How to Deploy a CloudGen Firewall Vx OVA on VMware Hypervisors

https://campus.barracuda.com/doc/96026595/

If you are deploying the Barracuda CloudGen Firewall Vx in a high-performance environment or require support for VLANs, do not deploy using the OVA packages. Instead, create a custom configuration using Barracuda Firewall Install. For more information, see How to Deploy a CloudGen Firewall Vx using Firewall Install on a VMware Hypervisor.

To ease deployment, the Barracuda CloudGen Firewall Vx units are available as prebuilt OVA images that can be imported into your VMware hypervisor. You do not need to create or configure a virtual machine (VM). Before deploying the CloudGen Firewall Vx unit, verify that the host system meets the minimum storage requirements and review the resource recommendations for the production system. You can deploy the firewall using either the VMware vSphere Client or the VMware OVF Tool (ovftool).

Before You Begin

- For information regarding the sizing of your CPU, disk, and RAM, see Virtual Systems (Vx).
- Before you start the Barracuda CloudGen Firewall Vx for the first time, assign a manual MAC address to the first virtual network interface. This lets you move the VM later without invalidating your license. For more information, see Best Practice - Performance Tuning on VMware Hypervisors.
- Download the VMware OVA image from the Barracuda Download Portal.
- Ensure that you have claimed your firewall at `ztd.barracudanetworks.com`. Without claiming your firewall prior to deploying it, activation will fail.
- While you are performing the steps listed below, you must send the token that you received in your purchase mail with the serial. Ensure that the firewall to be deployed is not connected behind another appliance that catches network traffic for packet inspection because this will break the activation process!

Use the VMware vSphere Client

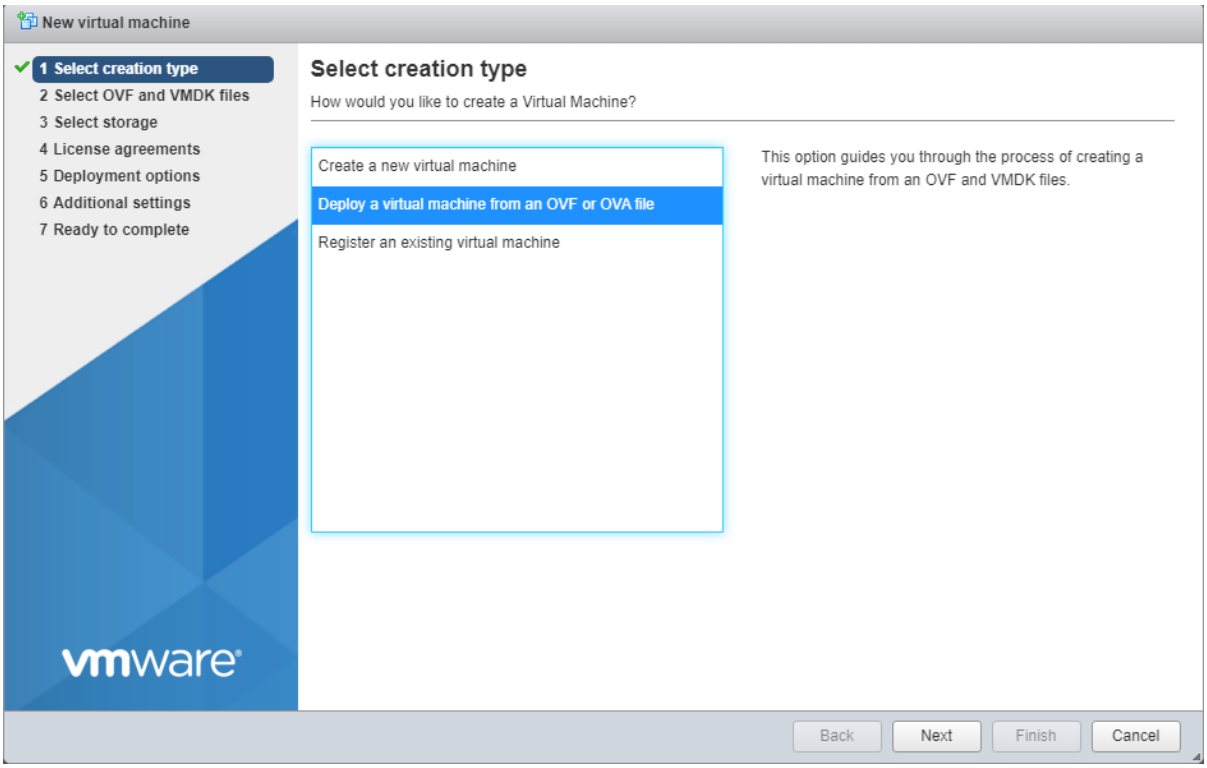
The following instructions require VMware's Hypervisor ESXi 7.0 and a CGF OVA file.

To start the deployment of a new CloudGen Firewall, perform the following steps:

Create a Virtual Firewall on Your ESXi Hypervisor

Step 1. Start the Deployment on the VMware Hypervisor.

