

How to Deploy the Barracuda Email Security Gateway in the New Microsoft Azure Management Portal

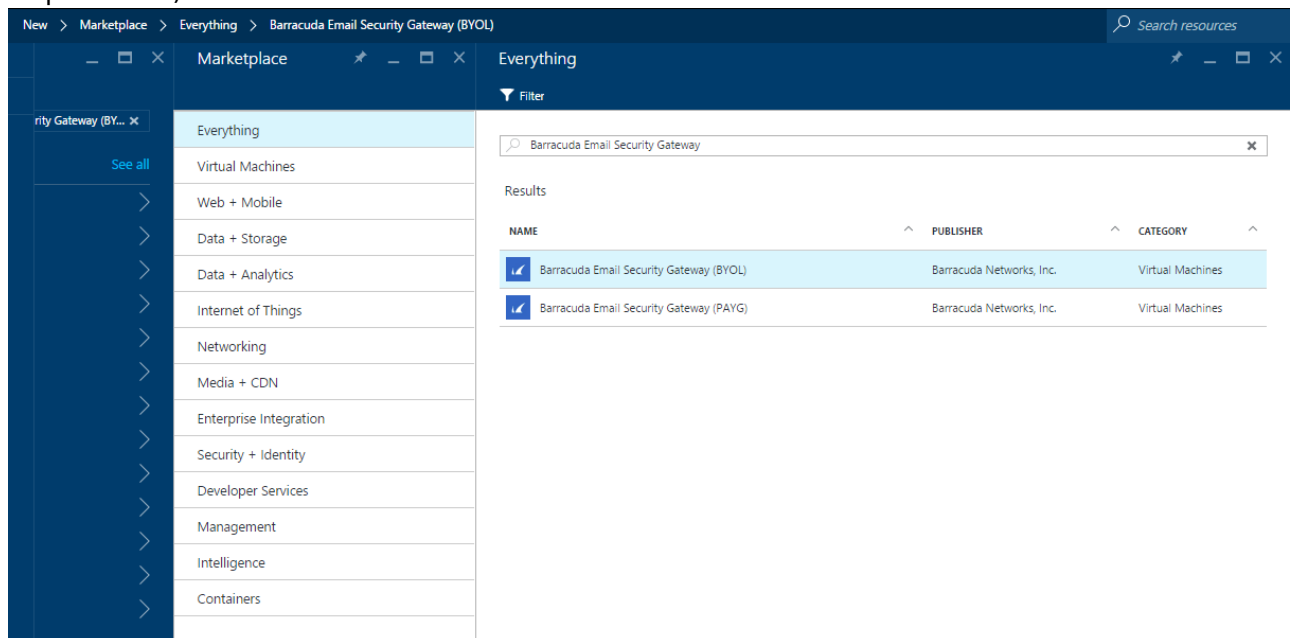
<https://campus.barracuda.com/doc/53248156/>

This guide walks you through the steps to deploy and provision the Barracuda Email Security Gateway on Microsoft Azure using either the Azure Resource Manager Model or the Classic Model.

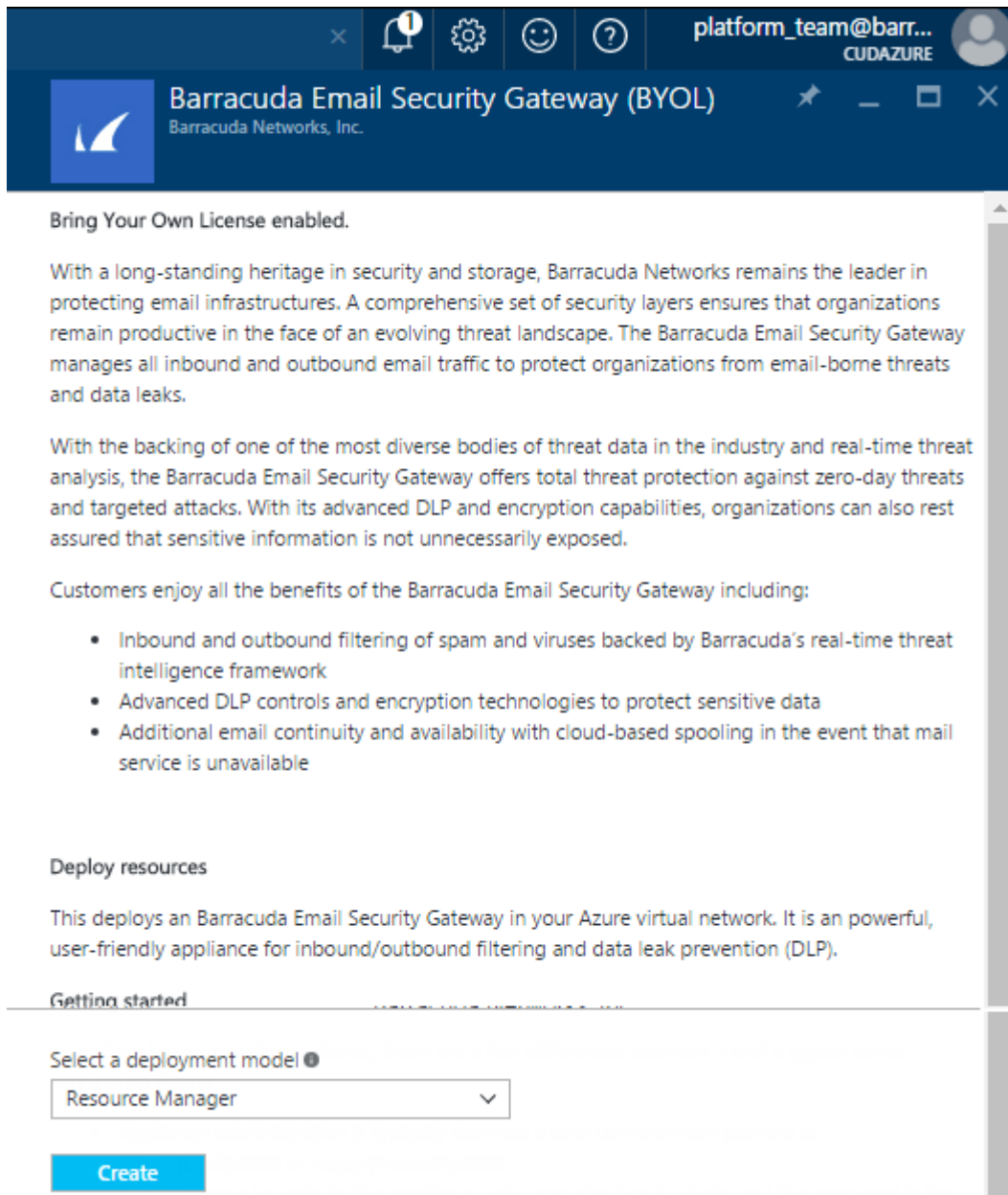
Deploying and Provisioning the Barracuda Email Security Gateway Using the Azure Resource Manager Model

Perform the following steps to deploy and provision the Barracuda Email Security Gateway using Resource Manager in the new Microsoft Azure portal:

1. Log into the [Microsoft Azure Management Portal](#).
2. Click **Marketplace** at the bottom of the screen.
3. In the **Everything** page, enter *Barracuda Email Security Gateway* in the text field.
4. In the search results, select Barracuda Email Security Gateway (**BYOL** or **PAYG** as per your requirement).



