Bitdefender Engine - Windows Agent User Guide

##

Computers are increasingly interconnected and as the number of malicious software (malware) threats exponentially increases it is vital that each computer is secured by an antivirus program both to protect itself as well as any devices it connects to. To combat these threats and provide endpoint security we have launched Managed Antivirus.

Managed by your network administrator, Managed Antivirus is a fully automated antivirus solution designed to protect your computer from all types of [malware threats](#topic_mav_bdagent_malware) including viruses, spyware and Trojans.

Managed Antivirus has minimal impact on the performance of your computer and automatically makes the majority of security related decisions for you.

[Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon)

[Managed Antivirus Console](#topic_mav_bdagent_consolemain)

[Status](#topic_mav_bdagent_notify)

[Events](#topic_mav_bdagent_events)

[Scans (Quick, Full, Custom)](#topic_mav_bdagent_scans)

[Custom Scan](#topic_mav_bdagent_customscan)

[Right-click File or Folder Scan](#topic_mav_bdagent_security)

[Scan Progress](#topic_mav_bdagent_scanprogress)

[Modules](#topic_mav_bdagent_status)

[Quarantine](#topic_mav_bdagent_quarantine)

[Check for Updates](#topic_mav_bdagent_events)

|  |
| --- |
| Protection configuration and management are performed remotely by your network administrator. |

This document is designed to cover the options available for Managed Antivirus end-users. It focuses on those installations where the network administrator has enabled end-user access to the Managed Antivirus agent via the System Tray icon (to manually run on-demand scans and manage quarantined items) or has opted to display notifications when an action is performed (for example start scan, item blocked by active protection, virus signature database updated).

## What is Malware?

Malware is a generic term that covers any type of unwanted malicious software designed to destroy, copy or intercept data that is installed on the computer without your consent. There are various forms of malware *in the wild* and we have covered four of the main threats below:

**Viruses** – A program or piece of code which normally attaches itself to an executable file. The virus will remain dormant on the computer until the program or file is interacted with, for example someone runs the program or opens the file. Once this interaction takes place the virus then infects the computer potentially damaging your hardware, software and files. Like their biological equivalent computer viruses can self-replicate to consume all of the computer’s resources and bring the system to a halt. More dangerous viruses can spread across networks and bypass security systems.

**Worms** – Similar to viruses, worms are programs that propagate over a network and can travel without human interaction. Worms are self-replicating, so rather than a single worm infecting the network, a compromised computer can send hundred or even thousands of copies of the worm. This can not only use up all of a single computer’s resources, possibly to the extent that the system shuts down, but can also affect the bandwidth of the whole network. Worms can also create a backdoor into your system to allow unauthorized access. Unlike viruses, worms do not attach themselves to other files or programs.

**Trojans** (**Trojan Horse**) – Named after the wooden horse of Troy from Homer’s Iliad, a Trojan is a non-replicating destructive program masquerading either as a legitimate application or as a file from a legitimate source. Trojans can damage and delete data as well as compromise security by retrieving and intercepting personal or confidential data and can also create a backdoor for unauthorized users to gain access to your system.

**Spyware** – Designed to covertly gather information through the internet connection and installed without the user’s knowledge, spyware applications are typically bundled as a hidden component with freeware of shareware programs. Once installed the user’s internet activity is monitored and this information diverted to someone else. Some spyware can record all of the user’s keystrokes, scan files and other applications and even install other spyware programs. The data intercepted by spyware can range from basic details that the recipient may use or sell on for advertising purposes through to the retrieval of email addresses, passwords, credit card and banking data. Spyware can be thought of a similar to Trojans, as both are unknowingly installed by the user when installing legitimate software. Spyware not only comprises the security, but through its use of the computer’s resources can also lead to system instability in addition to consuming high levels of network bandwidth.

### Managed Antivirus System Tray Icon

The Managed Antivirus agent and all of its features (manually run on-demand scans, manage quarantined items and update the virus detection files) is access through the Managed Antivirus system tray icon ****

**Double-click** on the Managed Antivirus system tray icon **** to open the agent console or **right-click** on the icon to display a context menu with the following choices:

**Show** opens the main Managed Antivirus agent.

**About** displays a window containing information on the product including the Technical Support contact details (where available). Opening the **About** window automatically initiates an on-demand update.

