



Tenable and Microsoft Azure Integration Guide

Last Revised: March 06, 2024



Table of Contents

| | |
|---|-----------|
| Welcome to Tenable for Microsoft Azure | 3 |
| Microsoft Azure Sentinel | 4 |
| Audit Microsoft Azure | 19 |
| Configure Azure for a Compliance Audit | 20 |
| Audit Microsoft Azure in Tenable Vulnerability Management | 27 |
| Audit Microsoft Azure in Tenable Nessus | 30 |
| Tenable Vulnerability Management | 33 |
| Integration Requirements | 34 |
| Create a Scan | 35 |
| Nessus Agent Scan of Azure Virtual Instances | 36 |
| Deploy a Nessus Agent | 37 |
| Tenable Web App Scanning | 38 |
| Provision Tenable Core Web Application Scanner (BYOL) | 39 |
| Web Application Scan | 46 |
| Deploy a Tenable Nessus Scanner | 47 |
| Provision Tenable Core Nessus (BYOL) in Azure Marketplace | 48 |
| Install Nessus on an Azure Virtual Machine | 55 |
| Deploy One-Click Tenable Nessus Agent | 56 |
| About Tenable | 63 |



Welcome to Tenable for Microsoft Azure

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

Additional benefits of integrating Tenable with Microsoft 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 [Microsoft Azure Connector](#) 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 [Microsoft documentation](#).

Required User Role: Basic User

Note: The Tenable integration with Microsoft Azure Sentinel works with a **Basic User** if that user is assigned **Can View** permissions on the assets they are to export, along with **Can Use** permissions on tags the assets are assigned. Without the **Can Use** tag permissions, the assets return undefined or the integration fails to export vulnerabilities if a tag filter is used. For more information on Tenable Vulnerability Management permissions and user roles, refer to [Permissions](#) in the *Tenable Developer Portal*.

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](#).

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

Create the Log Analytics Workspace.

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

The workspace homepage appears:



Microsoft Azure

Search resources, services, and docs (G+)

Home >


Microsoft Sentinel

Default Directory (bradley76hotmail.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query View incidents

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 0 to 0 of 0 records.

| Name | Resource group | Location | Subscr |
|---|----------------|----------|--------|
| <div><h3>No Microsoft Sentinel to display</h3><p>See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise.</p><p>Create Microsoft Sentinel</p><p>Learn more</p></div> | | | |

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

Microsoft Azure

Search resources, services, and docs (G+)


Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace

+ Create a new workspace Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...



No workspaces found

[Create a new workspace](#)



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

Microsoft Azure

Search resources, services, a

[Home](#) > [Microsoft Sentinel](#) > [Add Microsoft Sentinel to a workspace](#) >

Create Log Analytics workspace

Basics

Tags

Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations 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 monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Azure subscription AB

Resource group * ⓘ

Create new

Instance details

Name * ⓘ

Region * ⓘ

A resource group is a container that holds related resources for an Azure solution.

Name *

tenable-integration ✓

OK

Cancel

Review + Create

« Previous

Next : Tags >



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

Click **Review + Create**.

The settings are finalized and the page updates:



Microsoft Azure


Search resources, services

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >

Create Log Analytics workspace

Validation passed

BasicsTagsReview + Create

Log Analytics workspace
by Microsoft

Basics

SubscriptionAzure subscription AB

Resource grouptenable-integration

Nametenable-integration

RegionAustralia Southeast

Pricing

Pricing tierPay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created. [Learn more about Log Analytics pricing models](#).

Tags

None

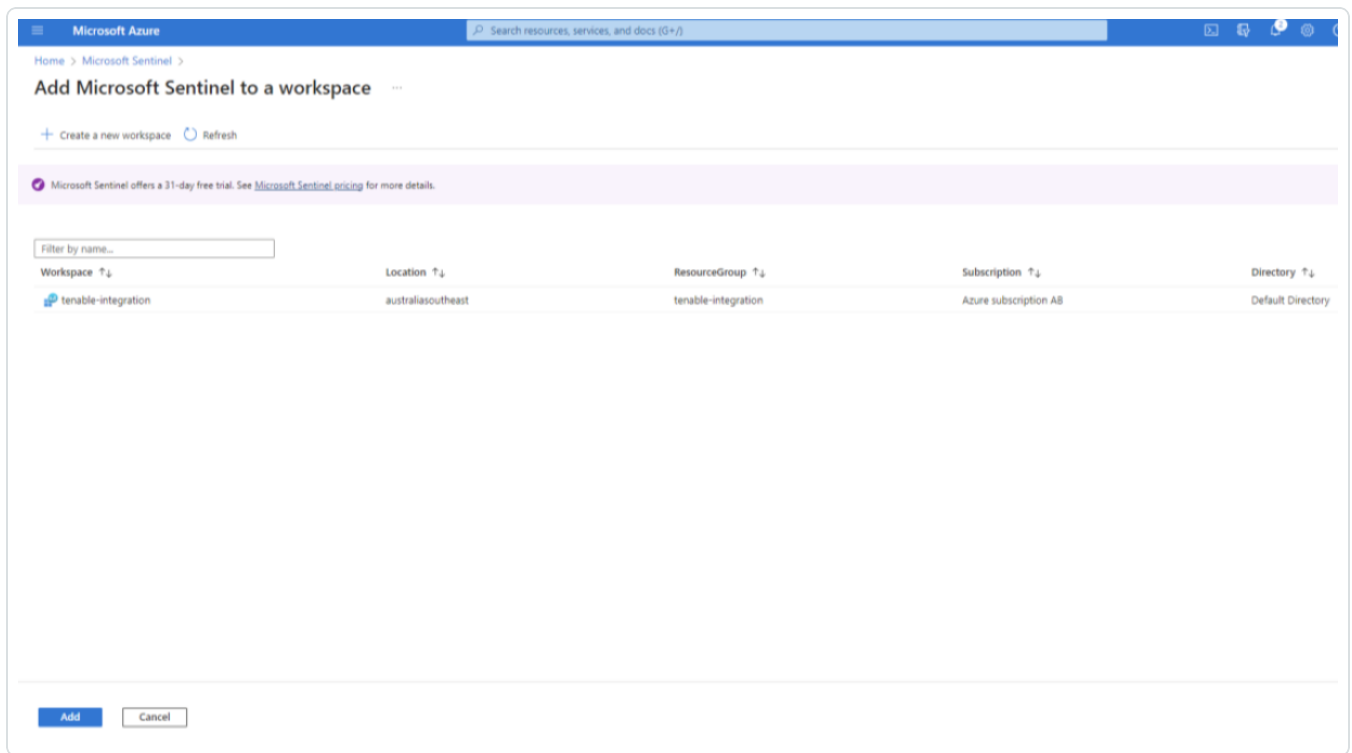
Create

« Previous

[Download a template for automation](#)

5. Click **Create**.

The workspace homepage appears with your new Microsoft Sentinel workspace:



