**Bitdefender Security for Amazon Web Services**

Contents

[Scope: 2](#_Toc115352587)

[Problem statement that we are trying to solve: 2](#_Toc115352588)

[Introduction: 2](#_Toc115352589)

[How to set up Bitdefender Security for AWS 3](#_Toc115352590)

[Step 1: Subscribe to Bitdefender Security for AWS 3](#_Toc115352591)

[Step 2: Integrate GravityZone with Amazon Web Services 4](#_Toc115352592)

[Step 3 – Install BEST on Instances 5](#_Toc115352593)

[Preparing for BEST Installation 5](#_Toc115352594)

[Local Installation 6](#_Toc115352595)

[Remote Installation 6](#_Toc115352596)

**Document Name: Bitdefender Security for Amazon Web Services**

**Owner: Pooja Sawat**

# Scope:

Bitdefender Security for Amazon Web Services helps customers prevent cyber-attacks and data breaches with real-time Antivirus and Antimalware protection for file systems, memory, processes and registry as well as Risk Management and Device Control to reduce the attack surface.

# Problem statement that we are trying to solve:

How to set up Bitdefender Security for AWS on your Amazon EC2 instances

# Introduction:

Bitdefender Security for Amazon Web Services helps customers prevent cyber-attacks and data breaches with real-time Antivirus and Antimalware protection for file systems, memory, processes and registry as well as Risk Management and Device Control to reduce the attack surface. Perfected over more than 10 years, machine learning and continuous process behavioral monitoring identify new malware and automatically detect and roll back threats that managed to execute. Despite the comprehensive feature set, Bitdefender minimizes resource consumption on protected instances by offloading scan tasks to Bitdefender-hosted Security Virtual Appliances. The proprietary scan offload and caching technologies help lower infrastructure costs significantly compared with traditional endpoint security. Bitdefender integration with AWS makes it very easy and fast to sync your GravityZone inventory with EC2 and automatically roll out protection to your AMIs. Simplify and streamline security by centrally managing protection from the same console, not just for AWS, but also for other cloud environments, and for physical and virtual machines hosted in any datacenter. Bitdefender Security for Amazon Web Services is a security solution designed for cloud infrastructures and integrated with GZ Cloud Console. An innovative and comprehensive solution, Bitdefender Security for AWS protects Amazon EC2 instances running Windows or Linux operating systems. It is useful to first get familiar with the Bitdefender Security for AWS components.

**Highlights**

Real-time Antivirus powered by machine learning perfected since 2008, Antimalware, Risk Management, Device Control, consistently ranked first in real-world independent tests

Offloads scan services to Bitdefender servers in AWS by employing a lightweight security broker on each instance, minimizing resource consumption and significantly reducing AWS infrastructure costs

Flexible pay-as-you-grow hourly billing and simple security console integrated with EC2 for fast rollout and simplified management of protection for AWS machine instances as well as physical and virtual machines hosted on different datacenters

# How to set up Bitdefender Security for AWS

To set up Bitdefender Security for AWS on your Amazon EC2 instances:

1. Subscribe to the service in AWS Marketplace.
2. Integrate GravityZone with Amazon EC2 inventory.
3. Install BEST on the instances you want to protect.

# Step 1: Subscribe to Bitdefender Security for AWS

1. Log in to your AWS Marketplace at this link: <https://aws.amazon.com/marketplace/>.
2. Access Bitdefender Security for Amazon Web Services page.
3. Click the Continue button on the right side of the page.
4. Read the subscription details and click Subscribe. A message will inform you that you are subscribed to Bitdefender Security for AWS.
5. Click Set Up Your Account. You will be redirected to a registration form hosted by Bitdefender. Follow these steps according to your customer status:
   * As new GravityZone customer:
     1. Fill in the required information.
     2. Click Finish purchase.
   * If the provided details are valid, a customer company and a user account will be created for you in the GravityZone Control Center. You will receive your login details to the specified email address. At this moment, you can access the GravityZone Control Center using the link provided in the email.
   * As existing GravityZone customer:
     1. Click the link provided under the form’s title.
     2. Enter your GravityZone credentials.
     3. Click Find company and finish purchase.
   * If the login credentials are valid, a confirmation message will appear. Access GravityZone Control Center using the provided link.

