

# **BIG-IP<sup>®</sup> Virtual Edition and VMware ESXi: Setup**

Version 13.1





# Table of Contents

<b>Getting Started with BIG-IP Virtual Edition in ESXi.....</b>	<b>5</b>
About single NIC and multi-NIC configurations.....	5
Steps to deploy BIG-IP VE.....	5
<b>Prerequisites for BIG-IP Virtual Edition on ESXi.....</b>	<b>7</b>
Host CPU requirements.....	7
Host memory requirements.....	7
Configure SR-IOV on the hypervisor.....	7
Virtual machine memory requirements.....	8
Virtual machine storage requirements.....	8
Virtual machine network interfaces.....	9
<b>Deploying BIG-IP Virtual Edition in ESXi.....</b>	<b>11</b>
Deploy BIG-IP VE on ESXi.....	11
Setting the BIG-IP VE management IP address and passwords.....	12
Use Common OVF Tool to set management IP address and default passwords.....	12
OVA properties file for setting management IP address and default passwords...	12
OVF tool for setting management IP address and default passwords.....	13
Edit vApp to set the management IP address and default passwords.....	14
Use Customization Specification to set management IP address.....	15
Use BIG-IP Configuration utility tool to set management IP address.....	16
Configure SR-IOV on the guest.....	16
<b>After Deploying BIG-IP VE on ESXi.....</b>	<b>17</b>
Configure the CPU reservation.....	17
About licensing BIG-IP VE.....	17
Configure TSO support.....	17
Turn off LRO or GRO.....	18
Increase disk space for BIG-IP VE.....	18
Change the NIC used for BIG-IP VE management.....	19
About routes in a single NIC configuration.....	19
Change from single NIC to multi-NIC.....	20
Change from multi-NIC to single NIC.....	20
<b>Updating BIG-IP VE.....</b>	<b>21</b>
Updating BIG-IP VE.....	21
Download and import a BIG-IP VE update.....	21
Install a BIG-IP VE update.....	21
Reboot after a BIG-IP VE update.....	22
<b>Legal Notices.....</b>	<b>23</b>
Legal notices.....	23



# Getting Started with BIG-IP Virtual Edition in ESXi

---

## About single NIC and multi-NIC configurations

---

A typical BIG-IP VE configuration might include four NICs: one for management, one for internal, one for external, and one for high availability.

However, if you want to create a VM for a quick test, you can create a configuration with just one NIC. In this case, BIG-IP VE creates basic networking objects for you.

When BIG-IP VE first boots, it determines the number of active NICs. If BIG-IP VE detects one NIC, then:

- Networking objects (vNIC 1.0, a VLAN named Internal, and an associated self IP address) are created automatically for you.
- The port for the Configuration utility is moved from 443 to 8443.
- High availability (failover) is not supported, but config sync is.
- VLANs must have untagged interfaces.

If BIG-IP VE detects multiple NICs, then you create the networking objects. The port for the Configuration utility remains 443.

You can change the number of NICs after first boot and move from single to multi-NIC and vice versa.

---

***Note:** If there is no DHCP server in your environment and no IP address automatically assigned, then the networking objects will not be created and the port will not be moved.*

---

## Steps to deploy BIG-IP VE

---

To deploy the BIG-IP® Virtual Edition (VE) system on ESXi, you will perform these tasks.

Step	Details
1	Choose the license you want to buy, the BIG-IP VE modules you want, and the throughput you need. See <i>K14810: Overview of BIG-IP® VE license and throughput limits</i> on the AskF5™ Knowledge Base ( <a href="http://support.f5.com">http://support.f5.com</a> ) for details.
2	Confirm that you are running a hypervisor version that is compatible with a BIG-IP VE release. See <i>Virtual Edition and Supported Hypervisors Matrix</i> on <a href="http://support.f5.com">http://support.f5.com</a> for details.
3	Verify that the host hardware meets the recommended requirements.
4	If you plan to use SR-IOV, enable it on the hypervisor.
5	Download a BIG-IP VE image and deploy it.
6	For a single NIC configuration, remove the internal, external, and HA NICs and power on the VM.
7	If you are running a multi-NIC configuration without DHCP, manually assign an IP address for the BIG-IP Config Utility.

