verified, click **Submit Ruleset**. If you selected a YARA ruleset from a file, the file gets uploaded.

When you create at least one ruleset, IBM® Storage Defender Sentinel anomaly scan software indexes all PE32 files during the next indexing operation. IBM® Storage Defender Sentinel anomaly scan software checks the PE32 files against the newly added YARA ruleset.

Editing a YARA ruleset

You can edit the existing YARA ruleset as per your requirement.

To edit a custom YARA ruleset, complete the following steps:

1. Go to **Settings › Advanced › Custom YARA Rulesets** page, select the edit icon for an existing ruleset.
2. On the **YARA Ruleset Editor** page, add the following information:
   - **Enable Ruleset:** Select to enable or disable the ruleset.
   - **Select Ruleset**: Select a ruleset file. The supported file types are `.yar` and `.yara`.
   - **Ruleset Name**: Name of the ruleset.
   - **Alert Severity**: Select an alert severity from the dropdown list.

   If needed, edit the YARA ruleset text in the editor pane.
3. After editing the YARA ruleset, click **Verify** to verify the correctness of the rule you have created. If you receive errors, fix errors and verify the ruleset again. When you are developing the ruleset in the editor, you must verify your rule to avoid errors.
4. When the ruleset has been verified, click **Submit Ruleset**. If you selected a YARA ruleset from a file, the file gets uploaded.

When you modify at least one ruleset, IBM® Storage Defender Sentinel anomaly scan software indexes all PE32 file during the next indexing operation, regardless of whether the files are changed or not IBM® Storage Defender Sentinel anomaly scan software checks the PE32 files against the updated YARA ruleset.

Deleting a YARA ruleset

You can delete the existing YARA ruleset if you do not need it.

Use one of the following steps to delete a YARA ruleset:

1. Deleting a YARA ruleset from the **Custom YARA Ruleset** page:
   a. Go to **Settings › Advanced › Custom YARA Rulesets** page.
   b. Select **Delete**. When prompted to confirm the deletion, select **Delete** in the confirmation window.
2. Deleting a YARA ruleset from the editor:
   - Go to **Settings › Advanced › Custom YARA Rulesets** page, select the edit icon for an existing ruleset.
   - On the **YARA Ruleset Editor** page, 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 IBM® Storage Defender Sentinel anomaly scan software as trusted files.

During analysis, IBM® Storage Defender Sentinel anomaly scan software identifies the type of each file based on its content. If IBM® Storage Defender Sentinel anomaly scan software cannot identify the file type. For example, 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 IBM® Storage Defender Sentinel

anomaly scan software is generating **Infection Found** alerts when there is no data corruption, use the trusted file 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 IBM® Storage Defender Sentinel anomaly scan software encounters a file of an unknown type and it matches a filename pattern, it consider the file type as known and trusted. This reduces the possibility of incorrect **Infection Found** alerts.

File types are displayed when the **Show Files** option is selected on an alert in the **Alerts** table on the **Alerts** page. File types that IBM® Storage Defender Sentinel anomaly scan software identifies as unknown but they match to a filename pattern in the trusted files list are labeled **Trusted**. File types that are identified as unknown are displayed as **Unknown**.

The **Alerts › Show Files** table indicates the status of the files at the time of the application generated alerts. Subsequent changes to the trusted files patterns only affect in the next analyses.

Creating a trusted file name pattern

You can create trusted file name patterns to reduce the number of false alerts generated by the application

To create a trusted file name pattern, complete the following steps:

1. Go to **Settings › Advanced › Trusted Files**.
2. Select **Add**.
3. In the displayed pane, type the file name patterns, you can enter multiple file patterns and separating them by using the **Enter** key.

   > **Note:** File name patterns are case-sensitive.

4. Click **Save** when complete addition of file name patterns.

The file name patterns are displayed. Files that are matching the patterns are considered as trusted files.

The **Alerts › Show Files** table indicates the status of the files at the time of the application generated alerts. Subsequent changes to the trusted files patterns only affect in the next analyses.

Editing a trusted file name pattern

You can edit an existing trusted file name pattern based on your requirement.

