Convert a Gen34 VM to a Gen4 Network Configuration

You can use this document to update the network configuration for your upgraded virtual machine.

In short, during the upgrade process, most upgraded virtual machines were updated with a temporary Gen34 network configuration. For optimal performance, these virtual machines must be upgraded to a native Gen4 network configuration.

⚠ Although your upgraded virtual machines will not experience a price increase, any virtual machine you create directly in the Armor Management Portal (AMP), will be priced to the Gen4 model.

⚠ If you prefer to have Armor perform these steps, you can open a support ticket; however, there is a charge for this service.

⚠ In this document, the term **upgraded virtual machine** refers to the original virtual machine that was upgraded from Gen3 to Gen4 Armor Complete.

Step 1: Review your permissions

⚠ In order to fully convert you Gen34 virtual machine to a Gen4 virtual machine, you must have the following permissions assigned to your account:

- Read Workload(s)
- Write Workload
- Read Virtual Machine Stats
- Read Virtual Machine(s)
- Write Virtual Machine
- Scale Virtual Machine
- Read Location(s)
- Read Virtual Data Centers
- Read Tasks
- Write Tasks
- Read Storage
- Read Network IP
- Write Network IP
- Read Network NAT
- Write Network NAT
- Read Firewall
- Write Firewall

To review your permissions:

1. In the Armor Management Portal (AMP), in the top-right corner, click the vertical ellipses.
2. Click **Settings**.
3. Click Roles.
4. Select a role that is **Granted**.
5. Review the list of marked permissions.

⚠ If you are listed as an **Admin**, then by default, your account already contains every permissions in AMP.

⚠ To learn more about roles and permissions, see Roles and Permissions.

Step 2: Create a new virtual machine

In the Armor Management Portal (AMP), you will essentially create a new virtual machine that contains the same configurations as your upgraded virtual machine. In a later step, you will delete your upgraded virtual machine.

1. In the Armor Management Portal, in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Hover over the plus (+) icon, and then click the **Virtual Machine** icon.
    - If you do not have any virtual machines listed, then click **Deploy New**, and then select **Virtual Machine**.
4. Locate and select the desired operating system and operating system version.
5. On the right side, use the **Region** drop-down menu to select the data center to host your virtual machine.

6. Select the desired virtual machine based on your CPU and memory needs (GB).
    - You can click **High CPU** or **High Memory** to filter the list of virtual machines. You can also click **Show All Options** to see every virtual machine offering.
    - Armor labels virtual machines by CPU and memory features. For instance, **2x4** indicates that the virtual machine has 2 CPU and 4 GB of memory.
7. In **Name**, enter a descriptive name for your virtual machine.
8. In **Workload**, select **New Workload**.
9. In **New Workload Name**, enter a descriptive name.
10. In **New Tier Name**, enter a descriptive name.
11. In **Location**, select and verify the data center to host your virtual machine.
12. Under **Access Credentials**, note your username to access the virtual machine.
13. In **Password**, enter a secure password to use to access the virtual machine.
    - Your password must contain:
        - An upper-case letter
        - A lower-case letter
        - A number
        - A special character: ! @ # $ % ^ * ( ) { } [ ]
    - You can also click **Generate Password** to allow Armor to create a password.
14. (Optional) For additional storage, under **Storage Substrate** and **Disk Size**, select your desired storage, and then click **Add Disk**.
15. On the right-side menu, review the pricing information, and then click **Purchase**.
    - When you order a virtual machine, you are also ordering Intelligence Security Model (ISM) for the virtual machine. Prices for ISM will vary based on the number of virtual machines you have ordered. IMS pricing is based on the following tiered structure:

Tier	Number of Virtual Machines
1	1 - 10
2	11 - 25
3	26 - 100
4	101- 250
5	251 - 500
6	500 +

16. To view the status of your newly created virtual machine, in the left-side navigation, click **Infrastructure**, click **Virtual Machines**, and then search for your newly created virtual machine.

To learn more about virtual machines, see Virtual Machines.

Step 3: Update firewall rules

Create and add firewall rules to your newly created virtual machine. These firewall rules should match the firewall rules associated with your upgraded virtual machine.

In the **Firewall** screen, each entry in the table represents a single firewall rule; however, each firewall rule can contain several IP addresses or just a single IP address.

You can combine related IP addresses into a single **IP Group**. For example, if you want to block traffic from three separate IP address, you do not have to create three separate firewall rules. Instead, you can combine the three separate IP addresses into a single, configurable **IP Group**. Then, when you create a firewall rule, you can pick the newly created **IP Group** as your **Source** or **Destination** IP addresses.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Click **IP Groups**.
5. Click **Actions**, and then click **New Group**.
6. In **IP Group Name**, enter a descriptive name.
    - Armor recommends that you add **Source** or **Destination** into the name of the IP Group to help you identify the IP Group as the **Source** or **Destination** IP group.
7. In **Add Members To Group**, enter a member, and then click the plus icon.
    - You can enter:
        - A single IP address
        - A range of IP addresses
        - CIDR
    - You must add at least one member.
    - You can add multiple members to a service group.
8. Click **Apply**.
    - The newly created IP group will appear at the bottom of the table.

