
EduSweep Documentation

Release 2.6.0

Paul Beesley

Jun 16, 2019

Contents:

1	Installation	1
2	Application Guides	11
3	Concepts	27
4	File Inspector Utility	29
5	Signature Studio Utility	33
6	Performance Tuning	35
7	System Requirements	37
8	Glossary	39
9	Support	41
10	Changelog	43
11	Welcome	49
12	Donate Coffee	51

1.1 Standard Installation

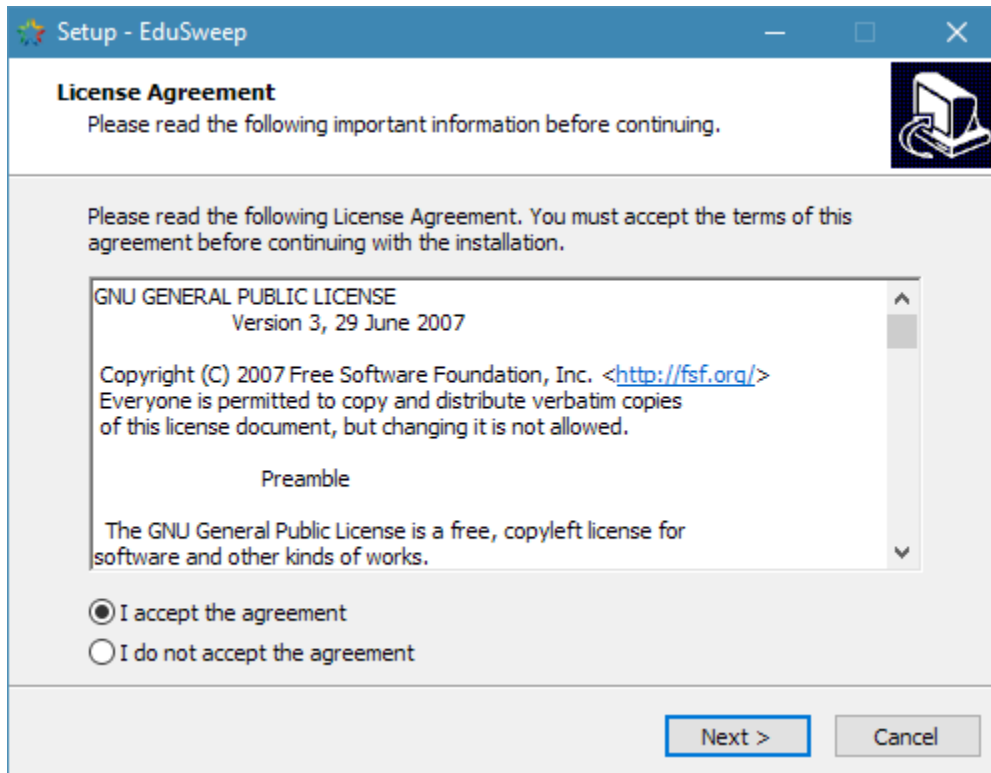
The EduSweep installer is provided as an executable (exe) setup program. The default name for the program is “EduSweep Installer.exe”.

Please review the requirements and prerequisites before beginning the installation process.

Double click on the downloaded installer file to begin the setup process. If User Account Control (UAC) is enabled then you will be prompted to provide elevated permissions to install the software. If you choose No then the installation will be cancelled and EduSweep will not be installed. Choose Yes to proceed with the installation.

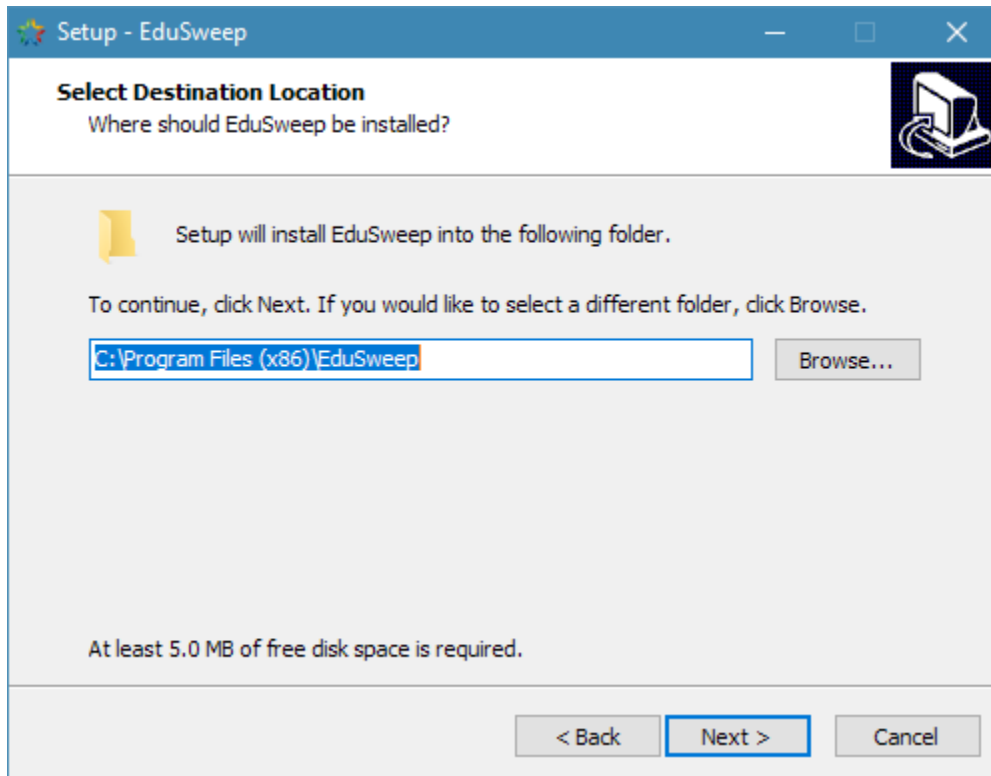
The setup wizard below will launch if the necessary prerequisites are installed on your system.

1.1.1 License Acceptance



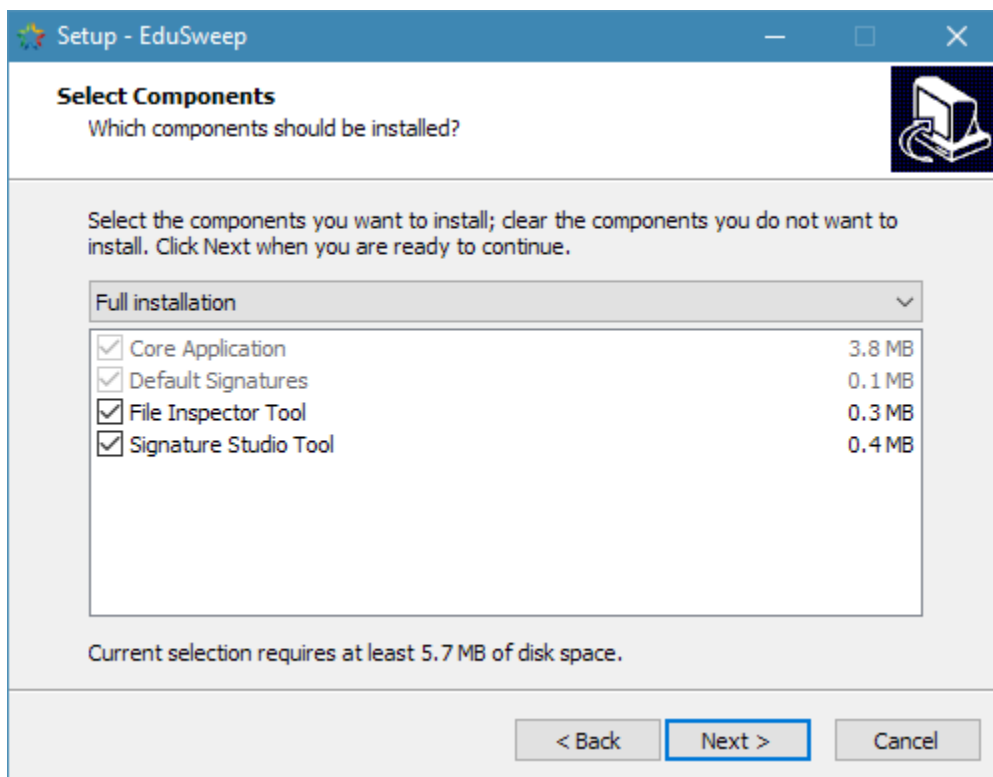
The first page of the installer prompts you to accept the terms of the license that EduSweep is provided under. Review these terms carefully and press Next > to indicate acceptance if you agree.

1.1.2 Directory Selection

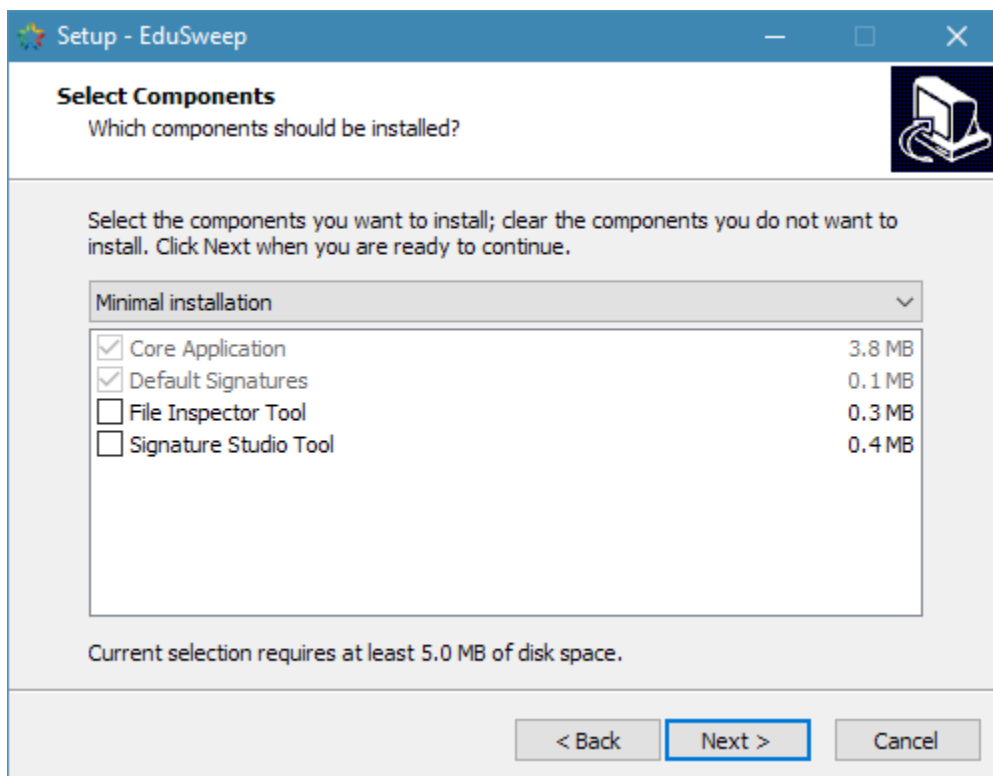


On the second page you can modify the directory into which EduSweep will be installed. EduSweep does not require write access to this folder after the installation is completed. Modify the directory path, or accept the proposed default, and choose Next > to proceed.

1.1.3 Component Selection

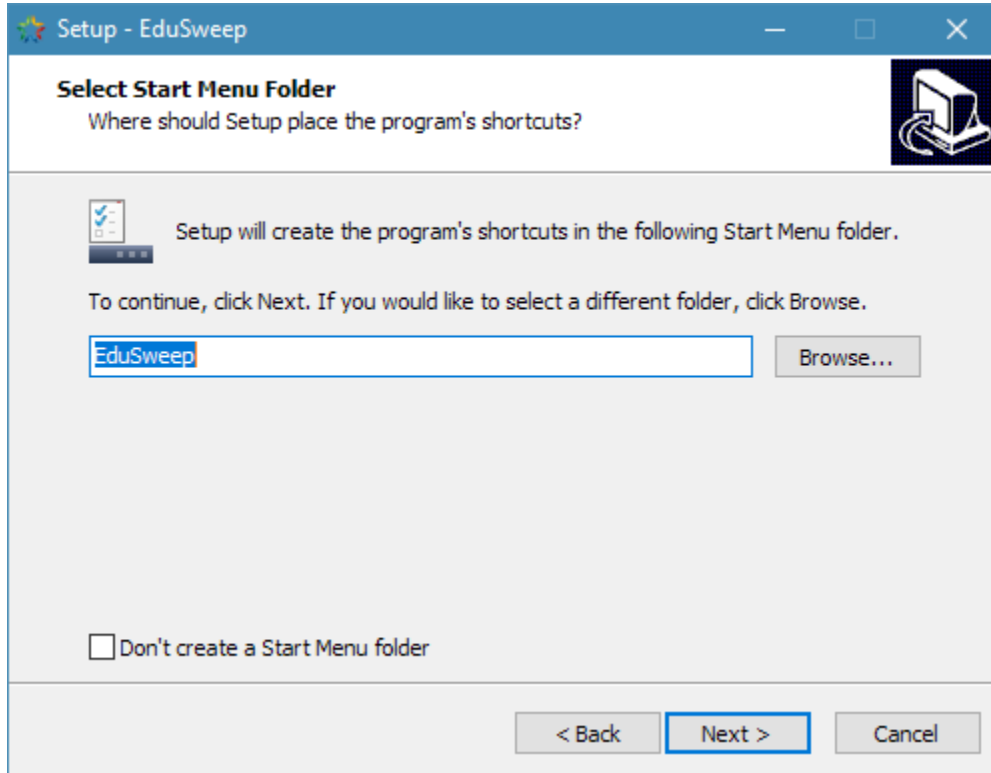


Select from a full installation (which includes the File Inspector and Signature Studio utilities), a minimal installation (which omits both utilities) or a custom installation that allows you to choose components manually.