To edit a trusted file name pattern, complete the following steps:

1. Go to **Settings › Advanced › Trusted Files**.
2. Select the **Edit** icon for the file name pattern to edit. In the displayed pane, edit the pattern. When done, click **Save**. The edited pattern is displayed in the list.

Deleting a trusted file name pattern

You can delete a trusted file name pattern if you want to remove the pattern from the application.

To delete a trusted file name pattern, complete the following steps:

1. Go to **Settings › Advanced › Trusted Files**.
2. Select the pattern to delete and then select **Delete**.
3. In the **Delete Filename Pattern(s)** window, select **Delete** to confirm.

The pattern is removed from the list.

Global resets

Global resets allow you to reset application-level features.

By using global resets, you can reset the following application-level settings:

- Application index
- YARA rulesets
- Existing thresholds

> **Note:** Resetting any of the settings cannot be reversed.

Resetting the index

You can reset the index to delete the current index and any associated data and create a new one.

> **Note:** Resetting the index deletes all the associated data. The action cannot be reversed.

To reset the index, complete the following steps:

1. Go to **Settings › Advanced › Global Resets**.
2. To delete the current index and create a new one, select **Reset Index**.
3. To confirm the reset of your index, type **reset index** in the text field and then select **confirm Reset Index**.

Resetting YARA rulesets

Reset the YARA rulesets to delete any existing YARA rulesets.

> **Note:** Resetting the YARA rulesets will delete all existing YARA rulesets. The action cannot be reversed.

To reset YARA rulesets, complete the following steps:

1. Go to **Settings › Advanced › Global Resets**.
2. To delete existing YARA rulesets, select **Reset YARA Rulesets**.
3. To confirm the deletion of the existing YARA rulesets, type **reset yara rulesets** in the text field and then click **Confirm YARA Ruleset Reset.**.
4.

Resetting custom and daily activity thresholds

Reset the thresholds to delete any existing custom thresholds and daily activity thresholds.

> **Note:** Resetting the thresholds deletes all existing thresholds. The action cannot be reversed.

To delete thresholds, complete the following steps:

1. Go to **Settings › Advanced › Global Resets**.
2. To delete existing thresholds, select **Reset Thresholds**.
3. To confirm the deletion of the existing thresholds, type **reset thresholds** in the text field and then click **Confirm Threshold Reset**.
4.

Global feature options

Global resets allow you to globally enable/disable all custom YARA rulesets.

> **Note:** Only users that have admin role assigned can access this page.

To globally enable or disable YARA rulesets, complete the following steps:

1. . Go to **Settings › Advanced › Global Feature Options** .
2. From the **All custom YARA rulesets** dropdown, select:
   - **Enable** to enable all custom YARA rulesets.
   - **Disable** to disable all custom YARA rulesets.
3. When prompted, select **Enable all YARA rulesets** or **Disable all YARA rulesets** to confirm the selection.

> **Note:** When you globally enable or disable YARA rulesets, the selected option resets the default configuration. You can enable or disable individual YARA rulesets on the **Custom YARA Rulesets** page and that setting overrides the global setting.

Upgrading the IBM® Storage Defender Sentinel anomaly scan software

This section provides instructions on upgrading the IBM® Storage Defender Sentinel anomaly scan software through the GUI. For new installations, see "IBM Storage Defender Sentinel anomaly scan software installation" on page 18.

> **Note:** Read the following sections in "Preparation" on page 9:
>
> - "Server requirements and recommendations" on page 9
> - "Special considerations" on page 16
> - "Tasks prior to installation" on page 16
>
> They contain additional information and steps that you will need to perform to ensure a smooth upgrade. This includes tips on server requirements, what to do if your host system does not have Internet access, and how to install the package dependencies from the repository bundle downloaded from the Passport advantage online.

Procedure to upgrade the software

Procedure

It is recommended that you do what is necessary to allow Analyze and Merge jobs to complete before performing an upgrade. Please follow these steps to update the IBM® Storage Defender Sentinel anomaly scan software:

> **Important:** It is recommended that you check the IBM Defender Sentinel Portal for repository bundle updates before updating. This is especially the case when upgrading between major releases (e.g., 8.12 to 8.15) as there may be new dependencies. If you choose not to do this step, you may encounter dependency errors while updating and you will need to download and install the new repository bundle.

