Net at Work
Building IT-Excellence.

NoSpamProxy

Installation Guide for Operation in Microsoft Azure

- Protection
- Encryption
- Large Files

Imprint

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn

Trademarks

1 October 2019

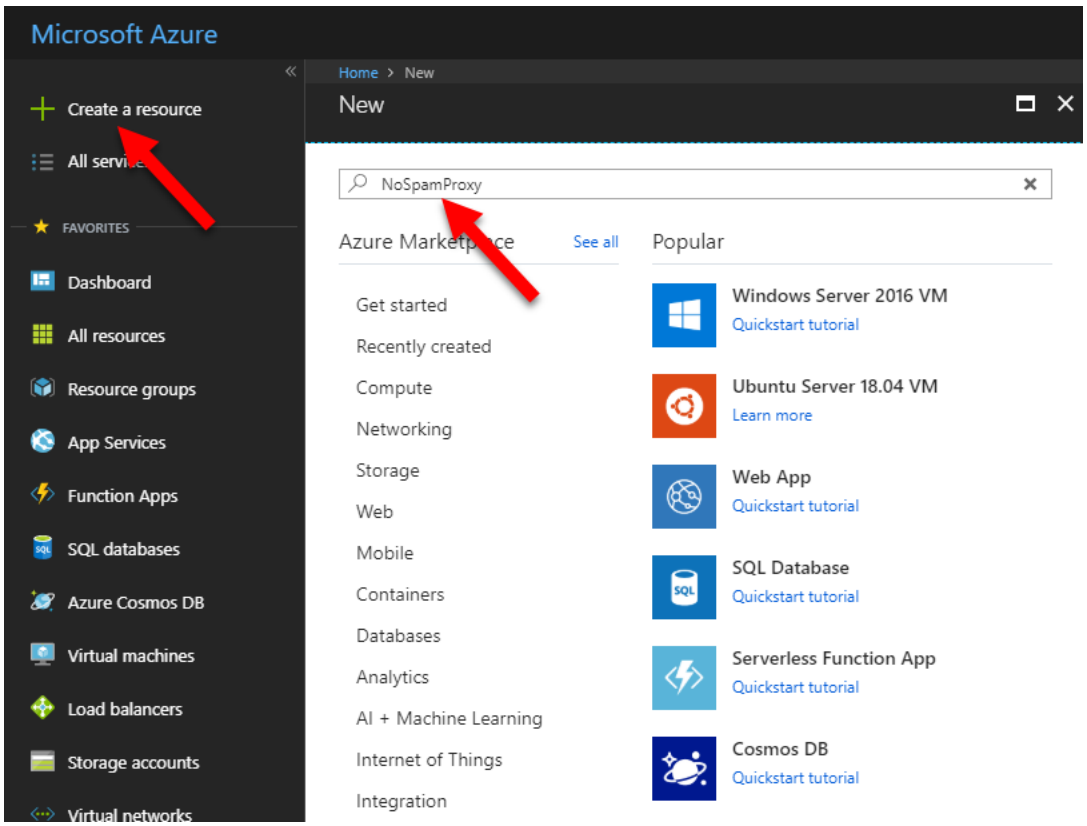
Contents

1. Creating a NoSpamProxy instance in Microsoft Azure

To use NoSpamProxy in Microsoft Azure, a NoSpamProxy instance must be installed on a virtual computer.