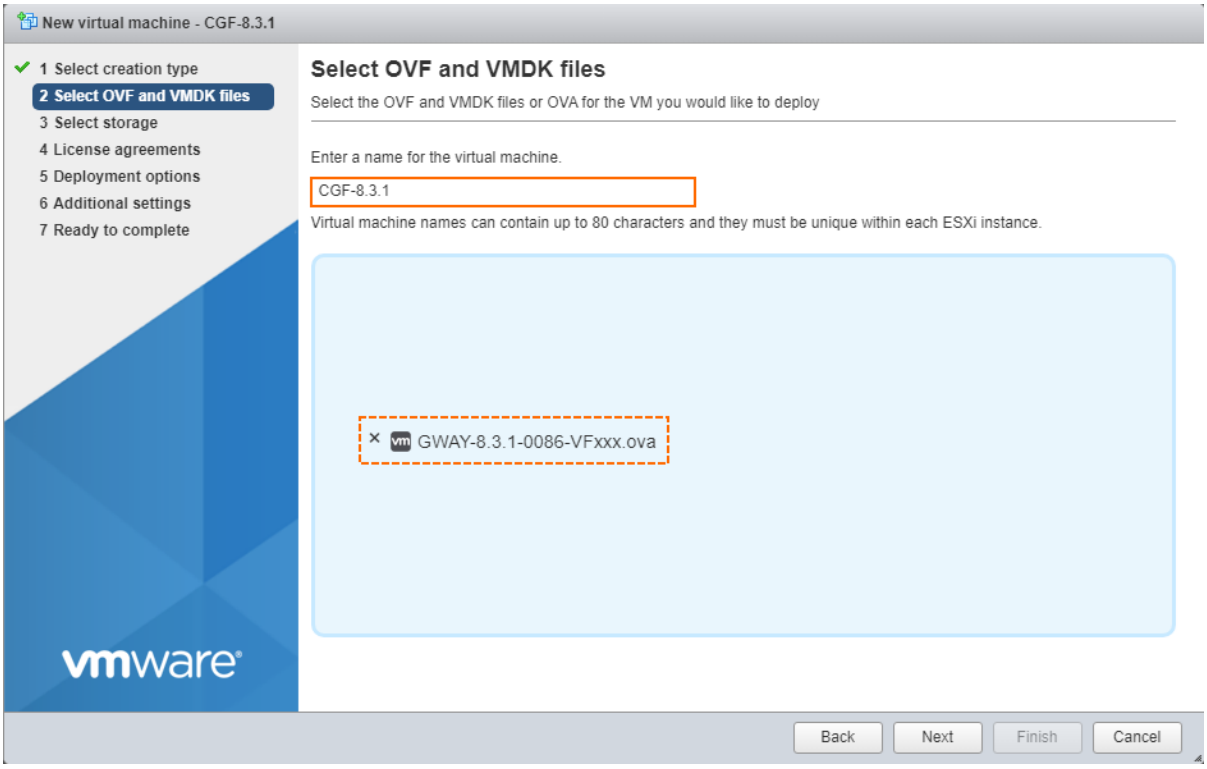
1. Log into your VMware Hypervisor and go to the menu for creating a new virtual machine.
2. The window **New virtual machine** opens.
3. From the menu list in the main view, select **Deploy a virtual machine from an OVF or OVA file**.



4. Click **Next**.

Step 2. Select the OVA for the VM You Want to Deploy

1. Select a meaningful name for your CloudGen Firewall, e.g., CGF-8.3.1
2. Enter the name of your CloudGen Firewall into the edit field.
3. Drag the symbol of your OVA file into the main view of the window.

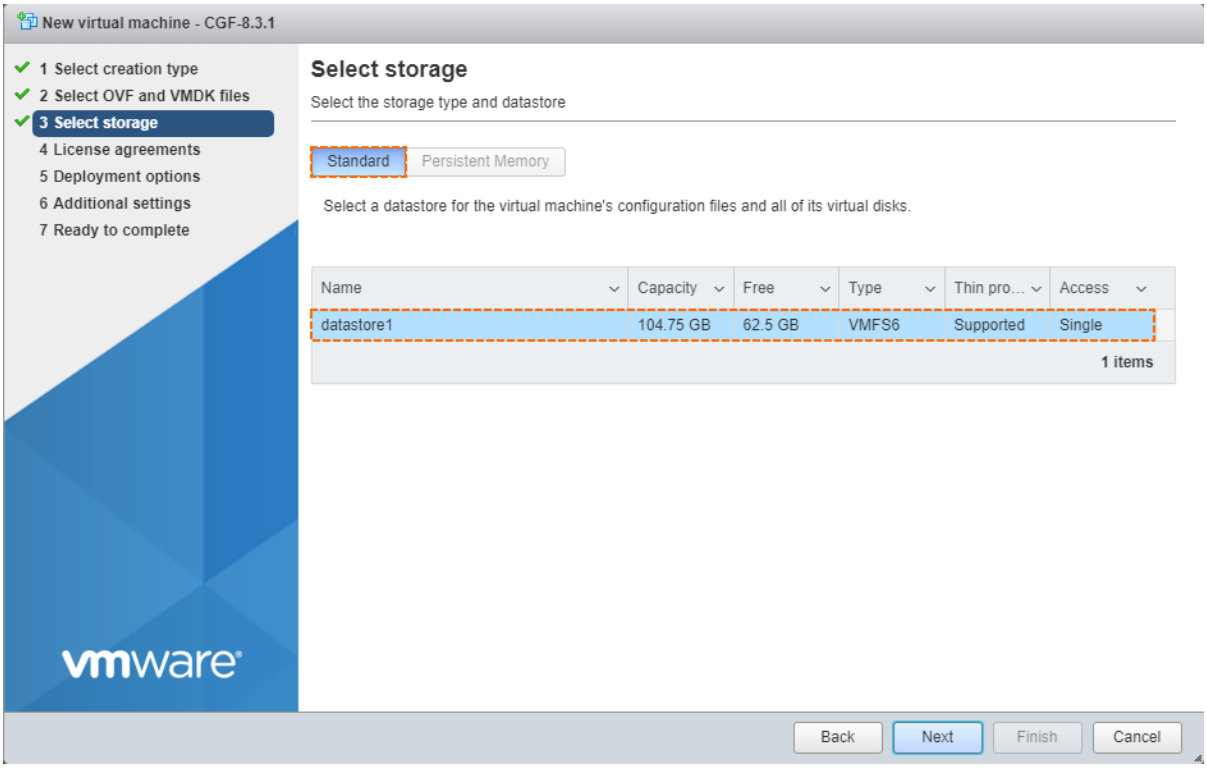


4. Click **Next**.

Step 3. Select the Storage for Your Virtual Machine

You must provide enough storage space for your virtual machine. In case of doubt, contact your system administrator.

1. Select the type of memory that best matches your requirements.
2. Select the storage that provides enough storage space for your virtual machine.

