



UNITED **ENDPOINT**
PROTECTOR

UNITED ENDPOINT PROTECTOR

MANUAL

1.4

Table of contents

1.	Introduction	4
2.	Installation	5
2.1.	System Requirements	5
2.2.	Local installation.....	6
2.3.	Software distribution	11
2.4.	Deinstallation.....	12
2.5.	User interface.....	12
3.	License Management	14
3.1.	Unlock vendors	14
3.2.	End of term and extension	15
4.	Update	16
4.1.	Create task.....	17
4.2.	Proxy settings.....	19
5.	File Security	21
5.1.	General settings.....	22
5.2.	Strategy.....	23
6.	Memory Security	24
6.1.	Run.....	25
6.2.	General settings.....	25
6.3.	Strategy.....	27
7.	Registry Security	28
7.1.	General settings.....	29
7.2.	Strategy.....	30
8.	On-Demand Scans	31
8.1.	Create scan task.....	32
8.2.	Strategy.....	35
9.	Technologies	36
9.1.	Avira	36
9.2.	CYREN	39
9.3.	IKARUS	41
10.	Blacklist	42
10.1.	File-Blacklist	42
10.2.	Registry-Blacklist	44
10.3.	Strategy	47
11.	Actions	48
11.1.	Quarantine.....	50
11.2.	Strategy.....	51
12.	Exclusions	52

12.1.	File-Exclusions	52
12.2.	Registry-Exclusions.....	54
12.3.	Strategy.....	55
13.	Dashboard	56
14.	Third party licenses	58
14.1.	Rekall Forensic.....	58
14.2.	WinPmem.....	58
14.3.	The Sleuth Kit.....	58

1. Introduction

The United Endpoint Protector (UEP) is a universal security system for Microsoft Windows to protect against cyber threats. The system unifies the operation of independent security vendors and makes them available by click. Thus, the United Endpoint Protector (UEP) is equipped with various anti-malware technologies that can be unlocked using technology licenses. After unlocking, the desired vendors can be activated and combined with each other at any time in the respective security features.

Implementing the United Endpoint Protector (UEP) involves the following steps:

1

Install the United Endpoint Protector instead of your previous antivirus product.
(see chapter 2)

2

Unlock the desired vendors with the help of technology licenses, which you will receive from us.
(see chapter 3)

3

Activate the desired vendors via the respective technology interface in the security features.
(see chapter 9)

4

Create an update task to update the active vendors with the latest information.
(see chapter 4)

This manual is designed to help you install and operate the United Endpoint Protector (UEP) on your Windows computer. The following chapters guide you step by step through this process and explain possible strategies.

2. Installation

The United Endpoint Protector (UEP) can be installed on a Windows computer using the installation package 'uepsetup.msi' which can be downloaded from the Tabidus website. Depending on the installation environment, the following chapters describe the required steps to install the UEP.

Before installing the UEP on productive machines, its functionality and configuration should be checked on test devices. Depending on the application area, the available hardware and the operation of other software components, special adjustments may be necessary for the UEP.

2.1. System Requirements

Before you perform an installation of the United Endpoint Protector (UEP) on a computer system, make sure that the following prerequisites are met:

- The operating system of the computer is one of the following:
 - Microsoft Windows 10
 - Microsoft Windows 11
 - Microsoft Windows Server 2012 R2
 - Microsoft Windows Server 2016
 - Microsoft Windows Server 2019
 - Microsoft Windows Server 2022

- The hardware of the computer has at least the following resources:
 - Intel compatible processor (4 cores recommended)
 - 4 GB memory
 - 2 GB free disk space

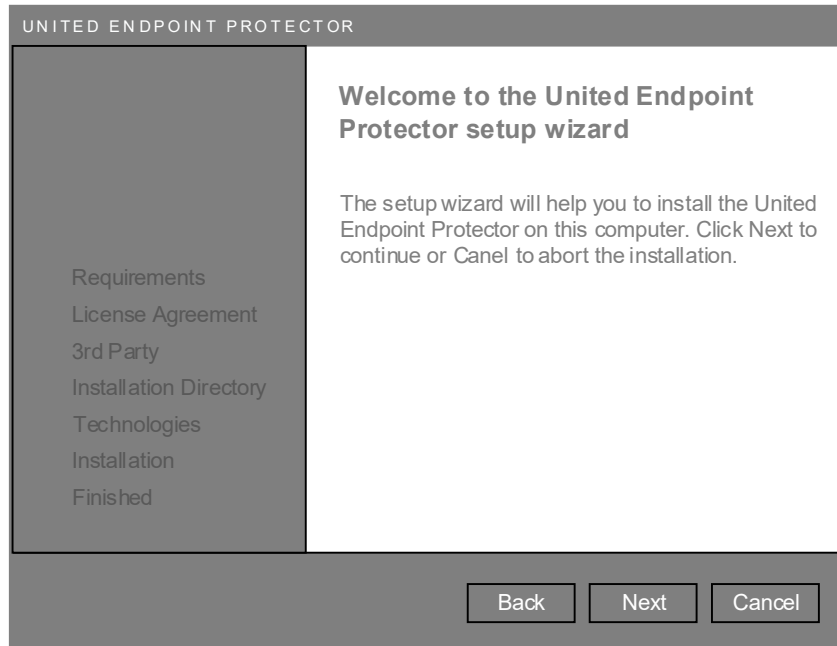
- Local administrator rights for the installation process are available.

- No other anti-virus software is installed on the device.

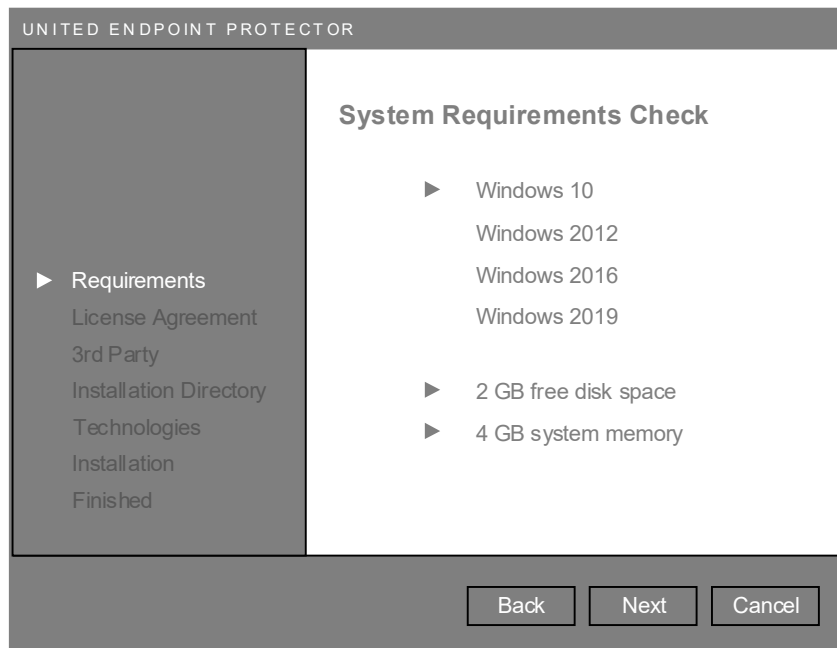
2.2. Local installation

The local installation is suitable for implementing the United Endpoint Protector (UEP) on individual computer systems. Before starting the installation, make sure that the requirements listed in chapter 2.1 are met.

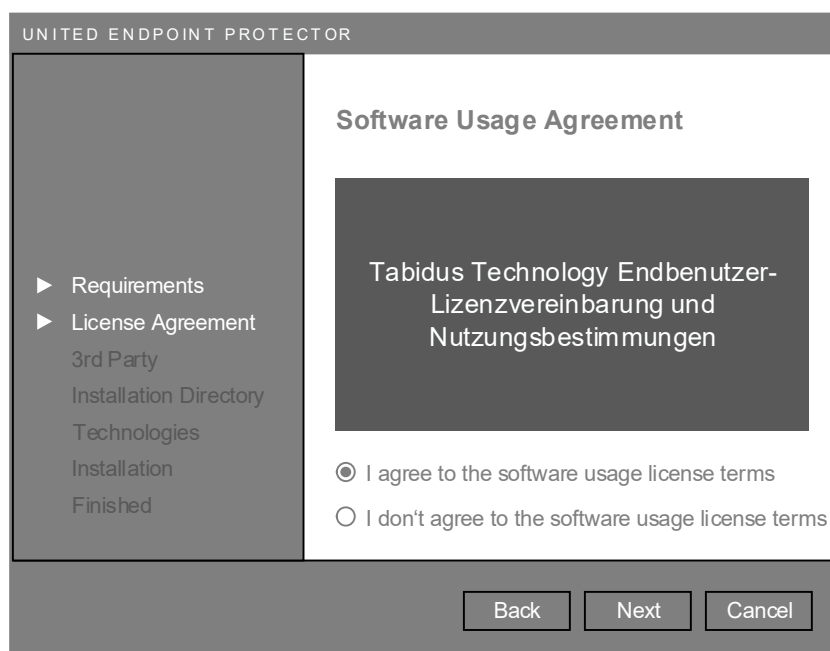
To start the local installation, execute the 'uepsetup.msi' with local administrator rights. After a short while, a Welcome window will appear. Click on 'Next' to start the installation.



The next step automatically verifies system compliance with operating system, disk space, and memory requirements. If the computer system meets the requirements, you can continue the installation with 'Next'. Otherwise, please abort with 'Cancel'.



In the next step, read the EULA for the use of the United Endpoint Protector carefully. These can also be found on our website at <https://www.tabidus.com/eula/>. To proceed with the installation, your consent to the terms is required. Then you can continue with 'Next'.



If there is any other security software on the computer system that has not yet been removed, it can be uninstalled automatically during the installation process. You can specify in this step up to three command-line commands to be executed. This procedure is particularly suitable for a quick product change without long downtimes.

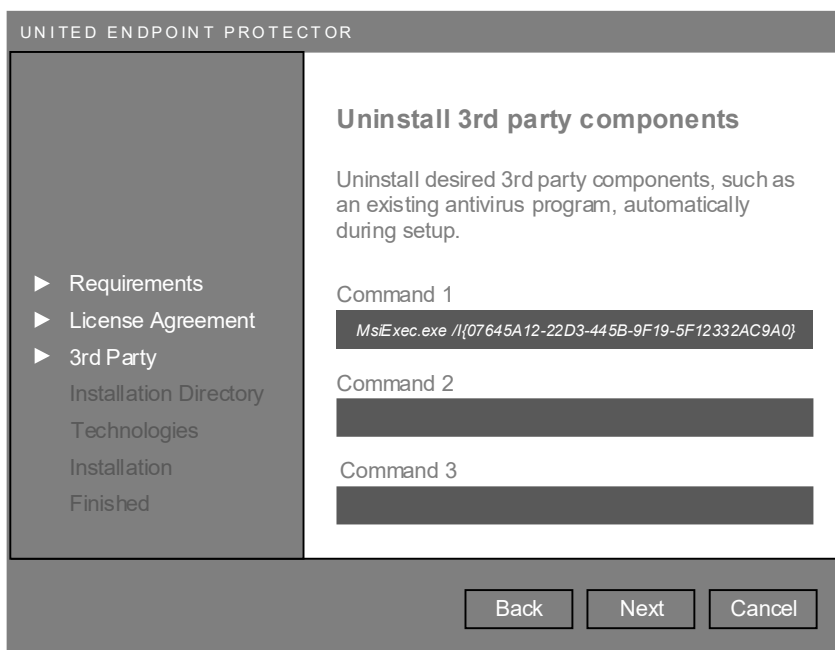
In many cases, suitable uninstall commands can be found in the Windows Registry at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall. Search for the desired component and check if there is an 'UninstallString' entry. For example, this might look like this:

```
MsiExec.exe /I{07645A12-22D3-445B-9F19-5F12332AC9A0}
```

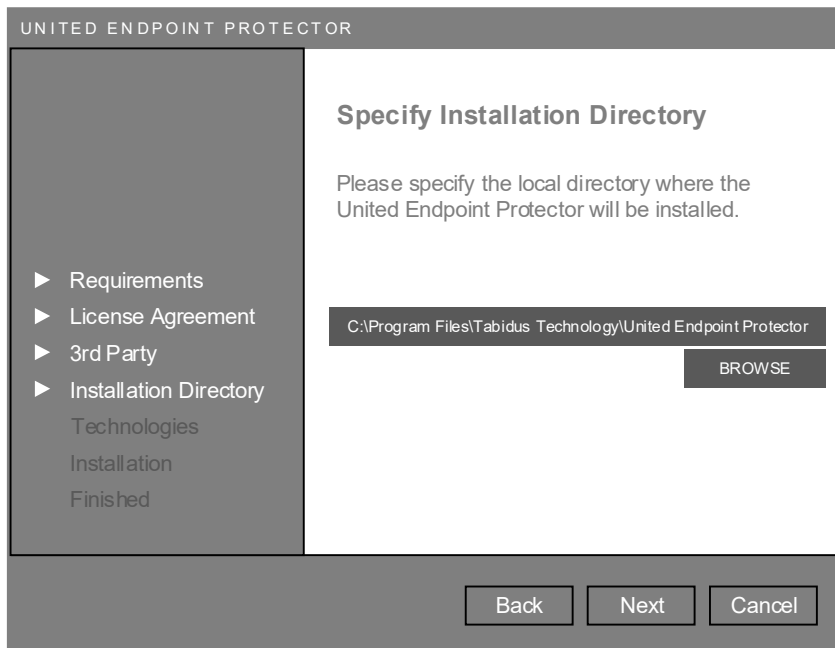
Copy the string into one of the text input fields of the setup. Keep in mind that your security software may have enabled self-defense mechanisms that prevent uninstallation. If in doubt, please contact your previous provider for detailed information on uninstalling the product.

