Bitdefender

Bitdefender Endpoint Security for Kaseya (Legacy)

USER GUIDE

Bitdefender GravityZone
User Guide

Publication date 2022.04.26

Legal Notice

Table of Contents

1. ABOUT ENDPOINT SECURITY PLUGIN FOR KASEYA

The Endpoint Security Plugin for Kaseya is a module for Kaseya VSA that provides a management console for deploying, monitoring, and interacting with the Bitdefender Endpoint Security agent, an enterprise-class award-winning antimalware solution. Kaseya administrators can use the plugin to remotely install the Bitdefender Endpoint Security agent, manage agent licensing across their organizations, assign custom policies to organizations, machine groups or individual machines, and initiate different types of malware scans.

Malware detection data is collected and can be used to generate reports and alerts. The plugin significantly enhances Kaseya administrator's ability to manage large deployments of Bitdefender agents.

The plugin uses a number of Kaseya technologies:

- **Agent Procedures**, to retrieve data from the agents and send commands.
- **Alerts**, including alarms, tickets, email and the notification bar.
- **LAN Cache**, to reduce network traffic and server load during agent installation.
- **Machine Filter Bar**, that maintains consistent filtering settings between the plugin and other Kaseya modules.

2. INSTALLATION

2.1. Kaseya Server Requirements

- Kaseya 7.0 or later
- On-premise Kaseya installation
- Microsoft .NET Framework 4 (Full)
- Microsoft Internet Information Server (IIS) 7.0 or later
- Windows 2008 or later
- SQL Server 2008 or later
- 8 GB RAM

2.2. Supported Browsers

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

2.3. Endpoint Requirements

- Kaseya agent
- Microsoft .NET Framework 4 (Full)
- Windows XP Service Pack 3 and later
- 1 GB RAM

2.4. Plugin Installation

1. Copy the installer on to the Kaseya server.
2. Double-click to run the installer.
3. Click **Next** to follow the prompts.
4. The last step of the installer has a check box that will start the Kaseya Reapply Schema process after the **Finish** button is pressed. Keep this box selected if

you want to start this process immediately, otherwise clear the check box and run the **Reapply Schema** process manually at a later time.

Note
The plugin is not available in Kaseya until the **Reapply Schema** process has run at least once.

2.5. Plugin Upgrades

When new versions of the plugin are released, download the new installer to the Kaseya server and run the normal installation process. This will copy the updated files on top of the existing installation, preserving existing settings and data.

However, it is strongly recommended to back up your data before each update to make sure that you are not going to lose anything. For a detailed step-by-step guide for manual backup, refer to this Bitdefender KB article.

2.6. Bitdefender Agent Installation

Instructions for remotely installing the Bitdefender agent on a Kaseya endpoint are listed in the Endpoints section of this guide.

2.6.1. Pre-installation Notes

- The 32 and 64 bit agent installers are not included in the plugin installation package.
- The latest versions of the installers are downloaded to the Kaseya server after the plugin is installed.
- These agent installers are automatically updated as new versions are released.
- Deployed agents automatically update themselves.
- Before installing the agent on an endpoint, it is highly recommended that any existing antimalware software is completely removed.
- Most of the security programs incompatible with Bitdefender Endpoint Security are automatically detected and removed at installation time. To learn more and to check the list of detected security software, refer to this Bitdefender KB article.

2.6.2. Bulk Deployment

The **Install** button on the **Endpoints** page will schedule an install to run on all selected machines at the same time. This is useful for small deployments or installing on individual machines. A large scale deployment can take advantage of Kaseya's built-in agent procedure distribution functionality by scheduling the install script through Kaseya's **Agent Procedure** module.

Note
Check the **Settings** page in the Bitdefender module to ensure the Bitdefender agent installers are available on the Kaseya server before starting this process.
Scheduling these procedures outside of the plugin means that the status of the endpoints will not change to **Installing** and the **Install** task won't be created for the endpoint. After the installation finishes, the status will be updated in the plugin.

Bulk Deployment Steps:

1. In Kaseya, open the **Agent Procedures** module.
2. On the **Schedule/Create** page, select the **Bitdefender Install** procedure from `System\Bitdefender Kaseya Module`.
3. On the **Schedule** tab, select the machines you want to deploy the Bitdefender agent to. Keep in mind you can use machine filters to select large numbers of endpoints.
4. Click the **Schedule Agent Procedure** button.
5. On the **Schedule Agent Procedure** tab, select a recurrence of **Once** and choose a distribution window based on the number of selected endpoints.
6. On the **Script Prompt** tab, enter **0** for the **Task Id** prompt.
7. Click **Submit** to schedule the installation agent procedures.

3. PLUGIN AT A GLANCE

Dashboard

View charts and graphs showing malware detections and the status of Bitdefender agents in the Kaseya environment. Each graph has details and can be opened in a separate page as a simple report.

Licenses

Assign licenses to organizations and control which endpoints use license slots.

Endpoints

View status and antimalware information about individual endpoints, along with initiating installs, uninstalls and scans.

Quarantine

View quarantined files from all endpoints, issue restore and delete commands.

Audit Log

View log messages for the entire plugin, including general and machine-specific log entries.

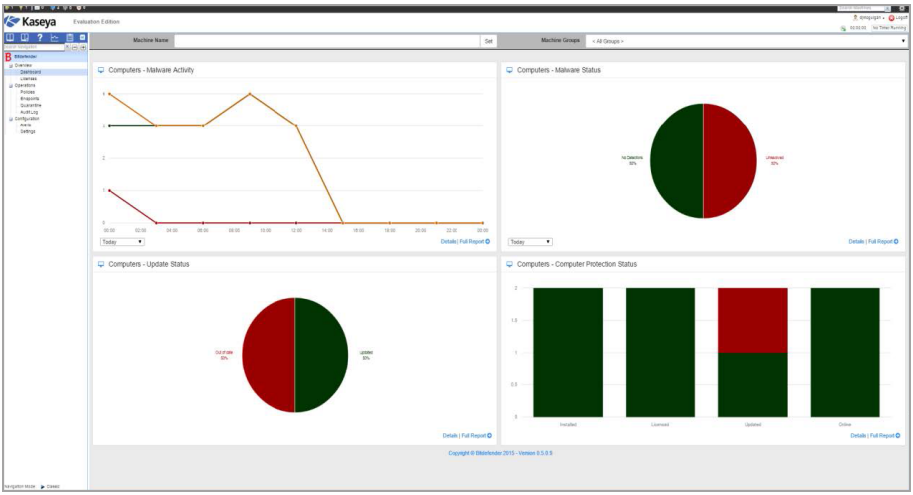
Alerts

Configure which alerts are enabled and how they send notifications.

Settings

Configure settings and view general information for the plugin, such as alert settings, refresh intervals, and agent install packages status.

4. DASHBOARD



The dashboard is the first page you will be greeted with upon entering the plugin. Here, you will be able to get a quick, at-a-glance overview of the state of all managed endpoints when it comes to malware detections and how up-to-date the endpoint agents are. This information is divided down into four primary reports:

- **Malware Activity**
- **Malware Status**
- **Update Status**
- **Computer Protection Status**

Each of these reports breaks down into three levels:

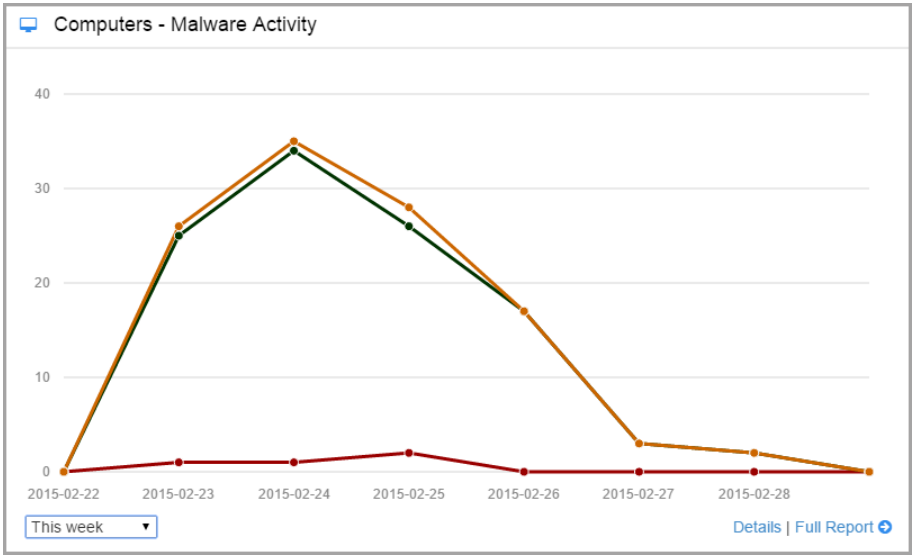
- a chart, which is visible on the main dashboard
- a table containing more detailed information related to the data in the chart
- a full report, which is a compilation of both the chart and detailed data information

4.1. Malware Activity

The **Malware Activity** chart demonstrates the current status of all endpoints being managed in Kaseya. It is comprised of a line chart, a drilldown table and a report.

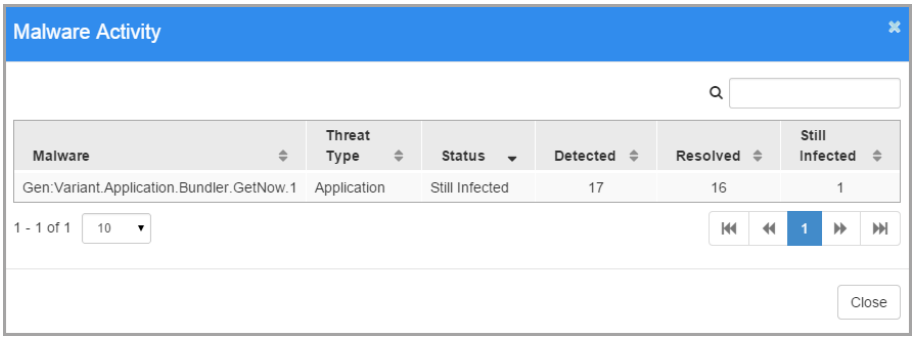
Chart

The **Malware Activity** chart displays a measure of the number of malware detected over time. It is composed of three data lines: number of detections, number of resolved detections and number of unresolved detections.



