



Bitdefender[®]

GravityZone

CONNECTWISE AUTOMATE INTEGRATION GUIDE

Bitdefender GravityZone ConnectWise Automate Integration Guide

Publication date 2022.02.23

Copyright© 2022 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.



Table of Contents

- 1. Overview 1
 - 1.1. Scope of This Document 1
- 2. Requirements 2
- 3. Setting Up the Integration 3
 - 3.1. Plugin Installation via Solution Center 3
 - 3.2. Manual Installation of the Plugin 5
 - 3.3. Plugin Update 6
 - 3.4. Configuring the Integration 7
 - 3.4.1. Generating the API Key 7
 - 3.4.2. Configuring Plugin Settings 9
 - 3.4.3. Configuring Alert Settings 10
 - 3.4.4. Configuring Package Defaults 12
 - 3.4.5. Configuring Client Mapping 13
 - 3.4.6. Configuring Client Subscriptions 16
 - 3.4.7. Configuring Computer Mapping 18
 - 3.5. Configuring Deployment 18
 - 3.5.1. Auto Deployment 18
 - 3.5.2. Deployment Actions 19
 - 3.5.3. Deployment Exclusions 20
 - 3.5.4. Deployment History 20
 - 3.6. Reviewing Plugin Status 21
- 4. Using the Integration 22
 - 4.1. Client Screen 22
 - 4.2. Location Screen 23
 - 4.2.1. Deployment Settings 24
 - 4.3. Computer Screen 25
 - 4.4. Tasks and Actions 26
 - 4.5. Security Events 27
 - 4.5.1. Advanced Threat Control 28
 - 4.5.2. Advanced Anti-Exploit 28
 - 4.5.3. Antimalware 29
 - 4.5.4. Antiphishing 29
 - 4.5.5. Endpoint Detection and Response 29
 - 4.5.6. Hyper Detect 30
 - 4.5.7. Network Attack Defense 30
 - 4.5.8. Ransomware Mitigation 31
 - 4.5.9. Web Traffic Scan 31
 - 4.6. Managing Quarantine 31
 - 4.7. Monitors 32
 - 4.7.1. Monitor Types 33
 - 4.7.2. Managing Monitors 34
 - 4.8. Audit Actions 35



1. OVERVIEW

1.1. Scope of This Document

This document is intended to guide Managed Service Providers through the integration process between ConnectWise Automate and GravityZone Control Center.

The Bitdefender integration plugin allows you to manage endpoint security through ConnectWise Automate.

2. REQUIREMENTS

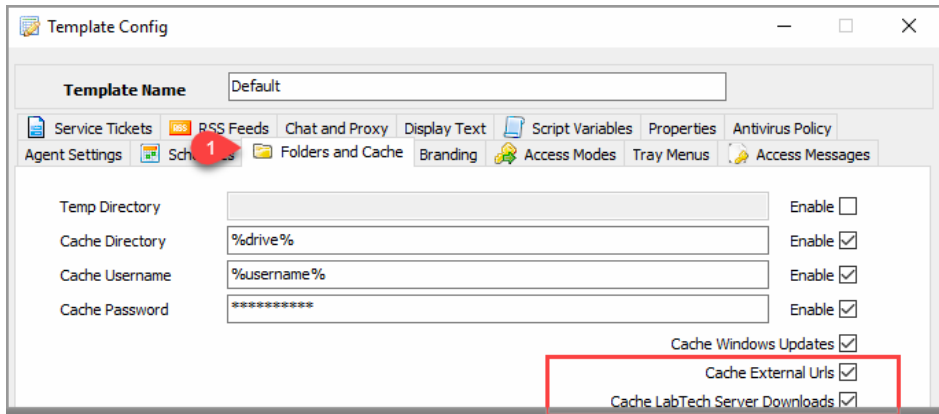
The ConnectWise Automate integration requires the following:

- GravityZone license key or valid MSP subscription. If you do not have a valid MSP subscription, you can find out more information on the [Bitdefender MSP program](#). Integration is available for Partner companies.
- GravityZone set up into your environment.
- ConnectWise Automate v11 or newer.
- Location cache for Bitdefender security agent deployment enabled.

During deployment, the Bitdefender security agent installer downloads a large file size to each target machine. Enable the following checkboxes in ConnectWise Automate to configure a location cache for the Bitdefender security agent deployment:

- Cache External URLs
- Cache LabTech Server Downloads

For more information, refer to [Caching in ConnectWise Automate Documentation](#).



ConnectWise Automate Template Config

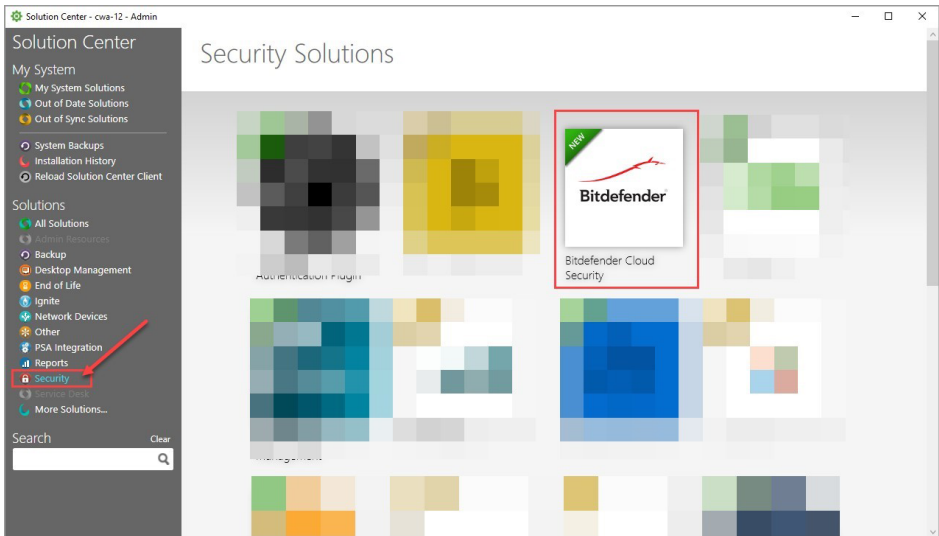


3. SETTING UP THE INTEGRATION

To integrate GravityZone Control Center with ConnectWise Automate, follow the steps below:

3.1. Plugin Installation via Solution Center


1. Log in to Automate Control Center and navigate to **System > Solutions > Solution Center**.
2. In **Solution Center** go to **Security**.
3. Choose **GravityZone Cloud Security** from the **Security Solutions** options.