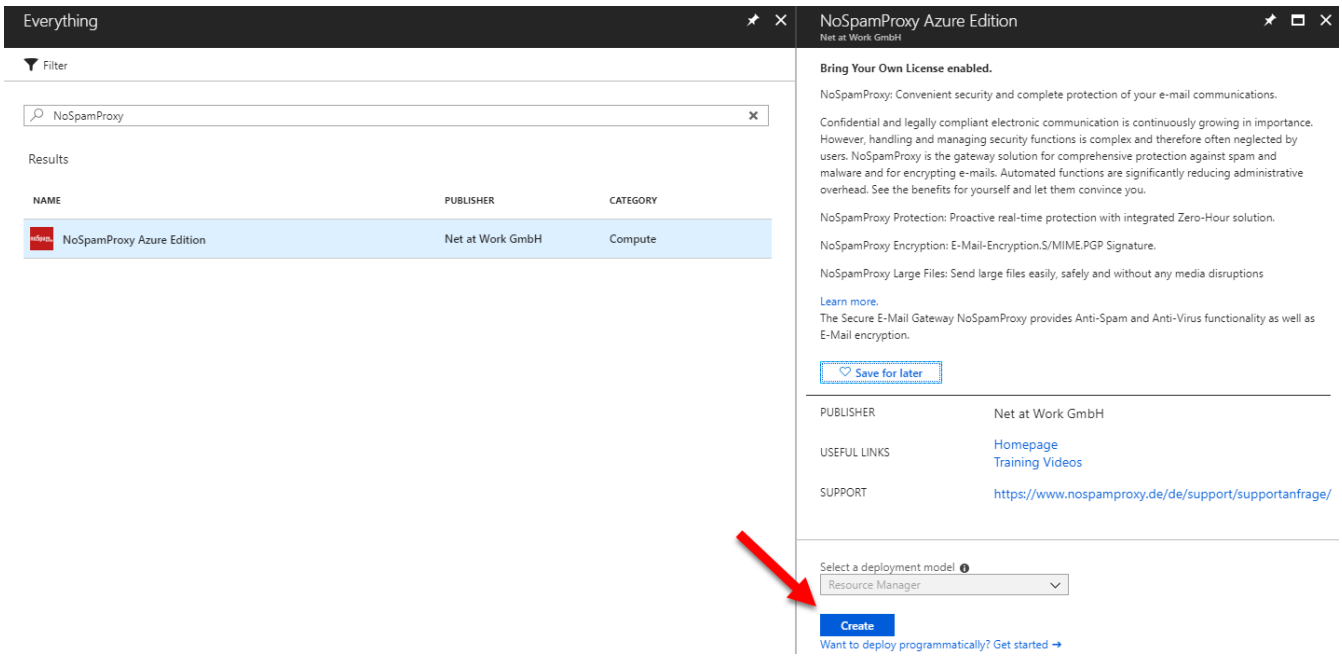
First, sign in to your Azure Tenant at https://portal.azure.com/.

Click **Create a resource** and search for **NoSpamProxy**.



Picture 1: The Azure Marketplace wizard

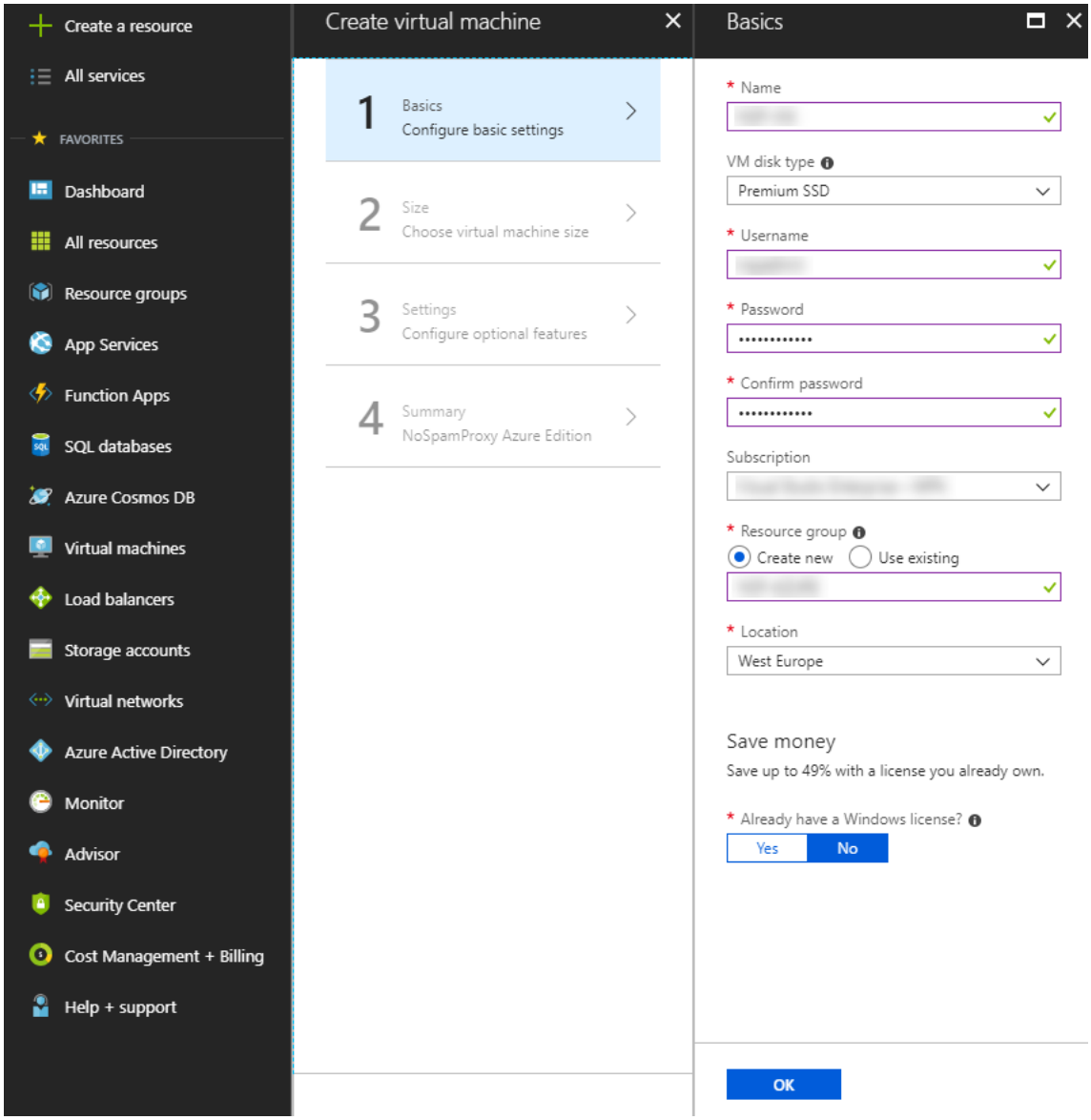
Select **NoSpamProxy Azure Edition** and click **Create**.