**Language** returns the list of languages currently available for the console. Simply choose the required language from the list to apply.

The system tray icon also acts as an *at a glance* indicator for the computer’s security and scan status (when a scan is in progress). So, you can easily see if any issues are currently reported, along with their severity.

|  |  |
| --- | --- |
|  | There are no issues affecting the security of the computer |
|  | Critical issues affecting the security of the computer |
|  | Non-critical issues affecting the security of the computer |
|  | Scan in progress |

|  |
| --- |
| The System Tray icon is generally found in the taskbar beside the system clock. However, depending on the number of icons in the taskbar it may be necessary to expand the *Show hidden icons* section by clicking on the arrow  to display the Managed Antivirus system tray icon. |

** **

**What do you want to do?**

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Managed Antivirus Console

The main window of the Managed Antivirus console allows you to check the current protection status, review the events timeline, run scans and view items in quarantine. Double-click or right-click on the Managed Antivirus [system tray icon](#topic_mav_bdagent_trayicon) to access the console.

The console window is organized into two main sections.

[**Status** area](#topic_mav_bdagent_notify)

[**Events** timeline](#topic_mav_bdagent_events)

Once finished in the console click **X** to exit. This only closes the dialog and Managed Antivirus continues to run on the computer, providing protection against threats.

****

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Status

The **Status** area provides useful information on the computer’s current security status using an easy to identify traffic light and icon notification system. These notifications falling into one of three levels of severity.

|  |  |
| --- | --- |
|  | Green tickNo issues to fix. Your computer and data are protected. |
|  | Yellow exclamationNon-critical issues are affecting the security of the system |
|  | Red crossCritical issues are affecting the security of the system |

Click on an issue in the notification area to view a detailed security status message on the issue in a new dialog. Depending on the issue, this dialog can include a link to perform a resolution action. For example, run a Full Scan.

To return to the main window, click the back arrow at the top left corner of the dialog.

****

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Events

Managed Antivirus records any actions in its log files and reports the event in the main window of the console underneath the status area. Along with the action category and text description, events use an easy to identify traffic light and icon notification system. Green for successful operation, yellow for warning (non-critical issue) and red for a critical issue. This allows you to easily see the actions performed, from definition file updates to threat discovery and their status.

If an event contains multiple entries, click on its down arrow to expand the event and view more detailed information. Click the up arrow to close.

Depending on the event type, the entries can have the option to **View Log** in a new dialog. For example, the Contextual Scans dialog returns sections on the scan Target, Results and Statistics.

To return to the main window, click the back arrow at the top left corner of the dialog.

****

**Filter Events**

By default, the Events timeline lists all actions ordered by date. To limit these results and only display relevant information, you can apply Even Filters.

Click on the **Filters** button ****then select the information to display in the main window from the Filters panel. Click **Reset Filters** to clear your selection.

After making the selection, click in the main window to close the Filters panel.

**Modules**

**General Settings**: Valid license received etc.

**Antimalware**:File deleted, Scan started, Scan finished, On-access scanning enabled, On-access scanning disabled etc.

**Update**: Update succeeded, failed etc.

**Date Range**

**Start** to **End**: choose the Reporting Period from the calendar then click **GO** to apply or **RESET** to clear.

**Severity**

**Information:** Scan started, scan finished (no threats found), on-access scanning enabled, Update successful etc.

**Warning**: File deleted; Scan finished (threats found) etc.

**Critical**: Update failed; On-access scanning disabled etc.

|  |
| --- |
| Combine filters to provide more targeted results. For example, only show events for selected **Modules** with a certain **Severity** within a specified **Date Range**. |

** **

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Scans (Quick, Full, Custom)

To manually run a Managed Antivirus scan on the computer, or create your own bespoke custom scan, click the **Actions** button **.**

Click on the scan you wish to run from the **Scan Tasks** panel or create a new custom scan.

**Quick scan**

A lightweight scan that (by default) scans running process in the drive for threats. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

**Full scan**

Scans the entire computer for all types of malware threats. Including viruses, spyware, adware, rootkits and others. As the Deep Scan scans the entire computer it can take a while to complete. We recommend running this scan when the computer is not in use.

**Custom scan (Favorite)**

Run a previously configured custom scan saved as a favorite.