Security Solutions in Solution Center

4. Click **Queue** to add this solution in queue.






Bitdefender Cloud Security

Bitdefender Cloud Security provides antivirus/antimalware that is light, fast and simple to deploy.

Version: 1.0.0.1
Released 25/07/2018
Your Version: Not Installed

[Release Notes](#)

[Refresh Solution Info](#)



Queue

Items in this Solution

Type	Name	Version	Update Status
Plugins	Bitdefender GravityZone	1.0.0.1	Not Installed
Virus Scanner	Bitdefender GravityZone	1.0.0.1	Not Installed
Plugins	Bitdefender GravityZone Remote Agent	1.0.0.1	Not Installed

Bitdefender Cloud Security

The Solution Center displays **1 Solution in Queue** in the upper left corner.

5. In the **Queued Solutions** section, click **Install/Update**.

Solution Center

1 Solution in Queue


My System


- My System Solutions
- Out of Date Solutions
- Out of Sync Solutions
- System Backups
- Installation History
- Reload Solution Center Client

Solutions

- All Solutions
- Admin Resources
- Backup
- Desktop Management
- End of Life

Queued Solutions






Bitdefender Cloud Security

Version: 1.0.0.1
25/07/2018
Your Version: Not Installed

Solution Item Status		Select an item type for details	
Current:	0	Local Changes:	0
Not Installed:	3	Init Failed:	0
Update Available:	0	Deprecated:	0
Total Items:	3		

Remove Solution

Show Item Details



Install/Update

Queued Solutions in Solutions Center

6. Navigate to **System > Solution > Plugin Manager**.
7. Find **Bitdefender GravityZone plugin**, right-click on it and select **Enable**.
8. Find **Bitdefender GravityZone Remote Agent plugin**, right-click on it and select **Enable**.

Setting Up the Integration

4



Enabled	Name	Version	Author	Description	Category	DB Loaded	IIS Loaded	Remote Ag...
	Bitdefender GravityZone	1.0.0.1	Bitdefender	Bitdefender GravityZone Integration				
	Remote Agent	1.0.0.1	Bitdefender	Bitdefender GravityZone Integration - Remote Agent				
	<ul style="list-style-type: none"> Enable Disable Refresh About 							

Plugin Manager

9. A confirmation window prompts you to restart the Control Center. Select **No**.



Note

Restarting the Database Agent terminates any scripts running at that time.

10. Navigate to **Advanced > Reload Plugins** and select **Update Remote Agent Plugins**.

This restarts the Database Agent and Remote Plugins.

11. Restart IIS server.

12. Close and re-open the Automate Control Center.

Continue [configuring the integration](#).



Important

The above procedure also applies when updating the Bitdefender plugin. Restarting the Database Agent, IIS server and the Control Center is mandatory for completing the update.

To check if the installation or the update of the Bitdefender plugin has completed successfully:

1. Go to **Tools > Bitdefender GravityZone**.
2. In the left-side menu, go to **Other > Plugin Status**.
3. Verify the components statuses and, in case of issues, take actions as indicated in **Recommendations**. Once done, restart the ConnectWise Automate Control Center.

3.2. Manual Installation of the Plugin

The following steps describe how to install the Bitdefender plugin manually:

1. Download the [Bitdefender plugin](#) and extract the archive.
2. In Automate Control Center, navigate to **System > Solutions > Plugin Manager**.

3. Click **Advanced** in the upper right-hand corner.
4. Navigate to **Manage Plugins > Add Plugin**.
5. Navigate to the folder where you extracted the Bitdefender plugins and select `Bitdefender GravityZone.dll`.
A confirmation dialog appears.
6. Click **Yes** to confirm the action.
The **Bitdefender GravityZone** plugin will appear under the **Name** column.
7. Repeat steps 2 – 5 and select `Bitdefender GravityZone Remote Agent.dll` to install the remote agent.
The **Bitdefender GravityZone Remote Agent** will appear under the **Name** column.
8. Navigate to **Advanced > Reload Plugins** and select **Update Remote Agent Plugins**.
This restarts the Database Agent and Remote Plugins, and updates the plugins.
9. Restart IIS server.
10. Close and re-open the Automate Control Center.



Important

The above procedure also applies when updating the Bitdefender plugin. Restarting the Database Agent, IIS server and the Control Center is mandatory for completing the update.

To check if the installation or the update of the Bitdefender plugin has completed successfully:

1. Go to **Tools > Bitdefender GravityZone**.
2. In the left-side menu, go to **Other > Plugin Status**.
3. Verify the components statuses and, in case of issues, take actions as indicated in **Recommendations**. Once done, restart the ConnectWise Automate Control Center.

3.3. Plugin Update

Every time a new version is available, you can update the Bitdefender plugin via Solution Center or manually.

- To update the Bitdefender plugin via Solution Center, follow the same procedure as described at “[Plugin Installation via Solution Center](#)” (p. 3).
- To update the Bitdefender plugin manually, follow the same procedure as described at “[Manual Installation of the Plugin](#)” (p. 5).

In both cases, to complete the update successfully, you must restart the Database Agent, IIS server and the Automate Control Center.

To check if the update of the Bitdefender plugin has completed successfully:

1. Go to **Tools > Bitdefender GravityZone**.
2. In the left-side menu, go to **Other > Plugin Status**.
3. Verify the components statuses and, in case of issues, take actions as indicated in **Recommendations**. Once done, restart the ConnectWise Automate Control Center.

3.4. Configuring the Integration

ConnectWise Automate requires access to GravityZone services. To authorize access you need to generate an API key in GravityZone Control Center and configure the integration.

Configure the integration as follows:

- [Generate API Key](#)
- [Configure Package Defaults](#)
- [Configure Plugin Settings](#)
- [Configure Alert Settings](#)
- [Configure Client Mapping](#)
- [Configure Computer Mapping](#)
- [Review Plugin Status](#)

3.4.1. Generating the API Key

1. Log in to GravityZone Control Center using your Partner account credentials.
2. Click the username at the upper-right corner and choose **My Account**.
3. Go to the **API keys** section and click **+ Add** at the top side of the table.



