

Tenable and Microsoft Azure Integration Guide

Last Revised: September 11, 2023

Table of Contents

Welcome to Tenable for Microsoft Azure	
Microsoft Azure Sentinel	
Audit Microsoft Azure	
Configure Azure for a Compliance Audit	
Audit Microsoft Azure in Tenable Vulnerability Management	27
Audit Microsoft Azure in Tenable Nessus	
Tenable Vulnerability Management	
Integration Requirements	
Deploy a Nessus Agent	
Create a Scan	
Nessus Agent Scan of Azure Virtual Instances	
Tenable Web App Scanning	
Provision Tenable Core Web Application Scanner (BYOL)	
Web Application Scan	
Deploy a Nessus Scanner	
Provision Tenable Core Nessus (BYOL) in Azure Marketplace	
Install Nessus on an Azure Virtual Machine	
Deploy One-Click Tenable Nessus Agent	
About Tenable	

- Ø

Welcome to Tenable for Microsoft Azure

Tenable for Microsoft Azure (Azure) offers security visibility, auditing, and system hardening that allows you to reduce the attack surface and detect malware across your Azure deployments.

Additional benefits of integrating Tenable with Azure include:

- Improved ROI due to the removal of manual verification for misconfigurations on cloud virtual machines
- Reduced security exposure through the prioritization of vulnerable machines and compromised systems

For information about integrating different Tenable products in a Microsoft Azure cloud environment, see the following:

- Audit Microsoft Azure
- Tenable Core Nessus (BYOL)
- Tenable Core WAS (BYOL)
- Nessus Agent Scans of Microsoft Azure Cloud Instances

Note: For information on configuring Microsoft Azure Connectors with Tenable Vulnerability Management, see the <u>Microsoft Azure Connector</u> documentation in the *Tenable Vulnerability Management User Guide*.

Microsoft Azure Sentinel

The Tenable integration for Microsoft Azure Sentinel combines Tenable's Cyber Exposure insights with Sentinel's collection, detection, and investigation capabilities. This integration supports Tenable Vulnerability Management and exports asset and vulnerability data from Tenable Vulnerability Management directly to Microsoft Sentinel.

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM), and security orchestration automated response (SOAR) solution. For more information about Microsoft Sentinel, see the <u>Microsoft documentation</u>.

Required User Role: Administrator. For more information, see <u>API Permissions</u>.

Note: The Microsoft Azure Sentinel integration does not export fixed vulnerabilities.

Before you begin:

- You must have a Logs Analytics Workspace with Microsoft Sentinel enabled in your Azure subscription.
- For assistance with launching Microsoft Sentinel, see the Microsoft Sentinel quick start guide.

Create the Log Analytics Workspace.

 Navigate to Microsoft Sentinel within the Microsoft Azure Portal and click Create Microsoft Sentinel.

The workspace homepage appears:

	(Ö		
	<u>^</u>		
E Microsoft Azure	$\mathcal{P}_{\rm c}$ Search resources, services, and docs (G+/)		
Home >			
Microsoft Sentinel 🖈 … Default Directory (bradles76hotmail.onmicrosoft.com)			
🕂 Create 🛞 Manage view 🗸 🕐 Refresh 🞍 Export to C	5V 😤 Open query 📄 🖹 View incidents		
Filter for any field Subscription equals all Res	urce group equals all $ imes$ Location equals all $ imes$ $\dagger_{\overline{Y}}$ Add filter		
Showing 0 to 0 of 0 records.			
Name 🗘	Resource group 14	Location 1.	Subscr
	No Micro	soft Sentinel to display	
		with SIEM reinvented for a modern world. Microsof ye view across the enterprise.	ft Sentinel is your
	c	reate Microsoft Sentinel	
		Learn more of	

2. Add a workspace for Microsoft Sentinel. Click **Create a new workspace**.

Home > Microsoft Sentinel >	
Add Microsoft Sentinel to a workspace	
+ Create a new workspace 🕐 Refresh	
Microsoft Sentinel offers a 31-day free trial. See <u>Microsoft Sentinel pricing</u> for more details.	
Filter by name	
	No workspaces found
	Create a new workspace

To create the Log Analytics workspace, you must first create a new Resource Group. Click
 Create new under Resource Group Connector.

0 -

Create Log Analytics workspace Basics Tags Review + Create A Log Analytics workspace is the basic management unt of Azure Monitor Logs. There are specific you should take when creating a new Log Analytics workspace. Learn more Wth Azure Monitor Logs you can easily store, retain, and query data collected from your monitor and other environments for valuable insights. A Log Analytics workspace is the logical storage units collected and stored. Project details Select the subscription to manage deployed resources and costs. Use resource groups like folderst manage all your resources. Subscription * Resource group * Resource group * Region * Region * Resource group is a container that holds relater resources for an Azure solution. 	Azure Sentinel > Add Microsoft Sentinel to a workspace >	ces, service
A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific you should take when creating a new Log Analytics workspace. Learn more With Azure Monitor Logs you can easily store, retain, and query data collected from your monitor and other environments for valuable insights. A Log Analytics workspace is the logical storage unit is collected and stored. Project details Select the subscription to manage deployed resources and costs. Use resource groups like folders manage all your resources. Subscription * ① Resource group * ① Instance details Name * ① Region * ② Region * ③	Analytics workspace	
you should take when creating a new Log Analytics workspace. Learn more With Azure Monitor Logs you can easily store, retain, and query data collected from your monitor and other environments for valuable insights. A Log Analytics workspace is the logical storage units collected and stored. Project details Select the subscription to manage deployed resources and costs. Use resource groups like folders manage all your resources. Subscription * ③ Resource group * ④ Aresource group is a container that holds relating resources for an Azure solution. Name * Region * ④	Review + Create	
and other environments for valuable insights. A Log Analytics workspace is the logical storage units collected and stored. Project details Select the subscription to manage deployed resources and costs. Use resource groups like folders manage all your resources. Subscription * ③ Resource group * ④ Instance details Name * ④ Region * ④ Name * Tenable-integration		5 ×
Select the subscription to manage deployed resources and costs. Use resource groups like folders manage all your resources. Subscription * Resource group * Create new Create new A resource group is a container that holds relate resources for an Azure solution. Name * Region * Name * Region *	ents for valuable insights. A Log Analytics workspace is the logical storage unit where your l	
Resource group * () Instance details Name * () Region * ()		nd
Instance details A resource group is a container that holds relative resources for an Azure solution. Name * Image: Create new Name * Image: Create new Region * (i) Image: Create new	Azure subscription AB	\sim
Instance details resources for an Azure solution. Name *		\sim
Region * () tenable-integration	A resource group is a container that holds related resources for an Azure solution.	
	tenable-integration 🗸	\sim

4. Input a **Name** for the instance detail and select the appropriate Azure **Region** from the dropdown menu.

0 -

Click **Review + Create**.

The settings are finalized and the page updates:

Iome > Microsoft Sentinel > Add Create Log Analytics Validation passed Basics Tags Review + Create		
Validation passed	workspace	
Basics Tags Review + Create		
Basics Tags Review + Create		
Log Analytics workspace		
by Microsoft		
Basics		
Subscription	Azure subscription AB	
Resource group	tenable-integration	
Name	tenable-integration	
Region	Australia Southeast	
Pricing		
Pricing tier	Pay-as-you-go (Per GB 2018)	
The cost of your workspace depends are available on the Azure Monitor pr Learn more about Log Analytics pricir	icing page. You can change to a diffe	how long it is retained. Regional pricing details erent pricing tier after the workspace is created.
Tags		
None		

5. Click **Create**.

The workspace homepage appears with your new Microsoft Sentinel workspace:

		- Ø		
Microsoft Azure	₽ Search resource	s, services, and docs (G+/)		D 🗗 🖓 @
ome > Microsoft Sentinel >				
dd Microsoft Sentinel to a wor	kspace			
Create a new workspace 💍 Refresh				
Microsoft Sentinel offers a 31-day free trial. See <u>Microsoft Sen</u>	tinel pricing for more details.			
iter by name				
orkspace 1	Location $\uparrow \downarrow$	ResourceGroup ↑↓	Subscription 14	Directory
tenable-integration	australiasoutheast	tenable-integration	Azure subscription AB	Default Dire
Add Cancel				

The Log Analytics Workplace for Microsoft Sentinel has been created.

