How-to Guide: Tenable Core Web Application Scanner for Microsoft Azure

Last Updated: May 16, 2018

Table of Contents

Introduction

Tenable is the first and only solution to offer security visibility, Azure cloud environment auditing, system hardening, and continuous monitoring so you can regain visibility, reduce attack surface, and detect malware across your Microsoft Azure deployments. This document describes how to deploy the following Tenable solutions to help ensure a secure and compliant Microsoft Azure cloud environment:

- Auditing Microsoft Azure Cloud Environment
- Tenable Core Web Application Scanner BYOL (Bring Your Own License) Scanner

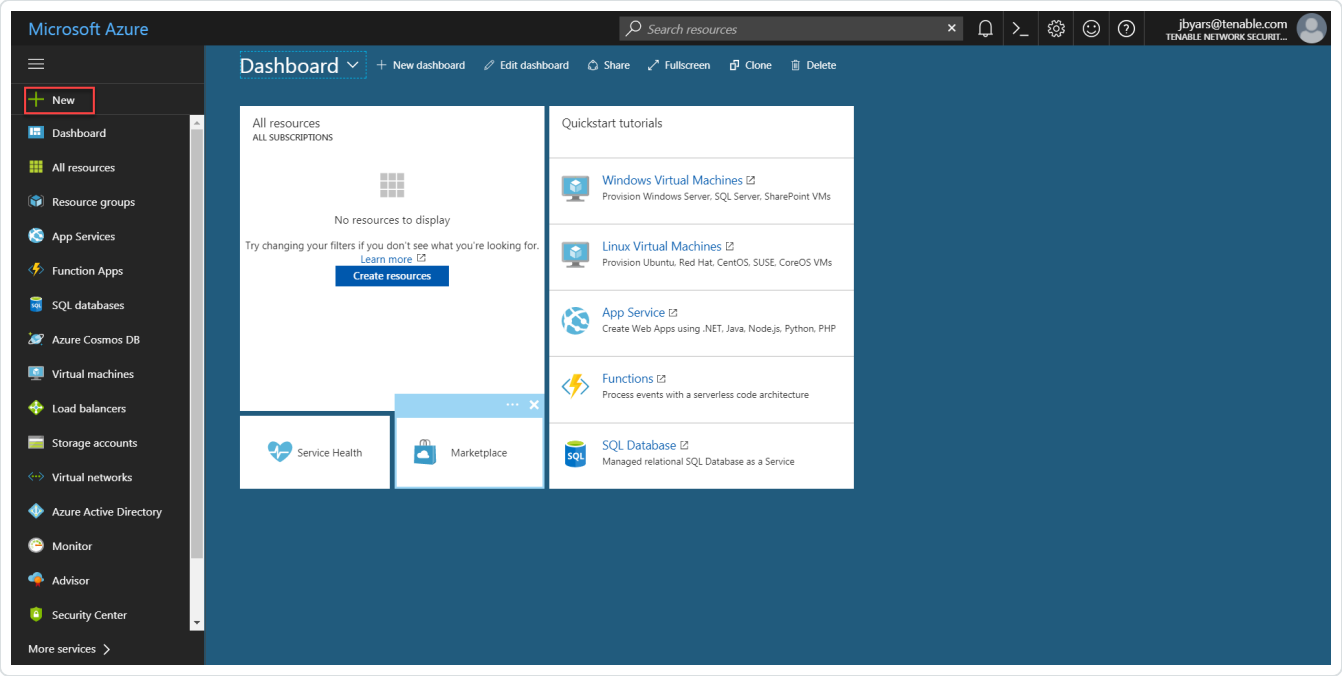
It is as important to run these assessments in Microsoft Azure as it is in any other IT environment.

Please email any comments and suggestions to support@tenable.com.

