Dr.WEB

FixIt!

User manual

Trademarks

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for any errors or omissions, or for any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, or by the use of or inability to use the information contained in

Dr.Web FixIt!
Version 2.4
User manual
1/16/2025

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

We thank all our customers for their support and devotion to Dr.Web products!

Table of Contents

1. Conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
⚠	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

2. About Product

Dr.Web FixIt! is a service that analyzes the security of computers running Microsoft Windows operating systems. It allows information security experts to perform a detailed analysis of the state of computers, remove detected threats, and overcome potential vulnerabilities.

Dr.Web FixIt! is operable through a web interface, which means you do not need to install it. You can analyze files and eliminate threats even if you have third-party anti-virus products installed on the computer you are checking.

Parameters of Dr.Web FixIt! are easily adjustable, which makes it efficient in the following scenarios:

- Analyze computers cured from a known infection.
- Analyze computers with suspected malicious activity.
- Investigate traces of malicious activity after infection.
- Check and analyze an IT system for vulnerabilities.
- Restore a computer after malicious attacks.
- Collect data to investigate targeted attacks on IT systems.

To analyze and cure your device, the service generates a customized FixIt! tool based on the parameters set by you.

You can use **Help** to learn more about the service. To open Help, click ? in the top right corner.

How Dr.Web FixIt! works

1. You create a task in the service, generate a FixIt! tool, and send it to a user whose computer needs to be scanned.
2. The user runs FixIt! tool. It scans the computer and generates a report.
3. You analyze the report in the service, create a curing FixIt! tool, and send it to the user.
4. The user runs the tool, which executes the curing script and generates a new report.
5. Repeat steps 3 and 4 until all of the threats on the client machine are eliminated. Then you can close the task.

Tasks are organized into spaces. Spaces are groups of users and managers that belong within a certain structure, such as an organization or a department. Users can create their own tasks and view other tasks within their space.

User accounts are managed by managers of the respective space.

Spaces are managed by administrators. Administrators have access to all tasks, spaces, and accounts of the service.

3. System Requirements

In order for Dr.Web FixIt! to work properly, you need a computer that meets the following system requirements:

Parameter	Requirements
Browser	One of: • Google Chrome 56.0 or later • Mozilla Firefox 45.0 or later • Safari 11.0 or later • Microsoft Edge 44.0 or later • any version of Microsoft Edge Chromium
Screen resolution	At least 1024x768

In order for a FixIt! tool to work properly, you need a computer that meets the following system requirements:

Parameter	Requirements
Operating system	For 32-bit platforms: • Windows XP with Service Pack 2 or later • Windows XP with Service Pack 2 or later • Windows Server 2003 with Service Pack 1 • Windows Server 2008 with Service Pack 2 or later • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 For 64-bit platforms: • Windows Server 2008 with Service Pack 2 or later • Windows Server 2008 R2 with Service Pack 1 or later • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Vista • Windows 7 • Windows 8

	- Windows 8.1 - Windows 10 - Windows 11
Free disk space	1 GB and more
RAM	256 MB and more

4. Getting Started

To start using Dr.Web FixIt!, you need to purchase a license and log in to the FixIt! service.

You can purchase the Dr.Web FixIt! license on the Doctor Web website.

4.1. Authorization

To sign in, enter your user name and password as credentials. Those should be provided by the person who registered your account in the service.

To sign in

1. Open the Dr.Web FixIt! log-in page.
2. Enter the user name and password.
3. Select the **Remember me** check box if you want to save the log-in credentials.
4. Click **Sign in**.

> ⚠ One hour of inactivity will end your session if you didn’t select the **Remember me** check box on the main page of the web service, redirecting you to the login page with a warning in the lower left corner.

4.2. Profile

The **Profile** menu is located in the top right corner of the Dr.Web FixIt! web interface.

The following options are available by clicking the **Profile** menu:

- **Settings:** allows you to set the interface language and reset your current password (if this option is available for your account type).
- **Sign out:** allows you to log out of your profile.

To change interface language

1. Click the **Language** drop-down list to pick the language you need.
2. Click **Save**.

To change your password

3. Enter your current password and then the new one twice.
4. Click **Save**.

Depending on the account type, resetting the password may not be available.

5. Accounts

There are three types of accounts (roles) in Dr.Web FixIt!: administrator, manager, and user. Availability of some of the functions offered by Dr.Web FixIt! depends on the type of account.

The table below details the actions users can perform based on their role.

Actions	Administrator	Manager	User	Notes
Spaces				
Create spaces	yes	no	no	
Edit spaces	yes	no	no	
Block and open spaces	yes	no	no	
Set a task limit for a space	yes	no	no	
Set an expiration period for tasks within a space	yes	no	no	
Add related spaces	yes	no	no	
View a list of related spaces	yes	no	no	Managers and users are unable to view a list of related spaces, but are able to share tasks with spaces from this list.
Accounts				
Delete accounts	yes	yes	no	An administrator can create other administrators, managers, and users. A manager can only delete managers and users within their space.
Delete accounts	yes	yes	no	An administrator can delete other

Actions	Administrator	Manager	User	Notes
				administrators, managers, and users. A manager can only delete managers and users within their space.
Change an account type	yes	yes	no	
Reset an account password	yes	yes	no	An administrator can reset passwords of other administrator, manager, and user accounts. A manager can only reset passwords of managers and users within their space.
Block and activate an account	yes	yes	no	An administrator can block or activate other administrators, managers, and users. A manager can only block or activate managers and users within their space.
Tasks				
Create tasks	yes	yes	yes	
Rename tasks	yes	yes	yes	
Close tasks	yes	yes	yes	
Reopen tasks	yes	yes	yes	
Delete tasks	yes	yes	no	

Actions	Administrator	Manager	User	Notes
Share tasks with related spaces	yes	yes	yes	
Request expert support for tasks	yes	yes	yes	
Filters				
Create new filters	yes	yes	yes	Administrators can create the **All users**, **Task**, or **Only me** filters. Managers and users can create the **Space**, **Task**, or **Only me** filters. The **For space** filters are only visible for managers and users of this space. The **Only me** filters are only visible to the users who created them (it could be an administrator, manager, or user).
Change filter availability	yes	yes	yes	Managers and users cannot changes the **For all** filters.
Change filters	yes	yes	yes	Managers and users cannot changes the **For all** filters.
Add filters to groups	yes	yes	yes	Managers and users cannot changes the **For all** filters.
Delete filters	yes	yes	yes	Managers and users cannot delete the **For everyone** filters.

Actions	Administrator	Manager	User	Notes
Reports				
Rename reports	yes	yes	yes	
Delete reports	yes	yes	no	
Widgets				
Create new widgets	yes	yes	yes	Administrators can create the **All users**, **Task**, or **Only me** widgets. Managers and users can create the **Space**, **Task**, or **Only me** widgets.
Enable or disable widgets	yes	yes	yes	
Edit widgets	yes	yes	yes	
Delete widgets	yes	yes	yes	

5.1. Administrator

Administrators have access to all spaces, tasks, and accounts of the service. Administrators can:

- manage spaces:
  - create new spaces,
  - edit spaces,
  - block and open spaces,
  - set task limits for spaces,
  - set an expiration period for tasks within spaces,
  - add related spaces to share tasks with them,
  - view lists of related spaces;
- manage accounts:
  - create new administrators,
  - create new manager and user accounts within their spaces,
  - delete administrator, manager, and user accounts,
  - change account types within spaces,
  - reset passwords to administrator, manager, and user accounts,

  - block and activate administrator, manager, and user accounts;
- edit tasks:
  - reopen tasks,
  - rename tasks,
  - close tasks,
  - delete tasks,
  - share tasks,
  - request expert support for tasks;
- edit filters:
  - create new filters,
  - change availability of any filter,
  - add any filter to group,
  - delete any filter;
- rename and delete reports.

5.2. Manager

A manager can view tasks and accounts of the space they belong to. Managers can:

- manage accounts within their space:
  - create new manager and user accounts within their spaces,
  - delete accounts,
  - change user name or email address of an account,
  - change account types within spaces,
  - reset passwords to accounts,
  - block and activate accounts within their space;
- edit tasks within their space:
  - reopen tasks,
  - rename tasks,
  - close tasks,
  - delete tasks,
  - share tasks with related spaces added by an administrator,
  - request expert support for tasks;
- edit filters within their space:
  - create new filters,
  - delete filters,
  - change filters,

  - add filters to groups.

5.3. User

A user has access to tasks of their space. A user can:

- reset a password to their account;
- edit their tasks:
  - create tasks,
  - rename tasks,
  - close tasks,
  - share tasks with related spaces added by an administrator,
  - request expert support for tasks;
- edit filters within their space:
  - add filters,
  - delete filters,
  - change filters,
  - add filters to groups.

6. Managing Spaces

Administrators can access all spaces in the service. They can:

- View a list of all spaces
- Create spaces
- Edit spaces
- Block or reopen spaces
- Add related spaces

6.1. How to View a Space List

You can find a complete list of spaces in the **Spaces** tab on the **Management** page.

To access this tab, click **Management** on the top FixIt! panel.

The table on this tab provides the following information for each space:

- **Space:** a space name.
- **Status:** Active or Blocked.
- **Tasks used:** the number of tasks used in this space. When there is no set limit, the value shown is **Unlimited**.
- **Members:** the total number of managers and users in this space.
- **Last modified:** the date and time of the last update to this space.

You can reorder rows of the space table by the contents of a column. To do this, click the column header. To reverse the direction of your sort, click the same header again.

To view detailed information about a specific space, click its name in the space table.

6.2. How to Create a Space

Administrators can create spaces and add members (managers or users) to these spaces.

To create a space

1. Click + above the table.
2. In the **New space** pop-up window, enter the name of the new space in the **Name** field.
3. If needed, you can also set a limit on the number of tasks for this space and specify their duration. To do this, select the check boxes and fill in the corresponding fields next to them.
4. Click **Save**.

6.3. How to Edit a Space

You can edit a space name, a limit on the number of tasks for a space and the task duration, as well as a member list.

To edit a space name, a limit on the number of tasks and the task duration

1. On the far right of the space row, click ✎.
2. Make the changes.
3. Click **Save**.

To edit a member list

1. In the space table, click a space name.
2. Create a new member account or delete an existing one.

6.4. How to Block or Reopen a Space

How to block a space

You can block a space if the partnership with its members has ended. If a space is blocked, space members will not be able to work there. Upon logging in, they will see a message stating that their space is blocked.

To block a space

- Via the space table

  1. On the far right of the space row, click 🔒.
  2. Click **Block**.

- On a specific space page

  1. In the space table, click a space name.
  2. In the top-right corner of the space page, click ··· > **Block space**.
  3. Click **Block**.

How to reopen a space

You can reopen the space that was blocked earlier.

To reopen a space

- Via the space table: On the far right of the space row, click 🔓.
- On a specific space page
  1. In the space table, click a space name.
  2. In the top-right corner of the space page, click ··· > **Open space**.

6.5. How to Search Across Spaces

You can search for the space table contents. For your convenience, the search starts as you type.

To search across the space table

1. Enter your query into the 🔍 **Search** field above the table.
2. Left-click outside the search field or press the ENTER key to lock the query.

> ⚠ Search and filtration are performed on the data currently displayed in the table. Therefore, if you set a filter or search across the table, the following search or filtration operation will be applied to the results of the previous one.

6.6. How to Filter Spaces

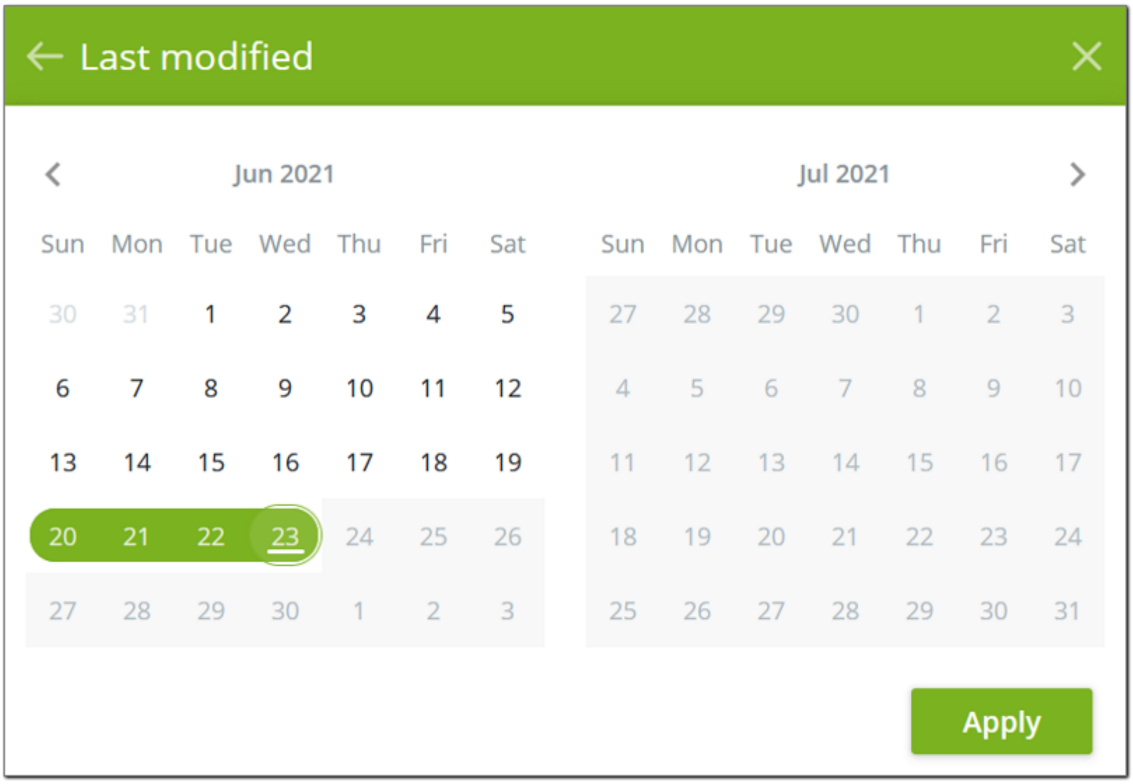
For your convenience, you can filter the space table contents by space name, status, or last change date.

To set a filter for the space table

1. Click ▽ above the table.
2. Select the parameter to filter the data by.
3. If it is **Name** or **Status**:
   - Select the check boxes next to the values you want and click **Add**.

   If it is **Last modified**:

- Select the date you need. To set a time period, click the start date and drag the cursor to the end date. Then click **Apply**.



Last modified

Jun 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

Jul 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Figure 1. Filtering by time period

In the **Filter** pop-up window, you can select only one parameter at a time. To filter the space table by multiple parameters, set multiple filters one by one.

> Search and filtration are performed on the data currently displayed in the table. Therefore, if you set a filter or search across the table, the following search or filtration operation will be applied to the results of the previous one.

7. Managing Administrators

The **Administrators** tab contains the full table of all administrators. For each administrator, the following information is available in the table:

- **Name**;
- **Email**;
- **Status**: Active or Blocked;
- **Tasks (open/closed)**: the number of tasks opened and closed by the administrator;
- **Date created**.

You can sort the table data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by.

Filter and search

You can filter the full table of administrators and search across the table data.

You can filter the table by the following parameters of the administrator account:

- name,
- email,
- status,
- date created.

To set a filter for the administrator table

1. Click ⏚ above the table.
2. Select the parameter to filter the data by.
3. If it is **Name**, **Email** or **Status**:
   - Select the check boxes next to the values you want and click **Add**.

   If it is **Date created**:
   - Select the dates of interest. To set a time period, click the start date and drag the cursor to the end date. Then click **Apply**.

You can select only one parameter per filter. Set multiple filters to filter the table by multiple parameters simultaneously.

To search across the administrator table

1. Enter your query into the 🔍 **Search** field above the table. Search is executed dynamically as you type.

2. Left-click outside the search field or press the ENTER key to lock the query.

The search and filtration operations are performed on the data currently displayed in the table. If you set a filter or search across the table, the following search or filtration operation will be applied to the results of the previous one.

Managing administrator accounts

The 👤 **Administrators** tab also allows you to manage administrator accounts: create a new account, edit or delete an existing one.

To create a new administrator account

1. In the top-right corner of the page, select 👥 **Management**.
2. Go to the 👤 **Administrators** tab.
3. Click ⊕.
4. In the **New administrator** pop-up window, enter a name, email address, and password.
5. Click **Create**.

You can change the details of any administrator account: name, email address, or status. You can also set a new password for an administrator account.

To edit an administrator account

1. In the right part of the row you want to edit, click ✎.
2. Change the values you need to change in the **Administrator information** pop-up window.
3. Click **Save**.

This pop-up window also allows you to block the administrator. The blocked administrator will be unable to continue using the service. Only an administrator can activate a blocked administrator account.

To block or activate an administrator account, use the **Status** toggle in the edit window.

You can also delete an administrator account if the administrator no longer uses the service. You will not be able to restore a deleted account.

To delete an administrator account

1. In the right part of the row you want to delete, click 🗑.
2. Click **Delete**.

> ⚠ Deleting an administrator does not delete tasks and spaces created by the administrator.

8. Dr.Web Settings

The **Dr.Web Settings** tab can be found on the top pane. This section allows you to add, view, and edit the default preferences of a Doctor Web product installed on the computer. This section is only visible to administrators.

The data in this section is organized in a table with the following columns.

- **Setting**: name of the setting, defined by the administrator;
- **Version**: the product version;
- **Key**: Windows registry key associated with this setting;
- **Value name**: Windows registry value name;
- **Value data**: Windows registry value data;
- **Description**: information about this setting.

> ⚠ The administrator manually adds settings by entering all the required data into the pop-up window.

To add a setting

1. Click + on the top of the page.
2. In the **Add setting** pop up, enter all the information about the setting.
3. Click **Save**.

> ⚠ The **Save** button will become active once you fill in all required fields. All fields are mandatory except for the **Description**.

To edit a setting

1. In the right part of the setting row you want to edit, click ✎.
2. In the **Edit setting** pop up, enter new data.
3. Click **Save**.

To delete a setting

1. In the right part of the setting row you want to delete, click 🗑.
2. In the **Uninstall settings** window, click **Delete**.

9. Filters

The **Filters** section in the top right corner of the screen allows you to create and edit filters used for data search in the report (see Search and Analyze). Filters facilitate data analysis by displaying only relevant information. The **Filters** section allows you to view, create, and edit filters and filter groups outside the report data analysis.

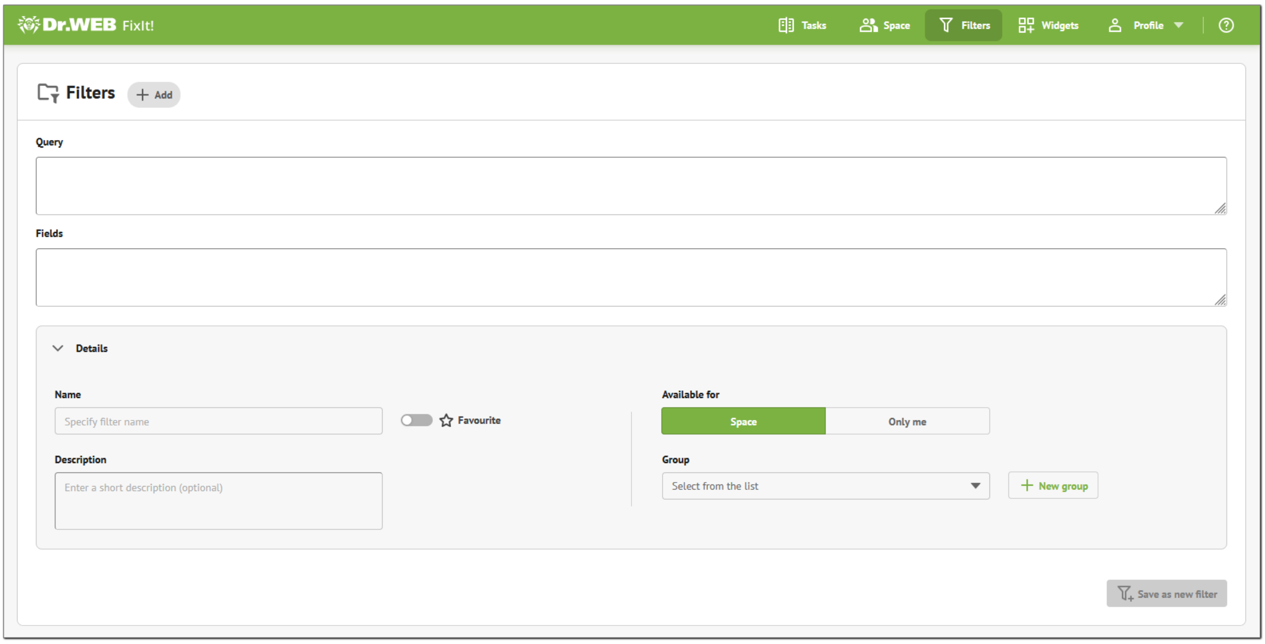


Figure 2. Filters

Administrators can create, edit, or remove any filters, including the preinstalled ones. Managers and users can create, edit, or remove filters created in the space to which they belong.

A filter consists of:

- **A query**, which is used for searching across data. A query consists of arguments (that is, categories of objects you are searching for) and their values (that is, parameters of objects that belong to categories).
- **Fields**, which define what data is displayed in the search results. One filter can include multiple fields, separated by commas.

Read more on queries and fields in the Making Queries section.

You can make a filter visible to other service users or only to you. The following access options are available:

- **All users**—this option is available only for administrators. The filter will be visible to all service members.
- **This space**—the option is available only for managers and users. The filter will be visible to all space members.

- **Only me**—option available for all service members. The filter will be visible only to the member who created it.

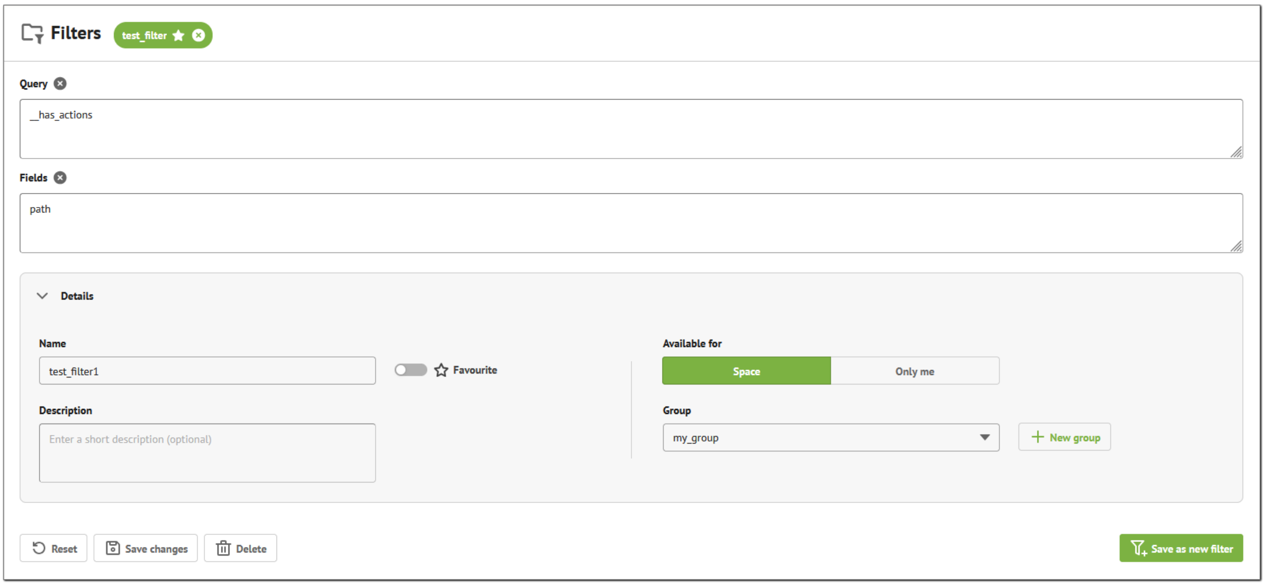
To create a filter

1. Fill in **Query** and **Fields**.
2. On the **Details** panel, fill in the **Name** and **Description** fields.
3. (Optional) Add the filter to Favorites by enabling **Favourite** toggle.
4. In the **Available for** field, select who will see the filter.
5. Select a group or create a new one by clicking **New group**.
6. Click **Save as new filter**.

> Administrators can hide data listed in the **Query** field by using the **Hide query** toggle button.