5. In the **Bring Your Own License enabled/Free Trial enabled** page:
 1. Read the product overview.
 2. Select **Resource Manager** as a deployment model from the **Select a deployment model** drop-down list.
 3. Click **Create**.



Bring Your Own License enabled.

With a long-standing heritage in security and storage, Barracuda Networks remains the leader in protecting email infrastructures. A comprehensive set of security layers ensures that organizations remain productive in the face of an evolving threat landscape. The Barracuda Email Security Gateway manages all inbound and outbound email traffic to protect organizations from email-borne threats and data leaks.

With the backing of one of the most diverse bodies of threat data in the industry and real-time threat analysis, the Barracuda Email Security Gateway offers total threat protection against zero-day threats and targeted attacks. With its advanced DLP and encryption capabilities, organizations can also rest assured that sensitive information is not unnecessarily exposed.


Customers enjoy all the benefits of the Barracuda Email Security Gateway including:


- Inbound and outbound filtering of spam and viruses backed by Barracuda's real-time threat intelligence framework
- Advanced DLP controls and encryption technologies to protect sensitive data
- Additional email continuity and availability with cloud-based spooling in the event that mail service is unavailable

Deploy resources

This deploys an Barracuda Email Security Gateway in your Azure virtual network. It is an powerful, user-friendly appliance for inbound/outbound filtering and data leak prevention (DLP).