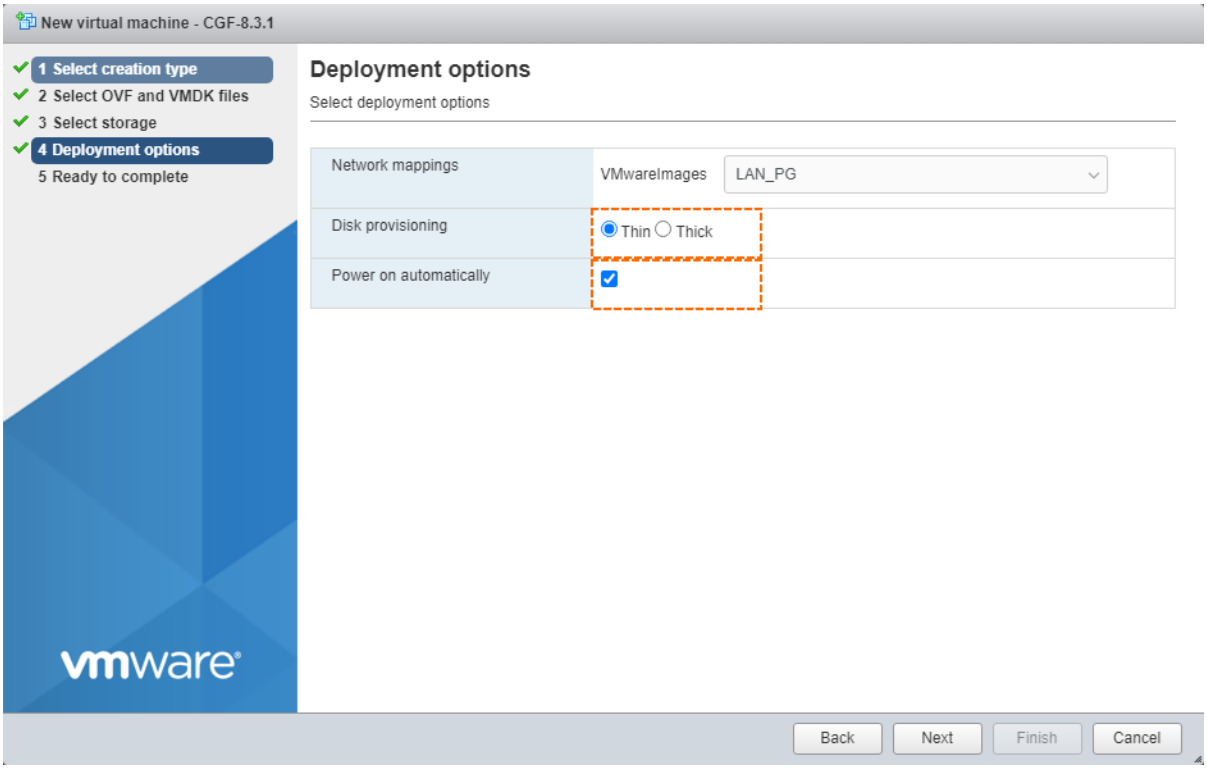


3. Click **Next**.

Step 4. Configure Specific Deployment Options

You must configure certain deployment options regarding how the virtual machine handles storage and behaves in certain situations.

1. Depending on your individual preferences, select **Thin** or **Thick** for **Disk Provisioning**.
2. Select the check box for **Power on automatically**.

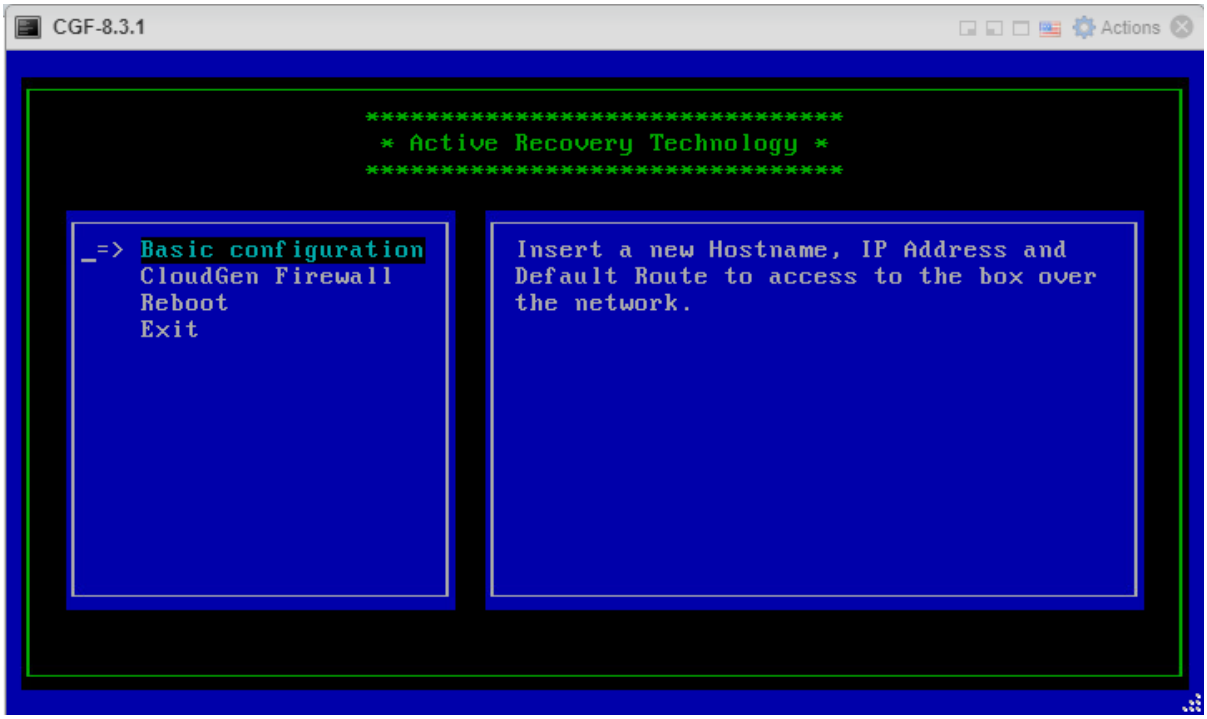


3. Click **Finish**.
4. The firewall is installed on your ESXi Hypervisor and finally starts.

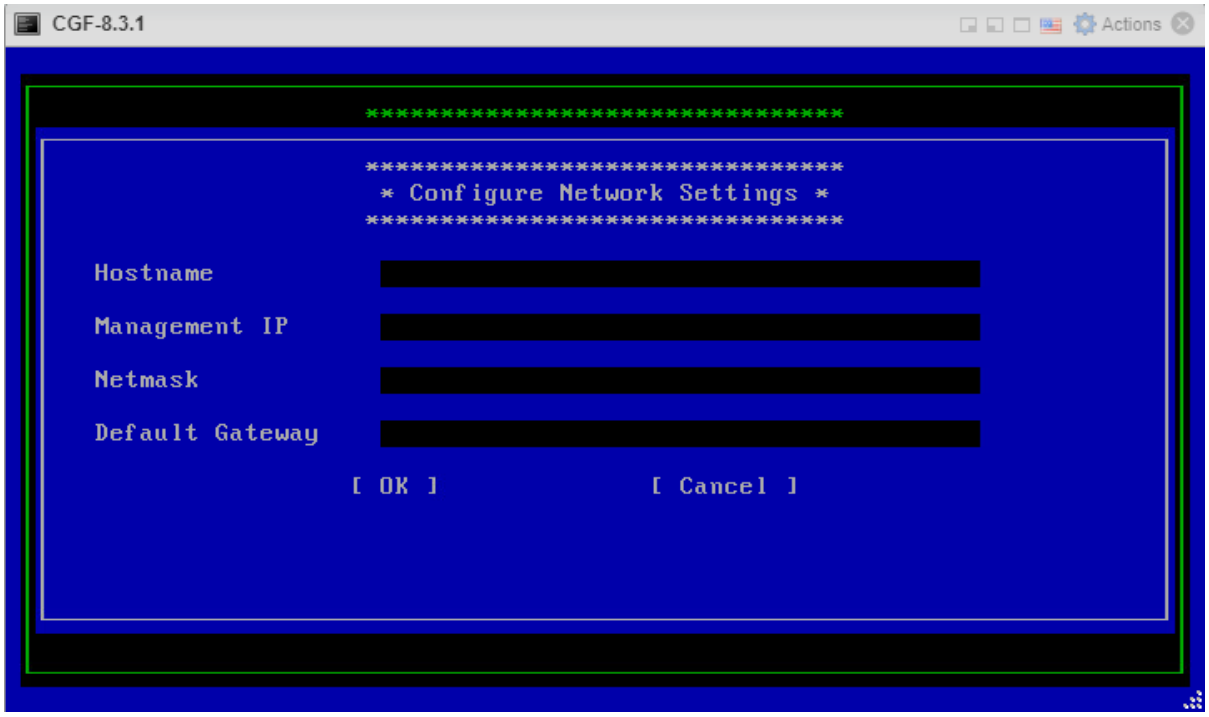
Perform Basic Configurations on Your Firewall