On Windows Server 2016 and 2019, you can uninstall the Windows Defender role, if necessary, with the following command: *Uninstall-WindowsFeature -Name Windows-Defender*

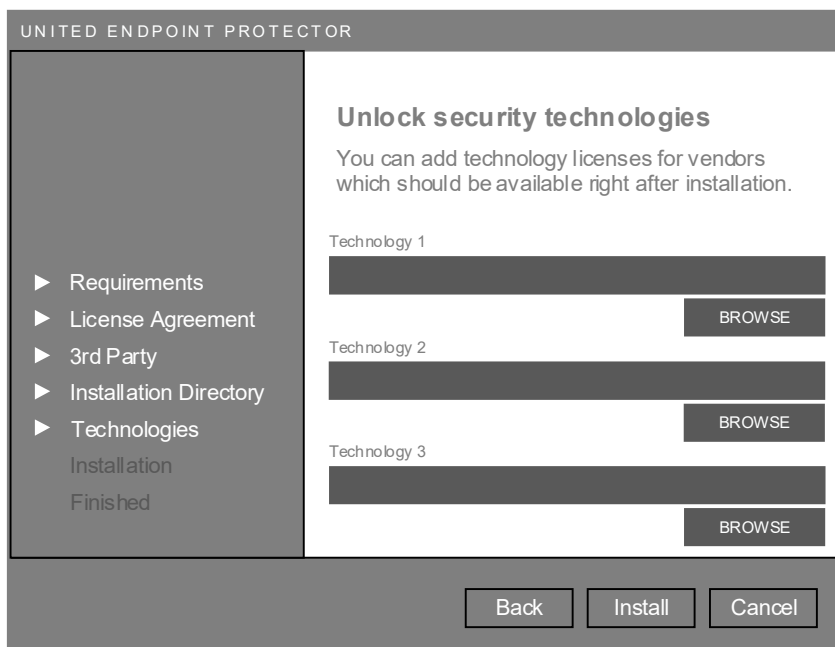
This information is optional. If you do not want to uninstall any components, click 'Next' to continue.



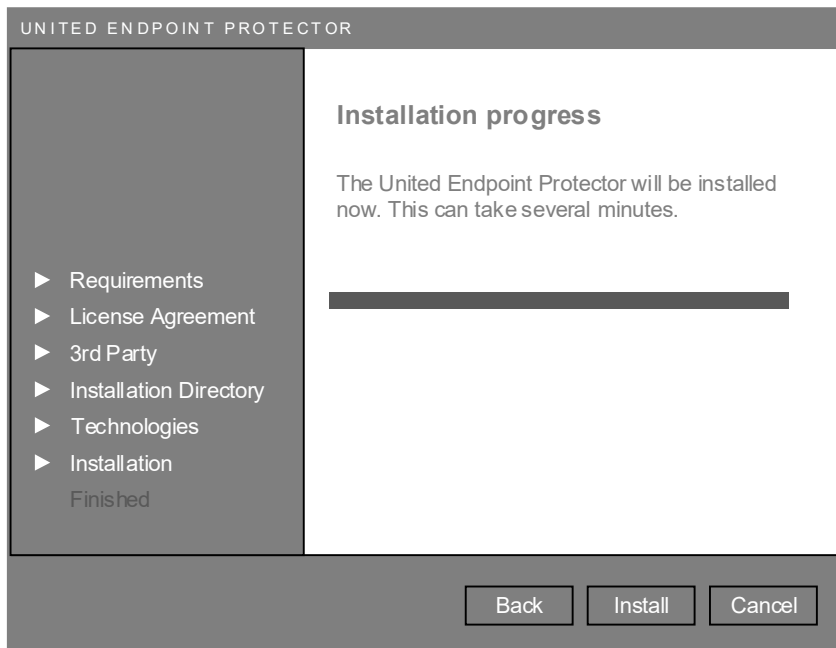
In the next step, specify the desired installation directory in which the UEP is to be installed. With the help of the 'Browse' button, you can select a different directory. Then click on 'Next' to continue.



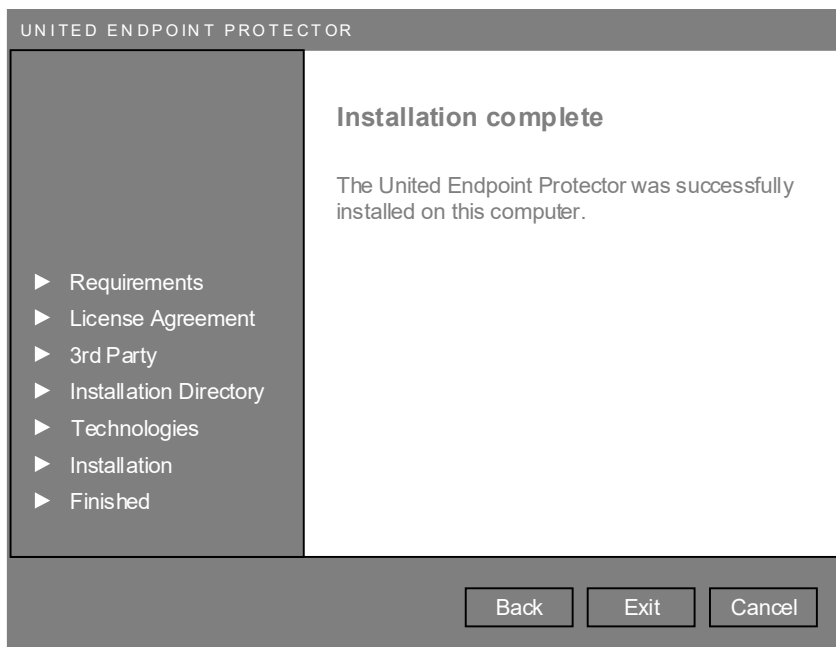
If you want to make certain security providers available immediately after installation, you can specify the appropriate technology licenses (see chapter 3) in the next step. Otherwise, this option will also be available to you at any time after installation. Then click on 'Install' to start the installation process.



During the installation process, all specified information is taken into account and the United Endpoint Protector (UEP) is installed on the computer system. This process can take several minutes.



Finally, the installation result will be presented to you. If an error has occurred during the process, a detailed installation log will be available afterwards.



2.3. Software distribution

To install the United Endpoint Protector (UEP) on multiple computer systems, a form of software distribution is appropriate. In addition to various third-party solutions, Microsoft also provides a feature for distributing MSI packages via Active Directory.

To perform an unattended, automatic installation of UEP, the 'uepsetup.msi' can be started with the following parameters:

<code>accepteula=true</code>	Accepts the terms of the End User License Agreement and Terms of Use as found at https://www.tabidus.com/eula/ .
<code>uninstall1="" uninstall2="" uninstall3=""</code>	Allows you to uninstall third-party components, such as existing security software, during the installation process, as described in chapter 2.2.
<code>installdir=""</code>	Defines the installation directory in which the UEP should be installed.
<code>tech1="" tech2="" tech3=""</code>	Let's you specify desired technology licenses to make certain security vendors available after installation, as described in section 2.2.
<code>/qn</code>	Suppresses the display of the installation process and executes it in the background.
<code>/qb</code>	Suppresses an interaction with the installation process and displays a progress bar. This parameter is mandatory if /qn is not used.

Sample:

```
msiexec /i uepsetup.msi accepteula=true uninstall1="MsiExec.exe /I{07645A12-22D3-445B-9F19-5F12332AC9A0}" uninstall2="MsiExec.exe /I{01395A12-11AA-3F91-8FE9-11117452A1111}"  
installdir="D:\Program Files\UEP" tech1="E:\licenses\mylicense.dat" tech2="E:\licenses\secondlicense.dat"  
/qb
```

2.4. Deinstallation

In order to uninstall the United Endpoint Protector (UEP), its self-protection (see chapter 5.1) must be deactivated beforehand. Afterwards, the uninstall routine can be called in the Windows Control Panel under 'Programs and Features'. Alternatively, deinstallation is possible with the command 'MsiExec.exe /X{GUID}', which can be found in the Windows Registry under the key HKLM\SOFTWARE\Microsoft\CurrentVersion\Uninstall\{GUID}.

2.5. User interface

To verify the operation and configuration of the United Endpoint Protector (UEP), the user interface (uepconsole.exe) is available. This can be accessed via the system tray icon of Tabidus or the Windows start menu.



UEP user interface

The most important control of the interface is the main menu, in the upper left corner. All features of the UEP can be called up via this.

- **Status**

Status display of all important operating parameters in order to be able to check the condition and the mode of operation of the UEP at a glance (see chapter 13).

- **File Security**
Real-time monitoring of all file accesses on the local hard disk, network drives and removable media (see chapter 5).
- **Memory Security**
Forensic check of the computer's memory with different methods (see chapter 6).
- **Registry Security**
Real-time monitoring of all accesses to the Microsoft Windows Registry and other Application HIVES (see Chapter 7).
- **On Demand**
Creation and administration of scan tasks for the timed inspection of certain areas of the computer system (see chapter 8).
- **Update**
Status display of security technologies and task management to update technologies (see chapter 4).
- **Licenses**
License management for activating desired security vendors and monitoring their validity (see chapter 3).

Each menu item has a submenu, which provides all related configuration options for the feature. Further information on their exact functioning and operation is explained in the corresponding chapters. If infections are detected, their count is also displayed in the main menu.

By clicking on a menu entry, the respective interface in the main window is called up. Depending on the feature, a menu bar with further operating elements is displayed in the lower area of the interface.

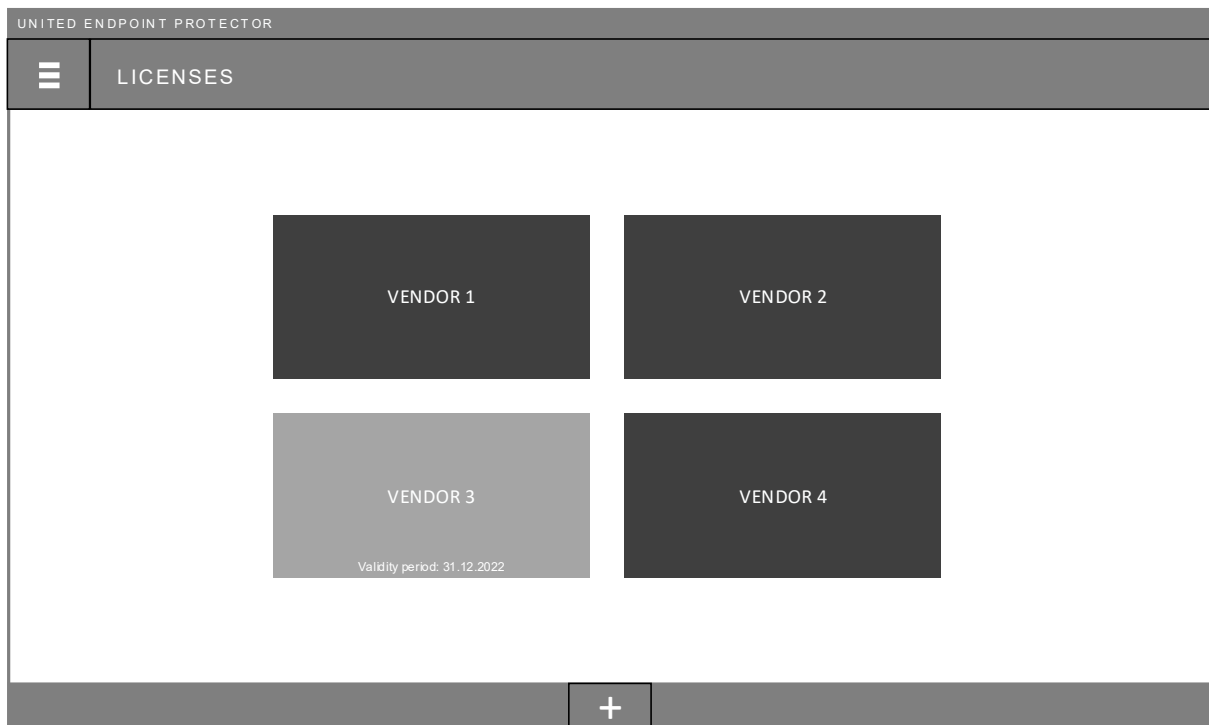
If the UEP is managed centrally by the United Control Center (UCC), access to the user interface may be restricted. In this case, a password prompt appears when the interface is opened. Only by entering the password, which was set by your administrator, will access to the various functions be released.

There is a language selection button in the upper right corner of the interface. With this you can switch the interface language at any time between English and German.

The user interface is a tool to administrate the UEP. The protection function of the UEP does not depend on its execution. Even when the user interface is closed, the UEP is fully functional and performs the configured protection functions.

3. License Management

License management lets you control which security vendors should be used for protection. Click on 'Licenses' in the main menu to open the overview of all available providers. With the help of technology licenses that you receive from us, you can unlock the desired vendors. Which vendors have already been activated, and how long the respective provider is available to you, will be displayed on this overview page.