Add the Tenable App to Microsoft Sentinel.

1. Go to the Content Hub and perform a search for "Tenable."

Microsoft Azure			earch resources, se	rvices, and docs (G+/	0				
Microsoft Sentin	Microsoft Sentinel to a workspace								
Selected workspace: 'tenable-integ		Update 📋 Delete 🔗	Guides & Feedback	(
Overview	306 Solutions	256 Standalone contents	💉 0 Installed	-					
Logs News & guides Search	,O Tenable	×	Status : All	Content type : All	Support : All	Provider : All	Category : All	Content sources : All	88 🗮
at management	Content title		Content source	Provider	Support	Category		Status	
ncidents	Tenable App	2	Solution	Tenable	Tenable				
Norkbooks	1	-	55101011	10110010	12112012				
Hunting									
Notebooks									
Entity behavior									
Threat intelligence									
MITRE ATT&CK (Preview)									
ent management									
Content hub									
Repositories (Preview)	1								
Community									
iguration									
Norkspace manager (Preview)									
Data connectors									

Ø

2. Select **Tenable App**. In the bottom-right corner click **Install**.

₽ Search «	💍 Refresh 过 Install/Uj	pdate 🔋 Delete 🔗	Guides & Feedback									
P Logs	307	253 Standalone contents	🛷 0 Installed	1 Upd	-							
C Search	,O tenable	×	Status : All	Content type : All	Support : All	Provider : All	Category : All	Content sources : All	88 📃	Omania Tenable Ar	00	
hreat management	>> tenable	~	Status : All	ontent type : An	support : All	Provider : All	category : All	Content sources : All	00	remaine rep	·P	
Incidents	Content title		Content source	Provider	Support	Category		Status		Tenable Provider	Tenable Support	2.0.2 Version
Workbooks					seppere					Description		
Hunting	Tenable App		Solution	Tenable	Tenable						choology and deliver	ed via the cloud, Tenable.io
Notebooks	4									provides the industry's	s most comprehensiv	e vulnerability management curity issues to remediate fir
Entity behavior										to reduce your cyber e		conty issues to remediate in
Threat intelligence												Exposure insights with nd investigation capabilities
MITRE ATT&CK (Preview)										This integration suppo	irts Tenable.io and ex	ports asset and vulnerability
ontent management										data from Tenable.io d		entinel. olidated way to acquire
Content hub										Microsoft Sentinel con	tent including data o	onnectors, workbooks, ce with a single deployment
Repositories (Preview)										step.	oons in your workspa	ce with a single deployment
Community										Learn more about Ten	ableCore with Nessus	1
onfiguration										Learn more about Nes	sus and Microsoft Az	ure
Workspace manager (Preview)										Content type ①		
Data connectors										1	2	WI 3
Analytics										Data connector	Parser	Playbook
Watchlist										Category ①		
										Pricing ①		

3. Once installed, in the bottom-right corner, click **Manage**.

Selected workspace: 'tenable-integrat												
P Search «	 Refresh d Install 	'Update 🗐 Delete 🔗	Guides & Feedback									
ieneral	<u></u> 306	256	# 1	0	0							
Overview	Solutions	Standalone contents	Installed	Upd	ates							
Logs News & guides	, Tenable	×	Status : All	Content type : All	Support : All	Provider : All	Category : All	Content sources : All	88 📰	Swatson Tenable A	pp	
Search reat management	Content title		Content source	Provider	Support	Category		Status		Tenable Provider	Tenable Support	2.0.2 Version
Incidents	- Tenable Ap	-	Solution	Tenable	Tenable			Installed		Description		
Workbooks	- Tenable Ap	.p	Solution	lenable	Tenable						echnology and delivered	
Hunting									,	solution with the abil	's most comprehensive lity to predict which secu	
Notebooks										to reduce your cyber		
Entity behavior										Microsoft Sentinel's o	bines Tenable's Cyber Ex collection, detection, and	investigation capabilit
Threat intelligence											orts Tenable.io and expo directly to Microsoft Ser	
MITRE ATT&CK (Preview)											lutions provide a consol	
tent management										analytics, and autom	intent including data cor ations in your workspace	
Content hub										step.	nableCore with Nessus	
Repositories (Preview)											nableCore with Nessus	
Community										sadern more exoluting	and microsoft Acti	-
iguration										Content type ①	2	W 3
Workspace manager (Preview)										Data connector	Parser	Playbook
										Category ①		
Data connectors												

Deploy the data connector.

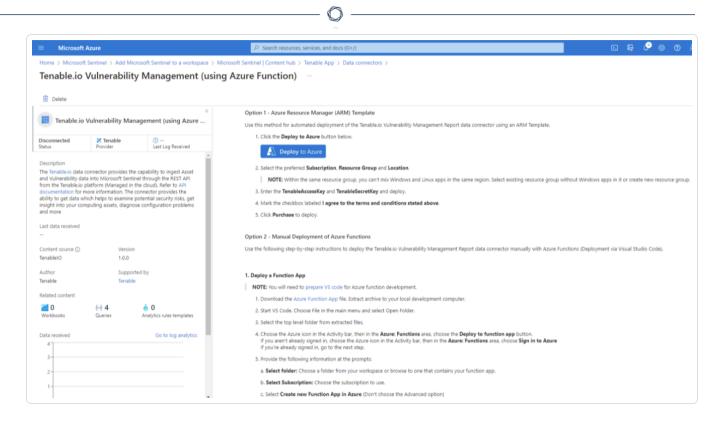
 In your newly created Tenable App, click **Tenable.io Vulnerability Management (using Azure** Function) in the content list.

			Ø			
≡ Microsof	it Azure		\mathcal{P}^{-} Search resources, services, and docs (G+/)			
Home > Microso		oft Sentinel to a workspace	> Microsoft Sentinel Content hub >			
🖒 Refresh 📋	Delete 👤 Reinstall					
✓ 8 Installed content in	items Configu	iration needed				
Tenable A	Арр	«	,⊅ Search			
Tenable Provider	Tenable Support	2.0.2 Version	Content name	Created content	Content type	Version
lescription	Support	version	🔚 Tenable.io Vulnerability Management (using Azure Function) 🔺	1 item	Data connector	1.0.0
owered by Nessus 1	technology and delivered vi		(A) Tenable.io - Enrich incident with asset info 🔺		Playbook	1.0
	y's most comprehensive vul ility to predict which security r exposure.		🕅 Tenable.io - Enrich incident with vulnerability info 🔺		Playbook	1.0
his integration com	bines Tenable's Cyber Expo collection, detection, and in		🕅 Tenable.io - Launch Scan 🔺		Playbook	1.0
his integration supp	ports Tenable.ic and exports directly to Microsoft Sentin	asset and vulnerability	TenableiCAssets	1 item	Parser	1.0.0
	olutions provide a consolida ontent including data conne		Tenable/OVulnerabilities	1 item	Parser	1.0.0
inalytics, and autom tep.	nations in your workspace w	ith a single deployment	٩			
earn more about Te.	enableCore with Nessus					
earn more about N	essus and Microsoft Azure					
Content type ① 1 Nata connector		A) 3 Playbook				
ategory 🛈						
ricing 🛈	Actions View detail	•				
Manage	Actions View detail	IS				

2. Select the name of the connector and in the bottom-right corner, click **Open connector page**.

Refresh 🔗 Guides & Feedback			
1 ar 0 consected Consected at Consected but December 1 at			
TenabletOAPI X Providers : All Data Types : All Status : All	Tenable.i	Vulnerability Mana	igement (using Azu
atus Connector name †	Disconnected Status	X Tenable Provider	C Last Log Received
Tenable	and Vulnerability d from the Tenable is documentation for ability to get data	connector provides the ta into Microsoft Sentin platform (Managed Fin more information. The co ihich helps to examine p mputing assets, diagnosi Version	el through the REST API he cloud). Refer to API prinector provides the otential security risks, ge
	Tenable/O Author Tenable Related content	1.0.0 Supporte Tenable	ed by
	0 Workbooks	€⁄} 4 Queries	o 0 Analytics rules templates

3. Deploy the ARM template by clicking **Deploy to Azure**.



4. Select the **Resource Group** and populate the remaining four fields.

Note: The Tenable export schedule is set for every 24 hours (1440 minutes) by default. This can be adjusted to suit the requirements needed to gather asset and vulnerability data in a timely manner.