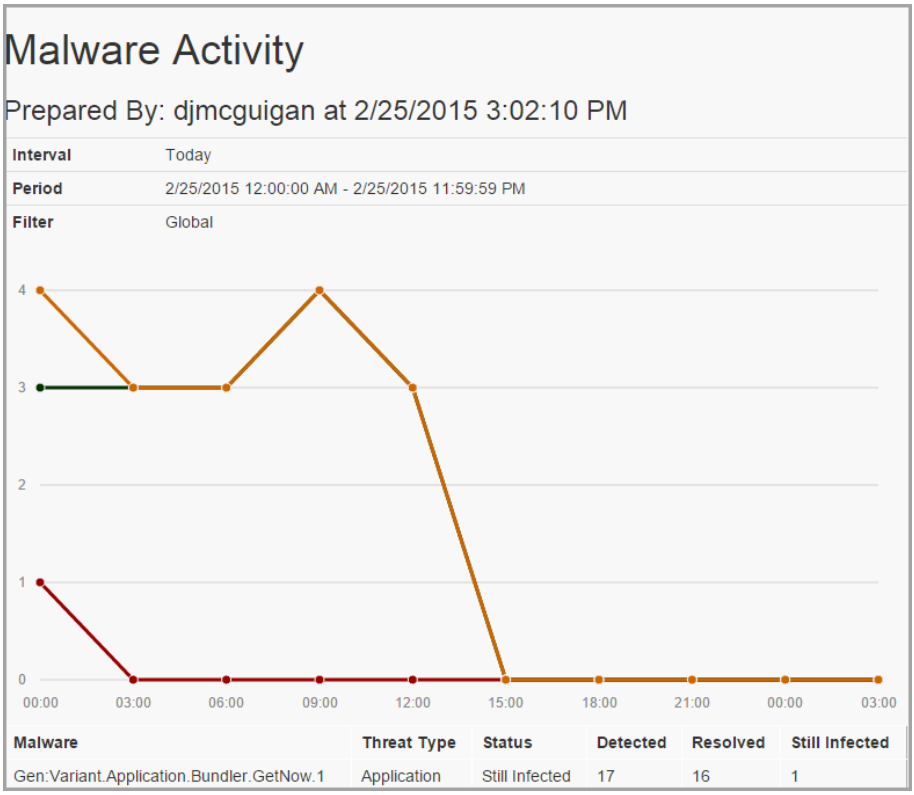
Table

The details view is contained in a dialog window that is accessed by clicking the **Details** link in the bottom right of the pane. The table contains a list of all unique malware detected on the licensed endpoints. Each subsequent detection increases the quantities in the record for that malware.



Report

The report view is a combination of the chart and drilldown details for the selected interval on the main panel, with a cutoff time at the time the report was generated.

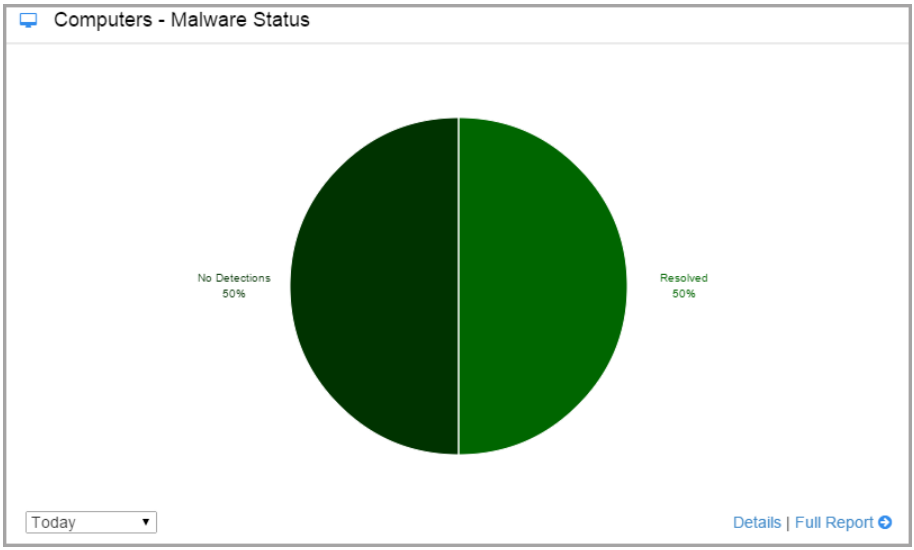


4.2. Malware Status

The **Malware Status** chart demonstrates the current status of all endpoints being managed in Kaseya. It is comprised of three pieces: a pie chart, a drilldown table, and a report.

Chart

The **Malware Status** chart is a pie chart that gives a quick breakdown on the percentages of licensed endpoints that fall into three categories: **No Detections**, **Resolved** and **Still Infected**.

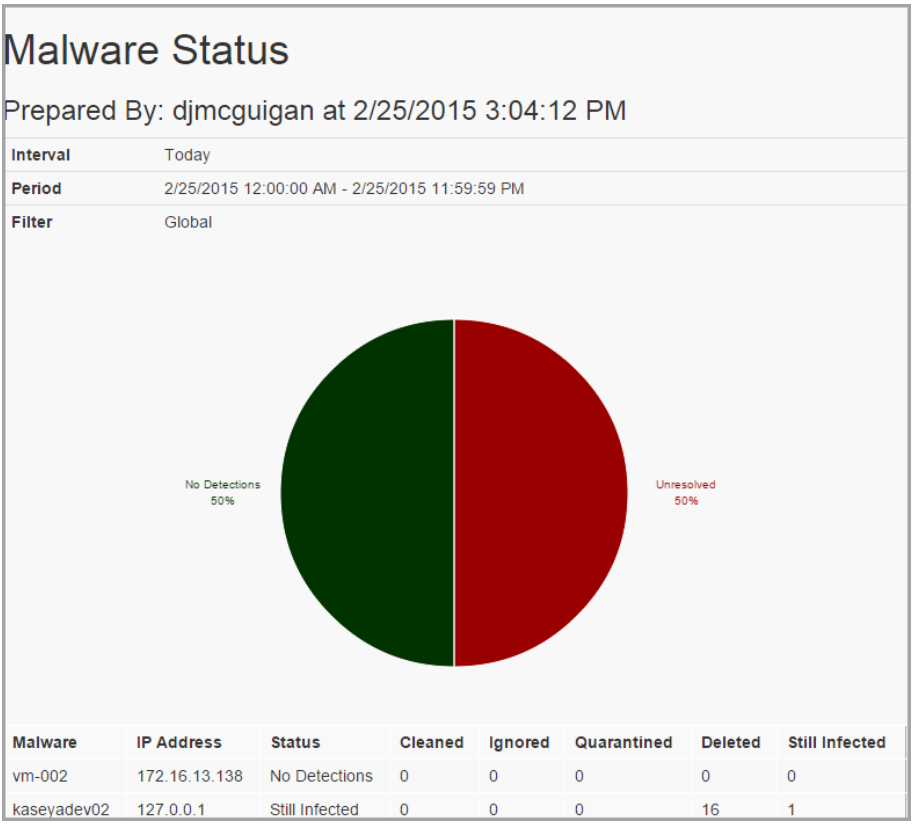


Table

The details drilldown for the **Malware Status** report is a table that displays the endpoints that Bitdefender has been installed and licensed on. Each record has the latest counts of detected malware and what actions were taken on them, as well as the latest status of the endpoint based on the detected malware.

Report

The report view is a combination of the chart and drilldown details for the selected interval on the main panel, with a cutoff time at the time the report was generated.



Malware Status

Prepared By: djmcguigan at 2/25/2015 3:04:12 PM

Interval	Today
Period	2/25/2015 12:00:00 AM - 2/25/2015 11:59:59 PM
Filter	Global

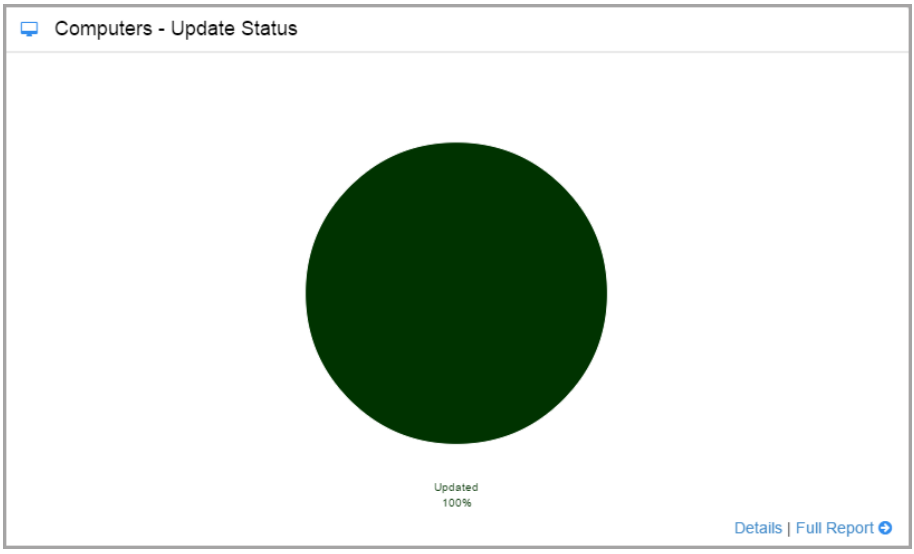
Malware	IP Address	Status	Cleaned	Ignored	Quarantined	Deleted	Still Infected
vm-002	172.16.13.138	No Detections	0	0	0	0	0
kaseyadev02	127.0.0.1	Still Infected	0	0	0	16	1

4.3. Update Status

The **Update Status** chart demonstrates the current status of all endpoints being managed in Kaseya. It is comprised of three parts: a pie chart, a drilldown table and a report.

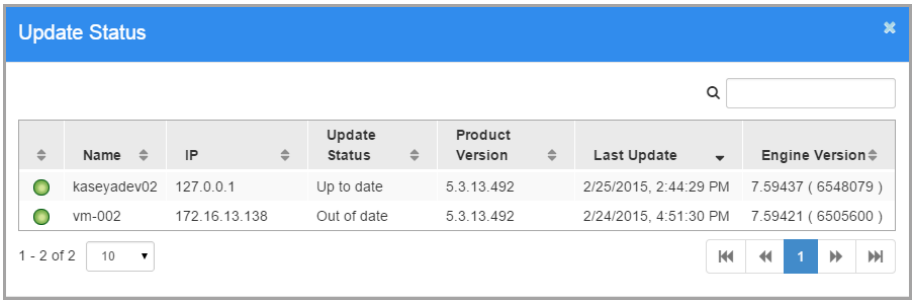
Chart

The **Update Status** chart displays the percentages of licensed endpoints that have various update statuses. The possible statuses are: **Up To Date**, **Out of Date**, **Out of Date (Product)**, **Out of Date (Definitions)**, **Disabled**, **Disabled (Product)**, **Disabled (Definitions)** and **Restart Required**.