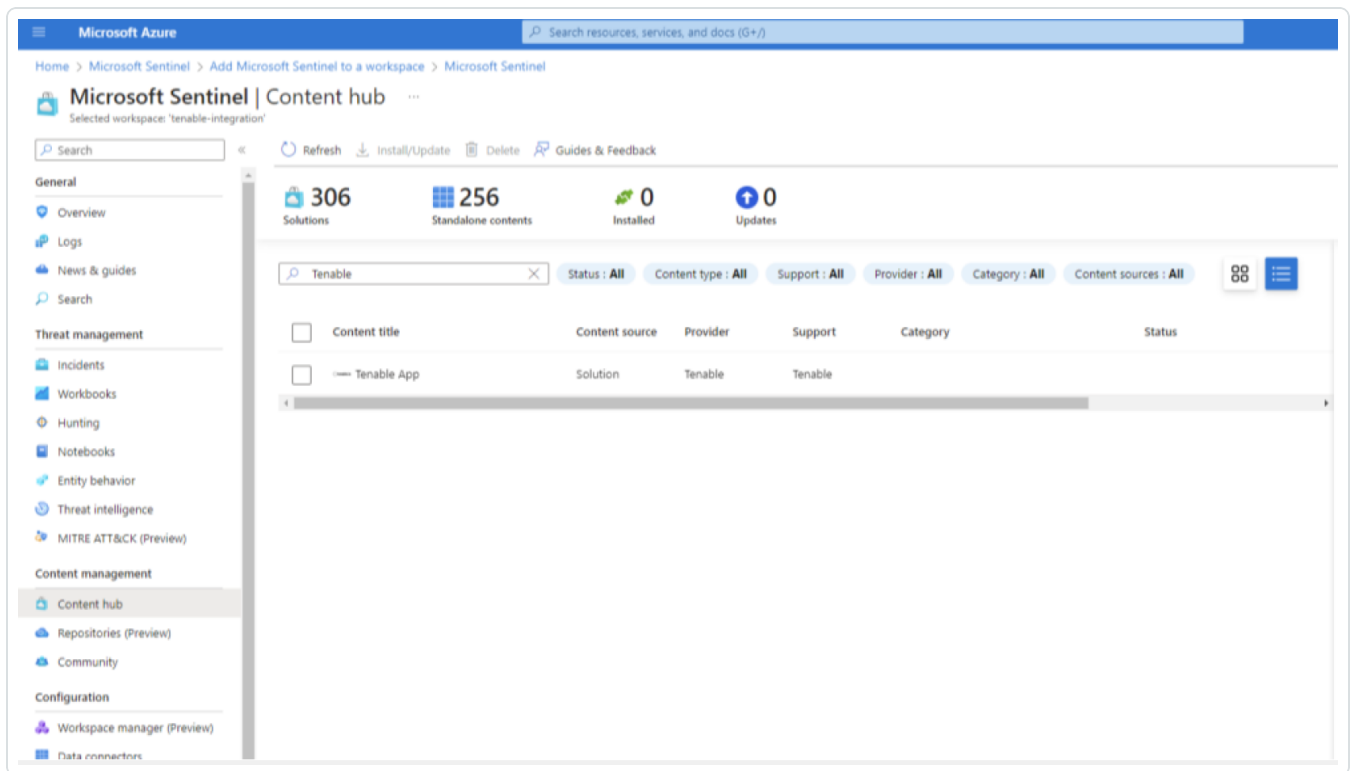
The Log Analytics Workplace for Microsoft Sentinel has been created.

Note: Navigate to **Log Analytics workspace > Network Isolation** and ensure that the two **Virtual network access configuration settings** (required to accept data ingestion and queries from public networks not connected through a Private Link Scope) are set to **Yes**.

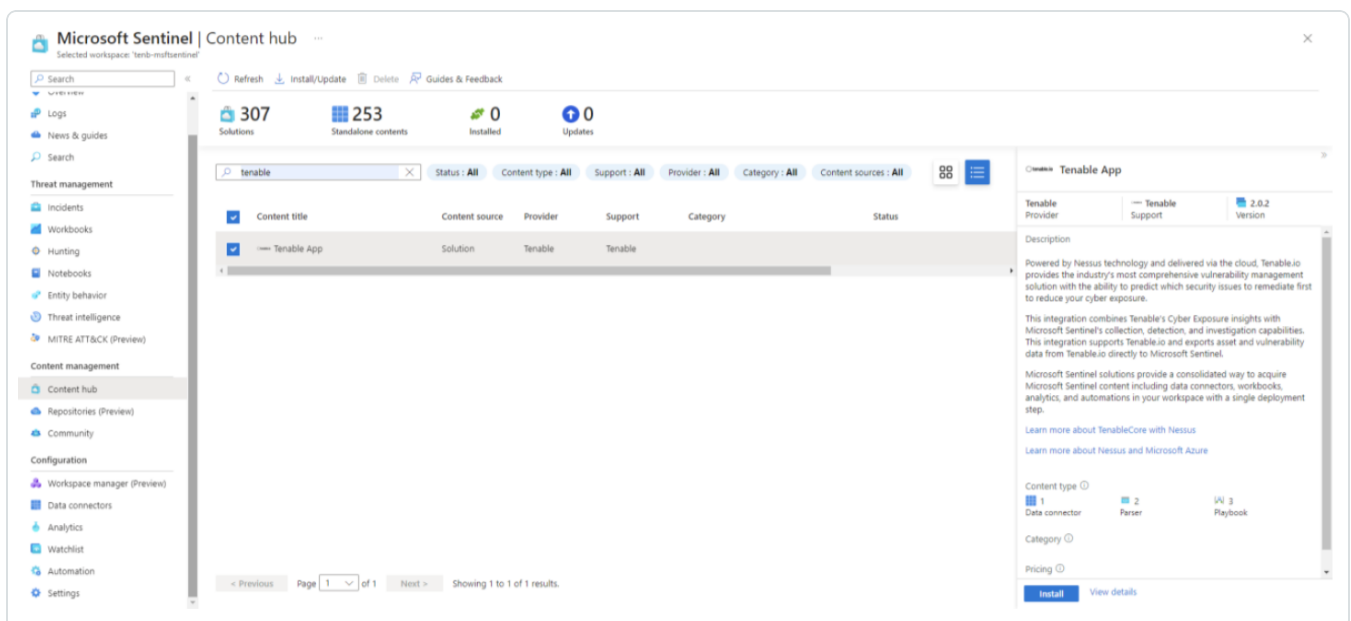
Add the Tenable App to Microsoft Sentinel.



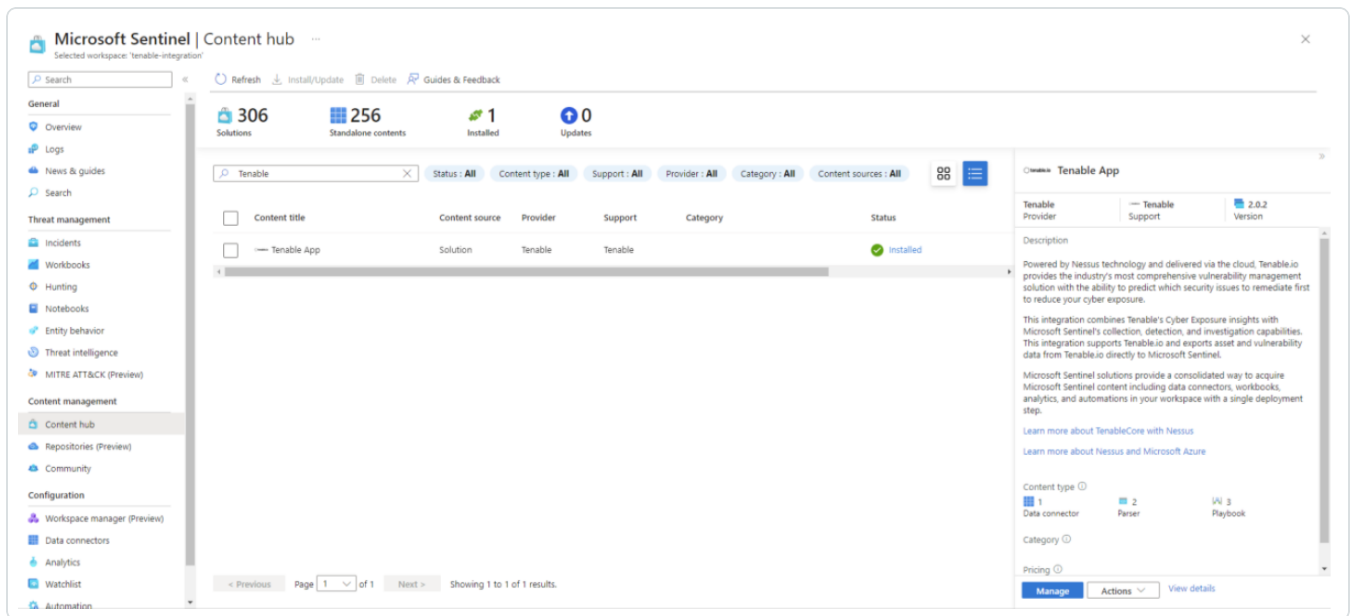
1. Go to the Content Hub and perform a search for "Tenable."