To edit a filter

1. At the top of the **Filters** tab, click **Add** and select a filter you want to edit.
2. Edit the values (see Figure 3).
3. If needed, change filter availability in the **Available for** field.
4. Select a group or create a new one by clicking **New group**.
5. Click **Save changes** to save changes. To create a new filter, click **Save as new filter**.



Query: __has_actions

Fields: path

Name: test_filter1

Description: Enter a short description (optional)

Available for: [✓ Space] Only me

Group: my_group

Figure 3. Filter editing

To delete a filter

1. At the top of the **Filters** tab, click **Add** and select a filter you want to delete.

2. Click 🗑 **Delete**.
3. Confirm the action in the **Delete filter** pop-up window.

If a filter was created, edited, or deleted successfully, a notification will appear in the bottom left corner of the screen. You can cancel filter deletion by clicking the **Undo** button in the notification.

Filter groups

You can sort the created filters into groups. If you did not select a group when creating a filter, it will be automatically saved to **No group**. A new group can be created only when editing a filter on the **Filters** tab or when creating a filter on the **Filters** or **Search and Analyze** tabs.

10. Space

A space is a group of managers and users.

Managers manage tasks and user and manager accounts within a space. Users can create and work on tasks as well as view other users' tasks within a space. Managers and users can access only their space. Only an administrator can create a new space.

Spaces can be related to other spaces. Members of such spaces can mutually share tasks and work on them together. Only administrators can add related spaces.

Managers and users can view the space page by clicking **Space** in the top right corner of the screen. Administrators can go to a space page from the Spaces section.

Space tab

The **Space** tab contains detailed information on a space, as well as the full table of its members.

The following information about a space is available:

- **Space name**: displayed at the top of the page.
- **Tasks expire in**: the expiration period of all tasks within this space in days or hours and minutes (if the task expires in less than a day). When tasks expire, you can no longer work on them. By default, tasks expire in 10 days, and after that only old reports remain available.
- **Tasks used**: the number of tasks used in this space out of its task limit, if any. If a limit is not set, the value is Unlimited.
- **Members**: total number of managers and users in this space.
- **Date created**: date and time when the space was created.
- **Note**: space description.

Only an administrator or a space manager can add or edit a space description. Click + Note to add a description. Click ⋮ on the right of the space description and select the corresponding option to edit or delete the description.

Only an administrator can edit a space name, a limit on the number of tasks for a space and the task duration, as well as block a space.

Space members

The full table of all space members is displayed below the space information. For each member, the following information is available in the table:

- **Name**;

- **Email**;
- **Role**: Manager or User;
- **Status**: Active or Blocked;
- **Tasks (Open/Closed)**: the number of tasks opened and closed by the member;
- **Date created**.

You can sort the data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by.

Filter and search

You can filter the member table and search across the table.

You can filter the table by the following parameters of the member account:

- name,
- email,
- status,
- date created.

To set a filter for the member table

1. Click ▽ above the table.
2. Select the parameter to filter the data by.
3. If it is **Name**, **Email** or **Status**:
   - Select the check boxes next to the values you want and click **Add**.

   If it is **Date created**:
   - Select the dates of interest. To set a time period, click the start date and drag the cursor to the end date. Then click **Apply**.

You can select only one parameter for a filter. Set multiple filters to filter the task table by multiple parameters simultaneously.

To search across the member table

1. Enter your query into the 🔍 **Search** field above the table. Search is executed dynamically as you type.
2. Left-click outside the search field or press the ENTER key to lock the query.

Search and filtration are performed on the data currently displayed in the table. If you set a filter or search across the table, the following search or filtration operation will be applied to the results of the previous one.

Managing member accounts

The **Space** tab also allows administrators and space moderators to manage member accounts: create a new account; edit or delete an existing one. Users can only edit their own account details in the Profile menu.

To create a new member account

1. Click + above the member table.
2. In the **New user**pop-up window, select a role (**Manager** or **User**), then enter a name, email address, and password.
3. Click **Save**.

An administrator or manager can edit member account details: change the role of a member (to Manager or User), their name, email address, block or activate an account, or set a new password for an account.

To edit a member account

1. In the right part of the account row you want to edit, click ✎.
2. Enter the changes in the **User information** pop-up window.
3. Click **Save**.

This pop-up window also allows you to block the member. The blocked member will be unable to continue using the service. Only an administrator or manager can activate a blocked member account.

To block or unblock an administrator account, use the **Status** toggle in the edit window.

You can also delete a member account if the member no longer uses the service. You will not be able to restore a deleted account.

To delete a member account

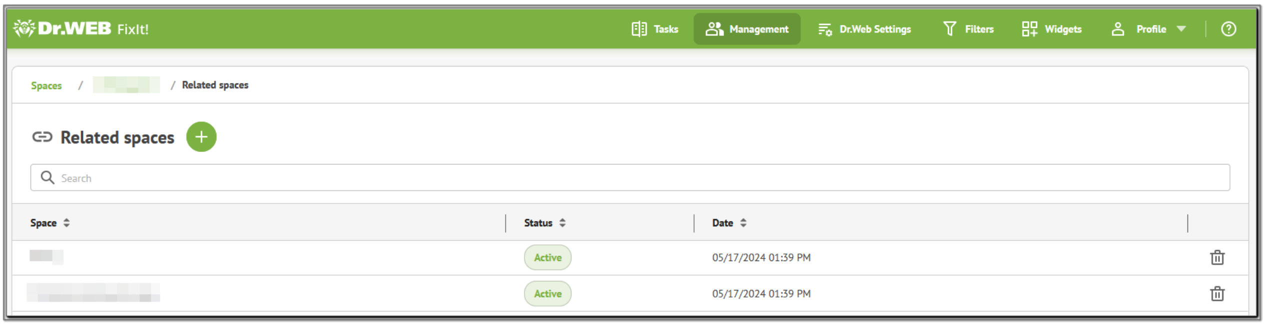
1. In the right part of the account row you want to delete, click 🗑.
2. Click **Delete**.

Related spaces

Dr.Web FixIt! allows you to create mutual relations between spaces, so that you can share tasks with members of other spaces. It can be beneficial for organizations that have multiple spaces for different divisions.

Only an administrator can add related spaces. Managers and users can share tasks with related spaces added by an administrator.

For an administrator to view or edit the list of related spaces, click the **Related spaces** button in the top right corner of the space page.



Spaces / [redacted] / Related spaces

Related spaces +

Search

Space	Status	Date
[redacted]	Active	05/17/2024 01:39 PM
[redacted]	Active	05/17/2024 01:39 PM

Figure 4. Related spaces

To add a related space

1. Click + next to the page title.
2. In the **Add space** pop-up, select spaces you want to set as related.
3. Click **Add**.

After that, managers and users of both spaces will be able to mutually share tasks.

List of support requests

From the space page, you can go to the list of support requests for all tasks in the respective space.

To go to the **Support requests** page, click the Expert support requests button in the top right corner of the page.

11. Tasks

Tasks allow you to organize computer scanning operations. Within a task you can create an analyzing FixIt! tool with customized parameters, get a report about system state, analyze the findings, and create a FixIt! tool for further analysis and curing of the system. A separate task is created for each computer.

Administrators can view all tasks in the service. Managers and users can access tasks of their own space only. Any space member can resume working in an open task created by another space member.

Tasks have an *expiration period*, after which all generated reports remain available, but no more work on the task can be done. The expiration period is set per space when it is created and applies to all tasks within the space. By default, tasks expire in 10 days.

Task information

On the main page of the service, you can view information on all tasks as well as start working on a specific task. To go to the main page of the service, click **Tasks** on the top pane or the Dr.Web FixIt! logo in the top left corner of the window.

At the top of the main page, you can find general information about service tasks (for administrators) or space tasks (for managers or users). Depending on the account type, the following information is available:

- **Tasks used:** the number of tasks used in this space out of the limit, if any (for managers or users).
- **Open:** the number of open tasks in the service (for administrators) or space (for managers or users).
- **Closed:** the number of closed tasks in the service (for administrators) or space (for managers or users).

Tasks table

Below the task information, you can find the full table of tasks.

For each task in the table, the following information is available:

- **Task name**
- **Expires in**
- **Creator**
- **Status:** Open or Closed
- **Space** (available only for administrators)
- **Reports:** the number of reports received within the task

- **Source** (available only for managers or users)
- **Date created**
- **Last modified**

You can sort the table data in descending/ascending order by clicking ▲▼ in the relevant column.

You can create a new task or select an existing task to start or resume working in the service.

To create a new task

1. Click the ⊕ icon on the **Tasks** page.
2. Enter the name of the new task.
3. Click **Create task**.

To go to a task

- Click the task name in the full table of tasks.

Filter and search

You can filter the table by the following task parameters:

- **Creator**
- **Space** (if available)
- **Status**
- **Date created**.
- **Last modified**

To set a filter for the task table

1. Click ▽ above the table.
2. Select the parameter to filter the data by.
3. If you selected **Creator**, **Space**, or **Status**:
   - Select the check boxes next to the values of interest and click **Add**.

   If you selected **Date created** or **Last modified**:
   - Select the dates of interest. To set a time period, click the start date and drag the cursor to the end date. Then click **Apply**.

You can select only one parameter for a filter. Set multiple filters to filter the report table by multiple parameters simultaneously.

To search across the task table

1. Enter your query into the 🔍 **Search** field above the table. Search is executed dynamically as you type.
2. To end the query input, left-click outside the search field or press ENTER.

Searching and filtering operations are performed on the data currently displayed in the table. If you set a filter or search across the table, the following searching or filtering operation will be applied to the results of the previous one.

11.1. Task

To scan and cure the computer, you need to create a task. You can open the task page by clicking the task name in the table of tasks on the main page of the web service.

Tasks have an *expiration period*, after which all generated reports remain available, but no more work on the task can be done. The expiration period is set per space when it is created and applies to all tasks within the space. By default, tasks expire in 10 days.

The task you have requested support for will have an unlimited expiration period.

How to work with a task

1. Create a task.
2. Create a FixIt! tool for data collection and send it to the owner of the scanned computer.

   The computer owner runs the FixIt! tool on their computer. The tool scans the system and generates a detailed report.
3. Upload the report on the state of the system. If the report is not uploaded to the task automatically, do it manually.
4. Analyze the report in the Search and analyze section.
5. Create a curing FixIt! tool for threat neutralization and send it to the owner of the scanned computer.
6. The computer owner runs the curing FixIt! tool on their computer. The tool runs the commands and generates a detailed report.
7. Repeat steps 3 to 6 until all of the threats on the client’s computer are neutralized.
8. If computer is cured or if the problem is no longer relevant, close the task.

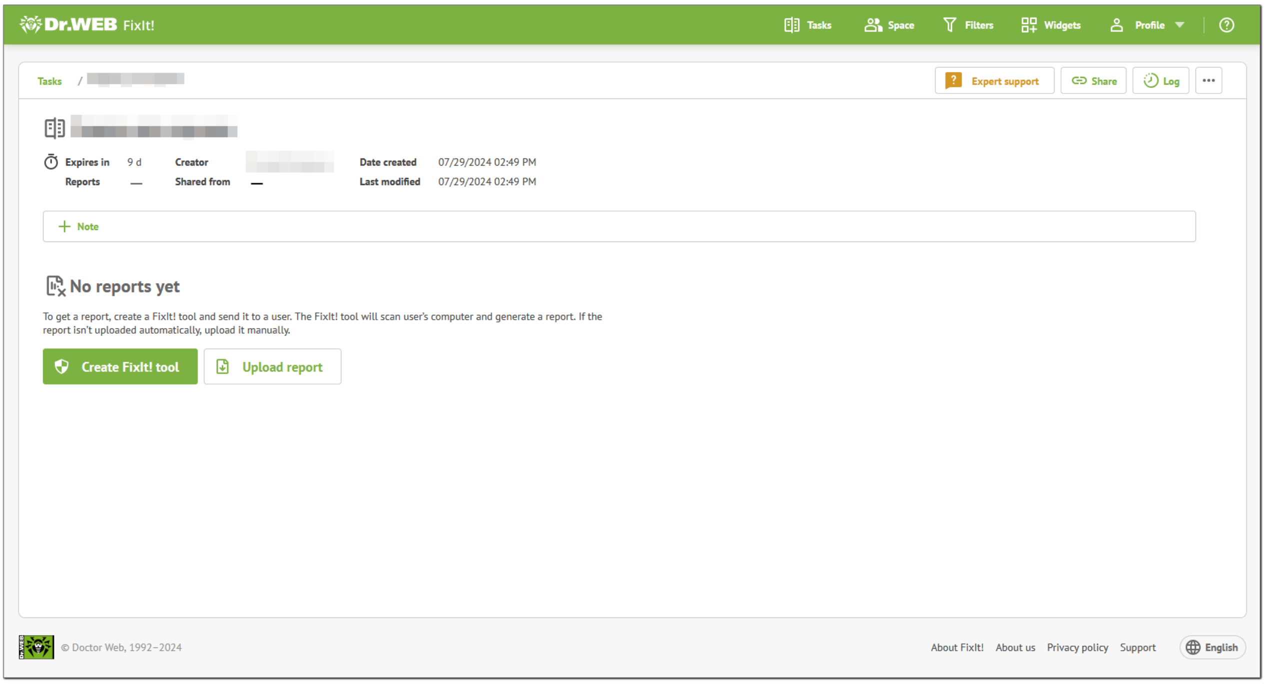
To start using Dr.Web FixIt!, create a new task or open an existing one. When you select a task, the task page opens.

Task information

The following information is displayed on the task page:

- task name,
- expires in,
- creator,
- date created,
- reports,
- source (available only for moderators and users),
- last modified,
- task description.

An administrator or any space member can add or edit the task description. Click + **Note** to add the description. Click ⋮ to the right of the task description and select the corresponding option to edit or delete the description.



Tasks / [redacted]

[redacted]

Expires in 9 d
Reports —
Creator [redacted]
Shared from —
Date created 07/29/2024 02:49 PM
Last modified 07/29/2024 02:49 PM

No reports yet

To get a report, create a FixIt! tool and send it to a user. The FixIt! tool will scan user's computer and generate a report. If the report isn't uploaded automatically, upload it manually.

© Doctor Web, 1992–2024

Figure 5. A task

An administrator or any space member can upload reports, rename, close or reopen any task, as well as share a task with a related space. Administrators and managers can also delete a task.

To rename a task

1. Do one of the following actions:

- In the top right corner of the page, click … and then select **Rename**.
- Hover over the task name and click ✎ .

2. Enter the new task name.

Changes are saved automatically.

To close a task

1. In the top right corner of the page, click ….
2. Select **Close**.
3. Confirm the action.

> ⚠ Closed tasks are read-only. Reopen the task to resume working with it.

To reopen a task

1. In the top right corner of the closed task page, click ▯▯.
2. Confirm the action in the pop-up.

To delete a task

1. In the top right corner of the page, click … and then select **Delete**.
2. Confirm the action.

Sharing tasks

You can share tasks with related spaces to collaborate.

To share a task

1. In the top right corner of the task page, click 🔗 **Share**.
2. On the **Share** page, click ⊕ .
3. In the **Add space** pop-up window, select the space you want to share the task with. An administrator can select among all spaces in the service; managers and users can select only among related spaces.
4. Click **Add**.

When you successfully share a task, the 🔗 icon appears next to it on your task list, and this task appears on the task list of the space you shared it with.

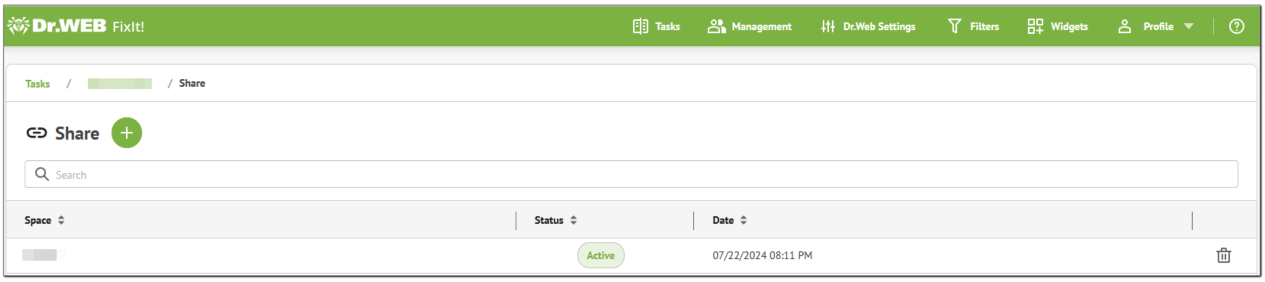
Name of the space the task is shared from is displayed in the **Shared from** field on the task page.

To revoke access to a task

1. In the top right corner of the task page, click **Share**.
2. On the **Share** page, click for the space.
3. In the **Uninstall settings** pop-up window, click **Delete**.

Share page

You can view and edit the table with the list of spaces that can access the task on the **Share** page by clicking **Share** on the task page.



Space	Status	Date
	Active	07/22/2024 08:11 PM

Figure 6. Share page

The table with the list of spaces that can access the task contains the following information:

- space,
- space status,
- date.

> If the space you shared a task with is removed from the list of your related spaces, you will lose access to that shared task automatically. You will also lose access to the tasks this space shared with you.

Reports

The task page contains the list of reports on the state of the scanned computer that were generated within the current task. Reports are generated by the FixIt! tool.

If a task contains no reports, you need to create a FixIt! tool and get a report, or upload a previously generated report manually (see the How to Upload a Report to a Task section).

Log

The Dr.Web FixIt! web service logs everything that is changed with tasks (see the Log section).

Expert support

Dr.Web FixIt! allows you to request help with your task from Doctor Web experts (see the Expert Support section).

11.2. Log

The log lists changes made in the task in the order they occurred.

To open a log

1. Select the respective task in the task list.
2. In the top right corner of the page, click ⏱ **Log**.

The log entries are presented in a table format. Each entry contains the following information:

- **action**,
- **date**,
- **source/initiator**: user or system,
- **description**.

To view an entry, click > next to it.

Actions in a log

The logged events are presented in a table format. The following actions are recorded in a log:

- Actions related to tasks:
  - creating,
  - editing,
  - expert support request—specifies an URL of the request page, request ID, and serial number of the redeemed expert support certificate.
- Actions related to reports:
  - uploading,
  - renaming,
  - analyzing,
  - deleting,

  - downloading.
- Actions related to filters:
  - adding of a new filter,
  - editing,
  - saving,
  - deleting.
- File recognition error (an error text is displayed in a pop-up window).
- Actions related to a FixIt! tool:
  - successfully created (the tool script is displayed in a pop-up window),
  - failed to create (the error text is displayed in a pop-up window),
  - analyzing tool created,
  - tool downloaded.
- Report data analysis:
  - downloading the artifacts collected by a tool according to selected actions,
  - artifact archive downloading.
- Actions related to widgets:
  - creating,
  - editing,
  - removal,
  - adding to the **Widgets** tab,
  - removing from the **Widgets** tab.

You can sort the table data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by.

Filter and search

You can filter the log contents and search through them.

The parameters that can be filtered by are:

- date,
- source/initiator,
- action.

To set a filter for a log

1. Click ▽ above the table.
2. Select the parameter to filter the data by.

3. If you selected **Source/Initiator** or **Action**:
   - Select the check boxes next to the values of interest and click **Add**.

   If you selected **Date**:
   - Select the dates of interest. To set a time period, click the start date and drag the cursor to the end date. Then click **Apply**.

You can select only one parameter for a filter. Set multiple filters to filter the log by multiple parameters simultaneously.

To search through a log

1. Enter your query into the **Search** field above the table. Search is executed dynamically as you type.
2. Left-click outside the search field or press the ENTER key to lock the query.

Search and filtering apply to the data currently displayed in the table. If you set a filter or search across the log for the second time, the second operation will be applied to the results of the previous one.

Log update and download

To update a log, click **Refresh** in the top right corner of the log page.

To download a log, click **Download** on the log page. The log is saved as a file with the .log extension. You can open it using any text editor.

11.3. Expert Support

If you encounter difficulties solving the problem in your task, you can request *expert support*. This will allow you to consult Doctor Web specialists and receive step-by-step instructions.

To use this service, you need to obtain a certificate. Once you activate it, expert support will be available.

The task you have requested support for will have an *unlimited* expiration period.

Requesting expert support

To request expert support

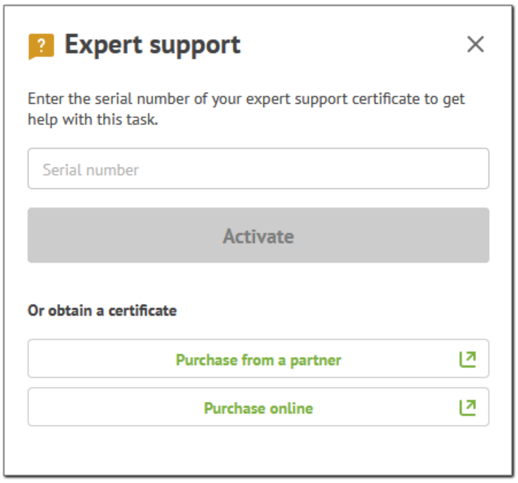
1. Go to the task page.
2. At the top right of the page, click the **Expert Support** button.

3. In the pop-up that opens next, specify the serial number of your expert support certificate (see Figure 7). The serial number should have the following format: XXXX-XXXX-XXXX-XXXX.
4. Click **Activate**.

To obtain an expert support certificate

1. Go to the task page.
2. Click the **Expert Support** button at the top of the page.
3. In the pop-up that opens next, choose one of the options:
   - Click **Purchase from a partner** to purchase a certificate from one of the Doctor Web partners.
   - Click **Purchase online** to purchase a certificate from the Doctor Web online store.

> ⚠ Please note that by clicking **Purchase online** you will generate a unique link that will only work once. To visit the store again, you will have to generate it once more as described above.



Expert support

Enter the serial number of your expert support certificate to get help with this task.

Figure 7. Requesting expert support

Request page

When you activate your certificate, the technical support page with your request will open in a new tab. Its header will contain the request ID and status (New, Acknowledged, Waiting, Closed).

On this page, you can:

- add a comment
- close the request

You will be notified by email on any replies or changes in the status of your request.

To go to the page of the existing request

1. Go to the page of the respective task.
2. At the top right of the page, click the **Expert Support** button.

OR

1. Go to the task Log page.
2. Find the row on the expert support event in the table and click > **to expand the information.**
3. Click the link in the **Support ticket URL** field.

OR

1. Go to the space page.
2. At the top of the page, click the **Expert support requests** button.
3. Select the request you need from the list (see Figure 8).
4. Click the request ID in the first column.

OR

1. Click the link in the notification email sent to you in the event of any changes in your request.

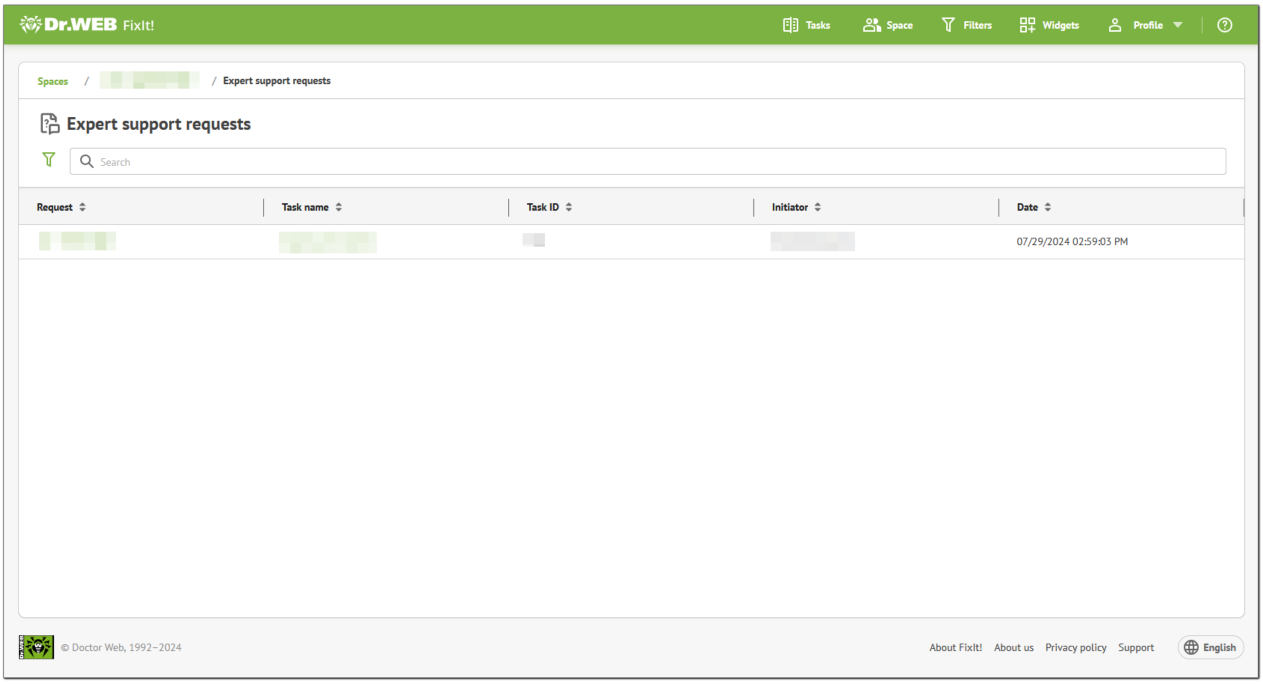
List of support requests

List of support requests for all tasks in the space can be found on the **Support requests** page.