4. Enable the following APIs:

- Companies API
- Licensing API
- Packages API
- Network API
- Integrations API
- Policies API
- Reports API
- Accounts API
- Incidents API
- Quarantine API
- Event Push Service API

API key ✕

Enabled APIs:

<input checked="" type="checkbox"/> Companies API	<input checked="" type="checkbox"/> Reports API
<input checked="" type="checkbox"/> Licensing API	<input checked="" type="checkbox"/> Accounts API
<input checked="" type="checkbox"/> Packages API	<input checked="" type="checkbox"/> Incidents API
<input checked="" type="checkbox"/> Network API	<input checked="" type="checkbox"/> Quarantine API
<input checked="" type="checkbox"/> Integrations API	<input checked="" type="checkbox"/> Event Push Service API
<input checked="" type="checkbox"/> Policies API	

Save Cancel

GravityZone Control Center API Configuration

5. Click **Save**.

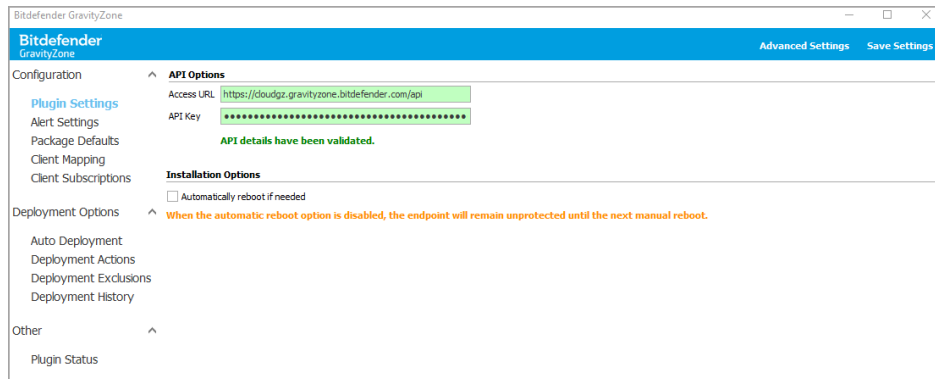
An API key is generated. To prevent the leaking of sensitive information, do not share or distribute your own generated API keys.

6. Copy the Access URL from the **Control Center API** section.

3.4.2. Configuring Plugin Settings

The **Plugin Settings** page contains data necessary to connect ConnectWise Automate to GravityZone, like access URL, API key and installation options for the Bitdefender security agent.

1. In ConnectWise Automate Control Center, go to **Tools > Bitdefender GravityZone > Plugin Settings**.



Plugin Settings

2. Under **API Options**, enter the URL of GravityZone console along with the generated API key and click **Validate**.
3. Under **Installation Options**, select **Automatically reboot if needed**. This option is useful when the computer needs to restart following the Bitdefender security agent installation. If you leave this check box unselected, the endpoint will remain unprotected until the next manual reboot.
4. Click **Advanced Settings** at the upper right corner of the screen for more deployment options:
 - a. In the new window, next to **Automatic Deployment Retry**, select the time interval on which the Bitdefender security agent will try again to install if an error occurs.



- b. Next to **Download Timeout**, select a time limit within which the installation package should be downloaded.
- c. Use the On/Off switch to enable or disable **Setup Downloader** for the security agent deployment.

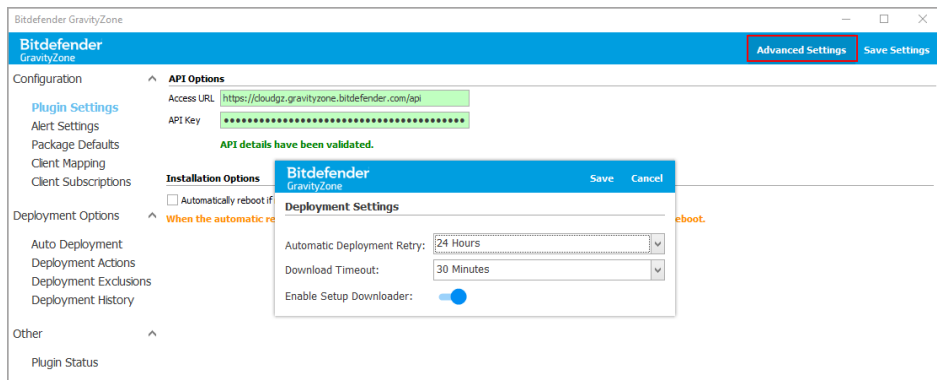
When Setup Downloader is enabled, the Bitdefender plugin uses this file to deploy the Bitdefender security agent on Windows and macOS computers instead of the full kit.



Note

The **Enable Setup Downloader** option does not support Linux. On computers running Linux, the plugin continues using the full kit when deploying the Bitdefender security agent.

- d. Click **Save** to apply the changes and to close the window.



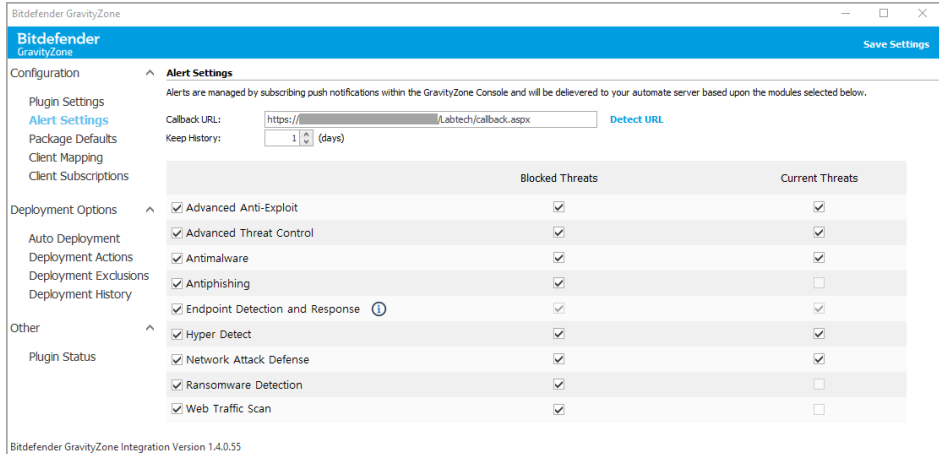
Plugin Settings

- 5. Click **Save Settings** in the upper right corner of the screen to confirm changes.