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

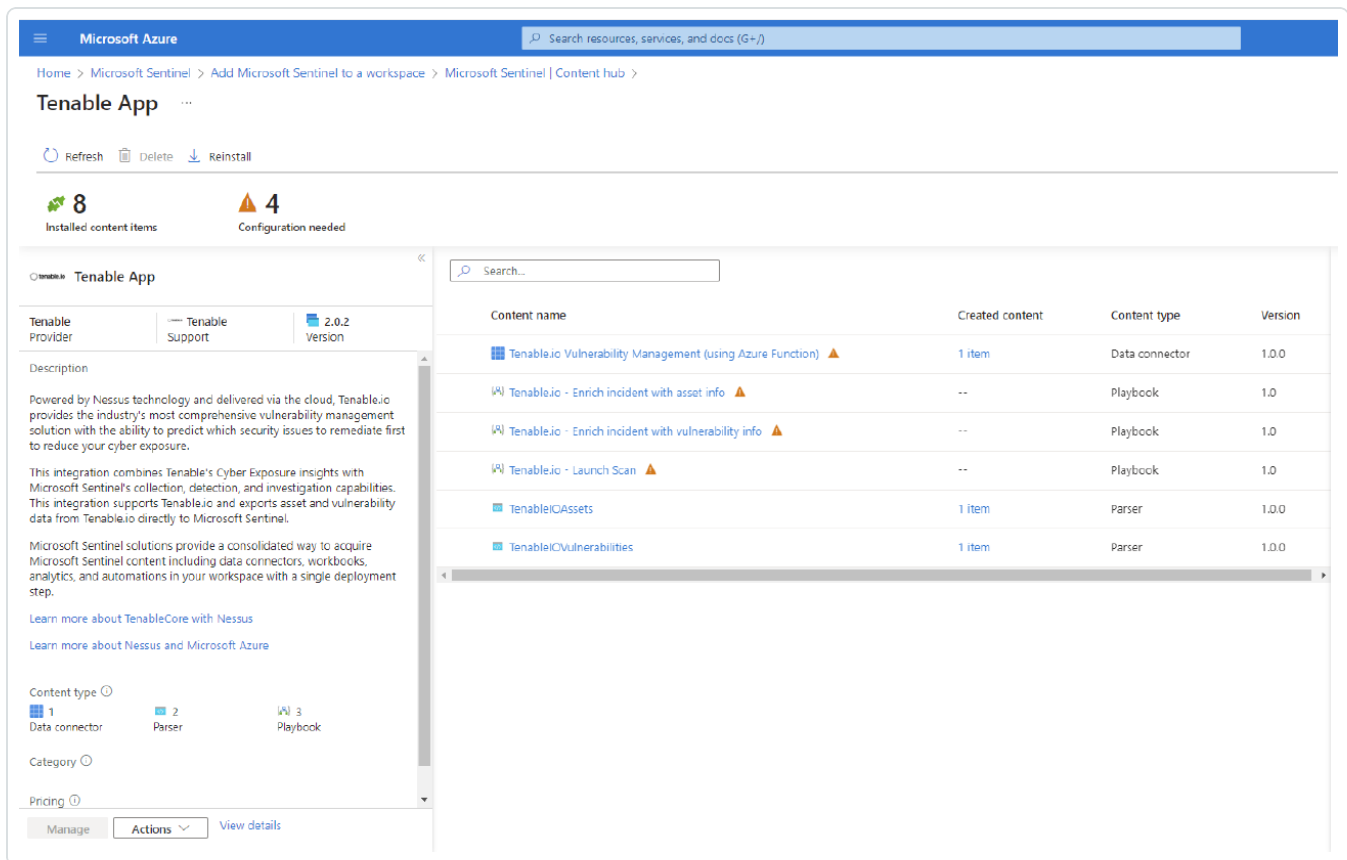


3. Once installed, in the bottom-right corner, click **Manage**.



Deploy the data connector.

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



Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub >

Tenable App

Refresh Delete Reinstall

8 Installed content items 4 Configuration needed

Tenable App

Tenable Provider Tenable Support 2.0.2 Version

Description

Powered by Nessus technology and delivered via the cloud, Tenable.io provides the industry's most comprehensive vulnerability management solution with the ability to predict which security issues to remediate first to reduce your cyber exposure.

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

Microsoft Sentinel solutions provide a consolidated way to acquire Microsoft Sentinel content including data connectors, workbooks, analytics, and automations in your workspace with a single deployment step.

[Learn more about TenableCore with Nessus](#)

[Learn more about Nessus and Microsoft Azure](#)

Content type

1 Data connector 2 Parser 3 Playbook

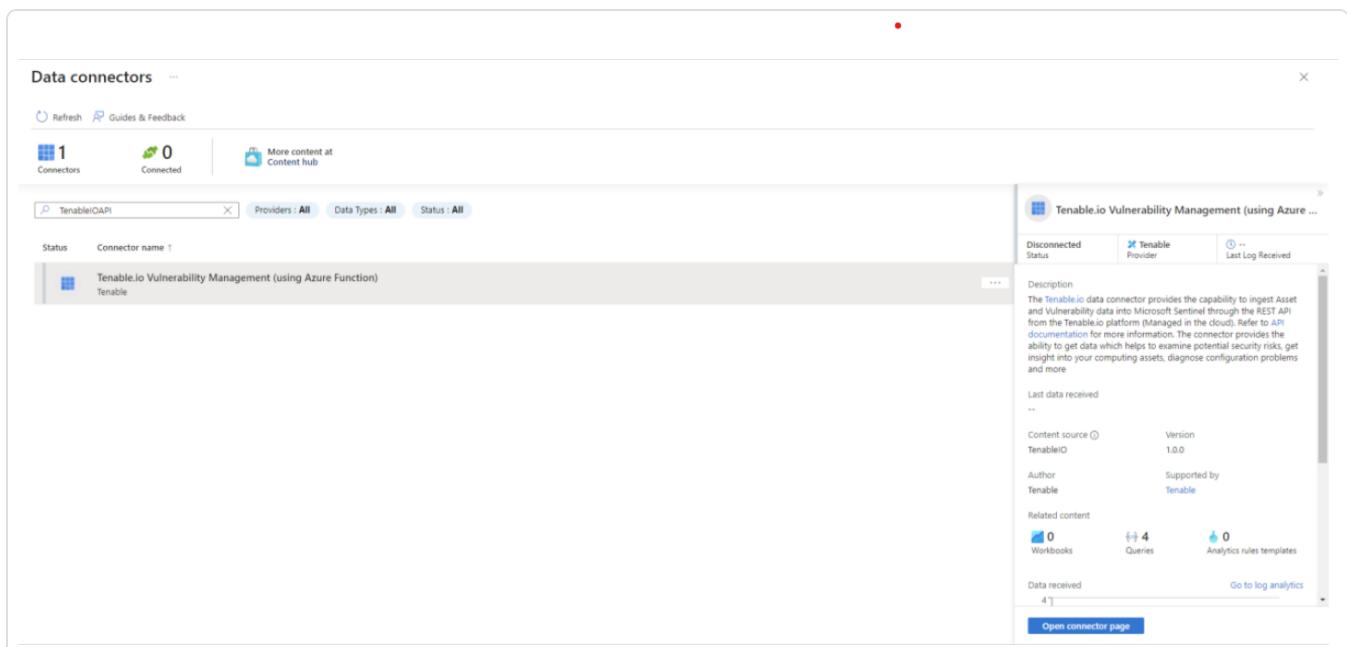
Category

Pricing

Manage Actions View details

| Content name | Created content | Content type | Version |
|--|-----------------|----------------|---------|
| Tenable.io Vulnerability Management (using Azure Function) | 1 item | Data connector | 1.0.0 |
| Tenable.io - Enrich incident with asset info | -- | Playbook | 1.0 |
| Tenable.io - Enrich incident with vulnerability info | -- | Playbook | 1.0 |
| Tenable.io - Launch Scan | -- | Playbook | 1.0 |
| TenableIOAssets | 1 item | Parser | 1.0.0 |
| TenableIOVulnerabilities | 1 item | Parser | 1.0.0 |

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



Data connectors

Refresh Guides & Feedback

1 Connectors 0 Connected More content at Content hub

TenableIOAPI Providers: All Data Types: All Status: All

| Status | Connector name | Provider |
|--------------|--|----------|
| Disconnected | Tenable.io Vulnerability Management (using Azure Function) | Tenable |

Tenable.io Vulnerability Management (using Azure ...)

Disconnected Status Tenable Provider Last Log Received

Description

The Tenable.io data connector provides the capability to ingest Asset and Vulnerability data into Microsoft Sentinel through the REST API from the Tenable.io platform (Managed in the cloud). Refer to API documentation for more information. The connector provides the ability to get data which helps to examine potential security risks, get insight into your computing assets, diagnose configuration problems and more

Last data received

--

Content source

TenableIO Version 1.0.0

Author Tenable Supported by Tenable

Related content

0 Workbooks 4 Queries 0 Analytics rules templates

Data received 4 Go to log analytics

Open connector page

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



Microsoft Azure

Search resources, services, and docs (G+/J)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Content hub > Tenable App > Data connectors >

Tenable.io Vulnerability Management (using Azure Function) ...