## Getting Started with BIG-IP Virtual Edition in ESXi

After you complete these tasks, you can log in to the BIG-IP VE system and run the Setup utility to perform basic network configuration.

# Prerequisites for BIG-IP Virtual Edition on ESXi

---

## Host CPU requirements

---

The host hardware CPU must meet the following requirements.

- The CPU must have 64-bit architecture.
- The CPU must have virtualization support (AMD-V or Intel VT-x) enabled.
- The CPU must support a one-to-one, thread-to-defined virtual CPU ratio, or on single-threading architectures, support at least one core per defined virtual CPU.
- In VMware ESXi 5.5 and later, do not set the number of virtual sockets to more than 2.
- If your CPU supports the Advanced Encryption Standard New Instruction (AES-NI), SSL encryption processing on BIG-IP® VE will be faster. Contact your CPU vendor for details about which CPUs provide AES-NI support.

## Host memory requirements

---

The number of licensed TMM cores determines how much memory the host system requires.

Number of cores	Memory required
1	2 Gb
2	4 Gb
4	8 Gb
8	16 Gb

## Configure SR-IOV on the hypervisor

---

To increase performance, you can enable Single Root I/O Virtualization (SR-IOV). You need an SR-IOV-compatible network interface card (NIC) installed and the SR-IOV BIOS must be enabled.

You must also load the `ixgbe` driver and blacklist the `ixgbev` driver.

1. In vSphere, access the command-line tool, `esxcli`.

2. Check to see what the `ixgbe` driver settings are currently.

```
esxcli system module parameters list -m ixgbe
```

3. Set the `ixgbe` driver settings.

In this example, `16,16` is for a 2 port card with 16 virtual functions.

```
esxcli system module parameters set -m ixgbe -p "max_vfs=16,16"
```

4. Reboot the hypervisor so that the changes take effect.

When you next visit the user interface, the SR-IOV NIC will appear in the Settings area of the guest as a PCI device.

5. Using vSphere, add a PCI device, and then add two virtual functions.

```
05:10.0 | Intel Corporation 82599 Ethernet Controller Virtual Function
```

```
05:10.1 | Intel Corporation 82599 Ethernet Controller Virtual Function
```

6. Use either the console command line or user interface to configure the VLANs that will serve as pass-through devices for the virtual function. For each interface and VLAN combination, specify a name and a value.
  - Name - `pciPassthru0.defaultVlan`
  - Value - 3001

To complete SR-IOV configuration, after you deploy BIG-IP® VE, you must add three PCI device NICs and map them to your networks.

## Virtual machine memory requirements

The guest should have a minimum of 4 GB of RAM for the initial 2 virtual CPUs. For each additional CPU, you should add an additional 2 GB of RAM.

If you license additional modules, you should add memory.

Provisioned memory	Supported modules	Details
4 GB or fewer	Two modules maximum.	AAM can be provisioned as standalone only.
4-8 GB	Three modules maximum.	BIG-IP® DNS does not count toward the module limit. Exception: Application Acceleration Manager™ (AAM®) cannot be provisioned with any other module; AAM is standalone only.
8 GB	Three modules maximum.	BIG-IP DNS does not count toward the module-combination limit.
12 GB or more	All modules.	N/A

**Important:** To achieve licensing performance limits, all allocated memory must be reserved.

## Virtual machine storage requirements

The amount of storage you need depends on the BIG-IP modules you want to use, and whether or not you intend to upgrade.

**Note:** These values apply to BIG-IP VE 13.1.0.2 and later.

Provisioned storage	Supported modules	Details
9 GB (LTM_1SLOT)	Local Traffic Manager™ (LTM®) module only; no space for LTM upgrades.	You can increase storage if you need to upgrade LTM or provision additional modules.
40 GB (LTM)	LTM module only; space for installing LTM upgrades.	You can increase storage if you decide to provision additional modules. You can also install another instance of LTM on a separate partition.
60 GB (ALL_1SLOT)	All modules except Secure Web Gateway (SWG); no space for installing upgrades.	The Application Acceleration Manager™ (AAM®) module requires 20 GB of additional storage dedicated to AAM. If you are not using AAM, you

Provisioned storage	Supported modules	Details
		can remove the datastore disk before starting the VM.
82 GB (ALL)	All modules except SWG and space for installing upgrades.	The Application Acceleration Manager™ (AAM®) module requires 20 GB of additional storage dedicated to AAM. If you are not using AAM, you can remove the datastore disk before starting the VM.