Picture 2: Creating a new resource in Azure

Enter the requested basic information on the virtual computer (name, disk type, user name and password) and add the following details:

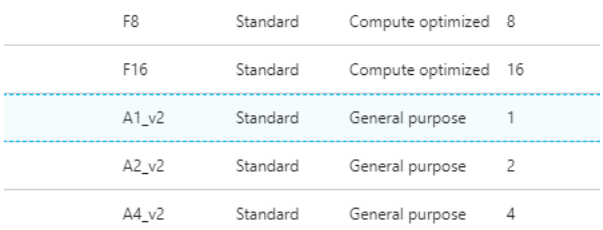
- Subscription: Here, your Azure subscription will be displayed. If you own more than one subscription and would like to use another subscription for NoSpamProxy in Microsoft Azure, select the respective subscription from the drop-down menu.
- Resource group: We recommend organising services used on your Azure tenant in resource groups. If you have already set up a resource group for NoSpamProxy, select **Use existing** and select the respective resource group from the drop-down menu. If you have not yet created a resource group, select **Create new** and enter a name for the new resource group.
- Location: Enter a location for the data center which hosts NoSpamProxy in Microsoft Azure.



Picture 3: Basic information on the virtual computer

Click **OK**.

Select the size of your virtual computer. To view all available sizes, click **View all**. The smallest available size is B1s. For processing up to 100 emails per minute this is sufficient, albeit with a reduction in performance of the management console. We recommend starting with a A1_V2 size. It is possible to upgrade to a A2_V2 at any time during operation.



F8	Standard	Compute optimized	8
F16	Standard	Compute optimized	16
A1_v2	Standard	General purpose	1
A2_v2	Standard	General purpose	2
A4_v2	Standard	General purpose	4