Getting started

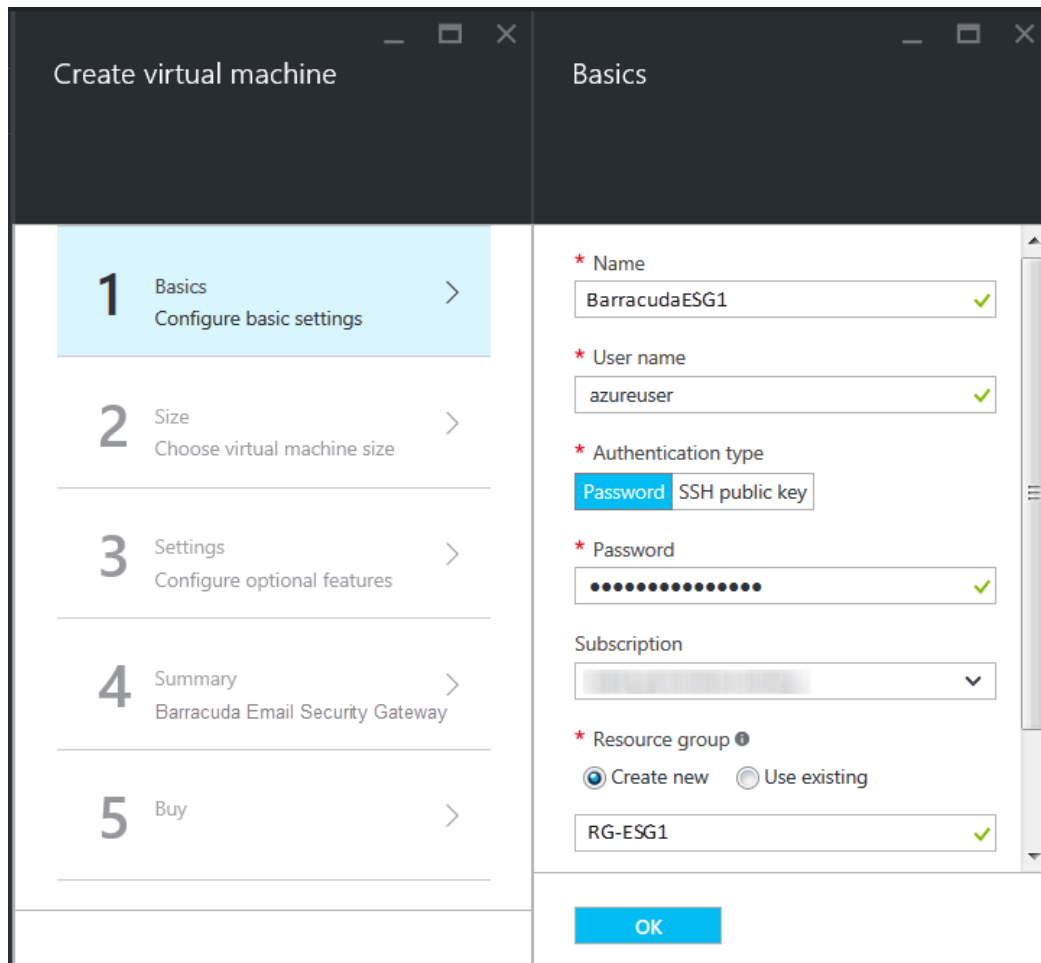
Select a deployment model 

Resource Manager 

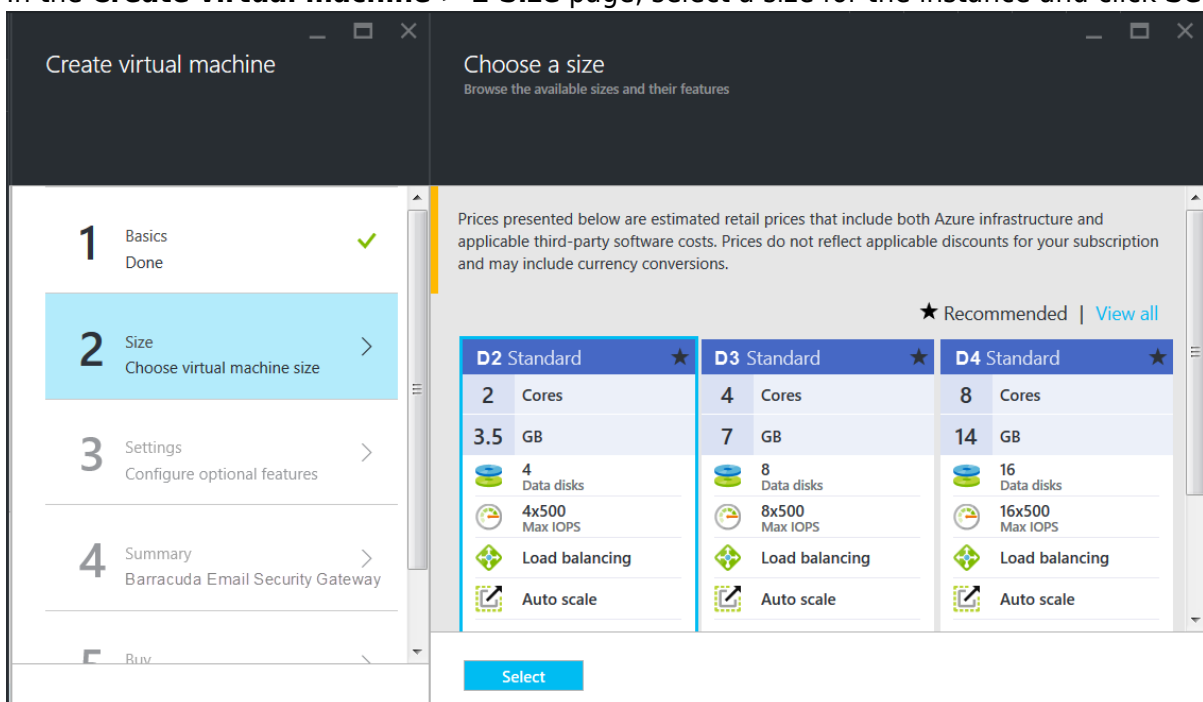
Create

6. In the **Create virtual machine > 1 Basics** page:

1. **Name:** Enter a name for the virtual machine.
2. **User name:** Enter a username. **Note:** This entry is not used by the Barracuda Email Security Gateway.
3. **Authentication Type:** Choose **Password** and enter a password for the authentication. Note that this will be your password to access the Barracuda Email Security Gateway web interface.
4. **Resource Group:** Create a new resource group or select a resource group from the existing **Resource group** list.
5. **Location:** Select a location for the resource group.
6. Click **OK**.