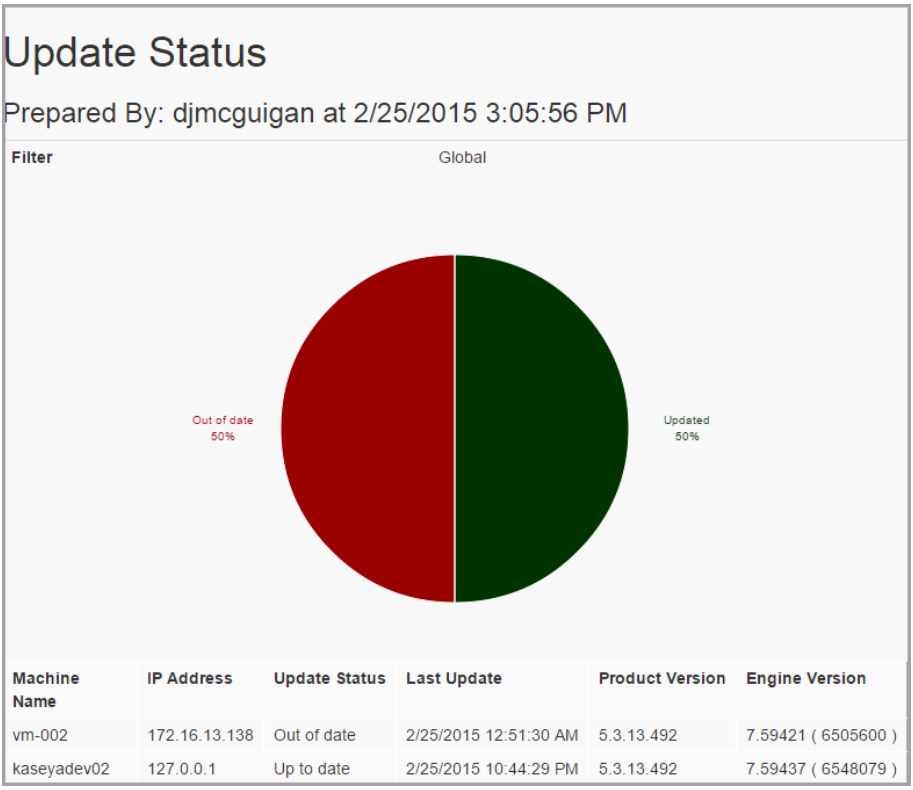
Table

The details drilldown for the **Update Status** chart lists out the endpoints that Bitdefender has been installed and licensed on. Each record has the latest product and engine versions for the endpoint, as well as the last time an update was run.



Report

The report view is a combination of the chart and drilldown details for the selected interval on the main panel, with a cutoff time at the time the report was generated.



Machine Name	IP Address	Update Status	Last Update	Product Version	Engine Version
vm-002	172.16.13.138	Out of date	2/25/2015 12:51:30 AM	5.3.13.492	7.59421 (6505600)
kaseyadev02	127.0.0.1	Up to date	2/25/2015 10:44:29 PM	5.3.13.492	7.59437 (6548079)

4.4. Computer Protection Status

The **Computer Protection Status** chart demonstrates the current status of all endpoints being managed in Kaseya. It is comprised of three pieces: a bar chart, a drilldown table and a report.

Chart

The chart has 4 columns:

Installed

Displays how many Kaseya managed agents have Bitdefender installed. The height of the installed column will always equal the number of endpoints that the Kaseya server manages, and will be split green and red to indicate the proportion of endpoints that have a Bitdefender agent

installed on them versus those that do not have a Bitdefender agent installed.

Licensed

Indicates how many agents with Bitdefender installed have a valid license applied to them. The height of the licensed column will always equal the height of the green segment of the **Installed** column, and will again be split between green and red to indicate licensed and unlicensed Bitdefender agents.

Updated

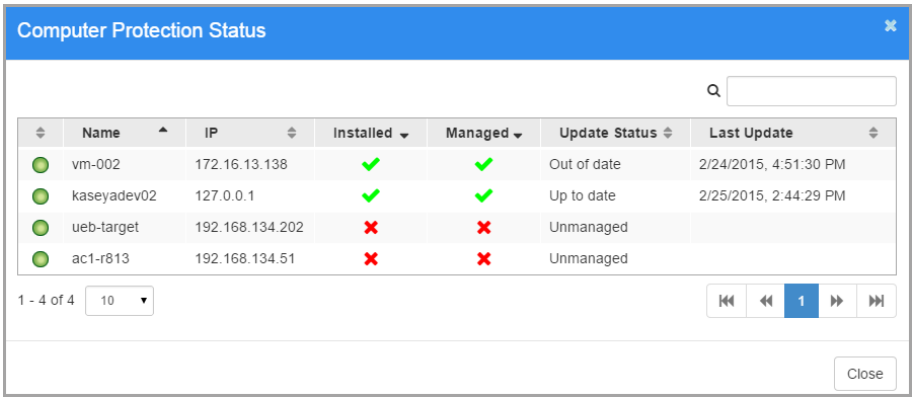
Indicates how many licensed Bitdefender agents have the latest product and engine updates applied. The height of the bar will be equivalent to the height of the green segment of the **Licensed** column and will be split green and red to indicate how many endpoints are fully up to date and those that are out of date.

Online

Indicates how many endpoints with a licensed Bitdefender agent installed are currently powered on and communicating with the Kaseya server. The height will always be equivalent to the height of the green segment in the **Licensed** column and will be split green and red to indicate the number of powered-on licensed endpoints vs powered-off licensed endpoints.

Table

Diplays a list of all the endpoints that have a Kaseya agent installed. For each endpoint, the status of different facets of Bitdefender installation and licensing are listed, as well as the last time an agent was updated, when applicable.



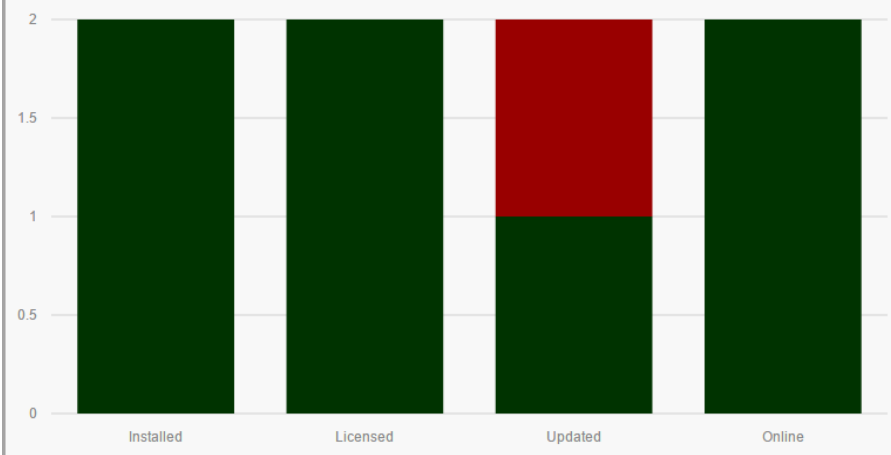
Report

The report view is a combination of the chart and drilldown details for the selected interval on the main panel, with a cutoff time at the time the report was generated.

Computer Protection Status

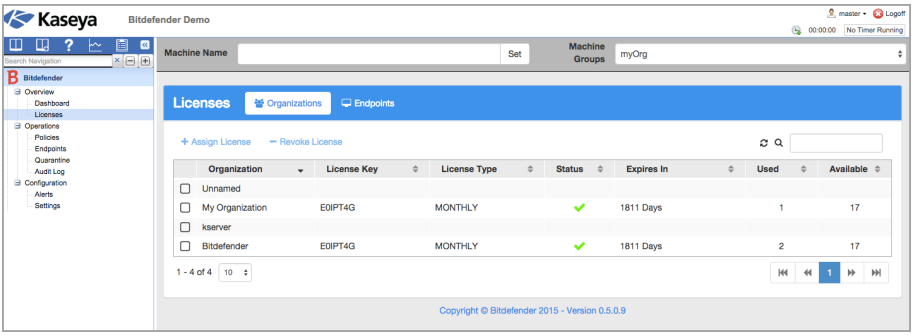
Prepared By: djmcguigan at 2/25/2015 3:07:20 PM

Filter Global



Machine Name	IP Address	Installed	Managed	Update Status	Last Update
vm-002	172.16.13.138	Installed	Managed	Out of date	2/25/2015 12:51:30 AM
kaseyadev02	127.0.0.1	Installed	Managed	Up to date	2/25/2015 10:44:29 PM
ueb-target	192.168.134.202	Not Installed	Unmanaged	Unmanaged	
ac1-r813	192.168.134.51	Not Installed	Unmanaged	Unmanaged	

5. LICENSING



Dashboard Components

- Kaseya Navigation Panel
- Machine Filter Bar – modifies the scope of data displayed in the charts
- License Page Toggle
- Organization Grid Toggle Function
- Organization Grid

5.1. Organizations Tab

The **Organizations** tab displays all organizations with license data (key, type, status, expiration, usage and number of licenses still available). From this pane, you can assign new licenses or revoke current licenses by simply clicking the box next to the organization name and then either **Assign license** or **Revoke license**.

5.1.1. Licensed Organizations Table

This table lists all of the organization in Kaseya, along with any licenses that are assigned to them.

Column	Description
Organization	Name of the organization
License Key	License key assigned to the organization

Column	Description
License Type	Type of license assigned to the organization (End User/Monthly)
Status	Status of the license (**Valid**, **Expired**, **Deactivated**, **Invalid**)
Expires in	How many days until the license expires
Used	License slots used by agents in the organization
Available	Total number of slots available on the license. For monthly licenses, this is the total number across all assigned organizations.

5.1.2. Assign License

Select and endpoint and click the button to open **Assign License** dialog window. On this window, the user is able to add new license keys and choose an active license to assign to the selected organization.

To add a new license key, enter the key in the text field at the top of the window and then click **Add**. There are four possible outcomes:

- **Success**: the license entered was valid, and was activated if it had not been already. The license is added to the database and is viewable in the list of available licenses to be assigned to an organization.
- **Expired**: the license entered has expired, and cannot be used within the plugin. It is not saved to the database.
- **Deactivated**: the license key entered has been actively deactivated by Bitdefender and cannot be used within the plugin. It is not saved to the database.
- **Unknown/Cracked**: the license key entered is not a valid license key and cannot be used by the plugin. It is not saved to the database.

After adding at least one license key, the list in the bottom half of the table should update. The user can then select from that list a license to map to the selected organization.

5.1.3. License Types

End User

The **End User** license type is a traditional fixed-machine-count fixed-duration license. It is purchased with a specific maximum agent count and lasts for a limited amount of time before it expires.

In the Kaseya plugin, you can only assign an **End User** license to a single organization. To license multiple organizations using **End User** licenses, you will need one **End User** license per organization.

After an **End User** license is assigned to an organization, it will be removed from the list of assignable licenses. Revoking the license from the organization will put it back in the list and it can then be assigned to another organization.

Monthly

The **Monthly** license type is an unlimited indefinite usage-based license. This license can be used on any number of agents – although in the system this would translate to a very large agent maximum – and last forever. Daily usage of the license is reported back to Bitdefender and each month the license holder will be billed according to the total number of agents using the license for that month.

The Kaseya plugin can have only one **Monthly** license added at a time. Attempting to add another **Monthly** license will overwrite the existing one, reassigning any licensed endpoints to the new license. However, that single **Monthly** license can be applied to any number of organizations.

A daily alert indicating the number of agents using the monthly license each day, per organization, is available. This could potentially be used to update invoicing information in another system or simply serve as a reminder of overall license usage. See the Alerts section for more details.