Picture 4: Choosing the size of the virtual computer

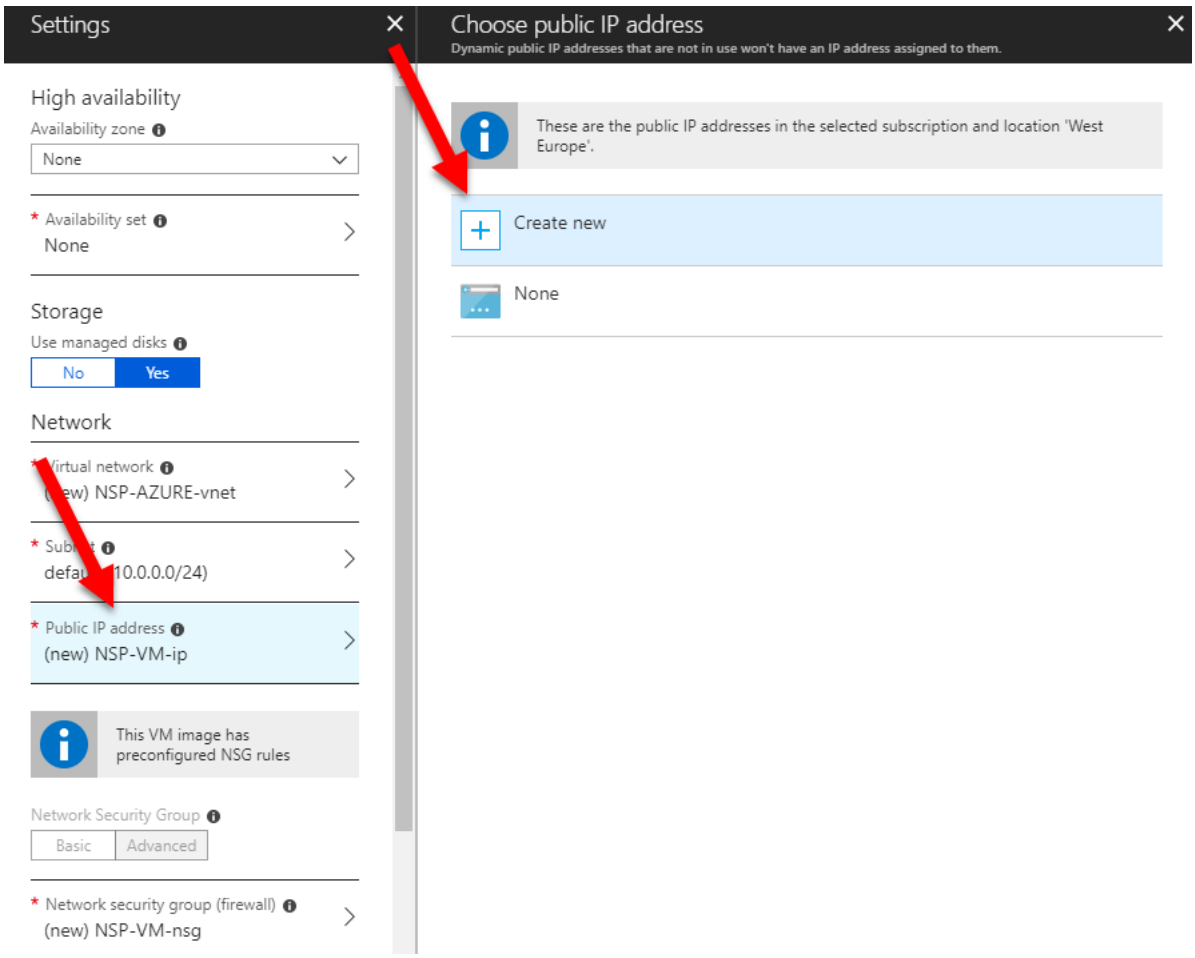
After you have made your selection, click **Create**.

You can now configure optional settings.

We recommend setting up a static public IP address:

If you have already set up a static public IP address on your Azure tenant which you want to use for NoSpamProxy in Microsoft Azure, select the respective address and click **OK**. Keep in mind that only public IP addresses are displayed which are included in the resource group selected earlier.

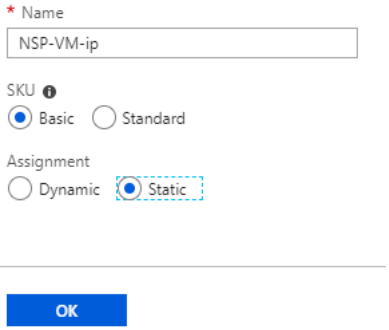
If you have not yet created a static public IP address, click **Public IP address** and then **Create new**.



Picture 5: Creating a new static public IP address

Enter a name for the IP address, then select **Static**.