5. Once all fields have been populated, click **Review + create**.

E Microsoft Azure		ervio
lome >		
Custom deployment		
	age the lifecycle of your deployments. Try it now $ ightarrow $	
Template		
Customized template 8 resources	Edit template Edit parameters Visualize	
Project details		
Select the subscription to manage deploy manage all your resources.	yed resources and costs. Use resource groups like folders to organize and	
Subscription * 🕡	Azure subscription AB	\sim
Resource group * 🕕	tenable-integration	\sim
	Create new	
Instance details		
Region * 🥡	(Asia Pacific) Australia Southeast	~
Function Name	TenableIO	~
Workspace ID *		~
Workspace Key *		~
	L	
		\checkmark
Tenable Access Key * 🥫		
	•••••	~
Tenable Access Key * 🗊 Tenable Secret Key *		~
	720	~

6. The fields are finalized. Click **Create**.

Search resources, services, and do

Microsoft Azure

Home >

Custom deployment

Deploy from a custom template

Terms

Azure Marketplace Terms Azure Marketplace

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

Subscription	Azure subscription AB
Resource group	tenable-integration
Region	Australia Southeast
Function Name	TenableIO
Workspace ID	*****
Workspace Key	035055000000000000000000000000000000000
Tenable Access Key	*******
Tenable Secret Key	***
Tenable Export Schedule In Minutes	720
Previous Next Create	

Check for the resources.

1. Once the deployment has been completed, click **Go to Resource Group** to see the resources that have been created.

O

Microsoft Azure		
lome > Microsoft.Tem Deployment	plate-20230903191657 Overview 🖈 …	
₽ Search	≪ 🗎 Delete 🛇 Cancel 📅 Redeploy 🕹 Download 🖒 Refresh	
Vverview	Your deployment is complete	
Inputs		Start time : 9/3/2023, 7:17:00 PM
Outputs	Subscription : Azure subscription AB	Correlation ID : 57cc79d2-d756-4abb-a5b6-5daf86fa5884
Template	Resource group : tenable-integration	
	> Deployment details	
	✓ Next steps	
	Go to resource group	
	Give feedback	
	$\widehat{\mathcal{R}}^{2}$. Tell us about your experience with deployment	

2. The app populates the following resources:

Note: The app may take up to ten minutes to populate the resources.

Microsoft Azure	P Search resources, services, and docs (G+/)		d 🖓 🖓
ome > Microsoft.Template-2023	30903191657 Overview >		
tenable-integrat	tion ≉ ☆ …		
Search	🔹 🕂 Create 🔞 Manage view 🗸 🗊 Delete resource group 🖒 Refresh 🞍 Export to CSV 😤 Op	en query │	Open in mobile
Overview	▲ ▲ Essentials		
Activity log	Subscription (move) : Azure subscription AB	Deployments : <u>5 Succeeded</u>	
Access control (IAM)	Subscription ID : 269b82d4-ef3b-4129-a3b0-a605cc76352c	Location : Australia Southeast	
Tags	Tags (edit) : Add tags		
Resource visualizer			
Events	Resources Recommendations		
tings			
tungs	Filter for any field Type equals all X Location equals all X Type Add filter		
Deployments	Filter for any field Type equals all X Location equals all X Typ Add filter Showing 1 to 8 of 8 records. Show hidden types O		No groupin
-	Showing 1 to 8 of 8 records.	Type ↑↓	No groupin
Deployments Security	Showing 1 to 8 of 8 records. Show hidden types ⊙ Name ↑		Location ↑↓
Deployments Security Deployment stacks	Showing 1 to 8 of 8 records. Show hidden types ⊙ Name ↑↓ Given Application Insights Smart Detection	Action group	Location ↑↓ Global
Deployments Security Deployment stacks Policies	Showing 1 to 8 of 8 records. Show hidden types ③ Name ↑↓ Gold Application Insights Smart Detection Gold AustraliaSoutheactLinuxDynamicPlan	Action group App Service plan	Location ↑↓ Global Australia Southea
Deployments Security Deployment stacks Policies Properties	Showing 1 to 8 of 8 records. Show hidden types ⊙ Name ↑↓ □ Image: Application Insights Smart Detection □ Image: AustraliaSoutheactLinuxDynamicPlan □ Image: AustraliaSoutheactLinuxDynamicPlan □ Image: AustraliaSoutheactLinuxDynamicPlan □	Action group App Service plan Smart detector alert rule	Location 1
Deployments Security Deployment stacks Policies Properties Lucks	Showing 1 to 8 of 8 records. Show hidden types ⊙ Name ↑↓ □ Image: Application Insights Smart Detection □ Image: AustraliaSoutheactLinuxDynamicPlan □ Image: Failure Anomalies - tenableofleftgee7geq □ Image: Security(Insights(tenable-integration) □	Action group App Service plan Smart detector alert rule Solution	Location 1. Global Australia Southea Global Australia Southea
Deployments Security Deployment stacks Policies Properties Locks et Management	Showing 1 to 8 of 8 records. Show hidden types ⊙ Name ↑↓ □ Image: Application Insights Smart Detection □ Image: Application Insights Compared to the state of the stat	Action group App Service plan Smart detector alert rule Solution Log Analytics workspace	Location 🛧 Clobal Australia Souther Global Australia Souther Australia Souther
Deployments Security Deployment stacks Policies Properties Locks et Management Cost analysis	Showing 1 to 8 of 8 records. Show hidden types ⊙ Name ↑↓	Action group App Service plan Smart detector alert rule Solution Log Analytics workspace Application Insights	Location ↑↓ Global Australia Souther Global Australia Souther Australia Souther Australia Souther
Deployments	Showing 1 to 8 of 8 records. Show hidden types ⊙ Name ↑↓ □ Image: Application Insights Smart Detection □ Image: Application Insights Compared to the state of the stat	Action group App Service plan Smart detector alert rule Solution Log Analytics workspace	Location ↑↓ Global Australia Southea

3. In the **Function App**, verify that you can see the listed functions:

tenableiowp6klc5 Function App	ukgnine x u				
Search e	+ Create 《 〉Set up local environment \checkmark 🕐 Refresh				
Overview	 P Filter by name 				
Activity log Access control (IAM)	Name	Trigger	Status	Monitor	
Tags	TenableAssetExportOrchestrator	Orchestration	S Enabled	Orchestration information	
Diagnose and solve problems Microsoft Defender for Cloud	TenableAssetExportStatusAndSendChunks	Activity	C Enabled	Invocations and more	
Events (preview)	TenableCleanTables	Activity	S Enabled	Invocations and more	
inctions	TenableCleanUpOrchestrator	Orchestration	S Enabled	Orchestration information	
App keys App files	TenableExportsOrchestrator	Orchestration	🖉 Enabled	Orchestration information	
Proxies	TenableExportStarter	Timer	S Enabled	Invocations and more	
rployment	TenableGenerate/obStats	Activity	C Enabled	Invocations and more	
Deployment slots	TenableProcessAssetChunkFromQueue	Queue	S Enabled	Invocations and more	
Deployment Center	TenableProcessFailedAssetChunkFromQueue	Queue	🖉 Enabled	Invocations and more	
Configuration	TenableProcessFailedVuInChunkFromQueue	Queue	C Enabled	Invocations and more	
Authentication	TenableProcessVuInChunkFromQueue	Queue	@Enabled	Invocations and more	
Application Insights	TenableStartAssetEsportJob	Activity	C Enabled	Invocations and more	
Identity					
Backups	TenableStartVulnExportJob	Activity	S Enabled	invocations and more	
Custom domains	TenableVuInExportOrchestrator	Orchestration	C Enabled	Orchestration information	

O

Audit Microsoft Azure

To audit Microsoft Azure, do the following:

- Configure Microsoft Azure for use with a compliance audit, as described in <u>Configure Azure</u> (Compliance Audit).
- Create an audit scan with Tenable Vulnerability Management or Tenable Nessus:
 - Audit Microsoft Azure in Tenable Vulnerability Management
 - Audit Microsoft Azure in Tenable Nessus

For more information on the Microsoft Azure audit, see <u>Microsoft Azure Audit Compliance Refer</u>-<u>ence</u> in the *Compliance Checks Reference*.