1. Download the desired .tar file from the Passport advantage online.

   > **Note:** For steps on how to use Passport advantage online website, refer to Download Information.

2. Log in to the host system via the command line interface using the root credentials.
3. Change directories to the directory containing the new .tar file.
4. Untar the file using following command:

   ```
   tar -xf indexengines-2.3.0-1.10-el9.x86_64.tar
   ```

5. Execute the following command to install the software:

   ```
   sh install_ie *.rpm
   ```

   > **Important:** If members show a loss of communication with the manager or if members report a license issue, you might need to unjoin and rejoin with the manager, restart the member, and reselect the original index to resume work.

Commands to manage the IBM® Storage Defender Sentinel anomaly scan software services

The IBM® Storage Defender Sentinel anomaly scan software “dservice” command is found in the `/opt/ie/bin` directory. The anomaly scan 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 anomaly scan software Services	`dservice status [all] <service name>`
Restart anomaly scan software Services	`dservice restart [all] <service name>`
Stop anomaly scan software Services	`dservice stop [all] <service name>`
Start anomaly scan software Services	`dservice start [all] <service name>`

Installation checklist

Follow the required steps below to complete the IBM® Storage Defender Sentinel anomaly scan software installation.

- **Prerequisites - Portal access**
  - The License Owner or other authorized user has signed the End User License Agreement (EULA).
- **Prerequisites - Host server**
  - Server is built that meets the requirements. For more information about requirements, see *Server requirements and recommendations* in IBM Documentation and ensure that the OS is updated.
  - Drives are partitioned to meet requirements.
  - Firewalls are either stopped/disabled OR configured.
  - SELinux is disabled or permissive
  - `/etc/hostname` configured with hostname.
  - `/etc/hosts` is configured with long and short hostname added to local host `127.0.0.1`.
  - Optional – postfix or sendmail is active and enabled. Successful email verified from anomaly scan software server to intended domain.
  - `atop` is installed, enabled, active and rotating properly.
  - DNS or `/etc/hosts` is configured as needed.
  - CLI access verified from your administration server (PC).
  - Run `CheckEngine.sh` to confirm that above before proceeding.
- **Prerequisites – Software**
  - Download/Install the IBM® Storage Defender Sentinel anomaly scan software provided repositories.
  - Download the IBM® Storage Defender Sentinel anomaly scan software .tar file.
- **Installation – Software**
  - Install the anomaly scan software – About 20 minutes.
  - Verify all services are running.
- **Configuration**
  - Log in to GUI - Record the manager Engine ID.
  - Receive email with the license (.txt file).
  - GUI – Upload the license.
  - GUI - **Administration › Home › Index Manager › Add Index** to add an index; then **Select Index** to select the index.
  - GUI - **Administration › Home › Index Manager › Defaults** to make these selections:
    Full Content, Map to Lowercase, CS Data Collection: Enabled, Synthetic Incremental: Enabled, Use Change Time for Incremental Indexing: Disabled
  - GUI - **Administration › Home › Index Manager › Merge Options** to set options.
    Purge after 30 Days, Pause Yes, Policy Purge Deleted, Days to Keep 30
  - GUI - **Administration › Home › Index Manager › Merge Segments**to add a merge job.
    Yes, Yes, No, Do Not Pause, 2, 720 – Schedule as required after first full scan
- **Validation**
  - Reboot the manager engine.
  - Run `CheckEngine.sh` to confirm the configuration and that all anomaly scan software processes are running.

- Confirm that you can log into the anomaly scan software GUI.
- If email is supported, confirm that email was received by the expected recipients.

Navigating the IBM® Storage Defender Sentinel anomaly scan software

This chapter will guide you through the IBM® Storage Defender Sentinel anomaly scan software and show you how to navigate the software application.