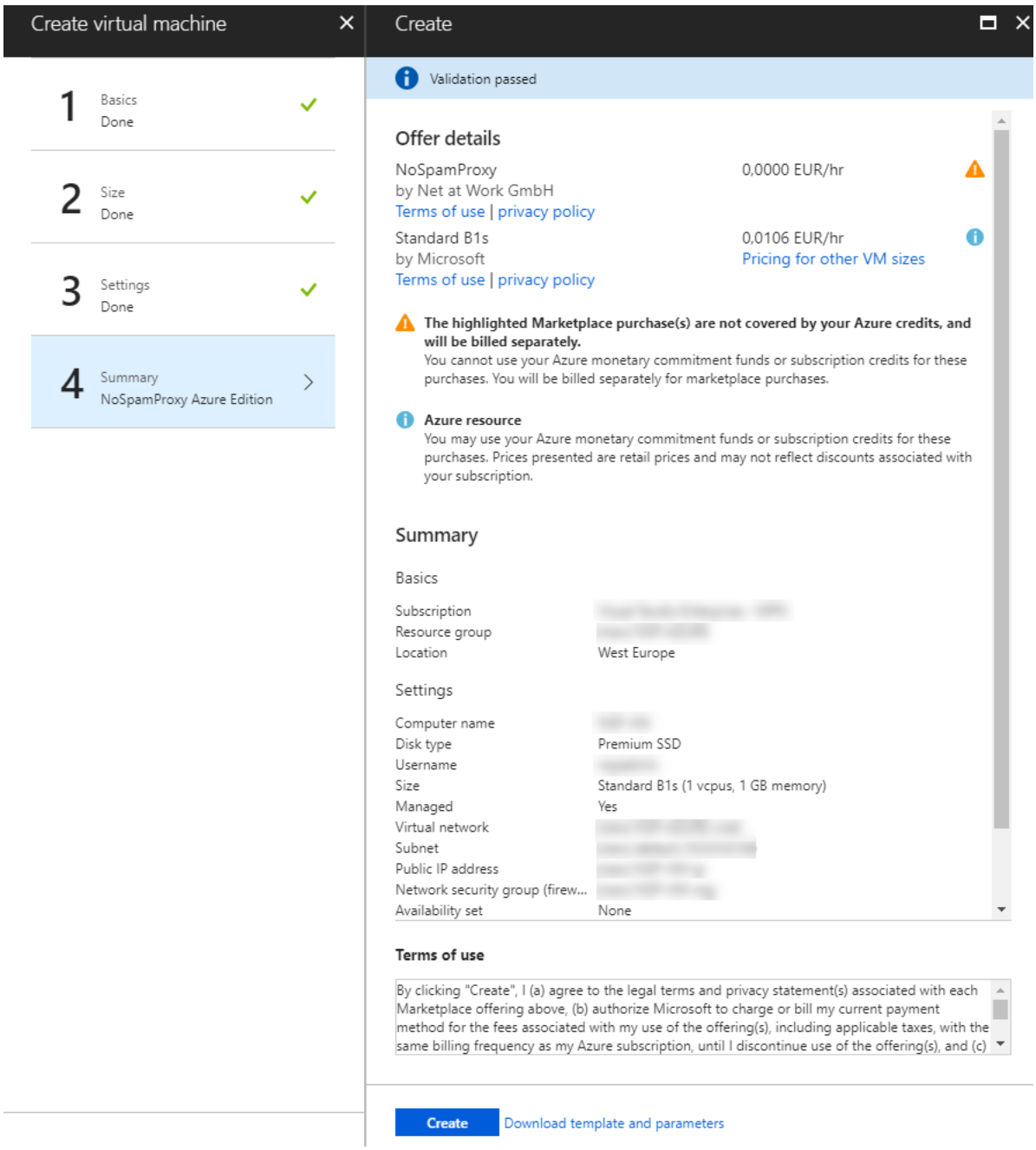
Click **OK**.



Picture 6: Setting up the public IP address as static

Check the accuracy of the basic information and click **OK**. A summary of the settings made is displayed.

Click **Create** to confirm that you agree to the purchase of the virtual computer. The virtual computer will be deployed.



Picture 7: Agreeing to the purchase of the virtual computer

2. Configuring Microsoft Azure

After installing NoSpamProxy in Microsoft Azure, additional configuration steps are necessary for two areas in Microsoft Azure.

Configuring the reverse DNS entry for the NoSpamProxy server

To configure the reverse DNS entry, follow the instructions in the section Configure reverse DNS for services hosted in Azure of the Microsoft Azure documentation.

If SPF entries (Sender Policy Framework entries) exist, you must enter the IP address of the NoSpamProxy server as a permitted sender. Alternatively, you can also enter the domain name proxy.nospamproxy.de.

Activating the Azure proxy server for NoSpamProxy

Since Microsoft Azure does not allow applications to send emails via port 25, NoSpamProxy cannot use this port. In addition, email addresses are often blacklisted by Microsoft Azure. For these reasons, we provide our customers with a free smart host that eliminates these problems.

You must activate this smart host via the "Gateway Role.config" file. To do this, proceed as follows:

Stop the gateway role.

Go to `C:\ProgramData\Net at Work Mail Gateway\Configuration` and open the file **Gateway Role.config**.

Search for the tag `<netatwork.nospamproxy.proxyconfiguration>`. Add the tag `<smtpServicePointConfiguration isProxyTunnelEnabled="true" />` anywhere within the above tag.

The tag `<smtpServicePointConfiguration>` may already exist. In this case, you only have to add the attribute `isProxyTunnelEnabled="true"`.

Start the gateway role.

3. Support

For questions about NoSpamProxy or the installation process in Microsoft Azure, please contact our support team:

- by phone at +49 5251304-636
- via email at support@nospamproxy.de
- on the NoSpamProxy website