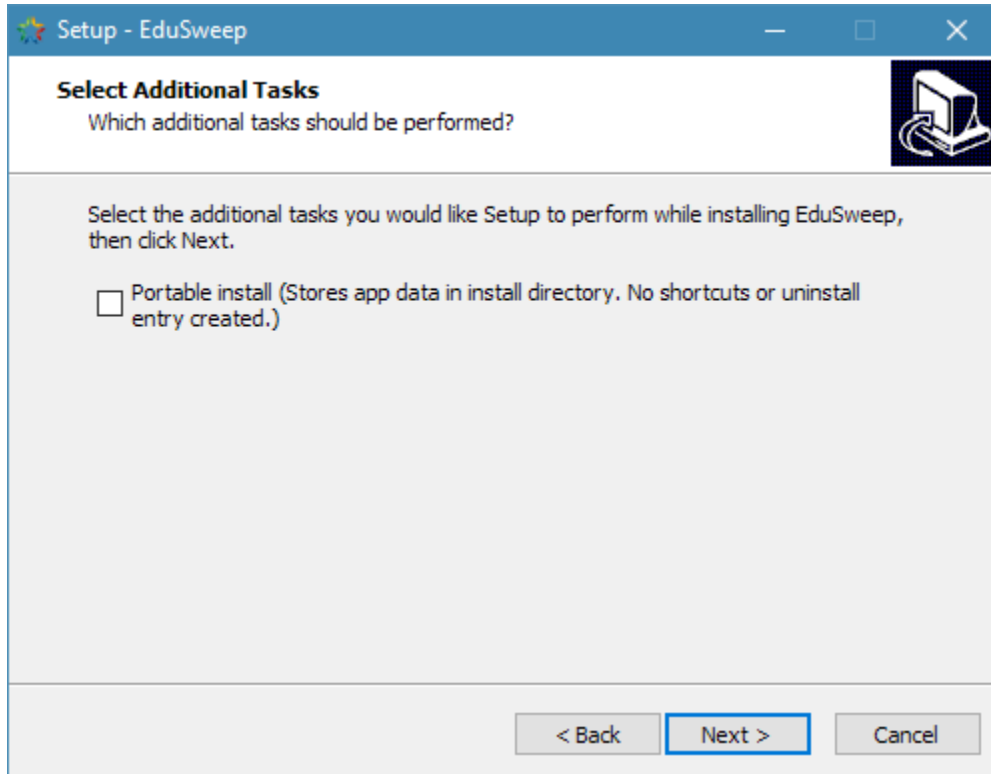
The core EduSweep application and its collection of default signatures are always required and cannot be deselected. Even in a minimal installation these are selected as shown above.

1.1.4 Start Menu Shortcuts



By default the installer will create Start Menu shortcuts for the EduSweep application and any utilities that were selected in the previous step. You may clear the checkbox in order to prevent the creation of these shortcuts.

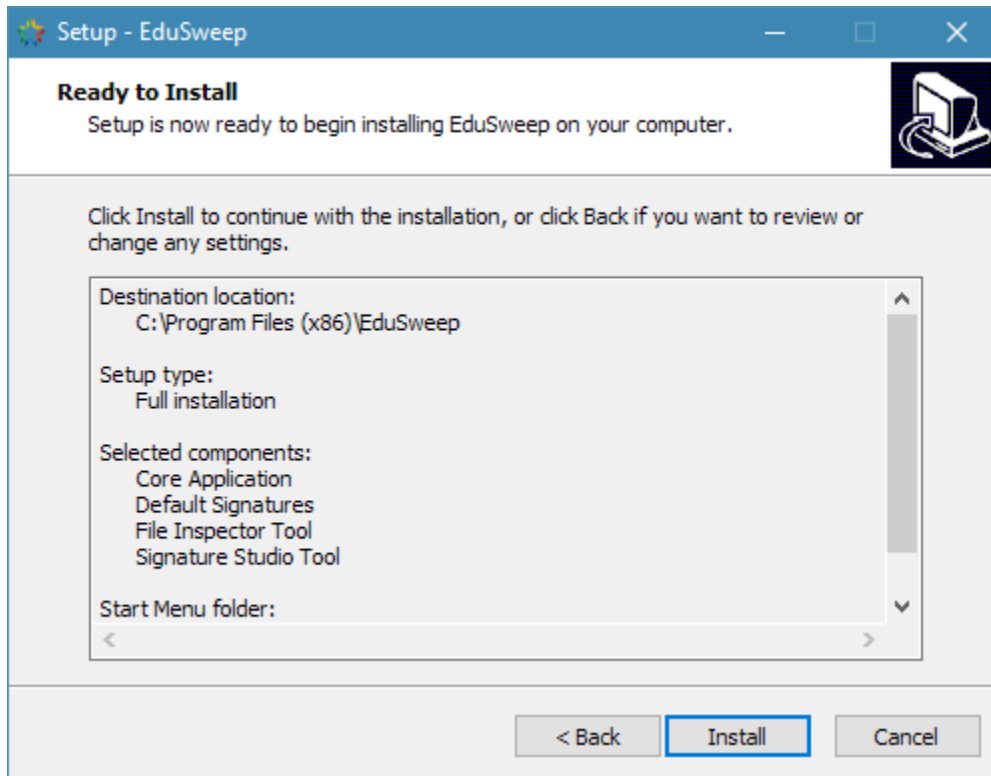
1.1.5 Portable Installation



The installer offers to install in portable mode. This option is not enabled by default. Portable mode will install to the specified folder but without registering the application with Windows. Application data will be stored within the install folder instead of in the users' roaming profile.

Note that the portable mode option also overrides the Start Menu option from the previous page. If portable mode is enabled then no shortcuts will be created in the Start Menu.

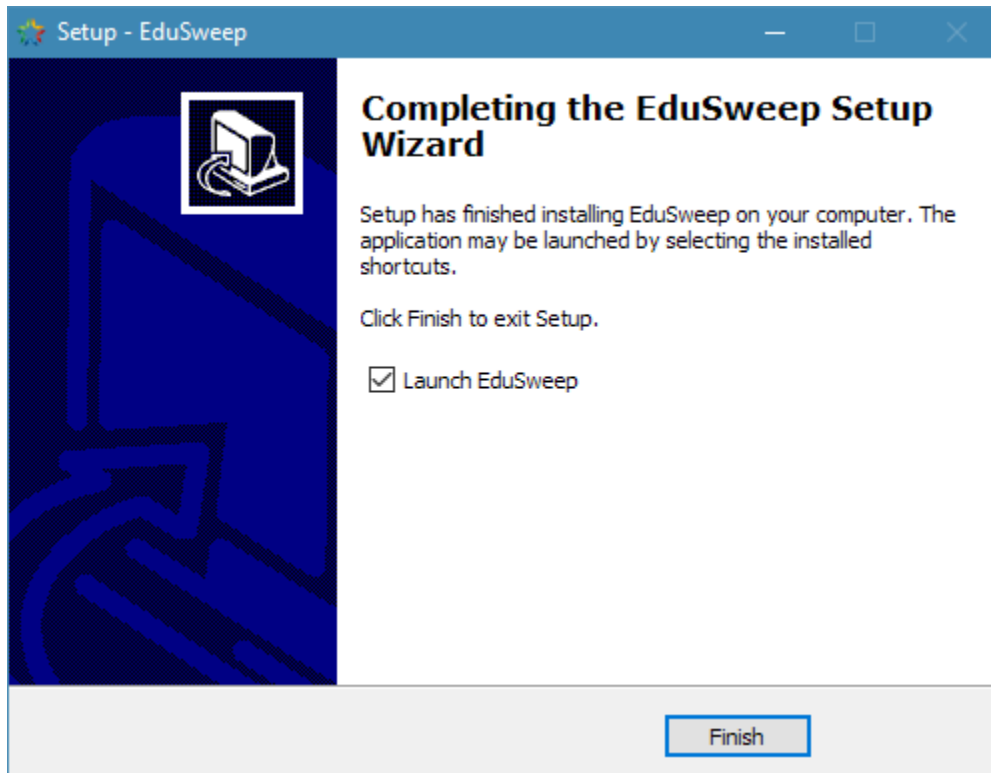
1.1.6 Review Installation Options



This page offers a chance to review the installation options and to cancel the installation if needed. Choose Install to continue and to install the application and any selected components.

At this stage the files required for EduSweep to run will be copied to the destination folder that was selected earlier in the installation process.

1.1.7 Completion



Once the file copy process completes the installation is finished and EduSweep can be started from its Start Menu shortcut. The installer offers to start EduSweep immediately as well.

1.2 Uninstallation

1.2.1 Standard Uninstallation

EduSweep can be removed from the Apps and Features page of the Settings application (Windows 10) or from the Programs and Features control panel entry (Windows 7 or 8).

Alternatively, it is possible to start the uninstallation process directly by executing the `unins000.exe` file in the root of the EduSweep install directory.

1.2.2 Removal of User Data

EduSweep stores user data into a working folder during its use. By default this is the `%appdata%\EduSweep` directory, part of the user's roaming Windows profile.

This data includes scan tasks, reports, quarantined files, etc. These files will not be removed when EduSweep is uninstalled (except when the installation was portable, see below). It is safe to remove this data manually after the uninstallation is complete, if desired.

1.2.3 Portable Uninstallation

To remove a portable installation simply delete the portable application folder in which the EduSweep application files are installed. For example, if the install path is D:\Apps\EduSweep then deleting the EduSweep directory is sufficient to completely remove all program files and user data.

Because user data in a portable installation is stored under the same directory as the program files this data will be completely removed as well.

1.3 Converting to a Portable Install

A standard installation can be quickly converted to a portable installation.

Make sure that the installation directory is writable, then create an empty file named *PORTABLE* in the root of the directory (next to the EduSweep executable). The next time that EduSweep starts up it will treat the installation directory as its working directory and will create some new folders there to store its state.

Note that a converted installation will effectively be reset to default settings. You will need to copy over any configuration files from the previous working directory (most likely *%appdata%\EduSweep*) if you want to recreate the state.

1.4 Upgrading from Older Versions

1.4.1 Remove Older EduSweep Installations

Older versions of EduSweep will try to place data in your roaming profile and this may conflict with newer data formats used by EduSweep 2.6 and later. It is recommended to remove any older versions of EduSweep to avoid such conflicts.

1.4.2 Remove Existing EduSweep Data

If you encounter issues when using EduSweep 2.6 or later on a machine that has been used with an older version, or if your roaming profile contains old EduSweep data, then the first step is to remove the EduSweep folder from your profile.

The default location for the EduSweep data folder is:

%appdata%\EduSweep

Remove the folder entirely, or all of its contents. Note that if you are using a different location for storing EduSweep data (such as in a portable installation) then the above path must be modified accordingly.

1.4.3 Scan Task Migration

Scan tasks created in older versions of EduSweep will not be imported into the new version because the task format has changed. A conversion tool for updating tasks to the new format may be released at a later date depending on demand.

1.4.4 Custom Signature Migration

Custom signatures created in older versions of EduSweep will not be imported into the new version because the file format has changed. A conversion tool for updating signatures to the new format may be released at a later date depending on demand.

1.5 Repackaging

Some network management systems, such as RM Community Connect, require installers to be repackaged before an application can be deployed through their management interfaces. This creates a new installer (usually in MSI format) that gets deployed to workstations instead of the application's original installer.

EduSweep has been designed to accommodate repackaging as far as possible:

- The installer does not create any registry entries beyond those necessary to register the application and its uninstaller entry in Windows' list of applications.
- The application does not require write access to its install directory
- No files are placed into the Windows directory (or other system directories)
- The application does not require elevated / administrator permissions to run
- Application data is stored in the user's roaming profile by default

Instructions for performing the repackaging process are beyond the scope of this guide. Refer to your management system's documentation for help with this process.