Step 5. Enter Basic Configuration Data for Network Settings

1. After the restart, the firewall will display the ART (Active Recovery Technology) screen. The highlighted menu entry is **Basic configuration**.

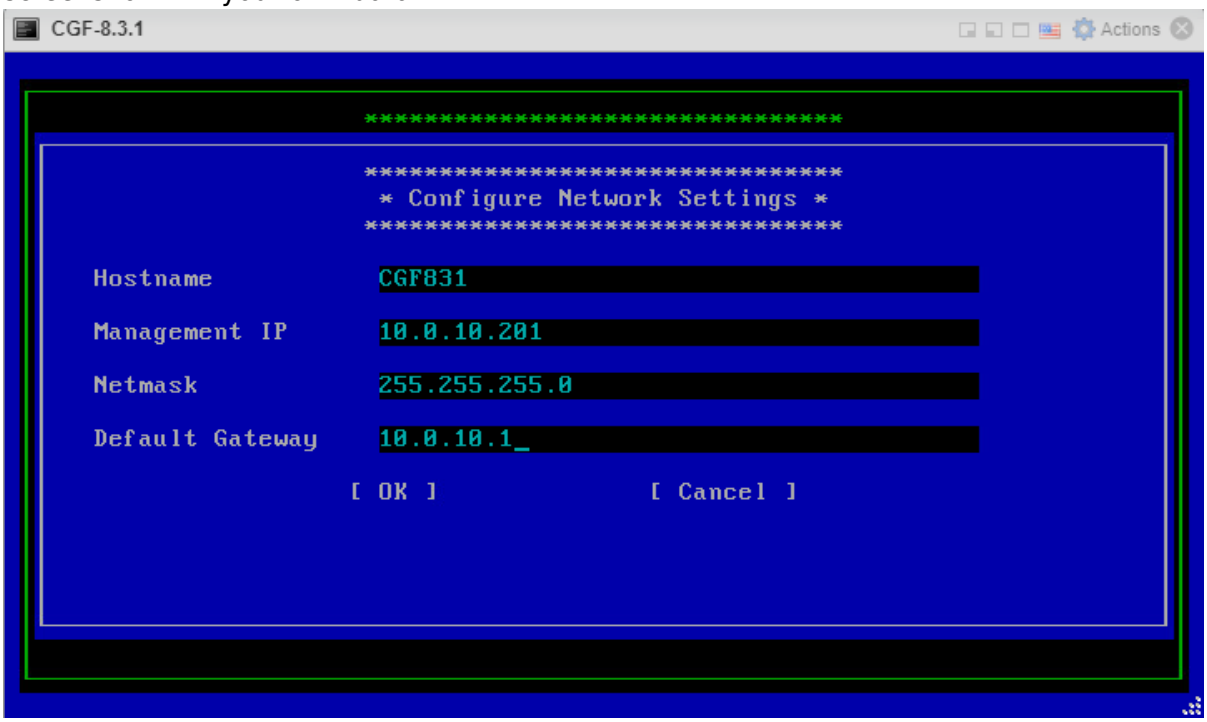


2. Press **Enter** on your keyboard.
3. An area is displayed for **Configure Network Settings**. The area shows the following labels with their related edit fields:
   - **Hostname** – The desired hostname for your firewall.
   - **Management IP** – The IP address that your firewall should be reachable through.
   - **Netmask** – The subnet mask in dotted quad notation. For example, `255.255.255.0`.
   - **Default Gateway** – The IP address of the next hop device that serves as an access point to another network.