5.1.4. Revoke License

After selecting one or more organizations with licenses assigned to them, click this button to remove the license from all endpoints within that organization. Any endpoints within the selected organizations will begin updating their license information, expiring the Antimalware module on the endpoints and updating the plugin to reflect this change. Once the process completes, if the license is still valid, it is added to the pool of available licenses to be provisioned out to other organizations.

5.2. Endpoints Tab

The **Endpoints** tab in the **License** page gives you control over licensing on a per-endpoint level. After a license is assigned to an organization, all endpoints under that organization will automatically try to use that license for their Bitdefender

agent, if they have an agent installed. You can prevent endpoints from using a license, and also see the status and availability of licenses on each endpoint.

5.2.1. Licensed Endpoints Table

This table lists all of the endpoints in Kaseya, filtered by the machine filter bar. For each endpoint, it shows its current agent status along with the status of any license associated to the endpoint.

Column	Description
Machine	Name of the Kaseya endpoint
Group	Machine group for the endpoint
IP Address	IP address of the machine
Status	Status of the agent (see Endpoints section for more information)
License	Status of the license in relation to the endpoint: is it already licensed, are there available slots in the license that could be used, is there a license assigned to the organization

5.2.2. Include

By default, all endpoints are included in the plugin unless they are running an unsupported operating system. You must manually exclude the endpoints that you do not want to be included in the plugin. To bring an excluded endpoint back into the plugin, select the endpoints (more than one can be selected) and click the **Include** button. This will move the selected endpoints out of the Excluded status and they will attempt to use a license slot if the Bitdefender agent is installed and their organization has an assigned license.

5.2.3. Exclude

If there are endpoints that you will not install the Bitdefender agent on, it makes sense to exclude them from the plugin. This prevents the plugin from attempting to do any background actions on them, such as periodically looking for an installed Bitdefender agent. It also prevents the endpoint from using a license slot. This is useful if you are nearing your license maximum capacity: you can exclude less critical endpoints to ensure that critical machines maintain their licenses, and then you can include those machines later, when you have a higher capacity license without having to reinstall the Bitdefender agent.

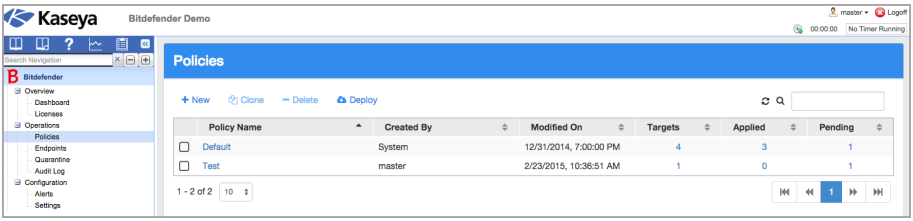
To exclude endpoints, select them from the list and click the **Exclude** button. This will move them to the **Excluded** status.

6. POLICIES

The settings and behavior of the Bitdefender Endpoint Security agent are controlled through policies. Each machine can have one policy assigned to it at a time and will inherit the nearest policy from the machine group or organization it is in. A default policy is always included in the plugin and will be used if no other policy is assigned on an endpoint.

6.1. Policies Table

Here you can see all of the policies that have been created in the plugin, along with how many machines they are targeting.



Column	Description
Policy Name	Name of the policy
Created By	Kaseya admin who created the policy
Modified On	The last time the policy was changed
Targets	The number of endpoints that will be applied to, if they have a licensed Bitdefender agent installed. Click the number to see the list of endpoints.
Applied	The number of endpoints that the plugin has applied the policy to. Click the number to see the list of endpoints.
Pending	The number of endpoints that are attempting to apply the policy to their Bitdefender agent. Click the number to see the list of endpoints.

6.2. New Policy

To create a new policy:

1. Click **New**. This will open the policy creation dialog.
2. Give the policy a name and set the technical support information under the **General - Display** tab.
3. Click **Save** when you are ready to create the policy. Any validation errors will be highlighted.

Note
See the **Policy Settings** section for information on what options are available in a policy.

6.3. Clone Policy

You can create a new policy based on an existing policy. To do this:

1. Select the policy you want to copy and click **Clone**.
2. Enter a name for the new policy and click **Save**. This will copy the settings from the existing policy into the new policy.

6.4. Edit Policy

To modify an existing policy:

1. Click the policy in the table. This will open an edit dialog with the same options as the **New policy** dialog window.
2. Amend the settings and click **Save**.

Note
After a policy is modified, it will be redeployed to all of its assigned endpoints. The default policy cannot be edited.

6.5. Delete Policy

If you want to remove a policy from the plugin:

1. Select the policy in the table and click **Delete**.
2. The policy is removed from the table. Any endpoints that were using the policy will be reassigned another policy, based on the inheritance rules defined in the **Deploy Policies** section.

6.6. Deploy Policies

To deploy new policies to your endpoints:

1. Click **Deploy** to open the deploy dialog.
2. Assign policies to organizations, machines groups, and endpoints. The assignment of policies obeys the following inheritance model: **Organization > Machine Group > Endpoint**.

Each endpoint determines what policy should be applied to itself by starting with itself and looking up the inheritance tree to find the closest assigned policy. Here are some examples:

- An endpoint has Policy A set directly on itself. It will use Policy A and ignore any policies applied to its machine group or organization.
- An endpoint does not have a policy directly set on it, but its machine group has Policy B set. The endpoints will use Policy B and ignore any policy applied to its organization.
- An endpoint does not have a policy and its machine group does not have a policy, but its organization has Policy C set. The endpoint will use Policy C.
- An endpoint does not have a policy and neither does its machine group or organization. The endpoints will use the default policy.

6.6.1. Organizations Tab

Here you can set a policy on an organization. Any machine groups and endpoints under the organization will use the policy set on the organization, as long as they do not have another policy set at machine group or endpoint level.

If no policy is set on an organization, it uses the default policy.

Column	Description
Name	Name of the organization
Policy	Current assigned policy. Bold text means that it is explicitly set on the organization
Machines	The number of machines under the organization

6.6.2. Machine Groups Tab

On this tab you can set a policy on a machine group. You can also see what policy each machine group is inheriting from its organization. Sub-machine groups are also supported, so assigning a policy to a machine group will cause all of that group's subgroups to inherit that policy.

Column	Description
Name	Name of the machine group
Policy	The policy that will be used by the machine group. Bold text means it was explicitly set on the machine group.
Inherited From	Where the policy is assigned from. **Self** means it was explicitly set on the machine group. **Blank** means it is using the default policy. Otherwise, it displayss the organization or machine group that is inheriting it from.
Machines	The number of machines in the machine group

6.6.3. Machines Tab

This is where you can override any inherited policy on an individual endpoint by assigning another policy explicitly.

Column	Description
Name	Name of the machine
Group	Machine group that the machine is in
Policy	The policy that will be used by the machine
Inherited From	Where the policy is assigned from. **Self** means it was explicitly set on the machine. **Blank** means it is using the default policy. Otherwise, it shows the organization or machine group that it is inheriting from.
Current Policy	Displays the last successfully applied policy. If you recently changed the policy assigned to the machine or there were problems deploying the policy, this value will be different than the **Policy** column.

6.6.4. Set Policy

To set the policy on an organization, machine group, or machine:

1. Select it from the appropriate table and click **Set Policy**. This will open a drop down list with the available policies.
2. Select the one you want to assign and click **Ok**. Multiple objects can be selected and assigned a policy at the same time.

Note
Policy update tasks will be created after the **Deploy** dialog is closed. This means you can make as many **Set** and **Clear Policy** choices as you want without flooding an unnecessary amount of policy update tasks on the machines.

6.6.5. Clear Policy

To unset a policy from an organization, machine group, or machine, select it from the table and click **Clear Policy**. This will remove any policy assignment that was set specifically on that object. The object will then start inheriting its policy based on the inheritance rules outlined earlier.

6.7. Policy Settings

General settings help you manage user interface display options, communication options, update preferences, password protection and other settings of Endpoint Security.

6.7.1. General, Details

The **Details** page displays general policy details:

- Policy name
- The user who created the policy
- The date and time when the policy was created
- The date and time when the policy was last modified

You can rename the policy by entering the new name in the corresponding field and clicking **Save**. Policies should have suggestive names so that you or other administrator can quickly identify them.

6.7.2. General, Display

In this section you can configure the user interface display options.

Enable Silent Mode

Use the check box to turn silent mode on or off. **Silent Mode** is designed to help you easily disable user interaction in Endpoint Security. When turning on **Silent Mode**, the following options are disabled: **Show icon in notification area**, **Display notification pop-ups** and **Display alert pop-ups**.

Show icon in notification area

Select this option to show the Bitdefender icon in the notification area (also known as the system tray). The icon informs users on their protection status by changing its appearance and displaying a corresponding notification pop-up. Additionally, users can right-click it to quickly open the Endpoint Security main window or **About** window. Opening the **About** window automatically initiates an on-demand update.

Display notification pop-ups

Select this option to inform users about important security events (such as the detection of malware) and the action taken, through small notification pop-ups. The pop-ups disappear automatically within a few seconds, without user intervention.

Display alert pop-ups

Different from notification pop-ups, alert pop-ups prompt users for action. If you choose not to display alert pop-ups, Endpoint Security automatically takes the recommended action. Alert pop-ups are generated in the following situations:

- If the firewall is set to prompt the user for action whenever unknown applications request network or Internet access.
- If Advanced Threat Control/Intrusion Detection System is enabled, whenever a potentially dangerous application is detected.
- If device scanning is enabled, whenever an external storage device is connected to the computer. You can configure this setting in the **Antimalware > On-demand** section.

Status Alerts

Users can determine when your endpoint has security configuration issues or other security risks, based on status alerts. For example, users can view

whenever there is a problem related to antimalware protection, such as: on-Access scanning module is disabled or a full system scan is overdue.

Users are informed about the protection status in two ways:

- By the notification area of the main window, which displays an appropriate status message and changes its color depending on the severity of the security issues. You have the possibility to view issue details as well, by clicking the available button.
- By the Bitdefender icon in the system tray, which changes its appearance when issues are detected.

Endpoint Security uses the following color scheme for notification area:

- **Green**: No issues are detected.
- **Orange**: The endpoint has non-critical issues that affect its security. Users do not need to interrupt current work for resolving these issues.
- **Red**: The endpoint has critical issues that require the user's immediate action.

To configure the status alerts, select the alerting level that best suits your needs: **Enable All**, **Custom**, **Disable All**.

If you want to customize alerts:

1. Select the **Custom** level of the scale.
2. Select the security aspects that you want to be monitored. The options are described herein:
   - **General**. The status alert is generated whenever a system restart is required during or after a product maintenance operation. You may choose to show the alert as a warning or a critical issue.
   - **Antimalware**. Status alerts are generated in the following situations:

     You may select how to show the alerts and define the number of days from the last full system scan.

     – On-Access scanning is enabled but many local files are skipped.

     – A certain number of days have passed since the last full system scan has been performed on the machine.

- **Update**. The status alert is generated whenever a system restart is required to complete an update operation. You may select to show the alert as a warning or a critical issue.