For production environments, virtual disks should be deployed Thick (allocated up front). Thin deployments are acceptable for lab environments.

---

*Note: To change the disk size after deploying the BIG-IP system, see Increase disk space for BIG-IP VE.*

---

## Virtual machine network interfaces

---

When you deploy BIG-IP® VE, a specific number of virtual network interfaces (vNICs) are available.

Four vNICs are automatically defined for you.

- For management access, one VMXNET3 vNIC or Flexible vNIC.
- For dataplane access, three VMXNET3 vNICs.

Each virtual machine can have a maximum of 10 virtual NICs.



# Deploying BIG-IP Virtual Edition in ESXi

---

## Deploy BIG-IP VE on ESXi

---

To create a BIG-IP® VE virtual appliance, download a template from F5® and deploy it in your environment.

1. In a browser, open the F5 Downloads page (<https://downloads.f5.com>) and log in.
2. On the Downloads Overview page, select **Find a Download**.
3. Under Product Line, select **BIG-IP v13.x/Virtual Edition**.
4. Under Name, select **Virtual-Edition**.
5. If the End User Software License is displayed, read it and then click **I Accept**.
6. Download one of the files that ends with `scsi.ova`.
7. Start the vSphere client and log in.
8. From the vSphere File menu, choose **Deploy OVF Template**.
9. Browse to the .ova file and click **Next**.  
The template is verified.
10. Click **Next** and complete the wizard. Note the following.

Section	Details
Configuration	Choose from the available configurations. You can change CPU or RAM later.
Storage	If you decide to increase storage later, you must also adjust the BIG-IP directories to use the extra storage space. See <i>Increasing disk space for BIG-IP® VE</i> for details.
Datastore	Choose <b>Thick</b> for production environments. <b>Thin</b> is sufficient for lab environments.
Source Networks	The wizard leads you through creating four networks: internal, external, management, and high availability (HA).
Ready to Complete	If you want to deploy with the four default networks, then select the <b>Power on after deployment</b> check box. If you want a single NIC deployment, do not select this check box.

11. Click **Finish**.
12. For a single NIC deployment, edit the virtual machine's properties and remove Network adapter 2, 3, and 4.

The virtual machine is created, as well as two user accounts.

- The root account provides access locally, using SSH, or the F5 Configuration utility. The root account password is `default`.
- The admin account provides access through the web interface. The admin account password is `admin`.

You should change passwords for both accounts before bringing a system into production.

If you need to create a redundant configuration, place the two BIG-IP VE virtual appliances (the active-standby pair) on separate physical hosts. You can accomplish this in one of two ways:

- Manually create a virtual machine peer on each host.

- If you are using VMware Dynamic Resource Scheduler (DRS), create a DRS rule with the **Separate Virtual Machine** option that includes each BIG-IP VE in the pair.

## Setting the BIG-IP VE management IP address and passwords

---

When you deploy BIG-IP VE:

- If you have DHCP in your environment, a management IP address is assigned.
- If you do not have DHCP, a generic management IP address (192.168.1.245) is assigned.
- A password is assigned to the default accounts: root (default) and admin (admin).

In ESXi 5.5 u2, 6.0, 6.5, and later, in BIG-IP VE 13.1.0.2 and later, you can specify a specific management IP address (IPv4 or IPv6) and different default passwords.

There are many different ways to do this.

- Before deploy, by editing the OVA file's properties:
  - By using the Common OVF Tool (COT)
  - By editing the OVA descriptor file, or
  - By using the VMware OVF tool
  - By using the tool of your choice
- During deploy, by using the API of your choice to set the vApp properties
- After deploy:
  - By manually updating the vApp properties
  - By using a Custom Specification
  - By using the BIG-IP management config tool

---

**Important:** This functionality is supported in a multi-NIC environment only.

---

## Use Common OVF Tool to set management IP address and default passwords

You can edit the OVA (template) properties so that when you deploy BIG-IP VE, you can specify values for the management IP address and default passwords.

To edit the OVA, you can use the Common OVF Tool (COT).

For more information about COT, see <http://cot.readthedocs.io/en/latest>.