3.4.3. Configuring Alert Settings

In the **Alert Settings** page you can configure the Bitdefender plugin to send you alerts based on push notifications from GravityZone protection modules.

- 1. Click **Detect URL** to auto discover the ConnectWise Automate Server and verify that the Callback URL field contains the correct address.



Alert Settings

2. Select the number of days for keeping old data (up to 120 days).
3. Select check boxes to enable alerts for specific security events and for **Blocked Threats** or **Current Threats** (which are still present on computers). Alerts are available for the following security events:
 - Advanced Threat Control
 - Advanced Anti-Exploit
 - Antimalware
 - Antiphishing
 - Endpoint Detection and Response (EDR)
 - Hyper Detect
 - Network Attack Defense
 - Ransomware Mitigation
 - Web Traffic Scan

For certain security events, such as Antiphishing, Ransomware Mitigation and Web Traffic Scan, you can only select **Blocked Threats**, as Bitdefender automatically takes action without waiting for user interaction.

For EDR incidents, you can only enable alerts for all threats, with no option to select separately the blocked or current ones. This limitation is due to the complex nature of the EDR incidents, on which Bitdefender may take actions while monitoring and reporting them. Therefore, in order to have a complete incident coverage, it is critical to receive alerts for both current and blocked threats. [Learn more about EDR incidents in ConnectWise Automate integration.](#)

4. Click **Save Settings** at the upper right corner of the screen to confirm your selection.

You can see the security events related to alerts in the GravityZone tab of the Client, Location and Computer screens. For details, refer to [“Security Events”](#) (p. 27).

3.4.4. Configuring Package Defaults

The integration creates a new deployment package in the GravityZone Control Center for each mapped Client or Location. Configure deployment packages to install the Bitdefender security agent on target machines

1. In Automate Control Center navigate to **Tools > Bitdefender GravityZone**.
2. Go to **Package Defaults**.

The screenshot shows the Bitdefender GravityZone Package Defaults configuration window. The window title is "Bitdefender GravityZone" and it has a "Save Settings" button in the top right corner. The left sidebar contains a navigation menu with "Package Defaults" selected. The main content area is titled "Deployment Package Defaults" and includes a descriptive paragraph: "A new deployment package will be created in GravityZone for each client and Location that is linked. Define the default settings to be applied to the package. You'll be able to modify each of these packages in the GravityZone Portal." Below this, there are several sections: "Language:" with a dropdown menu set to "English"; "Modules:" with a grid of checkboxes for various security features; "Installation:" with radio buttons for "Install and remove competitors" (selected) and "Install alongside competitor"; and "Settings:" with a checkbox for "Set uninstall password" and password input fields. A red warning message at the bottom states: "Must be at least 6 characters in length and it must contain at least one digit, one upper case, one lower case and one special character". The version number "Bitdefender GravityZone Integration Version 1.3.6.5" is visible at the bottom left.

Modules:	
<input checked="" type="checkbox"/> Antimalware	<input checked="" type="checkbox"/> Device Control
<input checked="" type="checkbox"/> Advanced Threat Control	<input type="checkbox"/> Power User
<input checked="" type="checkbox"/> Advanced Anti-Exploit	<input type="checkbox"/> Encryption
<input type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Patch Management
<input checked="" type="checkbox"/> Network Protection	<input checked="" type="checkbox"/> EDR Sensor
<input checked="" type="checkbox"/> Content Control	
<input checked="" type="checkbox"/> Network Attack Defense	

Package Defaults

3. Under **Language**, select the package language from the dropdown menu.
4. Under **Modules**, select the protection module enabled in the default package.

5. Under **Installation**, choose to uninstall existing security products or deploy on top of them.
6. Under **Settings**, you can set an uninstall password for the security agent.
7. Click **Save Settings** in the upper right-hand corner to confirm changes.

Making changes in the **Package Defaults** page does not update deployment packages already existing in the GravityZone console. In this situation, you need to either manually update them in the GravityZone console or to re-create them.

To re-create a package, follow these steps:

1. Delete the ConnectWise Automate deployment package from the GravityZone console.
2. In Automate Control Center, go to **Tools > Bitdefender GravityZone > Auto Deployment**.
3. Click **Refresh Package List**.

The plugin will recreate the deployment package based on the settings from the **Package Defaults** page.

3.4.5. Configuring Client Mapping

The Bitdefender plugin creates company records for existing ConnectWise Automate clients within GravityZone Control Center. You can control the creation of these company records using the settings on the **Client Mapping** page. Also, during this process, you can configure the product type or subscriptions for the new companies.



ConnectWise Automate Client	Bitdefender GravityZone Company	Create Location based Groups in GravityZone
A MSP	A MSP	<input checked="" type="checkbox"/>
Client A	Client A_PEMCY9	<input checked="" type="checkbox"/>
Client B	Client B_FPW9S7	<input checked="" type="checkbox"/>
Client C	Client C	<input checked="" type="checkbox"/>
Client E	Client E	<input checked="" type="checkbox"/>
Client F	Client F	<input checked="" type="checkbox"/>
Client Z	Not Selected	<input type="checkbox"/>

Company Names in GravityZone are required to be unique and a randomly generated identifier may be automatically appended to the Company Name within the GravityZone console.

Client Mapping

To automatically configure GravityZone companies **associated with ConnectWise Automate clients**, click the **Auto Map** button in the upper right corner of the page. Subsequent dialogs will ask you if you want to create GravityZone companies with random names and location based groups.

To manually configure GravityZone companies for **clients without previous mapping**:

1. In the **Bitdefender GravityZone Company** column, click the corresponding entries for Automate clients.
2. From the drop-down menu, choose one of the options:
 - **Create Customer Record** - creates a new company in GravityZone.
 - **Ignore Customer** - excludes that client from the mapping process (when using **Auto Map**, for example).
 - Select a GravityZone company already created to associate it to the ConnectWise Automate client.
3. Optionally, in the **Create Location based Group in GravityZone** column, select the check boxes for clients for which you want this setting.
4. Click the **Save Client Mappings** button. A configuration wizard will guide you through the synchronization process, which implies selecting the product type for the new companies and the available features. Follow the on-screen indications:

- a. Select the product. Depending on the product type, the Bitdefender security agent installed on computers belonging to that company will have certain features enabled.