Navigating the IBM® Storage Defender Sentinel anomaly scan software

After you received the license, then logged in to the IBM® Storage Defender Sentinel anomaly scan software to activate your license, it's a good idea to check the status of your system. The **Engine Status** page provides this information, and opens by default from now on, whenever you log in to the anomaly scan software.

Navigation is easy, for example to navigate to the **Engine Status** page at any time:

1. Start by selecting the **Administration** link, located along the top right portion of the screen.
2. Next, point to the **Administration** menu located on the far left. The **Administration** sub-menus open.
3. Point to the **Home** sub-menu. The **Home** sub-menus open.
4. Finally, select the **Engine Status** menu.

In the following sections, the navigation instructions have been shortened as follows:
Administration › Home › Engine Status, which assumes that the **Administration** link on the navigation bar was selected.

The **Engine Status** page is a good place to begin exploring the anomaly scan software. The key components of this page are covered next.

The numbered markers on the **Engine Status** page indicate the five key areas of the screen that follows:

1. Navigation Links
2. System Identification
3. Administration Menu
4. Engine Status
5. Service Status

An overview of each key area appears next, with additional details following.

Navigation links

The navigation links provide quick access to the following pages in the GUI:

Link	Action
Message Center	Opens the **Message Center** page that displays alerts and messages, providing a centralized location for information about IBM® Storage Defender Sentinel anomaly scan software services and jobs.
Setup	Opens the **Setup** page that provides system configuration and network settings as well as a tab for uploading anomaly scan software updates.
Manage	Opens the **Manage** page that lets you add, edit, and delete user accounts and roles, check engine and service status, manage Productions, Collections, archive jobs, and action queries.
Index	Opens the **Index** page where you can configure and launch file server indexing and/or catalog ingestion jobs. You can also view all related reports, such as backup hosts, segment and tape/extraction reports.
Search	Opens the **Search** page, providing access to the powerful features of the anomaly scan software.

Link	Action
Administration	Opens the (default) Engine Status page and access to the **Administration** drop-down menus and sub-menus such as **Tape Manager** and **Index Manager**, among many others.
Help	Provides access to anomaly scan software documentation and a link to the IBM Storage Defender Sentinel Support.
Sign Out	Logs you out of the anomaly scan software.

For detailed information about each of these pages and options, please see "IBM Storage Defender Sentinel anomaly scan software site map" on page 64.

System Identification

Your login and engine names always appear at the top right of the screen, along with the name of the currently selected index. This information is very important if you have:

- more than one index
- a platform consisting of several IBM® Storage Defender Sentinel anomaly scan software systems
- different users accessing the system.

Administration menu

The Administration menu becomes accessible after you select the **Administration** located along the top right of the screen or in the horizontal menu bar. As discussed in the previous example, use your mouse to hover over this menu option and then point to an option in the sub-menu that appears. This in turn sometimes opens another sub-menu of additional choices. The Administration menu options are shown and explained next.

The Administration menu provides access to the following sub-menus:

- **Home**

  Provides access to the Engine Status page and the following pages and their sub-menus: Extraction Service, Index Manager, Index Segments, Indexing Service, File Server Indexing, Action Query, and Tape Manager.

- **System**

  Provides access to various pages so you can accept the latest EULA, adjust settings, upload licenses, access log files, set up users and email alerts, select a collection, and recover a system backup.

- **Network**

  Provides direct access to the Location Manager page where you can access location data, path replacements, and define skip directories. You can also access NIS settings from this menu, as well as the User Identity pages for downloading and uploading user identity files. In addition, this menu provides an alternate way to access the **Setup › Network › Configuration** and **Software pages** for configuring Active Directory, Security settings, iSCSI, Login settings, Email alerts; and for installing software updates.

- **Reports**

  Provides an alternate way to access the **Index › Reports › Backup Hosts**, **Backupsets**, **Segments**, and **Tape and Extraction** pages.

For detailed information about each menu, please see "IBM Storage Defender Sentinel anomaly scan software site map" on page 64.