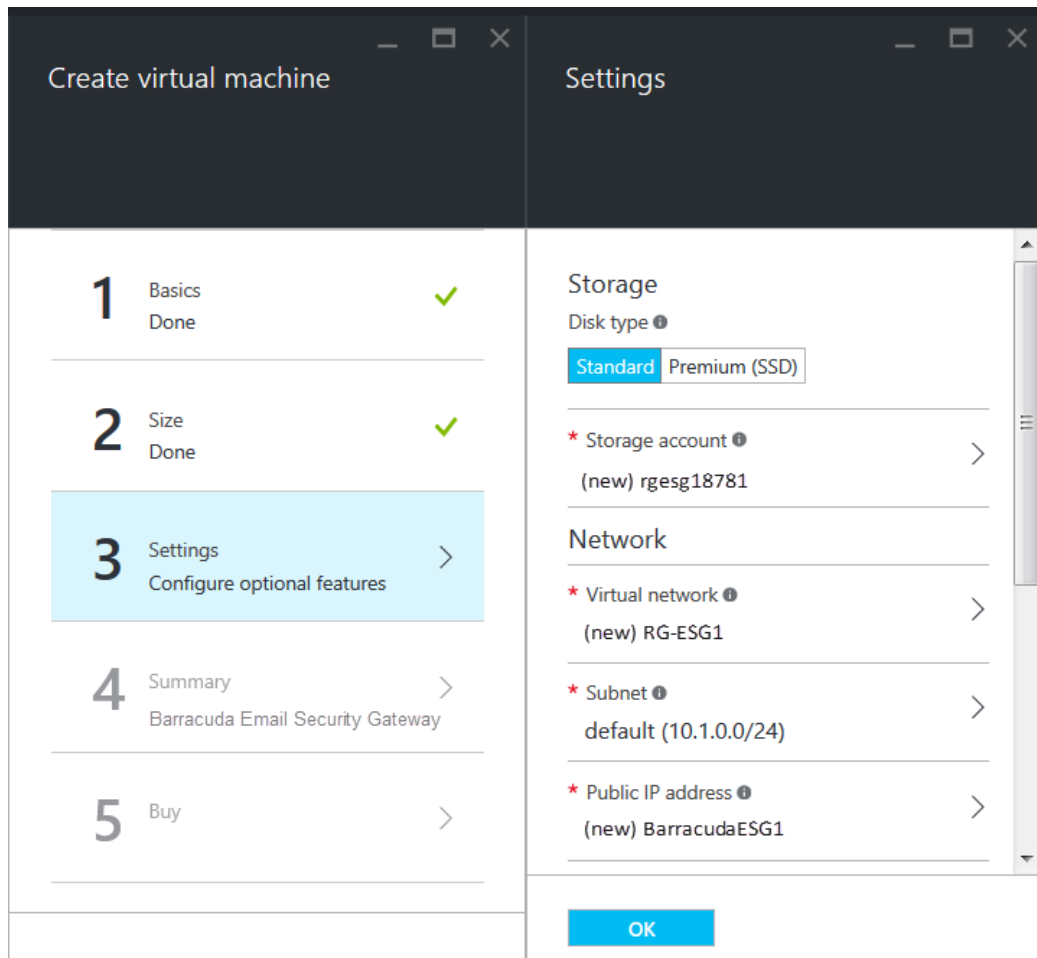


7. In the **Create virtual machine > 2 Size** page, select a size for the instance and click **Select**.

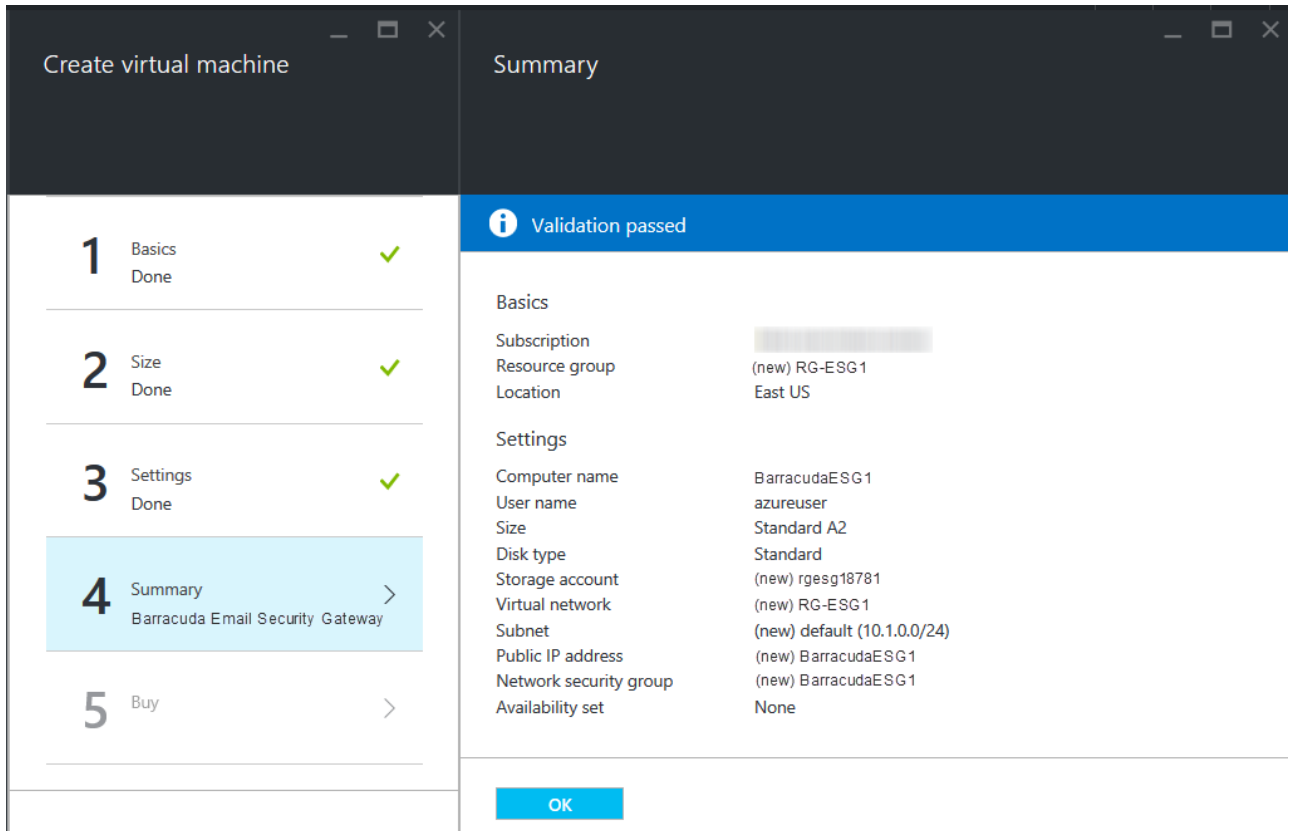


8. In the **Create virtual machine > 3 Settings** page:
 1. **Storage**

1. **Data type:** Select **Standard/Premium (SSD)** as per your requirement.
2. **Storage account:** Create a new storage account or select a storage account from the existing **Storage account** list.
2. **Network**
 1. **Virtual network:** Configure or select the network in which you want to deploy the Barracuda Email Security Gateway.
 2. **Subnet:** Configure or select the subnet in which you want to deploy the Barracuda Email Security Gateway.
 3. **Public IP address:** Configure or select the public IP address to the Barracuda Email Security Gateway.
 4. **Network security group:** By default, port 8000 (TCP), port 443 (TCP) and port 25 (TCP) will be opened as in your **Security Group**. Configure additional rules if required.
3. **Extensions**
 1. **Extensions:** Do not add any extension, as the Barracuda Email Security Gateway does not support extensions.
4. **Availability**
 1. **Availability set:** Create an availability set or select an availability set from the existing **Availability set** list. Note: If you intend to use this virtual machine in cluster, ensure all virtual machines in cluster is configured with same availability set.



9. In the **4 Summary** page, review the configuration settings and click **OK**.



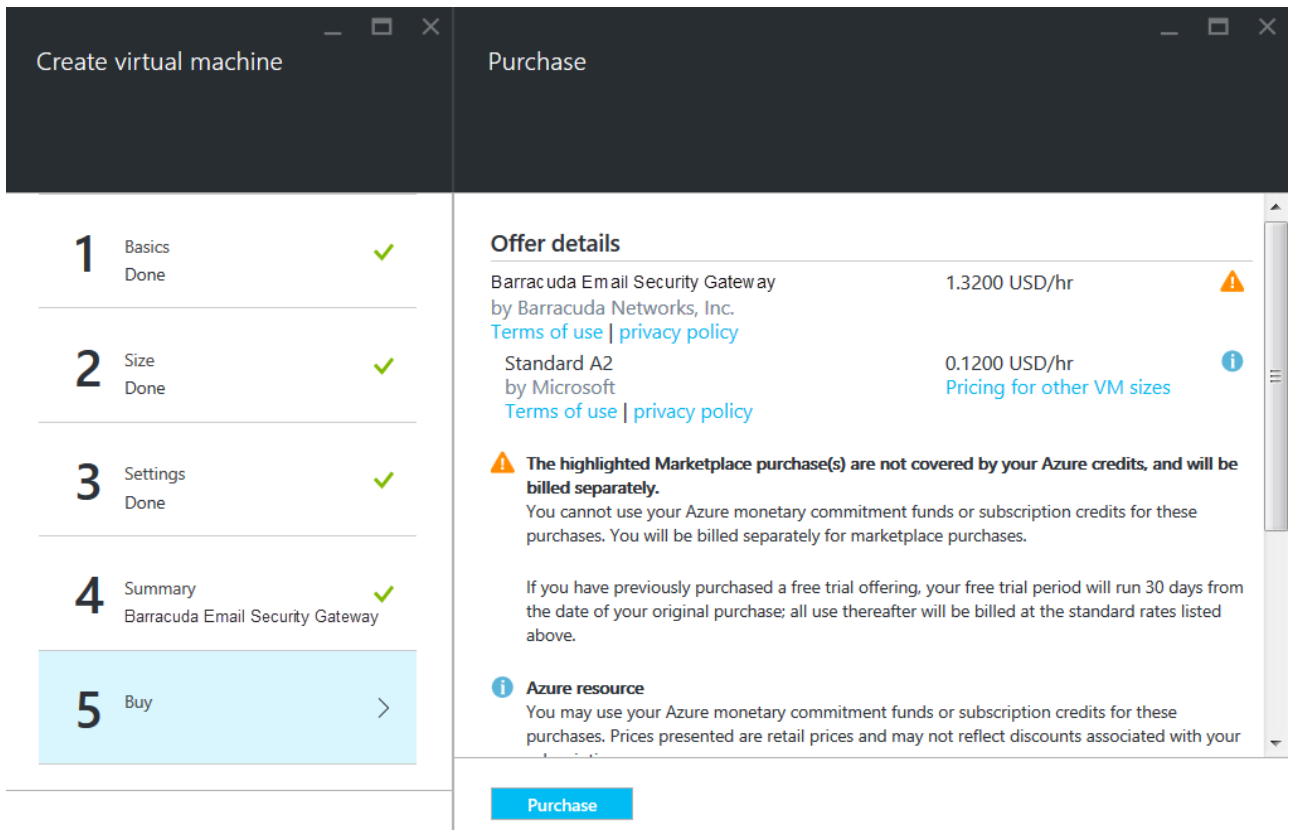
The screenshot shows the 'Create virtual machine' wizard in the Summary step. On the left, a progress bar shows five steps: 1 Basics Done, 2 Size Done, 3 Settings Done, 4 Summary (highlighted), and 5 Buy. The main area displays a 'Validation passed' message and a list of configuration details:

Basics	
Subscription	[Redacted]
Resource group	(new) RG-ESG1
Location	East US

Settings	
Computer name	BarracudaESG1
User name	azureuser
Size	Standard A2
Disk type	Standard
Storage account	(new) rgesg18781
Virtual network	(new) RG-ESG1
Subnet	(new) default (10.1.0.0/24)
Public IP address	(new) BarracudaESG1
Network security group	(new) BarracudaESG1
Availability set	None

An 'OK' button is located at the bottom of the configuration area.

10. In the **5 Buy** page, read the legal terms and click **Purchase** to complete the deployment.



The screenshot shows the 'Create virtual machine' wizard in the Purchase step. The progress bar on the left highlights step 5 Buy. The main area displays 'Offer details' for the selected VM:

Offer	Price	Notes
Barracuda Email Security Gateway by Barracuda Networks, Inc. Terms of use privacy policy	1.3200 USD/hr	Warning icon
Standard A2 by Microsoft Terms of use privacy policy	0.1200 USD/hr Pricing for other VM sizes	Info icon

Below the offer details, there is a warning message: **The highlighted Marketplace purchase(s) are not covered by your Azure credits, and will be billed separately.** It explains that Azure monetary commitment funds or subscription credits cannot be used for these purchases. A note also states that if a free trial was previously purchased, the trial period will run for 30 days from the original purchase date.