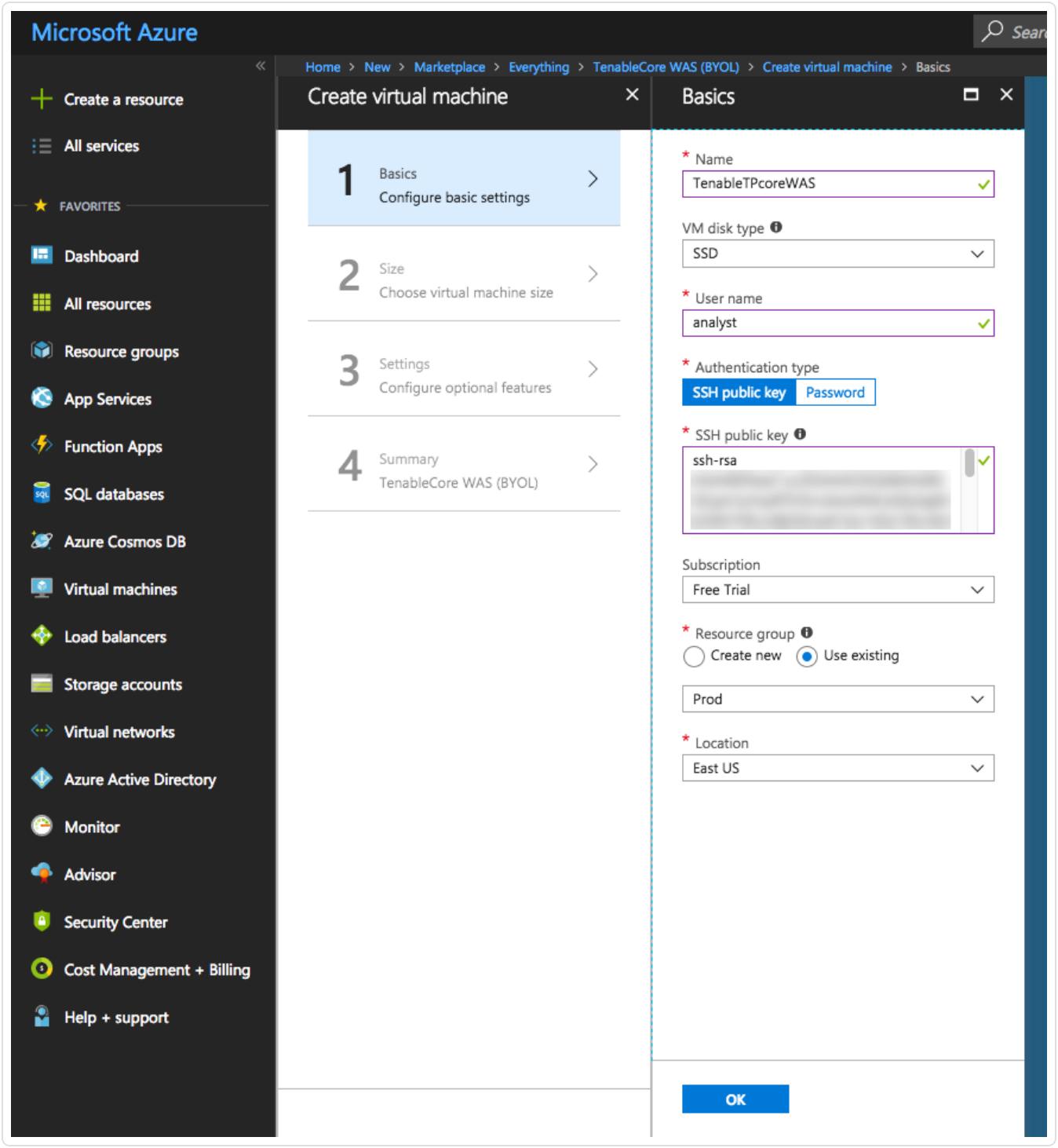
Provisioning Tenable Core Web Application Scanner (WAS) BYOL

The Tenable Core Web Application Scanner is an instance installed within Microsoft Azure that allows scanning of internally-facing web applications deployed within Microsoft Azure. The Tenable Core Web Application Scanner is a Dynamic Application Security Testing (DAST) technology. It is used to perform vulnerability assessments of web applications. Customers interested in leveraging Tenable Core Web Application Scanner BYOL to secure web applications must obtain an evaluation of Tenable.io Web Application Scanner through the drop down at the top of Tenable.io or purchase the add-on.