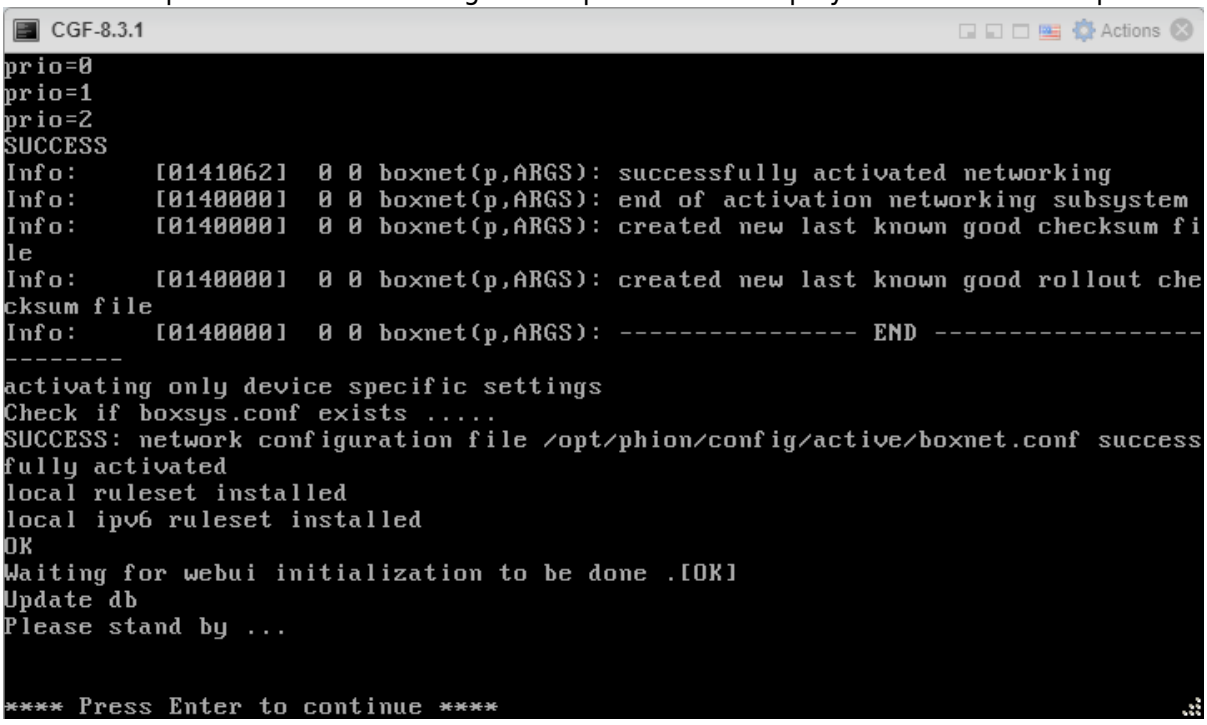


4. Enter the specific data that identifies your firewall in the network. Replace the values in the

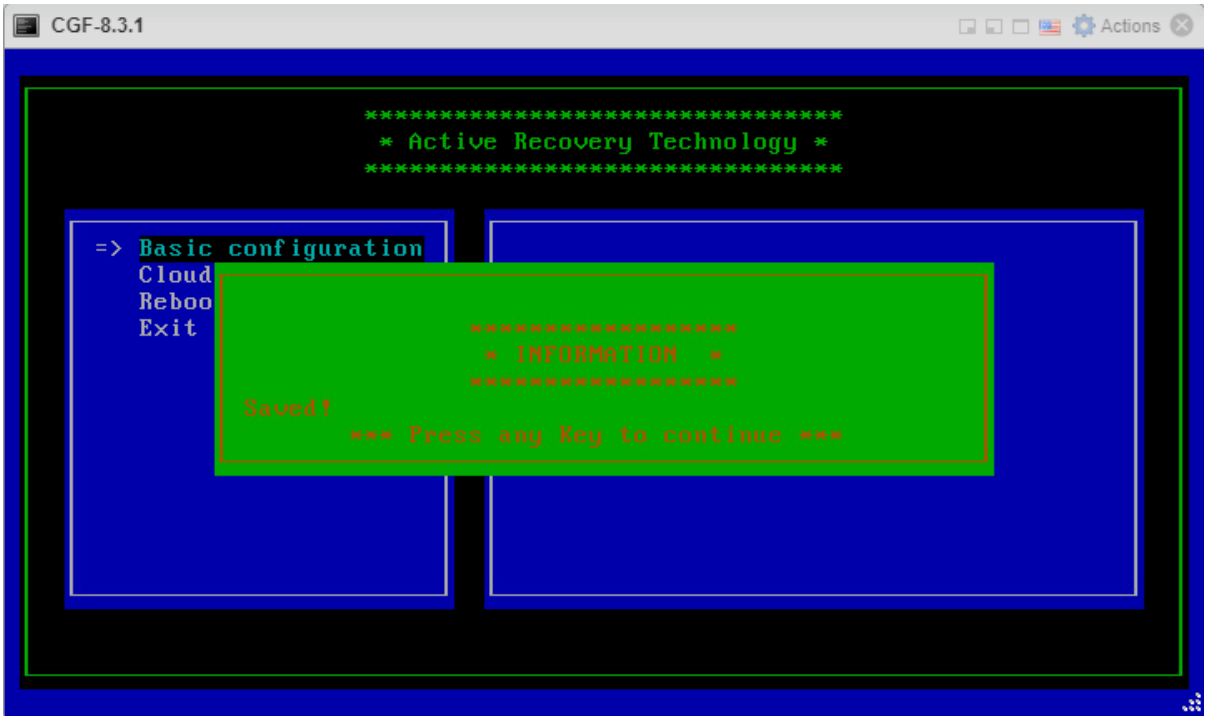
screenshot with your own data.



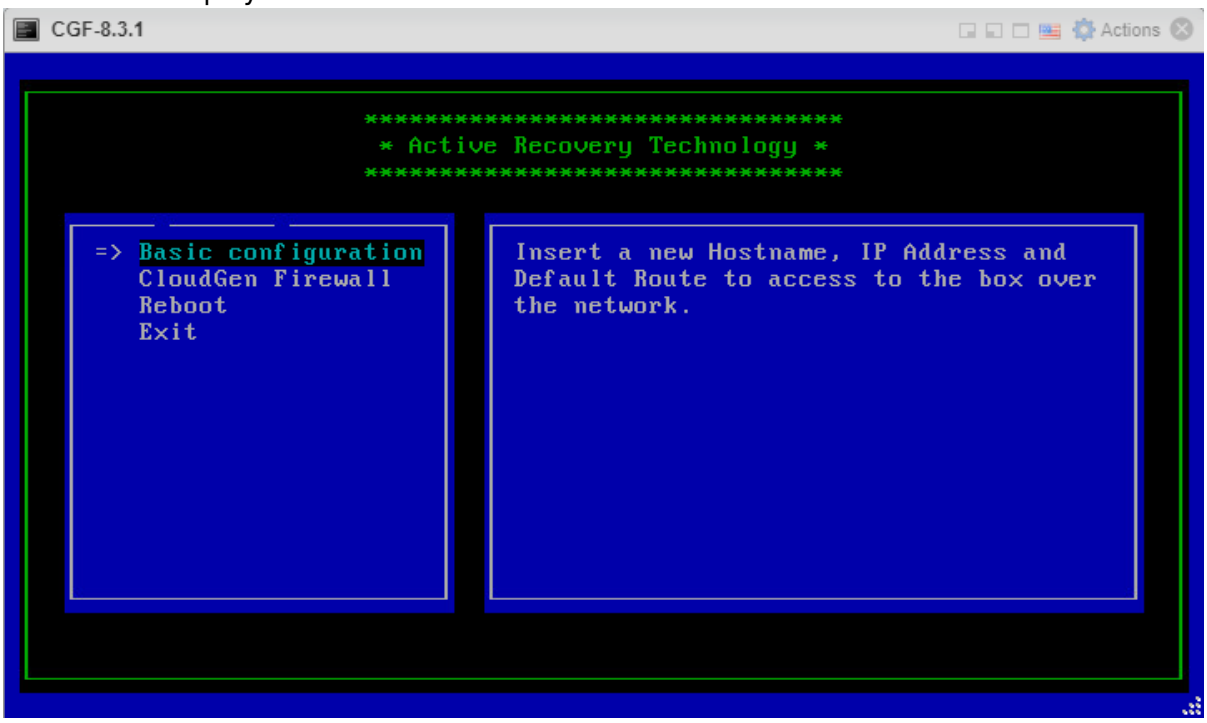
5. Click **OK**.
6. The firewall proceeds with its configuration process and displays a screen with output.