1. Copy the OVA to a machine with enough free space (at least two times the OVA file size).
2. Run a command like the following:

```
cot edit-properties <source filename>.ova -p net.mgmt.addr="" +string -p net.mgmt.gw="" +string -p user.root.pwd="" +string -p user.admin.pwd="" +string -u -o <destination filename>.ova
```

The OVA properties are updated.

Then, when you deploy the OVA file, you can specify the values.

---

**Note:** After you set the IP address and password, if you want to set it again, you must first delete this file on BIG-IP: `/shared/vadc/.ve_cust_done`

---

## OVA properties file for setting management IP address and default passwords

You can edit the OVA (template) properties so that when you deploy BIG-IP VE, you can specify values for the management IP address and default passwords.

Before deploy, you can extract the contents of the OVA file to edit the OVF properties directly.

Modify the OVF file and add the following properties to the <ProductSection> area of the descriptor file.

```
<Category>Network properties</Category>
  <Property ovf:key="net.mgmt.addr" ovf:type="string" ovf:value=""
  ovf:userConfigurable="true">
    <Label>mgmt-addr</Label>
    <Description>F5 BIG-IP VE's management address in the format of "IP/prefix"</
  Description>
  </Property>
  <Property ovf:key="net.mgmt.gw" ovf:type="string" ovf:value=""
  ovf:userConfigurable="true">
    <Label>mgmt-gw</Label>
    <Description>F5 BIG-IP VE's management default gateway</Description>
  </Property>
<Category>User properties</Category>
  <Property ovf:key="user.root.pwd" ovf:type="string" ovf:value=""
  ovf:userConfigurable="true">
    <Label>root-pwd</Label>
    <Description>F5 BIG-IP VE's SHA-512 shadow or plain-text password for "root" user</
  Description>
  </Property>
  <Property ovf:key="user.admin.pwd" ovf:type="string" ovf:value=""
  ovf:userConfigurable="true">
    <Label>admin-pwd</Label>
    <Description>F5 BIG-IP VE's SHA-512 shadow or plain-text password for "admin" user</
  Description>
  </Property>
```

## OVF tool for setting management IP address and default passwords

You can edit the OVA (template) properties so that when you deploy BIG-IP VE, you can specify values for the management IP address and default passwords.

Using VMware's OVF tool, here is an example of code you would use to deploy BIG-IP VE with these settings.

```
ovftool
  --sourceType=OVA \
  --acceptAllEulas \
  --noSSLVerify \
  --diskMode=thin \
  --skipManifestCheck \
  --X:logToConsole \
  --X:logLevel=verbose \
  --datastore='mylab' \
  --name='vmname' \
  --vmFolder='myfolder' \
  --deploymentOption='dualcpu' \
  --net:"Internal=Internal" \
  --net:"Management=Management" \
  --net:"HA=HA" \
  --net:"External=External" \
  --X:injectOvfEnv \
  --prop:net.mgmt.addr="10.10.10.124/22" \
  --prop:net.mgmt.gw="10.10.11.254" \
  --prop:user.root.pwd="mypassword" \
  --prop:user.admin.pwd="mypassword" \
  <path_to_bigip.ova> \
  "vi://user[@userdomain]:password@domain.com/<datacenter-name>/host/<esxi-host>"
```

## Edit vApp to set the management IP address and default passwords

After you deploy a VM running BIG-IP VE, you can manually assign a management IP address and root and admin passwords. Use this procedure if you want to set these values one time on a specific VM.

*Note: These instructions may differ slightly, based on your version of vSphere.*

1. Stop the VM.
2. Right-click the VM and choose **Edit Settings**.
3. Click the vApp Options tab.
4. In the Authoring section, expand the Properties area.
5. Click **New**.
6. On the Edit Property Settings window, complete the fields.