1. To provision a Tenable Core Web Application Scanner BYOL instance, go to Microsoft Azure (https://manage.windowsazure.com) and log in.
2. Click the green **+** to open the Azure **Marketplace**.



3. Enter **Tenable** in the search box and the **TenableCore WAS (BYOL)** instance will appear below.
4. Click **TenableCore WAS (BYOL)** to open the instance details. Choose an option under **Select a deployment model** and click **Create** to begin deployment of the Tenable Core Web Application Scanner BYOL virtual machine.
5. Enter the configuration information on the **Basics** screen and click **OK**. Refer to the *Tenable Core WAS BYOL Scanner Basics* table for details.



Tenable Core WAS BYOL Scanner Basics

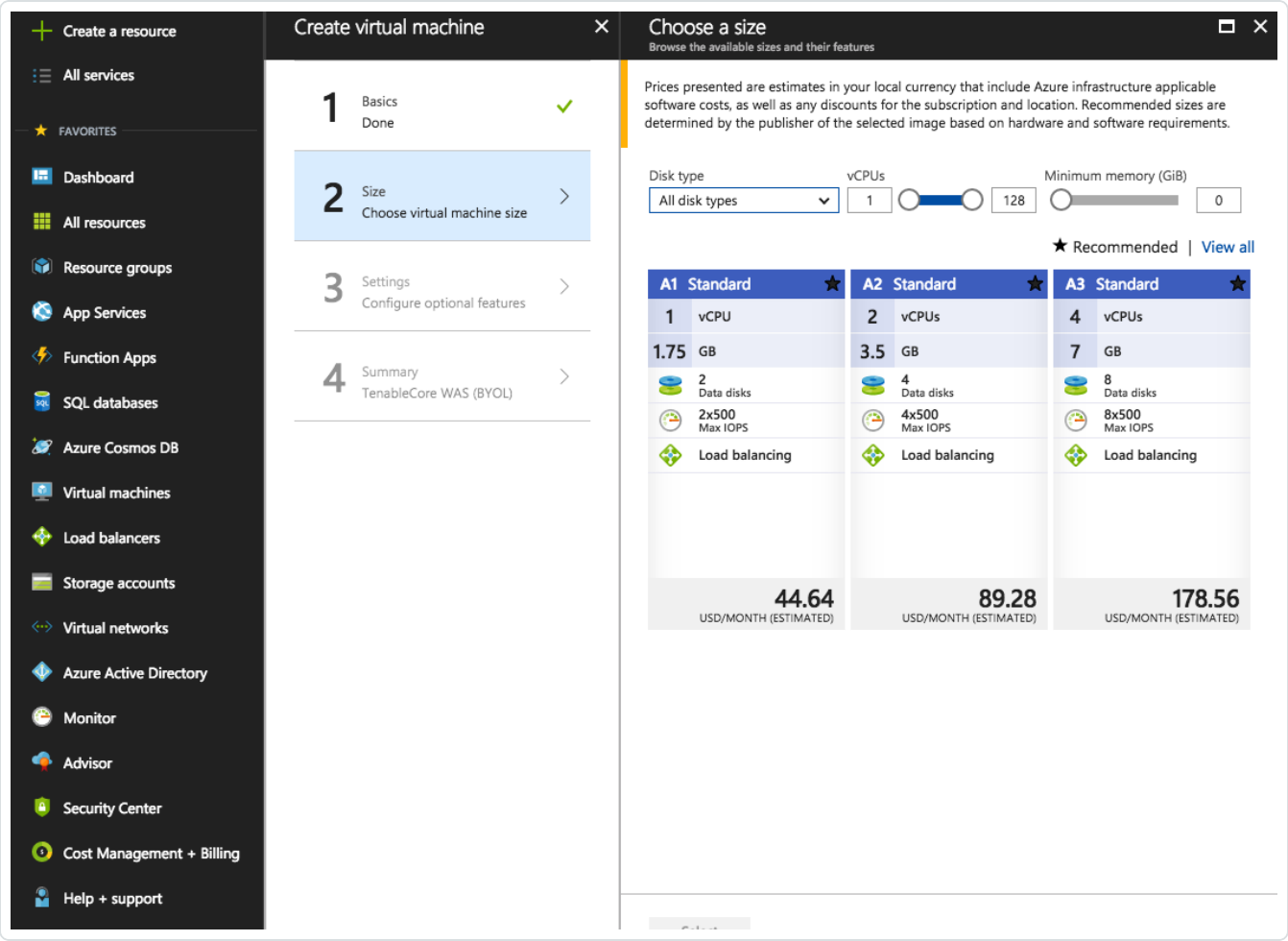
Option	Description

Name	Descriptive name for the Tenable Core WAS BYOL scanner.
VM disk type	Select between SSD and HDD drives.
User name	User account name used to access the Tenable Core WAS BYOL scanner.
Authentication type	Select **SSH public key**.

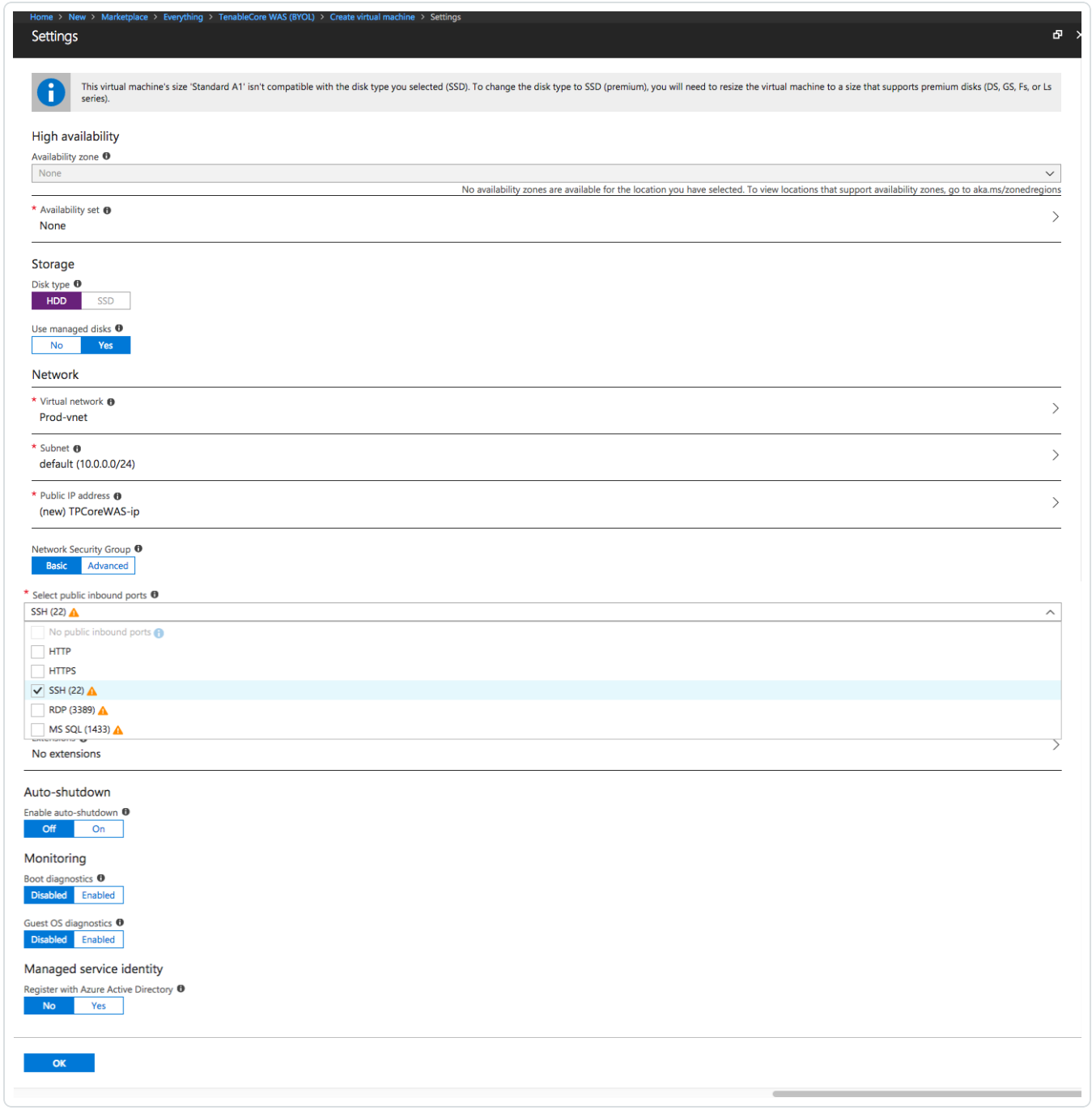
SSH Public Key	Once generated, enter the SSH public key.
	Note: Create a keypair if necessary:
	`ssh-keygen -t rsa`
	`cat ~/.ssh/id_rsa.pub`