To go to the Support requests page

1. Go to the space page.

2. At the top of the page, click the **Expert support requests** button.



Expert support requests

Request	Task name	Task ID	Initiator	Date
[redacted]	[redacted]	[redacted]	[redacted]	07/29/2024 02:59:03 PM

Figure 8. List of support requests

The table with the list of support requests contains the following data:

- the request ID with a link to the request page
- name of the task, for which support was requested
- task ID
- initiator of the request
- date of the request

12. Reports

Reports contain detailed information about the scanned computer state collected by a FixIt! tool. After analyzing a report in the service, you can create a curing FixIt! tool to neutralize threats found on the computer that was scanned.

You can rename, download, or delete reports. Additionally, you can compare two reports of the same task.

How to work with a report

- Upload a report to a task (you can do it automatically or manually).
- Use widgets to assess the status of the scanned computer and the level of risk it poses.
- View the report data.
- If needed, re-analyze the report using predefined and your own filters.
- Specify the actions, such as move, delete, or cure, that should be applied to each report object.
- Generate a curing FixIt! tool that will implement the actions you selected in the previous step, on a user's computer.

12.1. How to Upload a Report to a Task

Reports can be uploaded to the task automatically or manually. The maximum size allowed for a report to be uploaded is 12 GB.

To upload a report automatically

- Turn on the **Automatically upload reports** toggle when generating a FixIt! tool (see How to Scan a Computer with a FixIt! Tool for more details).

To upload a report manually

If the task does not contain any uploaded reports:

1. Open the task page.
2. Click **Upload report**.
3. Drag a report archive to the upload area in the pop-up window, or click **Browse** and select the archive in Windows Explorer or File Explorer.
4. Click **Upload**.

If the task contains uploaded reports:

1. Open the task page.
2. Click ⊕ next to the **Reports** table header.
3. Drag a report archive to the upload area in the pop-up window, or click 🗀 **Browse** and select the archive in Windows Explorer or File Explorer.
4. Click ⤓ **Upload**.

Once a report is uploaded to the task page, it is automatically parsed and prepared for analysis. The collected data is grouped into categories (see Data). If needed, you can re-parse the report by clicking ⟳ in the report list.

12.2. General Report Information

You can view general information about a report in the **Reports** tab at the task page. Additionally, the same information is provided on the report page (the **About** tab on the left).

To view general information about a report

- In the **Reports** table of a task
  - Open the task. The **Reports** table presents the general information for each report.
- On a specific report page
  - In the **Reports** table, click a report name. You will see the general information about report at the top of the page.

The following information is provided:

- **Upload method:** Manually or Auto.
- **Date created:** date when the report was generated.
- **Size, MB:** the size of the report file, in megabytes.
- **Key:** the password to the ZIP archive containing the report. Tap a key to copy it.
- **Device name:** the name of the scanned device.
- **Note:** the report description. In a note, you can outline the task goals or keep tracking of progress.

  You can add, edit, or delete notes. To add a note, click + **Note**, type a description and click **Save**. To edit or delete a note, click ⋮ on the right of the note area and select the option you need.

12.3. Information Collected by a FixIt! Tool

After you upload a report to a task, you can view:

- Data collected by a FixIt! tool from a scanned computer.
- The information about a scanned computer system, which is collected by a FixIt! tool.
- Files collected by a FixIt! tool during computer scanning.

12.3.1. Data

Data collected by a FixIt! tool from a scanned computer are categorized as follows:

- Dr.Web,
- Installed Apps,
- Processes,
- Drivers,
- Services,
- Network,
- Startups,
- Task scheduler,
- Web browsers,
- Event log,
- Registry,
- File system.

⚠ The report might miss certain categories if a FixIt! tool doesn’t detect them during the analysis.

To view the collected data, open a report page and select a category in the **System** drop-down menu on the left.

12.3.1.1. Dr.Web

The **Dr.Web** section displays the summary of information about the Dr.Web product installed on the computer. The **General** tab displays general information about the product, the **Changed settings** tab lists the product settings changed from the default ones, and the **Quarantine** tab contains information about the malicious objects moved to quarantine by the product.

The General tab

Information on the **General** tab is divided into collapsible blocks:

- **Product info**
- **Installed components**
- **Installed products**
- **Launched modules**
- **License files**
- **Anti-virus databases**
- **Installed software**

To collapse the block, click the ▾ icon. To expand it again, click ▸. Data in each block is presented in a table. You can sort them in the descending/ascending order by clicking ▲▼ in the respective column.

Product info

The table in this section lists the following data about the Dr.Web product installed on the computer:

- **Version:** the product version.
- **Hash:** the checksum of the application file.
- **Path:** the location of the program folder.
- **Repository:** the path to repository.
- **Path to bases:** the location of the anti-virus databases.

Installed components

The table in this section lists the following data on the anti-virus components:

- **Name:** the name of the component.
- **Status:** whether the component is installed or not. If it is installed, the tick icon is displayed in this column.

Installed products

The table in this section lists the following data on the Doctor Web products:

- **Name:** the name of the product.
- **Date created:** the date when the product file was created.

Launched modules

The table in this section lists the following data on the active modules of the anti-virus:

- **PID:** the process ID.
- **Name:** the name of the module.
- **Version:** the version of the module.

License files

The table in this section lists the following data on the license files of the Dr.Web product:

- **File name:** the name of the license file.
- **User number:** a unique number of the license holder.
- **User name:** the user name of the license holder.
- **Date created:** the date and time when the license file was created.
- **Expires:** the license expiration date and time.
- **Computers:** the number of devices where you can use the product according to the terms of the license.
- **Applications:** the list of product applications.
- **Settings:** the list of components, which are covered or not by the license.

To expand the information in a cell, click ›.

Anti-virus databases

The table in this section lists the following data on the databases of virus signatures used by Dr.Web to identify malicious code:

- **File name:** the name of the file with the virus signature database.
- **Number of records:** the number of recorded virus signatures in the database.
- **Version:** the version of the database.
- **Unix timestamp:** Unix time of the latest update of the database.
- **Date:** the date and time of the most recent update of the database.
- **Type of detects:** types of malicious code identified by the signatures in the database (such as viruses, adware, and so on).

Installed software

The table in this section lists the following data on the Dr.Web product installed on the computer:

- **Name:** the name of the Dr.Web product.

- **Location:** the location of the Dr.Web product.
- **Uninstall script:** the script that can be used to uninstall the Dr.Web product.

The Changed settings tab

In the tab, you can see a table with the following columns that show the changed settings of Dr.Web:

- **Name:** the setting name defined by the administrator.
- **Description:** information about the setting.
- **Key:** the Windows registry key associated with the setting.
- **Value name:** the name of the Windows registry value.
- **Default:** the default data of the Windows registry value.
- **Current:** the current data of the Windows registry value.

The Quarantine tab

In the tab, you can see a table with the following columns that show the malicious objects moved to quarantine:

- **Object:** the object name.
- **Threat:** the threat name.
- **Date added:** the date when the object was added.
- **Path:** the object path.
- **Type:** the object type.
- **Component:** the component that moved the object to quarantine.

You can filter the table of the quarantined objects by type and component. To do this, click ▽ and select the filter option you need.

You can also search for the quarantined objects. To do this, enter the object name (or part of it) in the search bar above the table.

12.3.1.2. Installed Apps

The **Installed apps** tab contains data on applications installed on the inspected computer at the time the report was generated.

The data is sorted into categories and displayed in drop-down boxes. To collapse the box, click the ▾ icon. To expand it again, click ▸.

Category	Parameters
Installed applications	• ID • Name • Location • Removal • Hidden
Applications from Microsoft App Store	• Name • Version • ID
MSI applications	• Name • Version • Vendor

You can sort the data in the table in the descending/ascending order by clicking ▲▼ in the respective column. You can also search for data within the table. To do it, enter your search query in the 🔍 **Search** field above the table and press ENTER..

FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.

The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.

The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

12.3.1.3. Processes

The **Processes** tab contains data about active processes on the scanned computer at the moment of the report generation.

The data is presented in the form of a table. For each process, the following information is available in the table:

- **PID:** a process ID.
- **Command line:** process start arguments.
- **File:** an executable process file.
- **Company:** an executable file publisher.
- **Signed:** whether the file is signed.
- **Reputation:** a suggested service status according to the internal Metawave service database, which contains information on previous detects.

Each row of the Processes table is a drop-down block that contains a table displaying the files used by the process. The table has the following columns:

- **File**
- **Company**
- **Signed**
- **Reputation**

You can reorder rows by the contents of a column. To do this, click ▲▼ in the column header.

You can also search across the Processes table and all its nested tables. To do this, enter your query into the 🔍 **Search** field above the Processes table and press ENTER.

> FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.
>
> The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.
>
> The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

If you want to view the details of a process or file, click its name in the table. On the right side of the screen, the **Details** pop-up window appears, showing information about the object parameters:

Tab	Available parameters
Process	• Status • Properties: ▪ PID ▪ Session ▪ Address ▪ Path ▪ Command line ▪ Current directory ▪ Bitness ▪ PEB address ▪ Debugged ▪ Isolation level ▪ Date created • Resources: ▪ Kernel time ▪ User time

Tab	Available parameters
	▪ Priority ▪ Handles • Parent: ▪ PID ▪ Session ▪ Path ▪ Command line ▪ Bitness ▪ Isolation level ▪ Date created
File	• Path • Status: ▪ Certificate ▪ File ▪ Type ▪ Cloud ▪ Software type • Hash: ▪ SHA1 ▪ SHA256 ▪ A link to VirusTotal • Properties: ▪ Size ▪ Date created ▪ Last modified ▪ Last accessed ▪ Build date • Attributes: ▪ Value ▪ Archive ▪ Security • Version: ▪ Description ▪ Version ▪ Company ▪ Origin name
Certificates	• Status • Date and time

Tab	Available parameters
	• Certificates: ▪ Subject ▪ Issuer ▪ Valid from ▪ Valid to ▪ SHA1 fingerprint ▪ SHA256 fingerprint ▪ Serial number ▪ Name
Data *(for files only)*	• Memory address • Path • Size • Status • Build date

12.3.1.4. Drivers

The **Drivers** tab contains information about drivers detected on the device.

Driver data is displayed in the form of a table. The table contains the following information:

- **file**: driver file path;
- **status**: driver activity status;
- **type**: driver type;
- **launch**: by whom or how the driver was launched;
- **company**: driver manufacturer;
- **signed**: signature;
- **reputation**: a suggested service status according to the internal Metawave service database, which contains information on previous detects.

You can sort the table data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by. You can also search across the table. Enter your query into the 🔍 **Search** field above the process data table and press ENTER.

FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.

The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.

The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

You can see detailed driver information by clicking on the path to the driver file in the table. The following information is available:

Tab	Available parameters
Info	• path, • size, • address, • status.
File	• path; • status: ▪ certificate, ▪ file, ▪ type, ▪ cloud, ▪ software type; • hash: ▪ SHA1, ▪ SHA256, ▪ a link to VirusTotal; • properties: ▪ size, ▪ date created, ▪ last modified, ▪ last accessed, ▪ date created; • attributes: ▪ value, ▪ archive, ▪ security; • version: ▪ description,

Tab	Available parameters
	▪ version, ▪ company, ▪ origin name.
Certificates	• status; • date and time; • certificates: ▪ subject, ▪ issuer, ▪ valid from, ▪ valid to, ▪ SHA1 fingerprint, ▪ SHA256 fingerprint, ▪ serial number, ▪ name.

12.3.1.5. Services

The **Services** tab provides information about services on the scanned computer.

Service data is presented in the form of a table. The table contains the following data:

- **name**: service name;
- **launch**: by whom or how the service was launched;
- **state**: service activity status;
- **PID**: service process ID;
- **command line**: service file path;
- **signed**: whether the file is signed;
- **reputation**: a suggested service status according to the internal Metawave service database, which contains information on previous detects.

You can sort the table data in the descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by. You can also search across the table. Enter your query into the 🔍 **Search** field above the service data table and press ENTER.

> FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.
>
> The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.
>
> The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

You can view detailed information on a service by clicking on the service name or service path in the table. The following information on services is available:

Tab	Available parameters
Info	• status, • name, • description, • type, • start mode, • state, • accepted commands, • error control, • exit code, • Win32 exit code, • process.
File	• path; • status: ▪ certificate, ▪ file, ▪ type, ▪ cloud, ▪ software type; • hash: ▪ SHA1, ▪ SHA256; ▪ a link to VirusTotal; • properties: ▪ size, ▪ date created, ▪ last modified, ▪ last accessed,

Tab	Available parameters
	▪ date created; • attributes: ▪ value, ▪ archive, ▪ security; • version: ▪ description, ▪ version, ▪ company, ▪ origin name.
Certificates	• status; • date and time; • certificates: ▪ subject, ▪ issuer, ▪ valid from, ▪ valid to, ▪ SHA1 fingerprint, ▪ SHA256 fingerprint, ▪ serial number, ▪ name.

12.3.1.6. Network

The **Network** tab provides information about network connections on the scanned computer.

Network data is presented in tabs in the form of tables.

Tab	Parameters
Interfaces	• Description • DHCP • DHCP server • IP • Gate • DNS server
Static routes	• Network • Mask • Gate

Tab	Parameters
HOSTS file	• IP • Domains
Connections	• TCP • UDP • TCPv6 • UDPv6 Protocol data is displayed in tabs, which contain tables with the following protocol parameters: • PID • File • Company • Signed • Reputation • Local address • Local port • Remote address • Remote port
DNS settings	• Value • Object • SID • Key
DNS cache	• Name • Host • Type • TTL • IPv4 • IPv6
Proxy settings	• Value • Object • SID • Key

You can sort data in the **Network** tables in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by.

You can search across the tables on the **Connections** tab. Enter your query into the 🔍 **Search** field above the protocol data table and press ENTER.

> FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.
>
> The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.
>
> The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

12.3.1.7. Startups

The **Startups** tab displays information on startup processes on the inspected computer.

Startup information is displayed on the tabs that contain the following details:

Tab	Data
General	• WMI: ▪ path, ▪ namespace, ▪ CLSID, ▪ class, ▪ value, ▪ working directory; • Winsock name providers: ▪ name, ▪ launch, ▪ path, ▪ company, ▪ signed, ▪ reputation; • Winsock local name providers: ▪ name, ▪ launch, ▪ path, ▪ company, ▪ signed, ▪ reputation.
Registry startups	This tab contains the list of startup items. Click an item to view a table with the following details: • key,

Tab	Data
	• path, • company, • signed, • reputation.
Shortcuts	Click a shortcut name to view a table with the following details: • file, • command.

You can sort the table data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by.

You can search for data across the **Startups** and **Shortcuts** sections. To do it, enter your search query in the 🔍 **Search** field above the list and press ENTER.

> FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.
>
> The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.
>
> The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

You can view details on the file by clicking its name of the path to it in the table.

Tab	Available parameters
Information	On the **General** tab: • name, • state, • WOW64, • active, • GUID, • path. On the **Registry startups** tab: • status, • SID, • key, • value, • object.

Tab	Available parameters
	On the **Shortcuts** tab: • status, • name, • path, • arguments, • target, • data.
File	• path; • status: ▪ certificate, ▪ file, ▪ type, ▪ cloud, ▪ software type; • hash: ▪ SHA1, ▪ SHA256; ▪ a link to VirusTotal; • properties: ▪ size, ▪ date created, ▪ last modified, ▪ last accessed, ▪ date created; • attributes: ▪ value, ▪ archive, ▪ security; • version: ▪ description, ▪ version, ▪ company, ▪ origin name.
Certificates	• status; • date and time; • certificates: ▪ subject, ▪ issuer,

Tab	Available parameters
	▪ valid from, ▪ valid to, ▪ SHA1 fingerprint, ▪ SHA256 fingerprint, ▪ serial number, ▪ name.

12.3.1.8. Task Scheduler

Tab **Task scheduler** contains a list of tasks scheduled for the scanned computer.

Information about scheduled tasks is displayed in the form of a table containing the following data:

- **name**: scheduled task name;
- **status**: scheduled task status;
- **command**: scheduled task run command.

You can sort the table data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by. You can also search across the table. Enter your query into the 🔍 **Search** field above the process data table and press ENTER.

> FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.
>
> The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.
>
> The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

12.3.1.9. Web Browsers

The **Web browsers** tab contains profile data of web browsers installed on the scanned computer.

Web browser data is displayed in the form of drop-down lists of tables containing detailed information about browser profiles.

Category	Parameters
Extensions	• ID, • name, • path.
Settings	• SID, • path.

You can sort the table data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by.

You can view detailed information about extensions by clicking extension ID; to view detailed information about settings, click SID. You will see a table containing the following details:

Category	Details
Extensions	• browser, • status, • name, • ID, • version, • profile, • user SID, • location path, • URL, • path, • type. For some extensions, file details can be available.
Settings	• browser, • status, • URL, • profile, • SID, • path.

12.3.1.10. Event Log

The **Event log** tab contains information about events on the scanned computer.

The data is displayed in the form of a table containing the following event information:

- **ID**: event ID;
- **source**: event source;

- **file**: log type (application log or system log);
- **computer**: name of the scanned computer;
- **date**: event date;
- **message**: event description. Click › to see the full event description.

Filter and search

You can filter and search across the table contents.

You can filter the table by the following event parameters:

- source,
- file,
- computer,
- date.

To create a filter for the event table

1. Click ▽ above the table.
2. Select the filtration parameter.
3. If you selected **Source**, **File**, or **Computer**:
   - Select the check boxes next to the values of interest and click **Add**.

   If you selected **Date**:
   - Select the dates of interest. To set a time period, click the start date and drag the cursor to the end date.
4. Click **Apply**.

You can select only one parameter for a filter. Set multiple filters to filter the member table by multiple parameters simultaneously.

To search across the event table

1. Enter your query into the 🔍 **Search** field above the table. Search is executed dynamically as you type.
2. Left-click outside the search field or press the ENTER key to lock the query.

Search and filtration are performed on the data currently displayed in the table. If you set a filter or search across the table, the following search or filtration operation will be applied to the results of the previous one.

FixIt! allows you to use wildcard characters ‘*’ and ‘?’ in searches. The asterisk ‘*’ stands for any number of characters, including zero, and the question mark ‘?’ stands for any single character.

The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.

The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

12.3.1.11. Registry

The **Registry** tab contains information on the registry contents of the scanned computer.

The data in this category can be presented as a list or a tree. By default, the data is displayed as a list. To view the data as a tree, click the **Tree** tab.

On the **List** tab, the data is presented in the form of a table of registry keys. The table contains the following data:

- **key**: the full entry key;
- **name**: parameter name;
- **type**: parameter type;
- **size**: parameter size;
- **value**: parameter value.

You can sort the table data in the descending/ascending order by clicking ⇅ in the column of the table containing the data you want the table to be sorted by. You can search across the table. Enter your query into the 🔍 **Search** field above the process data table and press ENTER.

FixIt! allows you to use wildcard characters ‘*’ and ‘?’ in searches. The asterisk ‘*’ stands for any number of characters, including zero, and the question mark ‘?’ stands for any single character.

The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.

The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

Click a registry key in the list or a parameter name in the tree to view detailed information on it. The following information on registry contents is available:

Tab	Data
Information	• SID, • key, • subkeys, • last accessed, • security, • status.
Value	The data is presented in the form of a drop-down block. The following is available for each parameter: • name, • type, • size, • value, • status.

12.3.1.12. File System

The **File system** tab contains information about the file system of the computer you are checking.

The data in this category can be viewed as a list or a tree. By default, file system is displayed as a list. To view the data in a tree, click the **Tree** tab.

On the **List** tab, the data is displayed in the form of a summary table, which contains the following information:

- **Name**: path to file;
- **SHA1**: checksum of the file;
- **Signed**: whether the file is signed;
- **Size**, KB: file size;
- **Last modified**: latest modification date and time;
- **reputation**: a suggested service status according to the internal Metawave service database, which contains information on previous detects.

You can sort the table data in the descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by. You can search across the table. Enter your query into the 🔍 **Search** field above the process data table and press ENTER.

FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.

The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.

The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

You can view detailed information about a file by clicking the path in the table on the **List** tab or on the file name on the **Tree** tab. Depending on the file type, the following information will be available.

Tab	**Available parameters**
File	• path; • status: ▪ certificate, ▪ file, ▪ type, ▪ cloud, ▪ software type; • hash: ▪ SHA1, ▪ SHA256, ▪ a link to VirusTotal; • properties: ▪ size, ▪ date created, ▪ last modified, ▪ last accessed, ▪ date created; • attributes: ▪ value, ▪ archive, ▪ security; • version: ▪ description, ▪ version, ▪ company, ▪ origin name.

Tab	Available parameters
Certificates	• status; • date and time; • certificates: ▪ subject, ▪ issuer, ▪ valid from, ▪ valid to, ▪ SHA1 fingerprint, ▪ SHA256 fingerprint, ▪ serial number, ▪ name.

12.3.2. System

The information about a scanned computer system, which is collected by a FixIt! tool, is categorized and presented in a series of small panels.

Category	What a mini panel displays
Processors	• current processor frequency (in % and GHz), • Name • description (in tooltip) • max turbo frequency, GHz, • base frequency, GHz, • number of physical cores, • number of logical cores.
Memory	• used/total space of local memory, • used/total space of virtual memory.
Experience Index	• average score (calculated based on 5 parameter scores provided below), • score of Memory, • score of Processor, • score of Drive, • score of 3D graphics, • score of Graphics,
OS	• file name, • version, • location, • device name,

Category	What a mini panel displays
	• system type, • boot mode, • up time, • local time.
Anti-virus and firewall	• product, • version, • status, • company.
Localization	• country or region, • time zone, • OS language, • interface language.
Hard drives	Information about hard drives are provided in expandable sections. The section header shows: • hard drive name, • used/total space. The sections provides the following information about each hard drive: • drive (the letter of the drive), • serial number, • available space, GB, • file system, • tag. By clicking the **S.M.A.R.T.** button at the right of expandable section header, you can view the various indicators of the hard drive reliability in the pop-up.
Accounts	• name, • role, • description and group (in a tooltip).
Network drive	• username, • remote path, • provider name, • drive letter.
Network shortcut	• username, • name, • path.
Environment variables	• name, • path.

To view the collected information about a system, open a report page and click the **System** tab on the left.

12.3.3. Files

Files collected during the computer scan by a FixIt! tool are displayed in a table in the **Files** tab of the report page. The table includes the following columns.

Column name	Contents
File	File name
SHA1	SHA1 checksum
Size, KB	File size in kilobytes
Last modified	File modification date
Reputation	File checkup result in the Metawave service

The icons in the table stand for the following options:

- ⤓—download file;
- ↗—open file page on the VirusTotal website.

You can sort the table data in descending/ascending order by clicking ▲▼ in the relevant column.

File scan

You can launch a file scan by reputation.

Reputation defines the file status. Possible values are: malicious, suspicious, suspicious vendor, unknown, not found, clean.

You can scan a file again by clicking the ↻ icon.

If an error occurs during the scan, the **Error** status appears.

Search

You can search across the table. Enter your query into the 🔍 **Search** field above the process data table and press ENTER.

> FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.
>
> The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.
>
> The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

File download

You can download files from this section to your computer.

- To download a file, click ⤓ in the table row.
- To download several files at once, select check boxes next to the files you want to download and click **Download** above the table.

12.4. How to View a Report List

If at least one report has been uploaded to the task, the task page displays the table of all reports belonging to the current task. For each report, the following information is available in the table:

- **ID**: numeric report id within a task. Generated automatically.
- **Name**: report name. Generated automatically. You can change the name afterwards.
- **Status**: report analysis state.
- **Upload method**: Auto or Manually.
- **Uploaded**: date and time of upload.