Delete

Tenable.io Vulnerability Management (using Azure ...

Disconnected Status Tenable Provider Last Log Received

Description

The Tenable.io data connector provides the capability to ingest Asset and Vulnerability data into Microsoft Sentinel through the REST API from the Tenable.io platform (Managed in the cloud). Refer to [API documentation](#) for more information. The connector provides the ability to get data which helps to examine potential security risks, get insight into your computing assets, diagnose configuration problems and more

Last data received

--

Content source ⓘ TenableIO Version 1.0.0

Author Tenable Supported by Tenable

Related content

0 Workbooks 4 Queries 0 Analytics rules templates

Data received

Go to log analytics

4 3 2 1

Option 1 - Azure Resource Manager (ARM) Template

Use this method for automated deployment of the Tenable.io Vulnerability Management Report data connector using an ARM Template.

1. Click the **Deploy to Azure** button below.

Deploy to Azure

2. Select the preferred **Subscription**, **Resource Group** and **Location**.
NOTE: Within the same resource group, you can't mix Windows and Linux apps in the same region. Select existing resource group without Windows apps in it or create new resource group.
3. Enter the **TenableAccessKey** and **TenableSecretKey** and deploy.
4. Mark the checkbox labeled **I agree to the terms and conditions stated above**.
5. Click **Purchase** to deploy.

Option 2 - Manual Deployment of Azure Functions

Use the following step-by-step instructions to deploy the Tenable.io Vulnerability Management Report data connector manually with Azure Functions (Deployment via Visual Studio Code).

1. Deploy a Function App

NOTE: You will need to prepare VS code for Azure function development.

1. Download the **Azure Function App** file. Extract archive to your local development computer.
2. Start VS Code. Choose File in the main menu and select Open Folder.
3. Select the top level folder from extracted files.
4. Choose the Azure icon in the Activity bar, then in the **Azure: Functions** area, choose the **Deploy to function app** button.
If you aren't already signed in, choose the Azure icon in the Activity bar, then in the **Azure: Functions** area, choose **Sign in to Azure**.
If you're already signed in, go to the next step.
5. Provide the following information at the prompts:
 - a. **Select folder:** Choose a folder from your workspace or browse to one that contains your function app.
 - b. **Select Subscription:** Choose the subscription to use.
 - c. Select **Create new Function App in Azure** (Don't choose the Advanced option)

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**.

Microsoft Azure

Search resources, services, and

Home >

Custom deployment

...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Template

Customized template

8 resources

Edit template

Edit parameters

Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure subscription AB

Resource group *

tenable-integration

Create new

Instance details

Region *

(Asia Pacific) Australia Southeast

Function Name

TenableID

Workspace ID *

.....

Workspace Key *

.....

Tenable Access Key *

.....

Tenable Secret Key *

.....

Tenable Export Schedule In Minutes

720

Previous

Next

Review + create

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

Microsoft Azure

Search resources, services, and do

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 | |
| Tenable Access Key | |
| Tenable Secret Key | |
| Tenable Export Schedule In Minutes | 720 |

Previous

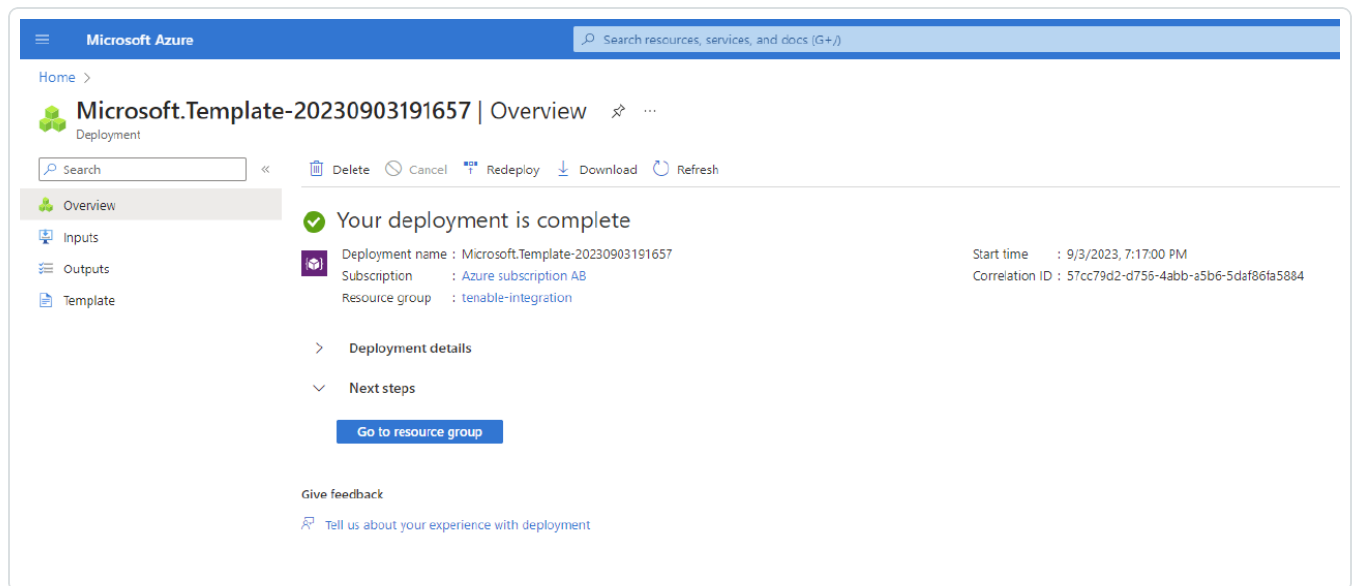
Next

Create

Check for the resources.

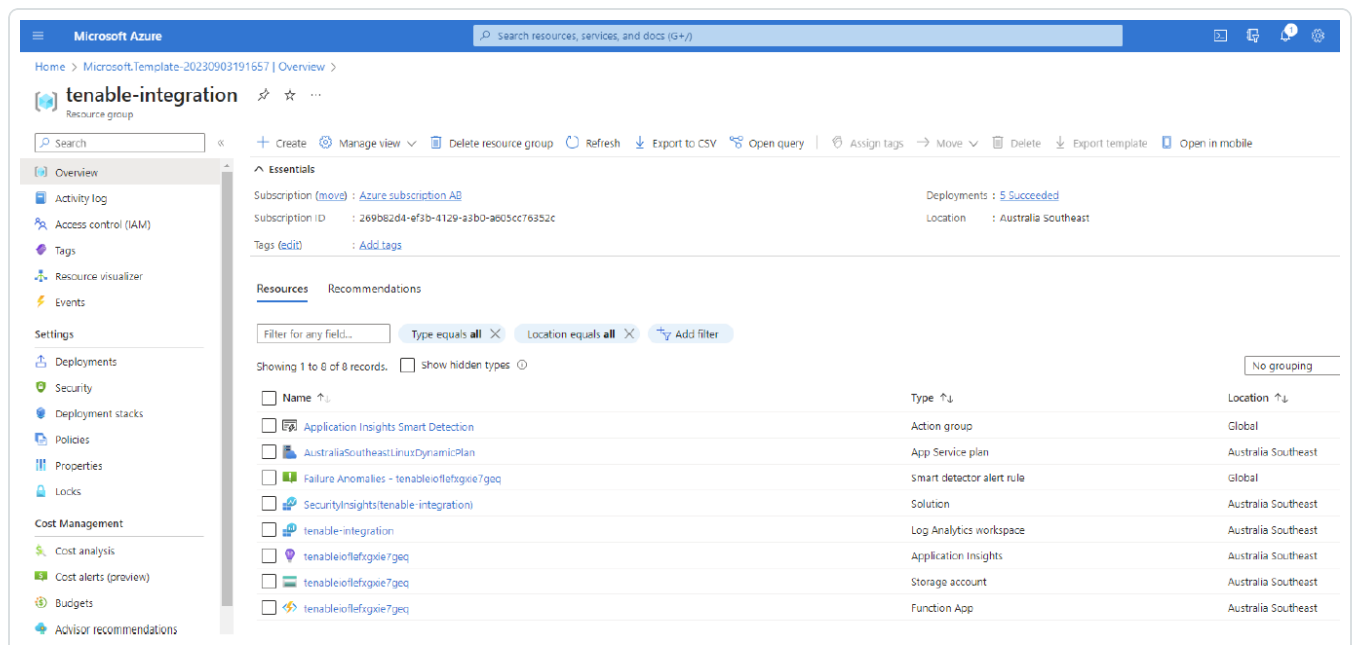
- 16 -

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



2. The app populates the following resources:

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



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



tenableiowp6klc5ukgmme

Function App

Search

+ Create

Set up local environment

Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Microsoft Defender for Cloud