7. If prompted to do so, press **Enter** on the keyboard.
8. The firewall confirms that your network information has been saved.



9. Press any key to continue.
10. The firewall displays the initial **ART** menu.



Activate Your Virtual CloudGen Firewall

You have two options for activating your firewall:

Option 1 - Step 1: Activate Your Firewall Using Zero Touch Deployment in the ART Window

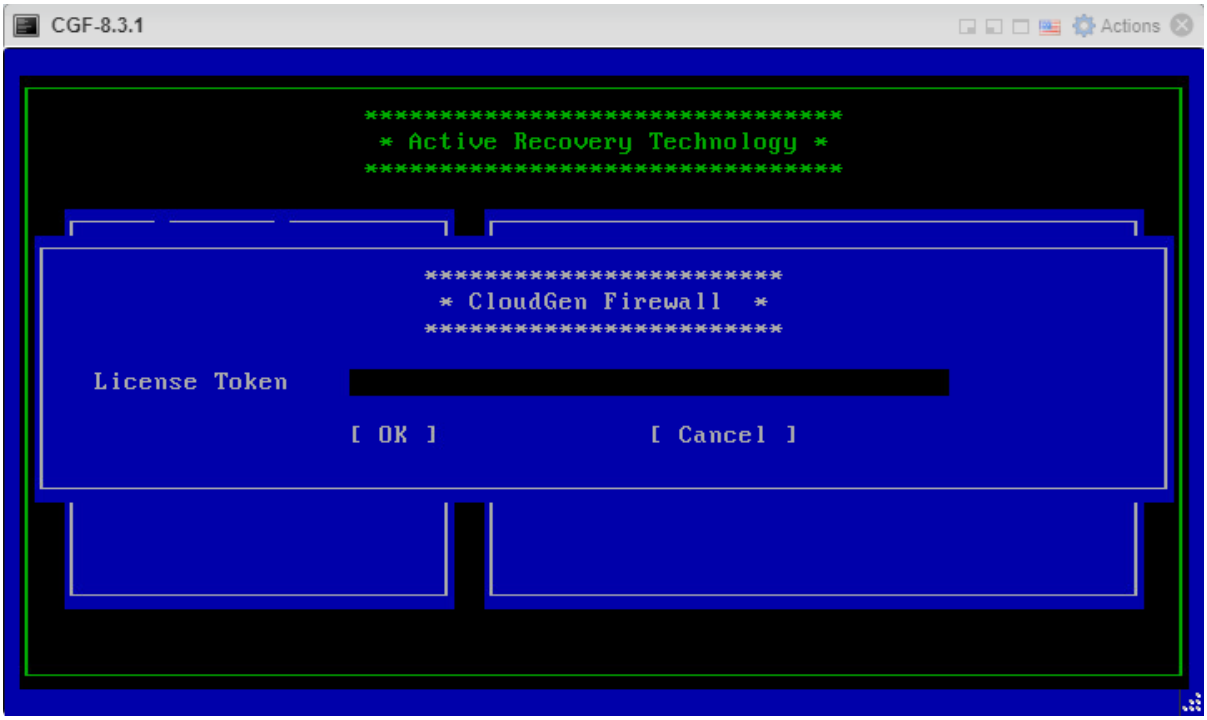
To reduce the activation process of virtual firewalls deployed on the VMware ESXi hypervisor on the basis of OVA files, the ART menu now contains a new option that uses the ZTD server for activating the virtual firewall.

Because the ART menu is the starting point for configuring a virtual appliance, the firewall is not yet fully configured at this point. To keep the activation from failing, consider the following:

1. Ensure that your network configuration is correct.
2. Ensure that you have claimed your firewall at `ztd.barracudanetworks.com`. Without claiming your firewall prior to deploying it, activation is not possible.
3. Ensure that you have already received your firewall-related token with the serial number in your purchase mail!
4. Ensure that the firewall to be deployed is not connected behind another appliance that catches network traffic for packet inspection because this will break the activation process!

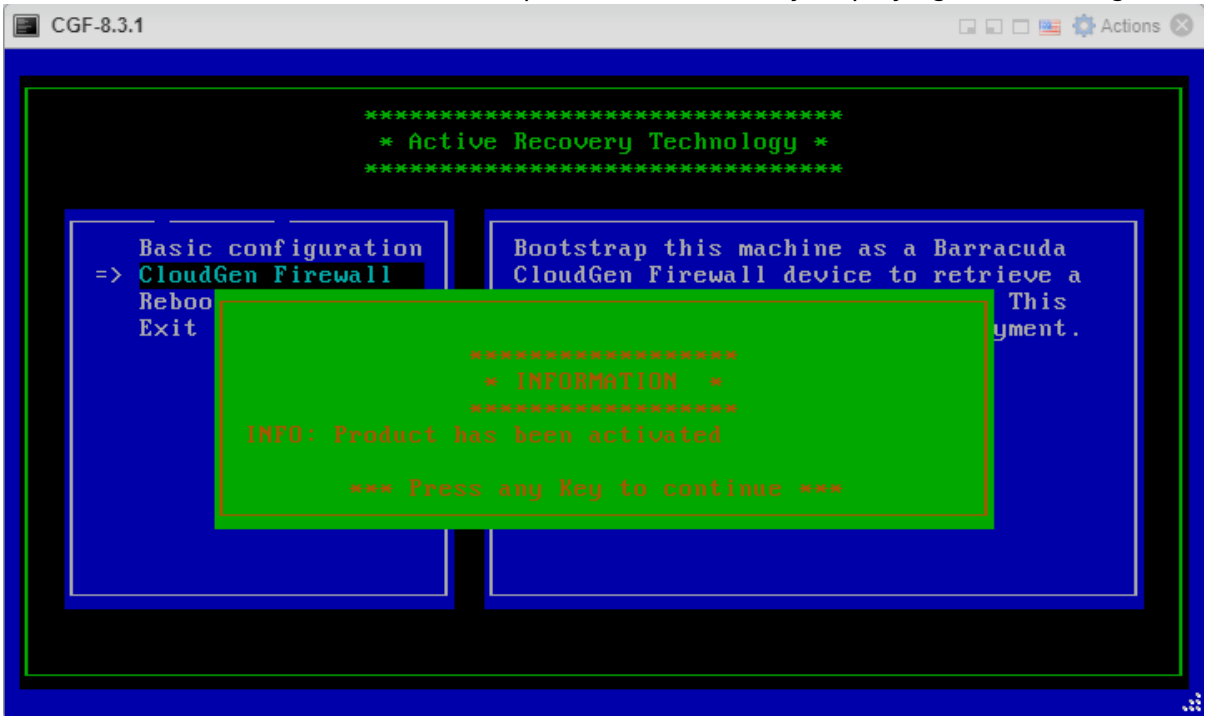
If you have received your token, perform the following steps:

1. Click the down button to go to the menu **CloudGen Firewall**.
2. Press **Enter**.
3. If your network was initially configured correctly, your firewall displays an area for entering the firewall-related token.