Engine status

The **Engine Status** panel provides a high level view of the current state of your IBM® Storage Defender Sentinel anomaly scan software system. Several small buttons associated with the Engine Status (and Service Status) listings also appear on this page. In the preceding screen image, for example, the square icon located to the right of the "Index Segments" status is a button. Clicking that button opens the **Index › Reports › Segments**

page, providing detailed information about the segments that make up your index. Similarly, you can access additional information regarding other listings by clicking their associated square icon buttons.

The two most important pieces of information on the **Engine Status** panel are **Disk Status** and **Disk Space**:

- **Disk Status**

  Informs you of the current state of the disk array on a physical system. This information does not pertain to VMs.

- **Disk Space**

  Reports on the currently available space in the /opt/ie file system. The anomaly scan software will not properly function without adequate free space in this file system. Please open a new case in the IBM Storage Defender Sentinel Support as soon as this starts to become an issue.

Service Status

The **Service Status** panel, located on the lower portion of the **Home** page, provides the current status of each service and indicates if any jobs are currently running. If any services are not running, or if any issues arise with the system license, appropriate messages appear on or below this section of the screen.

Post Attack workflow

This section explains what to do if you suspect a ransomware attack and also the steps you should take to qualify the alerts and identify known good backups.

Post Attack workflow

Once ransomware is detected, it is critical to take immediate action to resolve any potential issues. You need to immediately contact your internal Security team and IBM Storage Defender Sentinel Support to investigate the extent of the potential threat and fix it if necessary.

In some cases, you may need to recover your server's operating system and application installation before IBM® Storage Defender Sentinel anomaly scan software can recover the last known good application data. It's a good practice to have cold/offline servers standby that can be used as backups in an emergency.

If you have any questions about the detection status, contact IBM Storage Defender Sentinel Support. IBM® may assist with questions about the solution, troubleshoot recovery needs, and may refer you to IBM® Services for more extensive threat mitigation assistance.

IBM® Storage Defender Sentinel anomaly scan software analyze dashboard

The analyze dashboard displays information related to alerts resulting from analysis job. The dashboard is partitioned into several sections; each section displays information about the possible alerts, infected files, the state of the infection, and where the suspect files are located.

The alerts are reported in real-time to the dashboard and can be used to find which files were possibly infected by a ransomware attack. With this information, you can then perform company-instituted policies to clean up the suspect files and clear the infection from your system. The possible suspect files are identified during the analyze phase in the post-processing of an indexing job run on a particular policy. In the analyze dashboard, you can clear the alert, which stops the reporting of the infection alerts.

Logging into the analyze dashboard

Procedure

To log into the analyze dashboard:

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

   > **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 IBM® Storage Defender Sentinel anomaly scan software.
2. In **Username**, enter your login, or the default administrator login of "admin". In **Password**, enter your password, or the default password of "admin". Select **Log In**.

Result

The analyze dashboard is displayed.

The dashboard

The analyze dashboard is made up of three main sections, as shown in the below table, and displays a summary of the state of a system as alerts occur and then breaks down the information into more detail as you scan down the page.

Below table contains the section and the information that they provide is described below:

Section	Display information on	Description
A	Alerts summary and table	Indicates new alerts and also lists all new and cleared alerts in table form. Any alerts that you clear are moved from the **New Alerts** tab to the **Cleared Alerts** tab.
B	Selected alert details	Displays detailed information on an alert that was selected in the **Alerts** table. You can also clear the alert to stop the software from reporting it.
C	Alerts graphic and files list	Displays an overall summary line of the details in the alert and graphical representations of what hosts were infected, the type of file extensions of the affected files, and the modification time of the files. The table in this section lists the suspect files, which can be grouped by column headings. 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.

A - Alerts summary and table

The alerts summary section and table listing the alerts is located at the top of the dashboard page.

The list of new alerts displays any recently occurring alerts and groups them into three severity levels:

- Critical - indicates a possible ransomware infection found during a policy job.
- Error - indicates that an anomaly scan software policy job was started but ended abruptly. For future use.
- Warning - indicates issues during a anomaly scan software policy job, but the job completely. For future use.

The table of alerts displays more detail about each alert and groups them by the status in two tabs of either **New Alerts**, which indicates they have not been dealt with yet, or **Cleared Alerts**, which indicates that the alert for the suspect files affected by the possible ransomware infection has been manually cleared and will no longer be reported.