The following product types are available:

- **Endpoint Security**, the fully-featured security solution, with all modules available for deployment on machines running Windows, Linux or macOS.
- **Bitdefender EDR**, a lightweight Endpoint Detection and Response (EDR) solution for Windows-based systems that can run alongside any third-party protection platform.

Click **Continue**.

- b. Select what add-ons to be available with the product type. Depending on the add-ons, you will be able to install the Bitdefender security agent with certain features.

Click **Continue**.

- c. Configure the deployment package:

- i. Choose the default settings or customize the package by selecting certain modules and options.

Click **Continue**.

- ii. Set preferences for installing and updating the Bitdefender security agent.

Click **Continue**.

The plugin will create one or more companies in GravityZone having the specified product type. The Bitdefender security agent installed on computers within these companies will have features as configured in the wizard.

In case of **clients already associated to GravityZone companies**, changing the mapping does not move any installed Bitdefender agents to the newly selected companies within GravityZone Control Center. To show under the new company in GravityZone, you must uninstall and then reinstall the Bitdefender agents.

Once a company mapped, you can reconfigure the product type and the available Bitdefender services in the **Client Subscriptions** page.



Note

The Bitdefender plugin provisions companies for MSPs using Monthly Subscription, Monthly Subscription Trial, and Monthly License Trial.



3.4.6. Configuring Client Subscriptions

On the **Client Subscriptions** page you can control, through the Bitdefender plugin, the product type and the services enabled on clients.

Client Name	Security for Exchange	Full Disk Encryption	Security for Virtualized Environments	HyperDetect	Sandbox Analyzer	Patch Management	EDR	Email Security
[Greyed out]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Greyed out]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Greyed out]	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[Greyed out]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Greyed out]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Greyed out]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Greyed out]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Client Subscriptions

Configuring Services

To reconfigure the Bitdefender services for a client without changing the product type:

1. In the upper left-side corner of the **Client Subscriptions** page, click to view clients by product type.
2. Select or deselect the check boxes corresponding to the services you want to enable.
3. Click the **Save Settings** button.



Note

This operation does not automatically update the existing deployment packages. When creating a new package, you need to enable the corresponding modules in the **Package Defaults** page.

Changing the Product Type

To change the product type for a client:

1. In the upper left-side corner of the page, click to view clients by product type.

2. Select the client whose product you want to change.
3. Click the **Change Product** button. A wizard will guide you shows up. Follow the on-screen indications:
 - a. Select the product. The following product types are available:
 - **Endpoint Security**, the fully-featured security solution, with all modules available for deployment on machines running Windows, Linux or macOS.
 - **Bitdefender EDR**, a lightweight Endpoint Detection and Response (EDR) solution for Windows-based systems that can run alongside any third-party protection platform.

Click **Continue**.

- b. Select what add-ons to be available with the product type. Depending on the add-ons, you will be able to install the Bitdefender security agent with certain features.

Click **Continue**.

- c. Configure the deployment package:
 - i. Choose the default settings, or customize the package by selecting certain modules and options.

Click **Continue**.

- ii. Set preferences for installing and updating the Bitdefender security agent.

Click **Continue**.

The product will change for that client.

After changing the product, you need to you need to reconfigure the Bitdefender security agent installed on computers from GravityZone in order to include the new features. The existing product and its features expire in seven days.



Note

In case your license does not allow changing the product type for managed clients, the **Reconfigure Client** button replaces **Change Product** on the **Client Subscriptions** page. That means you can only modify the add-ons and the other settings within the existing product.

3.4.7. Configuring Computer Mapping

The integration automatically creates a record in Automate Control Center for computers with the Bitdefender security agent installed and maps computers associated with the GravityZone Control Center.

Computer mapping is required for the following functionalities to work correctly:

- Manage Quarantine
- Queue scans
- View security event history
- Alerts and Monitors to function correctly

If the Automatic Mapping is unable to create a successful mapping, you can manually adjust this by completing the following steps:

1. Click **Change Computer Mapping** on the Bitdefender tab on the Computer screen.
2. From the dropdown list select the target device in the GravityZone Control Center that you wish to link to
3. Select **Save** in the upper right-hand corner of the window to save the changes and close the window.

3.5. Configuring Deployment

The integration allows you to deploy the Bitdefender security agent to your managed machines in Automate Control Center.

3.5.1. Auto Deployment

The integration uses Auto Deployment to install the Bitdefender agent on new unprotected machines. The deployment attempts to install the Bitdefender agent once per day only if it is enabled for the specific location, and the target Computer has not been excluded.

You can select Auto Deployment for Windows workstations and servers, macOS, and Linux machines.

1. In Automate Control Center navigate to **Tools > Bitdefender GravityZone**.
2. Go to **Auto Deployment**.
3. Select the checkboxes corresponding to your target machines.

Bitdefender GravityZone							
Save Settings Refresh Package List							
Configuration	Client Name	Location	Windows Workstations	Windows Servers	Mac OS	Linux	Deployment Package
Plugin Settings	A4 Enterprises						
Package Defaults	A4 Enterprises	Marketing Division	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	CWA Deployment Package - A4 Enterprises
Client Mapping	A4 Enterprises	Marketing Division	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	CWA Deployment Package - A4 Enterprises
Client Subscriptions	A4 Enterprises	Sales Division	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	CWA Deployment Package - A4 Enterprises
Deployment Options	cw-comp-001						
Auto Deployment	cw-comp-001	Dev	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	CWA Deployment Package - cw-comp-001\Dev
Deployment Actions	cw-comp-001	QA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	CWA Deployment Package - cw-comp-001\QA
Deployment Exclusions	cw-comp-001	Sales	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	CWA Deployment Package - cw-comp-001\Sales
Deployment History							

Bitdefender GravityZone Integration Version 1.3.7.0

Auto Deployment

4. Click **Save Settings** in the upper right-hand corner to confirm changes.

Once enabled the automatic deployment starts within 10 to 15 minutes.

3.5.2. Deployment Actions

In the **Deployment Actions** section, you can manually start installation or uninstallation commands on machines, clients, or locations. Use the right-side menu to make specific selections.

To install the GravityZone agent:

1. Select one or more targets.
2. Click **Install GravityZone**.

An install task starts for selected machines. ConnectWise Automate Control Center must remain open until the installation is complete to avoid aborting the process.