Licenses -> Overview

3.1. Unlock vendors

To unlock a security vendor, click on 'Licenses' in the main menu to open the license overview. Then click on the Add icon in the lower menu bar and select the existing technology license. If you do not have any technology licenses yet, please contact us.

Upon successful unlock, the logo of the respective vendor changes within a few seconds and the term of the license becomes visible. In addition, a new submenu item will be added under 'Licenses' in the main menu, which will allow you to see details of your license. At this screen, it is also possible to delete a license, if necessary.

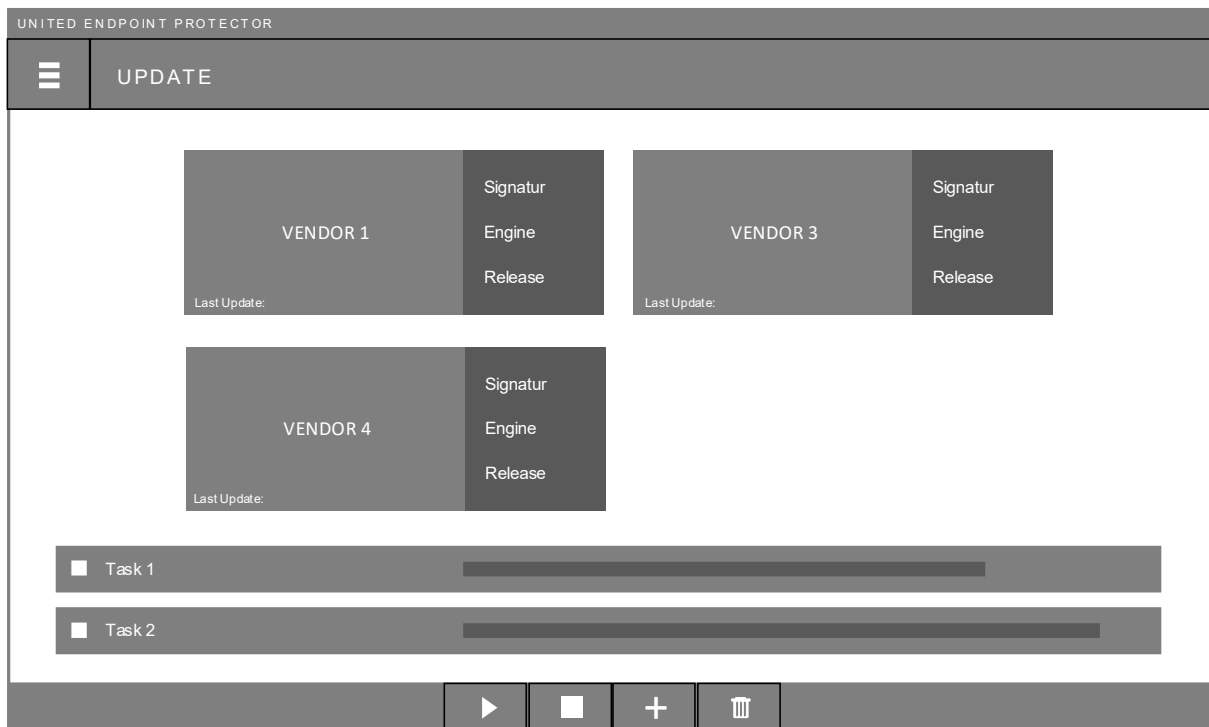
3.2. End of term and extension

When the expiration date of a technology license is reached, it automatically deletes itself and the respective vendor switches itself off. We therefore recommend that you obtain a new license for the vendor in good time, before the end of the term, so as not to jeopardize the security of your computer.

You can add multiple licenses to a security vendor with different durations at any time. To prevent an unwanted shutdown of a provider, we recommend adding another license before expiration. At the time the previous license ends, it will be deleted and the new license will automatically take over.

4. Update

Depending on the selected security vendors and their technical approaches, the technologies need continuous updates to reach their full protection potential. The United Endpoint Protector (UEP) is therefore equipped with an automatic update system, which you can use to supply the unlocked vendors with updates. For this, click on 'Update' in the main menu to open the update overview.



Update -> Overview

In the upper area of the interface, the unlocked vendors and their status are displayed. Depending on the vendor, the components to be updated may differ. The point at which the last update for each vendor took place is indicated. If this time is not within the last 24 hours, this is indicated by red font color.

At the bottom, one or more update tasks are displayed, which you can create as desired (see chapter 4.1). By selecting a task with its checkbox, various icons in the menu bar below become available. With these you can start, stop or delete tasks manually. The time of the last execution of each task is displayed. By clicking on the expander icon, you can see detailed information about the running execution.

4.1. Create task

To create an update task, click on 'Update' in the main menu to open the update overview. Then click on the 'Add' icon on the lower menu bar. This opens the configuration interface of the task.

UNITED ENDPOINT PROTECTOR

UPDATE | New Task

ENABLE TASK

Task Name:

Description:

Technologies: Vendor 1
 Vendor 3
 Vendor 4

Scheduling: Interval: Mnuten
Delay: Mnuten

SAVE

Update -> Task

On the configuration interface, you can make the following settings to define the task:

Enable Task	Enables the automatic execution of the task according to the specified schedule. If the task is not activated, it is ready for manual execution.
Task Name	Any designation for naming the task. This appears in the update overview, as well as in the submenu of 'Update' in the main menu.
Description	Any text that can optionally be entered for documentation purposes. This text is displayed only in the configuration interface of the task.
Technologies	Depending on the unlocked vendors and whether automatic updates exist for them, they will be listed. Use the check boxes to specify which vendor should be updated by this task. You can have multiple vendors updated with a single task. The UEP

	simultaneously downloads all updates and applies them one after another to the engines to prevent interruptions to security.
Scheduling	<p>Sets the schedule for the automatic execution of the task.</p> <p>'Interval' defines the number of minutes until the task should be run again.</p> <p>'Delay' describes the period when the task should start, if the last regular execution did not take place. For example, when the computer was turned off. The delay in this case indicates the number of minutes until the first run should occur after the computer is turned on.</p>

After all settings have been set, the task can be saved with the 'Save' icon in the lower menu bar. This makes the task visible in the update overview, where it can be monitored. The configuration interface of the task can be recalled at any time in the submenu of 'Update' in the main menu.

In order to download the updates, the United Endpoint Protector (UEP) will connect to the respective vendors' servers unless it is centrally managed by the United Control Center (UCC).

Vendor	URL
Avira	http://oem.avira-update.com
Cyren	http://oem.avdl.ctmail.com
IKARUS	http://*.ikarus.at

4.2. Proxy settings

If a proxy server is used to connect to the Internet, you can enter the required connection data in the Proxy settings. You can call these in the submenu of 'Update' via the 'Proxy' item.

The screenshot shows the 'UPDATE | Proxy Settings' configuration window. The title bar reads 'UNITED ENDPOINT PROTECTOR'. The main content area is titled 'PROXY SETTINGS' and contains the following fields and options:

- Address: proxy.srv.int
- Port: 8080
- Use name: serviceusr
- Password: *****
- Use Proxy for: Update-Tasks, Cloud connections, Memory Security Kernel data
- Bypass proxy if not reachable

A 'SAVE' button is located at the bottom right of the configuration window.

Update -> Proxy

The following proxy settings can be made in the configuration interface:

Address	Name or IP address of the proxy server to use.
Port	Port of the proxy server to use.
Username Password	Authentication to the proxy server. This supports basic authentication.
Use Proxy for	Defines the connection types for which the proxy server is to be used. 'Update-Tasks' refers to every connection to a vendor's update server. 'Cloud Connections' refers to all connections of a technology to the cloud of the respective vendor, if the corresponding feature has been activated.

	<p>'Memory Security Kernel Data' refers to the connection establishment of the Memory Security feature to the Microsoft Symbol Server.</p>
Bypass proxy if not reachable	<p>Defines whether the proxy entry should be ignored if it cannot be reached. This is the case, for example, when a mobile device leaves the corporate network.</p>

5. File Security

File security allows you to monitor and check all file accesses on the local hard disk, on network drives and on removable media, in real time. To detect malicious files, you can use any unlocked vendor, in any combination, in this security feature.

Click on 'File Security' in the main menu to open the File Security monitor. The monitor displays all file accesses in real time, as well as the scan and cleaning results of the active vendors.

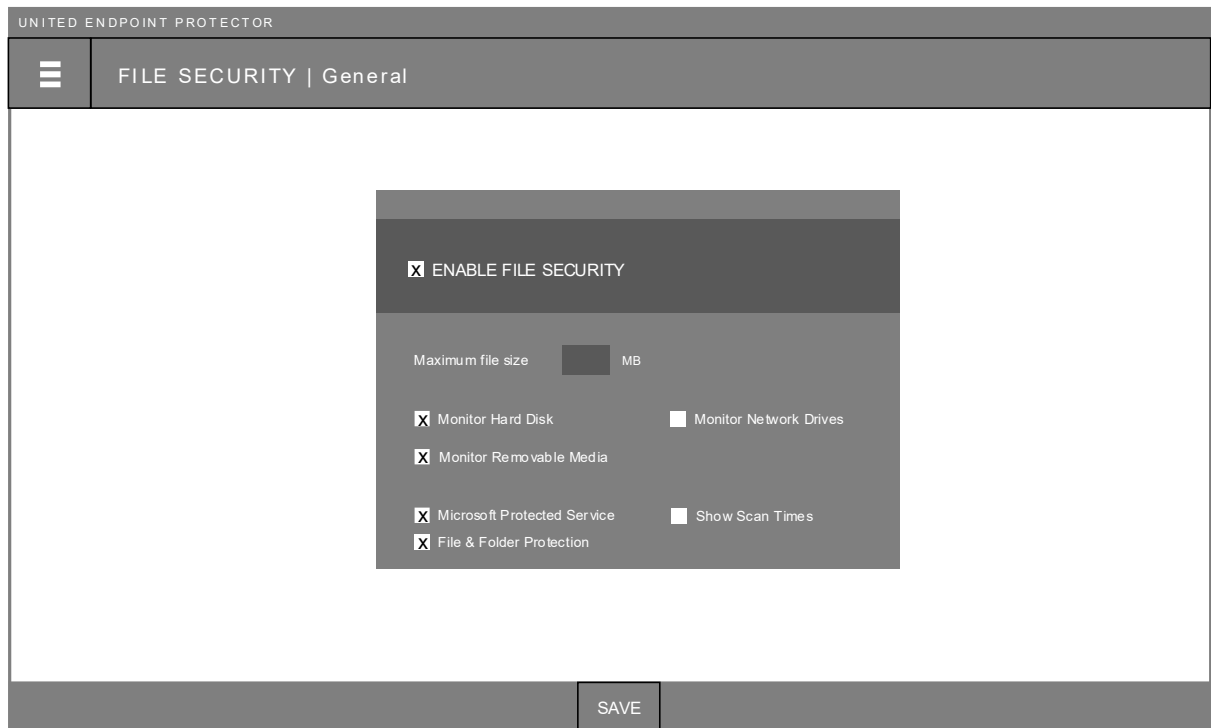


File Security -> Monitor

The user interface displays the last 10,000 accesses, which you can search in real time using the Filter bar. With the 'Export' icon, in the lower menu bar, you can export all recorded accesses to an XLS file. The 'Delete' icon, on the other hand, allows the manual deletion of all recorded data. An automatic deletion takes place by stopping the United Endpoint Protector service or at regular intervals if data is older than 24 hours.

5.1. General settings

The functionality of File Security can be defined via the General settings. To do this, click on 'General' in the submenu of 'File Security'.



File Security -> General

The following settings can be made on the configuration interface:

Enable File Security	Enables or disabled the monitoring of file accesses.
Maximum file size	Sets the maximum size of the files, in megabytes, to be monitored.
Monitor Hard Disk	Enables or disables the monitoring of file accesses on the local hard disk.
Monitor Network Drives	Enables or disables the monitoring of file accesses to network drives.
Monitor Removable Media	Enables or disables the monitoring of file accesses to removable media, such as USB sticks.

Show Scan Times	Displays, in the File Security Monitor, the time periods required to check file accesses.
Microsoft Protected Service	Enables or disables the protection of the United Endpoint Protector (UEP) by the operating system. With it, Windows prevented any manipulation of processes and the service of the UEP.
Enable Self Protection	Enables or disables tamper protection for the files of the United Endpoint Protector (UEP). Protection blocks every unauthorized access to the UEP installation directory. To allow access to the files of desired processes exceptions can be created for this (see chapter 12.1).

5.2. Strategy

File access monitoring is an important security feature to detect threats and prevent infections. Therefore, we recommend activating several security vendors to ensure reliable identification of malicious code.

In order to achieve optimum compatibility with the operating system and other programs when using this security feature, the processing speed of accesses is crucial. The United Endpoint Protector allows you to simultaneously use multiple technologies that perform their investigations in parallel. The total processing time of an access corresponds to that of the slowest vendor. For File Security, therefore, especially vendors with a high data throughput are suitable.

To assess the speed, you can enable in the General settings 'Show Scan Times' (see chapter 5.1). Thus, the individual scan times of all vendors are displayed in the File Security Monitor, including a calculation of the average values. This allows suitable providers for this feature to be identified.