1.5.1 Testing the Deployed Package

Once the repackaging process is complete you can test the correct operation of EduSweep after deployment by:

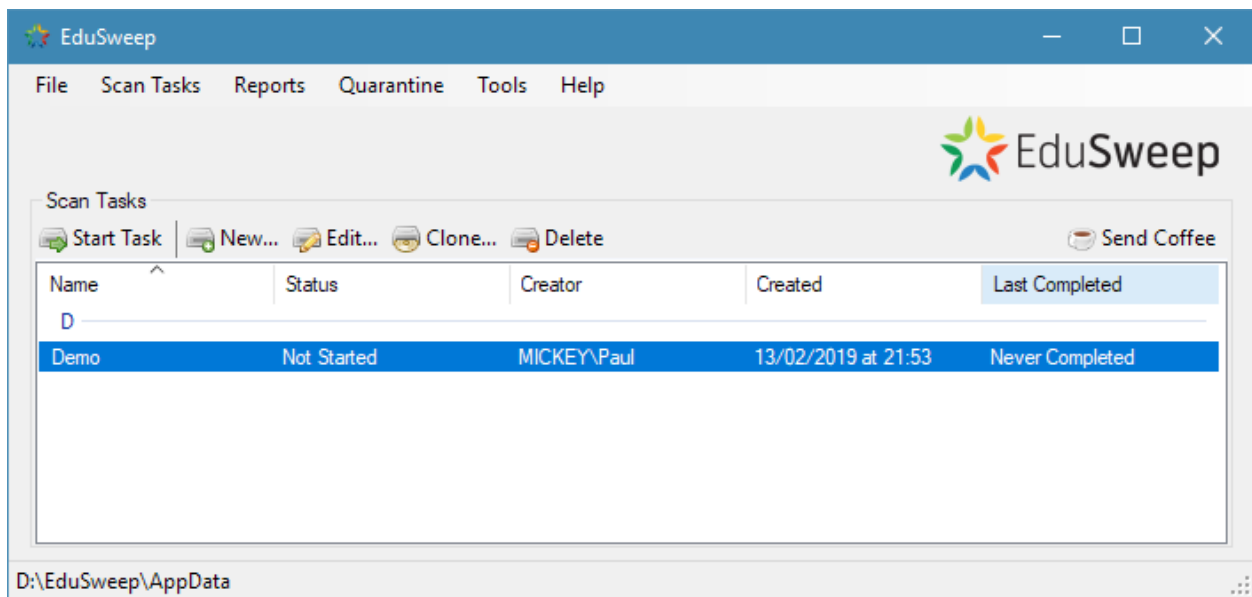
- Starting the application from the EduSweep entry in the Start Menu (and verifying that the entry is present)
- Creating and then deleting a new scan task
- Adding a file to quarantine (and, optionally, restoring it to its original location)
- Modifying the application settings
- Reviewing the application log file for warnings and errors

If you encounter difficulties repackaging EduSweep and you feel that the EduSweep installer is the cause then please raise an issue. See the [Support](#) page for links to do this.

The **Application Windows** provide descriptions of each of the windows that you will encounter while using EduSweep, as well as notes on their role within the overall workflow.

2.1 Main Window

Once EduSweep has been started, you will be presented with its main window as shown below. This window is used for managing and starting existing Scan Tasks, and for accessing other parts of the application such as reports or the Settings window.



2.1.1 Scan Tasks

The scan tasks list displays all existing scan tasks. When EduSweep is first installed this list will be empty as no tasks have been created yet. The *New* button on the toolbar is used to create a new task that will then be available from the list.

When a task is selected from the list the *Start Task*, *Edit* and *Delete* buttons on the toolbar will be enabled, as long as the task is not currently running.

Note: A new task can be created at any time, but a task cannot be started, edited or deleted while it is running.

The buttons on the toolbar provide the following functionality:

- Start Task: Opens the *Task Progress* window to run the selected scan task.
- New: Opens the *New Task* window to create a new scan task.
- Edit: Opens the *Edit Task* window to modify the selected scan task.
- Clone: Creates a copy of the selected task. The cloned task will be created with a name in the format: *<Old-TaskName> (Copy)*. Once cloned, the two tasks are not linked in any way.
- Delete: Removes and permanently deletes the selected scan task.

2.1.2 Menu Bar

The main menu bar at the top of the window is used to access other EduSweep features.

- File: Just the standard Exit menu item for closing EduSweep.
- Scan Tasks: Provides the same functionality as the Scan Tasks toolbar buttons.
- Reports: Access the Report Manager to view and edit reports.
- Quarantine: Access the Quarantine Manager to view, analyse, remove and restore quarantined files.
- Tools: Launch the File Inspector and Signature Studio utilities and access application settings.
- Help: Get information about EduSweep and the project.

Note: If utilities were not selected during the EduSweep installation then their menu items will be disabled. Reinstall EduSweep to make these available.

2.1.3 Status Bar

The status bar at the bottom of the window displays the working directory - the location that EduSweep is using for storing its scan tasks, reports, quarantine files, settings, logs and custom signatures. By default this will be within the roaming profile of the current user. In a portable installation this will be the directory containing the main EduSweep executable.

2.2 Scan Task Editor

Before scanning a directory with EduSweep a *Scan Task* must be created. The *Task Editor* is used for creating tasks that can be reused multiple times. Refer to the [Scan Tasks](#) document for more information about scan tasks and how

they are used in EduSweep.

Creating a scan task can be broken down into three steps:

1. Selecting a name for the task and checking the general settings
2. Adding one or more directories to scan
3. Adding one or more *elements* that will be used for detecting files

Once the task has been created it will be available from the task list on the Main Window.

2.2.1 General Settings

The screenshot shows the 'Task Editor: Demo' window. It has a title bar with standard window controls. Below the title bar is a header area with a clipboard icon and the text 'Task Editor: Demo'. A descriptive paragraph follows: 'Scan tasks are reusable profiles containing a list of target directories that will be scanned, along with a list of signatures that control which files are detected. Tasks are shown in the main window when ready.' Below this is a tabbed interface with three tabs: 'General Settings' (selected), 'Target Directories', and 'Signatures and Elements'. The 'General Settings' tab contains three sections: 'Name' with a text input field containing 'Demo'; 'Parallel Scanning' with a dropdown menu set to 'Full (Recommended)'; and 'Antivirus Integration' with a checked checkbox labeled 'Enable ClamAV antivirus scanning of detected items'. At the bottom are four buttons: '< Back', 'Next >', 'Save', and 'Cancel'.

This first tab is used for setting the name of the task, adjusting the parallel scanning modes and choosing whether to enable antivirus integration or not.

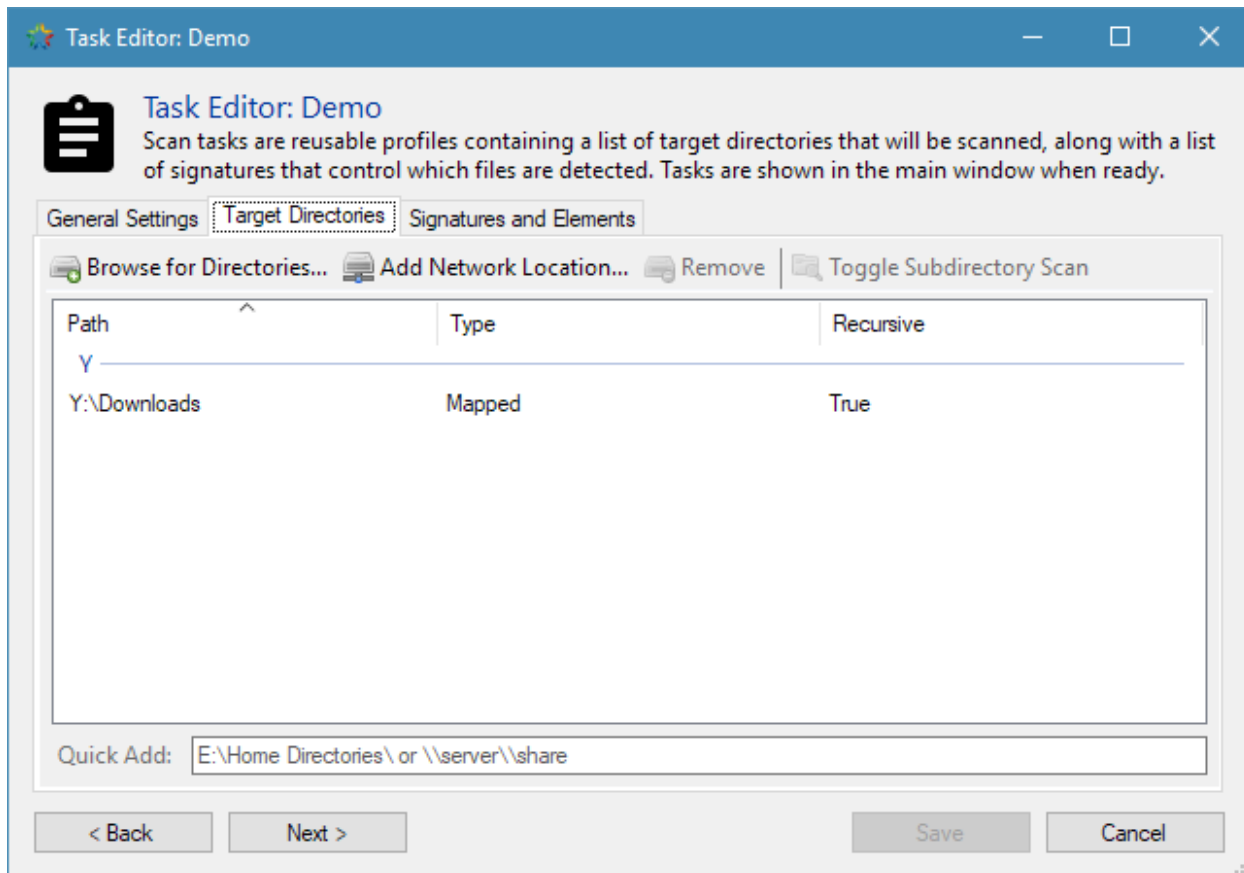
The task's name is used to help identify it. Choose a descriptive name such as "Year 10 Home Folders" so that its purpose is clear and explains loosely which files will be scanned. This name is also used in the title of the report that is created after running the task.

The *Parallel Scanning* setting governs the number of threads that EduSweep can use while scanning directories. Depending on the structure of the directory tree being scanned and the type of storage, this feature can provide a significant speed increase. Refer to the [Performance Tuning](#) document for more details on the performance considerations of this feature.

Antivirus Integration controls the state of virus scanning at the scan task level. There is also a global setting for this which works in combination with the task-level setting. This feature will only function properly if EduSweep has

been configured to communicate with a ClamAV server (clamd) instance. Refer to the [ClamAV \(Antivirus\) Integration](#) document for details.

2.2.2 Target Directories

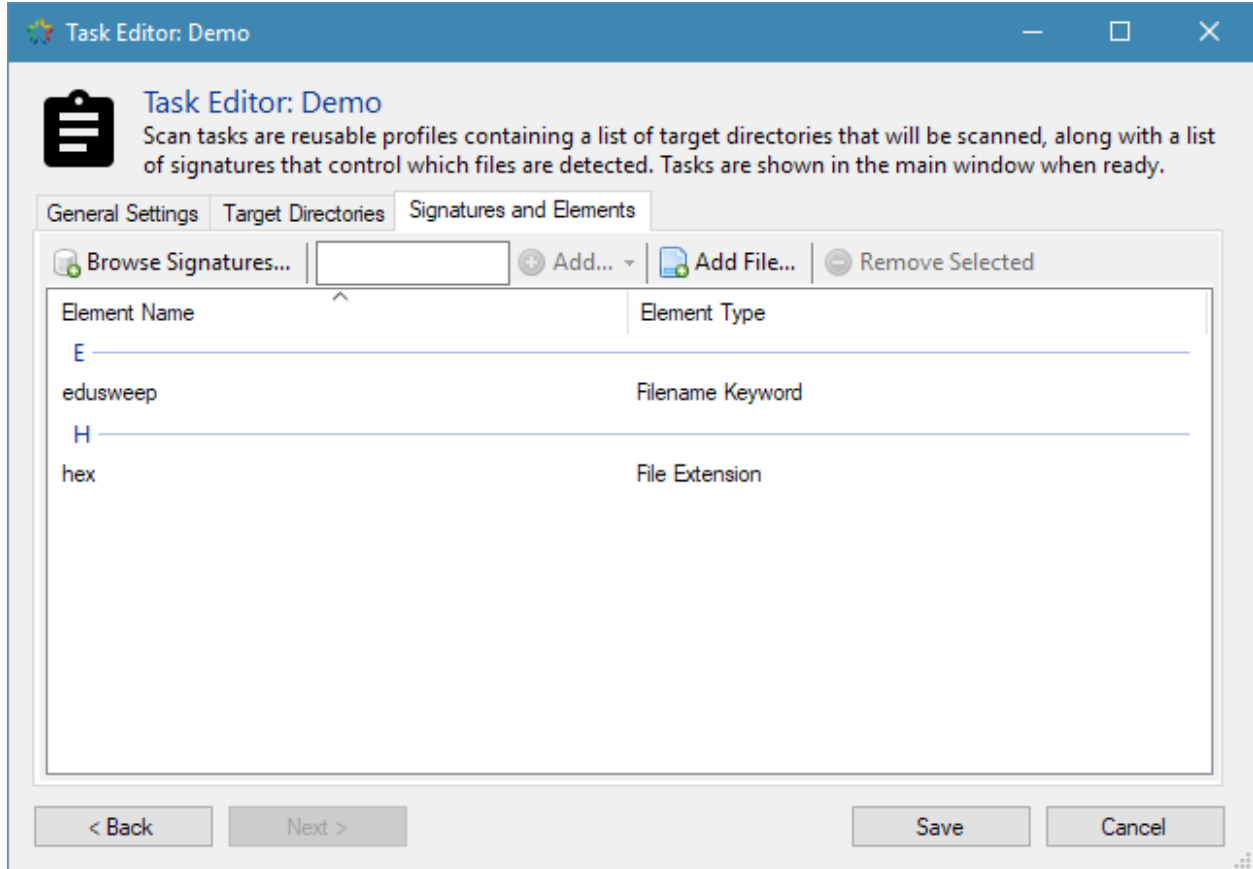


This tab shows the list of directories that will be scanned when the scan task is run.