Configure Azure for a Compliance Audit

The Tenable integration for Microsoft Azure supports two parallel methods for creating and registering the application: Key Authentication and Password Authentication. Choose either of the authentication methods, then complete the setup with the <u>Assign API Permissions</u> steps.

Key Authentication Method

Register Application: Key

- 1. Click Microsoft Entra ID > App Registrations.
- 2. Click the **New Registrations** application.
- 3. Give the application a name.
- 4. Choose the supported account types for your environment.
- 5. Choose **Public Client/Native** for the redirect URI type.
- 6. (Optional) Add a redirect URI.
- 7. Click Register.

Create Application Client Secret

- 1. Click your registered application in **Microsoft Entra ID > App Registrations**.
- 2. Click Certificates and Secrets.
- 3. Click + New client secret.

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
+ New client secret

4. Give the secret a name and click **Add**.

Tip Copy the secret somewhere safe for use in authenticating during a scan.

Assign the Application the Reader Role

1. Click Subscriptions > Your Subscription > Access Control (IAM) > Role Assignments > + Add.

0 -

- 2. Add the **Reader** role to the application you previously created for scanning.
- 3. Select **Reader** from the **Role** drop-down menu.
- 4. Assign access to User, Group, or Service Principal.
- 5. In the **Select** field, type the name of your created application.
- 6. Select the application.
- 7. Click Save.

Password Authentication Method

Create Microsoft Entra ID User Account

Create a new user to scan in the Microsoft Entra ID. See the <u>Microsoft Azure</u> documentation for steps to add a new user.

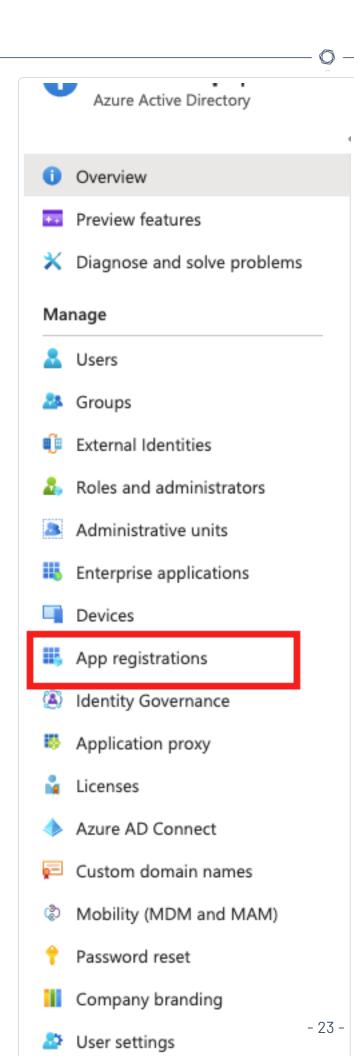
Assign User the Reader Role

- 1. Click Subscriptions > Your Subscription > Access Control (IAM) > Role Assignments > + Add.
- 2. Add the **Reader** role to the user account you created for scanning.

Register Application: Password

1. Click on **Microsoft Entra ID > App registrations**.

- Ø _____

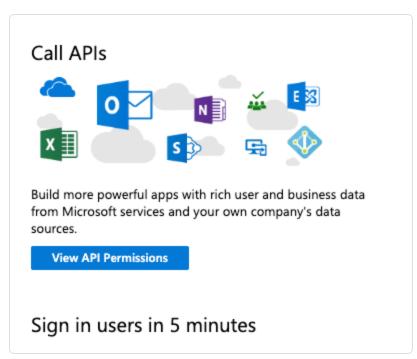


- 2. Click New Registrations application.
- 3. Give the application a name.
- 4. Choose the supported account types for your environment.
- 5. Click **Register**.
- 6. Click Authentication.
- 7. Choose Yes for Default Client Type/Treat application as a public client.

API Permissions

Assign API Permissions

- 1. Click your registered application in Microsoft Entra ID > App Registrations > Your Application
 - > API Permissions.



2. Select Microsoft Graph.

Note: If adding permissions for Key Authentication, then select **Application permissions**. If adding permissions for Password Authentication, then select **Delegated permissions**.

3. In the **Configured permissions** section, click **Add a permission**.

- 4. Add the following permissions:
 - Azure Service Management user_impersonation
 - Microsoft Graph Calendars.Read
 - Microsoft Graph DeviceManagementApps.Read.All
 - Microsoft Graph DeviceManagementConfiguration.Read.All
 - Microsoft Graph Directory.Read.All
 - Microsoft Graph Policy.Read.All
 - Microsoft Graph Reports.Read.All
 - Microsoft Graph User.Read.All

Scanning Microsoft 365 environment:

• Microsoft Graph – SecurityEvents.Read.All

Scanning Microsoft Intune:

- Microsoft Graph DeviceManagementApps.Read.All
- Microsoft Graph DeviceManagementManagedDevices.Read.All

API / Permissions name	Туре	Description	Admin consent req	Status	
✓ Azure Service Management (1)					
user_impersonation	Delegated	Access Azure Service Management as organization use	-	🤣 Granted for Bob Corp	
Microsoft Graph (7)					•••
Calendars.Read	Application	Read calendars in all mailboxes	Yes	🥑 Granted for Bob Corp	•••
DeviceManagementApps.Read	Application	Read Microsoft Intune apps	Yes	🤣 Granted for Bob Corp	
DeviceManagementConfigurat	Application	Read Microsoft Intune device configuration and policies	Yes	🤣 Granted for Bob Corp	
Directory.Read.All	Application	Read directory data	Yes	🥑 Granted for Bob Corp	
Policy.Read.All	Application	Read your organization's policies	Yes	🥑 Granted for Bob Corp	
Reports.Read.All	Application	Read all usage reports	Yes	🥑 Granted for Bob Corp	
User.Read.All	Application	Read all users' full profiles	Yes	🥑 Granted for Bob Corp	

- 5. Click Grant admin consent.
- 6. Click Add permissions.

What to do next:

Create an audit scan in either Tenable Vulnerability Management or Tenable Nessus:

_____ Ø _____

- Audit Microsoft Azure in Tenable Vulnerability Management
- Audit Microsoft Azure in Tenable Nessus

Audit Microsoft Azure in Tenable Vulnerability Management

Tenable offers the ability to audit the Microsoft Azure Cloud environment to detect misconfigurations in the cloud environment and account settings using Tenable Vulnerability Management. Complete the following steps to Audit Microsoft Azure in Tenable Vulnerability Management.

For more information on the Microsoft Azure audit, see <u>Microsoft Azure Audit Compliance Refer</u>-<u>ence</u> in the *Compliance Checks Reference*.

Before you begin:

• Configure Azure as described in <u>Configure Azure for a Compliance Audit</u>.

Note: No pre-authorization is needed from Microsoft to perform the audit, but a Microsoft Azure account is required.

To audit Microsoft Azure in Tenable Vulnerability Management:

- 1. Log in to Tenable Vulnerability Management.
- 2. In the upper-left corner, click the \equiv button.

The left navigation plane appears.

3. In the left navigation plane, in the Vulnerability Management section, click Scans.

The **Scans** page appears.

4. In the upper-right corner of the page, click \oplus Create a Scan.

The Select a Scan Template page appears.

5. Select the **Audit Cloud Infrastructure** template.

The Audit Cloud Infrastructure page appears.

- 6. In the **Name** box, type a descriptive name for the scan.
- 7. (Optional) In the **Description** box, enter information to describe your scan.

8. Click Compliance.

9. Click **Microsoft Azure**.

Tenable offers pre-configured compliance checks and provides the ability to upload a custom Azure audit file.

Note: For information on creating a custom audit, see <u>Microsoft Azure Audit Compliance Reference</u> in the Nessus Compliance Checks Reference Guide.

- 10. Click each compliance check you want to add to the scan.
- 11. If you choose to add a custom audit file, click **Add File** and select the file to upload.
- 12. Click Credentials.
- 13. Click **Microsoft Azure**.