Events (preview)

Functions

App keys

App files

Proxies

Deployment

Deployment slots

Deployment Center

Settings

Configuration

Authentication

Application insights

Identity

Backups

Custom domains

Certificates

Networking

Filter by name...

| Name | Trigger | Status | Monitor |
|---|---------------|---------|---------------------------|
| TenableAssetExportOrchestrator | Orchestration | Enabled | Orchestration information |
| TenableAssetExportStatusAndSendChunks | Activity | Enabled | Invocations and more |
| TenableCleanTables | Activity | Enabled | Invocations and more |
| TenableCleanupOrchestrator | Orchestration | Enabled | Orchestration information |
| TenableExportsOrchestrator | Orchestration | Enabled | Orchestration information |
| TenableExportStarter | Timer | Enabled | Invocations and more |
| TenableGenerateJobStats | Activity | Enabled | Invocations and more |
| TenableProcessAssetChunkFromQueue | Queue | Enabled | Invocations and more |
| TenableProcessFailedAssetChunkFromQueue | Queue | Enabled | Invocations and more |
| TenableProcessFailedVulnChunkFromQueue | Queue | Enabled | Invocations and more |
| TenableProcessVulnChunkFromQueue | Queue | Enabled | Invocations and more |
| TenableStartAssetExportJob | Activity | Enabled | Invocations and more |
| TenableStartVulnExportJob | Activity | Enabled | Invocations and more |
| TenableVulnExportOrchestrator | Orchestration | Enabled | Orchestration information |
| TenableVulnExportStatusAndSendChunks | Activity | Enabled | Invocations and more |



Audit Microsoft Azure

To audit Microsoft Azure, do the following:

- Configure Microsoft Azure for use with a compliance audit, as described in [Configure Azure \(Compliance Audit\)](#).
- 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 [Microsoft Azure Audit Compliance Reference](#) 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 [Assign API Permissions](#) 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 to the Reader Role



1. Click **Subscriptions > Your Subscription > Access Control (IAM) > Role Assignments > + Add**.
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 [Microsoft Azure](#) 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**.



Azure Active Directory



Overview



Preview features



Diagnose and solve problems

Manage



Users



Groups



External Identities



Roles and administrators



Administrative units



Enterprise applications



Devices



App registrations



Identity Governance



Application proxy



Licenses



Azure AD Connect



Custom domain names



Mobility (MDM and MAM)



Password reset



Company branding



User settings

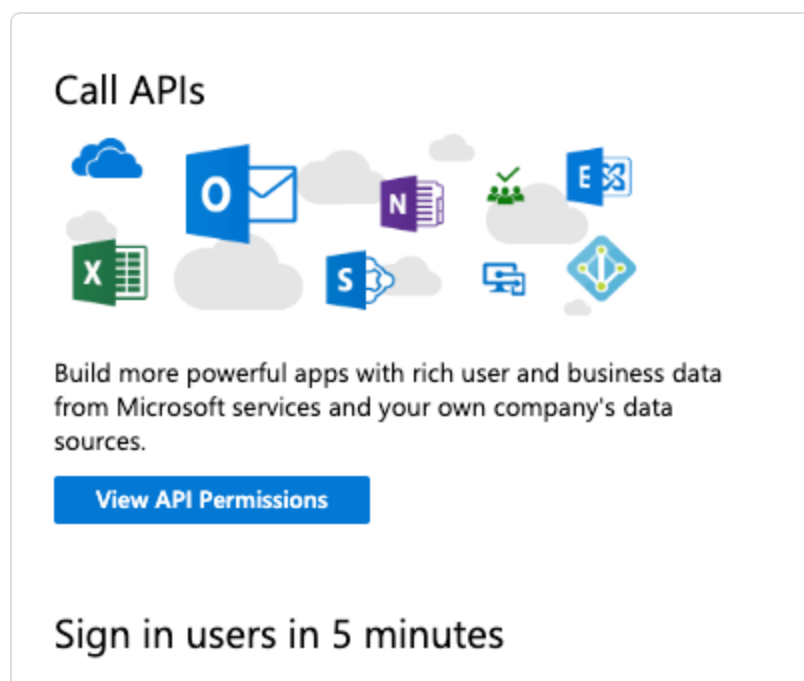


2. Click **New Registrations application**.
3. Give the application a name.
4. Choose the supported account types for your environment.
5. Click **Register**.
6. Click **Authentication**.
7. Choose **Yes** for **Default Client Type/Treat application as a public client**.

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 | Type | 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.Reac | Application | Read Microsoft Intune apps | Yes | ✔ Granted for Bob Corp |
| DeviceManagementConfigural | 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:

- [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 the [Microsoft Azure Audit Compliance Reference](#) 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 Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the ☰ 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 ⊕ **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 the [Microsoft Azure Audit Compliance Reference](#) 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 [Required User Privileges](#) section in the Nessus User Guide for the required Microsoft Azure privileges.

14. 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 Tenant ID or Directory ID for your Azure environment. | 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 |

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 [Tenable Vulnerability Management User Guide](#).



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 the [Microsoft Azure Audit Compliance Reference](#) 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 ☰ 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 ⊕ **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.

10. Click the **Authentication Method** drop-down menu to select your preferred authentication method: **key** or **password**.
11. Configure the credentials for your selected authentication method.

To configure key authentication:

| Option | Description | Required |
|------------------|--|----------|
| Tenant ID | The Tenant ID or Directory ID for your Azure environment. | 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 the [Microsoft Azure Audit Compliance Reference](#) 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 Tenable Nessus scans, refer to the [Tenable Nessus User Guide](#).



Tenable Vulnerability Management

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

- [Requirements](#)
- [Create a Scan](#)
- [Nessus Agent Scan](#)
- [Deploy a Nessus Agent](#)



Integration Requirements

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

- **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.



Create a Scan

Create a Tenable Vulnerability Management Scan

For instructions on creating a scan, see [Create a Scan](#) in the *Tenable Vulnerability Management User Guide*.

Create an Agent Scan

For instructions on creating an Agent scan, see [Create an Agent Scan](#) 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 [Tenable Downloads site](#), 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 targets 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. Before 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.

The screenshot displays the 'Agents' section of the Nessus interface. On the left, a sidebar shows a tree view of folders and resources, with 'Agents' selected. The main content area is titled 'Agents' and includes tabs for 'Linked Agents', 'Agent Groups', 'Blackout Windows', and 'Agent Settings'. Below the tabs, there is a section for 'Linked Agents' with a description and a 'Linking Key' field. A table below lists the linked agents, all of which are 'Offline'.

| Name | Status | IP Address | Platform | Groups | Version | Last Plugin Update | Last Scanned |
|-------------------------|---------|---------------|----------------------|-------------------------|---------|--------------------|--------------|
| 8bae46cd-4a10-44a1-... | Offline | N/A | Windows (win-x86-64) | N/A | N/A | N/A | N/A |
| 9488f67c-d668-41f2-8... | Offline | N/A | Windows (win-x86-64) | N/A | N/A | N/A | N/A |
| Server2012R2 | Offline | 172.26.38.65 | Windows (win-x86-64) | qa-agent, windows ag... | N/A | N/A | April 6 |
| Win81 | Offline | 172.26.37.79 | Windows (win-x86-64) | qa-agent, windows ag... | N/A | N/A | April 6 |
| WINDOWS10ANNIVE | Offline | 172.26.36.82 | Windows (win-x86-64) | qa-agent, windows ag... | N/A | N/A | April 6 |
| WINDOWS732 | Offline | 172.26.36.216 | Windows (win-x86) | qa-agent, windows ag... | N/A | N/A | April 6 |

For more information on installing and configuring Nessus Agents, refer to the [Nessus User Guide](#).



Deploy a Nessus Agent

For instructions on deploying a Nessus Agent, see the [Nessus Agent Deployment](#) section in the *Nessus Agent and Deployment and User Guide*.