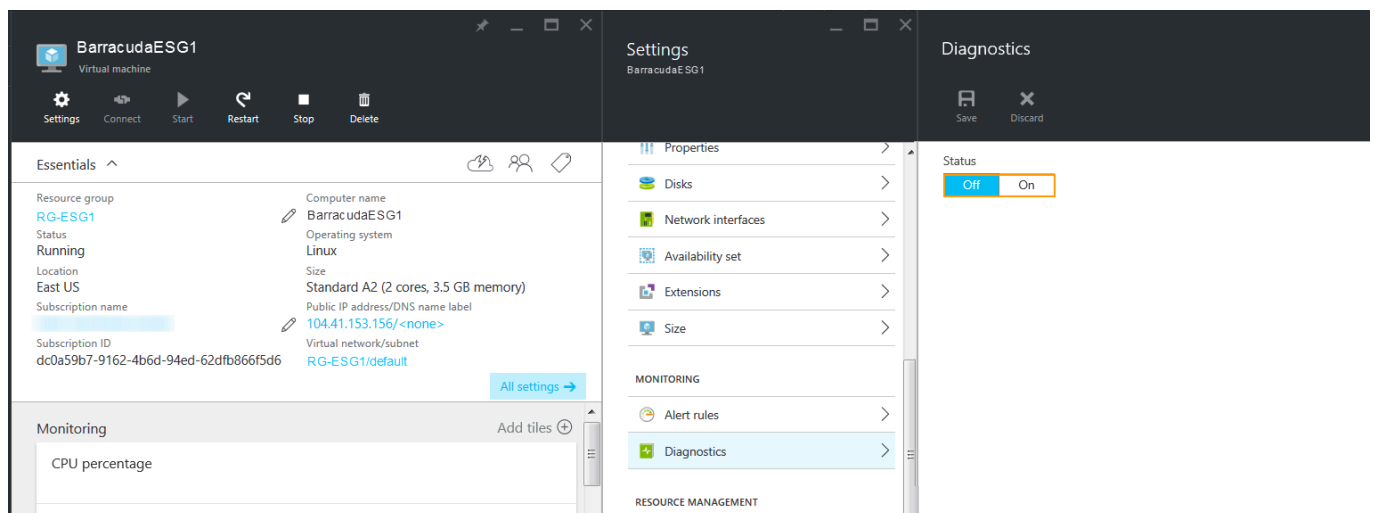
An 'Azure resource' info icon is present, with text stating that retail prices are shown and may not reflect discounts.

A 'Purchase' button is located at the bottom of the page.

After clicking **Purchase**, Microsoft Azure begins provisioning the Barracuda Email Security Gateway. You can check the status of the provisioned Barracuda Email Security Gateway from the [Microsoft Azure Portal](#). Allow a few minutes before taking any further actions in the Portal. During this time, the Microsoft Azure Linux Agent and Barracuda Email Security Gateway image boots up.

Make sure you do not restart the Barracuda Email Security Gateway while it is provisioning.

Monitoring is not supported by the Barracuda virtual machines/instances. Enabling **Monitoring Diagnostics** can cause the deployment to fail or timeout. It is recommended to contact [Barracuda Networks Technical Support](#) before enabling **Monitoring Diagnostics**.

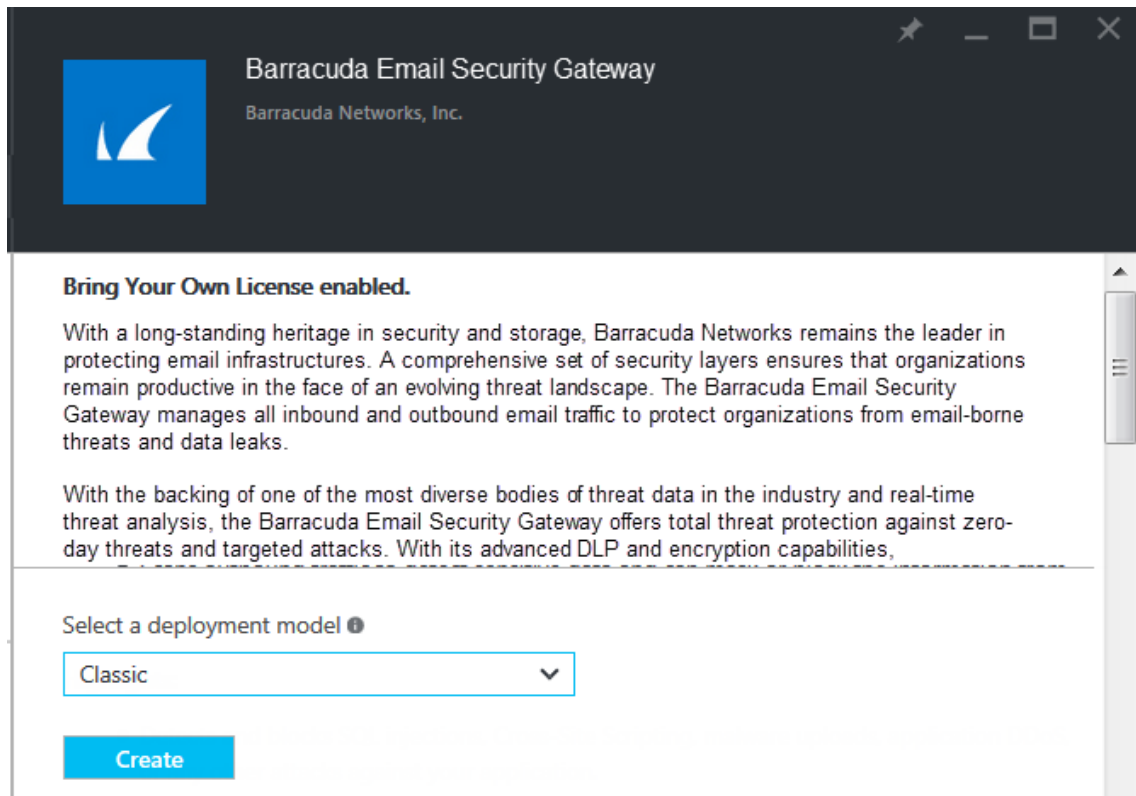


Deploying and Provisioning the Barracuda Email Security Gateway Using the Classic Model