[New custom scan](#topic_mav_bdagent_customscan)

Rather than scan the entire computer for malware threats, or only scan the running processes, you can select the locations to scan and configure the scan settings to precisely match your requirements. Click the **New Custom Scan** button to run a scan and [configure](#topic_mav_bdagent_customscan).

|  |
| --- |
| Where a scan discovers malware or rootkits, Bitdefender automatically begins the disinfection process. If disinfection is not possible, Bitdefender moves the files to the quarantine where it cannot do any harm.  |

The main console window displays the [scan progress](#topic_mav_bdagent_scanprogress), with pop-up messages notifying you when the scan started and stopped.

** **

**Attached Device Scanning**

Depending on the settings configured by your network administrator. Managed Antivirus can suppress any user messages and scan the attached device automatically, or prompt you to decide on the scan action to take.

Where the device configuration includes user confirmation, a separate message is displayed for each device when several items are detected at the same time.

|  |
| --- |
| Before running any scans we advise [updating](#topic_mav_bdagent_additional) the virus signature database to ensure any newly reported threats are discovered during the scan. |

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

#### Custom Scan

Custom Scans only scans the specified locations for malware threats and at a sensitivity level you determine.

To be begin a custom scan, click **New Custom Scan** in the Scans panel then configure the settings.

**Target**

Expand the tree and select the items to scan

**Scan Options**

1. Choose the sensitivity level applied by the scan: **Aggressive**, **Normal**, **Permissive** or **Custom**

2. Decide whether to **Run task with low priority**. This option reduces the impact of the scan on the computer and allows other programs to run faster, although the scan may take longer to complete.

**Custom Scan Options**

When selecting **Custom** as the sensitivity level, the next step is to click **Settings** and configure.

**File Types**

1. Select the **File Types** to scan. When selecting **Custom extensions** enter the comma separated extensions in the **Extensions** field.

2. Choose whether to scan **Archives** and set the maximum size and depth limits.

3. Decide whether to **Scan email archives**

**Scan**

Choose what to scan and threat types to look for. Tick the box to include in the scan and untick to ignore.

**Actions**

Select the actions to take on rootkit, infected or suspect file discovery.

**Save Custom Scan as a Favorite**

To save the scans settings, enter a name in the *Save favorite scan* field and click the star button. The custom scan then appears in the **Scan Tasks** panel with the option to run scan or click the trash can button and delete.

** **

|  |
| --- |
| Before running any scans we advise [updating](#topic_mav_bdagent_additional) the virus signature database to ensure any newly reported threats are discovered during the scan. |

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Right-click File or Folder Scan

**Specific File or Folder Scan**

When you have suspicions about files or folders on the computer, you can quickly run a scan on that item.

Navigate to the location, right-click on the suspect item and select **Scan with Managed Antivirus** from the context menu.

To scan multiple files and/or folders, use **Shift** and ***left-click*** to choose a range of items or **Control** and ***left-click*** for specific files or folders. When satisfied with the selection right-click on one of the suspect items and choose **Scan with Managed Antivirus** from the context menu.

****

|  |
| --- |
| Before running any scans we advise [updating](#topic_mav_bdagent_additional) the virus signature database to ensure any newly reported threats are discovered during the scan. |

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Scan Progress

When running a scan on the computer (either on-demand or scheduled) both the console and system tray icon  indicate its progress. Depending on policy settings, notification pop-ups can appear to let you know the scan has started and completed.

From the console you can opt to:

* **View Details**: Open the Scan dialog showing the current position and statistics. Click the back arrow at the top left corner of the dialog to return to the main window.
* **Pause**: Stop the scan at the current position and manually **Resume** at a later time.
* **Postpone**: Pauses the scan for the specified period of time (15 to 60 minutes) before automatically resuming.
* **Stop**: Exit out of a currently running scan. For example, when a Full Scan is taking longer than expected to complete on a laptop and the user has to leave.

Once a scan completes. The Events timeline and Status area provide information on the results.

**User Actions**

In the majority of cases any remediation action is automatically applied. Although depending on the detected threat or scanned object type you may receive a prompt to choose the appropriate action to take to protect your computer. This can also occur when a threat was detected, and the scan stopped.