To add a directory to the list, choose “Add Location” from the toolbar immediately above the locations list and a folder browser dialog will be presented so that you can select the folder to be scanned. Once you have navigated to the desired folder, press “OK” on the dialog (“Select Folder” on Windows Vista and above) and it will be added to the list.

By default, any directory added to the list will be scanned recursively; all sub-directories of the directory will be scanned, and their sub-directories, and so on. Use the *Toggle Subdirectory Scan* button to enable or disable this behaviour.

2.2.3 Signatures and Elements

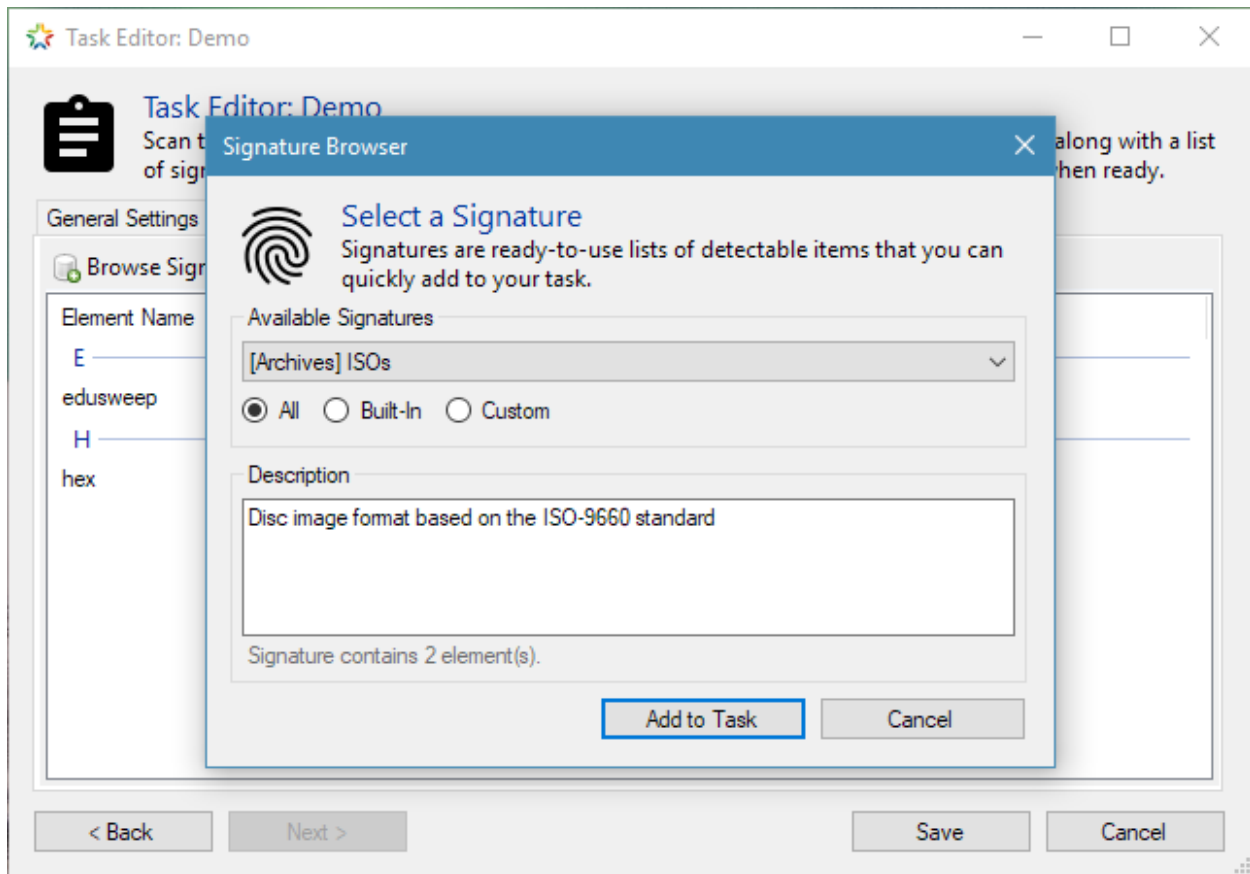


This tab controls what will be detected during the scan, using [Signatures](#) and [Signature Elements](#).

The three types of elements (file extensions, filename keywords and specific files) can be added to the scan task directly using the toolbar buttons. You can also add groups of elements from signatures using the *Browse Signatures...* button.

As an example, to detect .exe files and files containing the word “vpn” in their name we can add one extension-type element with the value “exe” and one keyword-type element with the value “vpn”.

Alternatively, we could add the *Windows Executables* signatures instead of the extension-type element to scan for a wider range of executable files all at once.



2.3 Scan Task Progress

The Task Progress window displays both the state of a running scan task and the results of the scan task when it has completed. When a scan task is started from the main window, this scan window will appear and the scan task will begin to run immediately.

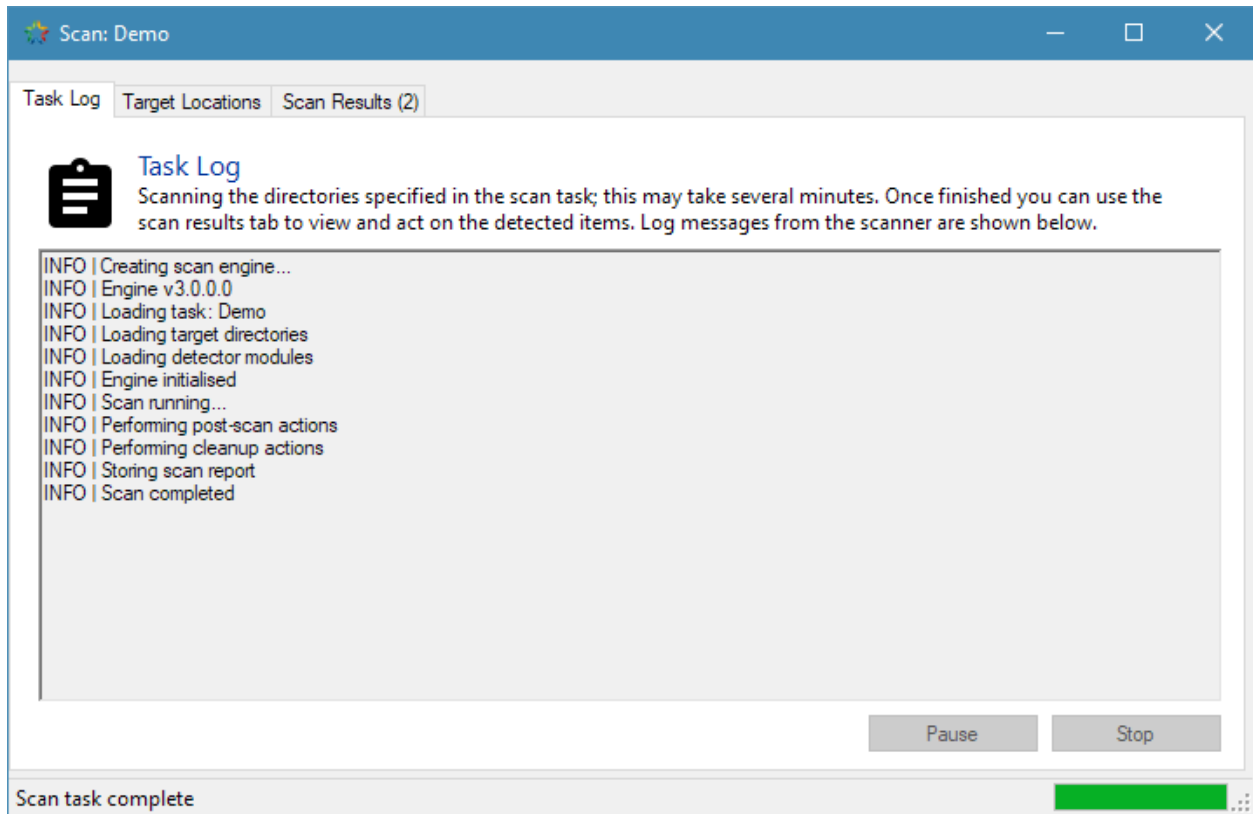
The status bar at the bottom of the window displays the overall status of the scan and, when the scan is running, the path of the most recently scanned directory. You can use this to check that the scan is proceeding properly and is not stalled.

You can pause or cancel the scan at any point before the target directories have all been scanned and the results are being collated for display.

The window is made up of three tabs - Task Log, Target Locations and Scan Results, with Task Log being the default.

2.3.1 Task Log Tab

This tab provides logging information about the scan process. Warnings are highlighted in an orange font, while critical errors are shown in a bold, red font.

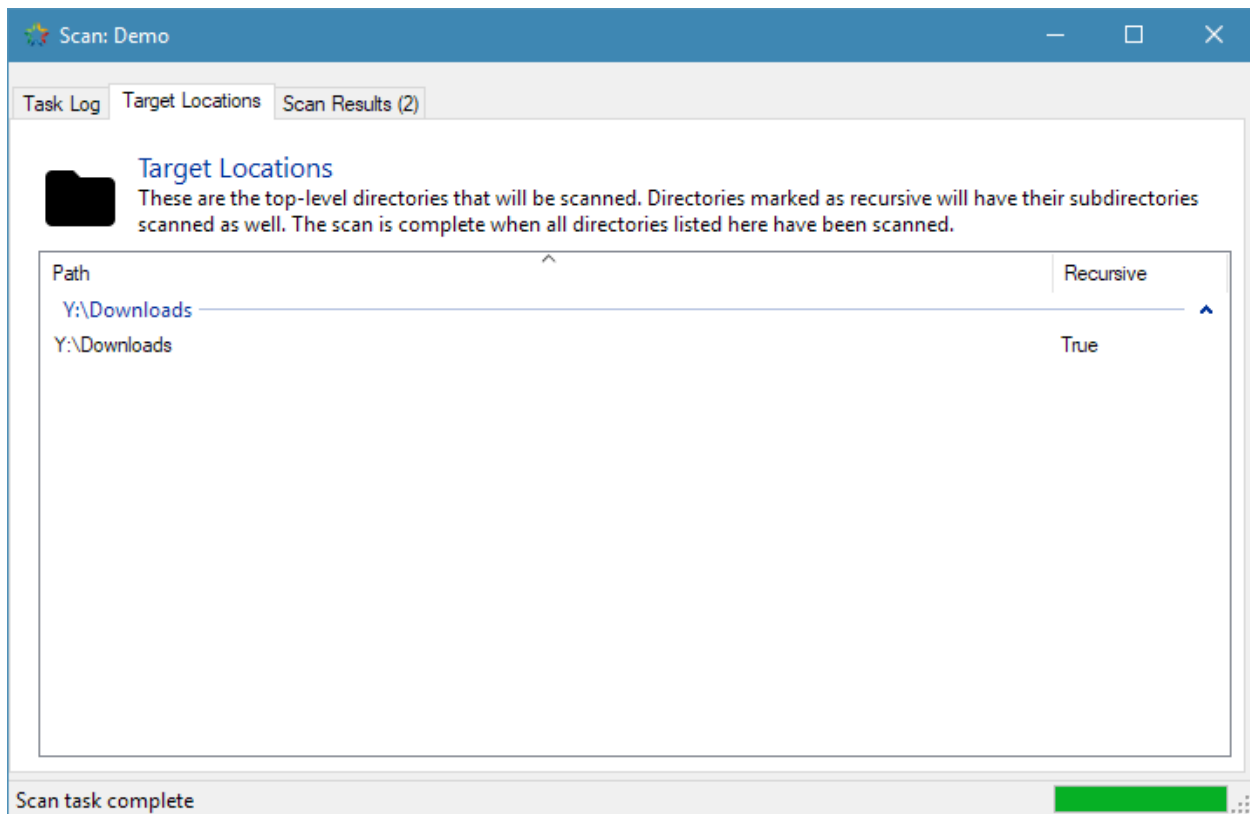


The log entries shown here are filtered according to the logging level that is configured from the `Logging` tab of the `Settings` window. When a more detailed logging level is selected the log file may contain more entries than the log displayed here, to prevent the sheer volume of log output potentially slowing down the user interface.

