

Airlock WAF For Google Cloud Engine



Quick Start Guide

Table of contents

1	About this quick start guide.....	3
1.1	Licensing information.....	3
1.2	General recommendations.....	3
1.2.1	High-availability and scaling.....	3
2	Deploy image in Google cloud service.....	4
2.1	Hardware sizing of your virtual machine.....	4
2.2	Launch Airlock WAF and API Gateway on GCE.....	4
3	Next steps.....	7

1 About this quick start guide

This guide explains how to deploy Airlock WAF and API Gateway on Google Cloud Engine (GCE) conveniently with only a few clicks.

INFO

Airlock WAF version 7.1 and later can also be deployed manually in IaaS cloud environments. To make the deployment process easier, Ergon provides a generic cloud image, available [via our Techzone download page](#).

For technical details, limitations and how to provision the Airlock WAF cloud image, please refer to the [Airlock WAF Cloud Image Usage document](#).

1.1 Licensing information

Airlock WAF and API Gateway is a Bring Your Own License (BYOL) solution. Licenses are available via our Airlock sales contact.

Further links

- Information about license parameters: [LICENSE PARAMETERS](#)
- To buy a license or get sales support, contact airlock-sales@ergon.ch.

1.2 General recommendations

- When deploying Airlock WAF in a cloud environment, make sure to restrict any access to the administration interface to trustworthy networks.
- It is recommended to have **at least two network interfaces** per instance:
 - One dedicated network interface for WAF administration and the connections to the back-end servers.
 - One or more additional network interfaces to handle the incoming web traffic.
- The Airlock WAF active-passive cluster is not supported in a cloud environment. For high availability, active-active setups with multiple instances sharing the same session store are recommended. See also: "[High-availability and scaling](#)".

1.2.1 High-availability and scaling

The following services are required in order to obtain a high availability setup for Airlock WAF:

- A Redis DB service, to have a central session store for all Airlock WAF instances.
- A load-balancer, to forward traffic to the WAF instances.

INFO

Some cloud providers offer Redis DB "as a service". Otherwise, the Redis DB service can be set up individually. At minimum Redis DB version 3.0 is required.

2 Deploy image in Google cloud service

Chapter-related prerequisites

- You understand basic networking.
- You must be able to sign in to the Google Cloud Platform (GCP) using a Google user account.
- You have a basic working knowledge of Google Cloud services (GCP, GCE) and its GUI control panels:
 - Navigation
 - Creating instances
- You have enrolled in a free trial with available credit or a payment account set up with GCP.

Further links

- Register a new Google user account: [Google account](#)
- Pricing information to use cloud services: [Google cloud pricing information](#)

2.1 Hardware sizing of your virtual machine

Depending on your estimated load (i.e. number of parallel HTTP sessions), you have to choose your initial VM hardware during the deployment process.

See [Hardware Sizing and System Requirements Airlock WAF](#) for typical reference values.

2.2 Launch Airlock WAF and API Gateway on GCE



INFO

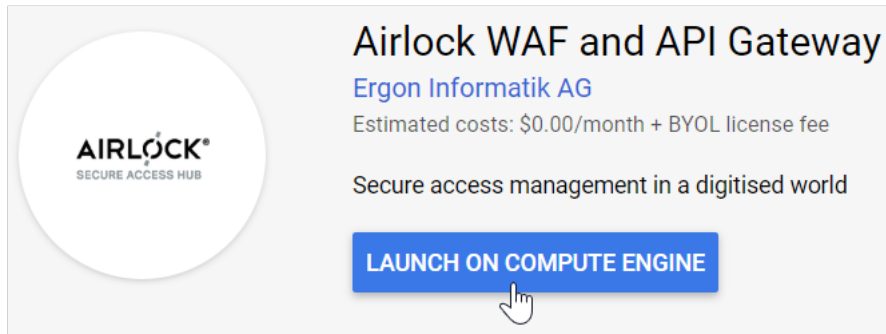
Visit our product page [Airlock Secure Access Hub on Google Cloud](#) to find more information about our products and the starting point for your new Airlock WAF and API Gateway deployment.

Procedure-related prerequisites

- A public SSH key must be available.
- An Airlock WAF license must be available.

Step by step

1. Click the LAUNCH ON COMPUTE ENGINE button:



✓ The configuration page opens for your new virtual machine (VM) opens.

2. Choose the hardware settings according to your needs.

3. Enter your public SSH key in the format `cloudinit:ssh-rsa {your_ssh_key}`.

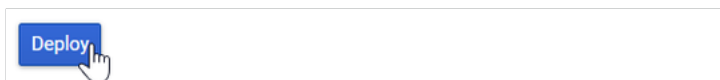
NOTICE Do not use brackets {}, as they are just placeholders!