Subscription	Select the subscription to which the virtual machine will be added.
Resource group	Enter the name of a new Resource group or select an existing Resource group.
Location	Select the geographical location for the virtual machine.

6. Once the **Basics** information is entered, instance sizes, and pricing are displayed. Scroll down to view all of the available options. Choose a desired virtual machine size by clicking on one of the displayed options and clicking **Select**.



7. On the **Settings** screen, enter the required information and click **OK** (highlighted below). Refer to the *TenableCore WAS BYOL Scanner Settings* below for details.

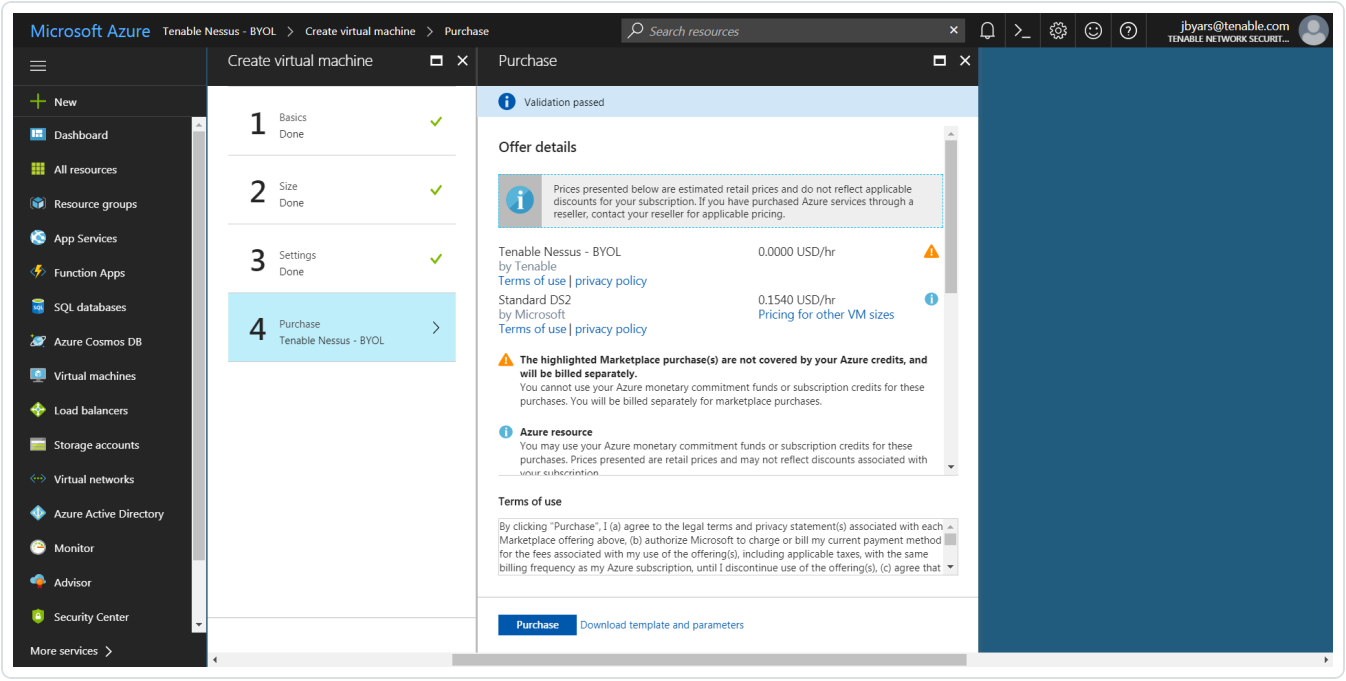


Tenable Core WAS BYOL Scanner Settings

Option	Description
Storage accounts	Create or select a storage account type and select Standard or Premium disk type.