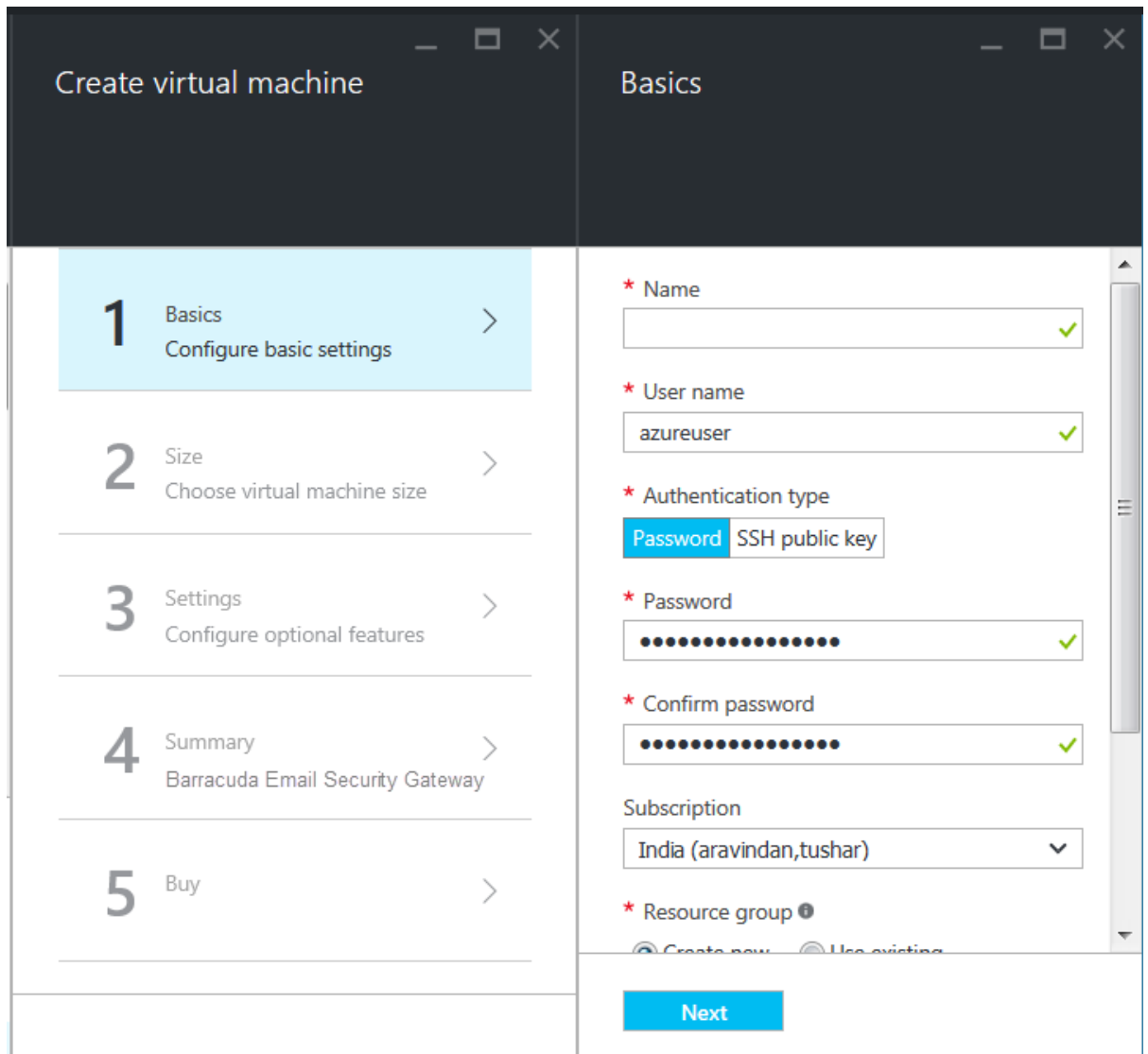
Perform the following steps to deploy and provision the Barracuda Email Security Gateway using the classic deployment model in the new Microsoft Azure portal:

1. Log into the [Microsoft Azure Management Portal](#).
2. Click **Marketplace** at the bottom of the screen.
3. In the **Everything** page, enter *Barracuda Email Security Gateway* in the text field. In the search results, select Barracuda Email Security Gateway (**BYOL** or **PAYG** as per your requirement).
4. In the **Bring Your Own License enabled/Free Trial enabled** page:
 1. Read the product overview.
 2. Select **Classic** as a deployment model from the **Select a deployment model** drop-down

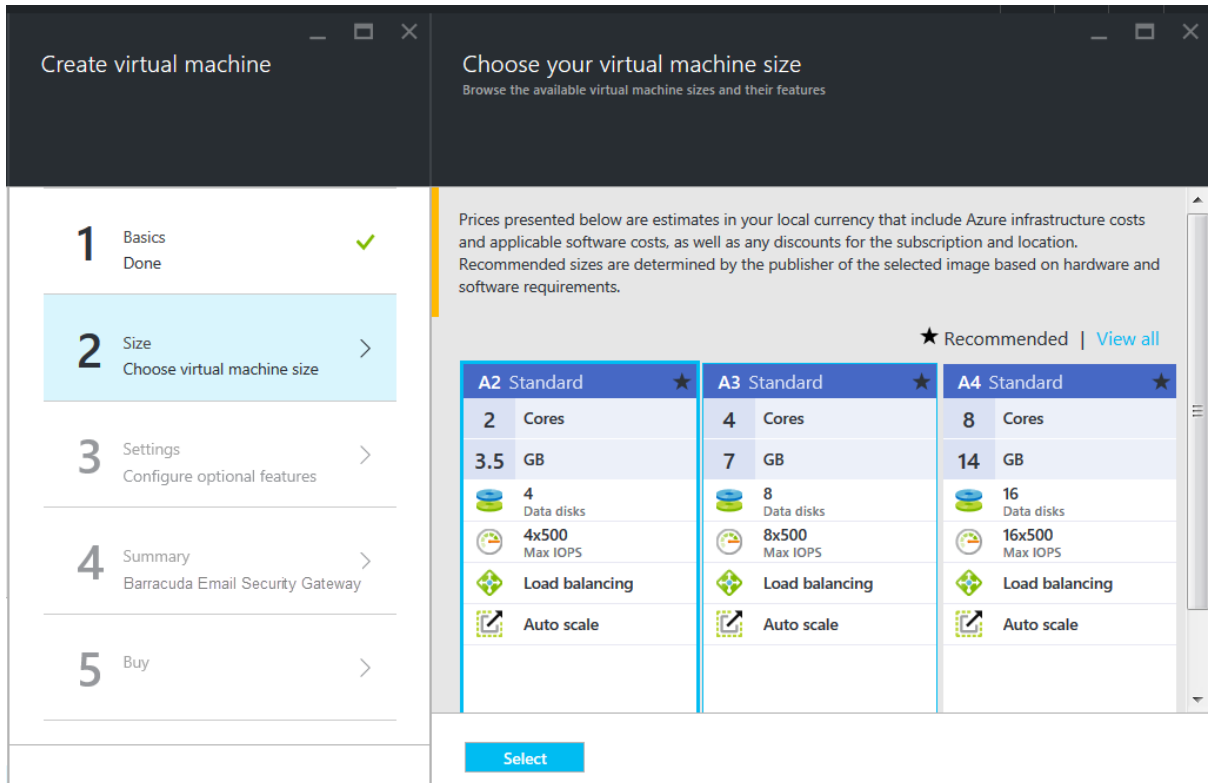
- list.
3. Click **Create**.