Tenable Web App Scanning

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

- [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**.

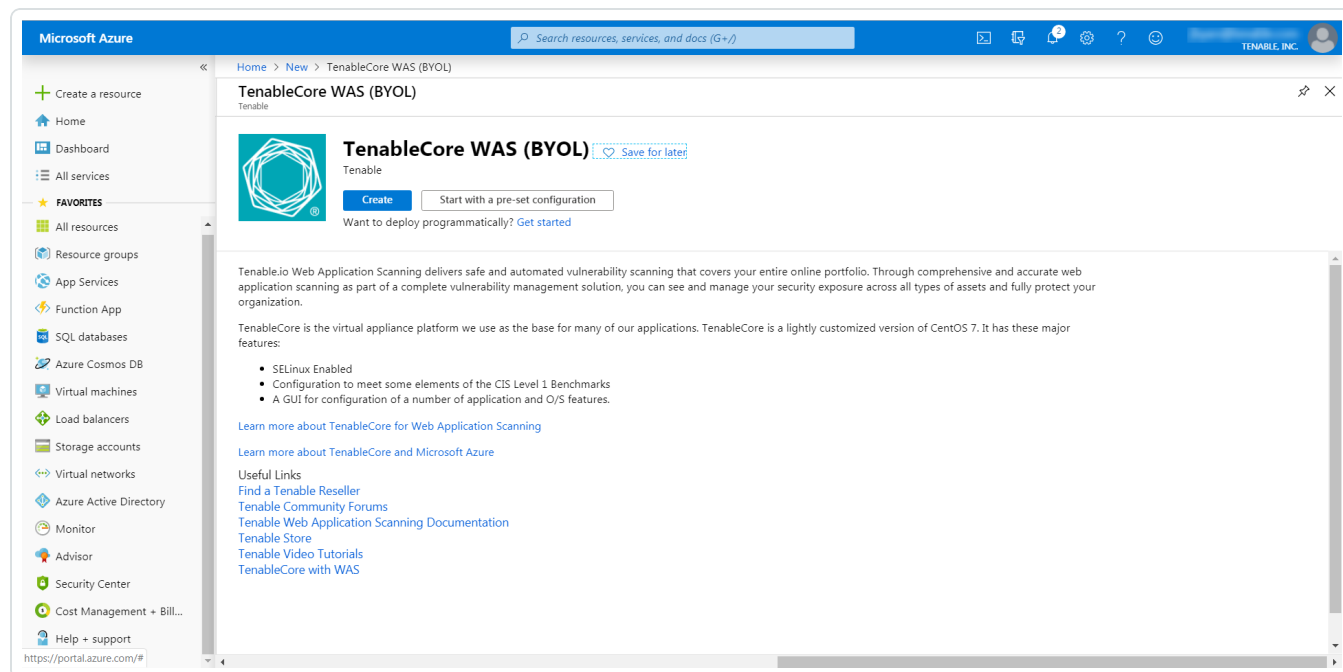
The **New** page appears.

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.





5. Click the **Create** button.

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

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

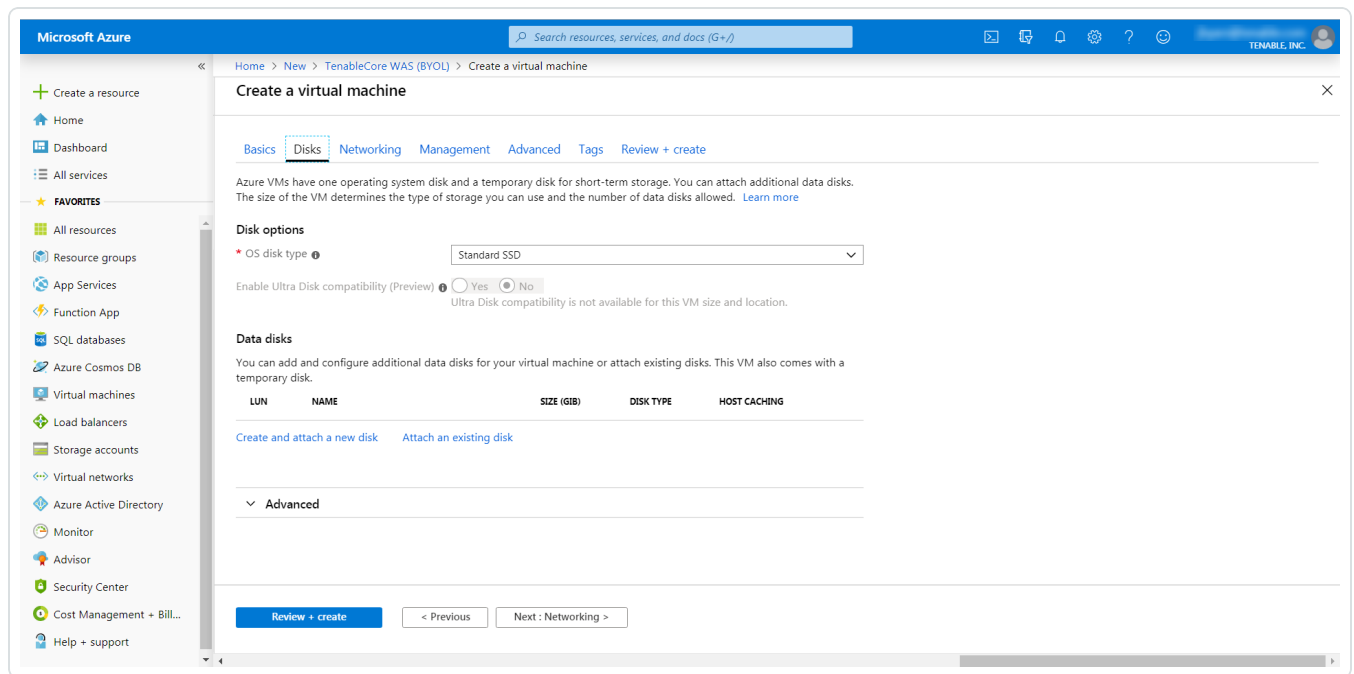
| Option | Description |
|----------------------|--|
| Project Details | |
| Subscription | The account through which resources are reported and services are billed. |
| Resource Group | The collection of resources that share the same lifecycle, permissions, and policies. |
| Instance Details | |
| Virtual machine name | <p>The name used for both, the virtual machine and host name.</p> <div>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.</div> |
| Region | <p>The regional location most suitable for you and your customers.</p> <div>Note: Some virtual machine sizes are not available in certain regions.</div> |
| 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 | <p>(Only available when you select SSH for Authentication Type) The single-line RSA public key or multi-line PEM certificate.</p> <p>For additional information on setting up your SSH account, see Create a Password for the Initial Administrator User Account.</p> |
| Password | (Only available when you select Password for Authentication Type) The administrator password for the virtual machine. |
| Confirm Password | (Only available when you select Password for Authentication Type) Verification for the administrator password for the virtual machine. |