B - Selected alert details

This second section of the dashboard displays the details of a selected alert in the top alert table.

The details include:

- the file location of the infection
- what type of encryption or infection method was used by the ransomware
- the policy name
- the MAC address of the anomaly scan software server.

You can scroll to another alert by selecting the arrow on the left or right of the text box. After verifying the alert per company protocol, select **Clear** to change the status of the alert from **Pending** to **Resolved OK** and the alert will appear under the **Cleared Alerts** tab in the upper section.

C - Alerts graphics and files list

The last section on the dashboard lists the statistics of the selected alert in various configurable ways.

This section can be displayed in three different ways. Select the desired icon to display:

Icon	Displays...
	Only the graphical representation of the suspect hosts, file extensions, and modification times of the suspect files.
	Only the list of suspect files.
	Both the graphs and the file list.

The top portion lists the number of suspect files, the number of suspect hosts, and the policy name that was run. These statistics change depending on which alert you selected in the top alert table.

The three graphs that are displayed show the distribution of:

- the suspect files per each host
- the suspect file extension per type
- the suspect file's modified time per date.

The list of suspect files is displayed at the bottom of the dashboard. The list can be grouped by the fields listed in the column headers. You can also choose which fields and columns to display by selecting the **Settings** icon.

Analysis and alerts

The analyze dashboard displays critical alerts that indicate a possible ransomware infection has corrupted files. A typical workflow to remediate the infected files are:

- view the details of the critical alert indicating the ransomware attack
- restore those suspect files from a clean backup copy
- clear the alert in the analyze dashboard.

Identifying the suspect files

New critical alerts may appear after a policy job runs, and, during the post-processing phase, analyzed by anomaly scan software. When a new alert is listed in the **New Alerts** table, it displays the number of infected hosts, the policy name used for the anomaly scan software analysis job, the status, the type of alert, and the severity.

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

To see more detail on the critical alert, select it in the **New Alerts** table. The details are displayed just below the table with the **Clear** button, which is used to stop the alert reporting once the files have been restored to a clean condition.

From the alert details, you learn the policy name, which is the identifier of the anomaly scan software analysis job, along with the type of encryption or infection method used by the ransomware, and the MAC address of the anomaly scan software server. The next step is remediation of the suspect files.

Remediate the suspect files

Once the suspect files are located, follow your company's policy to remediate the files, which could include instructions on:

- remove the corrupted files
- restore the files from a recent backup
- verify that the files are no longer infected.

Stop Reporting an infection on the IBM® Storage Defender Sentinel anomaly scan software

About this task

This procedure describes how to stop reporting if the infection on database server is cleaned up or removed and the IBM® Storage Defender Sentinel anomaly scan software continues to report an infection for each future scan.

Procedure

Once the files have been restored, the alert for that infection will continue to report previously cleared infection unless you manually stop the reporting. To stop reporting previously cleared infections do the steps that follow:

1. Open a web browser. In the browser's URL field, enter the IP address of the host where the anomaly scan software system is installed. The **Sign In** page opens.

   > **Note:** If you are unable to access this page, verify that ports 80 and 443 are open on the firewall.

2. In the **Username** field, type the administrator username. In the **Password** field, type the administrator password. Select the **Sign In** button.
3. Select the **Alerts** tab to access the message center.
4. The infection found are listed in the message table as logs with a **jobname number** (four-digit number), this is where the **Stop Reporting** is performed. Select **Stop Reporting** to stop reporting the infection that is reported.

   > **Remember:** For the Federation setup the procedure for stop reporting only needs to be performed on the member.

5. The alert will stop reporting the infection and move to the **Cleared Alerts** tab in the **Alerts** table.

Additional Administrative Functions

This section of the guide covers additional administrative tasks that you may need to perform. These administrative tasks include managing collections, how to use the IBM® Storage Defender Sentinel anomaly scan software for disaster recovery, and shutting down the engine.