4. Choose your network interface settings and change the firewall settings if required.

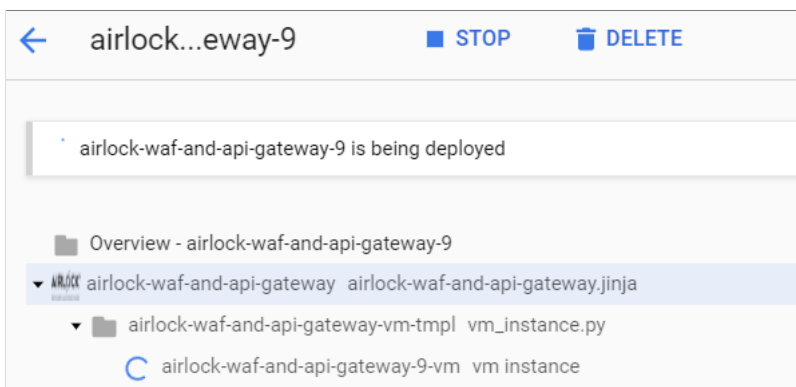
The screenshot shows the 'Networking' section of the GCP console. Under 'Network interfaces', there is a single interface named 'default default (10.172.0.0/20)' with an edit icon. Below it is a button to '+ Add network interface' and a message: 'You have reached the maximum number of one network interface'. The 'Firewall' section has a warning: 'Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. Learn more'. There are four firewall rules, each with a checked checkbox: 'Allow TCP port 22 traffic from the Internet', 'Allow HTTPS traffic from the Internet', 'Allow HTTP traffic from the Internet', and 'Allow TCP port 8443 traffic from the Internet'. Each rule has a text input field for 'Source IP ranges' containing '0.0.0.0/0, 192.169.0.2/24'. At the bottom, 'IP forwarding' is set to 'On'.

SECURITY RISK Access to the web management console (TCP port 8443) is disabled by default. If you open port 8443, make sure to restrict access to trusted source IP ranges.

5. Read and accept the GCP Marketplace Terms of Service and click the Deploy button.



6. The automatic deployment starts. Wait until the process is finished.



- ✓ The deployment is now ready to be configured.

3 Next steps


After successful deployment, the new Airlock WAF instance must be configured. Follow the Suggested next steps to finalize your installation.

NOTICE

The button **Log into the admin panel** (using SSH) provided by Google will not work, because key pairs are not provisioned automatically to the Airlock WAF image.


- On the command-line:
Log in via **SSH** as user *root*. Use the key pair configured in the previous section.

AIRLOCK® Airlock WAF and API Gateway
SECURE ACCESS HUB Solution provided by Ergon Informatik AG


Admin URL	https://34.65.65.159:443/ 
Instance	airlock-waf-and-api-gateway-10-vm
Instance zone	europa-west6-a
Instance machine type	n1-standard-4


[More about the software](#)



Get started with Airlock WAF and API Gateway



[Log into the admin panel](#) SSH 

Suggested next steps

- Buy a license
Please [contact Airlock](#)  to get a valid license.
- Create a GUI administrator account
Use SSH to access Airlock. Then, use the user manager tool to create an administrator account.

```
$ airlock-user-manager-tool --set --user admin --password [secret] 
```
- Create a REST API key
Use SSH to access Airlock. Then, use the user manager tool to create an API key for the Airlock REST API.

```
$ airlock-user-manager-tool --set --user rest-admin --role airlock   
# show the generated token  
airlock-user-manager-tool --list --user rest-admin --jwt
```
- Open TCP port 8443 traffic
This firewall rule is not enabled. To allow specific network traffic from the Internet, create a firewall rule to open TCP port 8443 traffic for target tag "airlock-waf-and-api-gateway-10-deployment". [Learn more](#) 
If you are using Google Cloud SDK, type the following command in the terminal:

```
$ gcloud --project=ergon-public compute firewall-rules create "air 
```
- Assign a static external IP address to your VM instance
An ephemeral external IP address has been assigned to the VM instance. If you require a static external IP address, you may promote the address to static.
[Learn more](#) 

You can find further instructions under **Documentation and Support** below.

Documentation

[Airlock WAF cloud deployment guide](#) ↗

Support

First, register an account on our service desk. Then, open a ticket. [Go to Ergon Informatik AG support](#) ↗

[Show Support ID](#)

Template properties

∨ [More](#)

Further information and links

- A setup guide is available here: [Airlock WAF cloud deployment guide](#)

Awards:



Airlock protects:

- more than 30,000 applications
- over 20 million active identities
- at 550 customers

Airlock – Security Innovation by Ergon Informatik AG

Ergon Informatik AG
Merkurstrasse 43
CH-8032 Zürich
+41 44 268 89 00
info@airlock.com

ergon

Copyright © 2019 Ergon Informatik AG. All Rights Reserved. All technical documentation that is made available by Ergon Informatik AG is the copyrighted work of Ergon Informatik AG and is owned by Ergon Informatik AG. Ergon, the Ergon logo, «smart people – smart software» and Airlock are registered trademarks of Ergon Informatik AG. Microsoft and ActiveDirectory are registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries. Other products or trademarks mentioned are the property of their respective owners.