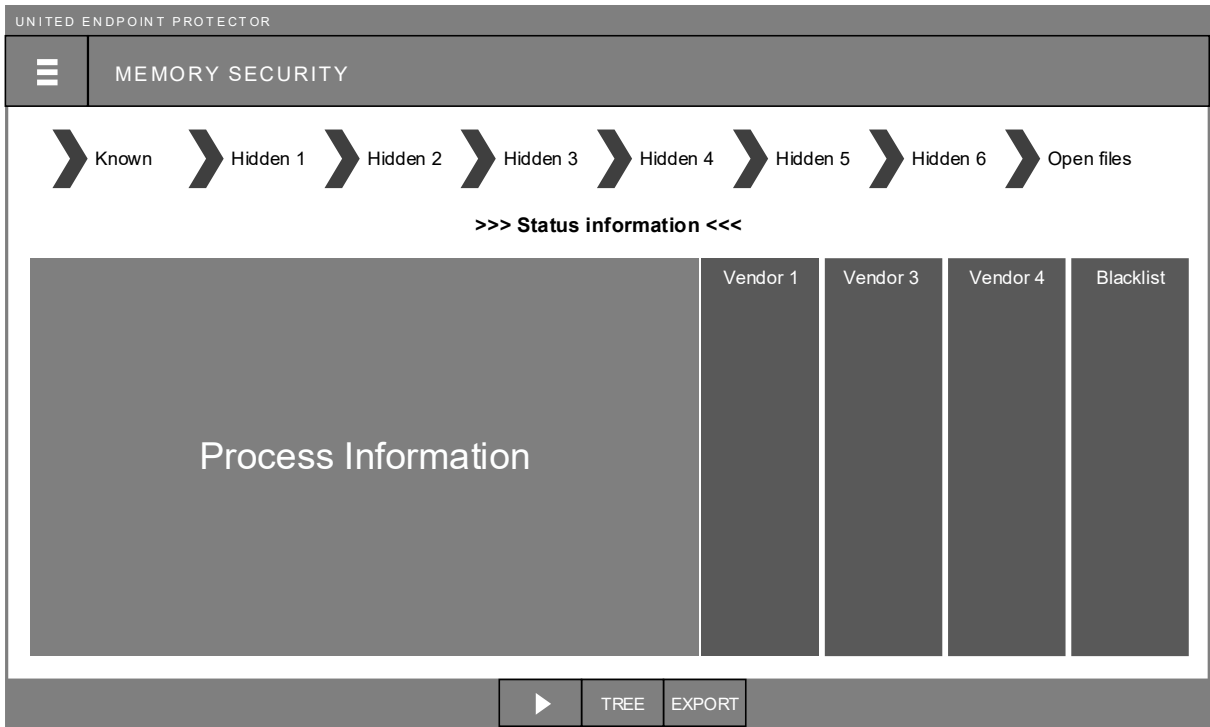
In addition to the selection of suitable providers, the determination of the maximum file size to be examined also has an effect on the overall performance. The larger a file is, the more time is needed to scan it. The size should therefore be as small as possible, but as large as necessary. An average of 10 MB is recommended by many security vendors, but this can be determined at your discretion.

The use of exclusion rules represents another optimization option (see chapter 12). Targeted scan exclusions can reduce the workload and prevent unwanted delays.

6. Memory Security

Memory Security allows you to check the memory of a computer. This is an important security feature to detect and stop the active execution of malicious code. For this task, different forensic methods of Rekall Forensics are available to examine the memory from different perspectives and reveal hidden code executions. The disclosed data can then be assessed by desired security vendors to detect threats.

Click on 'Memory Security' in the main menu to open the Memory Security Monitor. This displays the result of the last or current scan run of the memory.



Memory Security -> Monitor

The top section of the monitor shows the various forensic methods that are run during the scan. Colored markers indicate the progress and duration of the examination and the number of detected processes. Below this, status information is displayed that shows the last time of scan or the currently examined file.

The detailed examination result is prepared in the lower area. This includes information about the discovered processes, their loaded files, and the scan results of the activated security vendors.

In the lower menu bar, an examination can be manually started or stopped, the result visualized in the form of a tree, or exported to an XLS file.

6.1. Run

The examination of the memory can be done manually or at a time interval. At the beginning of a scan, the version of the Windows Kernel is checked. If it has changed since the last scan (e.g. through Windows updates), a connection is made to the Microsoft Symbol Server (<https://msdl.microsoft.com/download/symbols>) to download required kernel data. These serve as a map for the Windows Kernel and are required by forensic methods to correctly identify the memory addresses and entry points.

If a proxy server is used for the Internet connection, this can be in proxy settings 'Update -> Proxy' (see chapter 4.2). Make sure that 'Use Proxy for' has the 'Memory Security Kernel Data' option enabled. If no Internet connection can be established, or if Microsoft has not yet released the Kernel data for the current Windows version, the forensic methods will not work. In this case, the Memory Security switches to emergency operation. This uses traditional Windows APIs, instead of the forensic methods, to identify known processes and performs their investigation. Emergency operation is symbolized by grey arrows in the Memory Security Monitor.

6.2. General settings

The functionality of Memory Security can be defined via the General settings. To do this, click on 'General' in the submenu of 'Memory Security'.



Memory Security -> General

The following settings can be set on the configuration interface:

Enable Memory Security	Enables the automatic examination of memory, based on the configured schedule options. If it is not activated, it is ready for manual execution.
Forensic methods	Defines the forensic methods to be used in the examination. Non-activated methods are skipped.
Scheduling	Sets the schedule for the automatic execution of the examination. 'Scan Interval' defines the count of minutes when the examination should be repeated after the previous run has finished. 'Delay' describes the period when the examination should start, if the last regular execution was missed. For example, when a computer was turned off. The delay in this case indicates the number of minutes until the first run should start after the computer is turned on.
Resource usage	Allows you to specify the CPU load to use during an examination. It should be considered that the more the CPU is used, the shorter an investigation takes. The less a CPU is used, the longer it takes to investigate.
Maximum file size	This configuration option has a double function. First, it sets the maximum size of a file to be scanned by security vendors. If a discovered file is larger than the specified value, it will not be scanned. On the other hand, this value defines the maximum memory size of a process for examination. If the used memory of an active process is smaller than the specified value, it is completely extracted from the memory and used for scans. If the used memory is larger, no extraction takes place and only the referenced executable file is scanned.
Show Scan Times	Displays in the Memory Security Monitor the time periods of the security vendors required to scan the discovered files.

6.3. Strategy

Checking the memory for malicious code execution is an important security feature. Although a regular process start requires a file access beforehand, which can be scanned by File Security, this scan occurs only at the time when the process starts. If, at this time, the threat knowledge is not yet available by the chosen security vendors, the starting process itself is not malicious (such as file-less malware), or code is injected through other means, infection may occur. We therefore recommend having the memory scanned at regular time intervals.

As a possible alternative or supplement to the interval scans, you can also use an on-demand scan (see chapter 8) with other scheduling options. Another option is to combine the examination of the memory with a scan action (see chapter 11). For example, if the File Security identifies a malicious file on the hard disk, a memory check may be triggered in response to detect currently executing malicious code.

The choice of security vendors does not depend on data throughput, compared to File Security. Therefore, slower vendors or more time-consuming investigation techniques can be used. A possible strategy might be to use fast vendors in the File Security and slower vendors for the Memory Security. Also, the variety of providers and techniques could be extended with it.

7. Registry Security

The Registry Security allows real-time monitoring of all accesses to the Microsoft Windows Registry, as well as to other application HIVEs. These are popular targets of malware for making malicious manipulations, storing their own data, or nesting into the computer system. In addition to monitoring, you can use available security vendors to assess the accesses or use the Blacklist (see chapter 10) to set up preventive protection.

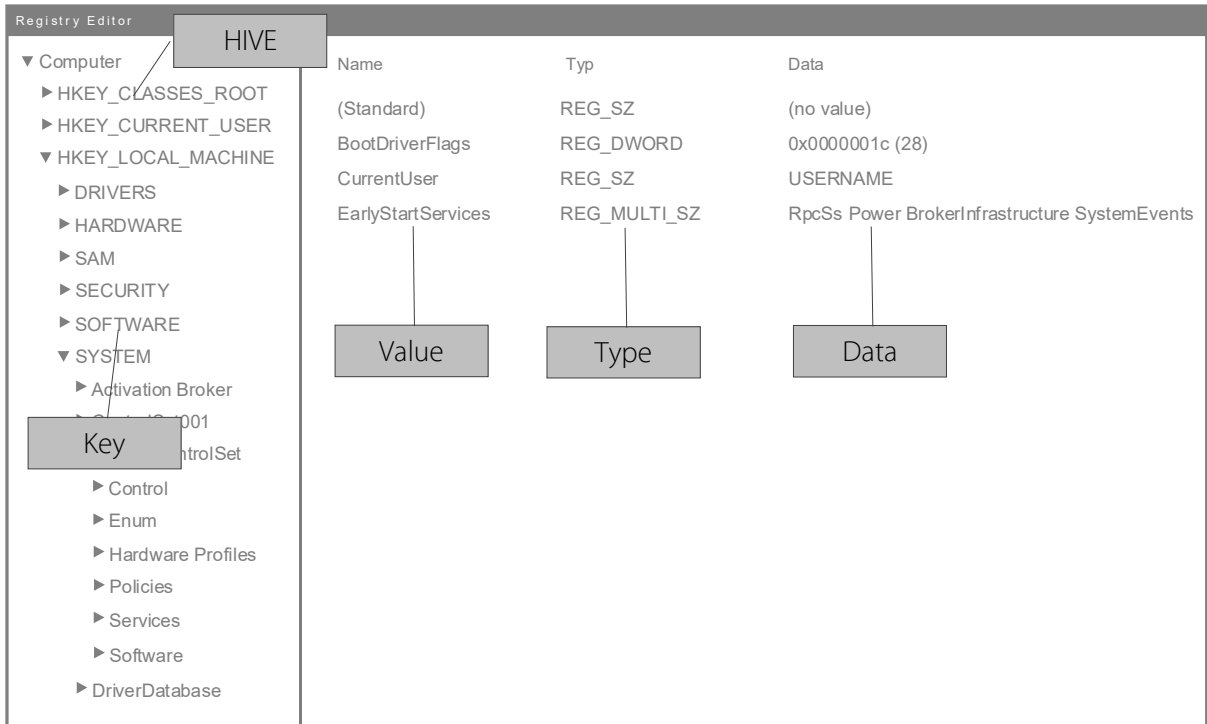
Click on 'Registry Security' in the main menu to open the Registry Security Monitor. The monitor displays all accesses in real time, as well as the respective security assessment and cleaning results of the activated vendors.



Registry Security -> Monitor

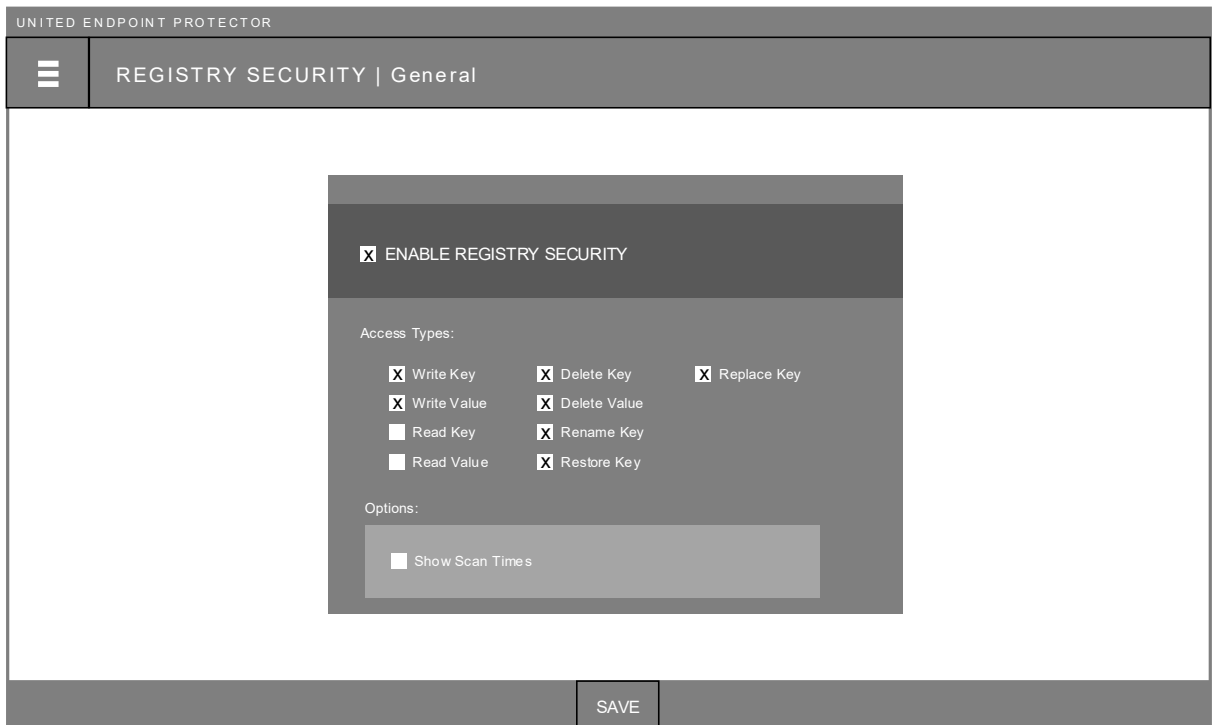
The user interface displays the last 10,000 accesses that you can search in real time using the filter bar. With the 'Export' icon, in the lower menu bar, you can export all recorded accesses to an XLS file. The 'Delete' icon, on the other hand, allows the manual deletion of all recorded data. An automatic deletion takes place by stopping the United Endpoint Protector service or at regular intervals if data is older than 24 hours.