You can sort the data in descending/ascending order by clicking ⇅ in the column of the table containing the data you want the table to be sorted by.

Filter and search

You can filter the full table of reports and search across the table data.

You can filter the table by the following report parameters:

- upload method,
- uploaded.

To set a filter for the report table

1. Click ▽ above the table.

2. Select the parameter to filter the data by.
3. If it is **Upload method**:
   - Select the check boxes next to the values you want and click **Add**.

   If it is **Uploaded**:
   - Select the dates of interest. To set a time period, click the start date and drag the cursor to the end date. Then click **Apply**.

You can select only one parameter for a filter. Set multiple filters to filter the report table by multiple parameters simultaneously.

To search across the report table

1. Enter your query into the 🔍 **Search** field above the table. Search is executed dynamically as you type.
2. Left-click outside the search field or press the ENTER key to lock the query.

Search and filtration are performed on the data currently displayed in the table. If you set a filter or search across the table, the following search or filtration operation will be applied to the results of the previous one.

To view and analyze a report, click its name in the Reports table.

12.5. How to Compare Reports

If a task contains more than one report, you can compare reports generated at different times to see the differences in the state of the system at the moment of report generation, including the resolution of previously discovered issues and the appearance of new ones.

To compare reports

1. In the top-right corner of the **About** tab, click ⇄ **Compare**.
2. On the **Compare reports** page, select a pair of reports to compare.

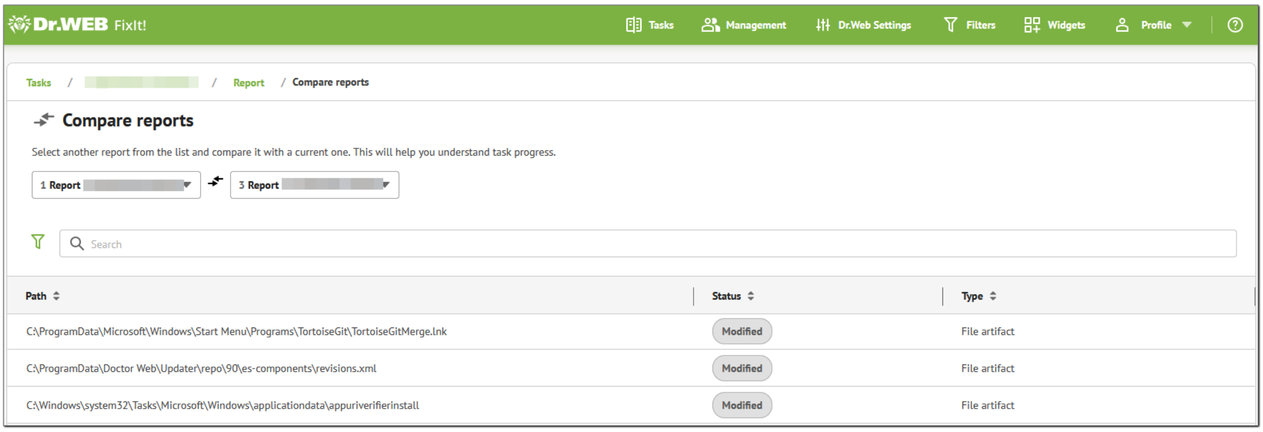
To switch reports around, click ⇄.

Compare reports table

The following information is provided in the table on the **Compare reports** page:

- **Path**: path to an object on a scanned computer.
- **Status**: Modified, New, or Deleted.

- **Type**: object category in the report.



Tasks / [redacted] / Report / Compare reports

Compare reports

Select another report from the list and compare it with a current one. This will help you understand task progress.

1 Report [redacted] ⇄ 3 Report [redacted]

Search

Path	Status	Type
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TortoiseGit\TortoiseGitMerge.lnk	Modified	File artifact
C:\ProgramData\Doctor Web\Updater\repo\90\es-components\revisions.xml	Modified	File artifact
C:\Windows\system32\Tasks\Microsoft\Windows\applicationdata\appuriverifierinstall	Modified	File artifact

Figure 9. Compare Reports

You can sort the table data in descending/ascending order by clicking ▲▼ in the relevant column.

Filter and search

You can filter the full table of compared objects and search across the table data.

You can filter the table by the following parameters of the object:

- status,
- type.

To set a filter for the object comparison table

1. Click ▽ above the table.
2. Select the parameter to filter the data by.
3. Select the check boxes next to the values of interest.
4. Click **Apply**.

You can select only one parameter per filter. Set multiple filters to filter the table by multiple parameters simultaneously.

To search across the object comparison table

1. Enter your query into the 🔍 **Search** field above the table. Search is executed dynamically as you type.
2. Left-click outside the search field or press the ENTER key to lock the query.

Search and filtration are performed on the data currently displayed in the table. If you set a filter or search across the table, the following search or filtration operation will be applied to the results of the previous one.

FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.

The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.

The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

12.6. How to Download a Report

You can download reports as ZIP files to your local machine.

To download a report

- Via the **Reports** table in a task
  1. In the right part of the row, click ⤓.

     You have the option to download the report while it is being analyzed, as the ⤓ icon will remain available.
- On the report page
  1. In the **Reports** table, click the report name.
  2. In the top right corner of the report page, click ⋯ > ⤓ **Download**.

12.7. How to Rename a Report

You can change a report's name to something more user-friendly.

To rename a report

1. On the report page, do one of the following:
   - In the top-right corner of the **About** tab, click ⋯ > ✎ **Rename**.
   - Hover over the report name and click ✎.
2. Enter a new name and press ENTER.

12.8. How to Delete a Report

Requires the Administrator or Manager role.

To delete a report

1. Go to the report page.
2. Click ··· > **Delete**.
3. Confirm the action.

12.9. Widgets

Widgets enable you to quickly evaluate the status of the scanned computer and the level of risk it poses.

Widgets are mini panels containing filter sets that are automatically applied to a report. By assessing the filters that were triggered during the analysis of the report, you can rapidly grasp the situation on the scanned computer. For analysis, you can use pre-set widgets that are created by administrator or your own widgets, if, for instance, you like to conduct further custom analysis. You can disable widgets, display widgets based on danger level, or show widgets created for a particular task. That helps you easily choose widgets suitable for your purposes.

Managing widgets

To manage widgets, use the **Widgets** panel. This panel offers a convenient way to view, edit, or delete widgets. To access the **Widgets** panel, click **Widgets** at the top right of the main FixIt! page.

If you want to use the widgets that are only limited to a particular task, go to the **Widgets** section of a report. To do this:

1. Open the **Tasks** panel.
2. Select a task in the task list.
3. Open a report that you want to see the summary for.
4. At the left, select **Widgets**.

12.9.1. How to Use Widgets for Report Analysis

Using widgets, you can quickly analyze a received report and assess the situation on the scanned computer.

How to Analyze a Report Using Widgets

1. Open the **Tasks** panel.
2. Select a task in the task list.

3. Open a report you want to analyze.
4. At the left, select **Widgets**.
5. On the **All widgets** tab, you can assess the results of applying different filters to the report. This can be easily done using danger level icons: Threat, ⚠ Suspicious and ⓘ Info.

Then you may choose to filter widgets by danger level, review triggered filter details for the specific widget and restart analysis for the specific widget.

12.9.2. Widget Categories

Widgets are divided into categories based on their availability to users.

Category	Description	Possible actions
All users	Pre-set widgets.	Space members can only enable or disable these widgets. **Note:** An administrator can protect widgets of this category from being disabled. The protected widget is always enabled.
Space	Widgets that can only be used within a particular space.	Space members can enable, disable, edit, or delete them.
Task	Widgets that can only be used within a particular task.	Space members can enable, disable, edit, or delete them.
Only me	Widgets that are only visible to their creator.	These widgets can only be enabled, disabled, edited, or deleted by their creators.

Furthermore, widgets differ based on their contents: they can only consist of individual filters or filter groups, but not both.

12.9.3. How to View a Widget List

You can view the widgets by categories.

To view a list of widgets of the For all category

1. At the top right of the main FixIt! page, click **Tasks**.
2. Select any task from the task list, and then select any report related to that task.
3. On the left panel, select **Widgets**.
4. In the top right corner of the **Widgets** panel, click **All widgets**.

5. In the **All widgets** window, select the **For all** category on the left. In the center, all widgets of this category appear.

To view a list of widgets of the For space category

There are two ways to view a list of widgets of the **For space** category:

- In the **All widgets** window (within a report). To do this:

    1. At the top right of the main FixIt! page, click **Tasks**.
    2. Select any task from the task list, and then select any report related to that task.
    3. On the left panel, select **Widgets**.
    4. In the top right corner of the **Widgets** panel, click **All widgets**.
    5. In the **All widgets** window, select the **For space** category on the left. In the center, all widgets of this category appear.

- On the **Widgets** tab. To do this:

    1. At the top right of the main FixIt! page, click **Widgets**.
    2. On the **Widgets** panel that opens, select the **For space** tab.

To view a list of a widgets of the For task category

1. At the top right of the main FixIt! page, click **Tasks**.
2. Select any task from the task list, and then select any report related to that task.
3. On the left panel, select **Widgets**.
4. In the top right corner of the **Widgets** panel, click **All widgets**.
5. In the **All widgets** window, select the **For task** category on the left. In the center, all widgets of this category appear.

To view a list of a widgets of the For me category

To view a list of a widgets of the **For space** category, do one of the following:

- In the **All widgets** window (within a report)

    1. At the top right of the main FixIt! page, click **Tasks**.
    2. Select any task from the task list, and then select any report related to that task.
    3. On the left panel, select **Widgets**.
    4. In the top right corner of the **Widgets** panel, click **All widgets**.
    5. In the **All widgets** window, select the **For me** category on the left. In the center, all widgets of this category appear.

- On the **Widgets** tab

  1. At the top right of the main FixIt! page, click **Widgets**.
  2. On the **Widgets** panel that opens, select the **For me** tab.

12.9.4. How to Create a Widget

You can create your own widgets, adding filters and filter groups you need there.

To create a widget

1. Open the **New widget dialog**. You have two options to do it:

- From a report

  a. At the top right of the main FixIt! page, click **Tasks**.
  b. Select any task from the task list, and then select any report related to that task.

  > If you want to create a widget of the **For task** category, you need to choose a specific task, not just any task.

  c. At the left, select **Widgets**.
  d. On the **Widgets** tab, click +.

- From the **Widgets** panel in the main window

  a. At the top right of the main FixIt! page, click **Widgets**.
  b. At the top of the **Widgets** tab, click +.

2. From the **Available** drop-down menu, select a widget category: **For space**, **For task** or **For me**.

   > The **For task** category only appears in a list, if you create a widget from a report.

3. From the **Type** drop-down menu, choose a widget type (widgets can consist of filters or filter groups).
4. Click **Add** and specify filters or filter groups you want to use in this widget.
5. Enter the name of the new widget.
6. Specify a danger level for the widget. Then you'll be able to filter or sort widgets by this level.
7. (Optional) Enter a description for the widget.

8. Click **Create**.

> Newly created widgets will applied to a report automatically, when you open the report’s **Widget** tab. It allows you to use the new widgets to analyze the reports that were created before these widgets.

12.9.5. How to Edit a Widget

You can edit any widgets except for the pre-set ones (i.e. the **For all** category).

To edit a widget of the Space or Only me category

1. At the top right of the main FixIt! page, click **Widgets**.
2. Hover over the widget name in the list and select ✎.
3. Change the widget settings and click **Save**.

To edit a widget of the For task category

1. At the top right of the main FixIt! page, click **Tasks**.
2. Click the task you want to edit the widget for, then select any report for the task.
3. At the left, select **Widgets**.
4. Go to the **For task** tab.
5. In the top right corner of a mini panel of the widget you want to edit, click ··· > **Edit**.
6. Change the widget settings and click **Save**.

12.9.6. How to Enable or Disable a Widget

You can disable the widgets that you do not need and re-enable them later.

> Some widgets in the **For all** category can be protected by admins from being disabled. Such widgets are always enabled.

To enable a widget

1. At the top right of the main FixIt! page, click **Tasks**.
2. Click the task you want to enable a widget for, then select any report for the task.
3. On the left panel, select **Widgets**.
4. In the top right corner of the **Widgets** panel, click **All widgets**.
5. In the **All widgets** window, select the category of a widget you want to enable on the left.

6. In the center part, select the widget you need.
7. On the right, activate the **Enable** toggle. The widget turns on and appears on the **Widgets** panel of the report.

To disable a widget

1. At the top right of the main FixIt! page, click **Tasks**.
2. In the task list, select the task you want to disable a widget for, and then select any report related to that task.
3. At the left, select **Widgets**.
4. If needed, go to the tab of the specific category.
5. To disable a widget of the **For all**, **For space**, or **For me** category, in the top right corner of the widget click ⏻. To disable a widget of the **For task** category, in the top right corner of the widget click ··· > **Disable**.

12.9.7. How to Delete a Widget

You can delete any widgets except for the pre-set ones (i.e. the **For all** category).

To delete a widget of the Space or Only me category

1. At the top right of the main FixIt! page, click **Widgets**.
2. On the right of the widget you want to delete, click 🗑.
3. Click **Delete**.

To delete a widget of the For task category

1. At the top right of the main FixIt! page, click **Tasks**.
2. Click a task you want to edit the widget for, then select a report for the task.
3. At the left, select **Widgets**.
4. Go to the **For task** tab.
5. In the top right corner of the widget you want to edit, click ··· > **Delete**.
6. Confirm the action by clicking **Delete**.

12.9.8. How to View the Widget's Contents

Widgets can only contain filters or filter groups.

To view the widget's contents

- In the **All widgets** window

1. At the top right of the main FixIt! page, click **Tasks**.
2. Select a task in a task list, then select a report for the task.
3. At the left, select **Widgets**. The **Widgets** panel for this report appears.
4. In the top right corner of the **Widgets** panel, click **All widgets**.
5. In the center part of the **All widgets** window, select the widget you need.
6. At the right, the widget's contents appear.

- On the **Search and analyze** panel

1. At the top right of the main FixIt! page, click **Tasks**.
2. Select a task in a task list, then select a report for the task.
3. At the left, select **Widgets**. The **Widgets** panel for this report appears.
4. Find the widget and click **Details**.
5. The **Search and analyze** panel appears displaying all filters of this widget.

> ⚠ If no filters in a widget are triggered, the **Details** button is grayed out. In that case, use the first approach to explore the widget's contents.

12.9.9. How to Manage Widgets

You can search for widgets by name, sort them, or filter by category (For all, For me, etc.) or danger level.

How to search for a widget

You can search for widgets by name. For your convenience, the search starts as you type.

To search for a widget

1. At the top right of the main FixIt! page, click **Widgets**.
2. Go to a tab of the widget category: **All widgets**, **Space** or **Only me**.
3. In the search bar, enter a widget name (or part of it).

> ⚠ Before you start searching, make sure you go to the appropriate widget category tab. As an example, if you search when on the **For me** tab, FixIt! searches across the widgets of this category. To search across all widgets, go to the **All widgets** tab.

How to sort widgets

You can sort widgets by name, category, danger level, or type.

To sort widgets

1. At the top right of the main FixIt! page, click **Widgets**.
2. Go to a tab of the widget category: **All widgets**, **Space** or **Only me**.
3. To sort widgets by column, click the relevant header. To reverse the direction of your sort, click the same header again.

How to filter widgets

You can filter widgets by category (For all, For me, etc.) or danger level (Danger, Suspicious, Info).

To filter widgets by category

- From the **Widgets** panel in the main window

  1. At the top right of the main FixIt! page, click **Widgets**.
  2. Go to a tab of the widget category: **All widgets**, **Space** or **Only me**.

- From a report

  1. At the top right of the main FixIt! page, click **Tasks**.
  2. Select a task in a task list, then select a report for the task.
  3. At the left, select **Widgets**. The **Widgets** panel for this project appears.
  4. Go to a tab of the widget category: **All widgets**, **Space**, **Task**, or **Only me**.

To filter widgets by danger level

- From the **Widgets** panel in the main window

  1. At the top right of the main FixIt! page, click **Widgets**.
  2. On the right of the search bar, turn on ○.
  3. On the right of the toggle, select a danger level.

  To clear the filter, turn off the toggle.

- From a report

  1. At the top right of the main FixIt! page, click **Tasks**.
  2. Select a task in a task list, then select a report for the task.

3. At the left, select ⊞ **Widgets**. The **Widgets** panel for this project appears.
4. At the top right of the **Widgets** panel, turn on ○.
5. On the right of the toggle, select a danger level.

To clear the filter, turn off the toggle.

13. Search and Analyze

The **Search and analyze** tab allows you to analyze report data. You can perform search queries using filters, apply actions to malicious objects, and create a curing FixIt! tool for solving the detected problems.

The section contains the following tabs:

- Defined Filters
- New Filter
- Selected Actions

13.1. Defined Filters

On the **Defined Filters** tab, you can select and apply filters that you and other users created.

All defined filters are sorted into the following categories:

- **All users**—filters that are available to all web service users.
- **Only me**—filters that are available to you only.
- **This space**—filters that are available to the space members.
- **Current task**—filters that are only available within the task.

To select a defined filter

1. On the **Defined filters** tab, click **Add**. The **Add filters** dialog appears where all defined filters are shown organized in categories, as well as your favorite defined filters.
2. Select the filters you need and click **Add**.

> ⚠ To find the filter you need in the **Add filters** dialog quickly, use the search bar.

Filter results

The report data that matches the applied filters can be found under the filter list. The data is presented in drop-down panels that contain lists of objects. Each drop-down panel corresponds to one filter. The drop-down panel is only shown if filter data is found.

Each drop-down panel contains a table with the data filtered out from the report. The table includes the following columns:

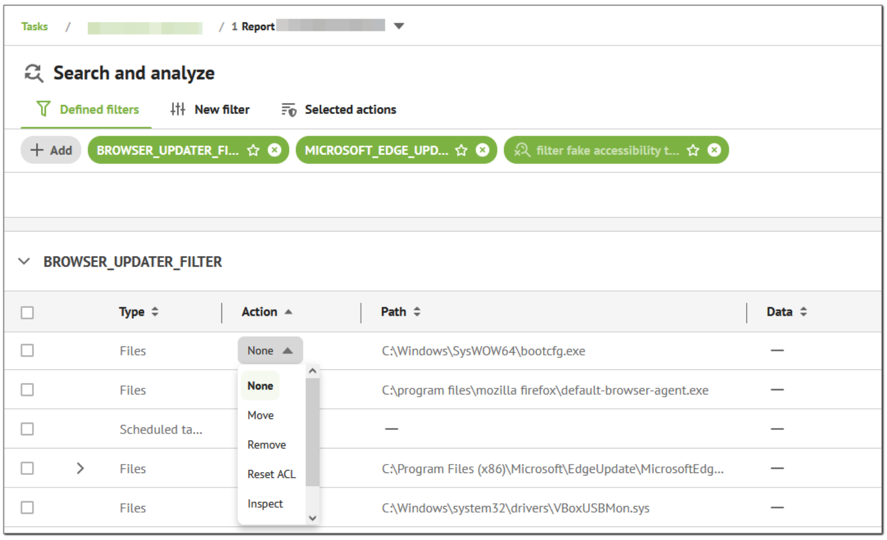
- **Type:** the object type.
- **Action:** an action that will be applied to the selected item.

The other columns correspond to fields specified in the filter.

Actions

For each object found with the filter, you can select an action that will be applied to it by the curing FixIt! tool. Actions are used for resolving issues on the scanned computer. Different objects have different action available for them.

Available actions are displayed as a drop-down list in the **Action** column in the filter results table.



Tasks / [redacted] / 1 Report [redacted]

Search and analyze

Defined filters | New filter | Selected actions

+ Add | BROWSER_UPDATER_FI... ☆ ⊗ | MICROSOFT_EDGE_UPD... ☆ ⊗ | filter fake accessibility t... ☆ ⊗

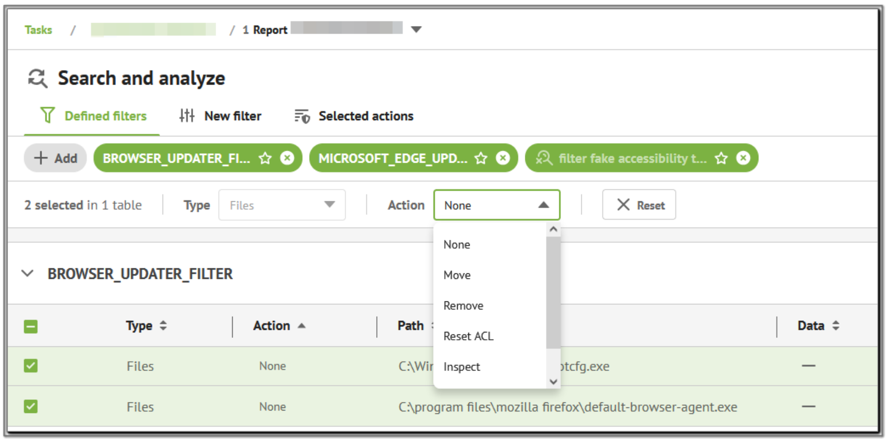
BROWSER_UPDATER_FILTER

□	Type	Action	Path	Data
□	Files	None	C:\Windows\SysWOW64\bootcfg.exe	—
□	Files		C:\program files\mozilla firefox\default-browser-agent.exe	—
□	Scheduled ta...		—	—
□	Files		C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdg...	—
□	Files		C:\Windows\system32\drivers\VBoxUSBMon.sys	—

Figure 10. Selecting actions for a file

To select several objects at once, select the corresponding check boxes. To select all objects on the current page of the filter table, select the check box in the column header.

If you select check boxes against objects, a group action menu will appear above the table.



Tasks / [redacted] / 1 Report [redacted]

Search and analyze

Defined filters | New filter | Selected actions

+ Add | BROWSER_UPDATER_FI... ☆ ⊗ | MICROSOFT_EDGE_UPD... ☆ ⊗ | filter fake accessibility t... ☆ ⊗

2 selected in 1 table | Type: Files | Action: None | ✕ Reset

BROWSER_UPDATER_FILTER

▣	Type	Action	Path	Data
☑	Files	None	C:\Wir...otcfg.exe	—
☑	Files	None	C:\program files\mozilla firefox\default-browser-agent.exe	—

Figure 11. Selecting group action

To select action for a group of objects

1. Select the check boxes against objects you want to apply actions to. You can select them in several filters at once.
2. Select an object type in the **Type** drop-down menu above the tables (if you have selected objects of more than one type).
3. Select the action you need to apply in the **Action** drop-down menu.
4. Do the same for each object type. Existing selections will be saved.

   To deselect all objects, click **Reset**.

> Please note that if you have already set actions for the selected objects, deselecting them will not reset the actions.

The table below lists all available actions and their descriptions.

Action	Description	Object type
Move	Relocate or rename the object	Files
Remove	Delete the object	Files, mium Extensions, Registry, Shortcuts, Firefox add-ons
Reset ACL	Install parent ACL for a file or directory	Files, Registry
Inspect	Get additional information about the object	Files, Processes, Drivers, Registry
Disinfect	Cure the object	Files, Registry startups, Registry, Non-signature detections, DNS settings, Internet Explorer settings, Proxy settings
Execute	Start the process	Processes
Kill	Terminate the process	
Suspend	Freeze the process	
Start	Start the service	Services
Stop	Stop the service	
Control	Send the control code to the service	

Action	Description	Object type
Delete	Delete the object	Services, Scheduled tasks, Namespace service providers, Layered service providers, WMI providers, WMI
Clear	Comment out ("#" + line) the specified strings from the HOSTS file	HOSTS file
	Remove the URL from browser configuration	Firefox configuration, Chromium configuration
Cure	Cure the object	Signature detections
Run	Start the task	Scheduled tasks
Set Value	Set value for the key	Registry

Actions represent the commands that will be included into the curing FixIt! tool (see Tool commands).

Actions selected for each object are displayed on the Selected actions tab.

13.2. New Filter

On the **New filter** tab, you can create a new filter. You can edit an defined filter and save it as new, or create a new filter from scratch. The tab also allows you to:

- Edit filters
- Delete filters
- Create filter groups
- Run search queries using existing filters or fill in the query and field values manually
- Apply actions to threats

Filter structure

A filter consists of:

- **Query**, which is used for searching across data. A query consists of arguments (that is, categories of objects you are searching for) and their values (that is, parameters of objects that belong to categories).
- **Fields**, which define what data is displayed in the search results. One filter can include multiple fields, separated by commas.

The **Query** field also allows for standard search queries, such as name of a file you have already determined as malicious. The only difference is that you have to enter fields for the results to show. Fields will be displayed as columns in a table with search results.