Note: See the <u>Required User Privileges</u> section in the Nessus User Guide for the required Microsoft Azure privileges.

 Click the Authentication Method drop-down menu to select your preferred authentication method: key or password.

Configure the credentials for your selected authentication method.

To configure key authentication:

Option	Description	Required
Tenant ID	The <u>Tenant ID</u> or Directory ID for your Azure envir- onment.	Yes
Application ID	The application ID (also known as client ID) for your registered application.	Yes
Client Secret	The secret key for your registered application.	Yes
Subscription IDs	List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	No

To configure password authentication:

Option	Description	Required
Username	The username required to log in to Microsoft Azure.	Yes
Password	The password associated with the username.	Yes
Client ID	The application ID (also known as client ID) for your registered application.	Yes
Subscription IDs	List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	No

O

15. Do one of the following:

- Click Save.
- Click the drop-down arrow next to **Save** and select **Launch** to initiate the scan.

Note: For additional information on configuring Tenable Vulnerability Management scans, refer to the <u>Tenable Vulnerability Management User Guide</u>.

Audit Microsoft Azure in Tenable Nessus

Tenable offers the ability to audit the Microsoft Azure Cloud environment to detect misconfigurations in the cloud environment and account settings using Tenable Nessus. Complete the following steps to Audit Microsoft Azure in Tenable Nessus.

For more information on the Microsoft Azure audit, see <u>Microsoft Azure Audit Compliance Refer</u>-<u>ence</u> in the *Compliance Checks Reference*.

Before you begin:

• Configure Azure as described in Configure Azure for a Compliance Audit.

Note: No pre-authorization is needed from Microsoft to perform the audit, but a Microsoft Azure account is required.

To Audit Microsoft Azure in Tenable Nessus:

- 1. Log in to Tenable Nessus.
- 2. In the upper-left corner, click the \equiv button.

The left navigation plane appears.

3. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.

The **Scans** page appears.

4. In the upper-right corner of the page, click \oplus Create a Scan.

The Select a Scan Template page appears.

5. In the **Compliance** section, select the **Audit Cloud Infrastructure** template.

The Audit Cloud Infrastructure page Settings tab appears.

- 6. In the **Name** box, type a descriptive name for the scan.
- 7. (Optional) In the **Description** box, enter information to describe your scan.
- 8. Click the **Credentials** tab.
- 9. In the **Categories** section, click **Microsoft Azure**.

The **Microsoft Azure** options appear.

 Click the Authentication Method drop-down menu to select your preferred authentication method: key or password.

Ø

11. Configure the credentials for your selected authentication method.

To configure key authentication:

Option	Description	Required
Tenant ID	The <u>Tenant ID</u> or Directory ID for your Azure envir- onment.	Yes
Application ID	The application ID (also known as client ID) for your registered application.	Yes
Client Secret	The secret key for your registered application.	Yes
Subscription IDs	List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	No

To configure password authentication:

Option	Description	Required
Username	The username required to log in to Microsoft Azure.	Yes
Password	The password associated with the username.	Yes
Client ID	The application ID (also known as client ID) for your registered application.	Yes
Subscription IDs	List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	No

12. Click **Compliance**.

13. Click **Microsoft Azure**.

Tenable offers pre-configured compliance checks and provides the ability to upload a custom Azure audit file.

Note: For information on creating a custom audit, see <u>Microsoft Azure Audit Compliance Reference</u> in the Nessus Compliance Checks Reference Guide.

- 14. Click each compliance check you want to add to the scan.
- 15. If you choose to add a custom audit file, click **Add File** and select the file to upload.
- 16. Click Save.

The credential saves and the My Scans page appears.

Note: For additional information on configuring Nessus scans, refer to the <u>Tenable Nessus User Guide</u>.

Tenable Vulnerability Management

View the following sections for steps on how to configure Tenable Vulnerability Management with Microsoft Azure.

O

- <u>Connector</u>
 - Create Azure Principal Account
- Deploy a Nessus Scanner
 - Provision Tenable Core for Nessus (BYOL) in Azure Marketplace
 - Install Nessus on an Azure Virtual Machine
- Create a Scan
- Deploy a Nessus Agent
- Configure Microsoft Azure for Auditing
 - Audit Microsoft Azure in Tenable Vulnerability Management

Integration Requirements

To integrate Tenable Vulnerability Management with Microsoft Azure, you need the following:

 \bigcirc

• Tenable Vulnerability Management account

To purchase a Tenable Vulnerability Management account or set up a free evaluation, visit http://www.tenable.com/products/tenable-io

• Azure account

To create a free account, visit https://azure.microsoft.com/en-us/free/

• Internet connection

You must have a <user>@<somedomain>.onmicrosoft.com account.

Deploy a Nessus Agent

For instructions on deploying a Nessus Agent, see the <u>Nessus Agent Deployment</u> section in the *Nessus Agent and Deployment and User Guide*.

O

Create a Scan

Create a Tenable Vulnerability Management Scan

For instruction on creating a scan, see the <u>Create a Scan</u> steps in the Tenable Vulnerability Management User Guide.

O

Create an Agent Scan

For instruction on creating an Agent scan, see the <u>Create an Agent Scan</u> steps in the *Tenable Vulnerability Management User Guide*.

Nessus Agent Scan of Azure Virtual Instances

Tenable's Nessus Agents provide the ability to perform local scans on instances within the Microsoft Azure cloud environment. Nessus Agent Scans, which are configured, managed, and updated through Tenable Vulnerability Management or Tenable Nessus Manager, help identify vulnerabilities, compliance violations, misconfigurations, and malware.

Download Nessus Agents from the <u>Tenable Downloads site</u>, install it on an instance running in the Microsoft Azure cloud environment, and link it to Tenable Vulnerability Management or Nessus Manager.

Note: Agents can be installed on your target(s) manually, via Group Policy, SCCM, or other third-party software deployment applications.

Nessus Agents are linked to Tenable Vulnerability Management or Nessus Manager in the same manner as linking to a secondary scanner. Prior to installing Nessus Agents, you must acquire the Agent Key from within Tenable Vulnerability Management or Nessus Manager.

- 1. To acquire the Agent Key, log in to Tenable Vulnerability Management or Nessus Manager.
- 2. Click Settings > Scanners > Agents > Linked.
- 3. A key is generated for the Nessus Agents to link to the scanner.

	Agents								
My Scans	Agents								
6.10 scans 2 cen7-172.26.16.224	Linked Agents	Agent Groups Black	out Windows Agent S	ettings					
cent6-172.26.17.40 scans 3 scans2 ub16-172.26.18.225 uploads				p instructions. Once linked, the ess takes several minutes and i					
win10x-172.26.18.2 win732-172.26 1 win764-172.26 1	Filter Search A	Agents Q	6 Agents IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned	
All Scans			IF Address		Groups	version	Last Plugin opuate	Last Scallieu	
Trash	8bae46cd-4a1	10-44a1 🔍 Offline	N/A	Windows (win-x86-64)	N/A	N/A	N/A	N/A	
	9488f67c-d66	8-41f2-8 Offline	N/A	Windows (win-x86-64)	N/A	N/A	N/A	N/A	
Policies	Server2012R2	Offline	172.26.38.65	Windows (win-x86-64)	qa-agent, windows ag	N/A	N/A	April 6	
Plugin Rules	Win81	Offline	172.26.37.79	Windows (win-x86-64)	qa-agent, windows ag	N/A	N/A	April 6	
-		ANNIVE Offline	172.26.36.82	Windows (win-x86-64)	qa-agent, windows ag	N/A	N/A	April 6	
Scanners	WINDOWS10								

For more information on installing and configuring Nessus Agents, refer to the Nessus User Guide.

Tenable Web App Scanning

View the following sections for steps on how to configure Tenable Web App Scanning with Microsoft Azure.

Ø

- Provision Tenable Core Web Application Scanner (BYOL) in Azure Marketplace
- Create a Tenable Web App Scanning Scan

Provision Tenable Core Web Application Scanner (BYOL)

Tenable Core Web Application Scanner Bring Your Own License (BYOL) is an instance of a Tenable Vulnerability Management Web Application Scanner installed in Microsoft Azure that allows you to scan internal-facing web applications deployed in Microsoft Azure. The Tenable Core Web Application Scanner (BYOL) is used to perform vulnerability assessments of web applications.