Technical Support Information

You can customize the technical support and contact information available in Endpoint Security by filling in the corresponding fields. Users can access this information from the Endpoint Security window by clicking the icon in the lower right corner or, alternatively, by right-clicking the Bitdefender icon in the system tray and selecting **About**.

6.7.3. General, Advanced

In this section you can configure general settings and the uninstall password.

Remove events older than (days)

Endpoint Security keeps a detailed log of events concerning its activity on the computer (also including computer activities monitored by Content Control). By default, events are deleted from the log after 30 days. If you want to change this interval, choose a different option from the menu.

Submit crash reports to Bitdefender

Select this option if you want reports to be sent to Bitdefender Labs for analysis if Endpoint Security crashes. The reports will help our engineers find out what caused the problem and prevent it from occurring again. No personal information will be sent.

Password configuration

To prevent users with administrative rights from uninstalling protection, you must set a password.

The uninstall password can be configured before installation by customizing the installation package. If you have done so, select **Keep current settings** to keep the current password.

To set a password or to change the current one, select **Enable password** and enter the desired password. To remove password protection, select **Disable password**.

6.7.4. General, Update

In this section you can configure the Endpoint Security and malware signature update settings. Updates are very important as they allow countering the latest threats

Product Update

Endpoint Security automatically checks for, downloads and installs updates every hour. Automatic updates are performed silently in the background.

- **Recurrence**. To change the automatic update recurrence, select a different option from the menu and configure it according to your needs.
- **Postpone reboot**. Some updates require a system restart to install and work properly. By selecting this option, the program will keep working with the old files until the computer is restarted, without informing the user. Otherwise, a prompts the user to restart the system whenever an update requires it.
- If you choose to postpone reboot, you can set a convenient time when computers will reboot automatically if (still) needed. This can be very useful for servers. Select **If needed, reboot after installing updates** and specify when it is convenient to reboot (daily or weekly on a certain day, at a certain time of day).

Signature Update

Endpoint Security automatically checks for signature updates every hour. Automatic updates are performed silently in the background. To change the automatic update recurrence, choose a different option from the menu and configure it according to your needs.

Proxy Settings

Select this option if computers connect to the Internet (or to the local update server) through a proxy server. There are three options to set the proxy settings:

- **Import proxy settings from default browser**. Endpoint Security can import proxy settings from most popular browsers, including the latest versions of Internet Explorer, Mozilla Firefox and Opera.
- **Auto-detect network proxy**. Endpoint Security uses the Web Proxy Auto-Discovery (WPAD) protocol included in Windows to automatically retrieve proxy settings from a Proxy Auto-Configuration (PAC) file published on the local network. If no PAC file is available, updates will fail.
- **Use custom proxy settings**. If you know the proxy settings, select this option and then specify them:
  - **Server** - enter the IP of the proxy server.
  - **Port** - enter the port used to connect to the proxy server.

- **Username** - enter a user name recognized by the proxy.
- **Password** - enter the valid password of the previously specified user.

> **Note**
> Changing the proxy configuration option will overwrite existing proxy settings in Endpoint Security.

- Additionally, you can select the **Use Proxy** check box corresponding to the update location to which the settings apply (the Internet or local update server address).

Update Locations

To avoid overloading the outside network traffic, Endpoint Security is configured to update from the local GravityZone update server. You can also add other update server addresses to the list and configure their priority using the up and down buttons displayed on mouse-over. If the first update location is unavailable, the next one is checked and so on.

To set the local update address:

1. Enter the address of the local update server in the **Update Server URL** field. Use one of these syntaxes:
   - `update_server_ip:port`
   - `update_server_name:port`

   > **Note**
   > The default port is 7074.

2. Select **Use a Proxy** if client computers connect to the local update server through a proxy server.
3. Click **Add**.

To remove a location from the list, move the cursor over it and click **Delete**. It is not reccommended to remove the default update location.

6.7.5. Antimalware

The Antimalware module protects the system against all kinds of malware threats (viruses, trojans, spyware, rootkits, adware and so on). The protection is divided in two categories:

- On-access scanning: prevents new malware threats from entering the system.
- On-demand scanning: allows detecting and removing malware already residing in the system.

When a threat is detected, Endpoint Security automatically attempts to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as **disinfection**. Files that cannot be disinfected are moved to quarantine in order to isolate the infection. When a malicious file is in quarantine, it cannot do any harm because it cannot be executed or read.

Advanced users can configure scan exclusions if they do not want specific files or file types to be scanned.

6.7.6. Anti-Malware, On-Access

In this section you can configure the two real-time antimalware protection components:

On-access Scanning Settings

On-access scanning prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA).

To configure on-access scanning:

1. Use the check box to turn on-access scanning on or off. If you turn on-access scanning off, computers will be vulnerable to malware.
2. For a quick configuration, click the security level that best suits your needs (**Aggressive**, **Normal** or **Permissive**).
3. You can configure the scan settings in detail by selecting the **Custom** protection level.

   Scan local files

   Use these option to specify which types of files you want to be scanned. Scan preferences can be configured separately for local files (stored on the

local computer) or network files (stored on network shares). If antimalware protection is installed on all computers in the network, you can disable the network files scan to allow for a faster network access.

You can set Endpoint Security to scan all accessed files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. **Scanning all accessed files** provides best protection, while **Scanning applications only** can be used for better system performance.

If you want only specific extensions to be scanned, select **User defined extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

For system performance reasons, you can also exclude large files from scanning. Select the **Maximum size (MB)** check box and specify the size limit of the files to be scanned. Keep in mind that malware can affect larger files too.

Archives

Select **Scan inside archives** if you want to enable on-access scanning of archived files. Scanning inside archives is a slow and resource-intensive process, therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having on-access scanning enabled.

If you decide to use this option, you can configure the following optimization alternatives:

- **Archive maximum size (MB)**. You can set a maximum accepted size limit of archives to be scanned on-access. Select the corresponding check box and type the maximum archive size (in MB).
- **Archive maximum depth (levels)**. Select the corresponding check box and select the maximum archive depth from the menu. For best performance, select the lowest value. For maximum protection, select the highest value.

Miscellaneous

Select the corresponding check boxes to enable the desired scan options.

- **Scan boot sectors**. Scans the system's boot sector. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become

inaccessible and you may not be able to start your system and access your data.

- **Scan only new or changed files**. By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan for keyloggers**. Keyloggers record what you type on your keyboard and send reports over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.
- **Scan for Potentially Unwanted Applications (PUA)**. A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with free software. Such programs can be installed without the user's consent (also called adware) or is included by default in the express installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

Scan Actions

Depending on the type of detected file, the following actions are taken automatically:

When a suspect file is detected, users will be denied access to that file in order to prevent a potential infection.

Though not recommended, you can change the default actions. You can define two actions for each type of file. The following actions are available:

Deny access: Deny access to detected files.
Disinfect: Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.
Delete: Delete detected files from the disk, without any warning. It is advisable to avoid using this action.
Move to quarantine: Move detected files from their current location to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantined files from the **Quarantine** page of the console.

- **Default action for infected files**. Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Endpoint Security can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as **disinfection**.

  If an infected file is detected, Endpoint Security automatically attempts to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

  Important
  For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- **Default action for suspect files**. Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Endpoint Security cannot be sure that the file is actually infected with malware. Suspect files cannot be disinfected, because no disinfection routine is available.

Advanced Threat Control Settings

Bitdefender Advanced Threat Control is an innovative proactive detection technology which uses advanced heuristic methods to detect new potential threats in real time.

Advanced Threat Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered harmful and Advanced Threat Control will automatically try to disinfect the detected file. If the disinfection routine fails, Advanced Threat Control will delete the file.

Note
Before applying the disinfect action, a copy of the file is sent to quarantine and you can restore the file later, in the case of a false positive. This action can be configured using the **Copy files to quarantine before applying the disinfect action** option available in the **Quarantine** tab of the policy settings. This option is enabled by default in the policy templates.

To configure Advanced Threat Control:

1. Use the check box to turn Advanced Threat Control on or off. If you turn Advanced Threat Control off, computers are vulnerable to unknown malware.
2. The default action for infected applications detected by Advanced Threat Control is **Disinfect**. To set another default action, use the available menu.
3. Click the security level that best suits your needs: **Aggressive**, **Normal** or **Permissive**.

   Note
   As you set the protection level higher, Advanced Threat Control requires fewer signs of malware-like behavior to report a process. This leads to a higher number of applications being reported and, at the same time, to an increased likelihood of false positives (clean applications detected as malicious).

4. You should create exclusion rules for commonly used or known applications to prevent false positives (incorrect detection of legitimate applications). Go to the **Exclusions** tab and configure **ATC process exclusion rules** for trusted applications.

6.7.7. Antimalware, On-Demand

In this section you can configure antimalware scan tasks that will run regularly on the target computers, according to the schedule you specify.

The scan is performed silently in the background. The user is informed that a scanning process is running through an icon that appears in the system tray. Though not mandatory, it is recommended to schedule a comprehensive system scan to run weekly on all computers. Scanning computers regularly is a proactive security measure that can help detect and block malware that might evade real-time protection features.

Besides regular scans, you can also configure the automatic detection and scanning of external storage media.

Managing Scan Tasks

The **Scan Tasks** table informs you of the existing scan tasks, providing important information on each of them:

- Task name and type

- Schedule based on which the task runs regularly (recurrence)
- Date and time the task was first run

There are two default system scan tasks which you can configure to run as needed:

- **Quick Scan** uses in-the-cloud scanning to detect malware running in the system. Running a quick scan usually takes less than a minute and uses a fraction of the system resources of a regular antimalware scan.
- **Full Scan** checks the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

The scan options of the default scan tasks are preconfigured and you cannot change them.

Besides the default scan tasks (which you cannot delete or duplicate), you can create as many custom scan tasks as you want. A custom scan task allows you to choose the specific locations to be scanned and to configure the scan options.

To create and configure a new custom scan task, click the **Add** button at the right side of the table. To change the settings of an existing scan task, click the name of that task. Refer to the following topic to learn how to configure the task settings.

To remove a task from the list, select the task and click **Delete**.

Configuring Scan Tasks

The scan task settings are organized under three tabs:

- **General**: set the task name and execution schedule.
- **Options**: set a scan profile for quick configuration of the scan settings and define scan settings for a custom scan.
- **Target**: select the files and folders to be scanned.

Options are described herein, from the first tab to the last:

Details

Enter a suggestive name for the task to easily identify what it is about. When choosing a name, consider the scan task target and possibly the scan settings.

Scheduler

You can set the scan to run every few hours, days or weeks, starting with a specified date and time.

Please consider that computers must be on when the schedule is due. A scheduled scan will not run when due if the computer is turned off, hibernating or in sleep mode, or if no user is logged on. In such situations, the scan is postponed until next time.

Note
The scheduled scan will run at the target endpoint local time. For example, if the scheduled scan is set to start at 6:00 PM and the endpoint is in a different timezone than Control Center, the scanning will start at 6:00 PM (endpoint time).

Scan Options

Click the security level that best suits your needs: **Aggressive**, **Normal** or **Permissive**.