For example, if you enter the `path` field, the results will show paths to the found files; the `state` field will show the state of the found objects; and the `hash.sha256` field will show SHA256 fingerprints.

> FixIt! allows you to use wildcard characters '*' and '?' in searches. The asterisk '*' stands for any number of characters, including zero, and the question mark '?' stands for any single character.
>
> The `files*` search query will return files with such names as `files`, `files111`, `files systems`, `files_more_worlds`, etc.
>
> The `files?` query will return files with such names as `files1`, `filess`, `files_`, but not `files`.

Refer to the Making queries section for more details about queries.

Access to filters

You can manage access to a filter by making it visible to other service users or to you only. The following access options are available:

- **All users**—the option is available only for administrators. The filter will be visible to all web service users.
- **This space**—the option is available only for managers and users. The filter will be visible to all space members.
- **Only me**—the option is available for all web service users. The filter will be visible only to the creator of the filter.
- **For current task**—the option is available for all web service users. The filter will be visible to all users working with this task.

Creating a new filter

Any web service user can create a new filter.

To create a filter

1. On the **New filter** tab, fill in the **Query and Fields** fields.

> To start a new line in the **Query** field, use the CTRL + ENTER shortcut.

2. Fill in **Fields**.
3. Click **Save as new filter**. The **Save filter** dialog appears.
4. In the **Name** field, enter the name of the filter.
5. (Optional) Add the filter to Favorites by enabling ☆ **Favourite** toggle.
6. (Optional) In the **Description** field, add detailed information for the filter.
7. In the **Available for** field, select who will see the filter.
8. (Optional) Select a group or create a new one by clicking + **New group** and filling in the required fields.
9. Click **Save**.

A notification is shown in the bottom left corner of the page if the filter is created successfully.

> ⚠ Please note that after saving, you will irreversibly change the filter for all web service users.

Editing or deleting a filter

Only administrators can edit and delete the filters of **For all** category. Any user of the web service can edit and delete the filters of **Space**, **Task** and **Only my** categories.

To edit a filter

1. On the **New filter** tab, click **Add**.
2. Choose the filter you want to edit and click **Add**.
3. Select the filtration parameters.
4. If you want to save the changes in the existing filter:

- Click **Save changes** and confirm this action in the pop-up.

> ⚠ Please note that after saving, you will irreversibly change the filter for all service users who can see it.

If you want to save the changes as a new filter:

- Click **Save as new filter**.

You can discard unsaved changes in the filter by clicking ↺ **Reset**.

After saving the changes you can use the newly created filter as a defined filter.

To delete a filter

1. On the **New filter** tab, click **Add**.

2. Choose the filter you want to delete and click **Add**.
3. Click 🗑 **Delete**.
4. Confirm the action in the pop-up window.

> ⚠ If you have deleted a filter by mistake, you have several seconds to cancel this action by clicking **Undo** in the pop-up notification appeared at the top of the page.

Quick applying of a filter

You can fill in **Query** and **Fields** on the **New Filter** tab and apply the filter right away without saving it.

To apply a filter quickly (without saving it)

1. On the **New filter** tab, fill in the **Query** and **Fields** fields.
2. Click **Apply**.

> ⚠ To apply a filter, you can also press the ENTER key in **Query** or **Fields**.

13.2.1. Making Queries

A **Query** is a part of a FixIt! filter that defines categories of objects, data on which you want to view.

The other part, **Fields**, defines the categories of data on the selected object categories.

This section contains information on *queries*.

Query structure and syntax

A query consists of:

- arguments (categories of objects you search for)
- values (parameters of certain objects within a category)

One query can contain several conditions, combined by logical operators. To group conditions together, use brackets `(...)`.

Example:

```
category_name: "files" AND arkstatus.file: (ts_malware OR ts_suspicious)
```

This query will return all objects with the type File, whose value of `arkstatus.file` corresponds to malicious and suspicious files.

Query operators

The main operators used to combine conditions in queries are *AND*, *OR* и *AND NOT*.

- The AND operator helps find elements that match *all conditions at once*. It can be replaced with the (+) character before the value.
- The OR operator helps find elements that match *any one of the conditions*.
- The AND NOT operator helps find elements that *do not match any conditions* defined after it. It can be replaced with the (–) character before the value.

You can also use character operators in queries.

See the list of character operators and their description in this table.

Operator	Value
.	Replaces any character. Example: `ab.` will return `aba`, `abb`, `abz`, etc.
?	Makes the preceding character optional. Example: `abc?` will return `ab` and `abc`.
+	Repeats the preceding character at least once. Example: `ab+` will return `ab`, `abb`, `abbb`, etc.
*	Repeats the preceding character any number of times, including zero. Example: `ab*` will return `a`, `ab`, `abb`, `abbb`, etc.
{...}	Curly brackets can contain the number of repetitions of the preceding character. Two numbers will represent min and max values. Example: • `a{2}` will return `aa` • `a{2,4}` will return `aa`, `aaa`, and `aaaa` • `a{2,}` will return `a` repeated twice and more times.
|	Corresponds to the OR operator. Results will match either left or right part of the query divided with this character. Example: `abc|xyz` will match `abc` and `xyz`.
(...)	Combines values in groups. Such a group will be treated as a single value. Example: `abc(def)?` will return `abc` and `abcdef`, but not `abcd`.

[...]	Returns results matching one of the values within brackets. Example: `[abc]` will return `a`, `b`, `c` Inside the square brackets, the hyphen (`-`) indicates a range unless - is the first character or escaped using the `\` character. Example: • `[a-c]` will return `a`, `b`, or `c` • `[-abc]` will return `-`, `a`, `b`, or `c` (the hyphen will be treated as the first value) • `[abc\-]` will return `a`, `b`, `c`, or `-` (the hyphen is escaped)
^	When put before a value in square brackets, the `^` character excludes this value or range of values from results. Example: • `[^abc]` will return everything but `a`, `b`, or `c` • `[^a-c]` will return everything but `a`, `b`, or `c` • `[^-abc]` will return everything but `-`, `a`, `b`, or `c` • `[^abc\-]` will return everything but `a`, `b`, `c` , or `-`.

Value ranges

For objects with the data types ‘date’, ‘integer’, or ‘string’, you can specify ranges in queries.

- If both upper and lower bound are included in the required range, use square brackets `[...]`: `[min TO max]`
- If both upper and lower bound are excluded from the required range, use curly brackets `{...}`: `{min TO max}`
- If only one of the bounds is included in the range, use both types of brackets: `[min TO max}`
- If the range only has one bound, use the `*` character: `[min TO *]`

You can also use simplified syntax for ranges.

For ranges with one bound:

- `size:>10`
- `size:>=10`
- `size:<10`
- `size:<=10`

Ranges with both bounds require grouping of conditions when using simplified syntax:

- `size:(>=10 AND <20)`
- `size:(+>=10 +<20)`

13.3. Selected Actions

The **Selected actions** tab displays actions that were set for the objects on the **Defined filters** tab. These actions will be performed on the objects when a curing FixIt! tool is running. What actions can be done depends on the object properties.

The **Selected actions** tab allows you to:

- view selected actions,
- change selected actions,
- proceed with creating a curing FixIt! tool that incorporates the selected actions.

Objects with selected actions are listed on the **Selected actions** tab in drop-down blocks corresponding to object types. For each object type, a table with object parameters of this type is displayed. The first table column shows actions selected for each object. You can sort the table data in descending/ascending order by clicking ▲▼ in the column of the table containing the data you want the table to be sorted by.

To refresh the list of objects with selected actions

- Click ⟳ **Refresh**.

To change a selected action

1. Click the selected object action.
2. Choose a new action in the drop-down list.

To create a FixIt! tool with the selected actions

- Click **Create** on the **Selected actions** tab. The FixIt! tool tab will open.

14. FixIt! Tool

A FixIt! tool is an executable (*.exe) file that collects system data and generates a detailed report. A FixIt! tool inspects:

- Installed programs and updates.
- Launched and launchable processes.
- Suspicious registry entries and their relations to other objects.
- Installed drivers and browser extensions.
- Modules loaded into processes.
- System logs.
- Disk partitions.

Once you've analyzed a report, you can add curing commands to a FixIt! tool. Beyond data collection, this tool will address issues and neutralize detected threats on the scanned computer.

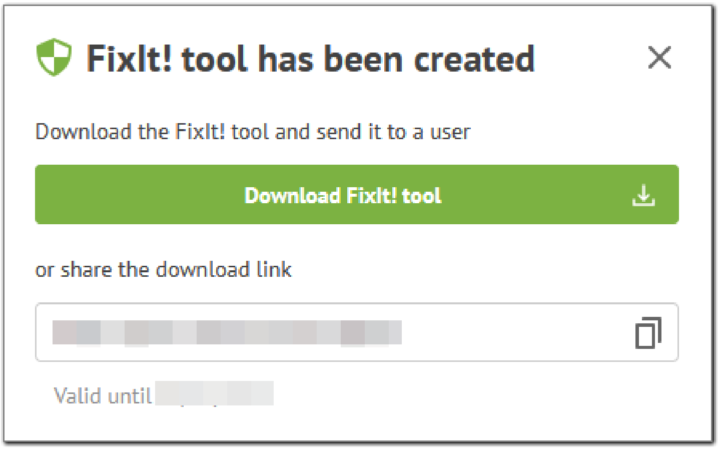
A tool that collects data is called *an analyzing tool*, while one that fixes issues are referred to as *a curing tool*.

14.1. How to Create a FixIt! Tool

- If a task does not contain any uploaded reports:
  1. Open the task page.
  2. Click **Create FixIt! tool**.
  3. (Optional) Change FixIt! tool settings. To do this, click **Settings** in the bottom right corner of the **FixIt! tool** panel and specify the settings.
  4. (Optional) On the **FixIt! tool** panel, enter the commands you want to add to the script.
  5. Click **Create FixIt! tool**.
- If a task contains uploaded reports:
  1. Open the task page.
  2. Open a report from the list.
  3. At the left, select **FixIt! tool**.
  4. (Optional) Change FixIt! tool settings. To do this, click **Settings** in the bottom right corner of the **FixIt! tool** panel and specify the settings.
  5. (Optional) On the **FixIt! tool** panel, enter the commands you want to add to the script.
  6. Click **Create FixIt! tool**.

Once a FixIt! tool is created, a pop-up window appears allowing you to select how to deliver the tool to the scanned computer's user.

- If you want to save the tool to your computer and send it to a user of the scanned computer, click **Download FixIt! tool** and send the downloaded file.
- If you want a user of the scanned computer to download the tool, copy the link by clicking the ⧉ icon and send it to the user.



FixIt! tool has been created

Download the FixIt! tool and send it to a user

Download FixIt! tool

or share the download link

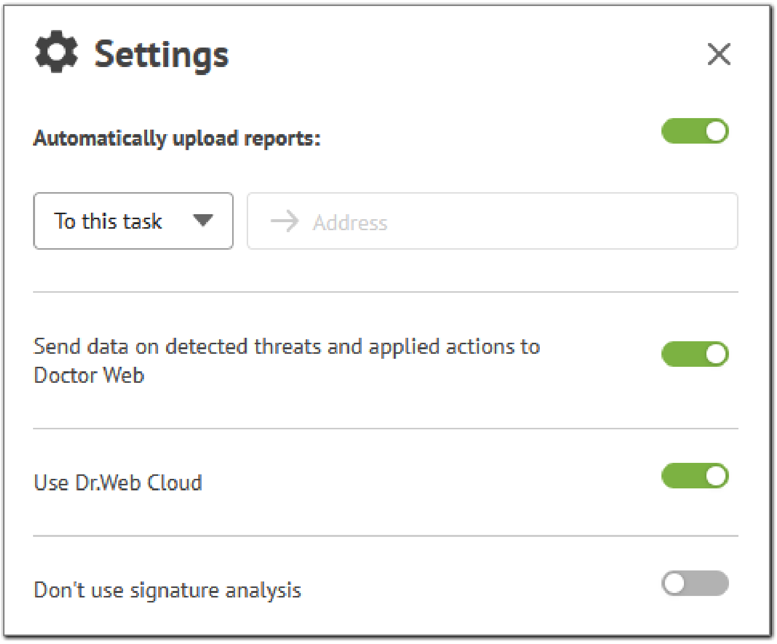
[redacted]

Valid until [redacted]

Figure 12. FixIt! tool has been created

14.2. Tool Settings

You can configure FixIt! tool settings before creating a tool. These settings will applied to all FixIt! tools created later in the task. To change the settings, create a FixIt! tool once again.



Settings

Automatically upload reports: ☑

To this task ▾ → Address

Send data on detected threats and applied actions to Doctor Web ☑

Use Dr.Web Cloud ☑

Don't use signature analysis ☐

Figure 13. FixIt! tool settings

The following table lists the descriptions of all FixIt! tool settings.

Setting	**Description**
Automatically upload reports to this task	Automatically upload reports to the task after system scan. It requires an active internet connection on the scanned computer. If the report is not uploaded to the task automatically, upload it manually. The report is saved locally on the scanned computer. You can find a link to the file in the FixIt! tool window after the scan is completed.
Automatically upload reports to URL	Automatically upload reports to the specified URL after system scan. To do it, the computer you are checking must be connected to the internet. If the report is not uploaded to the task automatically, upload it manually. The report is saved locally on the scanned computer. You can find a link to the file in the FixIt! tool window after the scan is completed.
Send data on detected threats and applied actions to Doctor Web	Send statistics on detected threats and applied actions to improve Doctor Web products. No personal data is sent.
Use Dr.Web Cloud	Use Dr.Web Cloud while scanning to improve threat detection. The cloud service stores information on threats which are not yet added to Dr.Web anti-virus databases. It also allows you to detect the latest threats without having to update the anti-virus databases on your computer.
Don't use signature analysis	Do not use Dr.Web Scanning Engine and Dr.Web anti-virus databases while scanning the system. The setting allows you to reduce the tool size. Recommended only if a Dr.Web anti-virus product is installed on the scanned computer.

14.3. Tool Commands

You can manually incorporate the needed data collecting and curing commands to a FixIt! tool.

Syntax

Each command starts on a new line and has the following format:

```
<Command name> <Options, arguments, or values separated by spaces>
```

Argument values can be string, binary, or numeric. A value is interpreted as a string unless stated otherwise.

Type	Description	Examples

String	If a value starts with a double quote `(")`, it is read up to the same closing double quote. Escaped quotes `(\")` are replaced with regular ones and interpreted as a part of the string.
	Otherwise, a value is read up to a space, comment, or the end of the line or file.
		`fs-remove c:\con`
		`fs-remove "c:\con 2"`

Binary	Values are read in pairs of HEX digits.	`0B8E` (2 bytes)

Numeric	Values are unsigned and represented either in decimal or hexadecimal format.	`15`
		`0xFE`

If you want to comment on a command, start the comment with the # symbol.

Code validation

Rows with syntax errors are marked with red. You can find error descriptions on the expandable > **Errors** panel below the command input area. To create a FixIt! tool, fix all the errors first.

List of commands

A script with commands is run sequentially in three steps:

1. Anti-rootkit scanner. These commands are executed in a random order.
2. Script commands. These commands are executed in the given order.
3. Data collection. These commands are executed in a random order.

14.3.1. Data Collection Commands

Data collection commands are used to get data on objects that were not included in the report during the regular data collection. To collect data on a specific object, add a data collection command to the script manually. To do this, enter the commands on the **FixIt! tool** tab.

Below, you will find a list of all the commands. To view the list in the service, click {i} **Commands** on the **FixIt! tool** tab.

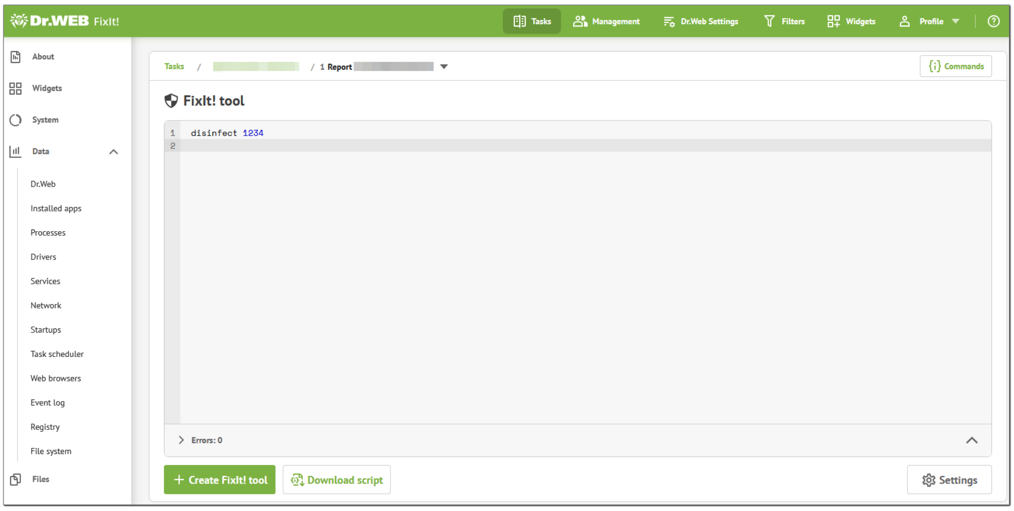
Command	Description
`inspect-fs [-r] [-p]` *<Path>*	Collect information about the file or directory. If the `-r` option is specified, data on the specified directory will be collected, as well as data on each file and subdirectory recursively.

Command	Description
	If the `-p` option is specified, then the parser of the file system (FAT/NTFS) will be used to retrieve the file list whenever possible. This is only valid for directories. The files go to the `ARTEFACTS` directory. Example: `inspect-fs -r "C:\Malware"` File names can be entered using a mask. A mask specifies the common part of a file name. At that: • the asterisk “*” character replaces any, possibly empty, sequence of characters; • the question mark “?” replaces only one character; • other mask characters do not replace anything and represent the exact same character. Examples: • report*.pdf defines all PDF documents whose names start with the word “report”. For example, report-february.pdf, report121209.pdf, etc.; • *.exe defines all EXE files, for example, setup.exe, iTunes.exe, etc. • photo????09.jpg defines all JPG images whose names start with the word "photo” and end with "09" and contain exactly four other characters in the middle. For example, photo121209.jpg, photoJohn09.jpg, photo----09.jpg, etc.
`inspect-reg` *<SID>* *<Key path>*	Collect information about the registry key. The possible values for *<SID>* are: `.DEFAULT`, `HKLM`, `HKCU`, `HKU`, and values starting with `S-1-5`. Example: `inspect-reg HKLM "SOFTWARE\Malware"`
`inspect-proc --pid` *<PID>* `/--imagename` *<Name>* `/--imagepath` *<Path>* `/ --cmdline` *<Command line>*	Collect information about the processes. The files go to the `ARTEFACTS` directory.

Command	Description
	Example: `inspect-proc --imagename win32calc.exe`
`inspect-disk` <*Disk ID*> <*Sector*> <*Number*>	Collect information about the disk sectors. The files go to the `ARTEFACTS` directory. Example: `inspect-disk 0 10 2`
`inspect-drv --imagebase` <*Image base*> / `--imagesize` <*Image size*> / `--imagename` <*Name*> / `--imagepath` <*Path*>	Collect information about the drivers with a specified base, size, name, or path to a file. The files go to the `ARTEFACTS` directory. Example: `inspect-drv --imagebase 0xfffff8064e540000`

14.3.2. Curing Commands

Once you receive the system status report, you can analyze the data (see Search and Analyze) using filters, apply actions to selected threats, and create a curing FixIt! tool with a specified curing script.



```
disinfect 1234
```

Errors: 0

Figure 14. Creating a curing FixIt! tool

You can add curing commands to the script manually. Commands correspond to object types.

Below, you will find all the available curing commands. I can also view a list of these commands directly in the service. To do this, click {i} **Commands** on the **FixIt! tool** tab.

Anti-rootkit scanner

Command	**Description**
`disinfect` *<ID>*	Cure the system object that has the specified internal identifier. It is usually applied to objects of the Non-signature detections type. The identifier is assigned to the object while generating a report. Example: `disinfect "10b2e828339cae479b1e5310b5980b717b7bcc57"`
`disinfect-reg` *<ID>*	Cure the registry startup item that has the specified internal identifier. It is applied to objects of the Scheduled tasks type. The identifier is assigned to the object while generating the report. Example: `disinfect-reg "629387a5dbc86d60842f12af5c43ffa5816140cc"`
`ark-disinfect --imagepath` *<Path>* `/ --sha256` *<Value>*	Neutralize the active object that has the specified parameter. If `Path` is specified, the file at the specified location will be deleted. The corresponding processes will also be stopped, if it is an executable file. If you specify a `SHA256` value, the system will search for files with that hash among active processes. If any files are found, they will be deleted. The corresponding processes will also be stopped. Example: `ark-disinfect --sha256 "71b969b079beba0db952399b918cdb6781aa5b5a1c3295129df92a0dd0fa457f"`

Script commands

Command	**Description**
Signature detections	
`cure-file` *<Path>*	Cure the file that has the detected threat signature. Actions (such as deleting, curing the content, replacing it, and additional system actions) are defined by the signature detected in the file. File

Command	Description
	location, its activity in the system, etc. are considered when curing by deleting. Additional actions such as pending delete, cleaning up startup items, blocking path till restart, etc. are performed if necessary. If the file is clean when invoking the command, nothing happens. Example: `cure-file C:\Windows\System32\malware.exe`
File system	
`fs-move` *<Source> <Destination>*	Move or rename the file or directory. If `Destination` is an existing directory, `Source` will be moved to `Destination`. Otherwise `Source` is renamed to `Destination`. Example: `fs-move c:\con c:\lpt1`
`fs-remove` *<Path>*	Delete the file or directory with the specified path. All remaining links between the object and other elements in the system will be specified at the end of the report. Example: `fs-remove c:\con`
`fs-reset-acl [-r]` *<Path>*	Set parent ACL for the file or directory. If the `-r` option is specified, ACL is set recursively for each file and subdirectory. If setting the ACL fails for the specified directory, the recursive traversal is stopped for the directory to avoid incorrect ACL setting for child elements. Example: `fs-reset-acl -r c:\test1\test2`
`fs-clear-ads` *<Path>*	Delete all ADS of the file or directory.

Command	**Description**
	Example: `fs-clear-ads C:\windows\explorer.exe`
Registry	

`reg-remove` *<SID>* *<Key path>* `[`*<Value>*`]`	Delete a value or key. *<SID>* is a profile specified in the registry.
	The possible values for *<SID>* are: `.DEFAULT`, `HKLM`, `HKCU`, `HKU`, and values starting with `S-1-5`.
	All remaining links between the object and other elements in the system will be specified at the end of the report.
	Examples:
	`reg-remove HKLM SOFTWARE\Test`
	`reg-remove HKLM SOFTWARE\Test Value`

`reg-set-value [-f]` *<SID>* *<Key path>* *<Value name>* *<Type>* *<Value data>*	Set a value for the specified key. *<SID>* is a profile specified in the registry.
	The possible values for *<SID>* are: `.DEFAULT`, `HKLM`, `HKCU`, `HKU`, and values starting with `S-1-5`.
	If the `-f` option is specified, parent keys are created (if they do not exist) and the key is overwritten with the new type.
	• To specify REG_SZ or REG_EXPAND_SZ type values, the string format is used.
	• To specify REG_BINARY or REG_MULTI_SZ type values, the binary format is used.
	• To specify REG_DWORD or REG_QWORD type values, the numeric format is used.
	Examples:
	`reg-set-value -f HKLM SOFTWARE\Test TestSZ REG_SZ "Test"`
	`reg-set-value -f HKLM SOFTWARE\Test TestBINARY REG_BINARY "5300530044005000530052005600"`
	`reg-set-value -f HKLM SOFTWARE\Test TestDWORD REG_DWORD 0x1`

Command	Description
`fs-reset-acl [-r]` *<Key path>*	Set parent ACL for the key. If the `-r` option is specified, ACL is reset recursively for each subkey. If setting the ACL fails for the specified directory, the recursive traversal is stopped for the directory to avoid incorrect ACL setting for child elements. Example: `reg-reset-acl -r HKLM SOFTWARE\Test`
Processes	

`proc-dump [-f] --pid` *<PID>* `/ --imagename` *<Name>* `/ --imagepath` *<Path>* `/ --cmdline` *<Command line>*	Generate a short or full (`-f`) memory dump for a process that meets given criteria. A dump is created in the temporary directory and then stored in the artefacts during report generation.
	Examples:
	`proc-dump --pid 4123`
	`proc-dump -f --imagepath C:\tools\procexp.exe`
	`proc-dump -f --cmdline C:\test\procexp64.exe`

`proc-execute [-w]` *<Path>* `[`*<Arguments>*`]`	Start the process at the specified path with the specified arguments. In the path, system variables can be used. Adding the `-w` flag makes the command wait until the process is done.
	Example:
	`proc-execute c:\Windows\System32\win32calc.exe`
	Examples with system variables:
	`proc-execute %TEMP%\sample.exe`
	`proc-execute \\/?\%windir%\notepad.exe`

`proc-kill --pid` *<PID> /* `--imagename` *<Name> /* `--imagepath` *<Path>* `/ --cmdline` *<Command line>*	Terminate the specified process.