Network	Create or select a virtual network where the Tenable Core WAS BYOL will reside.
Subnet	Assign Tenable Core WAS BYOL to a subnet in the virtual network.
Public IP Address	Option to create a public IP address so that the Tenable Core WAS BYOL virtual machine is accessible outside the virtual network.
Network security group	Enables firewall rules to control traffic to and from the Tenable Core WAS BYOL virtual machine.
Extensions	Adds new features, like configuration management or anti-virus protection, to your virtual machine.
High availability	Provides redundancy by grouping two or more virtual machines in an availability set.
Monitoring	Enable system diagnostics and create a diagnostics storage account to analyze the results.

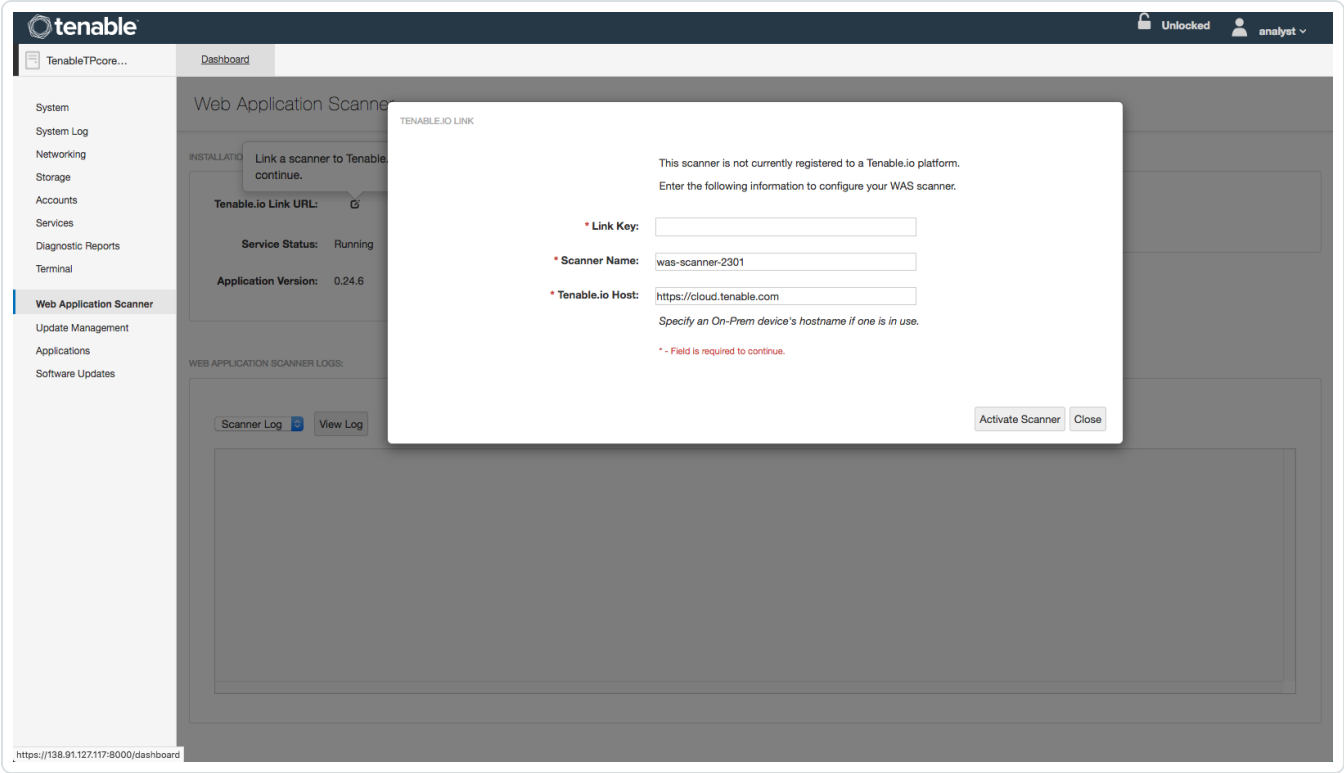
8. Offer details will display. Review, then click **Purchase** to buy the Tenable Core WAS BYOL virtual machine you configured.