Application backup and recovery

The backup and recovery procedures provide disaster recovery options so you can restore an engine back to its state at the time of the backup. The procedures let you back up, restore, and recover your anomaly scan software configuration files, indexes, databases, log files, and license files. This is largely achieved via commonly used third party commercial backup and restore software, with the final recovery phase accomplished through the IBM® Storage Defender Sentinel anomaly scan software graphical user interface.

Once you restore a backup image to /opt/ie/backup using a backup tool, open the freshly installed anomaly scan software and use the graphical user interface to recover the anomaly scan software system configuration, database, and index data.

Note: Requirements for a Successful Recovery:

- Stop or cancel any indexing, querying, extraction, or archive jobs before attempting a recovery. Otherwise, the recovery procedure will stop all anomaly scan software services and any running jobs, which may have a negative impact.
- The hardware must have the same MAC address as the Backup.
- The installed anomaly scan software version must be the same or newer than the Backup version.
- The restore from the backup server must have successfully completed, with the backed-up files now residing on the client system with the anomaly scan software.
- Anomaly scan software systems depend on the ability to resolve host names to IP addresses. The recommended and normal way to accomplish this is to use the Domain Name System (DNS). If, however, you are not using DNS, then the `/etc/hosts` file on each appliance must have the hostnames/IP addresses of the manager.

Using CLI tools for backup restore and recovery

This topic describes how to use command-line interface (CLI) tools to manually back up, restore, and recover IBM® Storage Defender Sentinel data. These procedures provide an alternative to using third-party backup applications.

Use CLI tools to perform the following tasks:

- Back up IBM® Storage Defender Sentinel data
- Restore IBM® Storage Defender Sentinel data
- Recover IBM® Storage Defender Sentinel data

Taking a backup of IBM® Storage Defender Sentinel data

Use the following procedure to manually create a local backup of IBM® Storage Defender Sentinel system configuration, database, and index data:

1. Log in to the IBM® Storage Defender Sentinel server as the root user
2. Run the following command to create a backup in the default directory `/opt/ie/backup`:

   ```
   /opt/ie/bin/ie_app_backup
   ```

   The backup is created in the `/opt/ie/backup` directory. A log of the backup process can be found at `/var/log/ie_backup`.

You can copy the resulting backup directory to external storage or backup media for recovery.

Restoring a backup of IBM® Storage Defender Sentinel data

Use the following procedure to restore IBM® Storage Defender Sentinel system configuration, database, and index data to a target IBM® Storage Defender Sentinel server:

1. Stop or cancel any indexing jobs that are currently running.
2. Log in to the target IBM® Storage Defender Sentinel server as the root user.
3. Copy the backup directory and its entire contents to the same path (`/opt/ie/backup`) on the target system.

> **Note:** The IBM® Storage Defender Sentinel version on the target server must match the version from which the backup was taken.

Recovering a backup of IBM® Storage Defender Sentinel data

> **Note:** If you are recovering the backup to a new server that has a different MAC address than the one from which the backup was taken, you need to create a support case with requesting the required override key needed to allow licensing to be valid. You need to include the MAC address from the original server and the new server in your request. The support team provides the override key.

Use the following procedure to complete the recovery process after a restore:

1. If you are recovering to a server with a different MAC address, set the override key by using the following command:

   ```
   setdbenv engine id_override <override_key>
   ```

2. Run the following command to restore from the default directory of `/opt/ie/backup`:

   ```
   /opt/ie/bin/restore_from_backup -s
   ```

After a successful recovery, IBM® Storage Defender Sentinel data is recovered from the backup and a recovery log file is created at: `/var/log/ie_backup/recovery.<timestamp>`. The files from the source backup are automatically removed after a successful recovery.

System shutdown/reboot

If maintenance is needed on your IBM® Storage Defender Sentinel anomaly scan software system, you will first need to perform a shutdown. The **Administration › System › Shutdown** page lets you initiate a **System Reboot** or a **System Halt**. In each case, access becomes unavailable to the browser-based administrative and search interfaces, although you will regain access after the system restarts if you chose a System Reboot.

> **Note:** All indexing is stopped while your anomaly scan software system reboots or halts. If an indexing job was running, it terminates and is marked incomplete. Whenever possible, it is best to reboot your engine when indexing will not be disrupted.