The log scrolls automatically during the scan as events occur.

2.3.2 Target Locations Tab

The locations tab displays a list of the top-level directories chosen for scanning. This list of directories comes from the scan task.

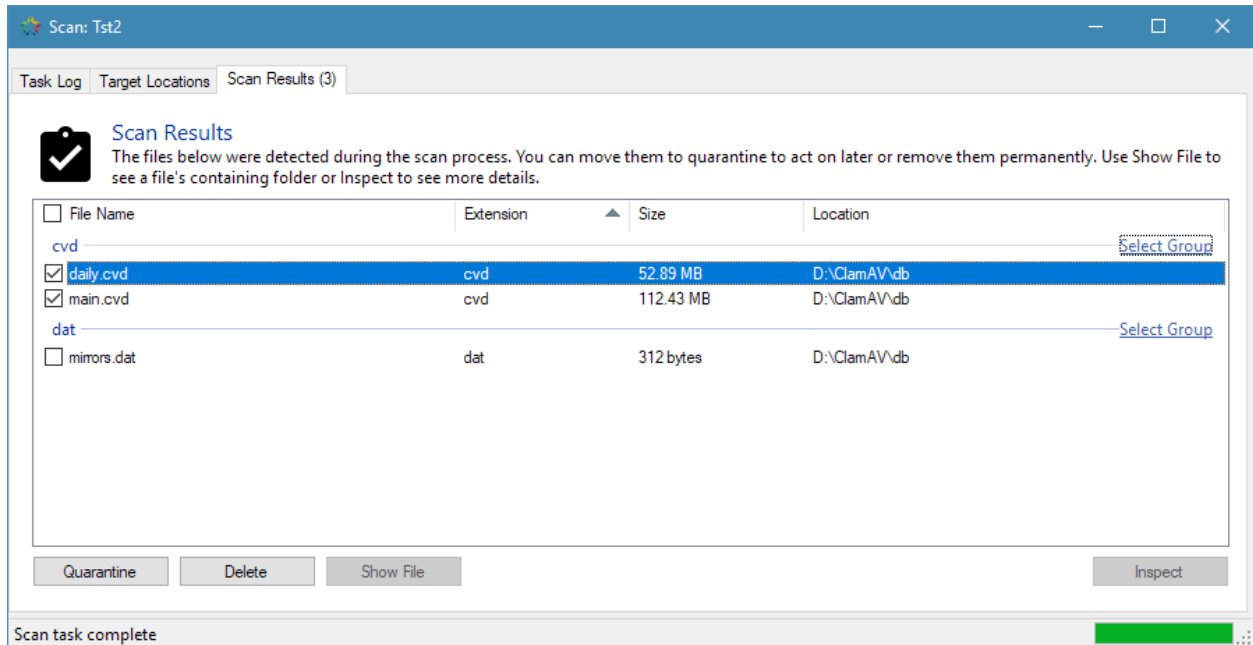


Each top-level directory also shows whether it will be scanned recursively or not.

The locations are shown as a reminder of what was specified in the scan task; there are no actions that can be taken from this tab.

2.3.3 Scan Results Tab

Files shown in this list have been marked as detected by one or more detectors during the scan process. A file may be detected by more than one detector (for example, the extension and filename keyword detectors) but it will be shown only once in the list.



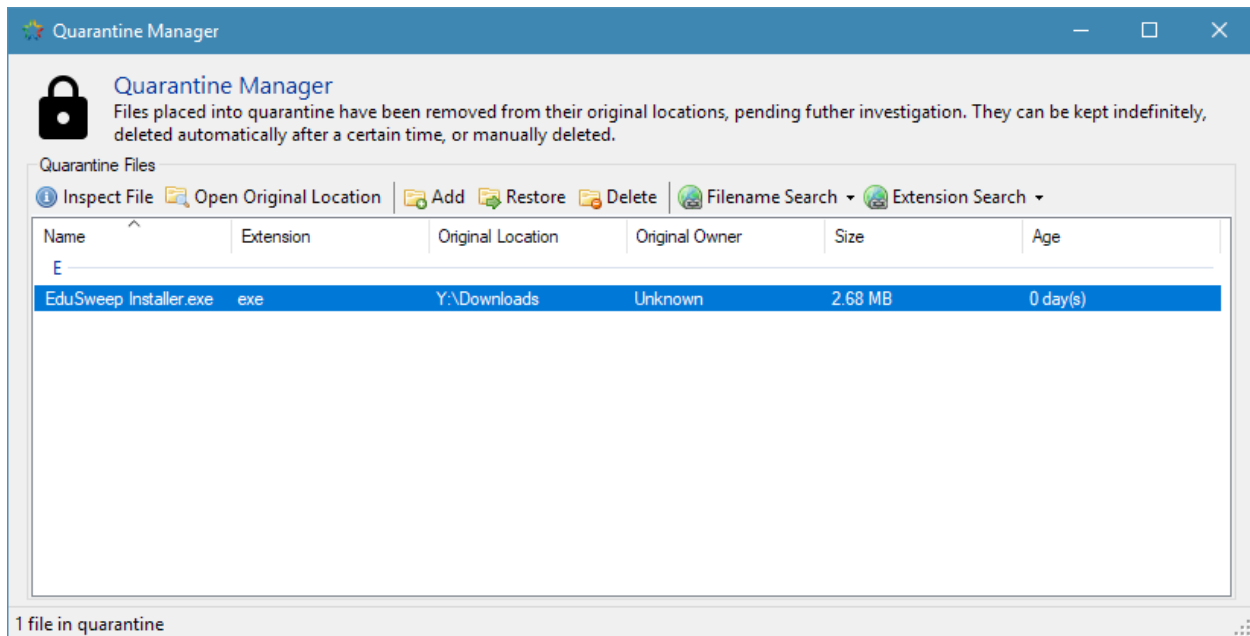
For performance reasons, the list is not populated until the scan process has completed.

The strip of buttons along the bottom of the tab give you the option of moving the currently selected files into quarantine or deleting them.

When only a single file is selected, the “Show File” and “Details” buttons are enabled. These open the file’s location in Explorer and open the File Inspector utility, respectively.

2.4 Quarantine Manager

Files can be placed into quarantine if they are suspect or if they need to be removed from their original location yet still preserved for evidence collection. The Quarantine Manager lists files that have been stored in quarantine following a scan, or those that have been added manually. It also provides functions for deleting and restoring these files, as well as local and online resources for finding out more information about them.



2.4.1 Quarantining Files

When adding a file to quarantine EduSweep will attempt to move it from its original location. If the file cannot be moved (when it is located on a read-only filesystem, for example) then the quarantine process will fail and the file will remain in its original location.

2.4.2 Restoring Files

Restoring a previously-quarantined file first copies the file to its original location. If the copy process succeeds then the file is then deleted from EduSweep's quarantine along with its metadata. If the file cannot be copied back then the restore process is aborted and the file remains in quarantine.

The original location of the file is stored as part of the quarantine metadata at the time that the file is quarantined. If restoring the file from a different machine from the one on which it was quarantined then be aware that paths may be interpreted differently. For example, two different, mapped network drives may have the same drive letter on different machines.

Note: In a standard, non-portable installation the quarantine folder for the current user will be part of their roaming profile (%appdata%\EduSweep\Quarantine). Moving large files into the quarantine folder can slow down the logon process as these files need to be fetched along with the profile.

2.5 Report Manager

Report Manager
A report is produced each time a scan task completes. Reports contain information about the scan and details of any detected items.

Available Reports

Print Print Preview Delete Save as Web Page

Task Name	Completed	Duration	Run By	Age
Demo	13/02/2019 at 22:00	0 day(s)	MICKEY\Paul	0 day(s)

Report Contents

Task Summary

Started: 13/02/2019 at 22:00
 Completed: 13/02/2019 at 22:00
 Duration: 0 hours, 0 minutes, 3 seconds
 Started By: MICKEY\Paul

Detected Items (2)

File Name	Triggered Elements	Owner	Size	Path
planck_rev4_default_cb81afcc.hex	Extensions: hex	Unknown	74.62 KB	Y:\Downloads
EduSweep Installer.exe	Keywords: edusweep	Unknown	2.68 MB	Y:\Downloads

1 report available

A report is produced each time a scan task completes. The report contains a summary of the task (start time, duration, etc) along with a list of detected files, if any were found.

Report contents are displayed in the Report Manager window using an embedded web browser. The Report Manager also provides functions for removing, printing and exporting reports.

2.5.1 Printing

The HTML-formatted report can be printed directly from EduSweep, avoiding the need to first export the report and then open it in a separate web browser.

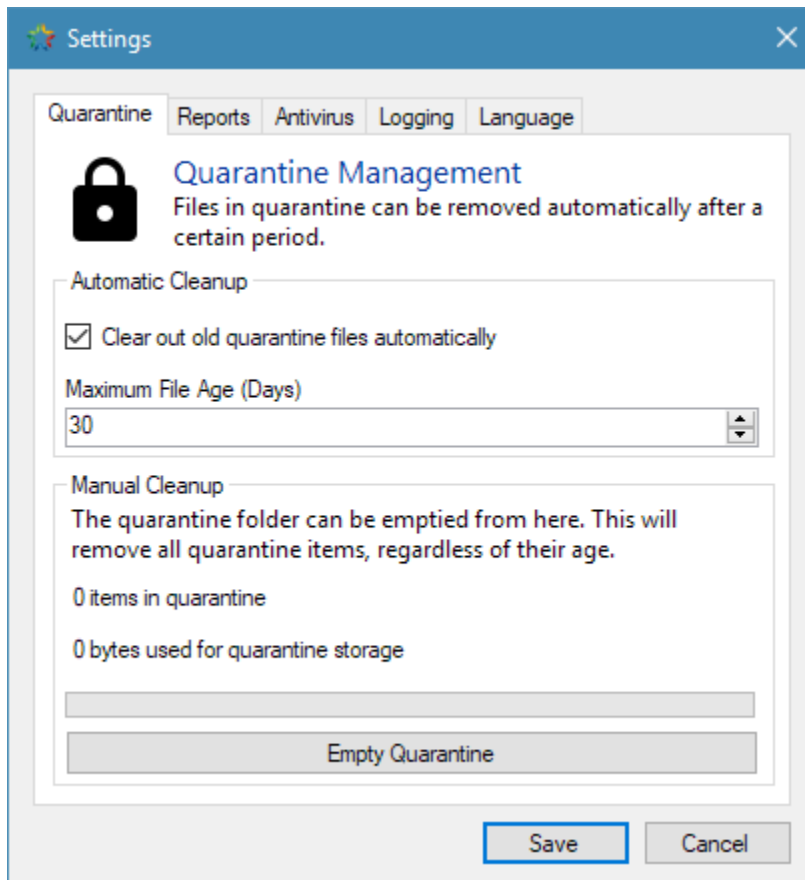
2.5.2 Export

Reports can be exported in HTML format for archiving or for viewing in an external web browser.

2.6 Settings

The settings window provides configuration options for EduSweep that affect reports, quarantined files, logging and antivirus (ClamAV) integration.