For a better understanding of the presented Registry data, the following illustration explains the terms using the example of the Windows Registry Editor.



7.1. General settings

The functionality of the Registry Security can be defined via the General settings. Click on 'General' in the submenu of 'Registry Security' in the main menu.



Registry Security -> General

The following settings can be made on the configuration interface:

Enable Registry Security	Enables or disables the monitoring of Registry accesses.
Access Types	Defines the type of access to be monitored.
Show Scan Times	Displays in the Registry Security Monitor the time periods of the security vendors required to assess the accesses.

7.2. Strategy

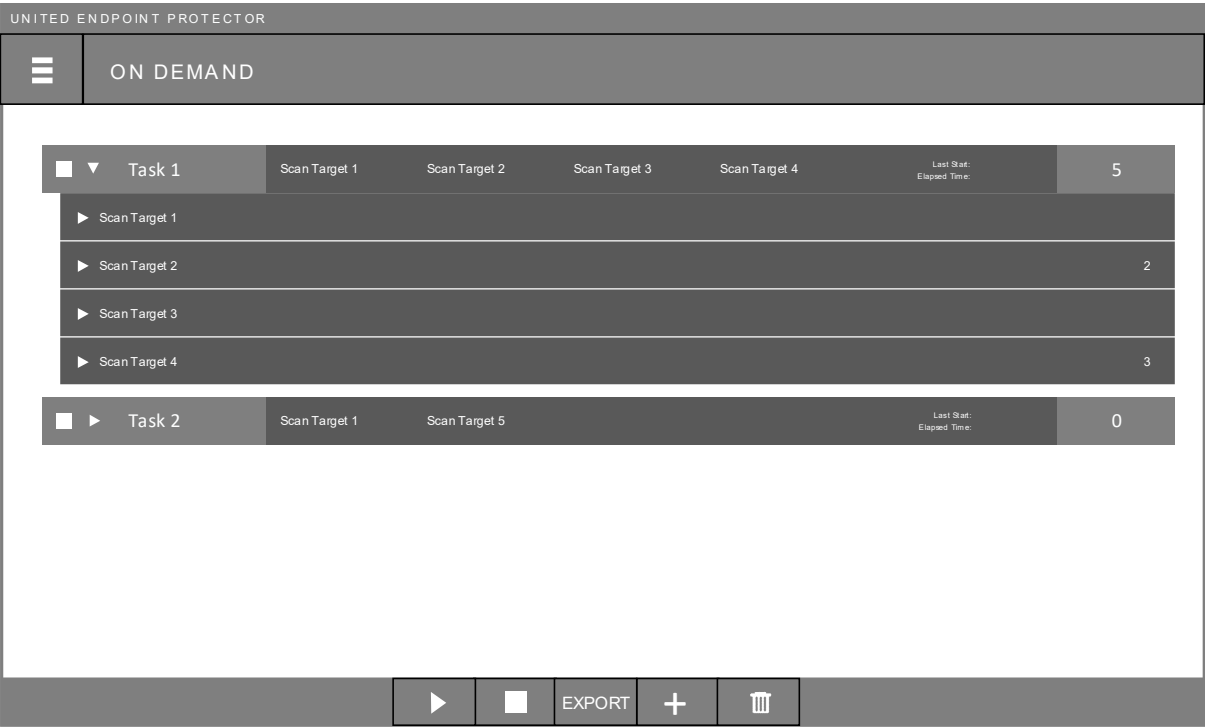
Monitoring Registry accesses can be an important tool for detecting and removing threats. For this, an important decision is to define the types of access to be monitored. Registry accesses occur in greater numbers than file accesses, and thus their validation requires more system resources. We therefore recommend restricting the monitoring to those accesses that make changes to the Registry and thus pose a potential threat. Other accesses, such as 'Read Key' or 'Read Value' can be monitored as needed, but with a noticeable effect on system performance.

The assessment of whether an access is malicious or not can be done by security vendors, if there are vendors available that support it. In any case, the Blacklist (see chapter 10) can be used to block specific accesses. One possible strategy may be the acquisition of known, malicious activities in order to realize manual protection. Another option is the establishment of a preventive protection. For example, changing the start page of a web browser could be restricted to certain processes (Blacklist blocks all accesses and allowed processes are set by exceptions).

8. On-Demand Scans

On-demand scans allow you to create scheduled investigations of different areas of the computer. These can be used to detect previously unseen threats and introduce another level of security.

In the main menu, click 'On Demand' to open the overview of the on-demand scans. This overview shows all created scan tasks. Each task displays the investigated scan targets, the number of detected threats, and the last execution information. With the help of the expander, the last or current scan result can be displayed in detail. A renewed execution of the scan task deletes the previous scan result.



On Demand -> Overview

Selecting a task via the corresponding check box makes various functions in the lower menu bar available. These can be used to manually start or stop tasks, to export the last scan result to an XLS file, or to delete a task.

8.1. Create scan task

To create a new scan task, click 'On Demand' in the main menu and on the Add icon in the bottom menu bar. This opens the configuration interface for a new task.

On Demand -> Scan Task -> General

To give the task a name and an optional description, the following scan targets can be selected on this configuration interface:

All Fixed Drives	Uses forensic methods to make all data visible on all local hard disks and to scan them with selected security vendors.
All Removable Media	Uses forensic methods to make all data on connected removable media (e.g. USB sticks, external hard disks) visible and scans them with selected security vendors.
Drivers	Uses forensic methods to make all device drivers registered in the system visible and scans them with selected security vendors.
Services	Uses forensic methods to make all Windows services registered in the system visible and scans them with selected security vendors.

Boot Sectors	Depending on the unlocked security vendors, it is possible to examine master and volume boot records. The respective vendor decides on the scope of the investigation.
Windows Registry	Compared to Registry Security, it is also possible, depending on available security vendors, to check the Windows Registry in time. The respective provider decides which parts of the Registry are to be examined.
Memory	Allows the same memory check as Memory Security, but with different scheduling options.
Specific Folders	Allows you to scan one or more specific folders with desired security vendors, based on forensic methods.

In addition to specifying the desired scan targets, the following schedule options allow you to set the time of scan:

Manually	There is no automatic execution of this task, but this can be started manually via 'On-Demand – Overview'.
Scan Interval	The task is repeated at the specified minute interval. If the last regular execution did not happen because the computer was down, for example, the delay determines when the next execution should take place.
Daily	The task is performed every day at the specified time (24-hour format)
Weekly	The task will run every week, at the specified days of the week, at the specified time (24-hour format).
Monthly	The task is run every month, on the specified days of the month, at the specified time (24-hour format).

In addition, the following options can be set to perform the task:

Maximum file size	Sets the maximum size of a file to be scanned by the security vendors. Any file greater than the specified value is ignored. In the case of the scan target 'Memory', this value also defines the maximum size of used memory of a process for extraction.
Resource usage	Allows you to specify the CPU load to use during a scan. It should be noted that the more the CPU is used, the faster the task is completed. The less the CPU is used, the longer the runtime of the task.
Stop scan after	Specifies the number of hours or minutes after which the task should automatically stop.
Run missed scan	Specifies whether a scan task that missed the regular execution time should be made up. The delay indicates the time when the next execution should take place.
Show Scan Times	Displays the time periods required to scan a file, in the detailed views of the scan targets, in the 'On-demand overview'.

8.2. Strategy

The main duty of on-demand scans is to create monitoring instances to detect unrecognized threats. Also, scan tasks can be used as a possible reaction to a detected threat (see chapter 11). The maximum benefit is achieved through the use of other or additional security vendors, which may not be used in other security features for some reason. Compared to File Security, the choice of vendors for an on-demand scan does not depend on the data throughput. Consequently, more time-consuming scan techniques can be used in this field of application.

We recommend the use of two different on-demand scans:

Hot-Spot Scan

This scan has the duty to check the most important areas of a computer, which are frequently used by malware. These include the scan targets 'Drivers', 'Services', 'Boot Sector' and 'Windows Registry'. Individual directories, such as the Windows folder, temp directories, or users' profile folders, might be eligible for this task too. Depending on the number of selected scan targets and which system resources are available on the computer system (CPU capacity, hard disk speed), this check should take place in a time interval of a few hours. The resource usage can be adapted to the circumstances in order to avoid negative effects for the end user.

Full Scan

This scan has the task of checking the local hard disks. The scan target 'All Fixed Drives' is suitable for this. The purpose of this check is to detect and remove malicious files that were not identified by File Security at the time of file access. Depending on the amount of data available, this check may take several hours. Therefore, a time should be chosen that is compatible with the IT operation. For servers, the weekend or night hours are usually suitable, whereas workstations must be checked at times when they are turned on. In this case, we recommend a low resource usage to avoid negative effects for the end user.

9. Technologies

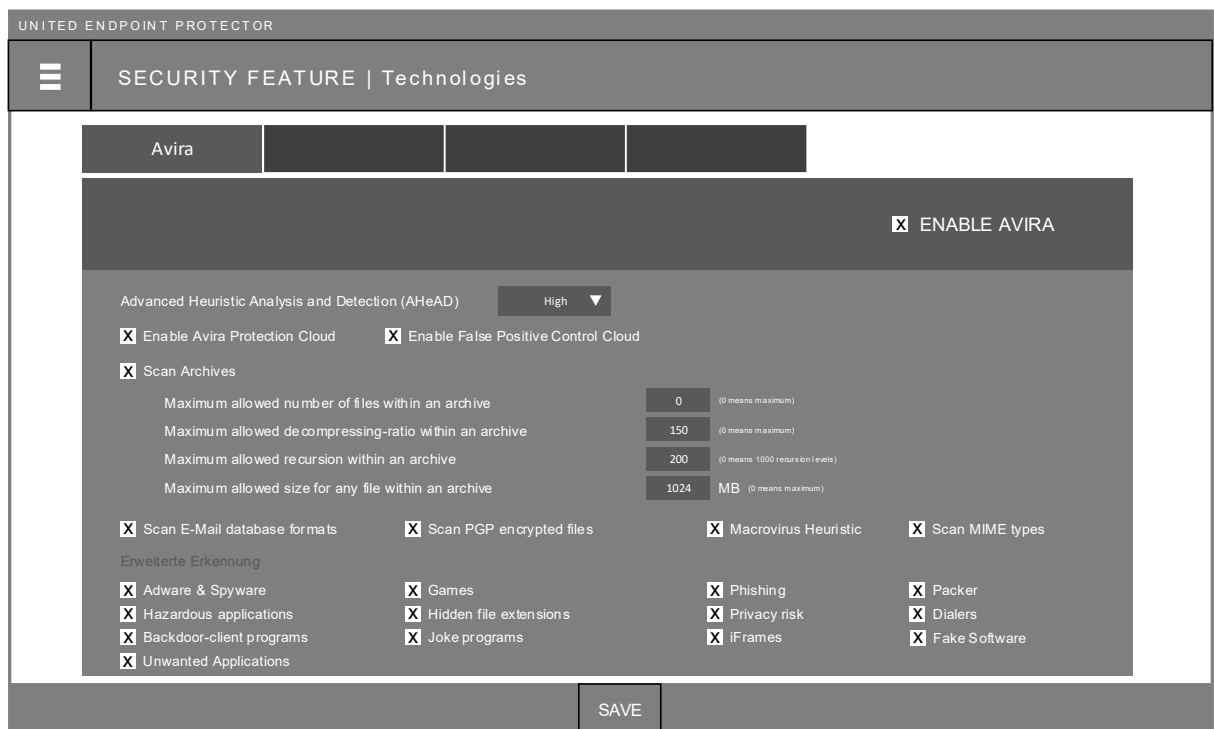
Depending on the unlocked security vendors (see chapter 3), the appropriate configuration interfaces for the technologies are available. With their help, you can set various settings for each vendor. For maximum flexibility, the interfaces are available in each security feature, to specify individual settings for the respective feature.

The surfaces are located in the respective submenu of the Security feature in the main menu. The most important setting is the activation of the various technologies. With this you can define - for each security feature - which security vendors, in which combinations, should check the respective data.

Below, we explain the settings options for the vendors available in the United Endpoint Protector (UEP).