5. In the **Create virtual machine > 1 Basics** page:
 1. **Name:** Enter a name for the virtual machine.
 2. **User name:** Enter a username. **Note:** This entry is not used by the Barracuda Email Security Gateway.
 3. **Authentication type:** Choose **Password** and enter a password for the authentication. Note that this will be your password to access the Barracuda Email Security Gateway web interface.
 4. **Confirm password:** Re-enter the password to confirm.
 5. **Subscription:** Select the subscription from the drop-down list.
 6. **Resource group:** Create a new resource group or select a resource group from the existing **Resource group** list.
 7. **Location:** Select a location for the resource group.



6. In the **Create virtual machine > 2 Size** page:
 1. Select a size for the instance and click **Select**.



Create virtual machine

Choose your virtual machine size
Browse the available virtual machine sizes and their features

Prices presented below are estimates in your local currency that include Azure infrastructure costs and applicable software costs, as well as any discounts for the subscription and location. Recommended sizes are determined by the publisher of the selected image based on hardware and software requirements.

★ Recommended | [View all](#)

A2 Standard ★		A3 Standard ★		A4 Standard ★	
2	Cores	4	Cores	8	Cores
3.5	GB	7	GB	14	GB
4	Data disks	8	Data disks	16	Data disks
4x500	Max IOPS	8x500	Max IOPS	16x500	Max IOPS
+	Load balancing	+	Load balancing	+	Load balancing
+	Auto scale	+	Auto scale	+	Auto scale

Select

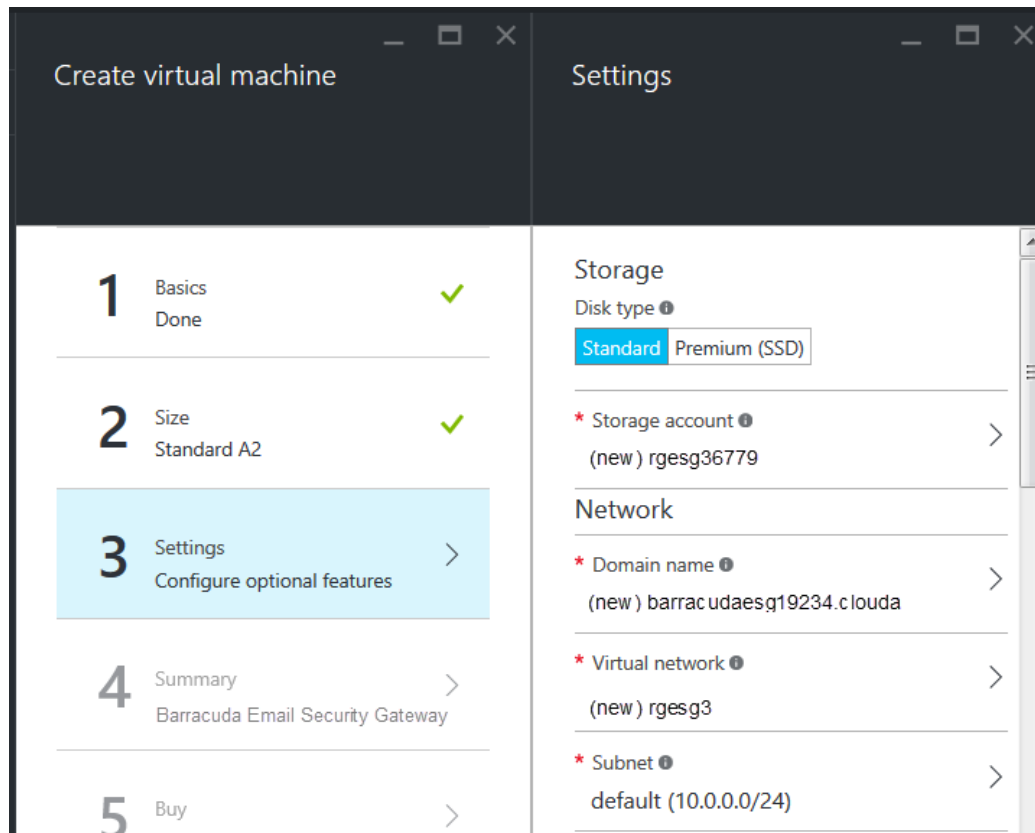
7. In the **Create virtual machine > 3 Settings** page:

8. **Storage**

1. **Data type:** Select **Standard/Premium (SSD)** as per your requirement.
2. **Storage account:** Create a new storage account or select a storage account from the existing Storage account list.

9. **Network**

1. **Domain name:** Enter the domain name for the Barracuda Email Security Gateway VM.
2. **Virtual network:** Configure or select the network in which you want to deploy the Barracuda Email Security Gateway.
3. **Subnet:** Configure or select the subnet in which you want to deploy the Barracuda Email Security Gateway.



4. **Private IP address:** Select **Dynamic/Static**.

1. **Dynamic** to auto assign the private IP address to the Barracuda Email Security Gateway.
2. **Static** to configure the static private IP address to the Barracuda Email Security Gateway.

5. **Virtual IP address:** Select **Assign a new reserved IP address/Dynamic IP address**.

The instance can be accessed from outside the virtual network using this virtual IP address. Ensure that at least one endpoint is configured.

1. **Assign a new reserved IP address:** Specify a name for the virtual IP address assigned by the Microsoft Azure.
2. **Dynamic IP address:** Select to auto assign the virtual IP address for the Barracuda Email Security Gateway.

6. **Endpoints:** Add the port 8000 (TCP), port 443 (TCP) and port 25 (TCP) as your endpoints.