To shut down the engine:

1. Go to **Administration › System › Shutdown**.
2. Select a shutdown action from the **Action** list:

Option	Description
System Reboot	Reboots the system. Normal operation resumes when the reboot completes. Your anomaly scan software system does not normally need to be rebooted; instead, you may be asked to perform this action at the direction of IBM Storage Defender Sentinel Support personnel.
System Halt	Halts the system in preparation for power-off. If you need to perform hardware maintenance, use this option before turning off the power.

> **Note:** You may not see any feedback while the reboot progresses. If you resubmit a Reboot Now request, the system informs you that you do not have access to the requested page and directs you to Sign In again-you will be able to sign in once the reboot completes. Otherwise, if you click elsewhere on the page while a reboot is in progress, an "Unable to Connect" error appears. In this case as well, you will be able to sign in once the reboot completes.

3. Next, from the **When** drop-down list, select when you want the action to be performed:

Option	Description
Now	Perform the selected action immediately, without delay. You should use this option only if you are certain that no one is accessing the engine at the console or via an SSH session.
In 1 minute	Perform the selected action with a one-minute delay. This option allows any console or SSH user sessions a chance to react to the shutdown request, possibly by cancelling it at the command line. This is the recommended delay. If the shutdown request is canceled by a console or SSH user, you will receive a shutdown cancelled message on the Administration page from which you submitted the request. In the absence of such a cancellation message, you can assume that shutdown is proceeding according to the selection options.
In 5 minutes	Similar to the 1-minute delay, but provides a little more time for users to react.

4. Select **Submit**.

IBM® Storage Defender Sentinel anomaly scan software site map

The information in this chapter provides details about the IBM® Storage Defender Sentinel anomaly scan software GUI, which includes details about the various pages, menus, sub-menus, and the functionality of these pages.

About

The About link displays the version and build numbers of your IBM® Storage Defender Sentinel anomaly scan software, as well as copyright information and trademark acknowledgments.

Help

The **Help** menu links to the following:

- The IBM® Storage Defender Sentinel anomaly scan software Installation and User Guide, i.e., the main User Guide, the Archive Guide, Search Guide, Catalog Ingestion Guide, and Query Operators Guide.
- The IBM Storage Defender Sentinel Support.

Sign Out

Sign Out logs you out of the IBM® Storage Defender Sentinel anomaly scan software.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM® representative for information on the products and services currently available in your area. Any reference to an IBM® product, program, or service is not intended to state or imply that only that IBM® product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM® intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM® product, program, or service.

IBM® may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM® Intellectual Property Department in your country or send inquiries, in writing, to:
Intellectual Property Licensing
Legal and Intellectual Property Law
IBM® Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM® may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM® websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM® product and use of those websites is at your own risk.

IBM® may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM® under terms of the IBM® Customer Agreement, IBM® International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM® products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM® has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM® products. Questions on the capabilities of non-IBM® products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM®, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM®, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM® shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM® Corp. Sample Programs. © Copyright IBM® Corp. _enter the year or years_.

Trademarks

IBM®, the IBM® logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM® or other companies. A current list of IBM® trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe™ is a registered trademark of Adobe™ Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open™, LTO™, and Ultrium™ are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

Intel™ and Itanium™ are trademarks or registered trademarks of Intel™ Corporation or its subsidiaries in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from the Linux® Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft™, Windows™, and Windows NT™ are trademarks of Microsoft™ Corporation in the United States, other countries, or both.

Java™ and all Java™-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat®, Inc. or its subsidiaries in the United States and other countries.

UNIX® is a registered trademark of The Open Group in the United States and other countries.

VMware, VMware vCenter Server™, and VMware vSphere™ are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM® website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM®.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM®.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.
IBM® reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM®, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM® MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM® Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM®’s Privacy Policy at http://www.ibm.com/privacy and IBM®’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM® Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

A glossary is available with terms and definitions for the IBM® Storage Defender Sentinel family of products.

See the IBM® Storage Defender Sentinel glossary.

Index