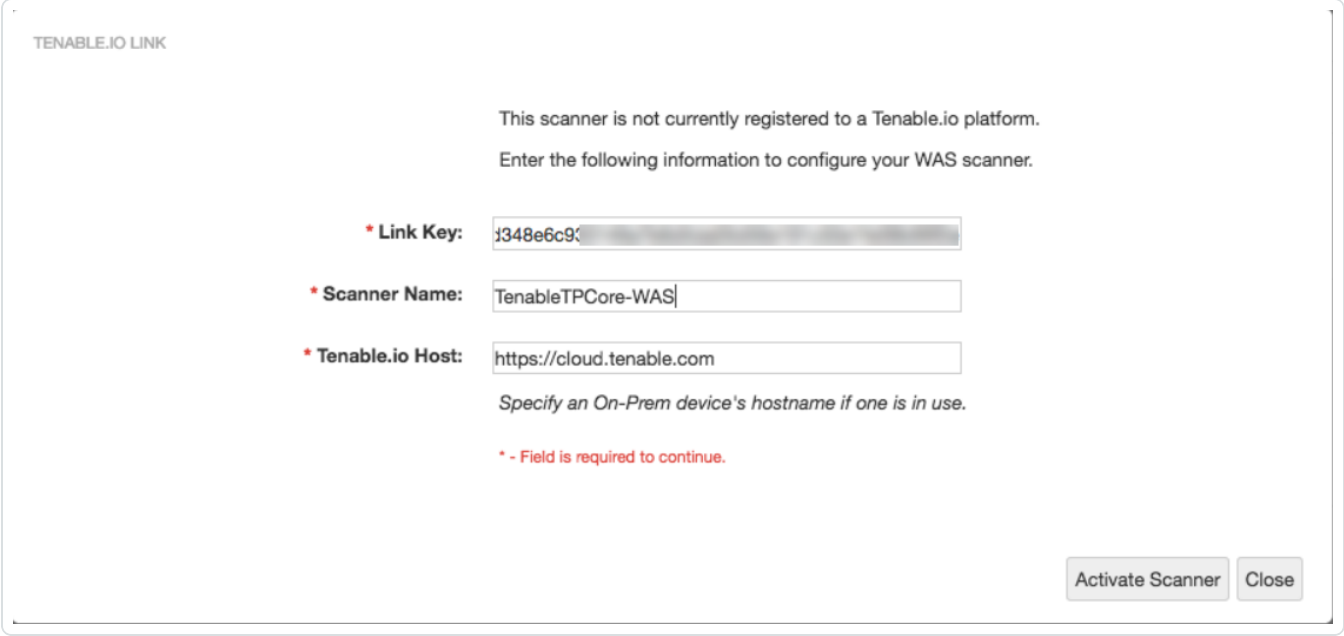
9. If you are deploying the instance into an Azure Virtual Network, you must ensure it can be reached via TCP port 8000 on an IP address associated with the instance. This is needed to complete the configuration process, as well as for the use of the product.
10. Configure the instance and/or the Azure Virtual Network so that Tenable Core WAS can communicate with Tenable servers; this is required for registration and plugin updates. If for some reason this is not possible, please refer to the Tenable Core for Web Application Scanning User Guide regarding off-line updates.
11. Generally, you will connect to the public IP address (or external hostname) associated with an instance. If you are connecting to Tenable Core WAS over a VPN to an Azure Virtual Network, it may be the private IP address. The IP addresses associated with the instance can be found under the virtual machine **Settings**.
12. Next, SSH into Tenable Core using the external IP or Azure's internal IP from another instance.