Based on the selected profile, the scan options in the **Settings** section are automatically configured. However, if you want to, you can configure them in detail. To do that, select **Custom**.

File Types

You can set Endpoint Security to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. **Scanning all files** provides best protection, while **Scanning applications only** can be used to perform a quicker scan.

Note
Application files are far more vulnerable to malware attacks than other types of files. If you want only specific extensions to be scanned, choose **User Defined Extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

Archives

Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

Note
Scanning archived files increases the overall scanning time and requires more system resources.

Scan inside archives. Select this option if you want to check archived files for malware. If you decide on using this option, you can configure the following optimization options:

- **Limit archive size to (MB)**. You can set a maximum accepted size limit of archives to be scanned. Select the corresponding check box and type the maximum archive size (in MB).
- **Maximum archive depth (levels)**. Select the corresponding check box and choose the maximum archive depth from the menu. For best performance select the lowest value, for maximum protection select the highest value.

Scan email archives. Select this option if you want to enable scanning of email message files and email databases, including file formats such as `.eml`, `.msg`, `.pst`, `.dbx`, `.mbx`, `.tbb` and others. Note that email archive scanning is resource intensive and can impact system performance.

Miscellaneous

Select the corresponding check boxes to enable the desired scan options.

Scan boot sectors. Scans the system's boot sector. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.

Scan registry. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.

Scan for rootkits. Select this option to scan for rootkits and objects hidden using such software.

Scan for keyloggers. Select this option to scan for keylogger software.

Scan memory. Select this option to scan programs running in the system's memory.

Scan cookies. Select this option to scan the cookies stored by browsers on the computer.

Scan only new and changed files. By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.

Scan for Potentially Unwanted Applications (PUA). A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with free software. Such programs can be installed without the user's consent (also called adware) or is included by default in the express installation kit (ad-supported). Potential effects of these programs include the

display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

Actions

Depending on the type of detected file, the following actions are taken automatically:

Default action for infected files. Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Endpoint Security can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

If an infected file is detected, Endpoint Security will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

> **Important**
> For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

Default action for suspect files. Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Endpoint Security cannot be sure that the file is actually infected with malware. Suspect files cannot be disinfected, because no disinfection routine is available.

Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine. Quarantined files are sent for analysis to Bitdefender Labs on a regular basis. If malware presence is confirmed, a signature is released to allow removing the malware.

Default action for rootkits. Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

Detected rootkits and hidden files are ignored by default.

Though not recommended, you can change the default actions. You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file. The following actions are available:

Take no action: No action will be taken on detected files. These files will only appear in the scan log.
Disinfect: Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.
Delete: Delete detected files from the disk, without any warning. It is advisable to avoid using this action.
Move to quarantine: Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the **Quarantine** page of the console.

Scan Target

To add a new file or folder to be scanned:

1. Select a predefined location from the drop-down menu or enter the specific paths you want to scan.
2. Specify the path to the object to be scanned in the edit field.
   - If you select a predefined location, complete the path as needed. For example, to scan the entire **Program Files** folder, it suffices to select the corresponding predefined location from the drop-down menu. To scan a specific folder from **Program Files**, you must complete the path by adding a backslash (\) and the folder name.
   - If you select **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.
3. Click the corresponding **Add** button.

   To edit an existing location, click it. To remove a location from the list, move the cursor over it and click the corresponding **Delete** button.

Exclusions

You can either use the exclusions defined in the **Antimalware, Exclusions** section of the current policy, or you can define custom exclusions for the current scan task. For more details regarding exclusions, refer to Exclusions.

Device Scanning

You can configure Endpoint Security to automatically detect and scan external storage devices when connected to the computer. Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- Mapped network drives
- Devices with more than a specified amount of stored data.

Device scans automatically attempt to disinfect files detected as infected or to move them to quarantine if disinfection is not possible. Take into account that no action can be taken on infected files detected on CDs/DVDs or on mapped network drives that allow read-only access.

Note
During a device scan, the user can access any data from the device.

If alert pop-ups are enabled in the **General > Display** section, the user is prompted whether or not to scan the detected device instead of the scan starting automatically.

When a device scan is started, a notification pop-up informs the user about the device scan, provided that notification pop-ups are enabled in the **General > Display** section. Once the scan is completed, the user must check detected threats, if any.

Select the **Device Scanning** option to enable the automatic detection and scanning of storage devices. To configure device scanning individually for each type of device, use the following options:

- **CD/DVD media**
- **USB storage devices**
- **Mapped network drives**
- **Do not scan devices with stored data more than (MB)**. Use this option to automatically skip scanning a detected device if the amount of stored data exceeds the specified size. Enter the size limit (in megabytes) in the corresponding field. Zero means that no size restriction is imposed.

  Note
  This option applies only to CDs/DVDs and USB storage devices.

6.7.8. Antimalware, Exclusions

Exclusions can apply to on-access scanning or on-demand scanning, or to both. Based on the object of the exclusion, there are four types of exclusions:

- **File exclusions**: the specified file only is excluded from scanning.
- **Folder exclusions**: all files inside the specified folder and all of its subfolders are excluded from scanning.
- **Extension exclusions**: all files having the specified extension are excluded from scanning.
- **Process exclusions**: any object accessed by the excluded process is also excluded from scanning. You can also configure process exclusions for the Advanced Threat Control and Intrusion Detection System technologies.

> **Important**
> Scan exclusions should only be used in special circumstances or following Microsoft or Bitdefender recommendations. If you have an EICAR test file that you use periodically to test antimalware protection, you should exclude it from on-access scanning.

Use the **Activate exclusions** check box to turn exclusions on or off.

To configure an exclusion rule:

1. Select the exclusion type from the menu.
2. Depending on the exclusion type, specify the object to be excluded as follows:
   - **Extension exclusions**. Specify one or more file extensions to be excluded from scanning, separating them with a semicolon ";". You can enter extensions with or without the preceding dot. For example, enter **txt** to exclude text files.

     > **Note**
     > Before you exclude extensions, document yourself to see which are commonly targeted by malware and which are not.

   - **File, folder and process exclusions**. You must specify the path to the excluded object on the target computers. Enter the full path to the object to be excluded. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

3. Select the types of scanning the rule will apply to. Some exclusions may be relevant for onaccess scanning only, some for on-demand scanning only, while others may be recommended for both. Process exclusions can be configured for on-access scanning and for the Advanced Threat Control and Intrusion Detection System technologies.

   Note
   On-demand scanning exclusions will not apply to contextual scanning. Contextual scanning is initiated by right-clicking a file or folder and selecting **Scan with Endpoint Security by Bitdefender**.

4. Click the **Add** button. The new rule will be added to the list. To remove a rule from the list, click the corresponding **Delete** button.

6.7.9. Antimalware, Quarantine

You can set Endpoint Security to automatically perform the following actions:

Delete files older than (days)
By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, select a different option from the menu.

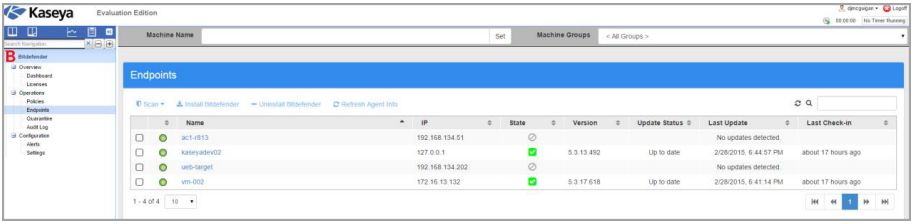
Submit quarantined files to Bitdefender Labs every (hours)
Keep this option selected to automatically send quarantined files to Bitdefender Labs. The sample files will be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware. By default, quarantined files are automatically sent to Bitdefender Labs every hour. If you want to change this interval, select a different option from the menu.

Rescan quarantine after malware signatures updates
Keep this option selected to automatically scan quarantined files after each malware signatures update. Cleaned files are automatically moved back to their original location.

Copy files to quarantine before applying the disinfect action
Select this option to prevent data loss in case of false positives and copy each file detected as infected to quarantine before applying the disinfect action. You can afterwards restore legitimate files from the **Quarantine** page.

7. ENDPOINTS

The **Endpoints** page is where Bitdefender can be installed, scans can be triggered, scan and task logs can be viewed, and agent specific audit logs can be found as well.



7.1. Endpoints Table

Column	Description
Name	The name of the endpoint
IP	The IP address of the endpoint
State	The current state of the endpoint (**Unknown**, **Unsupported**, **Unmanaged**, **Installed**, **Licensed**, **Discovering**, **Installing**, **Uninstalling**, **Updating License**)
Version	The current version number of the Bitdefender agent on the endpoint
Update Status	The current update status of the Bitdefender agent on the endpoint
Last Update	The last time the Bitdefender agent on the endpoint was updated
Last Check-in	The amount of time since the last refresh cycle was run on the endpoint.

7.2. Install/Uninstall

To install the Bitdefender agent on an endpoint, select it from the table. If the value in the **State** column is a grey question mark or an empty black square, then simply click **Install Bitdefender** to start the installation process. If the value in the **State** column is not either of those images, then Bitdefender either cannot be installed

or is already installed on that endpoint. In the case of the latter, the agent will detect that it is already installed and will reinstall if the downloaded package is of a higher version than the currently installed package. If more than one endpoint is selected when **Install Bitdefender** is clicked, the installation process will trigger for all selected endpoints.

To uninstall, select an endpoint from the table that currently has a Bitdefender agent installed. Like with installation, multiple endpoints can be selected at once. When the desired endpoints are selected, click **Uninstall Bitdefender**, and the uninstall process will begin.

7.3. Scans

In addition to installation controls, the **Endpoints** page also has controls for triggering scans on the licensed Bitdefender agents.

Full Scan

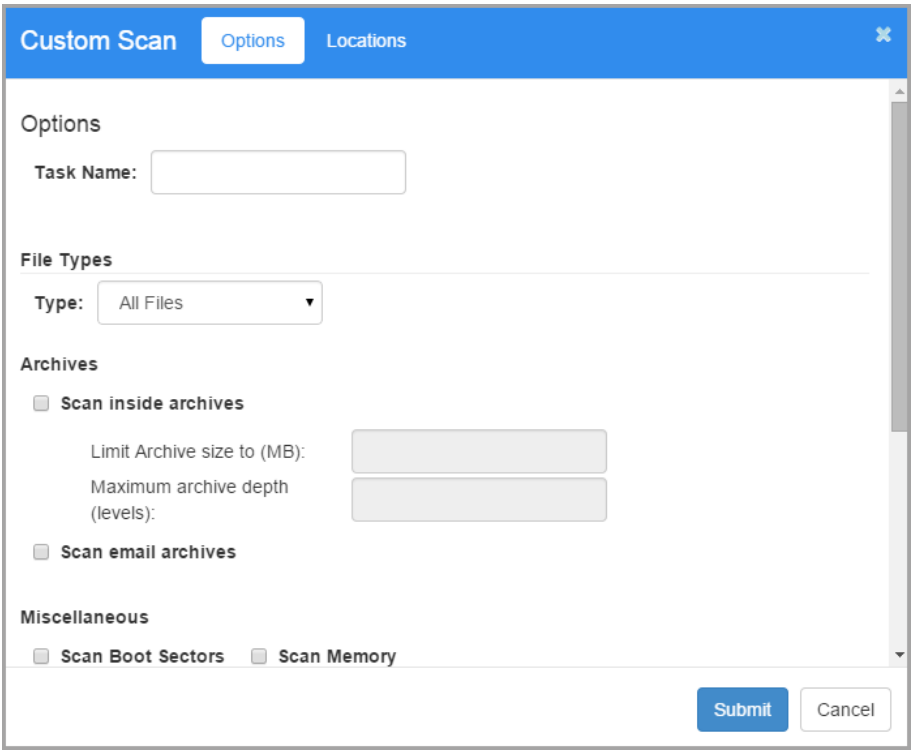
To perform a full scan, select the desired endpoints to run the scan on. As with the installation features, **Full Scan** supports multi-selection of endpoints so the scan can be run simultaneously on multiple endpoints. Click **Scan** and then select **Full Scan** from the drop down list.