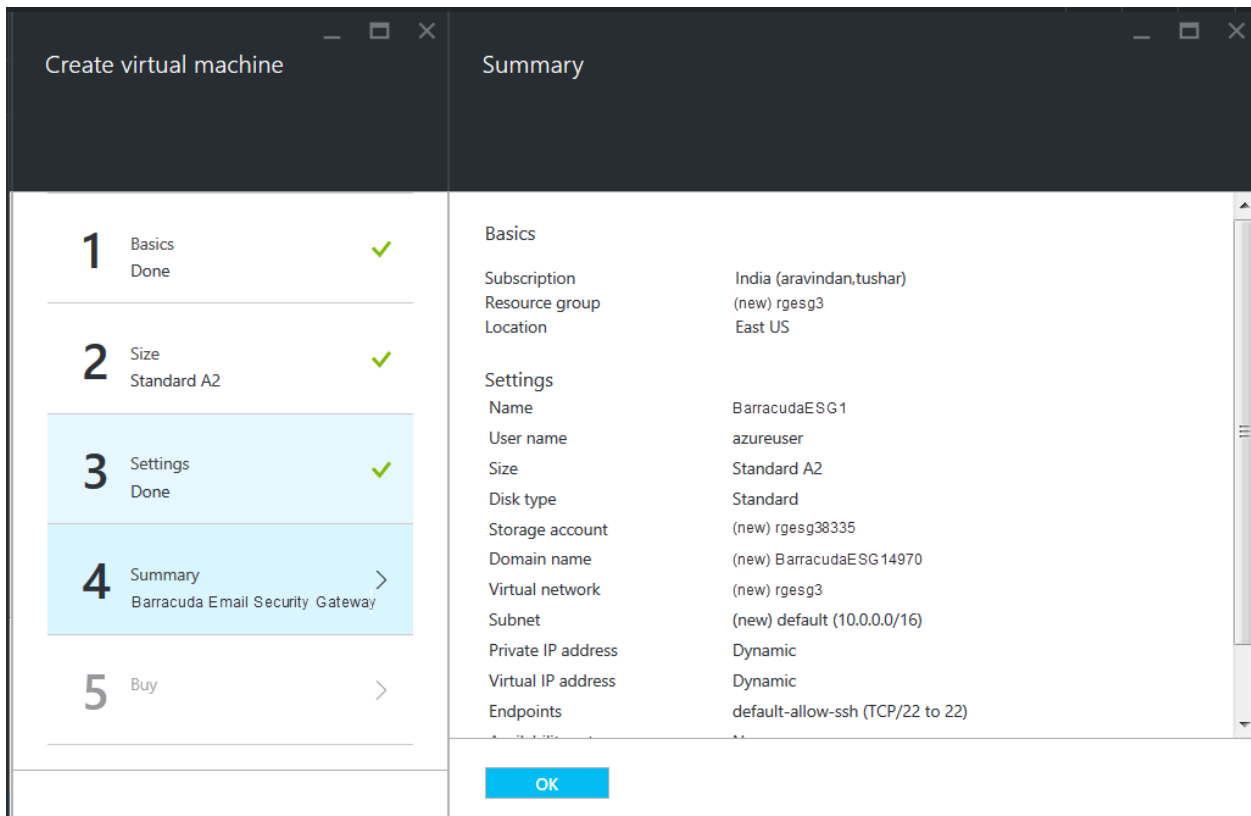
10. **Extensions**

1. **Extensions:** Do not add any extension, as the Barracuda Email Security Gateway does not support extensions.

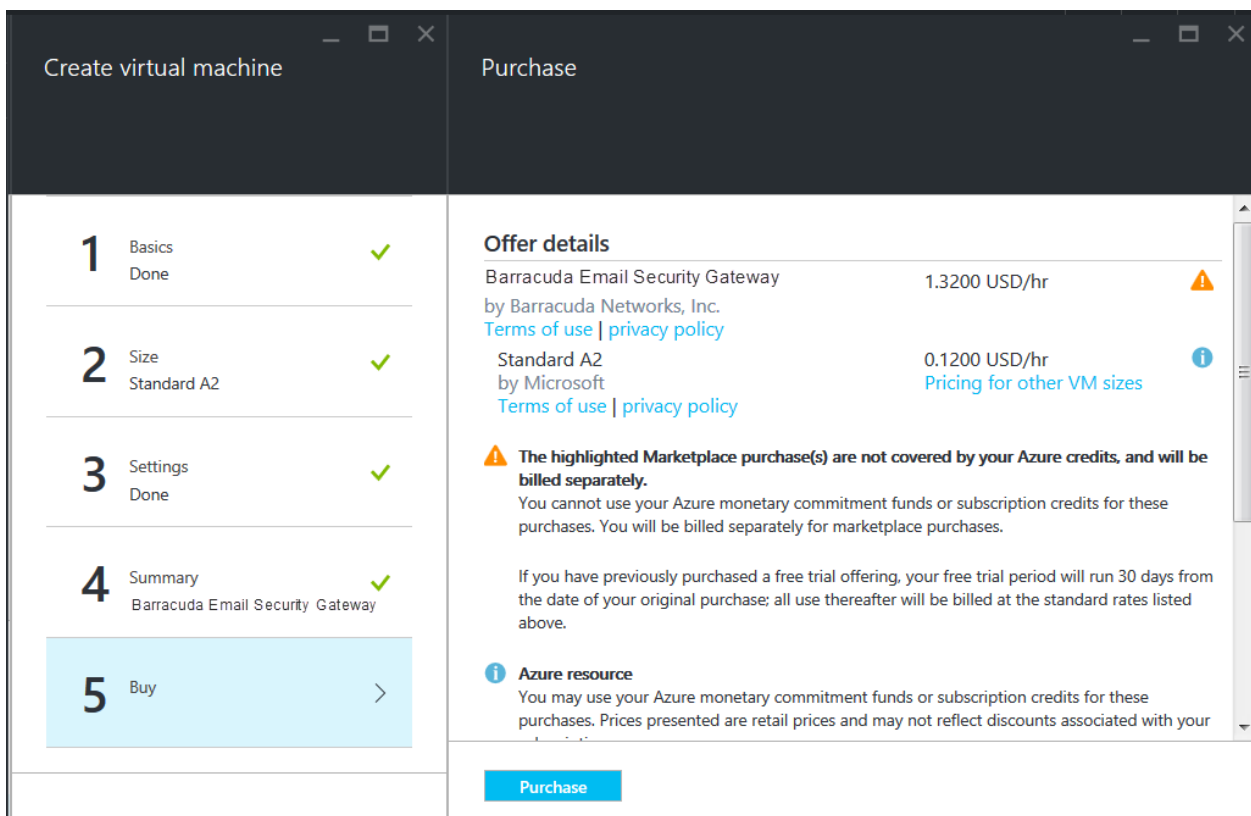
11. **Availability**

1. **Availability set:** Create an availability set or select an availability set from the existing Availability set list. Note: If you intend to use this virtual machine in cluster, ensure all virtual machines in cluster is configured with same availability set.

12. In the **4 Summary** page, review the configuration settings and click **OK**.



13. In the **5 Buy** page, read the legal terms and click **Purchase** to complete the deployment.



After clicking **Create**, Microsoft Azure begins provisioning the Barracuda Email Security Gateway. You can check the status of the provisioned Barracuda Email Security Gateway from the [Microsoft Azure Portal](#). Allow a few minutes before taking any further actions in the Portal. During this time, the Microsoft Azure Linux Agent and Barracuda Email Security Gateway image boots up.

Make sure you do not restart the Barracuda Email Security Gateway while it is provisioning.

Monitoring is not supported by Barracuda virtual machines/instances. Enabling **Monitoring Diagnostics** can cause the deployment to fail or time out. Barracuda recommends contacting [Barracuda Networks Technical Support](#) before enabling **Monitoring Diagnostics**.

Next Step

Continue with the [Barracuda Email Security Gateway Quick Start Guide on Microsoft Azure](#) for licensing and initial configuration of your virtual machine

Figures

1. MarketPlaceEverything.png
2. ResourceManager.png
3. Basic_Settings.png
4. ChooseSize.png
5. Settings.png
6. Summary.png
7. Purchase.png
8. Monitoring.png
9. Classic Model.png
10. Classic Portal Basic Settings.png
11. Classic_Choose_VM_Size.png
12. Classic_Settings.png
13. Classic_Summary.png
14. Classic_Purchase.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.