    > **Note:** Use the following command `ssh {useraccount}@{ip_address}`. The user account used here is the user account created in step 5.

13. Enter the following command using the user account created in step 5 and the Azure instance's public IP address to create a secure web UI: `sudo passwd {useraccount}`.
14. Open your browser and go to the URL - *https://{ip_address}:8000* to sign in to the web UI.
15. In the left menu, click on the Web Application Scanner option. A new window will display.

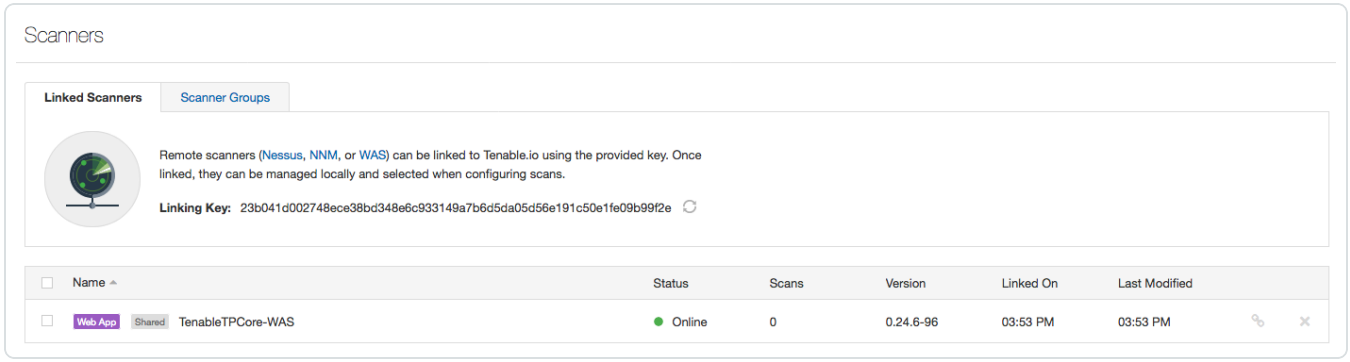


16. Enter the link key.



17. Click **Activate Scanner**. A confirmation will display.

18. The scanner displays under linked scanners.



To complete the configuration, see the Tenable Core for Web Application Scanning User Guide.

Note: Prior to scanning, you must request permission to conduct vulnerability and penetration testing on instances in the Microsoft Azure cloud environment. Please visit the following page to review the approval process and to submit a testing request: https://security-forms.azure.com/penetration-testing/terms.

About Tenable

Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.