Quick Scan

To perform a quick scan, select the desired endpoints to run the scan on. As with the installation features, **Quick Scan** supports multi-selection of endpoints so the scan can be run simultaneously on multiple endpoints. Click **Scan**, and then select **Quick Scan** from the drop down list.

Custom Scan

To perform a custom scan, select the desired endpoints to run the scan on. As with the installation features, **Custom Scan** supports multi-selection of endpoints so the scan can be run simultaneously on multiple endpoints. Click **Scan**, and then select **Custom Scan** from the drop down list.



This dialog provides for the customizing of the scan task to suit individual needs. There are two pages to configure, one with the scan settings, and the second page contains the scan path and exclusion settings. To switch between them, simply click on the name in the top of the dialog. Once all settings are configured, click **Submit** to start the scan.

7.4. Refresh Agent Info

The **Refresh Agent Info** button can be used to trigger an immediate refresh of the state of an endpoint. It executes the same process as what is run in the background, fetching the last update times, latest quarantine, and updating the license information for the Bitdefender agent.

7.5. Agent Information Dialog

Scan Log

The scan log pane provides an area to view the scan logs of all executed scans. To view a scan, select the respective entry based on the type of scan and time it occurred. Once selected, it populates the fields below the drop down list with the data from the selected scan.

Blocked Apps

The **Blocked Apps** pane lists all instances of Bitdefender detecting a suspicious application and blocking its execution on the endpoint.

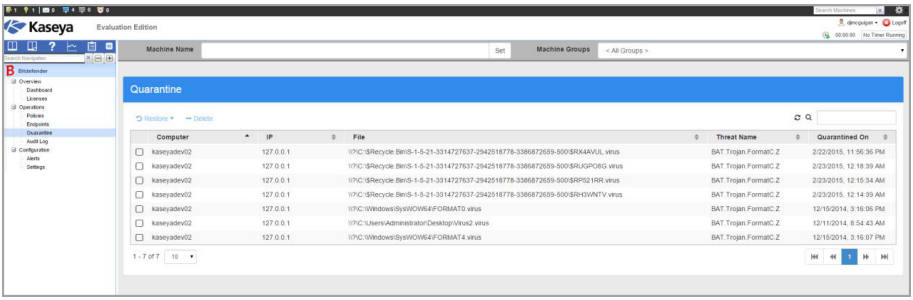
Tasks

The task pane is composed of a list of all tasks executed on the endpoint. Each entry lists the name of the task, what type of task it was, what its current status is (**Pending**, **Errored**, **Success**), a message (if one exists), and the time that the task was initiated. Generally this serves as a log of when scans, installs and quarantine commands were executed and whether or not they were successful.

Audit Log

The audit log pane is a filtered version of the global audit log. The records that can be viewed here are related to either the endpoint or to the plugin as a whole. Records related to other endpoints are excluded.

8. QUARANTINE



8.1. Quarantine Table

Column	Description
Computer	The name of the endpoint
IP	The IP address of the endpoint
File	The complete file path of the threat that was quarantined
Threat Name	The name of the threat that was quarantined
Quarantined On	The time when the file was quarantined on the endpoint

8.2. Restore

There are two options when it comes to restoring a file from the quarantine:

Original Location

To restore a file to its original location, select the file(s) that are to be restored, and then click **Restore** and select **Original Path**. This will remove the entry from the table and start the process to restore the file from the quarantine on the endpoint.

Custom Location

To restore a file to a custom location, select the file(s) that are to be restored. Click **Restore** and select **Custom Location**. This will bring up a dialog prompt asking for a path. Enter the path to be used to restore all selected files to and click **Restore**.

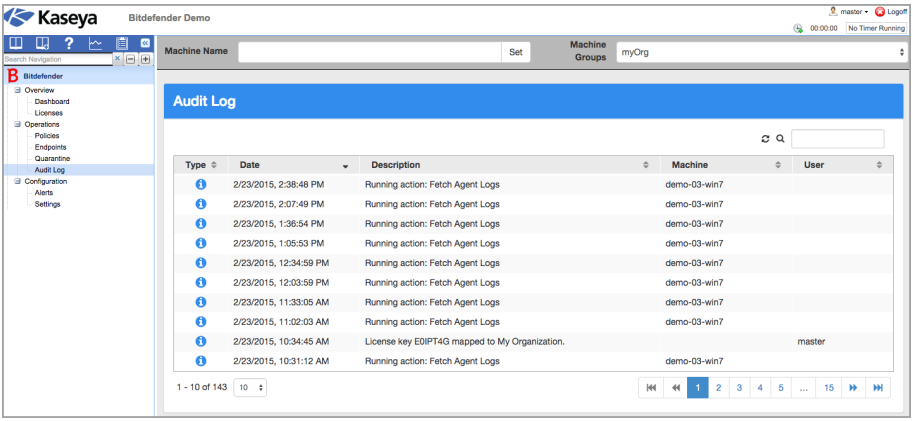
Note
The path submitted is used on all endpoints. If a unique path is desired for each file or by endpoint, then multiple custom restores will need to be done for each path that is to be used.

8.3. Delete

To delete a file from the quarantine, select the file(s) that you want to delete and click **Delete**. This will remove the entries from the table and begin the process to delete the file from the endpoint's quarantine.

9. AUDIT LOGS

The audit log is a global list of all actions taken within the plugin, as well as a log of errors or other information that would be relevant for end-users. If a task returns with an error, more information can be found in the audit log as to what specifically went wrong, and should there be a need to contact support, this will be a valuable location for gathering information for them to be able to determine the cause of the problems.

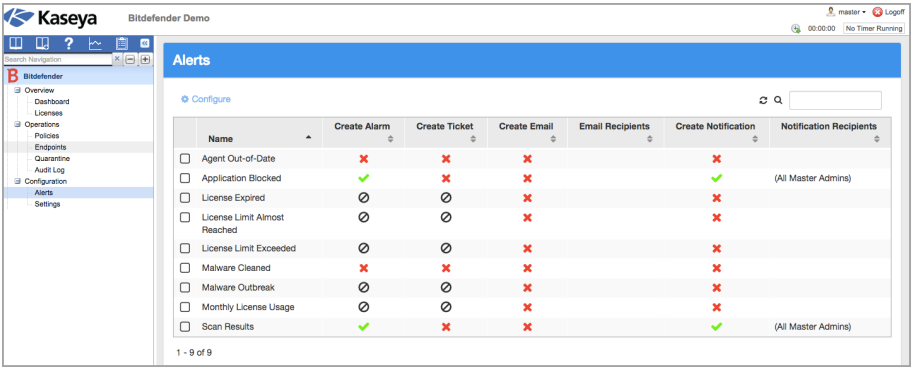


9.1. Audit Log Table

Column	Description
Type	The type of record entry (Info, Warning, Error)
Date	The time that the record was created
Description	The description of the log entry
Machine	The name of the endpoint related to the log entry. Can be blank.
User	The name of the account related to the log entry. Can be blank.

10. ALERTS

Alerts provide a mechanism for receiving notifications when certain events happen within the plugin. These notifications can be sent through four different Kaseya methods: alarms, tickets, emails, and the notification bar. Detection of alerting events happens in a background process on the Kaseya server. Settings for alerts are found on the **Settings** page.



10.1. Alerts Table

The **Alerts** table lists all of the alerts available in the plugin. It shows which method each of the alerts will use to send notifications.

Note
Some alerts do not have the **Alarm** and **Ticket** options available. Both the **Alarm** and **Ticket** methods require a specific endpoint to be specified, and some of these alerts are not specific to one machine.

Column	Description
Name	The name of the alert
Create Alarm	Will the alert create a Kaseya alarm when triggered?
Create Ticket	Will the alert create a Kaseya ticket when triggered?
Create Email	Will the alert send an email when triggered?
Email Recipients	The email address that the alert email will be sent to

Column	Description
Create Notification	Will the alert add a notification to the notification bar when triggered?
Notification Recipients	The Kaseya admins who will receive notifications in the notification bar for that alert.

10.2. Configure

To configure an alert, select the alert in the table and click the **Configure** button. This will open the **Configure Alert** dialog. Select the alert methods you want to use. Click **Save** when you are done and the **Alerts** table will update to reflect your selections.

10.3. Alert Methods

Alarm

The **Alarm** method creates a Kaseya alarm when the alert is triggered. These alarms can be found in the Monitoring module of Kaseya, under the **Alarm** page. Each alarm is tied to a specific machine, so this option is unavailable for general alerts. Alarms will also have a link to a ticket, if the ticket method is also used for the alert.

Ticket

The **Ticket** method creates a Kaseya ticket, either in the Ticketing module or, if configured, in the Service Desk module. Tickets are linked to a specific machine therefore unavailable for general alerts.

Email

The **Email** method uses the email mechanism in Kaseya to send an email when the alert is triggered. You can set up your email settings in the System module, under the **Outbound Email** page. The **From** address on the emails will be the default sender as it is configured on the **Outbound Email** page in Kaseya.

Notification Bar

The **Notification Bar message** method creates a notification that is displayed under the alarm clock icon on the top bar in Kaseya. You can specify which Kaseya admins see these notifications or generally send them to all Master administrators.

10.4. Types of alerts

Agent Out-of-Date

The **Agent Out-of-Date** alert triggers when a Bitdefender agent's **Last Updated** date is older than the default threshold, which is seven days. The number of days used for this threshold is configurable on the **Settings** page.

This classification of 'out-of-date' is different than the update status seen on the **Endpoints** page. The update status is set by the automatic update process running on each agent. If the update process has a problem, the status may go to **Out-of-Date**. However, because this process is happening down on the remote machine, if there is a problem receiving that information back to the Kaseya server, the update status will stay at whatever its last value was.

This alert, however, will trigger based on the **Last Update** date becoming too old. So if the Kaseya agent stops reporting information back to the Kaseya server, you will still get a notification.

