User Guide

HP Sure Sense

First Edition: June 2019

Document Part Number: L63508-001

Table of contents

1 Getting started

HP Sure Sense uses deep learning models to detect malicious files and prevent malware, zero-day, ransomware, and Advanced Persistent Threat (APT) attacks from harming your computer.

HP Sure Sense uses the following components:

- **Prediction Model:** A lightweight deep learning prediction model. It autonomously detects cyber threats and enables zero-day and APT protection.
- **File reputation Cloud Services:** A cloud-based database of information on known files that adds a second layer of classification. When this option is enabled, the hash for PE (Portable Executable) files is sent to the file reputation services in the cloud.
- **Content Delivery Network:** A system that distributes the latest prediction model and software updates for HP Sure Sense.

Main menu tabs

The main menu includes the following tabs:

- **Status**: Displays the protection status, threat summary, and other information.
- **Alert log**: Displays a table that lists security events and logs. It includes information about security, updates, and management. From this page, you can view additional details about security alerts and take further actions.
- **Quarantine**: Displays a table that lists all quarantined files. Each entry is based on a unique hash value. Entries include information related to the files and the original location of the file. You can restore quarantined files from the **Action** column.
- **Settings**: Allows you to configure whether notifications are displayed, set console languages, and manage other preferences. To view or change **Advanced Settings**: Select **Edit**, and enter the administrator credentials.

Full scan

Full scan analyzes all existing files on local drives of the computer. Any file identified as malicious is blocked and quarantined.

Enhanced threat protection

When Enhanced Threat Protection is enabled, it monitors the behavior of all running processes for malware. If a process is identified as ransomware, the process is terminated.

2 Security processes

Malware prevention

All files added to the local drives of the computer are automatically scanned and analyzed. When a file is identified as malicious, the following actions occur:

- The file is blocked and quarantined. The quarantine process copies the file to the quarantine folder, deletes the file from its original location, and adds the file to the quarantine table.
- An event is added to the **Alert Log** page. A notification is displayed to indicate that the threat is prevented. If you click the notification, the **Quarantine** page opens with the relevant entry highlighted.

NOTE: Malicious files on external storage devices are blocked and prevented from running, but are not quarantined.

Restoring and deleting quarantined files

Files moved to the quarantined folder can be restored or deleted as needed. Restored files are moved to their original locations and allowed to run. Deleting a quarantined file removes the entry from the quarantine table and deletes the file from the quarantine folder. It does not change the classification of the file, and any new instances of the file are blocked and quarantined.

To delete or restore quarantined files:

1. Open the **Quarantine** page.
2. Select the file you want to delete. Select the **Action** icon.
3. Select from the options to **Restore File**, **Delete File**, or view **File Details**.

IMPORTANT: Before you restore a quarantined file, verify that the file is not malware.

To delete all files at once:

▲ On the **Quarantine** page, select the trash can icon located to the right of the search box.

Adding and removing trusted files

Trusted files are files that were blocked and then restored and allowed to run by the user. You can add trusted files to the trusted files list from the **Quarantine** page or the **Alert Log** page. You can add processes to the trusted files list only from the **Alert Log** page.

Files added to the trusted files list are restored to their original folders and deleted from the quarantine folder. Processes added to the trusted files list are allowed to run and are no longer monitored for ransomware behavior. Files and processes added to the trusted files list are not scanned.

To add a trusted file or process:

1. Open the **Alert Log** page.
2. Select the Actions icon in the entry of the file or process that you want to add.
3. To add a file, select **Restore File**.

   To add a process, select **Add to Trusted Files**.

IMPORTANT: Before you add a file or process to the trusted files list, verify that it is not malware.

To remove a trusted file or process from the trusted files list:

1. From the **Settings** page, select **Edit Trusted Files**.
2. Select the file or process that you want to remove, and then select the **Actions** icon.
3. To remove a file, select **Quarantine File**.

   To remove a process, select **Remove From List**.

Exclusions

Folders and processes can be excluded from being scanned by using the **Exclusions** option.

IMPORTANT: Before you add a folder to the exclusion list, HP recommends the following:

- Add only read-only folders to minimize the opportunity for trusted folders to be abused by attackers.
- Do not add temporary folders. Malware tends to write modules to temporary folders. This advice is also relevant for system folders such as `Windows` or `system32`.
- If a specific solution continues to return false positives, look to the vendor of the solution for recommendations.

To access the exclusions list:

1. Open the **Settings** page, and scroll down to **Advanced Settings**.
2. Select **Edit Exclusions**.

A Uninstalling HP Sure Sense

If HP Sure Sense is currently installed and a new installation is required, you must first remove the current version. The method to uninstall is based on how HP Sure Sense was installed.

If HP Sure Sense was manually installed using the installation wizard:

- Run the installer, and select **Uninstall**.

If HP Sure Sense was preinstalled on your device:

1. In **Windows Settings**, go to **Apps & features**.
2. Uninstall the HP Sure Sense Installer.