Command	Description
	Example: `proc-kill --imagename win32calc.exe`
`proc-suspend --pid` *<PID>* / `--imagename` *<Name>* / `--imagepath` *<Path>* / `--cmdline` *<Command line>*	Freeze the specified process. Example: `proc-suspend --imagename win32calc.exe`
Services	
`svc-start` *<Name>*	Start the service with the specified name. Example: `svc-start TestService`
`svc-stop` *<Name>*	Stop the service with the specified name. Example: `svc-stop TestService`
`svc-delete` *<Name>*	Delete the service with the specified name. Information about remaining references (service-related files) is added to the end of the report. Example: `svc-delete TestService`
`svc-control` *<Name>* *<Control code>*	Send the control code to the service with the specified name. Example: `svc-control TestService 3`
Scheduled tasks	
`task-run` *<Path>*	Start the task with the specified name. Example: `task-run \Microsoft\Windows\TestTask`
`task-delete` *<Path>*	Delete the task with the specified name.

Command	**Description**
	Information about unprocessed references from the object to files is added to the end of the report. Example: `task-delete \Microsoft\Windows\TestTask`
Layered service providers	
`lsp-delete` *<GUID>*	Delete registered providers with the specified `GUID`. Example: `lsp-delete {f9eab0c0-26d4-11d0-bbbf-00aa006c34e4}`
Namespace service providers	
`nsp-delete` *<GUID>*	Delete registered providers with the specified `GUID`. Example: `nsp-delete {6642243a-3ba8-4aa6-baa5-2e0bd71fdd83}`
WMI providers	
`wmi-delete-eventconsumer` *<Namespace>* *<Class>* *<Name>*	Delete a WMI EventConsumer object from a specified namespace. Example: `wmi-delete-eventconsumer ROOT\subscription CommandLineEventConsumer CommandLineTemplate`
`wmi-query` *<Namespace>* *<Query>* *<Values>*	Run a WMI query and write returned values to a log. Example: `wmi-query root\cimv2 SELECT * FROM Win32_Process Name,ProcessId,CommandLine,ThreadCount,WorkingSetSize`
HOSTS file	
`hosts-clear` *<Path>* *<String>* `[`*<Strings>*`]`	Comment out ("#" + line) the specified strings from the HOSTS file. Numbering starts with 1.

Command	**Description**
	Example: `hosts-clear c:\Windows\System32\drivers\etc\hosts 44 45 46`
`hosts-default` *<Path>*	Restore the standard HOSTS file for the system. Example: `hosts-default c:\Windows\System32\drivers\etc\hosts`
`hosts-cure` *<Path>*	Check all entries in the HOSTS file and comment out those that contain malicious IP addresses. The command also adds the entry `# cured by Dr.Web`. Example: `hosts-cure c:\Windows\System32\drivers\etc\hosts`
Browser extensions and configuration	

`chromium-remove-ext` *<Browser>* *<SID>* *<Profile>* *<Extension ID>*	Remove the browser extension for the specified profile.
	The possible values for *<SID>* are: `.DEFAULT`, `HKLM`, `HKCU`, `HKU`, and values starting with `S-1-5`.
	Examples:
	`chromium-remove-ext Chrome S-1-5-21-120241661-1916511805-682617159-1001 default geadmilgigoffmcnlfdlpihockonlopf`
	`chromium-remove-ext Opera S-1-5-21-120241661-1916511805-682617159-1001 "" geadmilgigoffmcnlfdlpihockonlopf`

`firefox-remove-ext` *<Browser>* *<SID>* *<Profile>* *<Extension ID>*	Remove the browser extension for the specified profile. The possible values for *<SID>* are: `.DEFAULT`, `HKLM`, `HKCU`, `HKU`, and values starting with `S-1-5`.

Command	Description
	Example: `firefox-remove-ext Firefox S-1-5-21-120241661-1916511805-682617159-1001 default default-theme@mozilla.org`
`chromium-clear` *<Browser>* *<SID>* *<Profile>* *<URL>*	Remove the URL from browser configuration for the specified profile. The possible values for *<SID>* are: `.DEFAULT`, `HKLM`, `HKCU`, `HKU`, and values starting with `S-1-5`. Example: `chromium-clear Chrome S-1-5-21-120241661-1916511805-682617159-1001 Default malware.com`
`firefox-clear` *<Browser>* *<SID>* *<Profile>* *<URL>*	Remove the URL from browser configuration for the specified profile. The possible values for *<SID>* are: `.DEFAULT`, `HKLM`, `HKCU`, `HKU`, and values starting with `S-1-5`. Example: `firefox-clear Firefox S-1-5-21-120241661-1916511805-682617159-1001 default malware.com`
Dr.Web	
`drweb-remove`	Remove Dr.Web software and/or all of its traces from the system. Example: `drweb-remove`
Users	
`user-delete` *<User name>*	Delete a specified user in a workstation.
System	
`reboot [-f]`	Reboot the system with a 1-minute countdown timer in a system dialog box. The command will stop the generation of a report.
`shutdown [-f]`	Shut down the system with a 1-minute countdown timer in a system dialog box. The command will stop

Command	Description
	the generation of a report.

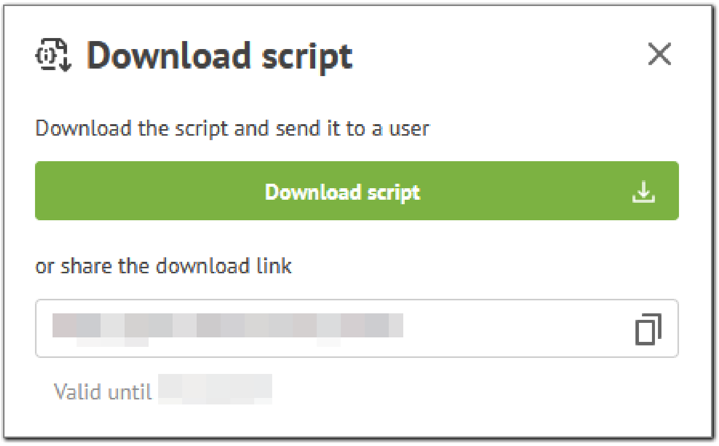
14.4. Script

You can download a command sequence (*a script*) shown in the command area on the **FixIt! tool** panel as a CFG file and send it to a user as an alternative to sending a tool. For instance, if you previously sent a FixIt! tool to the user and now want to scan the computer again, adding new commands to the tool (i.e. curing commands).

To send a script to a user

1. Open the task page.
2. Open a report from the list.
3. At the left, select **FixIt! tool**.
4. On the **FixIt! tool** panel, enter the commands you need to add to the script.
5. Click **Download script**.

Once a FixIt! tool has been created, the following window appears. There you can choose how to deliver the tool to a user of a scanned computer.



Download the script and send it to a user

or share the download link

[redacted]

Valid until [redacted]

Figure 15. The Download script window

- If you want to download the script and send it to a user of a scanned computer, click **Download script** and then send the downloaded file.
- If you want a user of a scanned computer to download the script, copy the link by clicking the ⧉ icon and send it to the user.

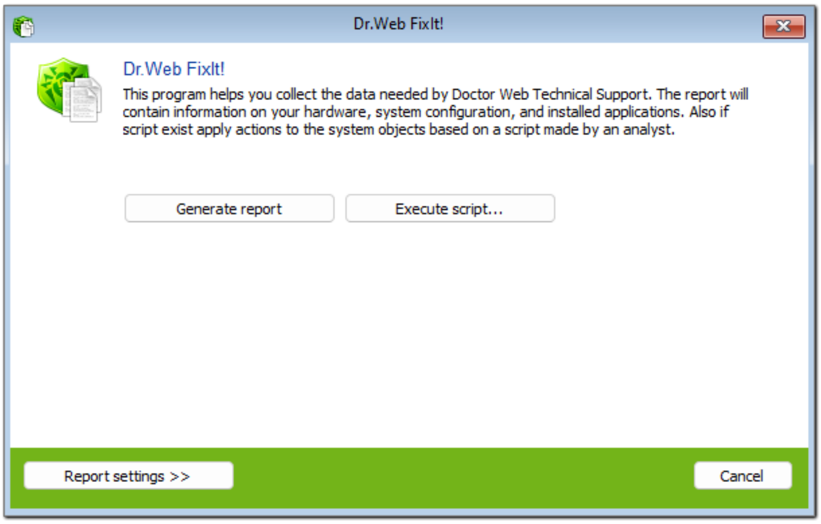
14.5. How to Scan a Computer with a FixIt! Tool

This section is for users of scanned computers.

A FixIt! tool does not require installation. To start work, simply run the executable tool file on a computer you need to scan.

To Scan a Computer with a FixIt! Tool

1. Run the FixIt! tool executable file on your computer. The FixIt! tool home screen appears.
2. (Optional) Change the default report settings and path to a folder where the report should be saved.
3. Click **Generate report**. The tool will collect information about your computer.

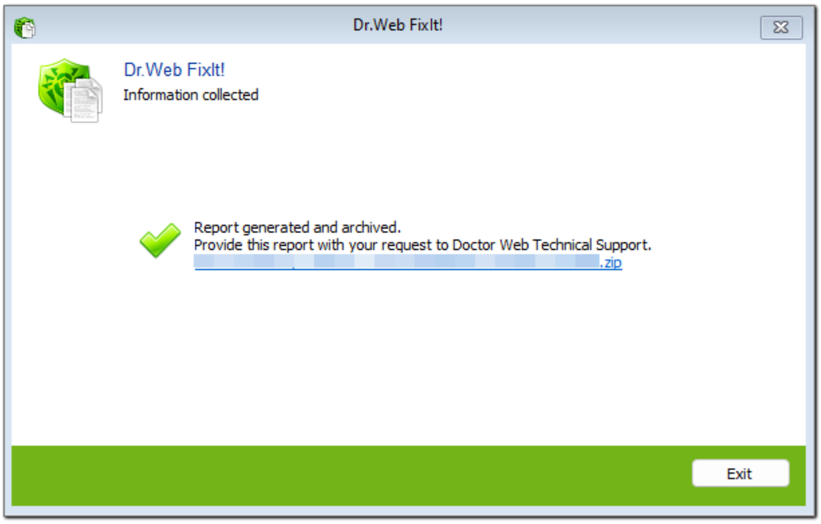

Dr.Web FixIt!

This program helps you collect the data needed by Doctor Web Technical Support. The report will contain information on your hardware, system configuration, and installed applications. Also if script exist apply actions to the system objects based on a script made by an analyst.

Figure 16. FixIt! tool home screen

If you need to stop collecting data, click **Cancel**. A terminated process cannot be resumed, so you will have to run the FixIt! tool again.

Once the scanning is done, a FixIt! tool will generate a ZIP archive containing the report in the folder specified in the report settings. The default path is `C:\Users\`<*User*>`\Doctor Web`. A text file with the `.zip_password.txt` extension containing a ZIP-archive password is saved to the same folder. The link to the file is displayed in the FixIt! tool window.



Dr.Web FixIt!
Information collected

Report generated and archived.
Provide this report with your request to Doctor Web Technical Support.
[redacted].zip

Figure 17. The link to the created report

Report settings

Before running a FixIt! tool, you can choose the data included in a report. To do this, run the executable FixIt! tool file on the scanned computer, click **Report settings** in the lower part of the FixIt! tool home screen and select the check boxes next to the data categories you want to include.

Additionally, you can specify a path to a folder where a ZIP archive containing a report should be saved. To do this, click **Browse**, choose the needed folder, then click **OK**.

Script

If you received a script from an operator, run it along with a FixIt! tool.

To run a script along with a FixIt! tool

1. Run a FixIt! tool executable file on your computer. The FixIt! tool home screen appears.
2. (Optional) Change the default report settings and path to a folder where the report should be saved.
3. Click **Execute script** and choose the script file that an operator sent to you. The FixIt! tool will automatically run together with the script.

15. Technical Support

If you should have any problems with product installation or running, consider the following options before contacting technical support:

- see the latest description and manual versions at https://download.drweb.com/doc/;
- read the frequently asked questions section at https://support.drweb.com/show_faq/;
- visit Dr Web forums at https://forum.drweb.com/index.php.

If you couldn't find a solution to your problem, you can contact Dr Web technical support using the following ways:

- fill in a web form in the corresponding section at https://support.drweb.ru/fixit;
- call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-7932 (a toll-free line for customers within Russia).

For information about Dr Web regional and international offices, please visit our official website at https://company.drweb.com/contacts/offices/.

16. Appendix A. Use Case

Here we will study how we used Dr.Web FixIt! to find and cure the Trojan.AutoIt.289 malware on a user's computer.

Stated Problem

A user was concerned that for an unknown reason, they could not open the website of an anti-virus product to activate a trial version.

We used Dr.Web FixIt! to look into the issue.

Solution

As usual, we started by going through our standard preparation steps:

- created a task
- generated the analyzing tool
- sent the tool to the user
- uploaded the report on the state of the system

We will not describe those steps in detail here, because they are simple and always the same. You can read more about them in the Task section.

Working with Report

The main event started when we received the report with the system analysis.

We went to the **Search and analyze** tab of the report to start by filtering out malicious and suspicious files.

We selected the following filters from the **General** group:

- Downloaded files
- Scripting language interpreters
- New executables
- Rootkits
- Unsigned executables
- Files with unusual arkstatus
- Suspicious software
- Hacktools software
- Files with unusual certificates

the following filters from the **Detects** group:

- Cloud URL detects
- Non-signature detects
- Signature detects
- Reputation-based detects

and the filter from the **Heuristics** group:

- Unsigned untrusted executables

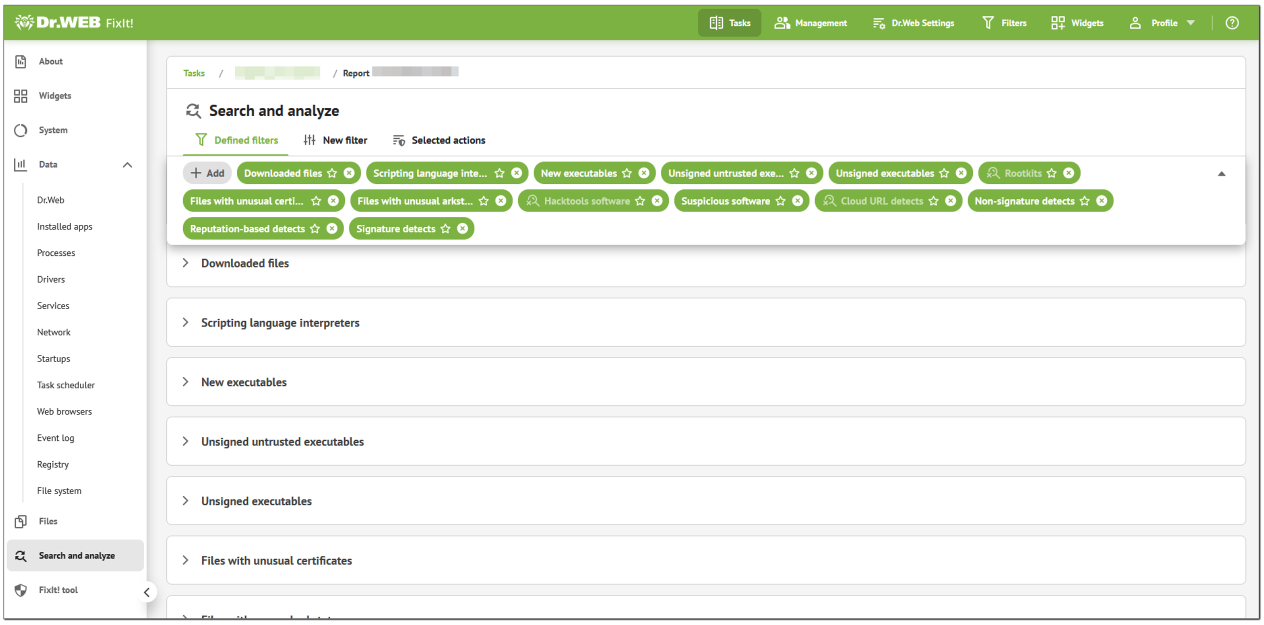


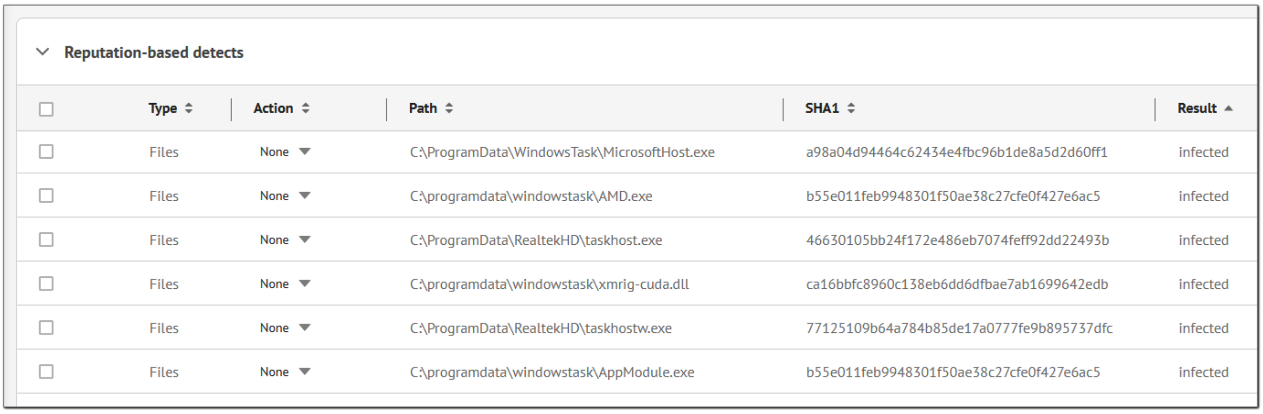
Figure 18. Selected filters

This is a standard set of filters that can help you find the majority of threats.

General filters are heuristic. We use them to look for unsigned, hidden, and generally suspicious files. If a file is detected by one of those filters, it does not automatically mean that the file is malicious, but if we add information from other filters, then we are able to draw conclusions.

Filters in the **Detects** section, as the name suggests, help us look for detectable malicious files. It greatly helps narrow the search from the start, so we started the analysis from there.

After a bit of looking around, we found a likely suspect amongst the **Reputation-based detects**. This filter displays verdicts from Doctor Web’s Metawave reputation database, that is, files that were at some point detected as infected, suspicious, coming from a suspicious vendor, or clean.



Reputation-based detects

□	Type	Action	Path	SHA1	Result
□	Files	None	C:\ProgramData\WindowsTask\MicrosoftHost.exe	a98a04d94464c62434e4fbc96b1de8a5d2d60ff1	infected
□	Files	None	C:\programdata\windowstask\AMD.exe	b55e011feb9948301f50ae38c27cfe0f427e6ac5	infected
□	Files	None	C:\ProgramData\RealtekHD\taskhost.exe	46630105bb24f172e486eb7074feff92dd22493b	infected
□	Files	None	C:\programdata\windowstask\xmrig-cuda.dll	ca16bbfc8960c138eb6dd6dfbae7ab1699642edb	infected
□	Files	None	C:\ProgramData\RealtekHD\taskhostw.exe	77125109b64a784b85de17a0777fe9b895737dfc	infected
□	Files	None	C:\programdata\windowstask\AppModule.exe	b55e011feb9948301f50ae38c27cfe0f427e6ac5	infected

Figure 19. Reputation-based detects

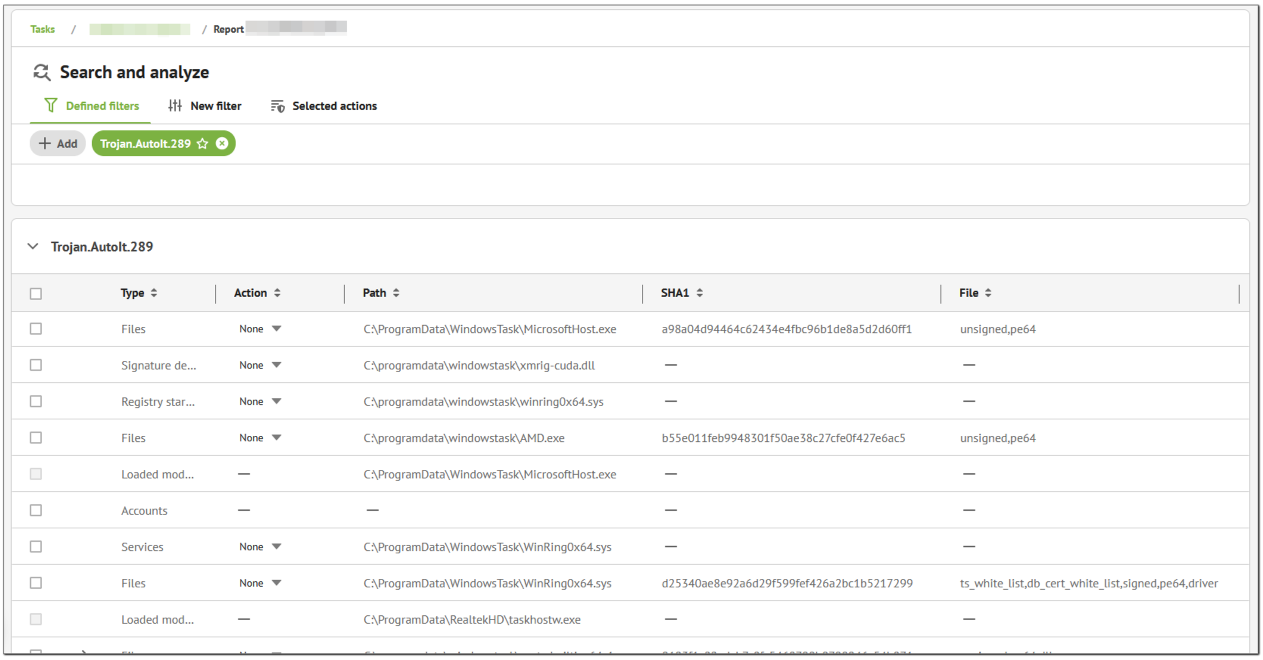
It showed us several files labeled as *infected*, including the widely known `xmrig-cuda.dll` malicious library, but our biggest find was the file `C:\ProgramData\RealtekHD\taskhostw.exe`, the signature move of *Trojan.AutoIt.289*. As soon as we saw it, we knew that the user’s computer was infected by this trojan.

Considering that Trojan.AutoIt.289 tends to come up often in our work, FixIt! has a specialized filter for it. We selected it to find all affected files and processes.

The Trojan.AutoIt.289 Filter

The **Trojan.AutoIt.289** filter displays files, processes, and startup elements affected by this trojan.

We selected this filter on the **Defined filters** tab and expanded the table to view results.