Application Blocked

The **Application Blocked** alert triggers whene a Bitdefender agent blocks an application from running because it detects malicious code. This is done on a per-application, per-endpoint basis.

License Expired

The **License Expired** alert triggers when one of your licenses expiration date is getting closer. The four times it notifies are:

1. Less than 30 days remaining on the license.
2. Less than 7 days remaining on the license.
3. Less than 1 day remaining on the license.
4. License is expired.

License Limit Almost Reached

The **License Limit Almost Reached** alert is triggered when the number of used slots on a license exceeds a certain percentage of the total license slots. By default this is set at 90% of license capacity, but this value is configurable on the **Settings** page. Use this alert to get advanced warning before a license runs out of slots.

License Limit Exceeded

The **License Limit Exceeded** alert is triggered when all of a license slots are used. At this point, the license will not activate any more Bitdefender agents, and if the total capacity has actually been exceeded for some reason (such as moving licensed Kaseya endpoints between organizations with different licenses), it will start to deactivate Bitdefender agents.

Malware Cleaned

The **Malware Cleaned** alert is triggered whenever a Bitdefender agent detects some kind of malware and either deletes, cleans or quarantines it.

Malware Outbreak

The **Malware Outbreak** alert is triggered when a certain percentage of licensed machines are infected with the same malware within a certain amount of time. By default, this is configured for 10% of endpoints within the last two days. Both of those numbers can be configured on the **Settings** page.

Monthly License Usage

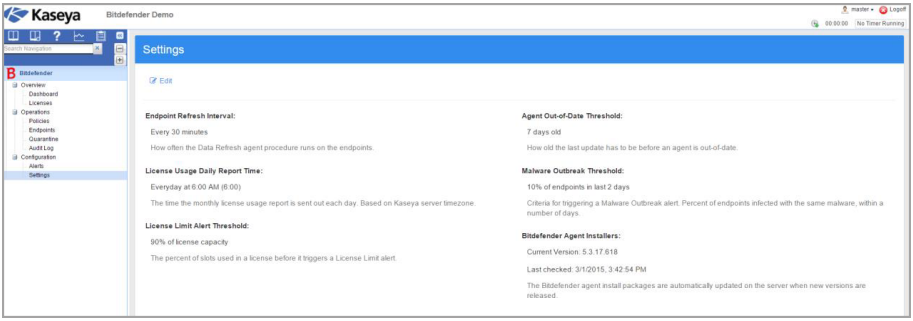
The **Monthly License Usage** alert is sent out every day and reports how much of the monthly license is being used and by what organizations. This alert is only useful if you are using a monthly license with the plugin. You can configure what time of day this alert is sent on the **Settings** page.

Scan Results

The **Scan Results** alert is triggered whenever a scan finished on an endpoint. After the scan logs are retrieved by the plugin, this alert will provide a brief summary of the scan's results, such as how many files were scanned, how many were clean, and how many were infected.

11. SETTINGS

The **Settings** pane displays the **Endpoint Refresh Interval**, **License Usage Daily Report Time**, **License Limit Alert Threshold**, **Agent Out-of-Date Threshold** and **Malware Outbreak Threshold** currently set in the module.



From this pane, you are able to make changes to each of these items by simply selecting edit. This allows you to customize alerts based on your specific needs as set by your organization.

11.1. Endpoint Refresh Interval

The endpoint refresh interval is the amount of time the system waits before fetching the next set of data from all of the licensed endpoints managed by the plugin. This is set to 30 minutes by default when the plugin is installed, and each endpoint has its own timer, as opposed to having all endpoints updated simultaneously based on the server cycle. What this means is that one endpoint may begin its refresh two minutes after another endpoint, every cycle.

To set a custom interval, click **Edit** at the top of the pane and enter the desired interval time in the text field for the **Endpoint Refresh Interval** section. Click **Save**.

11.2. License Usage Daily Report Time

The daily license usage report comes once a day at a specified time. It contains information about how many endpoints are making use of any recurring monthly licenses that have been added to the licenses page. The default time for this is 6:00 AM in the time zone that the Kaseya server has been set up in.

To customize this value, click **Edit** and select the desired time from the dropdown under the **License Usage Daily Report Time** section. Click **Save**.

11.3. License Limit Alert Threshold

The license limit alert threshold is the percentage of a license that needs to be used to trigger the alert. This value is set to 90% by default, but can be modified.

To customize this value, click **Edit** and edit the value under the **License Limit Alert Threshold** section to be the percentage of slots used on a license that will trigger an alert. Click **Save**.

Note
An alert will not be generatef if it is not configured on the **Alerts** page. For more information on this, please see the Alerts section of this guide.

11.4. Agent Out-of-Date Threshold

The out of date threshold is the number of days an agent has to have gone without an update before it is considered out of date by the plugin. This value is set to 7 by default.

To customize this value, click **Edit** and enter a value under the **Agent Out-of-Date Threshold** section to be the number of days to wait before firing an alert. Click **Save**.

11.5. Bitdefender Agent Installers

The Bitdefender agent installers section is an informational section, detailing the latest version of the Bitdefender agent obtained from Bitdefender's servers as well as the last time a check was made for a more recent version. If a newer version of Bitdefender is found, then the installer on the Kaseya server is updated automatically.

12. UNINSTALLING

12.1. Uninstalling the Bitdefender Agent

There are two approaches you can take to uninstalling the Bitdefender Endpoint Security agent from an endpoint. If the endpoint is visible in the Kaseya plugin, you can use the plugin's **Uninstall** function to start the uninstall process. Otherwise, or if the remote uninstall fails, you can log into the endpoint and manually uninstall the agent.

Remote Uninstall

To remotely uninstall the Bitdefender Endpoint Security agent through the plugin, follow these steps:

1. Open the **Endpoints** page in the Bitdefender module in Kaseya.
2. Select the endpoints you want to uninstall the agent from.
3. Click **Uninstall Bitdefender**.
4. Choose if you want the machine to reboot (only if needed after a successful uninstall).
5. Click **Continue**. The endpoint's state changes to **Uninstalling**.
6. Wait for a few minutes and check the task to see when the **Uninstall task** returns a result.

Manual Uninstall

To manually remove the Bitdefender Endpoint Security agent from a machine, follow these steps:

1. Log in to the endpoint.
2. Open the **Add/Remove Programs** window.
3. Select the **Endpoint Security by Bitdefender** entry.
4. Click **Uninstall**.
5. If you set an uninstall password on the policy for the agent or during installation, enter it now.
6. Follow the prompts to remove the agent.

Uninstalling the Plugin from Kaseya

To remove the plugin from Kaseya, follow these steps:

1. Log into the Kaseya server.
2. Open the **Add/Remove Programs** window.
3. Select the **Bitdefender Kaseya Plugin** entry.
4. Click **Uninstall**.
5. Follow the prompts to remove the plugin.

13. TROUBLESHOOTING

13.1. Troubleshooting Tips

The Bitdefender plugin has a number of services and utilities that need to run for the solution to work properly.

On the Kaseya server, there is a **Bitdefender Kaseya File Watcher** service that handles data coming back from the endpoints and runs continuous background processes. If this service goes down, the data on endpoints will stop updating in the plugin.

On the endpoints, there is a **Bitdefender Event Listener for Kaseya** service that is continuously listening for detection events from the Bitdefender Endpoint Security agent. Although Kaseya can still communicate with the Bitdefender agent without this service, it will not be able to get on-access malware detection or application blocked notifications unless it is running.

Logging Locations

Audit Log

The audit log is the primary logging location for the plugin. Everything, including the services on the Kaseya server and the endpoints, will attempt to get their logging messages into the audit log. You can access this log through the plugin's **Audit Log** page.

Agent Procedure Log

All of the actions and communication from the Kaseya plugin to the endpoints is done through agent procedures. There is always the possibility that an agent procedure could not execute correctly, so it is a good idea to check the Agent Procedure Logs in Kaseya is thing do not appear to be working correctly. These can be found in a number of ways, but one way is to hover over the dot icon next to an endpoint until the agent popup appears and then click on **Procedure Logs**.

Windows Event Logs

The two services that are used in the plugin will also write log entries to the Windows Event Log. You can see these by opening up the Event Viewer on the Kaseya server or one of the endpoints and looking under the **Application** log.

Enable Logging for Bitdefender Components

To enable logging for Bitdefender components on endpoints, such as Bitdefender.EndpointUtility.exe, follow these steps:

1. Login to endpoint.
2. Access the \kworking\Bitdefender folder (where you also find Bitdefender.EndpointUtility.exe) and create a file named debug.ini.
3. Write the line `=;` to the new file.

In this case, every time Bitdefender.EndpointUtility.exe will run, new entries will appear in debug.log file.

To disable logging, all you have to do is delete debug.ini.

Troubleshooting Scenarios

Problem	Troubleshooting Steps
Data is not getting updated on the endpoints (statuses aren't changed, scan logs are retrieved etc)	1. Check the agent procedure logs and verify that the Bitdefender procedures are returning successfully. 2. Check on the Kaseya server that the Bitdefender Kaseya File Watcher service is running, attempt to restart if it is.
Application blocked and on-access malware detection is not showing up from the endpoints	On the endpoint, check that the Bitdefender Event Listener for Kaseya service is running, restart if necessary.
Bitdefender agent procedures appear to be corrupted	1. Log into the Kaseya database through SQL Management Studio. 2. Run the following line: `EXEC [bitdef].[sp_DeleteAgentProcs]` 3. Then Run the following line: `EXEC [bitdef].[sp_ImportAgentProcs]`. This will remove and reimport the procedures.

Problem	Troubleshooting Steps
Uninstalling the product from multiple endpoints at once does not work	1. Log into the Kaseya database through SQL Management Studio. 2. Run the following line: `EXEC ksubscribers.bitdef.sp_DeleteAgentProcs` 3. Then run the following line: `EXEC ksubscribers.bitdef.sp_ImportAgentProcs`

13.2. Getting Help

Bitdefender strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issue with it or if you have any questions about your Bitdefender product, go to our online Support Center. It provides several resources that you can use to quickly find a solution or an answer. Or, if you prefer, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

Bitdefender Support Center

Bitdefender Support Center, available at http://www.bitdefender.com/support/business.html, is the place where you will find all the assistance you need with your Bitdefender product.

You can use several resources to quickly find a solution or an answer:

- Knowledge Base Articles
- Bitdefender Support Forum
- Product Documentation

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

Knowledge Base Articles

The Bitdefender Knowledge Base is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bug fixing activities of the Bitdefender support

and development teams, along with more general articles about malware prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Knowledge Base for business products is available any time at http://www.bitdefender.com/support/business.html.

Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others. You can post any problem or question related to your Bitdefender product.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic. The Bitdefender Support Forum is available at http://forum.bitdefender.com, in five different languages: English, German, French, Spanish and Romanian. Click the **Business Protection** link to access the section dedicated to business products.

Product documentation is the most complete source of information about your product.

You can check and download the latest version of documentation for Bitdefender Plugin for Kaseya in the **Settings** tab – **User Guide** link, bottom line.