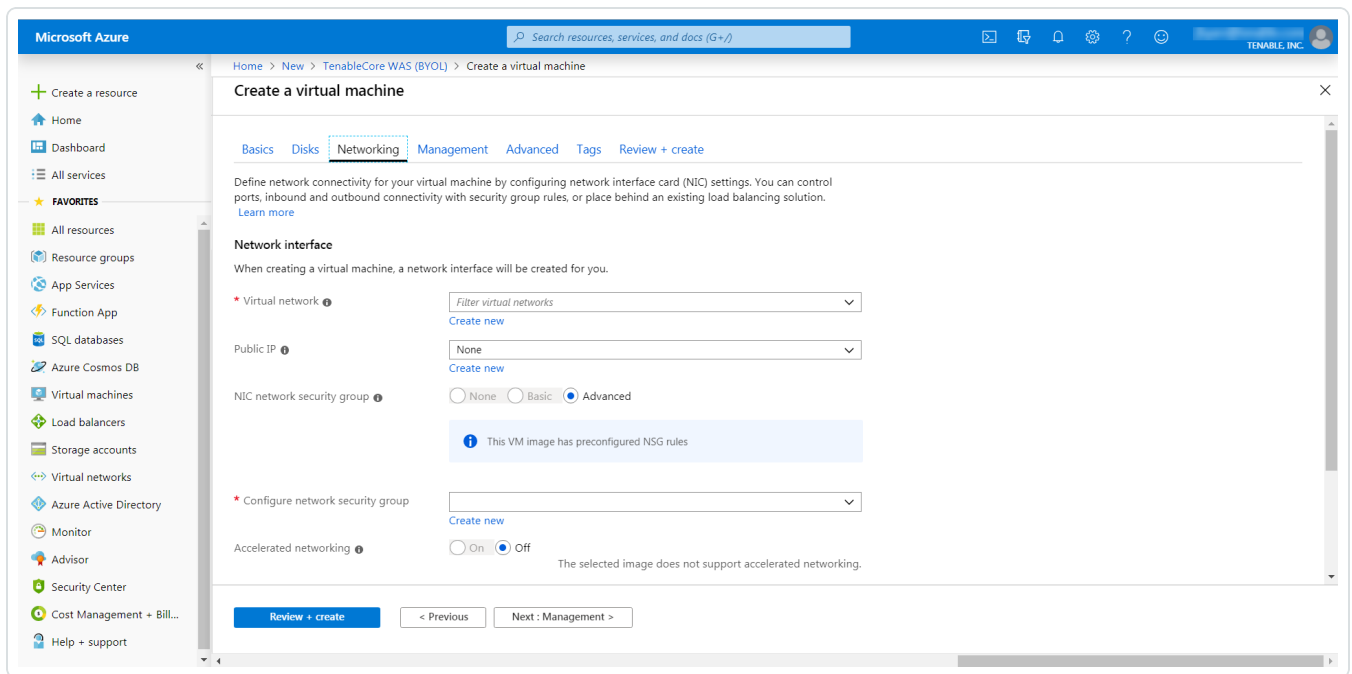
7. Click the **Disks** tab.

The **Disks** page appears.



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.



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 |



| | |
|--------------------------------------|---|
| | console 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 control. |
| 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 shutdown your virtual machine daily. |

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

The **Advanced** page appears.

19. (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 [Deploy Tenable Core + Tenable Web App Scanning in Microsoft Azure](#) 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 [Create a Scan](#) section in the *Tenable Web App Scanning User Guide*.



Deploy a Tenable Nessus Scanner

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

- [Provision Tenable Core for Nessus \(BYOL\) in Azure Marketplace](#)
- [Install Nessus on an Azure virtual machine](#)
- [Deploy One-Click Nessus Agent](#)



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**.

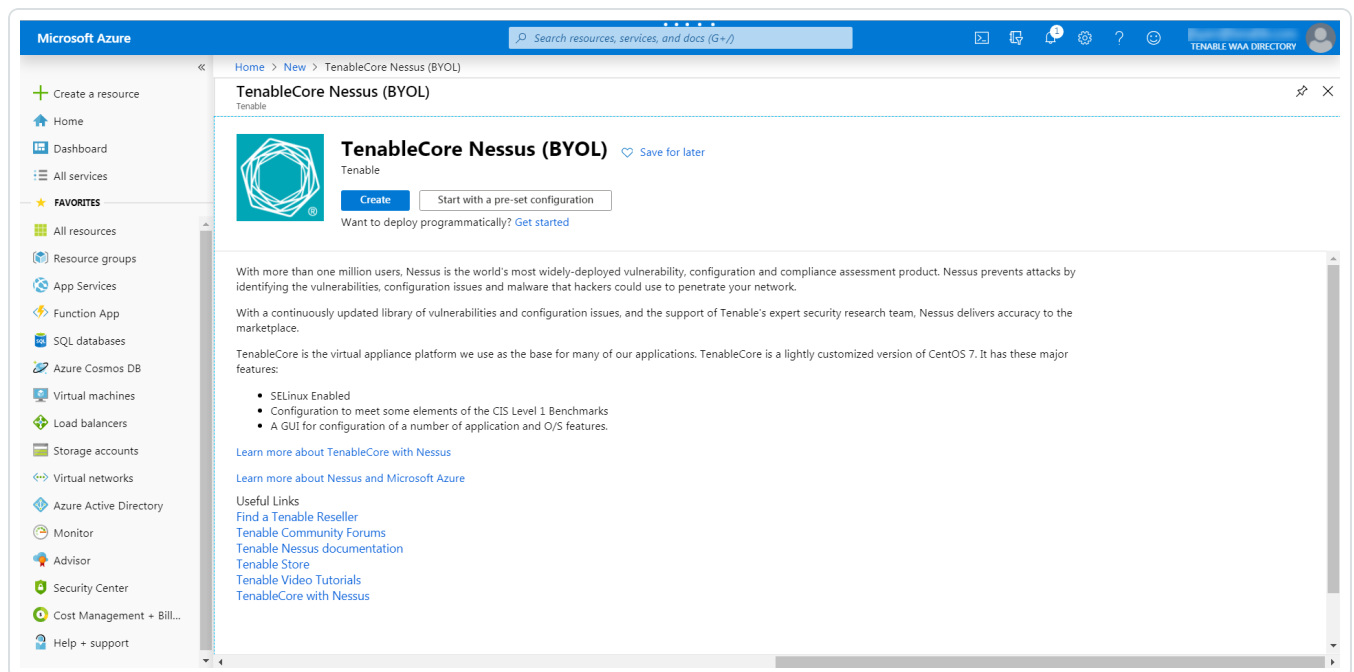
The **New** page appears.

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.





5. Click the **Create** button.

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

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

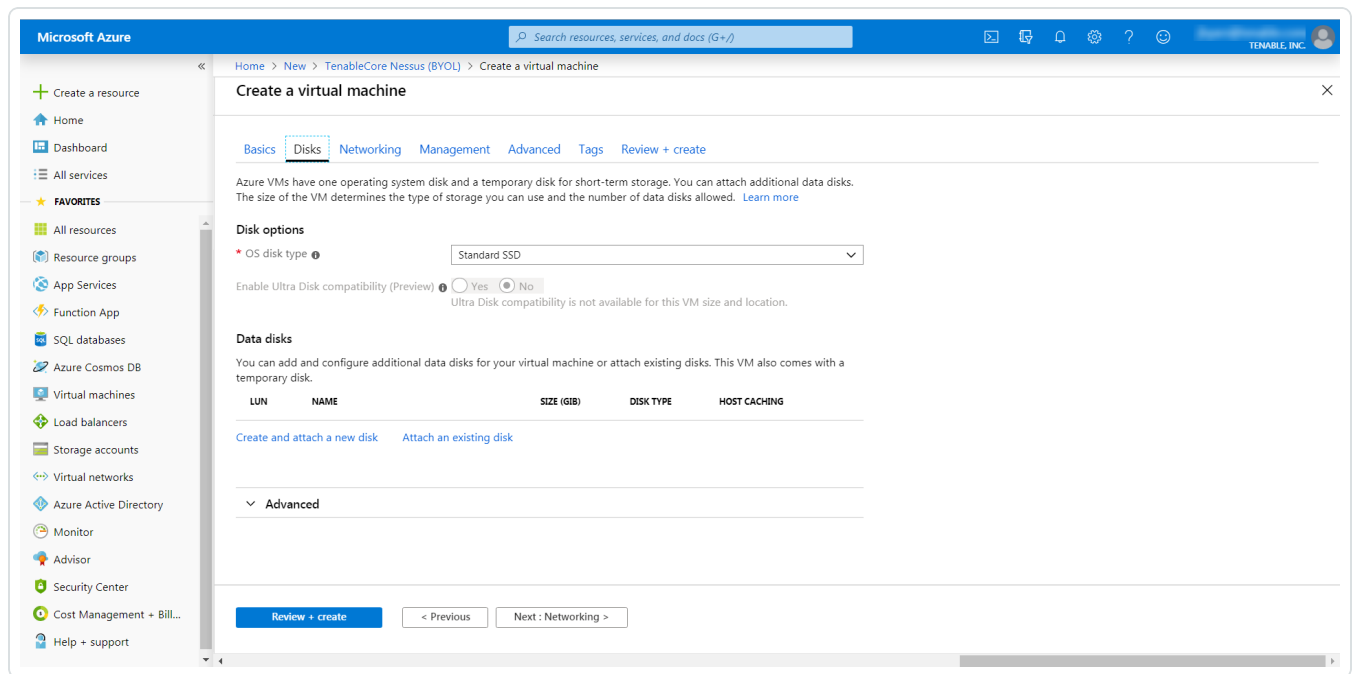
| Option | Description |
|----------------------|--|
| Project Details | |
| Subscription | The account through which resources are reported and services are billed. |
| Resource Group | The collection of resources that share the same lifecycle, permissions, and policies. |
| Instance Details | |
| Virtual machine name | <p>The name used for both, the virtual machine and host name.</p> <div>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.</div> |
| Region | <p>The regional location most suitable for you and your customers.</p> <div>Note: Some virtual machine sizes are not available in certain regions.</div> |
| 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 | <p>(Only available when you select SSH for Authentication Type) The single-line RSA public key or multi-line PEM certificate.</p> <p>For additional information on setting up your SSH account, see Create a Password for the Initial Administrator User Account.</p> |
| Password | (Only available when you select Password for Authentication Type) The administrator password for the virtual machine. |
| Confirm Password | (Only available when you select Password for Authentication Type) Verification for the administrator password for the virtual machine. |