# Step 2: Integrate GravityZone with Amazon Web Services

1. Log in to the Control Center using your GravityZone credentials.
2. In the upper-right corner of the console, go to Integrations.
3. If you do not have an active integration, click Add > Add Amazon EC2 Integration. The Amazon EC2 Integration Settings window will open.
4. Under External ID, click the Generate button.
5. Open a new tab in your browser and log in to the AWS console.
6. Click Services at the upper-side of the AWS console and select Security, Identity and Compliance > IAM.
7. In the left-side menu, click Roles. A new page is displayed.
8. Click the Create role button.
9. Select Another AWS account.
10. Switch to the Control Center and copy the Account ID from the Amazon EC2 Integration Settings window.
11. Go back to the AWS console and paste the string in the Account ID field.
12. Select Require external ID (Best practice when a third party will assume this role).
13. Switch to the Control Center and copy the External ID from the Amazon EC2 Integration Settings window. You can do this in two ways:
14. Select the string and use CTRL + C.
15. Click the Copy to clipboard icon at the end of the string.
16. Back in the AWS console, paste the string in the External ID field.
17. Click Next: Permissions.
18. Check the AmazonEC2ReadOnlyAccess permision and click Next: Review.
19. In the new page, provide a name and a description in the required fields.
20. Click Create Role. You will view the list of all existing roles. Wait for about 1 minute for the changes to propagate across all AWS regions.
21. Click your role name to view the details.
22. Copy the ARN.
23. Switch to the Control Center tab and paste the ARN into the dedicated field.
24. Click Save.  
    GravityZone will import the Amazon EC2 instances in Network, where they will be visible by regions and availability zones.

# Step 3 – Install BEST on Instances

To protect instances with Bitdefender Security for AWS, you must install BEST (the client software) on each of them. BEST uses automatic (default) scan modes for EC2 instances set on Central Scan with Bitdefender Security Server hosted in the corresponding AWS region, with fallback on Hybrid Scan (with Light Engines using in-the-cloud scanning and, partially, the local signatures).

## Preparing for BEST Installation

Prepare for Silent Agent installation as follows:

1. Make sure the instances you want to protect run a supported operating system.
2. BEST has the ability to remove competitor Antivirus solutions. Should automatic removal fail, uninstall (not just disable) any existing antimalware software from the instance. Running other security software simultaneously with Bitdefender Security for AWS may affect their operation and cause major problems with the system.
3. The installation requires administrative privileges. Make sure to have all the necessary credentials at hand (for example, the private keys of your Amazon EC2 key pairs).
4. Configure the Amazon EC2 security groups to allow SSH and Remote Desktop Protocol access from your computer and SSH access from the Control Center instance.
5. If you run firewall software on your instances, make sure to configure it to allow access to the [Bitdefender Security for AWS communication ports](http://enterprise.bitdefender.com/support/security-as-a-service-for-aws-components-1045.html?adobe_mc=MCMID%3D46962823975896837910819809400403592826%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1664269626).

### Local Installation

You connect to individual instances via a SSH or Remote Desktop client and use the installation link from Control Center to download and install Silent Agent locally.

To obtain the download links for the installation files:

1. Connect to the Control Center using your company account.
2. Go to the Computers > Installation Area Page.
3. Click Installation Link. The window that appears provides you with the download links for the Windows web installer and the Linux installation script.

Run the installation file using administrator/root privileges.

### Remote Installation

On instances running Linux operating systems, you can install BEST remotely, from the Control Center. For any of these methods, you must first specify the remote authentication credentials:

1. Connect to the Control Center using your Administrator's Account.
2. Go your name or company's name in the right upper corner of the page -> Credentials Manager.
3. Under Virtualization, click Amazon Credentials. You can view the list of key names imported from your AWS account and detailed information about them.
4. For each key name, you must specify the private key and, if needed, complete the list of user names to authenticate with. To specify the necessary credentials, click the Edit icon in the Action column. You can either upload the Amazon private key file or insert its content in the text box. You can remove or add user names as needed.

Remote Installation. To remotely install BEST from the GravityZone Control Center:

1. Go to the Computers > View Computers page. This page displays your Amazon EC2 instances.
2. Click the Show menu located above the table (to the left) and choose Unmanaged Computers.
3. Select the check boxes corresponding to the Linux instances on which you want to install protection. Use the menu under the OScolumn to filter instances by operating system.
4. Click Tasks and choose Install from the menu.
5. Click Install. A window will appear, prompting for additional information such as credentials and the package that is required for the install.

You can view task execution status and results on the Computers > View Tasks page. Installation takes minutes to complete.