In the **Firewall** screen, each entry in the table represents a single firewall rule; however, each firewall rule can contain several protocols (and ports).

You can combine related protocols (and ports) into a **Service Group**. For example, if you want to create a firewall rule to block three types of traffic, you do not have to create three separate firewall rules. Instead, you can combine the three types of traffic (protocols and ports) into a single, configurable **Service Group**. Then, when you create a firewall rule, you can pick the newly created **Service Group**.

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top drop-down menu, select the desired data center.
4. Click **Service Groups**.
5. Click **Actions**, and then click **New Group**.
6. In **Service Group Name**, enter a descriptive name.
7. In **Add Members To Group**, enter the service or sub-protocol, and then click the plus (+) icon.
    - You must add at least one member.
    - You can add multiple members to a service group.

Service or Sub-Protocol	Notes	Example
Services (TCP, UDP, etc.)	You must enter a port number. These services are not case-sensitive.	• tcp/80 • TCP/80 • Tcp/80 • tCp/80
Additional services (AARP, AH, etc.)	These additional services are not case-sensitive. Do not enter a port number with these additional services.	• ATALK • igmp • Gre
Sub-protocols (echo-reply, redirect, etc.)	You must enter **icmp**, followed by the specific sub-protocol. You must enter the sub-protocol in lower-case letters. Do not enter a port number.	• icmp/source-host-isolated • icmp/time-exceeded

8. Click **Apply**.
    - The newly created service group will appear at the bottom of the table.

ⓘ For a complete list of supported services and sub-protocol, see Review supported services and sub-protocols.

Step 3: Create a firewall rule

1. In the Armor Management Portal (AMP), on the left-side navigation, click **Security**.
2. Click **Firewall**.
3. If you have virtual machines in various data centers, then in the top menu, click the corresponding data center.
4. Click **Actions**, and then click **New Rule**.

    - If you do not see **Actions**, then click **Create a Firewall Rule**.
5. In **Name**, enter a descriptive name.
6. In **Action**, select **Allow** to allow specified traffic to access your virtual machine or **Block** to block specified traffic.
7. Under **Service**, enter and select the name of the desired Service Group.
    - To learn how to create a Service Group, see Create a service group.
8. Under **Source**, enter and select the name of the desired IP Group.
    - To learn how to create an IP Group, see Create an IP group.
9. Under **Destinations**, in the field, enter and select the name of the desired IP Group.
10. Click **Save Rule**.

After you create a rule, Armor recommends that you place the rule in the correct order.

To reorder a rule:

1. Under Rule, in the numbered fields, enter a number to move the rule to a different position.
    - If you have more than 25 rules, the additional rules will be placed in a secondary section within the **Firewall**screen. To reorder and move these additional rules into a higher position, enter a number under the **Order**column, and then press **Enter** on your keyboard.
2. In the top menu that appears, click **Save**.

If you are not familiar with ordering rules, contact Armor Support to help you properly order your firewall rules. It is extremely important to order rules in order to receive desired traffic.

To learn how to send a support ticket, see Support Tickets.

To disable a rule:

1. Locate and hover over the desired rule.
2. Click the vertical ellipses.
3. Click **Disable Rule**.
4. Click **Disable Rule** again.
5. In the top menu that appears, click **Save**.

To learn more about firewall rules, see Firewall Rules.

Based on your upgraded virtual machine, update your newly created virtual machine with the same add-on features.

Review Armor Marketplace document to view a list of available add-on products.

In a later step, you will power off your upgraded virtual machine. As a result, you must remove any add-on features from you upgraded virtual machine.

Contact Armor Support via a support ticket to update your IP addresses.

Internally, Armor Support will release the IP addresses assigned to your upgraded virtual machine. Then, these IP addresses will be reserved for your account so that you can add these IP addresses to your new virtual machine.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure.**
2. Click **IP Addresses**.
3. If you have virtual machines in various data centers, then in the top menu, click the corresponding data center.
4. Click **Public**.
5. Click the plus (+) icon.
6. Review the information under **Environment** and **Quantity**, and then click **Add IP Addresses**.
7. Locate and hover over the newly created public IP address.
8. Click the vertical ellipses.
9. Click **Assign to VM**.
10. In **Virtual Machine**, select the desired virtual machine.
11. In **IP Address**, select an available private IP address.
12. Click **Create NAT**.
    - This action may take a few minutes to complete.

To learn more about IP addresses, see IP Address.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Locate and select the desired virtual machine.
4. Next to **Instance State**, click the vertical ellipses.
5. Select Power Off, and then confirm.

There are two ways to delete a virtual machine. You can delete a virtual machine immediately or at the end of your billing cycle.

You can only delete virtual machines that are offline (**Power Off**).

If you delete a virtual machine before the end of the billing cycle, you will still be charged for the full amount; however, in the next invoice, you will receive a credit to offset the cost.

Additionally, any add-on products or add-on subscriptions associated with the deleted virtual machine must be canceled separately.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Power Off**.
6. Click **Power Off** again.
7. Hover over the virtual machine, and then click the vertical ellipses.
8. Click **Delete**.
9. Click **Delete VM**.

Was this helpful?

Your Rating: ☆☆☆☆☆ Results: ★★★★★ 1 rates