To provision a Tenable Core Web Application Scanner BYOL instance:

- 1. Log in to the Microsoft Azure portal.
- 2. In the left-hand menu, click + Create a resource.

The **New** page appears.

3. In the search box, type TenableCore WAS (BYOL).

As you type, Tenable options appear.

4. Select the TenableCore WAS (BYOL) option or press enter.

The TenableCore WAS (BYOL) page appears.

Microsoft Azure	P Search resources, services, and docs (G+)/	₽ ⊗	? 😳	TENABLE, INC.
«	Home > New > TenableCore WAS (BYOL)			
+ Create a resource	TenableCore WAS (BYOL)			\$ X
🛧 Home				
🛄 Dashboard	TenableCore WAS (BYOL) 😒 Save for later			
All services	Tenable			
+ FAVORITES	Create Start with a pre-set configuration			
All resources	Want to deploy programmatically? Get started			
(🕥 Resource groups				
🔇 App Services	Tenable io Web Application Scanning delivers safe and automated vulnerability scanning that covers your entire online portfolio. Through comprehensive and accu application scanning as part of a complete vulnerability management solution, you can see and manage your security exposure across all types of assets and fully			
🦘 Function App	organization.			
👼 SQL databases	TenableCore is the virtual appliance platform we use as the base for many of our applications. TenableCore is a lightly customized version of CentOS 7. It has these features:	• major		
🖉 Azure Cosmos DB	SELinux Enabled			
👤 Virtual machines	 Configuration to meet some elements of the CIS Level 1 Benchmarks A GUI for configuration of a number of application and O/S features. 			
💠 Load balancers	Learn more about TenableCore for Web Application Scanning			
Storage accounts	Learn more about TenableCore and Microsoft Azure			
💮 Virtual networks	Useful Links			
Azure Active Directory	Find a Tenable Reseller Tenable Community Forums			
🕒 Monitor	Tenable Web Application Scanning Documentation Tenable Store			
🜪 Advisor	Tenable Video Tutorials			
Security Center	IenableCore with WAS			
Oost Management + Bill				
🔒 Help + support				
https://portal.azure.com/#	¢			-

5. Click the **Create** button.

The **Create a virtual machine** page appears.

 On the Basics tab, enter the required information for each option in the Project details, Instance details, and Administrator account sections.

Ø

Option	Description
Project Details	
Subscription	The account through which resources are reported and services are billed.
Resource Group	The collection of resources that share the same lifecycle, permissions, and policies.
Instance Details	
Virtual machine name	The name used for both, the virtual machine and host name.
	Note: The virtual machine name cannot be changed after the virtual machine is created. You can change the host name when you log into the virtual machine.
Region	The regional location most suitable for you and your cus- tomers.
	Note: Some virtual machine sizes are not available in cer- tain regions.
Availability options	(Optional) Additional options to help manage availability and resilience of your applications. Provides options to use replicated virtual machines in availability zones or availability settings to protect your applications and data from outages and maintenance events.
Image	The base operating system or application for the virtual machine.

Size	The virtual machine size to support the workload you want to run.
Administrator Account	
Authentication Type	The type of authentication the administrator uses - SSH or password.
Username	The administrator username for the virtual machine.
SSH Key	(Only available when you select SSH for Authentication Type) The single-line RSA public key or multi-line PEM cer- tificate.
	For additional information on setting up your SSH account, see <u>Create a Password for the Initial Admin</u> - <u>istrator User Account</u> .
Password	(Only available when you select Password for Authentic- ation Type) The administrator password for the virtual machine.
Confirm Password	(Only available when you select Password for Authentic- ation Type) Verification for the administrator password for the virtual machine.

R

7. Click the **Disks** tab.

The **Disks** page appears.

Microsoft Azure			►.	RΩ	_{ණි} ?	0	TENABLE, INC.
«	Home > New > TenableCore WAS (E				· ·	Ŭ	TENABLE, INC.
Create a resource	Create a virtual machine						
Home							
Dashboard	Basics Disks Networking M	Management Advanced Tags Review + create					
All services							
FAVORITES		disk and a temporary disk for short-term storage. You can attach additional data disks. e of storage you can use and the number of data disks allowed. Learn more					
All resources	Disk options						
Resource groups	★ OS disk type 🚯	Standard SSD 🗸					
App Services	Enable Ultra Disk compatibility (Previe	w) 🚯 🔿 Yes 💿 No					
> Function App		Ultra Disk compatibility is not available for this VM size and location.					
SQL databases	Data disks						
Azure Cosmos DB	You can add and configure additional temporary disk.	data disks for your virtual machine or attach existing disks. This VM also comes with a					
Virtual machines	LUN NAME	SIZE (GIB) DISK TYPE HOST CACHING					
Load balancers							
Storage accounts	Create and attach a new disk Atta	ch an existing disk					
•> Virtual networks							
Azure Active Directory	✓ Advanced						
Monitor							
Advisor							
Security Center							
Cost Management + Bill	Review + create	Previous Next : Networking >					
Help + support							

 \bigcirc

- 8. On the **Disks** page, in the **Disks option** section, select an **OS disk type** from the drop-down.
- 9. (Optional) In the **Data disks** section, you can add and configure additional data disks or attach existing disks.
- 10. Click the **Networking** tab.

The **Networking** page appears.

Aicrosoft Azure			D	Ģ	? 🕸 (٢	TENABLE, INC.
*	Home > New > TenableCore WAS (B)	(OL) > Create a virtual machine					
 Create a resource 	Create a virtual machine						
Home							
Dashboard	Basics Disks Networking M	anagement Advanced Tags Review + create					
All services	Define network connectivity for your vi	tual machine by configuring network interface card (NIC) settings. You can control					
FAVORITES		ity with security group rules, or place behind an existing load balancing solution.					
All resources	Network interface						
Resource groups	When creating a virtual machine, a network	unrk interface will be created for you					
App Services	-						
Function App	* Virtual network 🚯	Filter virtual networks					
SQL databases	Public IP 👩	None V					
Azure Cosmos DB		Create new					
Virtual machines	NIC network security group 🚯	None Basic Advanced					
Load balancers							
Storage accounts		This VM image has preconfigured NSG rules					
Virtual networks							
Azure Active Directory	* Configure network security group	~ ·					
Monitor		Create new					
Advisor	Accelerated networking 👩	 On Off The selected image does not support accelerated networking. 					
Security Center							
Cost Management + Bill	Review + create <	Previous Next : Management >					

 \bigcirc

- 11. In the **Virtual Network** drop-down box, select a network.
- 12. (Optional) Select a **Public IP** and **NIC network security group**.
- 13. In the **Configure network group** drop-down box, select a resource group.

Note: You can create a new group by clicking the **Create new** link beneath the drop-down box.

- 14. (Optional) Enable or disable **Accelerated networking** option.
- 15. (Optional) In the **Load balancing** option, select to place the virtual machine behind an existing load balancing solution.
- 16. Click the **Management** tab.

The **Management** page appears.

17. Enter your management preferences.

Options	Description
Monitoring	
Boot diagnostics	(Optional) Enable to capture the serial con-

	sole output and screenshots of the virtual machine running on a host.
OS guest diagnostics	(Optional) Enable to receive metrics for your virtual machine.
Diagnostic storage account	The account used to store your metrics.
Identity	
System assigned managed identity	(Optional) Enable to grant permissions using the Azure role-based access con- trol.
Microsoft Entra ID	
Login with AAD credentials (preview)	(Optional) Enable to use your corporate Active Directory credentials to log in to the virtual machine, enforce MFA, and enable access via RBAC roles.
Auto-shutdown	
Enable auto-shutdown	(Optional) Enable to automatically shut- down your virtual machine daily.

k

18. (Optional) Click the **Advanced** tab.

The **Advanced** page appears.

- (Optional) On the Advanced page, enter information for the Extensions, Cloud init, Host, and VM generation sections.
- 20. (Optional) Click the **Tags** tab.

The **Tags** page appears.

- 21. (Optional) On the **Tags** page, use the drop-down boxes to create tags to help categorize your resources.
- 22. Click **Review + Create**.