9.1. Avira

The following configuration options are available for the Avira technology:



Technologies -> Avira

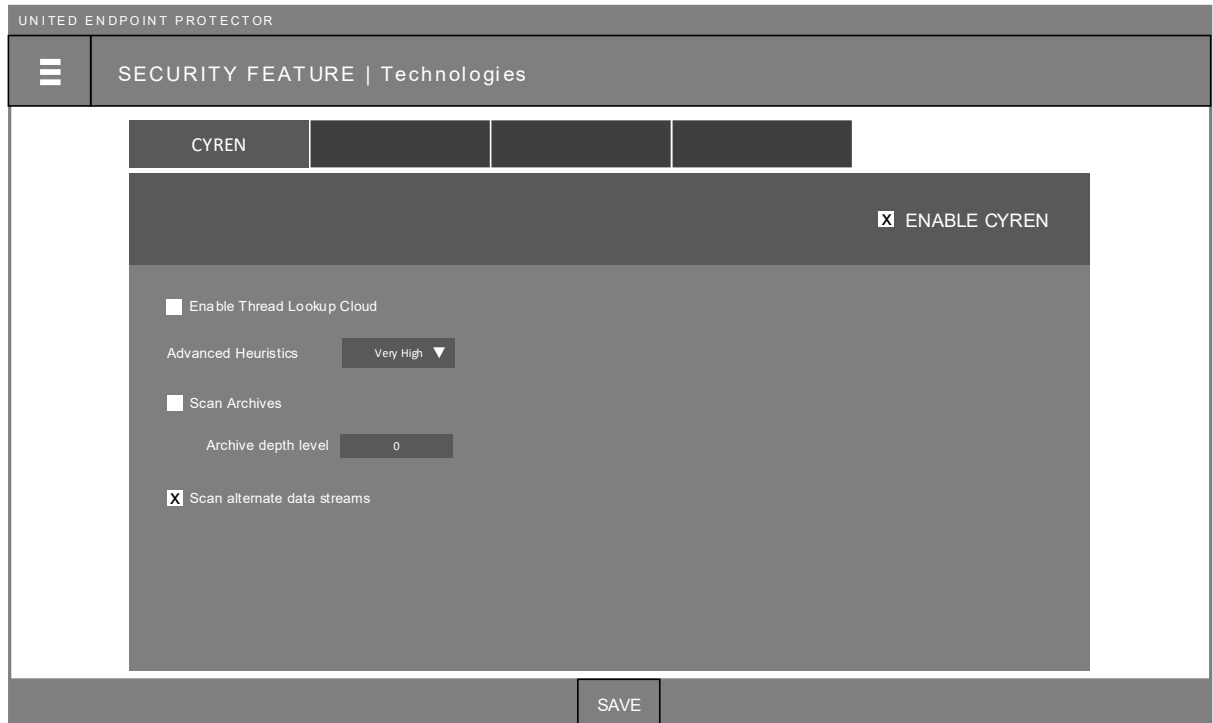
Enable Avira	Enables or disabled the data validation by Avira in the respective security feature.
--------------	--

Advanced Heuristic Analysis and Detection (AHeAD)	Enables or disables the heuristic threat detection and determines its sensitivity level.
Enable Avira Protection Cloud	Enables additional threat detection by the Avira Cloud. With this feature enabled, PE, non-PE, and other file types are additionally evaluated by the Cloud after a local review. For this, a HASH value of the file is calculated and transmitted to *.compute.amazonaws.com through port 443 and 80. If the HASH value is still unknown, the complete file is transferred for detailed analysis. If a proxy server is used for the Internet connection, you can enter it in the proxy settings (see chapter 4.2). Be sure to enable the 'Cloud connections' function in the proxy settings. The enabled use of the Cloud is symbolized in the head of the Avira column in the respective security feature by a Cloud icon.
Enable False Positive Control Cloud	Enables additional protection against false alarms (False-Positives) through the help of the Avira Cloud. If this feature is enabled and a threat has been detected during a local scan, the file's HASH value, along with other information (file name, threat name, file size, creation and modification date, etc.) will be sent to *.compute.amazonaws.com through port 443 and 80. This information is used in the Cloud to confirm the correct detection of the threat and straighten it in the event of a failure. If a proxy server is used for the Internet connection, you can enter it in the Proxy settings (see chapter 4.2). Be sure to enable the 'Cloud connections' function in the Proxy settings.
Scan Archives	Enables or disables scanning of archives, such as ZIP files, for contained malicious files.
Maximum allowed number of files within an archive	Defines the maximum number of files within an archive to be checked.
Maximum allowed decompressing-ratio within an archive	Sets the maximum decompression ratio within an archive to perform the check.
Maximum allowed recursion within an archive	Defines the maximum recursion depth within an archive to be checked.
Maximum allowed size for any file within an archive	Defines the maximum file size within an archive to be checked.

Scan E-mail database formats	Includes files in the investigation that have an email database format (e.g. EML).
Scan PGP encrypted files	Includes files in the investigation that are PGP encrypted.
Macrovirus Heuristic	Enables or disabled heuristic scans of Macros in Office documents.
Scan MIME types	Includes files in the investigation that have a MIME data type.
Advanced detection	Sets additional types of threats to be considered when evaluating files.

9.2. Cyren

The following configuration options are available for the Cyren technology:



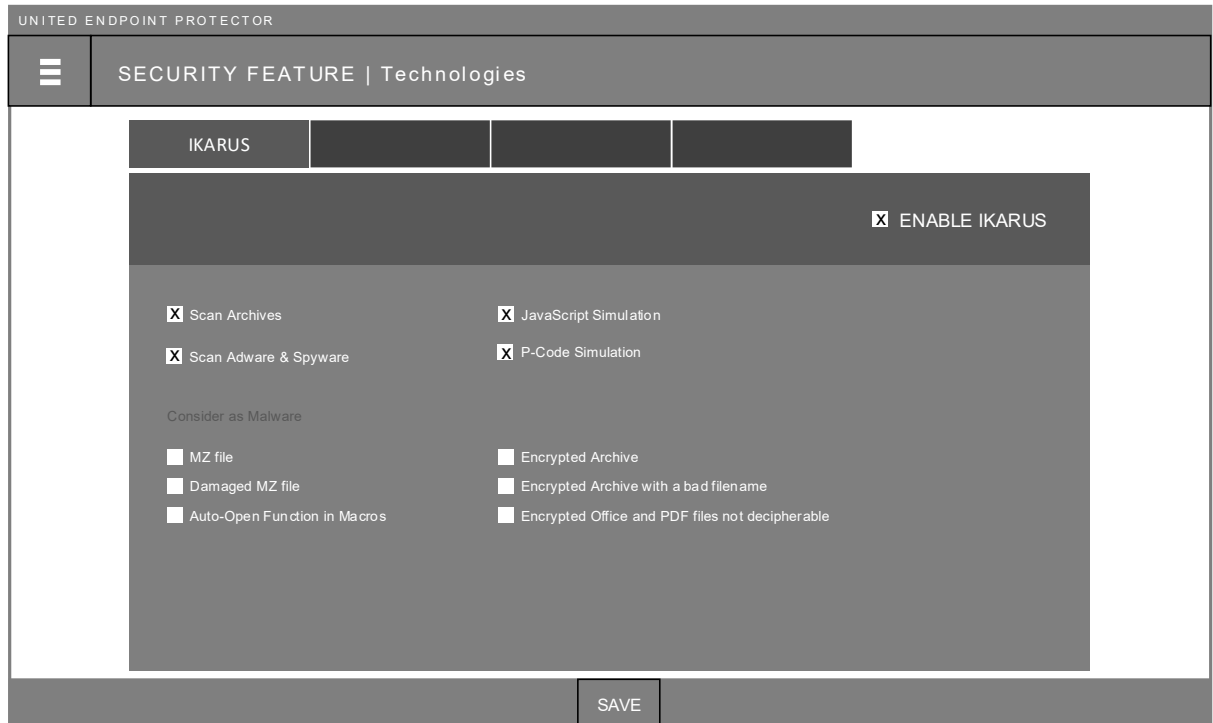
Technologies -> CYREN

ENABLE CYREN	Enables or disabled the data validation by Cyren in the respective security feature.
Enable Thread Lookup Cloud	Enables additional threat detection through the Cyren Thread Lookup Cloud. With this feature enabled, PE files are additionally evaluated by the Cloud after a local review. For this purpose, a HASH value of the file is calculated and transmitted to 84.39.152.194 through port 443 with additional information (signature version, engine version, triggered rule name, license ID). The enabled use of the Cloud is symbolized in the head of the Cyren column in the respective security feature by a Cloud icon.
Advanced Heuristic	Enables or disables the heuristic threat detection and determines its sensitivity level.
Scan Archives	Enables or disables scanning of archives, such as ZIP files, for contained malicious files.

Archive depth level	Sets the maximum number of archive levels to include in the scan.
Scan alternate data streams	Enables or disables the scan of alternative data streams from files.

9.3. IKARUS

The following configuration options are available for the IKARUS technology:



Technologies -> IKARUS

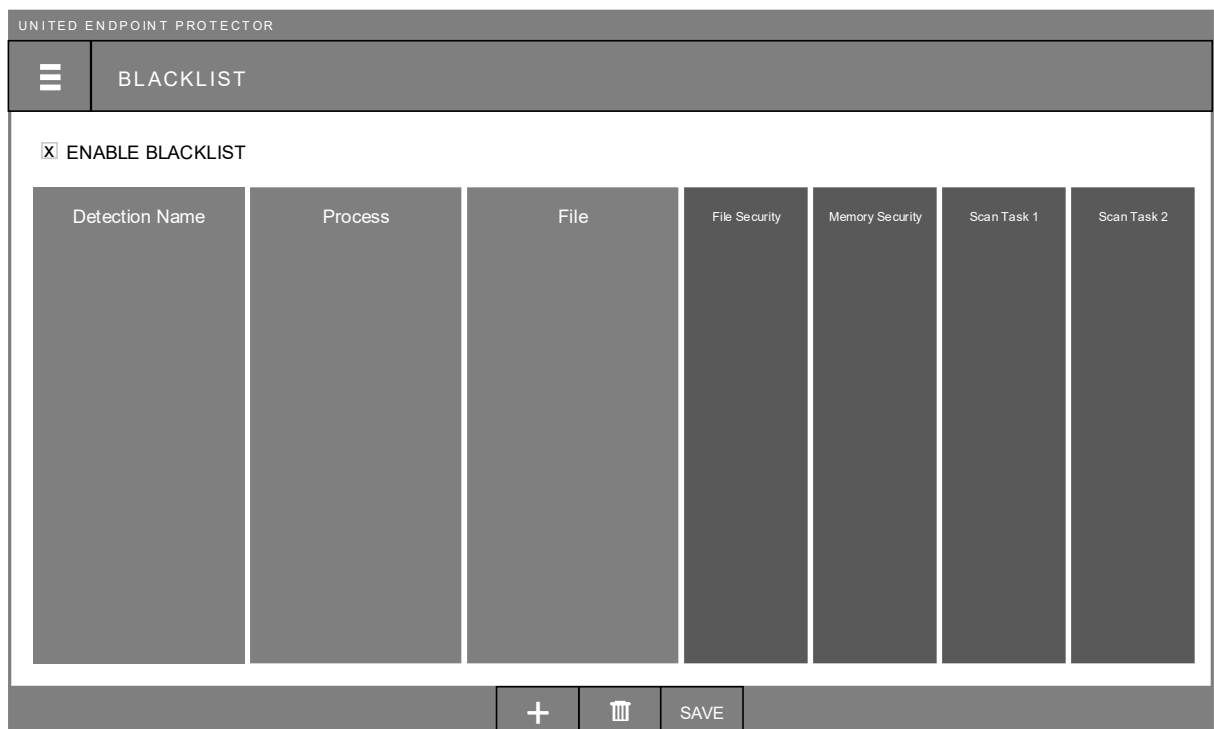
Enable IKARUS	Enables or disabled the data validation by IKARUS in the respective security feature.
Scan Archives	Enables or disables scanning of archives, such as ZIP files, for contained malicious files.
Scan Adware & Spyware	Enables or disables the Adware & Spyware threat category when evaluating files.
JavaScript Simulation	Enables or disables the virtual execution of Java Scripts to detect threats.
P-Code Simulation	Enables or disables the virtual execution of Pseudo-Machine code to detect threats.
Consider as Malware	Allows certain types of files to be considered as threats, regardless of their security status.

10. Blacklist

In addition to the use of professional security vendors, the Blacklist is available in all security features. This allows you to set manual detections. There are two different lists available in the United Endpoint Protector (UEP) where you can define files and accesses that should be treated malicious.

10.1. File-Blacklist

The File-Blacklist is a global list of entries for manual registration of file and process-based threats. This list can be found in the respective submenus of the security features 'File Security' and 'Memory Security' as well as on the configuration interface of on-demand scans (see chapter 8.1).



Security Feature -> Blacklist (Global)

The buttons in the lower menu bar can be used to add entries to the list, remove existing ones and save the changes made. In the upper area of the interface, the Blacklist can be activated for the respective security feature. This is represented in the overview of the security features in the same way as other technologies. In the case of an on-demand scan, the Blacklist activates automatically as soon as at least one entry has been activated for the scan task.

Each list entry can consist of the following information that is linked to a logical AND:

Detection Name	Any term for naming the threat. This term is displayed as a threat name in case of detection.
Process	A name or path to a process whose file access should be considered as malicious. This can be combined with a file entry, as well as described with the help of the wildcard *. In the case of 'Memory Security' this indication refers to a recognized main process.
File	A name or path to a file that should be considered as malicious. This can be combined with a process entry, as well as described with the help of the wildcard *. In the case of 'Memory Security' this indication refers to a file used by a main process.
Security Feature	By activating the respective check boxes, it is determined in which security feature the entry is to be recognized. 'File Security' and 'Memory Security' are always available. Additional columns may be available, depending on created scan tasks.