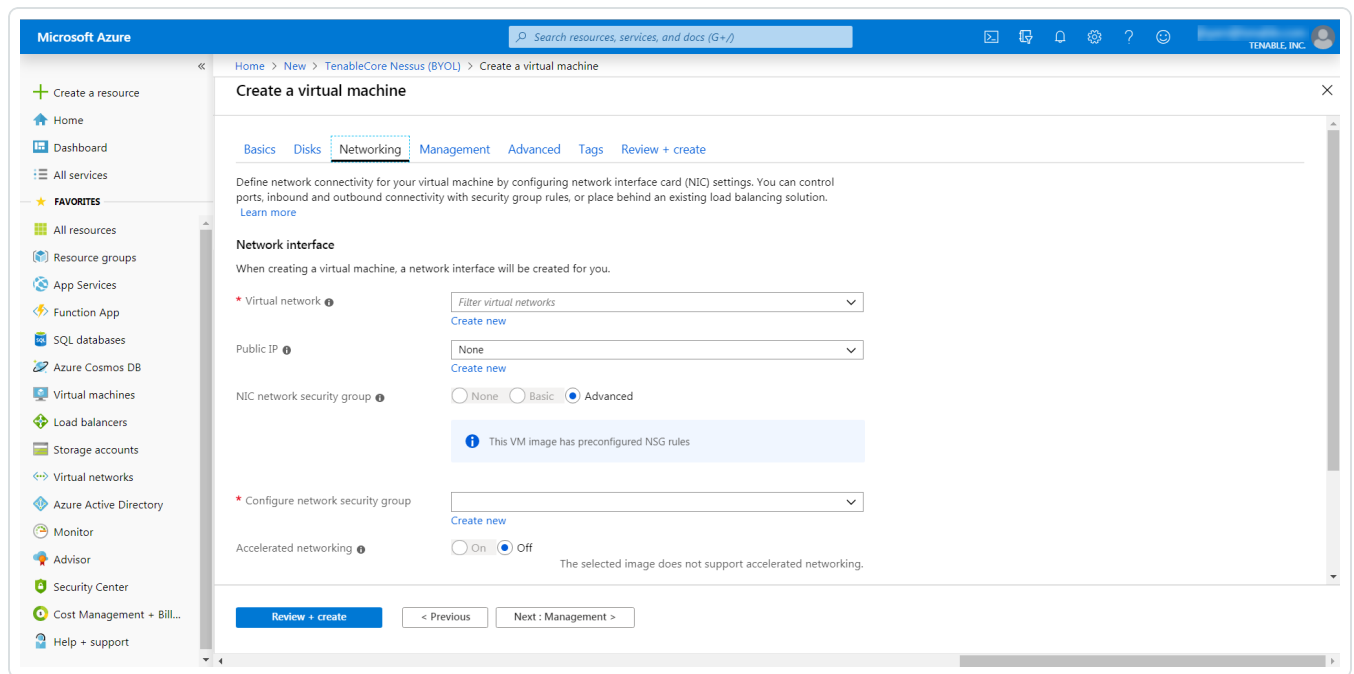
7. Click the **Disks** tab.

The **Disks** page appears.



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.



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 |



| | |
|--------------------------------------|---|
| | console 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 control. |
| 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 shutdown your virtual machine daily. |

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

The **Advanced** page appears.

19. (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 [Deploy Tenable Core + Nessus in Microsoft Azure](#) 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 [Install Nessus](#) section in the *Nessus User Guide*.



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.



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



Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Availability + scaling

Configuration

Identity

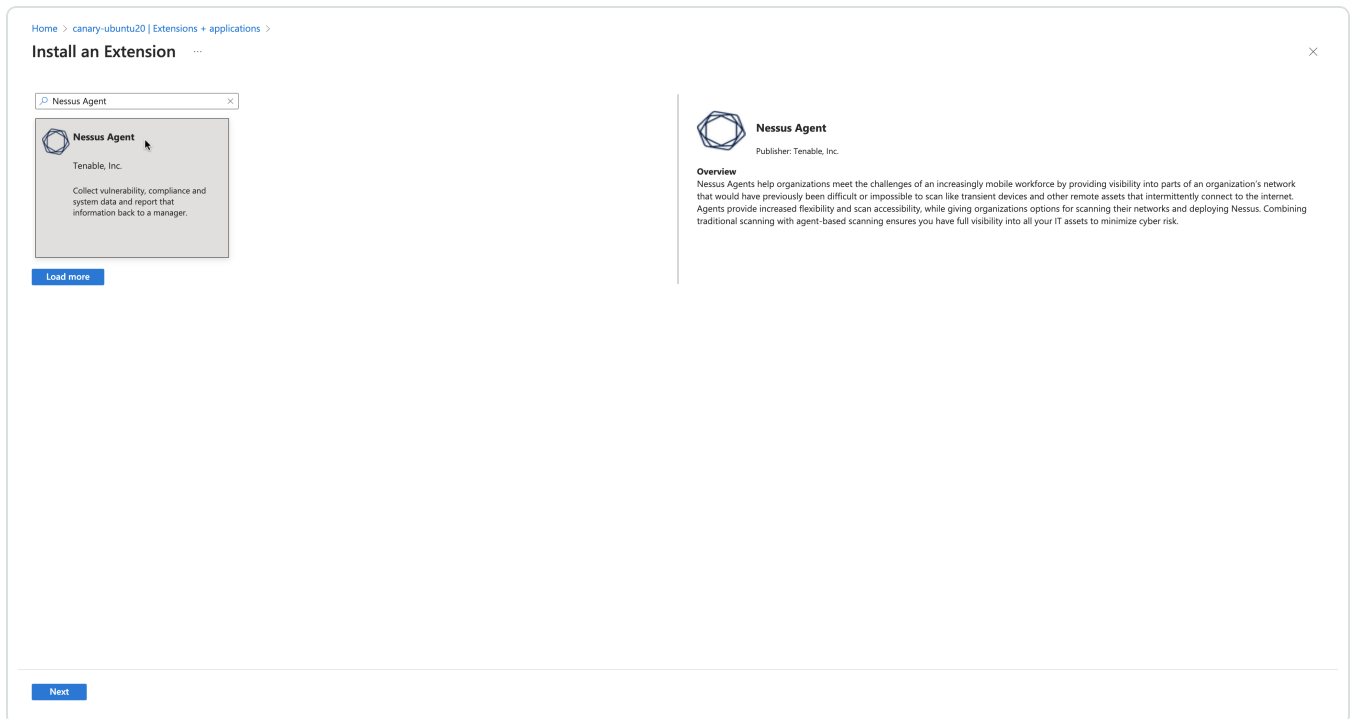
Properties

Locks

Operations



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.



[Home](#) > [canary-ubuntu20](#) | [Extensions + applications](#) > [Install an Extension](#) >

Configure Nessus Agent Extension ...

Create Review + create

Agent Linking

Nessus Linking Key * ⓘ

c7ea4dd7f16f0249fcd7e9591b74c3027f3768c738cbfe3ace6410a1553f... ✓

Link to: ⓘ

☐ Nessus Manager

☒ Tenable Vulnerability Management

TVM Network ⓘ

test ✓

Agent Identity

Agent Name ⓘ

NA_name1 ✓

Agent Group ⓘ

GROUP1 ✓

Previous

Next

Review + create

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 [Retrieve the Tenable Nessus Agent Linking Key](#). 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 **tenableIoNetwork**.

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 [Nessuscli Agent](#).

Parameters

| Parameter names | Equivalent Nessuscli parameters | Required |
|-----------------|---------------------------------|----------|
|-----------------|---------------------------------|----------|



| | | |
|-------------------|---------------------------------|-----|
| 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.