Category	Label	Key ID	Type
BIG-IP VE	admin-pwd	user.admin.pwd	String

*Important: The password can be plain text or SHA-512 encrypted.*

7. Click **OK**.
8. Create three more properties, using these values:

Category	Label	Key ID	Type
BIG-IP VE	root-pwd	user.root.pwd	String
BIG-IP VE	mgmt-addr	net.mgmt.addr	String
BIG-IP VE	mgmt-gw	net.mgmt.gw	String

*Important: The Key ID must be the exact value shown in the table.*

9. Scroll up and you should now have these settings available:

The screenshot shows a settings panel for 'BIG-IP VE' with a dropdown arrow and the text '4 settings'. Below this are four rows, each with a label and an empty text input field:

- admin-pwd
- mgmt-addr
- mgmt-gw
- root-pwd

10. Populate these fields and click **OK**.
11. Start the VM. The properties are applied.

After you set the IP address and password, if you want to set it again, you must first delete this file: /shared/vadc/.ve\_cust\_done

## Use Customization Specification to set management IP address

You can prompt the user to enter an IP address and mask after BIG-IP VE is deployed. To do this, you can create a VMware Custom Specification that you can use over and over on multiple VMs.

Notes:

- These instructions may differ slightly, based on your version of vSphere.
  - This procedure is for setting the management IP address; not for setting default passwords.
  - You can do this procedure after you deploy, not during.
1. Ensure the BIG-IP VE instance is powered off.
  2. Create a Custom Specification policy.
    - a) Open the vSphere Client Home page.
    - b) In the Navigator pane, under Policies and Profiles, click Customization Specification Manager.
    - c) Click **Create a new specification**.

Page	Setting	Value
Specify Properties	Target VM Operating System	Linux
Set Computer Name	Use the virtual machine name	Recommended
Set Computer Name	Domain	Your domain
Time Zone	Area	Your area/time zone
Configure Network	Manually select custom settings	<p>Create four NICs (management, internal, external, HA).            For the management NIC, click <b>Edit the selected adapter</b>. Then for IPv4 or IPv6, click <b>Prompt the user for an address when the specification is used</b> and click <b>OK</b>.</p> <p>If you enter static values, they are applied. However, if you want to re-use this Custom Spec, you likely want to prompt the user.</p> <hr/> <p><i>Note: For IPv6, you must set values for both IPv4 and IPv6.</i></p> <hr/>
Enter DNS and Domain Settings		Not supported. You may have to enter a value to move past this page.

3. Edit the VM to use this policy.
  - a) Right-click the VM and choose **Guest OS > Customize Guest OS**.
  - b) Select your specification from the list and click **Next**.
  - c) Enter the IP address and mask and click **Finish**.

---

**Note:** After you set the IP address and password, if you want to set it again, you must first delete this file: `/shared/vadc/.ve_cust_done`

---

## Use BIG-IP Configuration utility tool to set management IP address

If your network has DHCP, an IP address is automatically assigned to BIG-IP® VE during deployment. You can use this address to access the BIG-IP VE Configuration utility or `tmssh` command-line utility.

If no IP address was assigned, you can assign one by using the BIG-IP Configuration utility tool.

1. Connect to the virtual machine by using the hypervisor's console.
2. At the login prompt, type `root`.
3. At the password prompt, type `default`.
4. Type `config` and press Enter.  
The F5 Management Port Setup screen opens.
5. Click **OK**.
6. Select **No** and follow the instructions for manually assigning an IP address and netmask for the management port.

You can use a hypervisor generic statement, such as `tmssh show sys management-ip` to confirm that the management IP address was set properly.

You can now log into the BIG-IP VE Config utility, and license and provision BIG-IP VE.

## Configure SR-IOV on the guest

---

Before you can complete these steps, you must have configured Single Root I/O Virtualization (SR-IOV) on the hypervisor.

After deploying BIG-IP® VE, to configure SR-IOV on the guest, you must add three PCI device NICs and map them to your networks.

1. In vSphere, delete the existing Source Networks for External, Internal, and HA.

---

**Important:** *Leave the Source Network for Management.*

---

2. Edit the settings for the virtual machine to add a PCI device.  
If your hypervisor was set up correctly, there will be 16 virtual functions on each port (05:10.x and 05:11:x).
3. Map the new device to the VLAN for your internal subnet.
4. Repeat steps 2 and 3 for the external and HA VLANs.
5. When all four destination networks are correctly mapped, click **Next**.  
The Ready to Complete screen opens.

# After Deploying BIG-IP VE on ESXi

---

## Configure the CPU reservation

---

In VMware, based on selections you made when you deployed the OVA file, a specific amount of memory is reserved for the BIG-IP VE virtual machine.

CPU is not specifically reserved, so to prevent instability on heavily-loaded hosts, you should reserve it manually.