To uninstall the GravityZone agent:

1. Select one or more targets.
2. Click **Uninstall GravityZone**.
3. Specify the uninstall password, if configured. If not, select **Uninstall Password is not configured**.
4. Click **Uninstall**.

An uninstall task starts for selected machines.

The **Deployment Actions** page displays several statuses that indicate if the GravityZone protection is present on machines or not: Installed, Not Installed, Installed with Issues (related to macOS permissions for full disk access and kernel extensions, and to Linux critical services not started: `bdsrvscand`, `epagd` or `bdlogd`), Install Pending, Uninstall Pending.

3.5.3. Deployment Exclusions

In this section, you can exclude machines, clients, and locations from installing the GravityZone agent on them. Use the right-side menu to make specific selections.

To exclude certain machines from agent installation:

1. Select one or more machines.
2. Click **Enable Exclude**.

To remove an exclusion:

1. Select one or more excluded machines.
2. Click **Disable Exclude**.



Note

The **Deployments Exclusions** in the **Bitdefender GravityZone** dashboard and in the Client and Location screens.

3.5.4. Deployment History

This section displays the list of install and uninstall commands started on machines in the past. Each entry provides you the following details:

- Client name
- Location
- Computer name
- Command type (installation or uninstallation)
- Command status (whether the command was successful, failed or it is pending/executing)
- Output details
- Date and time of task completion.



Note

The **Deployments Exclusions** in the **Bitdefender GravityZone** dashboard and in the Client and Location screens.

3.6. Reviewing Plugin Status

The **Plugin Status** page provides you the insight and the tools to fix issues that may affect the ConnectWise Automate integration with Bitdefender GravityZone.

The screenshot shows the Bitdefender GravityZone interface. On the left is a navigation menu with items like 'Plugin Settings', 'Alert Settings', 'Package Defaults', 'Client Mapping', 'Client Subscriptions', 'Deployment Options', 'Auto Deployment', 'Deployment Actions', 'Deployment Exclusions', 'Deployment History', and 'Other'. The main content area is titled 'About' and contains a table with the following data:

Plugin	Enabled State	Automation Server	Web Server	Control Center
Bitdefender GravityZone	Enabled	No Issues Detected	No Issues Detected	No Issues Detected
Bitdefender GravityZone Remote Agent	Enabled	No Issues Detected	No Issues Detected	Not Applicable

Below the table are two buttons: 'Restart Database Agent' and 'Reload IIS'. Underneath is a 'Recommendations' section with the following text:

For Enabled State of "Disabled" go to **System > Solutions > Plugin Manager** and enable the appropriate Plugin.
 For Automate Server "Not Loaded", click **Restart the Database Agent**.
 For Automate Server "Version Mismatch", click **Restart Database Agent**.
 For Web Server "Not Loaded", click **Reload IIS**.
 For Web Server "Version Mismatch" click **Reload IIS**.
 For Control Center "Version Mismatch", close and open the ConnectWise Automate Control Center

Plugin Status

1. In ConnectWise Automate Control Center, go to **Tools > Bitdefender GravityZone > Other > Plugin Status**.
2. In the table, look for issues marked in red. Consult the recommendations below the table and act depending on the issue.

Solutions include:

- Enabling the **Bitdefender GravityZone** and **Bitdefender GravityZone Remote Agent** components of the plugin
- Restarting the database agent
- Reloading ISS (Web Server)

A similar page to **Plugin Status** will automatically appear on the Client, Location and Computer screens every time an issue occurs and requires manual intervention.

4. USING THE INTEGRATION

This section highlights the available features and configuration options for the following screens:

- [Client](#)
- [Location](#)
- [Computer](#)

In the main window of ConnectWise Automate Control Center, double-click a client, a location, or a computer to access the corresponding screen.

4.1. Client Screen

The Bitdefender GravityZone tab from the Client screen allows you to perform several tasks and view security events information.

- Configure manual deployment or removal of the Bitdefender agent for one or more devices
- Configure deployment exclusions
- View deployment history
- Create scan tasks and take certain actions on multiple devices
- Manage the quarantine for the client
- View security events

Location	Computer	Machine Type	Bitdefender Installed	Online State
CW-	wp000	Windows Workstation	Installed	Online
CW-	wp001	Windows Workstation	Installed	Offline
CW-	wp002	Windows Workstation	Installed	Offline
CW-	wp003	Windows Workstation	Installed	Online

Deployment Actions in Client Screen

Additional details relating to each of the Sub-sections on this screen can be found throughout this document.

Note

For uninstalls you will be prompted to enter an uninstall password. If you have not configured an uninstall password, select **Uninstall** at the top of the window.

4.2. Location Screen

The Bitdefender GravityZone tab from the Location screen allows you to perform several tasks and view security events information.

- Manage automatic deployment settings for the Location
- Manage manual deployment or removal of the Bitdefender Agent for one or more devices
- Configure deployment exclusions
- View deployment history
- Create scan tasks and take certain actions on multiple devices
- Manage the quarantine for the client
- View security events



Computer	Machine Type	Bitdefender Installed	Online State
wp000	Windows Workstation	Installed	Online
wp001	Windows Workstation	Installed	Offline
wp002	Windows Workstation	Installed	Offline
wp003	Windows Workstation	Installed	Online

Deployment in Location screen

4.2.1. Deployment Settings

By clicking the **Deploying Settings** button in the upper right-hand side of the Bitdefender GravityZone tab on the Location screen you are able to control how the Automatic Deployment settings are applied to this location.

Deployment Settings in Location screen

To configure the deployment settings:

1. Specify the deployment package for installing the Bitdefender agent.
2. Select the targets for deployment:

- Windows workstations
- Windows servers
- macOS machines
- Linux machines.

3. Click **Save**.

4.3. Computer Screen

The Bitdefender GravityZone tab on the Computer screen allows you to perform several tasks, and view security events and Bitdefender agent information.

- Exclude or disable automated deployments from occurring on the specified device.
- Manually trigger the installation or removal of the Bitdefender agent.
- View information relating to the Bitdefender agent.
- Manage the quarantine of the specified device.
- View security events.
- Queue a scan to run against the device in the GravityZone Control Center.
- View or change the computer mapping to the GravityZone Control Center.
- View alerts on issues detected on device. The issues may refer to such situations as macOS permissions for full disk access or kernel extensions.



Computer screen



Note

Additional information will only be available after the computer has been mapped to the correct device within the GravityZone Control Center.