The **Create a virtual machine** page appears, and the system begins a validation process.

After the validation completes, a success message appears at the top of the screen.

23. Click Create.

Azure begins the virtual machine deployment.

After the validation completes, a success message appears.

The TenableCore WAS (BYOL) virtual machine is added to your **Resource Groups**.

What to do next:

• To complete the configuration, see <u>Deploy Tenable Core + Tenable Web App Scanning in</u> <u>Microsoft Azure</u> in the *Tenable Core for Tenable Web App Scanning* user guide.

Note: Microsoft does not require pre-approval to conduct vulnerability scans against Azure resources.

Web Application Scan

For instructions on creating a scan, see the <u>Create a Scan</u> section in the *Tenable Web App Scanning User Guide*.

Ø

Deploy a Nessus Scanner

View the following links for steps on how to deploy a Nessus Scanner with Microsoft Azure.

O

- Provision Tenable Core for Nessus (BYOL) in Azure Marketplace
- Install Nessus on an Azure virtual machine

Provision Tenable Core Nessus (BYOL) in Azure Marketplace

Tenable Core Nessus Bring Your Own License (BYOL) is an instance of Nessus installed in Microsoft Azure that allows you to scan Azure cloud environments and assets. Tenable Core Nessus (BYOL) features include vulnerability detection, compliance misconfiguration detection, and malware detection.

To provision a Tenable Core Nessus (BYOL) instance:

- 1. Log in to the Microsoft Azure portal.
- 2. In the left-hand menu, click + Create a resource.

The **New** page appears.

3. In the search box, type TenableCore Nessus (BYOL).

As you type, Tenable options appear.

4. Select the TenableCore Nessus (BYOL) option or press enter.

The TenableCore Tenable Nessus (BYOL) page appears.

Microsoft Azure	, P Search resources, services, and docs (G+/) 🗵 🗔 🖓 🛞 🧉	? 🙂	
«	Home > New > TenableCore Nessus (BYOL)		
+ Create a resource	TenableCore Nessus (BYOL)		\$ ×
🛧 Home	I E MARE		
💷 Dashboard	TenableCore Nessus (BYOL) 🗢 Save for later		
∃ All services	Tenable		
+ FAVORITES	Create Start with a pre-set configuration		
All resources	Want to deploy programmatically? Get started		
(🕥 Resource groups	With more than one million users, Nessus is the world's most widely-deployed vulnerability, configuration and compliance assessment product. Nessus prevents attacks by		A
🔇 App Services	identifying the vulnerabilities, configuration issues and malware that hackers could use to penetrate your network.		
🦘 Function App	With a continuously updated library of vulnerabilities and configuration issues, and the support of Tenable's expert security research team, Nessus delivers accuracy to the		
🗟 SQL databases	marketplace.		
🖉 Azure Cosmos DB	TenableCore is the virtual appliance platform we use as the base for many of our applications. TenableCore is a lightly customized version of CentOS 7. It has these major features:		
Virtual machines	SELinux Enabled		
🚸 Load balancers	 Configuration to meet some elements of the CIS Level 1 Benchmarks A GUI for configuration of a number of application and O/S features. 		
Storage accounts	Learn more about TenableCore with Nessus		
💮 Virtual networks	Learn more about Nessus and Microsoft Azure		
Azure Active Directory	Useful Links Find a Tenable Reseller		
Monitor	Tenable Community Forums		
🌪 Advisor	Tenable Nessus documentation Tenable Store		
Security Center	Tenable Video Tutorials TenableCore with Nessus		
💽 Cost Management + Bill			
P Help + support			-
Ŧ	v 4		۱.

5. Click the **Create** button.

The **Create a virtual machine** page appears.

 On the Basics tab, enter the required information for each option in the Project details, Instance details, and Administrator account sections.

Ø

Option	Description
Project Details	
Subscription	The account through which resources are reported and services are billed.
Resource Group	The collection of resources that share the same lifecycle, permissions, and policies.
Instance Details	
Virtual machine name	The name used for both, the virtual machine and host name.
	Note: The virtual machine name cannot be changed after the virtual machine is created. You can change the host name when you log into the virtual machine.
Region	The regional location most suitable for you and your cus- tomers.
	Note: Some virtual machine sizes are not available in cer- tain regions.
Availability options	(Optional) Additional options to help manage availability and resilience of your applications. Provides options to use replicated virtual machines in availability zones or availability settings to protect your applications and data from outages and maintenance events.
Image	The base operating system or application for the virtual machine.

Size	The virtual machine size to support the workload you want to run.
Administrator Account	
Authentication Type	The type of authentication the administrator uses - SSH or password.
Username	The administrator username for the virtual machine.
SSH Key	(Only available when you select SSH for Authentication Type) The single-line RSA public key or multi-line PEM cer- tificate.
	For additional information on setting up your SSH account, see <u>Create a Password for the Initial Admin</u> - <u>istrator User Account</u> .
Password	(Only available when you select Password for Authentic- ation Type) The administrator password for the virtual machine.
Confirm Password	(Only available when you select Password for Authentic- ation Type) Verification for the administrator password for the virtual machine.

R

7. Click the **Disks** tab.

The **Disks** page appears.

	~^					
Microsoft Azure	, P Search resources, services, and docs (G+/)	Þ	Ģ	@ ·	? ©	TENABLE, INC.
«	Home > New > TenableCore Nessus (BYOL) > Create a virtual machine					
+ Create a resource	Create a virtual machine					×
🛧 Home						
🛄 Dashboard	Basics Disks Networking Management Advanced Tags Review + create					
E All services	Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks.					
+ FAVORITES	The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more					
All resources	Disk options					
(🕥 Resource groups	* OS disk type ● Standard SSD ✓					
🔕 App Services	Enable Ultra Disk compatibility (Preview) 🛛 🔿 Yes 💿 No					
Function App	Ultra Disk compatibility is not available for this VM size and location.					
🧧 SQL databases	Data disks					
🖉 Azure Cosmos DB	You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.					
👤 Virtual machines	LUN NAME SIZE (GIB) DISK TYPE HOST CACHING					
💠 Load balancers	Create and attach a new disk Attach an existing disk					
Storage accounts	Create and attach a new disk — Attach an existing disk					
😔 Virtual networks						
Azure Active Directory	✓ Advanced					
Monitor						
🌪 Advisor						
Security Center						
💽 Cost Management + Bill	Review + create < Previous Next : Networking >					
P Help + support						
•	(

 \bigcirc

- 8. On the **Disks** page, in the **Disks option** section, select an **OS disk type** from the drop-down.
- 9. (Optional) In the **Data disks** section, you can add and configure additional data disks or attach existing disks.
- 10. Click the **Networking** tab.

The **Networking** page appears.

Microsoft Azure		𝒫 Search resources, services, and docs (G+/)	Þ	Ð	Q &		TENABLE, INC.
«	Home > New > TenableCore Nessus	(BYOL) > Create a virtual machine					
Create a resource	Create a virtual machine						×
🕈 Home							
🗖 Dashboard	Basics Disks Networking M	anagement Advanced Tags Review + create					
■ All services	Define network connectivity for your vi	tual machine by configuring network interface card (NIC) settings. You can control					
+ FAVORITES		ity with security group rules, or place behind an existing load balancing solution.					
All resources							
Resource groups	Network interface						
S App Services	When creating a virtual machine, a netw	vork interface will be created for you.					
Function App	* Virtual network 👩	Filter virtual networks					
SQL databases		Create new					
Azure Cosmos DB	Public IP 🚯	None v Create new					
Virtual machines	NIC network security group 🚯	None Basic Advanced					
Load balancers							
Storage accounts		1 This VM image has preconfigured NSG rules					
🐡 Virtual networks							
Azure Active Directory	* Configure network security group	×					
Monitor		Create new					
🜪 Advisor	Accelerated networking 🚯	 On Off The selected image does not support accelerated networking. 					
Security Center		5 11 5					
Oost Management + Bill	Review + create <	Previous Next : Management >					
Help + support		v					

 \bigcirc

- 11. In the **Virtual Network** drop-down box, select a network.
- 12. (Optional) Select a **Public IP** and **NIC network security group**.
- 13. In the **Configure network group** drop-down box, select a resource group.