1. In vSphere, edit the properties of the virtual machine.
2. Click the Resources tab.
3. In the Settings area, click **CPU**.
4. In the Resource Allocation section, use the slider to change the reservation.

The CPU reservation can be up to 100 percent of the defined virtual machine hardware. For example, if the hypervisor has a 3 GHz core speed, the reservation of a virtual machine with 2 CPUs can be only 6 GHz or less.

5. Click **OK**.

## About licensing BIG-IP VE

---

In order to use BIG-IP VE, you must have a license from F5. Starting with BIG-IP VE version 13.1, you can revoke the license from a virtual machine and re-use it on another virtual machine.

From the Configuration utility, to revoke the license, go to **System > License** and click **Revoke**.

From tmsh, to revoke the license, run the command `tmsh revoke sys license`.

This functionality works for BIG-IP VE BYOL only.

## Configure TSO support

---

The TCP Segmentation Offloading (TSO) feature, which includes support for large receive offload (LRO) and Jumbo Frames, is enabled by default.

*Note:* You must have the `admin` user role to enable or disable TSO support.

---

1. Use an SSH tool to access the BIG-IP® VE command line.
2. Log in as `root`.
3. Type `tmsh` to open the `tmsh` utility.  
You will see `tmsh` at the prompt once the utility is opened.
4. To determine whether TSO support is currently enabled, use the command:  
`show sys db tm.tcpsegmentationoffload`
5. To enable support for TSO, use the command:  
`sys db tm.tcpsegmentationoffload enable`
6. To disable support for TSO, use the command:  
`sys db tm.tcpsegmentationoffload disable`

## Turn off LRO or GRO

---

Although there are a number of ways to turn off LRO, the most reliable way is to connect to the virtual machine and use the `ethtool` utility.

1. Use an SSH tool to access the BIG-IP® VE TMSH utility.
2. From the command line, log in as `root`.
3. Type `tmsh` to open the utility.
4. Run the following commands, replacing `<X>` in each of the examples with the NIC number.

To	Use this command
Turn off rx-checksumming.	<code>ethtool -K eth&lt;X&gt; rx off</code>
Turn off LRO.	<code>ethtool -K eth&lt;X&gt; lro off</code>
Turn off GRO.	<code>ethtool -K eth&lt;X&gt; gro off</code>

5. Confirm that LRO and GRO are turned off by running this command: `ethtool -k eth<X>`.

In the system response to your command, you should see this info:

```
generic-receive-offload: off
large-receive-offload: off
```

If either of these responses is `on`, your attempt to turn them off was not successful.

6. Repeat this process for each of the NICs that the BIG-IP VE uses to pass traffic.

See the ESXi documentation for more details.

## Increase disk space for BIG-IP VE

---

Before proceeding with these steps, use vSphere to expand the disk size for the BIG-IP® VE virtual machine and reboot.

Use the BIG-IP VE `tmsh` utility to increase the amount of disk space used by the four BIG-IP VE directories:

- `/config`
- `/shared`
- `/var`
- `/var/log`

---

**Note:** At the time of this release, decreasing the VE disk size is not supported.

---

For each directory you want to resize, complete these steps.

1. Use an SSH tool to access the BIG-IP VE `tmsh` utility.
2. From the command line, log in as `root`.
3. List the current size of the directories on your disk so you can determine which ones need to be resized.

```
tmsh show sys disk directory
```

4. Expand the size of the directories in which you need additional space.

```
tmsh modify sys disk directory <directory name> new-size <new directory
size in 1KB blocks>
```

For example, use `tmsh modify sys disk directory /config new-size 3145740` to increase the size of `/config` directory to 3145740 1KB blocks (or roughly 3,221,237,760 bytes).

5. To confirm that the command you just submitted is properly scheduled, you can show the new list of directories again.

```
tmsh show sys disk directory
```

6. If you change your mind about a submitted size change, you can revoke the size change.

```
tmsh modify sys disk directory /config new-size 0
```

In this example, the size of the `/config` directory is left as is, revoking any scheduled size changes.

After you submit this sequence of `tmsh` commands, the directory size changes will be scheduled to occur the next time the BIG-IP VE virtual machine (VM) is rebooted.