4.4. Tasks and Actions

In this page you can create scan tasks for multiple computers at once.

1. In the Client or Location screen, go to **Tasks and Actions**.
2. Select one or more computers and click **Create Scan**.
3. In the configuration window, select the type of scan:
 - Quick scan
 - Full scan
 - Memory scan
4. Optionally, enter a name for the scan task.
5. Click **Scan**. The Bitdefender plugin will create a scan task in GravityZone console.

4.5. Security Events

The **Security Events** section displays information regarding detections made by Bitdefender protection modules and relies on the Event Push Service API from GravityZone Control Center.

The following security events are available with the Bitdefender plugin:

- [Advanced Threat Control](#)
- [Advanced Anti-Exploit](#)
- [Antimalware](#)
- [Antiphishing](#)
- [Endpoint Detection and Response](#)
- [Hyper Detect](#)
- [Network Attack Defense](#)
- [Ransomware Mitigation](#)
- [Web Traffic Scan](#)

Each event corresponds to an alert you can configure in **Tools > Bitdefender GravityZone > Configuration > Alert Settings**.

Security events also have associated monitors. For details on how to operate them, refer to the [“Monitors”](#) (p. 32).

The **Security Events** section is available on the Client, Location and Computer screens.



Location	Computer Name	Process Path	Exploit Type	Process Status	Last Blocked At
CW-	cw-	C:\Windows\System32\reg.exe	AVC APP	Disinfected	11/4/2021 1:47 PM
CW-	cw-	C:\Windows\System32\reg.exe	AVC APP	Disinfected	11/4/2021 1:47 PM

Bitdefender GravityZone Integration Version 1.4.0.43

Security Events > Advanced Threat Control

4.5.1. Advanced Threat Control

This page displays information regarding to detections made by the Advanced Threat Control module. It includes details such as:

- Computer name
- Process path
- Exploit type
- Process status
- When the threat was last blocked

4.5.2. Advanced Anti-Exploit

This page displays information regarding to detections by the Advanced Anti-Exploit module. It includes details such as:

- Computer name
- Technique

- Action taken on the exploited process
- Process ID
- Process path
- Parent process ID
- Parent process path
- CVE
- Detection time

4.5.3. Antimalware

This page displays information regarding to detections made by the Antimalware module. It includes details such as:

- Computer name
- Malware name
- Malware type
- Infection status
- Infected file name
- Detection time

4.5.4. Antiphishing

This page displays information regarding to detections made by the Content Control module. It includes details such as:

- Computer name
- Threat type
- URL
- Status
- Timestamp

4.5.5. Endpoint Detection and Response

This page displays information regarding incidents monitored and reported by the Endpoint Detection and Response module. The main details include:

- Location (available in the Client screen)
- Computer name (available in the Client and Location screens)
- Incident ID
- Detection name
- ATT&CK techniques
- Severity
- Main action taken
- Last time the incident was updated with new information

Reporting on EDR incidents is much more complex. You can find all the details in the tickets generated by these incidents in the **Service Desk > Tickets** section of the ConnectWise Automate Control Center. Learn how tickets are generated in ConnectWise Automate and ConnectWise Manage [here](#).

4.5.6. Hyper Detect

This page displays information regarding to detections made by the Hyper Detect module. It includes the following details:

- Location
- Computer name
- Malware type
- Malware name
- File path
- Fileless attack (yes or no)
- Attack type
- Status (action taken on)
- Detection time

4.5.7. Network Attack Defense

This page displays information regarding to detections made by the Network Attack Defense module. It includes details such as:

- Computer name

- Attack technique
- Detection name
- Victim's IP address
- Attacker's IP address
- Port
- Action taken by Bitdefender

4.5.8. Ransomware Mitigation

This page displays information regarding to detections made by the Antimalware module. It includes details such as:

- Computer name
- Attack type
- Ransomware source
- The number of encrypted files
- Detection time

4.5.9. Web Traffic Scan

This page displays information regarding to detections made by the Content Control module. It includes details such as:

- Computer name
- Threat type
- URL
- Timestamp
- Access to website

4.6. Managing Quarantine

The **Quarantined Items** page displays items that are in the GravityZone quarantine. You can view this page on the Client and Computer screens.



To delete or restore quarantined files, use the check boxes and click the **Delete Selected Items** or **Restore Selected Items** buttons at the upper right corner of the screen.

The Quarantined Items page requires Quarantine API.

<input type="checkbox"/>	Threat Name	Path	Action Status	Quarantined On
<input type="checkbox"/>	Atch4.Detection	C:\Users\testadmin\Desktop\samples\..._exe	None	11/4/2021 1:47 PM

Quarantined Items

4.7. Monitors

The Bitdefender plugin creates several internal monitors to trigger alerts in ConnectWise Automate Control Center.

You can set an alert template for each monitor individually to take specific actions. Monitors generate tickets and errors messages depending on the alert's context.

To access the internal monitors for Bitdefender alerts, go to **Automation > Monitors** and click the **Internal Monitors** tab.