2.6.1 Quarantine Tab

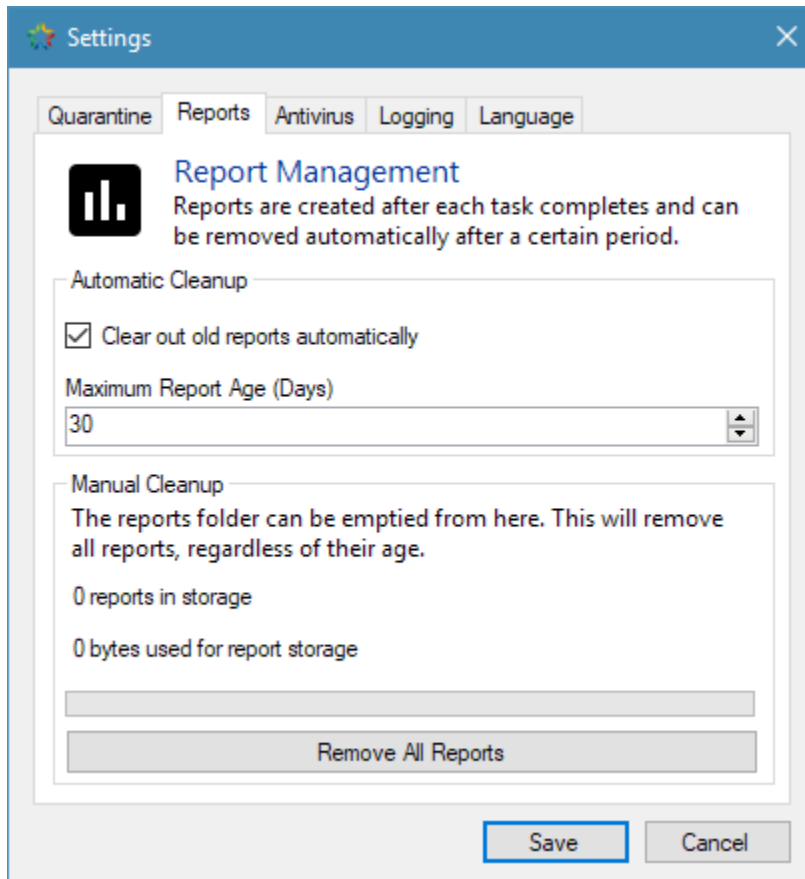


The quarantine tab sets the age limit for quarantine files and whether files older than this limit should be removed automatically or not. *Age*, in this context, refers to the number of days since a given file was moved into quarantine.

The automatic removal, if enabled, occurs each time EduSweep is started.

Regardless of whether automatic removal is enabled or not, the quarantine folder can be emptied using the *Empty Quarantine* button. This will remove **all** files from quarantine regardless of their age.

2.6.2 Reports Tab

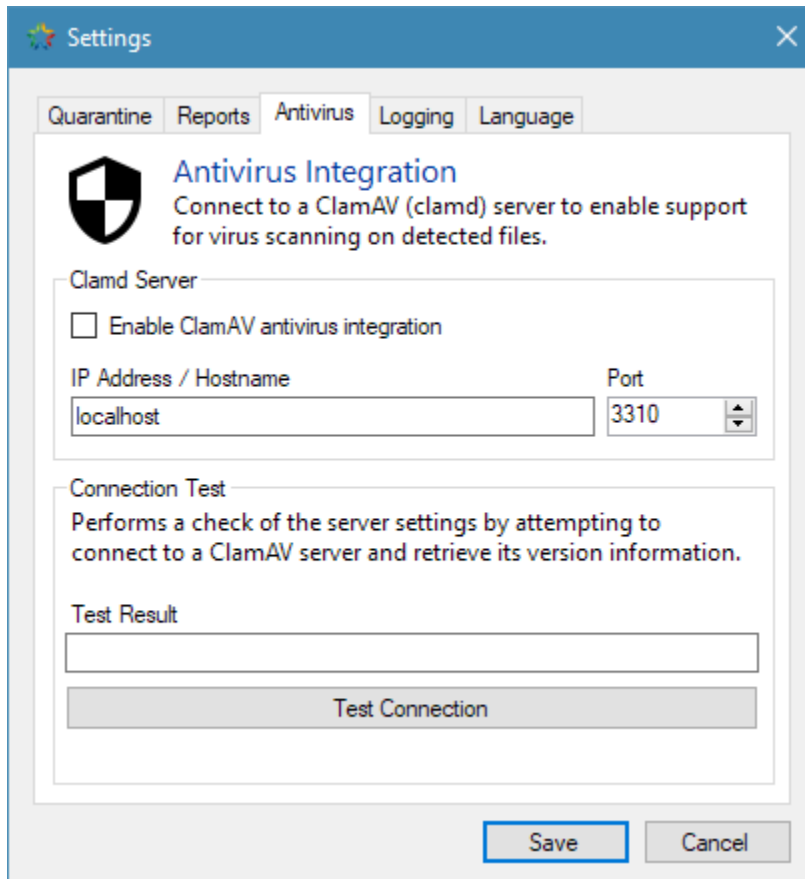


The reports tab sets the age limit for reports and whether reports older than this limit should be removed automatically or not. *Age*, in this context, refers to the number of days since a given report was generated.

The automatic removal, if enabled, occurs each time EduSweep is started.

Regardless of whether automatic removal is enabled or not, the reports folder can be emptied using the *Remove All Reports* button. This will remove **all** reports regardless of their age.

2.6.3 Antivirus Tab



The antivirus tab manages EduSweep's integration with a ClamAV server (clamd). If the *Enable ClamAV antivirus integration* checkbox is ticked then ClamAV integration is enabled at the application level. Scan tasks also provide this setting at a task level and the two work in combination:

Enabled at application level + Enabled at task level: ClamAV will be used
 Enabled at application level + Disabled at task level: ClamAV will not be used
 Disabled at application level + Enabled at task level: ClamAV will not be used
 Disabled at application level + Disabled at task level: ClamAV will not be used

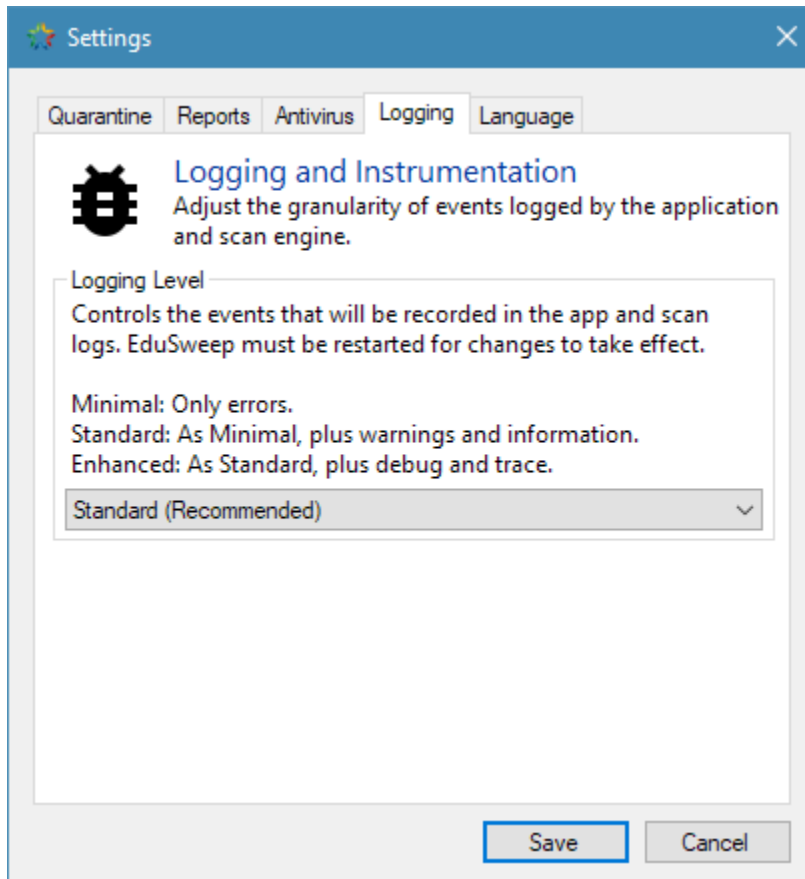
Note: If ClamAV is going to be used for a scan task then EduSweep will test connectivity with the clamd server before beginning the scan process. If the server does not respond then ClamAV integration will be disabled for the scan, overriding the above settings.

The address and port of the server can be set using the text box and numeric selector. The address may be given as a hostname (fully-qualified where possible) or as an IP address. Ensure that the host is reachable from all machines where EduSweep will be used.

EduSweep defaults to *localhost:3310*, which is appropriate for using EduSweep on a single machine which is also running clamd locally.

Use the *Test Connection* button to have EduSweep ping the clamd server to check the specified address and port for correctness.

2.6.4 Logging Tab



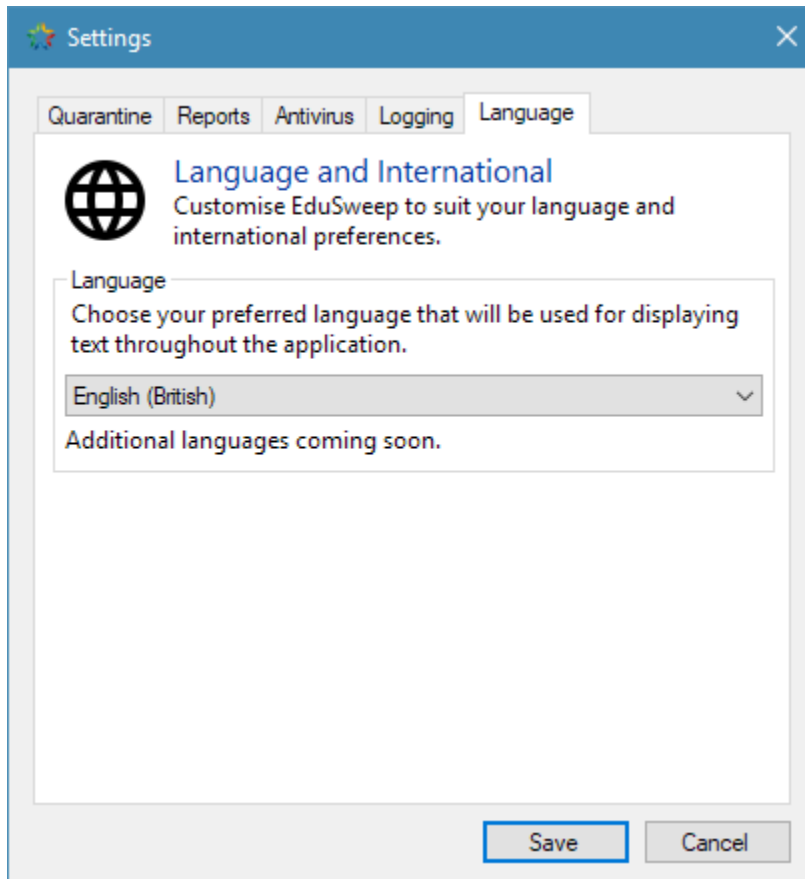
The logging tab allows the level of logging data generated by the application to be adjusted. This affects both the application log and the logs generated for scan tasks when they are run.

Reducing the logging level to *Minimal* will reduce the output in both the scan task log files on disk and the scan task log displayed in the *Task Progress* window. This option may be desired if you find that the default setting is too verbose.

Increasing the logging level to *Enhanced* will only affect the log files (because of the extreme verbosity) and the log in the *Task Progress* window will not display the additional log output.

In most cases it is sufficient to leave the logging level at its default setting unless you are encountering issues and requesting support.

2.6.5 Language Tab



The language tab is used to set the language used for the EduSweep interface. Currently only a single language is available (British English), additional translations are planned for future releases.

These guides cover supplemental topics such as the use of signatures and signature elements, ClamAV integration and advanced settings.

3.1 ClamAV (Antivirus) Integration

ClamAV is an open-source antivirus engine. It is integrated into several widely-used products and is also available as a standalone Windows application. EduSweep has the ability to connect to a ClamAV server instance (known as *clamd*) so that it can leverage its antivirus scanning functionality.

Warning: As described in more detail in the following sections, EduSweep is not a replacement for a comprehensive anti-malware application and should not be treated as such. ClamAV integration is provided for utility purposes only.

Warning: No application can provide 100% threat detection under all conditions. Check suspect files with additional anti-malware software if there is any doubt about their security status.

This approach is used for EduSweep because it presents three main advantages:

- EduSweep does not need to incorporate an antivirus scan engine into its codebase, or link against a ClamAV library. This would be quite a heavyweight solution.
- The ClamAV server does not need to run on the same machine that is running EduSweep. A centralised server may be used to host *clamd*, which multiple EduSweep instances can connect to in parallel.
- The ClamAV server handles antivirus signature updates centrally.

Note: Even with ClamAV integration enabled, EduSweep does not act as a real-time virus scanner. It does not

integrate into the operating system and so should not conflict with any existing antivirus applications.