The next time the VM running BIG-IP VE reboots, the changes are applied.

## Change the NIC used for BIG-IP VE management

---

By default, management traffic goes through the `eth0` NIC and data traffic goes through the other available NICs. If you need to use `eth0` for data traffic, you can change the NIC that management traffic goes through.

1. Use SSH to connect to BIG-IP VE.
2. If you need to determine which NICs are available, stop TMM by typing `bigstart stop tmm`. Then type `ip addr` to view the list of available NICs.
3. Change the management NIC by typing `tmsh modify sys db provision.managementeth value eth1` where `eth1` is the NIC you want to use for management. You can use any available NIC.
4. Press Enter.
5. Reboot BIG-IP VE by typing `reboot` and pressing Enter.

When BIG-IP VE is running again, you can use `eth0` for data.

---

*Note:* If the subnet associated with the management NIC does not have DHCP, you must assign a new IP address by using the BIG-IP Configuration utility tool.

---

## About routes in a single NIC configuration

---

If you want to configure a static route that relies on a gateway in the same subnet as the self IP address, you must first disable the setting that enforces single NIC setup:

```
modify sys db provision.lnicautoconfig value disable
```

Confirm that the value is correct by typing `list sys db provision.lnicautoconfig`.

The return value should be `disable`.

If you do not change this value, any time you reboot BIG-IP VE, the manually-configured static route will cause validation errors during `load sys config`.

## Change from single NIC to multi-NIC

---

When you initially boot BIG-IP VE, if it recognized only one NIC, then some network configuration was done automatically. If you want to use more than one NIC, complete the following steps.

1. Use an SSH tool to connect to BIG-IP VE.
2. Return to the default configuration.  

```
tmsm load sys config default
```
3. Save the changes.  

```
tmsm save sys config
```
4. Set a database variable so that the number of NICs will be recognized on reboot.  

```
setdb provision.lnic enable
```
5. Reboot BIG-IP VE.  

```
reboot
```

When the BIG-IP VE instance is up and running, multiple NICs will be recognized and you can begin configuring BIG-IP VE.

## Change from multi-NIC to single NIC

---

If you have a BIG-IP VE configuration with multiple NICs, you can simplify the configuration to have only one NIC. When you boot the BIG-IP VE and only one NIC is recognized, some networking objects are created automatically for you.

1. Use an SSH tool to connect to BIG-IP VE.
2. Return to the default configuration of BIG-IP VE.  

```
tmsm load sys config default
```
3. Save the changes.  

```
tmsm save sys config
```
4. Set a database variable so that the number of NICs will be recognized on reboot.  

```
setdb provision.lnic forced_enable
```
5. Reboot BIG-IP VE.  

```
reboot
```

When the BIG-IP VE instance is up and running, it will have a single NIC and related network objects will be created.

# Updating BIG-IP VE

---

## Updating BIG-IP VE

---

You do not need to reinstall BIG-IP® VE in order to install updates. You can use the Software Management tool in the Configuration utility, or you can upgrade the software from the command line.

To update BIG-IP VE, you will:

1. Download the ISO and MD5 files.
2. Install the downloaded files to an inactive boot location.
3. Boot the BIG-IP VE to the new boot location.

## Download and import a BIG-IP VE update

To install an update, BIG-IP software needs access to the ISO file. If the update is a hotfix, you need the ISO files for both the base version and the hotfix.

1. In a browser, open the F5® Downloads page (<https://downloads.f5.com>).
2. Download the version's base ISO file and its associated MD5 checksum file.
3. Download the update ISO file and its associated MD5 checksum file.

---

***Important:** Before you perform the installation, you should test the integrity of the ISO files to verify that you have downloaded clean copies. Use an MD5 verification program to ensure that the downloaded ISO files' checksums match the values in their corresponding MD5 files.*

---

4. In the BIG-IP VE user interface, on the Main tab, click **System > Software Management > Image List > Import**.
5. Click **Browse** to navigate to the downloaded base level installation file.
6. When the image name appears in the **Software Image** field, click **Import** to begin the operation.

---

***Important:** Do not navigate away from this screen before the operation is done.*

---

When the import is complete, the Import page closes and the downloaded base image displays as an available image.