Note: You can create a new group by clicking the **Create new** link beneath the drop-down box.

- 14. (Optional) Enable or disable **Accelerated networking** option.
- 15. (Optional) In the **Load balancing** option, select to place the virtual machine behind an existing load balancing solution.
- 16. Click the **Management** tab.

The **Management** page appears.

17. Enter your management preferences.

Options	Description
Monitoring	
Boot diagnostics	(Optional) Enable to capture the serial con-

	sole output and screenshots of the virtual machine running on a host.
OS guest diagnostics	(Optional) Enable to receive metrics for your virtual machine.
Diagnostic storage account	The account used to store your metrics.
Identity	
System assigned managed identity	(Optional) Enable to grant permissions using the Azure role-based access con- trol.
Microsoft Entra ID	
Login with AAD credentials (preview)	(Optional) Enable to use your corporate Active Directory credentials to log in to the virtual machine, enforce MFA, and enable access via RBAC roles.
Auto-shutdown	
Enable auto-shutdown	(Optional) Enable to automatically shut- down your virtual machine daily.

ð

18. (Optional) Click the **Advanced** tab.

The **Advanced** page appears.

- (Optional) On the Advanced page, enter information for the Extensions, Cloud init, Host, and VM generation sections.
- 20. (Optional) Click the **Tags** tab.

The **Tags** page appears.

21. (Optional) On the **Tags** page, use the drop-down boxes to create tags to help categorize your resources.

22. Click **Review + Create**.

The **Create a virtual machine** page appears, and the system begins a validation process.

23. Click Create.

Azure begins the virtual machine deployment.

After the validation completes, a success message appears.

The TenableCore Tenable Nessus (BYOL) virtual machine is added to your **Resource Groups**.

What to do next:

• To complete the configuration, see <u>Deploy Tenable Core + Nessus in Microsoft Azure</u> in the *Tenable Core + Nessus* user guide.

Note: Microsoft does not require pre-approval to conduct vulnerability scans against Azure resources.

Install Nessus on an Azure Virtual Machine

For instructions on installing Nessus, see the <u>Install Nessus</u> section in the *Nessus User Guide*.

0 -

Deploy One-Click Tenable Nessus Agent

Tenable now supports a one-click deployment of the Tenable Nessus Agent via the Microsoft Azure portal. This solution provides an easy way to install the latest version of Tenable Nessus Agent on Azure virtual machines (whether Linux or Windows) by either clicking on an icon within the Microsoft Azure Portal, or by writing a few lines of PowerShell script.

Before you begin:

- Ensure you have a Tenable Vulnerability Management (formerly known as Tenable.io), or Nessus Manager account.
- Ensure you have a Microsoft Azure account with one or more Windows or Linux virtual machines.

Deploy with the Microsoft Azure Portal and Tenable Vulnerability Management user interface:

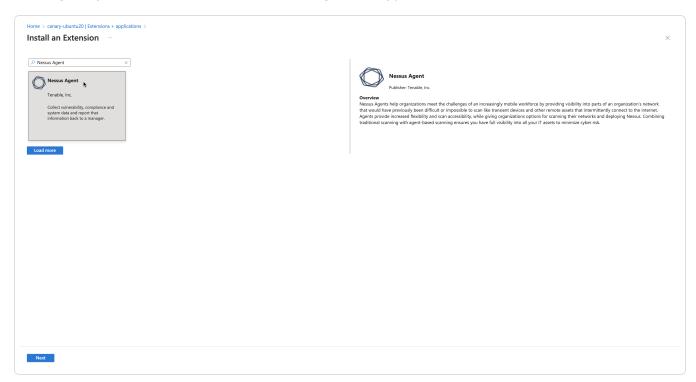
- 1. Log in to Microsoft Azure.
- 2. Select one of your virtual machines.

- Ø ------

3. In the left column click **Extensions + applications**.

		<u> </u>	
Q	Search		~~
Q	Overview		
-	Activity log		
ጽ	Access control (IAM)		
Ø	Tags		
Þ	Diagnose and solve problems		
Set	tings		
	Networking		
, CT	Connect		
8	Disks		
	Size		
0	Microsoft Defender for Cloud		
	Advisor recommendations		
	Extensions + applications		
Note: The second sec	Availability + scaling		
	Configuration		
	Identity		
111	Properties		
A	Locks		
Ор	erations		

- 4. Click **+ Add**.
- 5. In the gallery, scroll down to **N** (for Nessus Agent) or type *nessus* in the search bar.



- 6. Select the **Nessus Agent** tile and click **Next**.
- 7. Enter configuration parameters in the **Configure Nessus Agent Extension** user interface.

Agert Linking Key*	Create Review + create	
Link to: O Nessus Manager TVM Network O Lest Agent Identity Agent Name O NA_name1	Agent Linking	
Image: Tenable Vulnerability Management TVM Network ① test Agent Identity Agent Name ① NA_name1	Nessus Linking Key * 🛈	c7ea4dd7f16f0249fcd7e9591b74c3027f3768c738cbfe3ace6410a1553f 🗸
TVM Network ① test ✓ Agent Identity Agent Name ① NA_name1 ✓	Link to: 🛈	O Nessus Manager
Agent Identity Agent Name ① NA_name1 ~		Tenable Vulnerability Management
Agent Name ① NA_name1 ✓	TVM Network ①	test 🗸
Agent Name ① NA_name1 ✓	Agent Identity	
		NA name1
Agent Group U		

8. Click **Review + create**.

Deploy from the command-line interface:

You can deploy from the command-line interface available through PowerShell. For example, you can type:

```
PS> $publisherName="Tenable.NessusAgent"
PS> $typeName="Linux" (or $typeName="Windows")
PS> $name = $publisherName + "." + $typeName
PS> $version="1.0"
```

```
PS> $Settings = @{"nessusManagerApp" = "Cloud"; "nessusAgentName" = "example1";
"nessusAgentGroup" = "EXAMPLE1"}
PS> $ProtectedSettings = @{"nessusLinkingKey" =
"abcd1234vxyz5678abcd1234vxyz5678abcd1234vxyz5678abcd1234vxyz5678"}
PS> Set-AzVMExtension -ResourceGroupName "EXAMPLE-resource-group" -Location "East US 2"
-VMName "canary-example" -Name $name -Publisher $publisherName -ExtensionType $typeName
-TypeHandlerVersion $version -Settings $Settings -ProtectedSettings $ProtectedSettings
```

Note:Lines 1-4 identify the one-click agent extension. Lines 5-6 in the PowerShell example are equivalent to Step 5 in the user interface procedure. This is where you enter your configuration parameters for your Nessus Agent installation.

Nessus Linking Key

The most important field is the Nessus Linking Key (**nessusLinkingKey**). It is always required. For information on where to find the linking key, see <u>Retrieve the Tenable Nessus Agent Linking Key</u>. In the PowerShell interface, specify **nessusLinkingKey** under -ProtectedSettings so that Azure encrypts it. All other fields are passed unencrypted through -Settings. You can choose whether to link with Tenable Nessus Manager or Tenable Vulnerability Management (formerly known as Tenable.io). Do this by setting nessusManagerApp (**nessusManagerApp**) to cloud, or to local in the command-line interface. You have the following two choices:

- If you choose Tenable Nessus Manager, you must provide the Tenable Nessus Manager host (nessusManagerHost) and port number (nessusManagerPort). The extension accepts an IP address or fully qualified domain name.
- If you choose **Tenable.io** (Tenable Vulnerability Management), there is an optional field called **tenableloNetwork**.

The Agent Name (nessusAgentName) and Agent Group (nessusAgentGroup) are always optional.

Note: Both Agent Name and Agent Group are each a comma-separated list of group names.

For more definitions of these parameters, see <u>Nessuscli Agent</u>.

Parameters

Parameter names	Equivalent N

lent Nessuscli parameters 🛛 🛛 R

Required

	Õ	
nessusLinkingKey	key	yes
nessusManagerApp	N/A (unique to One-Click Agent)	yes
nessusManagerHost	host	no
nessusManagerPort	port	no
tenableIoNetwork	network	no
nessusAgentName	name	no
nessusAgentGroup	groups	no

_

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.