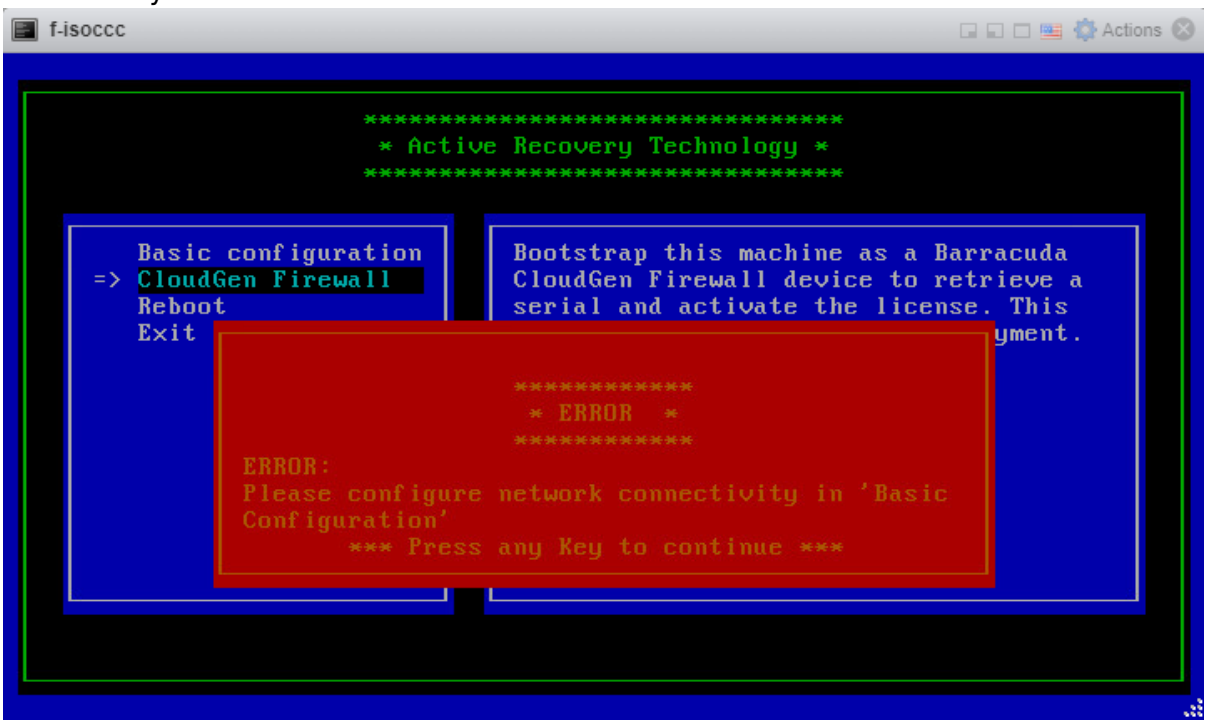


4. Enter the token that you received with your purchase order. Your license token has the format XXXXX-XXXXX-XXXXX, where each letter 'X' is a placeholder for a number or letter.

5. Click the down arrow on your keyboard to go to the **[OK]** button.
6. Press **Enter**.
7. If the firewall can connect to the ZTD server, your license is downloaded and installed automatically.
8. The firewall will confirm the successful product activation by displaying the following screen:



9. If an error is displayed in a red dialog requesting you to configure network connectivity, check if the values you entered earlier are correct.



If you had to change any of the values for the network configuration, repeat all the steps for the Basic Configuration on Your Firewall.

If activation still fails, reboot the firewall and continue with Option 2 below.

Step 6. Reboot the Firewall

1. Click the down arrow key on your keyboard to go to the menu entry **Reboot**.
2. Press **Enter**.
3. The firewall will reboot.
4. After the firewall has rebooted, check the activation status in the **Subscription Status** element in **DASHBOARD**.

If the **Subscription Status** element displays that the firewall is not licensed, then the activation has failed. Continue performing the steps in the following **Option 2**.

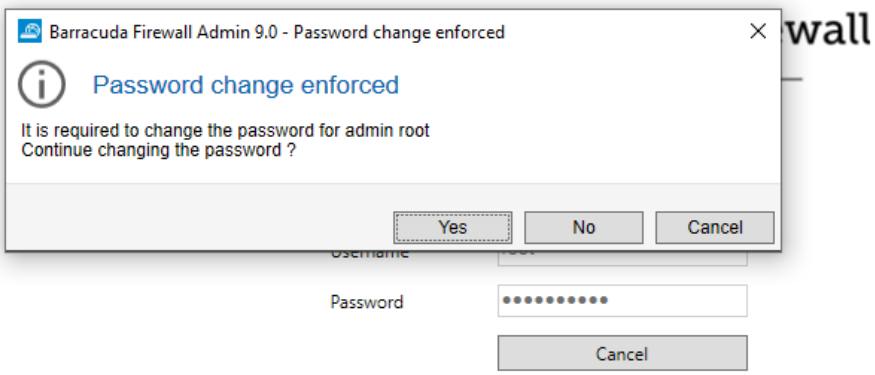
Option 2 - Activate Your Firewall Using Firewall Admin

If the deployment with activation does not succeed as described in Option 1 - Step 1: Activate Your Firewall Using Zero Touch Deployment in the ART Window, perform the following steps:

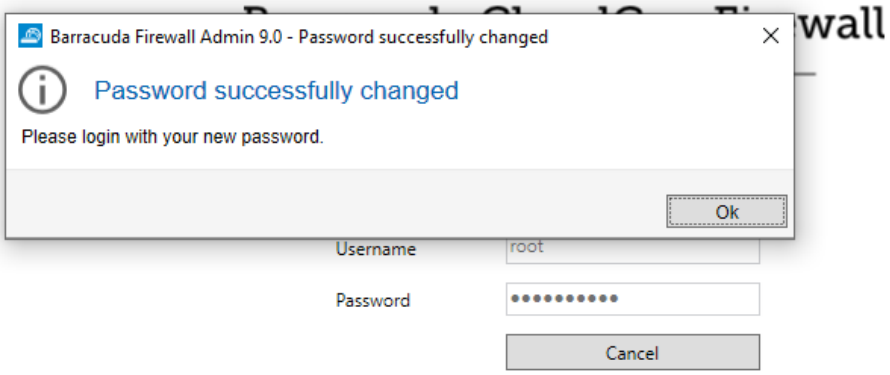
Step 1. Perform Finalizing Configurations

After the firewall has rebooted, you must change your password.