Tasks / [redacted] / Report [redacted]

Search and analyze

Trojan.AutoIt.289

□	Type	Action	Path	SHA1	File
□	Files	None ▾	C:\ProgramData\WindowsTask\MicrosoftHost.exe	a98a04d94464c62434e4fbc96b1de8a5d2d60ff1	unsigned,pe64
□	Signature de...	None ▾	C:\programdata\windowstask\xmrig-cuda.dll	—	—
□	Registry star...	None ▾	C:\programdata\windowstask\winring0x64.sys	—	—
□	Files	None ▾	C:\programdata\windowstask\AMD.exe	b55e011feb9948301f50ae38c27cfe0f427e6ac5	unsigned,pe64
□	Loaded mod...	—	C:\ProgramData\WindowsTask\MicrosoftHost.exe	—	—
□	Accounts	—	—	—	—
□	Services	None ▾	C:\ProgramData\WindowsTask\WinRing0x64.sys	—	—
□	Files	None ▾	C:\ProgramData\WindowsTask\WinRing0x64.sys	d25340ae8e92a6d29f599fef426a2bc1b5217299	ts_white_list,db_cert_white_list,signed,pe64,driver
□	Loaded mod...	—	C:\ProgramData\RealtekHD\taskhostw.exe	—	—

Figure 20. The Trojan.AutoIt.289 filter

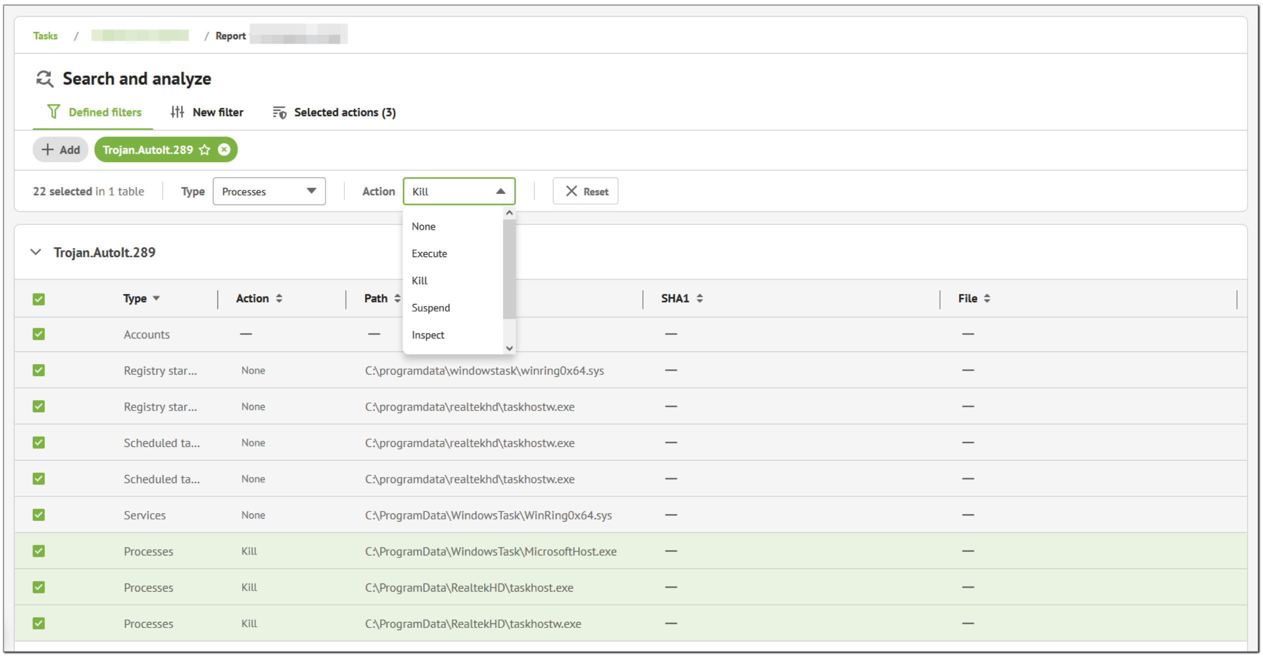
All we had to do next was to select an action for each element.

Curing

Actions vary for different element types. To group elements together, we selected the checkbox above the entire column. Note that only elements with available actions were selected (for instance, loaded modules have no action and they were not selected).

Then, we selected element types in the drop-down menu above the table and the respective action for each element, one by one.

For instance, for the **Processes** element type, we selected **Kill**, and it was applied to each element of this type.



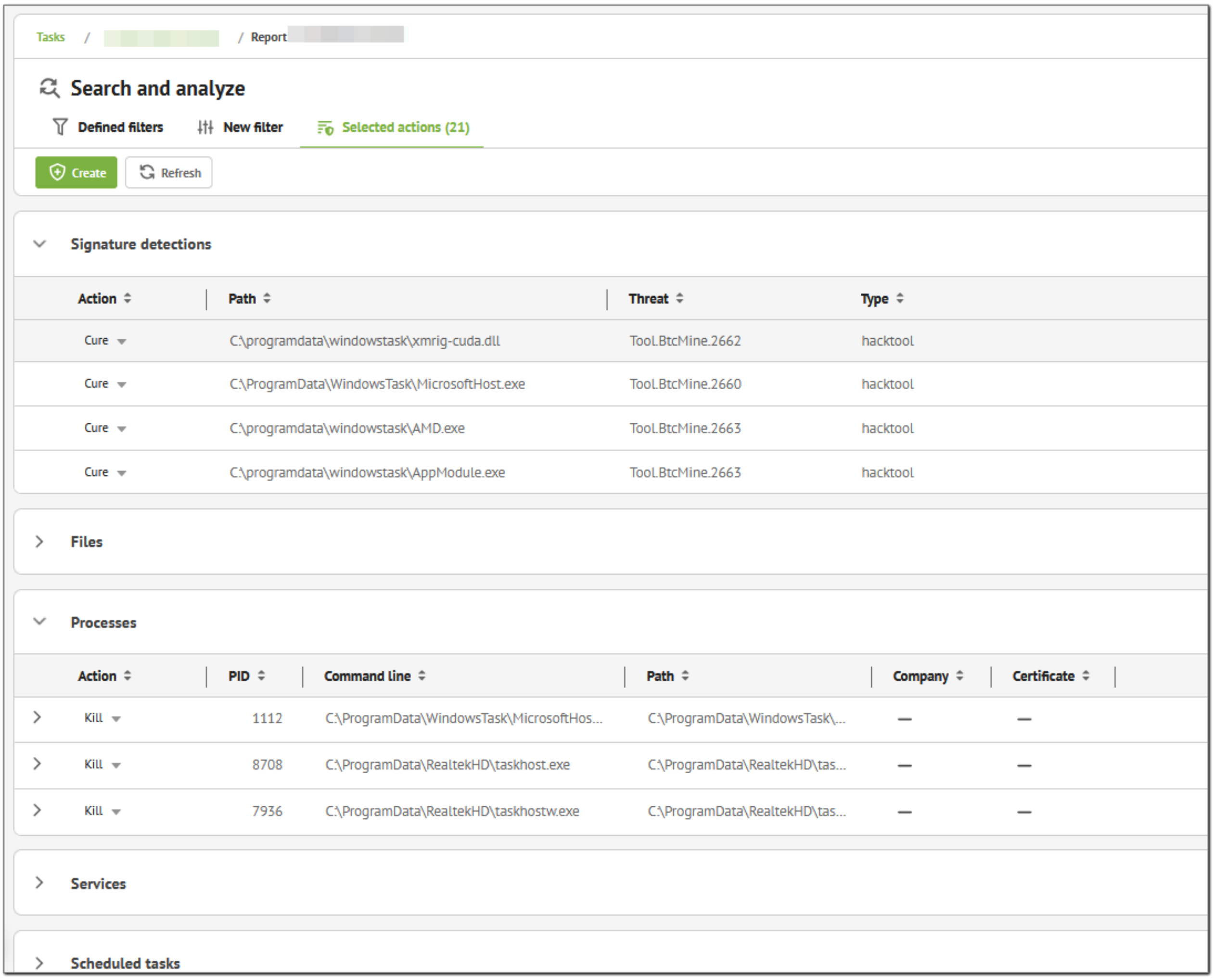
22 selected in 1 table | Type: Processes | Action: Kill

☑	Type	Action	Path	SHA1	File
☑	Accounts	—	—	—	—
☑	Registry star...	None	C:\programdata\windowstask\winring0x64.sys	—	—
☑	Registry star...	None	C:\programdata\realtekhd\taskhostw.exe	—	—
☑	Scheduled ta...	None	C:\programdata\realtekhd\taskhostw.exe	—	—
☑	Scheduled ta...	None	C:\programdata\realtekhd\taskhostw.exe	—	—
☑	Services	None	C:\ProgramData\WindowsTask\WinRing0x64.sys	—	—
☑	Processes	Kill	C:\ProgramData\WindowsTask\MicrosoftHost.exe	—	—
☑	Processes	Kill	C:\ProgramData\RealtekHD\taskhost.exe	—	—
☑	Processes	Kill	C:\ProgramData\RealtekHD\taskhostw.exe	—	—

Figure 21. Selecting actions for a file

Then we did the same for other element types, selecting for them **Cure**, **Delete**, and **Disinfect**, respectively.

Selected actions went on the Selected Actions tab for us to review.



Tasks / [redacted] / Report [redacted]

Search and analyze

Signature detections

Action	Path	Threat	Type
Cure	C:\programdata\windowstask\xmrig-cuda.dll	Tool.BtcMine.2662	hacktool
Cure	C:\ProgramData\WindowsTask\MicrosoftHost.exe	Tool.BtcMine.2660	hacktool
Cure	C:\programdata\windowstask\AMD.exe	Tool.BtcMine.2663	hacktool
Cure	C:\programdata\windowstask\AppModule.exe	Tool.BtcMine.2663	hacktool

Files

Processes

Action	PID	Command line	Path	Company	Certificate
Kill	1112	C:\ProgramData\WindowsTask\MicrosoftHos...	C:\ProgramData\WindowsTask\...	—	—
Kill	8708	C:\ProgramData\RealtekHD\taskhost.exe	C:\ProgramData\RealtekHD\tas...	—	—
Kill	7936	C:\ProgramData\RealtekHD\taskhostw.exe	C:\ProgramData\RealtekHD\tas...	—	—

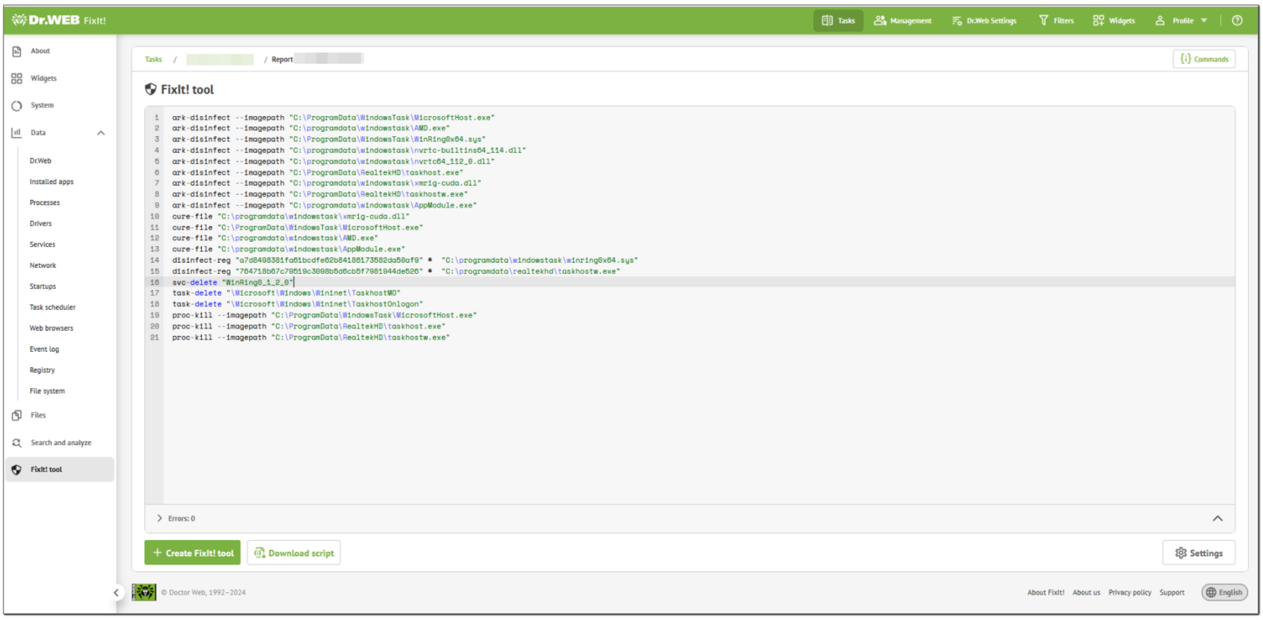
Services

Scheduled tasks

Figure 22. Selected actions

When we made sure that all required actions were properly saved, we clicked **Create** to generate a curing tool for the user.

Before creating the tool, FixIt! allowed us to review the script and add or edit commands manually as needed.



Tasks / [redacted] / Report [redacted]

FixIt! tool

```
ark-disinfect --imagepath "C:\ProgramData\WindowsTask\MicrosoftHost.exe"
ark-disinfect --imagepath "C:\programdata\windowstask\AMD.exe"
ark-disinfect --imagepath "C:\ProgramData\WindowsTask\WinRing0x64.sys"
ark-disinfect --imagepath "C:\programdata\windowstask\nvrtc-builtins64_114.dll"
ark-disinfect --imagepath "C:\programdata\windowstask\nvrtc64_112_0.dll"
ark-disinfect --imagepath "C:\ProgramData\RealtekHD\taskhost.exe"
ark-disinfect --imagepath "C:\programdata\windowstask\xmrig-cuda.dll"
ark-disinfect --imagepath "C:\ProgramData\RealtekHD\taskhostw.exe"
ark-disinfect --imagepath "C:\programdata\windowstask\AppModule.exe"
cure-file "C:\programdata\windowstask\xmrig-cuda.dll"
cure-file "C:\ProgramData\WindowsTask\MicrosoftHost.exe"
cure-file "C:\programdata\windowstask\AMD.exe"
cure-file "C:\programdata\windowstask\AppModule.exe"
disinfect-reg "a7d8498381fa61bcdfe62b84186173582da50af9" •  "C:\programdata\windowstask\winring0x64.sys"
disinfect-reg "764718b67c79519c3098b5d6cb5f7981944de526" •  "C:\programdata\realtekhd\taskhostw.exe"
svc-delete "WinRing0_1_2_0"
task-delete "\Microsoft\Windows\Wininet\TaskhostMO"
task-delete "\Microsoft\Windows\Wininet\TaskhostOnlogon"
proc-kill --imagepath "C:\ProgramData\WindowsTask\MicrosoftHost.exe"
proc-kill --imagepath "C:\ProgramData\RealtekHD\taskhost.exe"
proc-kill --imagepath "C:\ProgramData\RealtekHD\taskhostw.exe"
```

Figure 23. The resulting script

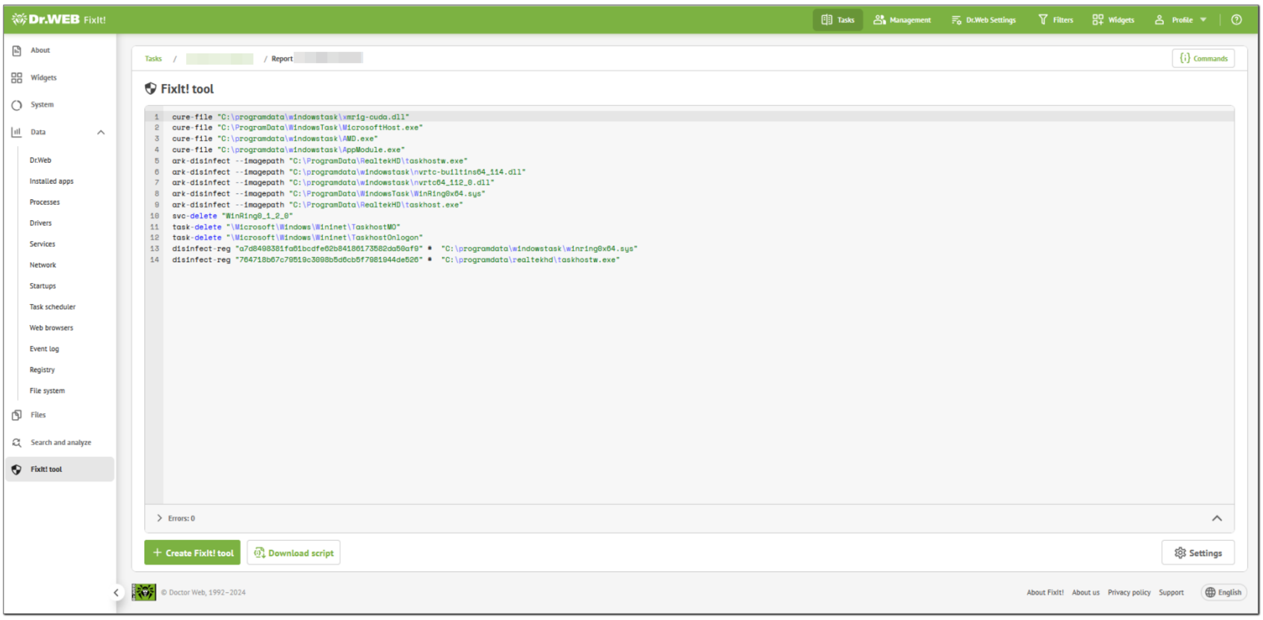
Optimizing

Although the script above is fully functional and able to solve the issues it was created for, an advanced FixIt! user can still optimize it, either when selecting actions or when reviewing the script.

What we found:

- Logically, the proc-kill commands should be placed in the script first, because all commands but the -inspect ones are run in the order of the script, and we have to kill the trojan's processes before we can cure the computer.
- When run, the cure-file and ark-disinfect commands kill the corresponding processes and remove startup elements, that is, all the other commands that do the same with the same objects can be safely removed from the script.
- The cure-file and ark-disinfect commands give essentially the same results when applied to the same object. In our case, some objects were detected both as **Signature detections** and **Files**, so that two kinds of actions could be applied to them, which we did before checking thoroughly whether it was necessary.

When we deleted all redundant commands from the script, it looked like the following.



```
cure-file "C:\programdata\windowstask\xmrig-cuda.dll"
cure-file "C:\ProgramData\WindowsTask\MicrosoftHost.exe"
cure-file "C:\programdata\windowstask\AMD.exe"
cure-file "C:\programdata\windowstask\AppModule.exe"
ark-disinfect --imagepath "C:\ProgramData\RealtekHD\taskhostw.exe"
ark-disinfect --imagepath "C:\programdata\windowstask\nvrtc-builtins64_114.dll"
ark-disinfect --imagepath "C:\programdata\windowstask\nvrtc64_112_0.dll"
ark-disinfect --imagepath "C:\ProgramData\WindowsTask\WinRing0x64.sys"
ark-disinfect --imagepath "C:\ProgramData\RealtekHD\taskhost.exe"
svc-delete "WinRing0_1_2_0"
task-delete "\Microsoft\Windows\Wininet\TaskhostMO"
task-delete "\Microsoft\Windows\Wininet\TaskhostOnlogon"
disinfect-reg "a7d8498381fa61bcdfe62b84186173582da50af9" •  "C:\programdata\windowstask\winring0x64.sys"
disinfect-reg "764718b67c79519c3098b5d6cb5f7981944de526" •  "C:\programdata\realtekhd\taskhostw.exe"
```

Figure 24. The optimized script

By pressing **Create** once again we generated the final version of our FixIt! curing tool and sent it to the user.

Result

After the user run the tool, we used the Compare reports feature to compare the resulting report with the previous one and made sure nothing suspicious was left on the affected computer.

17. Appendix B. The List of Fields

- artefacts_fs
- defender:computer_status
- defender:preference
- defender:threat
- defender:threat_detection
- disk_bootsect
- drivers
- drweb:bases
- drweb:components
- drweb:info
- drweb:launched_modules
- drweb:licenses
- drweb:products
- events
- files
- fixes
- hosts
- installed_apps
- modules
- msi_apps
- net_connections
- net_providers:namespaces
- net_providers:protocols
- processes
- services
- startups:mstasks
- startups:registry
- startups:wmi
- sysobj:chromium_config
- sysobj:chromium_extensions
- sysobj:detects
- sysobj:firefox_addons
- sysobj:firefox_config

- sysobj:ie
- sysobj:mstasks
- sysobj:proxy
- sysobj:registry
- sysobj:shortcuts
- sysobj:wmi
- system:accounts
- system:antivirus
- system:bios
- system:cpu
- system:dep
- system:dirs
- system:dns
- system:firewall
- system:hdd
- system:kernel_va_shadowing
- system:locale
- system:machine_scores
- system:mapped_disks
- system:memory
- system:net_adapters
- system:os
- system:persisted_routes
- system:policies
- system:routes
- system:secure_boot
- system:security_providers
- system:sessions
- system:shares
- system:smart
- system:speculation_control
- system:user_privelegies
- system:users
- system_reg_export
- winstore_apps

artefacts_fs

File artifacts

Field	Data type
analysis_results.metawave.datetime	date
analysis_results.metawave.result	text
analysis_results.metawave.status	text
category_name	text
hash.sha1	text
modify_datetime	date
path	text
sha1	text
size	long

defender:computer_status

The computer status based on Microsoft Defender data

Field	Data type
am_engine_version	keyword
am_product_version	keyword
am_service_enabled	boolean
am_service_version	keyword
antispyware_enabled	boolean
antispyware_signature_age	long

Field	Data type
antispyware_signature_last_updated	date
antispyware_signature_version	keyword
antivirus_enabled	boolean
antivirus_signature_age	long
antivirus_signature_last_updated	date
antivirus_signature_version	keyword
behavior_monitor_enabled	boolean
category_name	text
computer_id	text
computer_state	long
full_scan_age	long
full_scan_end_time	text
full_scan_start_time	text
ioav_protection_enabled	boolean
last_full_scan_source	long
last_quick_scan_source	long
nis_enabled	boolean
nis_engine_version	keyword
nis_signature_age	long
nis_signature_last_updated	date

Field	Data type
on_access_protection_enabled	boolean
quick_scan_age	long
quick_scan_end_time	date
quick_scan_start_time	date
real_time_protection_enabled	boolean
real_time_scan_direction	long

defender:preference

Microsoft Defender settings

Field	Data type
category_name	text
check_for_signatures_before_running_scan	boolean
computer_id	text
disable_archive_scanning	boolean
disable_auto_exclusions	boolean
disable_behavior_monitoring	boolean
disable_catchup_full_scan	boolean
disable_catchup_quick_scan	boolean
disable_email_scanning	boolean
disable_intrusion_prevention_system	text
disable_ioav_protection	boolean

Field	Data type
disable_privacy_mode	boolean
disable_realtime_monitoring	boolean
disable_removable_drive_scanning	boolean
disable_restore_point	boolean
disable_scanning_mapped_network_drives_for_full_scan	boolean
disable_scanning_network_files	boolean
disable_script_scanning	boolean
exclusion_path	text
high_threat_default_action	long
low_threat_default_action	long
maps_reporting	long
moderate_threat_default_action	long
quarantine_purge_items_after_delay	long
randomize_schedule_task_times	boolean
real_time_scan_direction	long
remediation_schedule_day	long
reporting_additional_action_time_out	long
reporting_critical_failure_time_out	long
reporting_non_critical_time_out	long
scan_only_if_idle_enabled	boolean

Field	Data type
scan_parameters	long
scan_purge_items_after_delay	long
scan_schedule_day	long
scan_schedule_quick_scan_time	date
scan_schedule_time	date
severe_threat_default_action	long
signature_au_grace_period	long
signature_definition_update_file_shares_sources	text
signature_disable_update_on_startup_without_engine	boolean
signature_fallback_order	text
signature_first_au_grace_period	long
signature_schedule_day	long
signature_schedule_time	date
signature_update_catchup_interval	long
signature_update_interval	long
submit_samples_consent	long
ui_lockdown	boolean
unknown_threat_default_action	long

defender:threat

Threats detected by Microsoft Defender

Field	Data type
category_id	long
category_name	text
did_threat_execute	boolean
is_active	boolean
resources	text
rollup_status	long
schema_version	keyword
severity_id	long
threat_id	long
threat_name	text
type_id	long

defender:threat_detection

Threat detection using Microsoft Defender

Field	Data type
action_success	boolean
additional_actions_bit_mask	long
am_product_version	keyword
category_name	text

Field	Data type
cleaning_action_id	long
current_threat_execution_status_id	long
detection_id	text
detection_source_type_id	long
domain_user	text
initial_detection_time	date
last_threat_status_change_time	date
process_name	text
remediation_time	text
resources	text
threat_id	long
threat_status_error_code	long
threat_status_id	long

disk_bootsect

Boot sectors of disks

Field	Data type
block.end_lba	text
block.start_lba	text
bytes_per_sector	integer
category_name	text

Field	Data type
cylinders	integer
gpt.header.backup_lba	text
gpt.header.disk_guid	text
gpt.header.first_usable_lba	text
gpt.header.header_crc	text
gpt.header.header_size	text
gpt.header.last_usable_lba	text
gpt.header.num_parts	text
gpt.header.part_entries_crc	text
gpt.header.part_entry_lba	text
gpt.header.primary_lba	text
gpt.header.reserved	text
gpt.header.revision	text
gpt.header.signature	text
gpt.header.sizeof_part_entry	text
gpt.partition.arkstatus	text
gpt.partition.attrib	text
gpt.partition.end_lba	text
gpt.partition.guid	text
gpt.partition.index	text