Monitor Name	Monitor Status	Monitor Duration	Monitor Scan Date	Monitor Next Scan	Alert Template Name
AV - Disabled	No Problems	Daily	11/7/2021 5:09:21 PM	11/8/2021 5:09:21 PM	Default - Do Nothing
AV - Out of Date	No Problems	Daily	11/7/2021 5:09:21 PM	11/8/2021 5:09:21 PM	Default - Do Nothing
AV - Software Missing	No Problems	Daily	11/7/2021 5:09:21 PM	11/8/2021 5:09:21 PM	Default - Do Nothing
Bitdefender GravityZone - Advanced Anti-Exploit Event	No Problems	Every 5 Minutes	11/8/2021 11:58:05 AM	11/8/2021 12:03:05 PM	Bitdefender GravityZone Advanced Anti-Exploit Event
Bitdefender GravityZone - Advanced Threat Control Event	No Problems	Every 5 Minutes	11/8/2021 12:00:05 PM	11/8/2021 12:05:05 PM	Bitdefender GravityZone Advanced Threat Control Event
Bitdefender GravityZone - Antimalware Event	No Problems	Every 5 Minutes	11/8/2021 12:00:05 PM	11/8/2021 12:05:05 PM	Bitdefender GravityZone Malware Detected
Bitdefender GravityZone - Antiphishing Event	No Problems	Every 5 Minutes	11/8/2021 12:01:05 PM	11/8/2021 12:06:05 PM	Bitdefender GravityZone Antiphishing Event
Bitdefender GravityZone - Hyper Detect Event	No Problems	Every 5 Minutes	11/8/2021 11:58:05 AM	11/8/2021 12:03:05 PM	Bitdefender GravityZone Hyper Detect Event
Bitdefender GravityZone - Installation Failure	No Problems	900 secs	11/8/2021 11:54:31 AM	11/8/2021 12:09:31 PM	Bitdefender GravityZone Install Fail
Bitdefender GravityZone - Installation Requires Reboot	No Problems	900 secs	11/8/2021 11:54:31 AM	11/8/2021 12:09:31 PM	Bitdefender GravityZone Install Requires Reboot
Bitdefender GravityZone - Network Attack Defense Event	No Problems	Every 5 Minutes	11/8/2021 11:58:05 AM	11/8/2021 12:03:05 PM	Bitdefender GravityZone Network Attack Defense Event
Bitdefender GravityZone - Ransomware Mitigation	No Problems	Every 5 Minutes	11/8/2021 11:58:05 AM	11/8/2021 12:03:05 PM	Bitdefender GravityZone Ransomware Mitigation Event
Bitdefender GravityZone - Uninstall Failure	No Problems	900 secs	11/8/2021 11:54:31 AM	11/8/2021 12:09:31 PM	Bitdefender GravityZone Uninstall Fail
Bitdefender GravityZone - Web Traffic Scan Event	No Problems	Every 5 Minutes	11/8/2021 11:58:05 AM	11/8/2021 12:03:05 PM	Bitdefender GravityZone Web Traffic Scan Event

Internal Monitors

4.7.1. Monitor Types

The following monitors are available with the Bitdefender plugin:

Monitor Name	Description
Bitdefender GravityZone - Installation Failure	A Bitdefender security agent installation process failed.
Bitdefender GravityZone - Installation Requires Reboot	A Bitdefender security agent installation process requires reboot to complete.
Bitdefender GravityZone - Uninstall Failure	A Bitdefender security agent uninstall process failed.
Bitdefender GravityZone - Antimalware Event	One or more Antimalware security events have been detected. This monitor uses the Bitdefender GravityZone Antimalware Event (Consolidated) template, which requires configuration. For details, refer to this article .
Bitdefender GravityZone - Advanced Threat Control Event	An Advanced Threat Control (ATC) security event has been detected.
Bitdefender GravityZone - Advanced Anti-Exploit Event	An Advanced Anti-Exploit security event has been detected.
Bitdefender GravityZone - Antiphishing Event	An Antiphishing security event has been detected.

Monitor Name	Description
Bitdefender GravityZone Endpoint Detection and Response	An EDR incident has been detected.
Bitdefender GravityZone - Hyper Detect Event	A Hyper Detect security event has been detected.
Bitdefender GravityZone - Network Attack Defense	A Network Attack Defense security event has been detected.
Bitdefender GravityZone - Ransomware Mitigation	A Ransomware Mitigation security event has been detected.
Bitdefender GravityZone - Web Traffic Scan Event	A Web Traffic Scan security event has been detected.

4.7.2. Managing Monitors

You can do the following actions with Bitdefender GravityZone monitors

- [Disable](#)
- [Delete and restore](#)

Disabling Monitors

To disable a monitor, you have to modify the alert template:

1. In Automate Control Center, go to **Automation > Monitors**.
2. Click on the **Internal Monitors** tab.
3. Locate the monitor and double click to edit.
4. Go to the **Alerting** tab.
5. Under **Alert Template** select **Default – Do Nothing** in the drop-down list.
6. Click **Save**.

Deleting and Restoring Monitors

To revert a monitor back to its default state, you need to delete it and trigger ConnectWise Automate database agent service restart.

1. In Automate Control Center, go to **Automation > Monitors**.
2. Click on the **Internal Monitors** tab.



3. Locate the monitor, right-click and select **Delete Monitor**.
4. Restart the Automate database agent. To do this:
 - a. Go to **System > Solutions > Plugin Manager**.
 - b. Click **Advanced** in the upper right corner of the window.
 - c. In the drop-down menu, select **Reload Plugins** and **Update Remote Agent Plugins**.
 - d. Confirm the database agent restart.
5. Close and open the Automate Control Center. Back in the **Internal Monitors** tab, the monitor should be restored.

4.8. Audit Actions

Through audit actions, you can keep tracking of changes that users made to made manually to the Bitdefender plugin settings. To view them, go to **System > Configuration > Dashboard > Management > Auditing**.

Auditing Action		Results					
Action	Level	Action	User	Date	ID	Message	Reversible
Backup - Config Alt...	1	Bitdefender GravityZone - Configuration		7/30/2020 10:35:42 AM	0	Updated Plugin Settings	No
Backup - Cancel R...	1	Bitdefender GravityZone - Configuration		7/30/2020 10:35:10 AM	0	Updated Plugin Settings	No
Backup - Databas...	1	Bitdefender GravityZone - Configuration		7/30/2020 10:29:05 AM	0	Updated Plugin Settings	No
Backup - Pause R...	1	Bitdefender GravityZone - Configuration		7/30/2020 10:17:56 AM	0	Updated Plugin Settings	No
Backup - Run Job ...	1	Bitdefender GravityZone - Configuration		7/30/2020 10:16:50 AM	0	Updated Plugin Settings	No
Bitdefender Gravit...	3	Bitdefender GravityZone - Configuration		7/30/2020 10:15:35 AM	0	Updated Plugin Settings	No
Bitdefender Gravit...	3	Bitdefender GravityZone - Configuration		7/30/2020 10:13:49 AM	0	Updated Plugin Settings	No
Bitdefender Gravit...	3	Bitdefender GravityZone - Configuration		7/30/2020 10:09:57 AM	0	Updated Plugin Settings	No
Bitdefender Gravit...	3	Bitdefender GravityZone - Configuration		7/28/2020 10:08:08 PM	0	Updated Plugin Settings	No

Audit Actions

The following auditing actions are available for Bitdefender GravityZone:

- Triggering Bitdefender agent installation.
- Triggering Bitdefender agent uninstallation.
- Changing location deployment settings.



- Changing client mappings.
- Changing plugin settings.
- Changing exclusion settings on individual machines.