Sample entries:

Detection Name:	Malware 1	Any file accessed by the process 'C:\Program Data\dummy.exe' is considered as threat 'Malware 1'.
Process:	C:\Program Data\dummy.exe	
File:		

Detection Name:	Malware 2	Any file ending in 'encrypt' located in a 'tmp' folder will be considered as threat 'Malware 2'.
Process:		
File:	*\tmp*.encrypt	

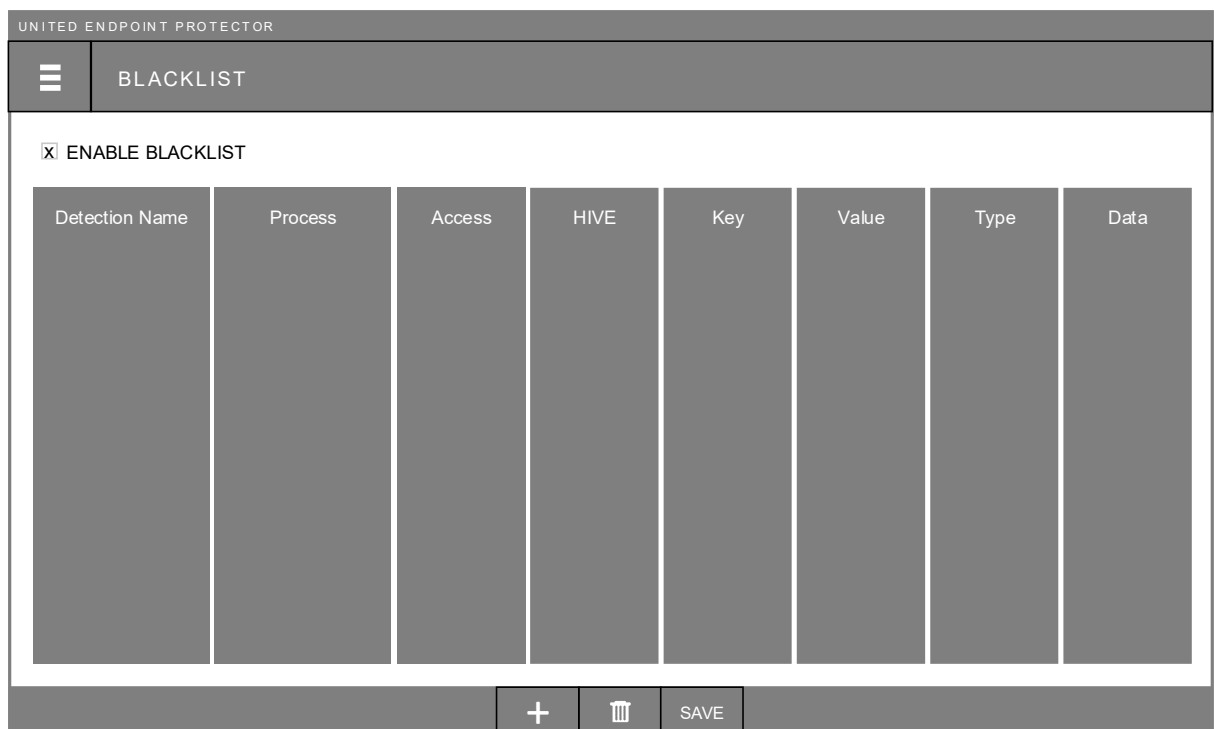
Detection Name:	Malware 3	Any file that begins with 'tmp' and is located in a subfolder of 'C:\Users\' and which is accessed by a process 'shh.exe', located in a subdirectory of 'C:\windows\', will be considered as threat 'Malware 3'.
Process:	C:\windows*\shh.exe	
File:	C:\Users*\tmp*.*	

CAUTION!

Incorrect entries, such as treating each EXE file as a threat, could cause damage to your computer system! We therefore recommend that you carefully and conscientiously deal with Blacklist entries and thoroughly test them prior to productive use.

10.2. Registry-Blacklist

The Registry-Blacklist is a special list for manual registration of malicious manipulations to the Windows Registry. This list can be found in the submenu of 'Registry Security' in the main menu.



Registry Security -> Blacklist (Registry Security)

The buttons in the lower menu bar can be used to add entries to the list, remove existing ones and save the changes made. With the checkbox 'Enable Blacklist' the Blacklist for the 'Registry Security' is activated and displayed in the Registry overview.

Each list entry can consist of the following information linked with a logical AND:

Detection Name	Any term for naming the threat. This term is displayed as a threat name in case of detection.
----------------	---

Process	A name or path to a process whose Registry access should be considered as malicious. This can be combined with all other information and described with the help of the wildcard *.
Access	Specifies the type of access to the Registry that should be considered as malicious.
HIVE	The name of the HIVE on which the access takes place. In addition to Microsoft's own HIVEs, Application HIVEs (/A) can also be specified. The use of the wildcard * is allowed.
Key	The name of the key being accessed and considered as malicious. The use of the wildcard * is allowed.
Value	The name of the value being accessed and considered as malicious. The use of the wildcard * is allowed.
Type	The type of value the access takes place on.
Data	The data of the value to be accessed and considered as malicious. The use of the wildcard * is allowed.

Sample entries:

Detection Name:	Malware abc	Any access of the process 'C:\Program Data\dummy.exe' is considered as threat 'Malware abc'.
Process:	C:\Program Data\dummy.exe	
Access:		
HIVE:		
Key:		
Value:		
Type:		
Data:		
Detection Name:	Malware xyz	Any access to a value 'Dummy' that is below HKEY_LOCAL_MACHINE\SYSTEM
Process:		

Access:		\CurrentControlSet will be considered as threat 'Malware xyz'.
HIVE:	HKEY_LOCAL_MACHINE	
Key:	SYSTEM\CurrentControlSet*	
Value:	Dummy	
Type:		
Data:		

Detection Name:	Tmp80	Any value that the process 'tmp80.exe' writes below HKEY_LOCAL_MACHINE\SOFTWARE\ is considered as threat 'Tmp80'.
Process:	*\tmp80.exe	
Access:	Write Value	
HIVE:	HKEY_LOCAL_MACHINE	
Key:	SOFTWARE*	
Value:		
Type:		
Data:		

CAUTION!

An incorrect entry, such as treating any access to a HIVE as a threat, could damage the computer system! We therefore recommend that you carefully and conscientiously deal with Blacklist entries and thoroughly test them prior to productive use.

10.3. Strategy

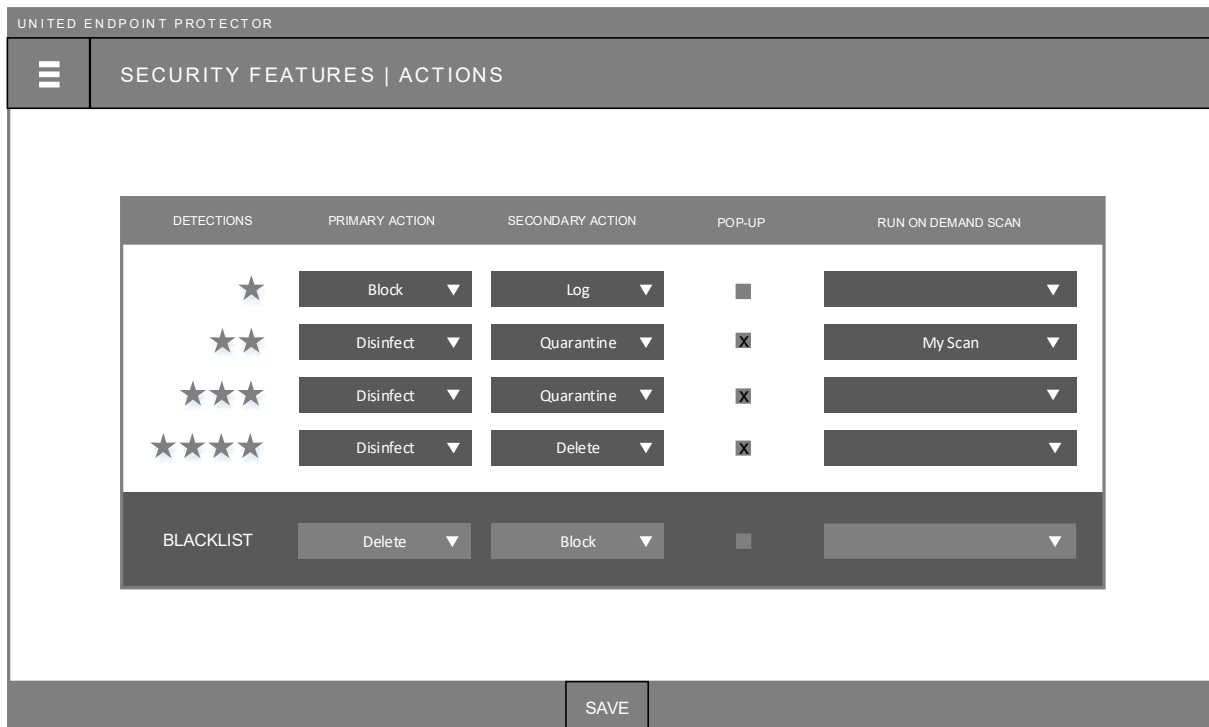
The Blacklist is a flexible tool that is mainly used for two duties. First, to manually combat threats that are not recognized by the used security technologies. Second, for the establishment of preventive protection measures to prevent unwanted activities in advance.

Signs, such as new files with suspicious filenames, running processes with suspicious labels, or unusual behavior of the computer system, may indicate a threat that was not recognized by the used security technologies. In this case, entries can be made on the Blacklist to treat these symptoms with a desired action. The information of the various security features can help to define matching Blacklist entries. In each security feature it can be determined whether the Blacklist should be active and with what action Blacklist detections should be dealt with (see chapter 11).

There are several scenarios in which the Blacklist can also be used to establish preventative protection measures. For example, if the change of the start page of a web browser should be prevented, attempts to modify the corresponding Registry value could be blocked by Blacklist entries. Also, the execution or installation of unwanted applications can be prevented or recorded with the Blacklist.

11. Actions

The United Endpoint Protector (UEP) is equipped with a number of possible actions to deal with identified threats. For each security feature, a separate configuration interface is available in the respective submenu of the main menu to determine the desired reactions.



Security Feature -> Actions

The actions to be taken will be set per matching security technologies. Depending on how many security vendors identify a threat, a primary and a secondary action can be performed automatically:

Log	Reports the detected threat, but does not perform any further cleanup steps.
Block	It is available in the real time features 'File Security' and 'Registry Security' and prevents the execution of the access.
Disinfect	Calls the cleaning method of the offering security vendor to remove the threat. If several vendors report the threat, the methods are started randomly one after the other. If the first vendor does not completely remove the threat, another provider may do so.

Quarantine	Moves the detected file to the quarantine of the UEP and isolates it there (see chapter 11.1).
Delete	Deletes the identified file. Note that no backup copy will be made!

The secondary action is called whenever the primary was unsuccessful. In addition, for each detected threat, it may be determined whether to open a notification window on the computer system. In response to an identified threat, an existing on-demand scan (see chapter 8) can be started automatically. In the case of a Blacklist detection, separate actions can be defined.

Within the security features, the scan and cleaning results are displayed in the respective columns of the security vendors. The following states can take place:

OK

The security vendor successfully scanned the access and classified it as clean.

The security vendor could not scan the access. Hovering over the entry will indicate the reason.

Threat Name

The security vendor detected a threat with the given access and was able to successfully neutralize it. Hovering over the entry will display the performed action.

Threat Name

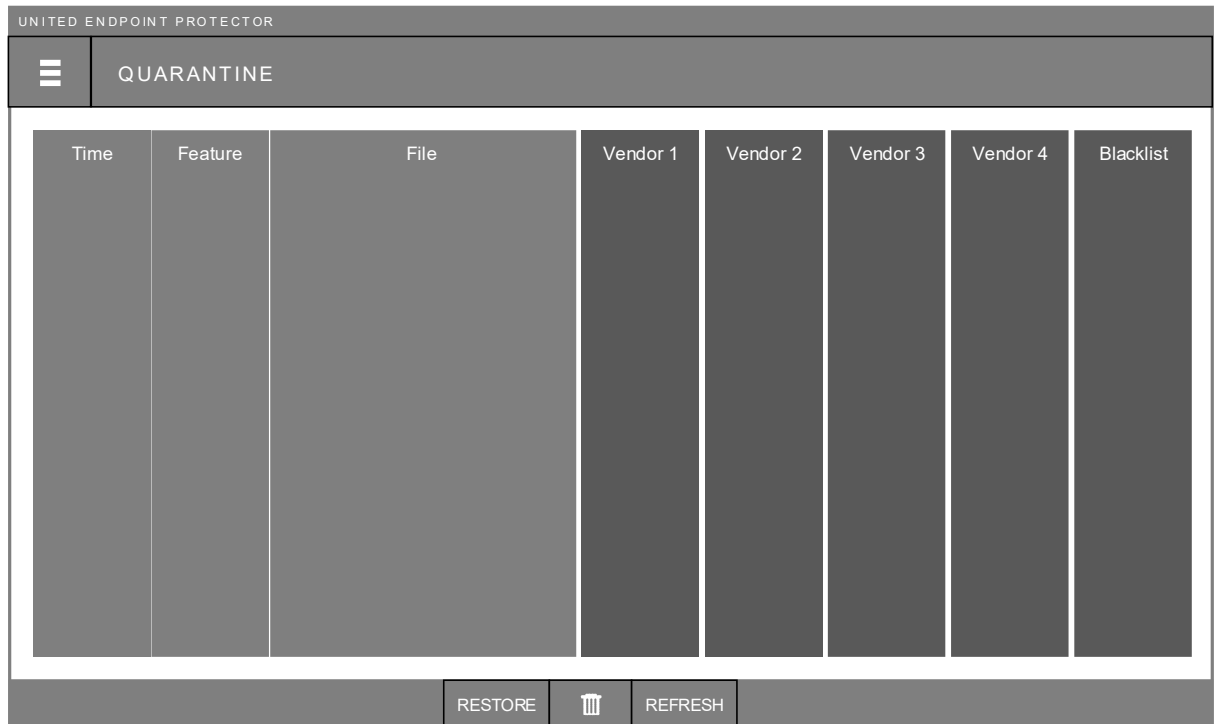
The security vendor detected a threat with the given access, but failed to neutralize it. This can be the case, for example, if the action 'Log' or 'Block' has been specified. Hovering over the entry will display the exact status.