3.1.1 Antivirus Behaviour

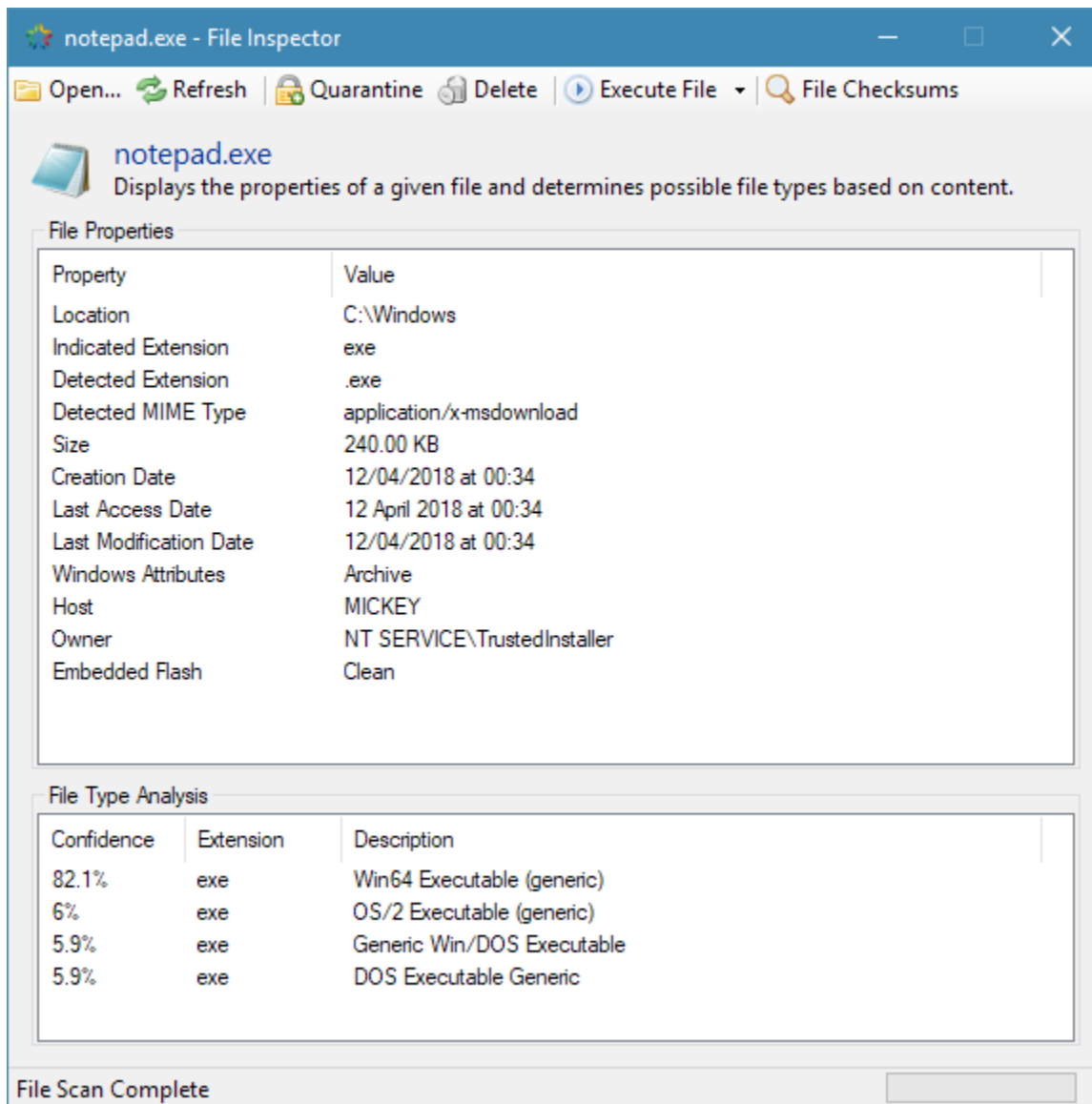
With ClamAV integration enabled EduSweep gains the ability to pass files to the ClamAV server for scanning, and to receive information about their state (clean / infected).

When running a scan, only files that have been detected by one or more detectors are passed to ClamAV for inspection. The EduSweep scan engine does not use ClamAV to check every encountered file for viruses.

Note: As with any application that makes file accesses, if a file on the filesystem contains a virus and EduSweep attempts to access it then an installed antivirus application on the system may detect and block the attempt.

4.1 Overview

The File Inspector is used to gather detailed information about a selected file. It provides file system information, such as creation and modification dates for the selected file, along with an analysis of the file contents. This tool can be used to check if the purported file type matches its actual content; an innocent-looking JPEG file may in fact be an executable with a modified extension and the file inspector can help to detect this kind of scenario.



4.1.1 Inspecting Files

From left to right the toolbar along the top of the window provides:

- An “Open...” button which is used to select and load a file for analysis
- A Refresh button for reloading the file in case of changes
- Buttons to move the file to quarantine or delete it permanently
- An “Execute File” menu for opening the file with its default handler program or in Notepad
- A “File Checksums” button that opens a window to generate checksums

In the lower parts of the window the File Inspector will list the possible file types that it has detected for the current file along with a confidence value.

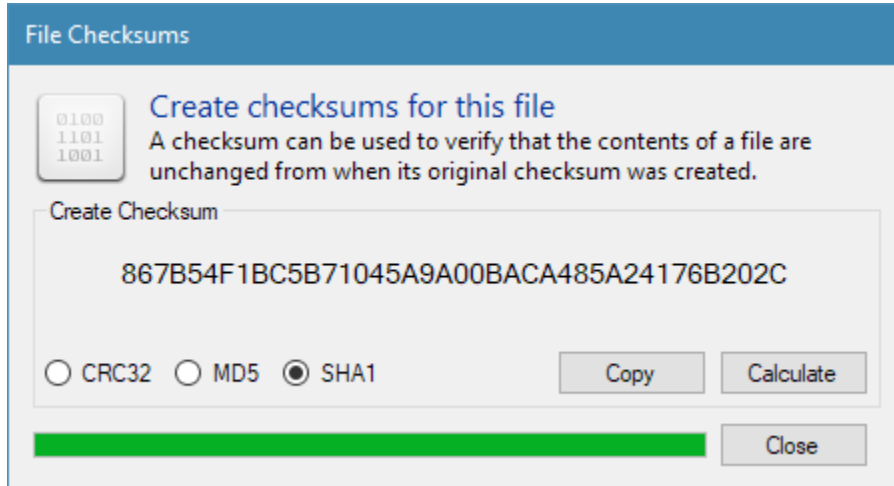
Note: Certain pieces of file metadata, such as the detected filetype are determined using a heuristic process. Be aware

that the result can be incorrect and that some file types are easier to accurately detect than others.

It is much more difficult to determine the file type for text-based formats (e.g. JSON, RTF, XML) than it is for binary formats (e.g. PDF, DOC, PNG). The file type may be given as “Unknown” for certain text-based file formats.

4.1.2 Generating Checksums

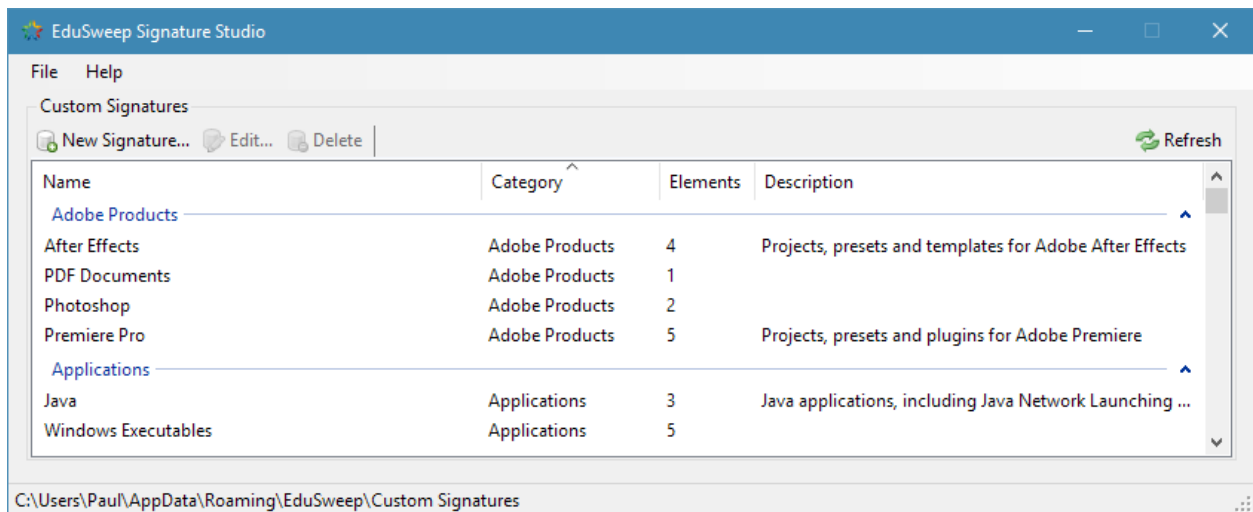
The File Inspector can also generate checksums (hashes) for the loaded file using three, popular hash functions: CRC32, MD5 and SHA-1.



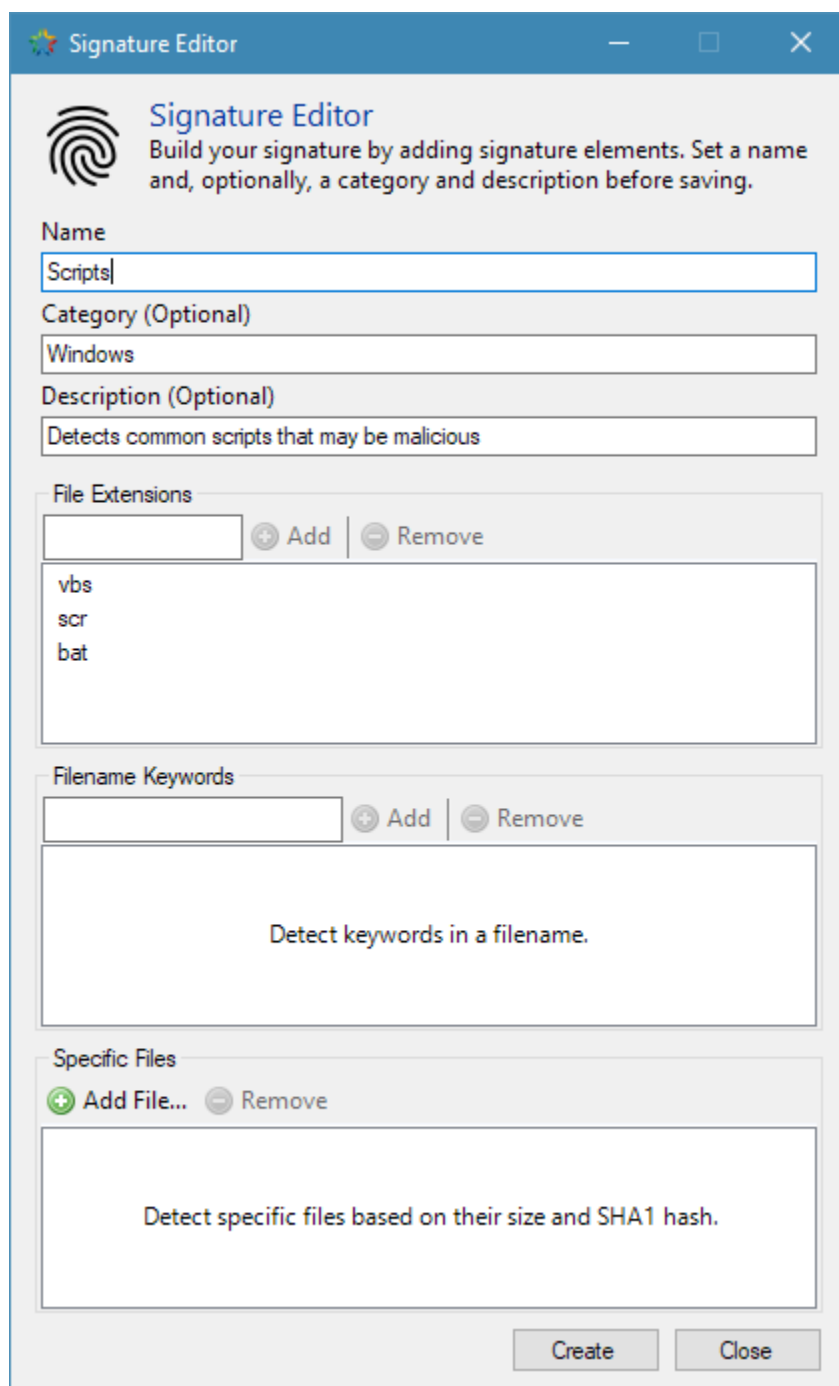
Signature Studio Utility

5.1 Overview

Utility used to manage and create custom signatures for use with the main EduSweep application.