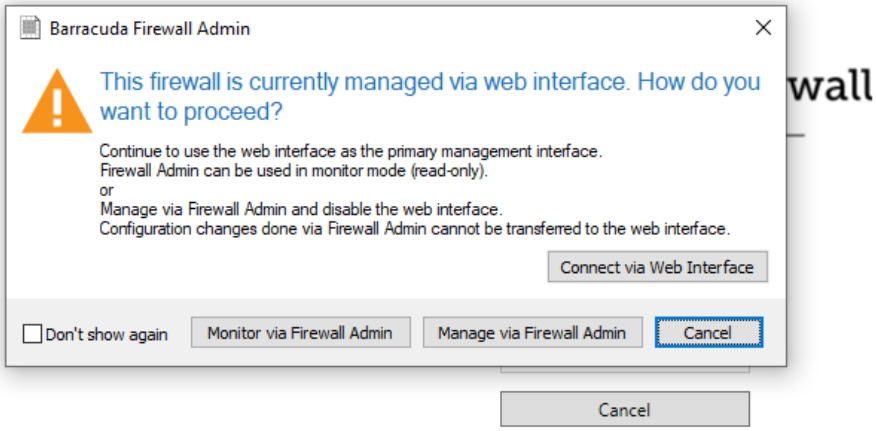
1. Log into your firewall.
2. When asked if you want to continue to change your password, click **Yes**.



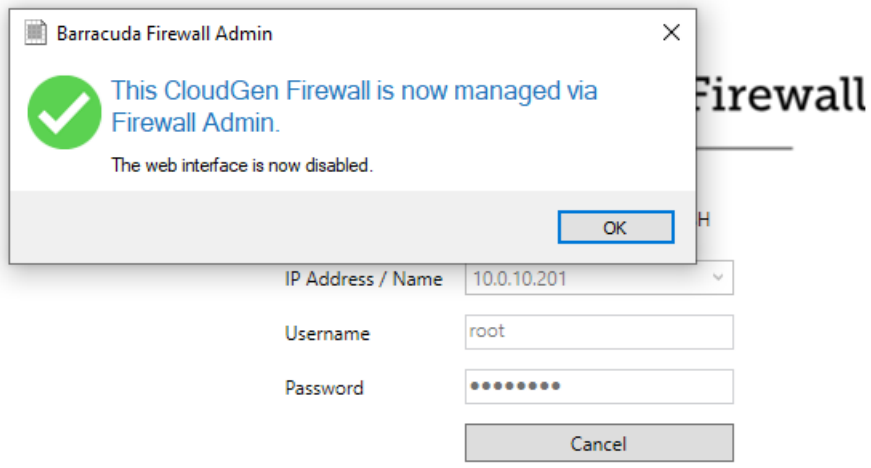
3. Enter a new password in the required edit field and confirm your input.
4. The firewall displays a dialog stating **Password successfully changed**.



5. Click **Ok**.
6. Re-log into your firewall.
7. The firewall displays a dialog window asking how you want to manage your appliance.



8. Click **Manage via Firewall Admin**.
9. The firewall confirms your choice by displaying a dialog window.



Step 2. License Your Barracuda CloudGen Firewall

For the firewall to get licensed, the Barracuda Firewall Admin application must be able to connect to the Internet directly or via proxy. You must enter a license token before activating your unit. Your token is sent to you by email from Barracuda Networks.

Your license token has the format XXXXX-XXXXX-XXXXX, where each letter 'X' is a placeholder for a number or letter.

Perform the following steps to complete the activation for your firewall:

1. Enter the license token.
2. Fill out the activation form.
3. Licenses are downloaded and installed automatically.

For more information, see How to Activate and License a Stand-Alone Virtual or Public Cloud Firewall or Control Center.

Use the VMware OVF Tool

On an ESXi7 Hypervisor, the VMware tools are installed already. In this case, it is not necessary to perform the following steps.

For any other lower version of the Hypervisor, perform the following steps:

1. Download the VMware OVF Tool from vmware.com. Use the following command:

`ovftool -datastore=`*`datastorename ovaimage`* `vi://`*`server-ip`*
where:
- `datastore` – The name of the data store.
- `ovaimage` – The path and name of the OVA file.
- `server-ip` – The IP address for the virtual appliance.

2. Configure the resources pool and the network mapping within the VMware virtual machine settings.
3. Using Barracuda Firewall Admin, connect to the virtual appliance for configuration.

Use the latest version of Barracuda Firewall Admin. If you configure the Barracuda CloudGen Firewall with a version of Barracuda Firewall Admin that is older than the firewall version, you might lose configuration data.

Next Step

After you deploy the Barracuda CloudGen Firewall Vx unit, continue with Get Started and optionally Best Practice - Performance Tuning on VMware Hypervisors.

Figures

1. vmdeploy_cgf_select_creation_type.png
2. vmdeploy_cgf_select_ovf_and_vmdk_files.png
3. vmdeploy_cgf_select_storage.png
4. vmdeploy_cgf_select_deployment_options.png
5. vmdeploy_cgf_art_basic_configuration.png
6. vmdeploy_cgf_art_configure_network_setup.png
7. vmdeploy_cgf_art_configure_network_setup_done.png
8. vmdeploy_cgf_writing_box_config.png
9. vmdeploy_cgf_writing_box_config_saved.png
10. vmdeploy_cgf_back_in_art_after_config_saved.png
11. vmdeploy_cgf_art_menu_enter_license_token.png
12. vmdeploy_cgf_product_has_been_activated.png
13. vmdeploy_cgf_missing_config_error.png
14. vmdeploy_cgf_box_rebootet_pwd_change_required.png
15. vmdeploy_cgf_box_rebootet_pwd_successfully_changed.png
16. vmdeploy_cgf_box_relogin.png
17. vmdeploy_cgf_box_managed_by_fwadmin.png