Self Protection


Access to Tabidus' own components was detected, which was not allowed by an exception rule (see chapter 12). This can happen if the self-protection of UEP is active (see chapter 5.1).

11.1. Quarantine

When a threat is detected and the action 'Quarantine' is selected, the file is moved to UEP's quarantine directory (... \Tabidus Technology \United Endpoint Protector \quar \) and isolated there. The administration interface of the Quarantine can be accessed from the submenu of 'Status' in the main menu.



Time	Feature	File	Vendor 1	Vendor 2	Vendor 3	Vendor 4	Blacklist

RESTORE  REFRESH

Status -> Quarantine

The interface represents all objects that are in quarantine. For each object, the time of isolation, the responsible security feature, the original location, and the scan results of the security vendors are displayed. The lower menu bar can be used to restore existing objects to their original location or to permanently delete objects from the quarantine. The screen data can be updated with the 'Refresh' button.

11.2. Strategy

The most important decision in determining the automatic actions is a balance between a potential False-Negative (the non-treatment of a threat) and a False-Positive (the mistreatment of a threat). Both are possible side-effects that can occur when identifying threats. Depending on which scenario represents the greater danger in the respective environment and in the respective operational area, the actions should be selected appropriately.

For example, if you have a special computer system running special software that is critical to production and no user works freely on that device, a potential False-Positive may be the greater threat. In this case, if only a single vendor identifies a threat, the action 'Block' or 'Log' might be set. Negative effects of a false alarm would thus be avoided with high probability. However, if a real threat occurs, a notification may be displayed and manually removed, as judged. On the other hand, if two or more providers agree on the classification of a threat, an automatic 'Disinfect' or 'Quarantine' could be considered.

On the other hand, if it is a simple workstation that does not perform an extremely important function and if, for example, foreign data are often processed on it, a potential False-Negative is the greater danger. In this case, the detection of a single vendor may already be accompanied by the actions 'Disinfect' and 'Quarantine'. If even two or more vendors agree, a 'Delete' could be considered.

The choice of whether a notification window should be displayed, and at how many matching vendors, may depend on the nature of the user and whether or not they can do anything with the given information.

Automatically executing an on-demand scan, triggered by the detection of a first threat, is a great method for advanced protection. For example, if the File Security detects a malicious file, there could be a bad process in memory or a malicious Windows service installed at that time. Immediate review by a 'Hot-Spot Scan' or even the entire hard disk, could uncover other components of the threat, perhaps from other vendors or with more intensive investigation techniques.

12. Exclusions

Checking files and Registry accesses for potential threats can slow down the computer system in certain situations. The United Endpoint Protector (UEP) therefore makes it possible to exclude desired accesses from the scans in order to prevent negative effects on special events. There are two different lists for the exception of File and Registry accesses.

12.1. File-Exclusions

In the submenu of the security features 'File Security' and 'Memory Security', as well as on the configuration interface of on-demand scans, the global list for file exceptions can be called.



Security Feature -> Exclusions

With the lower menu bar, new entries can be added to the list, existing ones deleted and changes saved. Each entry describes a file, folder or specific access that should be excluded from the scan. Depending on each entry, the check boxes can be used to specify in which security feature the respective exception should apply. Besides 'File Security' and 'Memory Security', exceptions for the 'Self-Protection' (see chapter 5.1) can be set (processes that may access Tabidus' own components), and for each created on-demand scan.

Each entry can consist of the following information:

Comment	Any term to describe the exception. For example, the associated program or the reason for the exception may be mentioned.
Process	The name or a path to a process whose file accesses should not be scanned. The use of the wildcard * is allowed. A process definition can be combined with a file definition.
File	The path to a file or folder that should not be scanned. The use of the wildcard * is allowed. A file definition can be combined with a process definition.
Security Feature	Activation of the security feature for which the entry should apply.

12.2. Registry-Exclusions

In the submenu of 'Registry Security' the second list can be called, with which the registration of exceptions for Registry accesses is possible. This allows to specify processes whose accesses to the Windows Registry should not be monitored.



Registry Security -> Exclusions

Each entry can consist of the following information:

Comment	Any term to describe the exception. For example, the associated program or the reason for the exception may be mentioned.
Process	The name or a path to a process whose Registry accesses should not be monitored. The use of the wildcard * is allowed.

12.3. Strategy

Any exception to monitoring through a security feature is a potential security risk. The use of exclusion rules should therefore only be for important reasons. Possible reasons might be the impairment of a particular application or the heavy burden of a particular process leading to high CPU usage. Classic examples are the used backup system or special server applications such as database servers. These cause, by their operation, a large number of file accesses whose monitoring can have negative effects.

To minimize the potential security risk of an exception, it should be described as precisely as possible. Instead of a simple filename that allows ambiguity, a more detailed description of the location (path) is recommended. In principle, exclusions can occur in three different ways:

- **File & Folder exclusion**

Is an exclusion that only contains the path to a file or an entire folder that should not be monitored. This can be a temporary help, for example, in the case of a False-Positive. In other cases, this can fix a potential problem, but the large ambiguity (who else can access this file or folder?) makes this exclusion type the least secure and should be avoided. If such an exception is nevertheless necessary, it should be checked regularly by an on-demand scan.

- **Process exclusion**

Is an exclusion that only contains the path to a process. The start of the process is preceded by a 'read' access to the associated EXE file, which is not affected by the exception. However, any access that this process subsequently makes is excluded from the scan. This form of exception is more secure because the process is checked at startup and the identity of the traffic is known. However, since a supposedly benign process can be manipulated during execution or processing foreign data, no high-risk processes such as iexplore.exe, explorer.exe, svchost.exe or similar should be excluded.

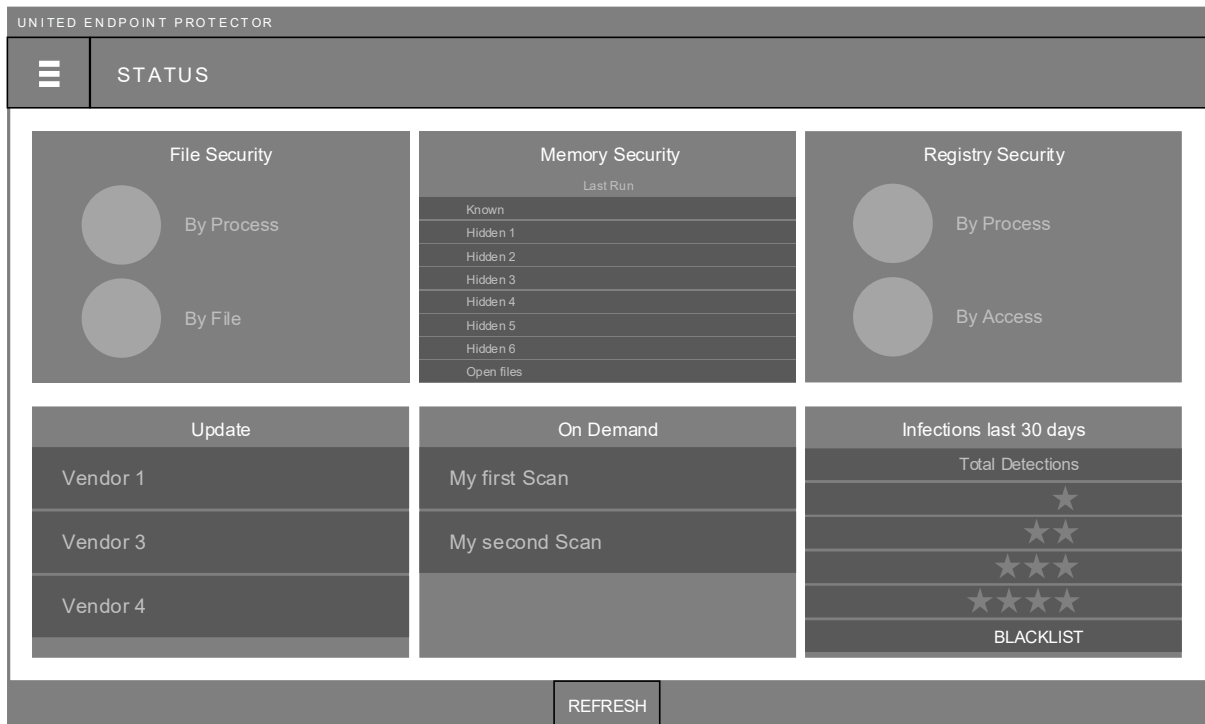
- **Process & File exclusion**

This is a combination of a Process and File & Folder exclusion. This is the most secure form of exception that allows least ambiguity. Exclusion from monitoring only occurs when a specified process accesses a specified file or folder. If the specified process accesses another destination or if another process accesses the specified file or folder, this is no longer affected by the exclusion.

The need to set exceptions may also refer to the operation of the 'Self-Protection' of the United Endpoint Protector (UEP) (see chapter 5.1). 'Self-Protection' blocks any access to Tabidus' own files, folders and processes to prevent potentially malicious manipulations of the UEP. However, if an operation requires access for good reason, it must be entered as an exception and activated for the 'Self-Protection' feature.

13. Dashboard

To monitor all important operating parameters and occurring events, the status dashboard is available. This can be called up in the main menu by clicking on 'Status'.



Status

The data of the dashboard can be updated with the 'Refresh' button in the lower menu bar. The following information can be found here:

- **File Security**
Displays all File Security audited traffic from the last 24 hours or since the last reboot. The data is sorted 'By Process' and 'By File'. The header area shows the number of infections that have occurred. Click on the respective heading to open the corresponding detail view to display all available data. This information can be used to make improvements to the File Security configuration (e.g. set exclusions – see chapter 12).
- **Memory Security**
Represents the Status of the Memory Security. In addition to the time of the last execution, the forensic methods passed through and the processes they detect in memory are displayed. The header area displays the number of detected infections.

- **Registry Security**

Displays all accesses monitored by the Registry Security in the last 24 hours or since the last restart. The data is sorted 'By Process' and 'By Access'. The header area shows the number of infections that have occurred. Click on the respective heading to open the corresponding detail view to display all available data. This information can be used to optimize the Registry Security configuration (e.g. set exclusions – see chapter 12).

- **Update**

Displays all unlocked security vendors (see chapter 3). For each vendor, automatic updates status is shown, which they receive through update tasks. The status is green if the last update occurred within the last 24 hours. Otherwise, this will be indicated by a red cross.

- **On Demand**

Displays all created scan tasks (see chapter 8). For each task, the time, as well as the number of detected threats, of the last execution is presented. Click on the task name to open the overview of the on-demand scans.

- **Infections last 30 days**

Shows all detected threats of the last 30 days. In addition to the total count, these are also presented by the number of matching security vendors who detected the threat. Clicking on an entry opens the corresponding detail view, which shows all available data.

14. Third party licenses

The United Endpoint Protector (UEP) uses the following open source components to perform various tasks, in addition to the integrated security vendors. These are available via the following licenses.

14.1. Rekall Forensic

Rekall Forensics is available in the form of the uepmanalyser.exe in the UEP and provides forensic data of the memory for further processing. The source code can be viewed via the following link:

<https://github.com/google/rekall>

Copyright (C) 2007-2011 Volatile Systems Copyright 2012-2016 Google Inc. All Rights Reserved.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

14.2. WinPmem

WinPmem is a kernel-mode driver used by Rekall Forensics to gain access to the computer's memory. The source code can be viewed via the following link:

<https://github.com/google/rekall/tree/master/tools/windows/winpmem>

WinPmem is available through the Apache License Version 2.0, whose license agreement can be found at the following link: <https://github.com/google/rekall/blob/master/tools/windows/winpmem/LICENSE>

14.3. The Sleuth Kit

The on-demand scans of the UEP use single libraries of the Sleuth Kit for forensic examination of data carriers. The source code can be found via the following link: <http://www.sleuthkit.org/sleuthkit/download.php>

The source code in TSK are distributed under several licenses. Each source code file identifies the license that applies to its contents.

Some of the files in TSK core (non-framework) have roots in The Coroner's Toolkit (TCT) and are distributed under the [IBM Public License](#). These files are limited to the file system code and mainly for the FFS and Ext2 file systems. Files that have been created since the fork are released under the [Common Public License](#). This includes all other files in the library. Note that the Common Public License is a generic form of the IBM Public License.

The framework code is distributed under the [Common Public License](#).