An example of a signature created with the utility:



The image shows a Windows-style application window titled "Signature Editor". The window has a blue title bar with standard minimize, maximize, and close buttons. Inside the window, there is a logo of a fingerprint and the title "Signature Editor" in blue. Below the title, a subtitle reads: "Build your signature by adding signature elements. Set a name and, optionally, a category and description before saving." The main area of the window is divided into several sections. The first section is "Name", with a text box containing "Scripts". The second section is "Category (Optional)", with a text box containing "Windows". The third section is "Description (Optional)", with a text box containing "Detects common scripts that may be malicious". The fourth section is "File Extensions", which includes a text box, an "Add" button, and a "Remove" button. Below this, a list of file extensions is shown: "vbs", "scr", and "bat". The fifth section is "Filename Keywords", which includes a text box, an "Add" button, and a "Remove" button. Below this, a text box contains the instruction "Detect keywords in a filename.". The sixth section is "Specific Files", which includes an "Add File..." button and a "Remove" button. Below this, a text box contains the instruction "Detect specific files based on their size and SHA1 hash.". At the bottom right of the window, there are two buttons: "Create" and "Close".

Signature Editor

Build your signature by adding signature elements. Set a name and, optionally, a category and description before saving.

Name

Scripts

Category (Optional)

Windows

Description (Optional)

Detects common scripts that may be malicious

File Extensions

+ Add - Remove

vbs
scr
bat

Filename Keywords

+ Add - Remove

Detect keywords in a filename.

Specific Files

+ Add File... - Remove

Detect specific files based on their size and SHA1 hash.

Create Close

Performance Tuning

This section covers some tips and tricks to maximise the performance of the EduSweep scan engine, reducing the time taken to run scan tasks. Some insights into the internals of the engine are also provided to give context to the advice.

Note: Performance may vary depending on a number of factors, including software configurations, machine hardware, network topology, background tasks and I/O activity.

While the advice given here should improve performance in the majority of situations, there is no guarantee that an improvement will be seen in your specific configuration.

6.1 Filesystem Proximity

The most significant factor affecting scan task runtime is the location of the directories and files being scanned, in relation to the machine on which EduSweep is running.

Scanning files on a physical disk within the same machine will almost always be **dramatically** faster than scanning a network share or mapped drive. This is because information on the directory structure and, in some cases, file contents must be transferred across the network during the scan process. The amount of data can be considerable if many directories are included in the scan.

If you have a single file server containing all of the directories that you wish to scan then it is preferable, from a performance standpoint, to install and run EduSweep directly on that server. This will provide better performance than scanning from a separate machine that has access to those directories over the network.

6.2 Parallel Scanning Mode

EduSweep 2.6 and above are able to utilise multiple processors to accelerate file scanning. This feature is controlled on a per-task basis and is fully enabled by default.

EduSweep's scan engine can operate in three parallel scanning modes:

- Full: Use (up to) all logical processor cores in the system
- Reduced: Use (up to) all physical processor cores in the system
- Disabled: Use only a single scanner thread (legacy mode)

Within the scan engine the number of parallel threads is set automatically on a per-directory basis, up to the limit set in the scan task. This is based on the number of files. A folder with only a small number of files is unlikely to benefit from parallel scanning due to the overhead of managing threads.

6.3 Number of Signature Element Types

Each type of signature element (extension, keyword, etc) is handled by a dedicated detector component within the scan engine. Initializing these detectors takes time at the start of the scan and adds to the time required to scan each file, since the file is checked by each detector in turn. The overall impact is small in comparison to other factors affecting scan performance.

6.4 Overall Number of Signature Elements

More elements means that each detector has a longer list of comparisons to make. Generally this is not a concern but extreme numbers of signature elements (hundreds) will have a cumulative performance impact that becomes noticeable.

6.5 Hash-Based (Specific File) Signature Elements

When this type of signature element is used in a scan task there is a small performance penalty as more file metadata must be examined.

EduSweep will not perform any file hashing - which is very slow - unless the size of the file being scanned matches the size of one or more specific file elements loaded by the scan task. There is still a small performance penalty from examining the size metadata of each file being scanned.

System Requirements

7.1 Desktop Operating Systems

Operating System	Supported?	Validation Level
Windows 10	Yes	Full
Windows 8/8.1	Yes	Community
Windows 7	Yes	Full
Windows Vista	No	None
Windows XP	No	None

7.2 Server Operating Systems

Operating System	Supported?	Validation Level
Windows Server 2016	Yes	Community
Windows Server 2012	R2 Only	Community
Windows Server 2008	No	None

7.3 Other Requirements

- .NET Framework 4.6.2 or higher. Included with Windows 10. See the [Microsoft .NET Framework Version Table](#) for details of supported OS configurations.

An overview of application-specific terminology used in EduSweep.

8.1 Detection

A detection is created whenever a file being scanned is matched by an element. The detection is associated with the detected file and will be presented in the scan report.

8.2 Element

An element may be a file extension, filename keyword or SHA1 hash of a specific file. When EduSweep scans a file it compares it against every element that has been loaded as part of the running scan task. If the element matches a particular property of the file then a detection is triggered and the file is added to the detected files list.

Elements can be added to signatures or added to a scan task directly.

8.3 File Inspector

Utility used to discover additional information about a specific file, including its filesystem properties and its most likely true file type, based on its content. Also generates common checksums such as CRC32, MD5 and SHA1.

8.4 Quarantine

Quarantine storage is where files are placed after detection during a scan, or manually quarantined from the File Inspector or the Quarantine Manager window. From quarantine the files can be restored, removed or inspected in more detail.

8.5 Report

An HTML-formatted summary of the outcome of a scan task, including details on any detected files.

8.6 Scan Task

A reusable profile that contains one or more directories to scan, one or more elements to detect and settings that govern how the scan is carried out.

8.7 Signature

A signature is a collection of one or more elements that are packaged for use together. Signatures can save time by removing the need to add multiple elements to a task one-by-one.

An example would be a signature designed to detect compressed files that includes the following extension elements: zip, gz, 7z, rar.

Signatures are grouped by category where listed, and then alphabetically within each category.

8.8 Signature Studio

Utility used to manage and create custom signatures for use with the main EduSweep application.

9.1 Need Help?

Ask a question on the [EduGeek Forum](#).

9.2 Request a Feature

- View and create [Feature Requests](#) on GitHub.

9.3 Report an Issue

- File a bug in [GitHub Issues](#).

9.4 Something Else?

- Use the [contact form](#) for other kinds of feedback.

Release notes for each stable, released version of EduSweep.

10.1 [2.6.3] - 2019-05

10.1.1 Fixed

- Moving files into quarantine may fail with an error about a file already existing

10.1.2 Developer Notes

- Fixed a few StyleCop issues

10.2 [2.6.2] - 2019-04

10.2.1 Added

- File Inspector now shows file content analysis for known file types
- “Select Group” buttons in the scan results list
- Right click menu to select or clear all scan results
- Check box at top left of scan results list to select or clear all scan results

10.2.2 Changed

- File Inspector is using new libraries to determine MIME type and file extension
- Grouping behaviour is improved in list views across the application

- Slightly improved performance when loading large lists of files
- Use monochrome logo on main window

10.2.3 Fixed

- The main window shows incorrect scan status information when running parallel scans
- Buttons on the task results tab have an incorrect state after deleting file(s)
- Default documentation link points to trunk version instead of stable
- Broken File Inspector images in documentation

10.2.4 Developer Notes

- Added EdUtilsTests project and some basic tests
- Added MIME library
- Added Analyzer interface
- Added MIMEAnalyzer analyzer
- Added ChecksumAnalyzer analyzer
- Added SizeDetector detector (not yet used)
- Removed TrID library
- Removed some unused code
- Signatures are now part of the EduEngine project instead of EdUtils
- Applications are now built with 64-bit targets

10.3 [2.6.1] - 2019-02

10.3.1 Added

- Overview documentation for Signature Studio and File Inspector utilities

10.3.2 Changed

- Automatic cleanup of reports now defaults to OFF (new installs only)
- Automatic cleanup of quarantine now defaults to OFF (new installs only)
- [Issue #7] List views now remember column sizes, sort order, etc across sessions * This affects the main window, Quarantine Manager and Report Manager
- [Issue #10] Resizeable windows now remember their sizes across sessions
- Inaccessible directory log entry is now INFO type instead of WARN
- Clarified portable mode checkbox actions in installer
- Minor interface improvements for Signature Studio tool

- Updated and corrected Performance Tuning document

10.3.3 Removed

- File Inspector quarantine button (pending review of how it integrates with main app)
- File Inspector “Root Location” info (will be restored in a File Inspector overhaul)

10.3.4 Fixed

- Crash when attempting to save a task, report or signature to a read-only directory
- Disabling parallel scanning does not limit engine to a single thread
- Task Editor “Remove” button for elements does nothing if multiple elements are selected
- File Inspector “Quarantine” menu button is broken
- Potential configuration file corruption due to race condition
- Doubled-up warning messages if a directory is inaccessible
- [Issue #2] TaskDialogs are not wrapped with the ‘using’ directive
- Outdated information in installer documentation
- Missing screenshots in some documentation pages

10.3.5 Developer Notes

- Added VS Code Analysis rules to run on build
- Pruned some dead code
- Config.Net library updated to version 4.13.2
- Castle.Core library updated to version 4.3.1

10.4 [2.6.0] - 2019-02

10.4.1 Added

- Third-generation scan engine
- Support for running multiple scan tasks at once
- Support for virus scanning of detected files using ClamAV
- Optional portable application mode
- Signature Studio utility (create and manage custom signatures)
- Full Windows 10 compatibility
- Complete user documentation

10.4.2 Changed

- File Inspector utility can now be run as a standalone application
- TrID filetype database updated to 2018-12-11 version
- Scan tasks can now be cloned (creating a copy with a new name)
- Folders can now be dragged and dropped onto the target directories list
- Lists in the UI can now be grouped and sorted
- Most windows are now resizable and snappable
- Old quarantine files and reports can be cleaned up automatically, or on-demand from the settings window
- Application settings are now in JSON format (instead of XML)
- Improved logging of application events and scan results
- Numerous performance improvements
- Signatures are now included with the installer (no need for software update)
- Installer changed to Inno Setup (more options during install, better cleanup)

10.4.3 Removed

- Aero Glass theme support
- Windows XP support
- Software Update feature (due to server removal)
- Detection support for embedded Flash (due to Flash slowly dying)

10.4.4 Fixed

- Tasks take a very long time to start running (directory pre-scan)
- Icons displayed in the File Inspector are not always high quality
- File Inspector scan time is excessive on very large files
- The application may hang when cancelling a task
- Crash when scanning very deep directory trees
- Crash when closing the File Inspector during a scan
- Crash with 'BadImageFormatException' when starting a task
- Crash when encountering invalid characters in a file extension or keyword
- Resizing of list column headers renders some text unreadable
- Network paths might be incorrectly marked as unavailable
- Files may be missed while scanning folders containing empty subfolders
- Incorrect dialog text when quarantining files
- Incorrect link to FILEExt extension lookup site
- External links are not always pointing to HTTPS versions

- Inconsistent sorting of items in lists

10.4.5 Developer Notes

- Substantial code rework and refactoring (about 50-60% rewritten)
- Visual Studio solution files updated for use with VS2017 Community
- Added StyleCop rules
- Added nClam library to interface with clamd
- Added Config.NET library to handle more portable setting storage
- Added NLog library to replace the old Bitfactory.Logging library
- Updated TrIDLib library (1.01 -> 1.02)
- Removed Mvolo.Shellicons library
- Removed Ionic.Zip library
- Removed SharpZipLib library
- Moved to the GNU GPLv3 license
- Improved license compliance for bundled libraries
- Now using nuget packages where possible
- Added license and copyright headers to all code files

CHAPTER 11

Welcome

EduSweep is a tool for finding and removing unwanted files - based on their extension, their name, or their content. It helps to keep your network free of files that contravene your usage policies, that take up too much space or that may be vectors for malicious content.

EduSweep offers features that go beyond what is offered by the built-in Windows search tools; it can help you to target specific types of unwanted files more easily while also offering evidence gathering and file inspection tools.

Scan tasks make repeated, regular scans quick and easy to run. Select relevant directories to scan then quickly target groups of files using signatures (premade sets of things to detect during the scan). The Signature Studio utility lets you create, manage and share custom signatures that extend the signatures included with the application.

Built-in reporting tools support evidence collection, with a report being produced each time a scan task completes. HTML export of reports is available to facilitate archiving and printing.

Quarantine functionality allows you to store files for further inspection, while the included File Inspector utility can offer insights into a file's true content using TrID technology to identify file types based on their binary signatures. This helps in finding files that have been disguised by having their extension changed.

The latest version of EduSweep adds ClamAV integration. This allows you to connect EduSweep to a ClamAV server (clamd) so that any files detected during an EduSweep scan will be automatically scanned for viruses, adding another layer of protection and threat detection.

CHAPTER 12

Donate Coffee

If you do find the software useful then please consider making a donation. Literally thousands of coffee beans gave their lives so that EduSweep could be born. Honour their tasty sacrifice today and help [purchase another cup!](#)