**Detected Threats**

You can choose to **Quarantine** the infected file to ensure it is not accessed, **Delete** the infected file from the disk or **Ignore** the detected file and take no action.

|  |
| --- |
| Care must be taken when selecting either the **Delete** or **Ignore** options. Once a file is deleted it will no longer be available. Ignoring a suspect file may lead to the infection of the computer. |

**Password Protected Objects**

During the scan, password-protected files or folders may be discovered and you are prompted on how to handle them.

Choose from entering the **Password**, **Don’t ask for password and skip this object from scan** or **Skip all password-protected items without scanning them**.

****

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Modules

The **Modules** window displays useful information about the status and activity of the installed protection modules.

Click the **Modules** button **** at the top left corner of the main window.

**Antimalware**

Antimalware protection is the foundation of your security. This protects the computer in real-time and on-demand against all sorts of malware, including viruses, trojans, spyware, adware, etc.

**On-Access** (Active Protection) scans for new malware threats to prevent them from entering the system. It scans local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA).

**Advanced Threat Control** (Behavioral Scanning) continuously monitors applications running on the endpoint for malware-like actions. Advanced Threat Control will automatically try to disinfect the detected file.

[**Quarantine**](#topic_mav_bdagent_quarantine)displays the list of quarantined files, their original path, quarantine action time and date and their security status.

Once finished in **Modules**, click the back arrow at the top left corner of the dialog.

****

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions

### Quarantine

When a malware-infected or suspicious file or program (showing signs of infection) is detected by Managed Antivirus it is isolated and placed in a secure area called the quarantine. Once in quarantine the file or program cannot be read or executed, this prevents any infection from spreading and protects not only the computer but potentially the network.

To open the quarantine, click the **Modules** button **** at the top left corner of the main window. View the number of items currently in quarantine and click on the **Quarantine** link.

Each quarantined item contains its **Filename** including original path, the **Threat Name** along with the date and time the item was **Quarantined** on.

Click the search button to filter each column and provide more targeted results.

To manage (delete or restore) quarantine items. Click the tick box against the files(s). To select all items in the current filtered view, click on the tick box beside **Filename**.

Once satisfied with the selection choose the required action.

**Restore**

When you have an incorrectly quarantined item or feel that an item was incorrectly quarantined (known as a false positive) this option returns the item to its original location.

**Restore to...**

When you have an incorrectly quarantined item or feel that an item was incorrectly quarantined (known as a false positive) this option returns the item to a new location.

|  |
| --- |
| Do not restore any items from quarantine unless **you are sure** these files no longer pose a threat, otherwise they can infect your computer. |

**Delete**

Permanently removes the selected items from your computer.

**Empty**

Purges the current quarantine and permanently removes **all**quarantined items from your computer, not just selected items.

|  |
| --- |
| Any files deleted from the quarantine are **permanently removed and** **cannot be restored**. As such we suggest taking extreme care when using this option. |

Once finished in the quarantine, click the back arrow at the top left corner of the dialog.

****

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 [Check for updates](#topic_mav_bdagent_additional)

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

### Check for Updates

When new malware threats are discovered *in the wild,* they are analyzed by antivirus laboratories and an updated version of the virus signature database released containing the information required to detect these threats.

As threats constantly emerge and antivirus laboratories develop new detection methods there can be frequent virus signature definition database releases.

To ensure your computer is fully protected, Managed Antivirus automatically updates to the latest virus signature on a schedule setup by the network administrator, normally checking for updates every few hours and downloaded a new version when available.

As scanning your computer using an outdated virus signature database may prevent the antivirus module from detecting newly identified malware, we would suggest manually updating the virus signature database before running an on-demand scan.

To update the virus signature database. Click the **Actions** button  in the console's main window, then click **Check for updates**.

****

**What do you want to do?**

 Discover [Managed Antivirus System Tray Icon](#topic_mav_bdagent_trayicon) functions

 Open the [Managed Antivirus Console](#topic_mav_bdagent_consolemain)

 Read about the information in the [Status Area](#topic_mav_bdagent_notify)

 Look at the [Event](#topic_mav_bdagent_events) timeline

 Scan a specific [File or Folder](#topic_mav_bdagent_security)

 Run a manual [scan](#topic_mav_bdagent_scans) (Quick, Full or Custom)

 Create a [custom scan](#topic_mav_bdagent_customscan)

 View [scan progress](#topic_mav_bdagent_scanprogress)

 Review items in [quarantine](#topic_mav_bdagent_quarantine) and perform actions