7. Click the Hotfix List tab.
8. At the right side of the screen, click **Import**.
9. Click **Browse** to navigate to the downloaded hotfix installation file.
10. When the image name appears in the **Software Image** field, click **Import** to begin the operation.

---

***Important:** Do not navigate away from this screen before the operation is done.*

---

When the import is complete, the Import page closes and the downloaded hotfix displays in the list of available images.

You can now install the downloaded update.

## Install a BIG-IP VE update

After you download and import the software installation image, you can initiate the installation operation. There are three boot locations on which you can install images on the BIG-IP® system. The process for installing a hotfix or a base version is essentially the same.

1. On the Main tab, click **System > Software Management**.  
The Software Management Image List screen opens.
2. In the Available Images area, select the software image you want to install and click **Install**.  
The Install Software Image popup screen opens.
3. Select the disk you want to install the image on, and then type or select a volume name, and click **Install**.

The upgrade process installs the software on the inactive disk location that you specify. This process usually takes between three and ten minutes.

---

***Tip:** If there is a problem during installation, you can use log messages to troubleshoot a solution. The system stores the installation log file as `/var/log/liveinstall.log`.*

---

The software image is installed.

When the installation operation is complete, you can safely reboot the newly installed volume or partition.

### Reboot after a BIG-IP VE update

When the installation operation is complete, you can safely reboot into the newly installed volume or partition.

1. On the Main tab, click **System > Software Management**.  
The Software Management Image List screen opens.
2. On the menu bar, click **Boot Locations**.  
The Boot Locations screen opens.
3. In the Boot Location column, click the link representing the boot location you want to activate.  
The properties screen for the boot location opens.
4. Click **Activate**.  
A confirmation screen opens.
5. Click **OK** to initiate the reboot operation.  
The system presents progress messages during the restart operation.

When the BIG-IP® VE system reboot is complete, the system presents the login screen. To configure the system, log in using an account that has administrative permissions.

# Legal Notices

---

## Legal notices

---

### **Publication Date**

This document was published on August 31, 2018.

### **Publication Number**

MAN-0347-10

### **Copyright**

Copyright © 2018, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

### **Trademarks**

For a current list of F5 trademarks and service marks, see <http://www.f5.com/about/guidelines-policies/trademarks>.

All other product and company names herein may be trademarks of their respective owners.

### **Patents**

This product may be protected by one or more patents indicated at: <https://f5.com/about-us/policies/patents>.

### **Export Regulation Notice**

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.



# Index

## A

admin password *12–14*

## B

BIG-IP VE on VMware overview *5*  
 BIG-IP Virtual Edition  
   updating *21*

## C

Common OVF tool *12*  
 COT *12*  
 CPU reservation for ESXi *17*  
 customization specification *15*

## D

deployment overview *5*  
 disk size, *See* virtual disk size  
 downloads  
   and importing update *21*  
   of ISO base file *21*  
   of ISO update file *21*

## E

eth0  
   changing *19*

## G

GRO  
   turning off *18*  
 guest memory *8*

## H

hypervisor  
   configuring for SR-IOV *7*  
   configuring for TSO *17*

## I

installation  
   rebooting after *22*  
 installation operation *21*  
 ISO file  
   and location on virtual machine *21*  
   downloading *21*  
   downloading base file *21*  
   downloading update file *21*

## L

licensing BIG-IP VE *17*  
 log file  
   and location *21*  
   and media speed messages *21*  
 log in  
   after updating *22*  
 LRO  
   turning off *18*

## M

management  
   accessing different port *19*  
 management IP address *12–14*  
 memory  
   guest *8*  
 multi-NIC *20*  
 multiple NIC configuration *5*

## O

OVA file, location *11*  
 OVA properties file *12*  
 OVF tool *13*

## P

PCI device NIC mapping *16*  
 PEM performance  
   optimizing *18*

## R

reboot operation  
   after updating *22*

## S

setting management IP address *15, 16*  
 single nic  
   routes *19*  
 single NIC *20*  
 single NIC configuration *5*  
 SR-IOV  
   configuring hypervisor for *7*  
 system update procedure *21*

## T

task list  
   for updating on virtual machine *21*  
 TSO support  
   configuring hypervisor for *17*

## Index

### U

update

    downloading and importing *21*

    installing *21*

### V

virtual disk size

    extending *18*

    increasing *18*

VMware virtual machine *11*