Field	Data type
gpt.partition.name	text
gpt.partition.start_lba	text
gpt.partition.type	text
id	integer
mbr.arkstatus	text
mbr.disk_signature	long
mbr.disk_signature	text
mbr.partition.arkstatus	text
mbr.partition.boot_id	integer
mbr.partition.boot_id	text
mbr.partition.index	integer
mbr.partition.index	text
mbr.partition.size_in_sectors	long
mbr.partition.size_in_sectors	text
mbr.partition.start_lba	long
mbr.partition.start_lba	text
mbr.partition.type	text
mbr.signature	integer
mbr.zero_padding	integer
media_type	integer

Field	Data type
part_style	text
sectors_per_track	integer
size	long
tracks_per_cylinder	integer

drivers

Drivers

Field	Data type
base	text
category_name	text
path	text
size	long

drweb:bases

Dr.Web anti-virus databases

Field	Data type
category_name	text
name	text
path	text
records	long
timestamp	date

Field	Data type
type	integer
version	text

drweb:components

Dr.Web components

Field	Data type
category_name	text
installation_datetime	date
name	text

drweb:info

Dr.Web product information

Field	Data type
bases_path	text
category_name	text
hash	text
hash_sha1	text
install_path	text
product_mode	text
product_type	text
product_version	text

Field	Data type
repo_path	text

drweb:launched_modules

Launched Dr.Web modules

Field	Data type
launched	boolean

drweb:licenses

Dr.Web licenses

Field	Data type
category_name	text
key.applications	text
key.created	date
key.expires	date
key.product_spec	text
key.product_type	text
key.products	text
key.subscription_expires	date
path	text
settings.app_control	text
settings.AppControl	text

Field	Data type
settings.file_server	text
settings.FileServer	text
settings.inet_gateway	text
settings.InetGateway	text
settings.lotus_spam_filter	text
settings.LotusSpamFilter	text
settings.mail_server	text
settings.MailServer	text
settings.spam_filter	text
settings.SpamFilter	text
settings.Users	text
settings.users	text
user.computers	integer
user.name	text
user.number	text

drweb:products

Dr.Web products

Field	Data type
category_name	text
installation_datetime	date

Field	Data type
name	text

engine_detects

Threats detected using signature databases

Field	Data type
category_name	text
path	text
threat	text
type	text

events

Events

Field	Data type
category	text
category_name	text
code	text
computer	text
content	text
id	text
index	text
instance_id	text

Field	Data type
keywords	text
logfile	text
msg	text
opcode	text
pid	text
source	text
task	text
tid	text
time	date
type	text
user	text

files

Files

Field	Data type
analysis_results.metawave.datetime	date
analysis_results.metawave.result	text
analysis_results.metawave.status	text
arkstatus.cert	text
arkstatus.cloud	text
arkstatus.confidence	text

Field	Data type
arkstatus.file	text
arkstatus.soft_type	text
arkstatus.soft_white	text
arkstatus.threat	text
arkstatus.type	text
atime	date
attrib.archive	boolean
attrib.compressed	text
attrib.dir	boolean
attrib.ea	text
attrib.hidden	boolean
attrib.invalid	boolean
attrib.normal	boolean
attrib.not_content_indexed	boolean
attrib.readonly	boolean
attrib.recall_on_open	text
attrib.reparse_point	text
attrib.security	text
attrib.sparse	text
attrib.system	boolean

Field	Data type
attrib.temporary	boolean
attrib.value	text
buildtime	date
category_name	text
certinfo.catfile	text
certinfo.creator_name	text
certinfo.creator_url	text
certinfo.item.alg	text
certinfo.item.ca	text
certinfo.item.eku	text
certinfo.item.flags	text
certinfo.item.from	date
certinfo.item.hash_alg	text
certinfo.item.hash_alg_type	text
certinfo.item.issuer.C	text
certinfo.item.issuer.CN	text
certinfo.item.issuer.DC	text
certinfo.item.issuer.L	text
certinfo.item.issuer.O	text
certinfo.item.issuer.OU	text

Field	Data type
certinfo.item.issuer.ST	text
certinfo.item.sn	text
certinfo.item.subject.C	text
certinfo.item.subject.CN	text
certinfo.item.subject.DC	text
certinfo.item.subject.L	text
certinfo.item.subject.O	text
certinfo.item.subject.OU	text
certinfo.item.subject.SERIALNUMBER	text
certinfo.item.subject.ST	text
certinfo.item.thumbprint	text
certinfo.item.thumbprint_sha256	text
certinfo.item.to	date
certinfo.timestamp	date
certinfo.type	text
ctime	date
device_characteristics	text
device_type	text
eainfo.item.data	text
eainfo.item.name	text

Field	Data type
eainfo.item.size	text
easize	integer
hash.pemd5	text
hash.pesha1	text
hash.pesha256	text
hash.pesha512	text
hash.sha1	text
hash.sha256	text
links	integer
path	text
signed	boolean
size	long
verinfo.company	text
verinfo.descr	text
verinfo.file_version_num	text
verinfo.origname	text
verinfo.product_name	text
verinfo.product_version	text
verinfo.product_version_num	text
verinfo.version	text

Field	Data type
wtime	date
zone_transfer.host_url	text
zone_transfer.id	text
zone_transfer.referrer_url	text
zone_transfer.package_name	text

fixes

Fixes

Field	Data type
__type__	text
caption	text
category.id	text
category.name	text
category_name	text
comment	text
csname	text
descr	text
hidden	text
id	text
installed_by	text
installed_on	date

Field	Data type
need_reboot	text

hosts

Hosts

Field	Data type
category_name	text
ip.address	ip
ip.category	text
ip.domain.address	text
ip.domain.category	text
line	integer
path	text
text	text

installed_apps

Installed applications

Field	Data type
category_name	text
hidden	text
id	text
location	text

Field	Data type
name	text
uninstall	text

modules

Modules

Field	Data type
category_name	text
path	text

msi_apps

MSI applications

Field	Data type
category_name	text
id	text
language	integer
msi_package_code	text
msi_product_code	text
name	text
vendor	text
version	text

net_connections

Network connections

Field	Data type
__type__	text
category_name	text
local_addr	ip
local_port	integer
local_scopeid	text
path	text
pid	integer
remote_addr	ip
remote_port	integer
remote_scopeid	text
state	text

net_providers:namespaces

Network providers (namespaces)

Field	Data type
active	boolean
broken	boolean
category_name	text
guid	text

Field	Data type
name	text
namespace	text
path	text
version	text
wow64	boolean

net_providers:protocols

Network providers (protocols)

Field	Data type
broken	boolean
category_name	text
entryid	text
flags	text
guid	text
name	text
path	text
protocol	text
scheme	text
version	text
wow64	boolean

processes

Processes

Field	Data type
appid	text
base	text
bit	integer
category_name	text
cmdline	text
create_time	date
curdir	text
handles	integer
ilevel	text
isdebugged	boolean
kernel_time	text
memory_usage.other_op	long
memory_usage.pagefaults	long
memory_usage.pagefile_usage	long
memory_usage.peak_pagefile_usage	long
memory_usage.peak_virtual_size	long
memory_usage.peak_workingset	long
memory_usage.quota_non_pagedpool	long

Field	Data type
memory_usage.quota_pagedpool	long
memory_usage.quota_peak_non_pagedpool	long
memory_usage.quota_peak_pagedpool	long
memory_usage.read_op	long
memory_usage.virtual_size	long
memory_usage.workingset	long
memory_usage.write_op	long
mitigations.aslr_policy.disallow_stripped_images	text
mitigations.aslr_policy.enable_bottom_up_randomization	text
mitigations.aslr_policy.enable_force_relocate_images	text
mitigations.aslr_policy.enable_high_entropy	text
mitigations.cfg_policy.enable_cfg	text
mitigations.cfg_policy.enable_export_suppression	text
mitigations.cfg_policy.strict_mode	text
mitigations.child_process_policy.allow_secure_process_creation	text
mitigations.child_process_policy.audit_no_child_process_creation	text
mitigations.child_process_policy.no_child_process_creation	text
mitigations.dynamic_code_policy.allow_remote_downgrade	text
mitigations.dynamic_code_policy.allow_thread_opt_out	text

Field	Data type
mitigations.dynamic_code_policy.audit_prohibit_dynamic_code	text
mitigations.dynamic_code_policy.prohibit_dynamic_code	text
mitigations.extension_point_disable_policy.disable_extension_points	text
mitigations.font_disable_policy.audit_non_system_font_loading	text
mitigations.font_disable_policy.disable_non_system_fonts	text
mitigations.image_load_policy.audit_no_low_mandatory_label_images	text
mitigations.image_load_policy.audit_no_remote_images	text
mitigations.image_load_policy.no_low_mandatory_label_images	text
mitigations.image_load_policy.no_remote_images	text
mitigations.image_load_policy.prefer_system32_images	text
mitigations.payload_restriction_policy.audit_export_address_filter	text
mitigations.payload_restriction_policy.audit_export_address_filter_plus	text
mitigations.payload_restriction_policy.audit_import_address_filter	text
mitigations.payload_restriction_policy.audit_rop_caller_check	text
mitigations.payload_restriction_policy.audit_rop_sim_exec	text
mitigations.payload_restriction_policy.audit_rop_stack_pivot	text

Field	Data type
mitigations.payload_restriction_policy.enable_export_address_filter	text
mitigations.payload_restriction_policy.enable_export_address_filter_plus	text
mitigations.payload_restriction_policy.enable_import_address_filter	text
mitigations.payload_restriction_policy.enable_rop_caller_check	text
mitigations.payload_restriction_policy.enable_rop_sim_exec	text
mitigations.payload_restriction_policy.enable_rop_stack_pivot	text
mitigations.redirection_trust_policy.audit_redirectiont_rust	text
mitigations.redirection_trust_policy.enforce_redirection_trust	text
mitigations.side_channel_isolation_policy.disable_page_combine	text
mitigations.side_channel_isolation_policy.isolate_security_domain	text
mitigations.side_channel_isolation_policy.smt_branch_target_isolation	text
mitigations.side_channel_isolation_policy.speculative_store_bypass_disable	text
mitigations.signature_policy.audit_microsoft_signed_only	text
mitigations.signature_policy.audit_store_signed_only	text
mitigations.signature_policy.microsoft_signed_only	text
mitigations.signature_policy.mitigation_opt_in	text

Field	**Data type**
mitigations.signature_policy.store_signed_only	text
mitigations.strict_handle_check_policy.handle_exceptions_permanently_enabled	text
mitigations.strict_handle_check_policy.raise_exception_on_invalid_handle_reference	text
mitigations.syscall_disable_policy.audit_disallow_win32k_syscalls	text
mitigations.syscall_disable_policy.disallow_win32k_syscalls	text
mitigations.systemcall_filter_policy.filter_id	text
mitigations.user_shadow_stack_policy.audit	text
mitigations.user_shadow_stack_policy.audit_block_non_cet_binaries	text
mitigations.user_shadow_stack_policy.audit_set_context_ip_validation	text
mitigations.user_shadow_stack_policy.block_non_cet_binaries	text
mitigations.user_shadow_stack_policy.block_non_cet_binaries_non_ehcont	text
mitigations.user_shadow_stack_policy.cet_dynamic_apis_out_of_proc_only	text
mitigations.user_shadow_stack_policy.enable	text
mitigations.user_shadow_stack_policy.enable_strict_mode	text
mitigations.user_shadow_stack_policy.set_context_ip_validation	text
mitigations.user_shadow_stack_policy.set_context_ip_validation_relaxed_mode	text

Field	Data type
module.arkstatus	text
module.base	text
module.buildtime	date
module.path	text
module.size	long
path	text
peb	text
pid	integer
ppid	integer
priority	integer
protection_level	text
section_info.checksum	text
section_info.committed_stack_size	long
section_info.dll_characteristics	text
section_info.image_characteristics	text
section_info.image_contains_code	boolean
section_info.image_file_size	long
section_info.image_flags	text
section_info.loader_flags	text
section_info.machine	text

Field	Data type
section_info.max_stack_size	long
section_info.os_major_ver	text
section_info.os_minor_ver	text
section_info.subsystem	text
section_info.subsystem_major_ver	text
section_info.subsystem_minor_ver	text
section_info.transfer_address	text
section_info.zero_bits	text
session_id	text
shell_info	text
shortcut	text
size	long
threads.count	text
threads.thread.base_priority	text
threads.thread.create_time	text
threads.thread.kernel_time	text
threads.thread.path	text
threads.thread.priority	text
threads.thread.start_address	text
threads.thread.state	text

Field	Data type
threads.thread.tid	text
threads.thread.user_time	text
threads.thread.win32_start_address	text
title	text
type	text
unique_id	text
user_time	text
window_flags	text

services

Services

Field	Data type
category_name	text
checkpoint	text
cmdline	text
controls_accepted	text
depends	text
display_name	text
error_control	text
flags	text
group	text

Field	Data type
name	text
path	text
pid	integer
start_name	text
startmode	text
state	text
svc_exitcode	text
tagid	text
type	text
waithint	text
win32_exitcode	text

startups:mstasks

Startup objects (task scheduler tasks)

Field	Data type
args	text
category_name	text
clsid	text
command	text
enabled	text
is_job	text

Field	Data type
name	text
path	text
state	text
type	text
workdir	text

startups:registry

Startup objects (registry)

Field	Data type
arkstatus	text
category_name	text
clsid	text
data	text
id	text
full_key	text
key	text
path	text
sid	text
value	text

startups:wmi

Startup objects (WMI)

Field	Data type
arkstatus	text
category_name	text
class	text
clsid	text
instance	text
name	text
namespace	text
path	text
value	text
workdir	text

sysobj:chromium_config

System objects (Chromium settings)

Field	Data type
browser	text
category_name	text
profile	text
sid	text
url	text

sysobj:chromium_extensions

System objects (Chromium extensions)

Field	Data type
browser	text
category_name	text
id	text
name	text
path	text
profile	text
sid	text
url	text
version	text

sysobj:detects

System objects (detected threats)

Field	Data type
category_name	text
data	text
id	text
object	text
path	text
threat	text

Field	Data type
type	text

sysobj:firefox_addons

System objects (Firefox addons)

Field	Data type
browser	text
category_name	text
id	text
name	text
path	text
profile	text
sid	text
type	text
url	text
version	text

sysobj:firefox_config

System objects (Firefox settings)

Field	Data type
browser	text
category_name	text

Field	Data type
profile	text
sid	text
url	text

sysobj:ie

System objects

Field	Data type
category_name	text
data	text
id	text
key	text
sid	text
value	text

sysobj:mstasks

System objects (task scheduler tasks)

Field	Data type
category_name	text
clsid	text
command	text
enabled	text

Field	Data type
is_job	text
name	text
path	text
state	text
type	text
workdir	text

sysobj:proxy

System objects (proxy)

Field	Data type
category_name	text
data	text
id	text
key	text
sid	text
value	text

sysobj:registry

System objects (registry)

Field	Data type
arkstatus	text

Field	Data type
category_name	text
clsid	text
data	text
full_key	text
id	text
key	text
path	text
sid	text
threat	text
value	text

sysobj:shortcuts

System objects (shortcuts)

Field	Data type
arg	text
arkstatus	text
category_name	text
data	text
mac	text
machine_id	text
name	text

Field	Data type
path	text
relative	text
target	text
threat	text
workdir	text

sysobj:wmi

System objects (WMI)

Field	Data type
arkstatus	text
category_name	text
class	text
clsid	text
data	text
instance	text
name	text
namespace	text
path	text
threat	text
value	text
workdir	text

system_reg_export

Registry

Field	Data type
arkstatus	text
category_name	text
hive	text
lastwrite	date
name	text
security	text
subkeys	integer
value.arkstatus	text
value.name	text
value.size	integer
value.type	text
value.value	text
values	integer

system:accounts

System (accounts)

Field	Data type
bad_passwd_count	integer
category_name	text

Field	Data type
codepage	text
country	text
descr	text
expires	date
flags	text
fullname	text
group.name	text
home	text
home_drive	text
last_logoff	text
last_logon	date
logons_count	integer
logons_server	text
name	text
password_age	text
profile	text
script	text
type	text
workstation	text

system:antivirus

System (anti-virus)

Field	Data type
category_name	text
company	text
enabled	boolean
guid	text
name	text
product_exe	text
product_exe_company	text
product_exe_version	text
reporting_exe	text
reporting_exe_company	text
reporting_exe_version	text
timestamp	text
uptodate	boolean
version	text

system:bios

System (BIOS)

Field	Data type
category_name	text

Field	Data type
manufacturer	text
primary	text
release_date	date
system_bios_major	integer
system_bios_minor	integer
version	text

system:cpu

System (CPU)

Field	Data type
category_name	text
cores	integer
cpuid	text
descr	text
enabled_cores	text
id	text
load	text
logical_cpus	long
manufacturer	text
max_speed	integer
name	text

Field	Data type
socket	text
speed	integer
threads	integer
vmmonitor_support	boolean
vt_support	boolean

system:dep

Field	Data type
available	boolean
category_name	text
for_32bit	boolean
for_drivers	boolean
policy	integer

system:dirs

System (directories)

Field	Data type
category_name	text
name	text
path	text

system:dns

System DNS

Field	Data type
category_name	text
name	text
server	text

system:firewall

System (firewall)

Field	Data type
category_name	text
company	text
enabled	boolean
guid	text
name	text
product_exe	text
product_exe_company	text
product_exe_version	text
reporting_exe	text
reporting_exe_company	text
reporting_exe_version	text
timestamp	text

Field	Data type
version	text

system:hdd

System (HDD)

Field	Data type
category_name	text
deviceid	text
firmware	text
model	text
name	text
partition.block_size	long
partition.bootable	boolean
partition.bootpart	boolean
partition.id	text
partition.index	text
partition.primary	boolean
partition.size	long
partition.start_offset	long
partition.type	text
partition.volume.compressed	boolean
partition.volume.descr	text

Field	Data type
partition.volume.dirty	boolean
partition.volume.drive	text
partition.volume.drive_type	text
partition.volume.free	long
partition.volume.fs_type	text
partition.volume.media_type	text
partition.volume.name	text
partition.volume.serial	text
partition.volume.size	long
partitions	integer
serial	text
size	long
type	text

system:kernel_va_shadowing

Field	Data type
category_name	text
enabled	boolean
flags	integer
invalid_pte_bit	text
invpcid	text

Field	Data type
invpcid_flushing_optimization	boolean
l1_data_cache_flush_supported	text
l1_terminal_fault_mitigation_present	text
pcid	text
pcid_flushing_optimization	boolean
required	text
required_available	text
status	text
user_global	text
user_pages_marked_global	boolean

system:locale

System (locale)

Field	Data type
category_name	text
code	text
codeset	text
country	text
descr	text
name	text
oslang	text

system:machine_scores

System (performance index)

Field	Data type
category_name	text
cpu	float
direct3d	float
disk	float
graphics	float
memory	float
timetaken	text
winsat_state	text
winsprlevel	float

system:mapped_disks

System (mapped disks)

Field	Data type
category_name	text
drive	text
free	text
fs_type	text
item.drive	text
item.free	text

Field	Data type
item.fs_type	text
item.path	text
item.session_id	text
item.size	text
item.volume_name	text
path	text
session_id	text
size	text
volume_name	text

system:memory

System (RAM)

Field	Data type
category_name	text
free	long
free_virtual	long
total	long
total_virtual	long

system:net_adapters

Network (interfaces)

Field	Data type
category_name	text
default_ip_gateway	ip
dhcp_enabled	boolean
dhcp_server	ip
dns	text
dns_server_search_order	ip
id	text
index	text
ip_enabled	boolean
mac	text
name	text
subnet	ip

system:os

System (OS)

Field	Data type
bit	integer
boot_device	text
boot_mode	text

Field	Data type
build	text
category_name	text
code_integrity	text
debug	boolean
install_date	date
last_bootup_time	date
local_time	date
name	text
pae	text
sp	text
suite	text
type	text
version	text

system:persisted_routes

Field	Data type
caption	text
category_name	text
descr	text
destination	text
item.caption	text

Field	Data type
item.descr	text
item.destination	text
item.mask	text
item.metric1	text
item.name	text
item.next_hop	text
mask	text
metric1	text
name	text
next_hop	text

system:policies

System policies

Field	Data type
__type__	text
category_name	text
full_key	text
key.item.name	text
key.item.size	integer
key.item.value	text
key.name	text

Field	Data type
name	text
sid	text
value.name	text
value.size	text
value.value	text

system:recovery

Field	Data type
auto_reboot	boolean
category_name	text
dump_path	text
dump_type	integer
kernel_dump_only	boolean
mini_dump_dir	text
overwrite_existing_dump	boolean
send_admin_alert	boolean
write_debug_info	boolean
write_to_eventlog	boolean

system:routes

Network (static routes)

Field	Data type
age	text
caption	ip
category_name	text
descr	text
destination	ip
information	text
interface_index	text
mask	ip
metric1	text
metric2	text
metric3	text
metric4	text
metric5	text
name	ip
next_hop	ip
protocol	text
type	text

system:secure_boot

Field	Data type
capable	boolean
category_name	text
enabled	boolean

system:security_providers

Field	Data type
category_name	text
health	text
name	text

system:sessions

System (sessions)

Field	Data type
category_name	text
client_device_id	text
client_dir	text
client_ip	text
client_name	text
connect_time	date
disconnect_time	date

Field	Data type
domain	text
envid	text
id	text
is_rdp	text
last_input_time	date
logon_time	date
name	text
remote_ip	text
state	text
station_name	text
user	text

system:shares

System (shared directories)

Field	Data type
caption	text
category_name	text
descr	text
name	text
path	text
type	integer

system:smart

S.M.A.R.T. attributes

Field	Data type
attribute.index	integer
attribute.name	text
attribute.raw	integer
attribute.threshold	integer
attribute.value	integer
attribute.worst	integer
category_name	text
firmware	text
id	text
model	text
serial_number	text

system:speculation_control

Field	Data type
bpb_disabled_kernel_to_user	text
bpb_disabled_no_hardware_support	text
bpb_disabled_system_policy	text
bpb_enabled	text

Field	Data type
branch_prediction_mitigation.disabled_by_system_policy	boolean
branch_prediction_mitigation.disabled_no_microcode_update	boolean
branch_prediction_mitigation.enabled	boolean
category_name	text
cpu_microcode_support_pred_cmd.enabled	boolean
cpu_microcode_support_pred_cmd.window_use_ibpb	boolean
cpu_microcode_support_spec_ctrl.enabled	boolean
cpu_microcode_support_spec_ctrl.windows_use_ibrs	boolean
cpu_microcode_support_spec_ctrl.windows_use_stipb	boolean
enhanced_ibrs	text
enhanced_ibrs_reported	text
flags	long
hv_l1tf_migitation_enabled	text
hv_l1tf_migitation_not_enabled_hardware	text
hv_l1tf_migitation_not_enabled_load_option	text
hv_l1tf_processor_not_affected	text
hv_l1tf_status_available	text
hvl_1tf_migitation_not_enabled_core_scheduler	text
ibrs_present	text
mb_clear_enabled	text

Field	Data type
mb_clear_reported	text
mds_hardware_protected	text
smep_present	text
spec_cmd_enumerated	text
spec_ctrl_enumerated	text
spec_ctrl_import_optimization_enabled	text
spec_ctrl_retpoline_enabled	text
speculative_store_bypas_sdisable_supported	text
speculative_store_bypass_disable_available	text
speculative_store_bypass_disable_required	text
speculative_store_bypass_disable_supported	text
speculative_store_bypass_disabled_kernel	text
speculative_store_bypass_disabled_system_wide	text
status	text
stibp_present	text

system:user_privelegies

User privileges in the system

Field	Data type
category_name	text
enabled	boolean

Field	Data type
name	text

system:users

System (users)

Field	Data type
category_name	text
folder.name	text
folder.path	text
home	text
name	text
network_drive.connect_flags	text
network_drive.connection_type	text
network_drive.defer_flags	text
network_drive.letter	text
network_drive.provider_name	text
network_drive.provider_type	text
network_drive.remote_path	text
network_drive.username	text
sid	text
type	integer

winstore_apps

Applications from Microsoft App Store

Field	Data type
arch	text
category_name	text
id	text
name	text
vendor.C	text
vendor.CN	text
vendor.L	text
vendor.O	text
vendor.OID.1.3.6.1.4.1.311.60.2.1.2	text
vendor.OID.1.3.6.1.4.1.311.60.2.1.3	text
vendor.OID.2.5.4.15	text
vendor.OU	text
vendor.S	text
vendor.SERIALNUMBER	text
version	text