# Table of Contents

Welcome to Tenable for Microsoft Azure ................................................................. 4

Audit Microsoft Azure ........................................................................................... 5
  Configure Azure for a Compliance Audit ......................................................... 6
  Audit Microsoft Azure in Tenable.io ............................................................... 13
  Audit Microsoft Azure in Nessus ................................................................. 19

Microsoft Azure Sentinel ..................................................................................... 22

Tenable.io Vulnerability Management ................................................................. 29
  Integration Requirements .................................................................................. 30
  Microsoft Azure Connector ............................................................................. 31
    Configure Azure (Connector) ....................................................................... 33
    Create Azure Application ............................................................................. 34
  Obtain Azure Tenant ID (Directory ID) ............................................................ 40
  Obtain Azure Subscription ID ......................................................................... 41
  Grant the Azure Application Reader Role Permissions .................................. 43
  Link Azure Subscriptions ............................................................................... 49
  Create a Microsoft Azure Connector .............................................................. 55

Deploy a Nessus Agent .......................................................................................... 58

Create a Scan ......................................................................................................... 59

Nessus Agent Scan of Azure Virtual Instances .................................................. 60

Tenable.io Web Application Scanner .................................................................... 61
  Provision Tenable Core Web Application Scanner (BYOL) ............................ 62
  Web Application Scan ...................................................................................... 69
Welcome to Tenable for Microsoft Azure

Tenable for Microsoft Azure (Azure) offers security visibility, auditing, system hardening, and continuous monitoring 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](#)
- [Azure Connector](#)
- [Tenable Core Nessus (BYOL)](#)
- [Tenable Core WAS (BYOL)](#)
- [Nessus Agent Scans of Microsoft Azure Cloud Instances](#)
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.io or Nessus:
  - Audit Microsoft Azure in Tenable.io
  - Audit Microsoft Azure in 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 Azure Active Directory > 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. Add a redirect URI.
7. Click Register.

Create Application Client Secret

1. Click your registered application in Azure Active Directory > 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. |

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.

2. Add the Reader role to the application you previously created for scanning.

3. Select Reader from the Role dropdown 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 Azure AD User Account

Create a new user to scan in the Azure Active Directory. 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 **Azure Active Directory > App registrations**.
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 Azure Active Directory > App Registrations > Your Application > API Permissions.

Call APIs
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API Permissions

Sign in users in 5 minutes
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:
   - Microsoft Graph – Directory.Read.All
   - Microsoft Graph – User.Read.All
   - Microsoft Graph – Policy.Read.All
   - Microsoft Graph – Reports.Read.All
   - Microsoft Graph – DeviceManagementApps.Read.All
   - Microsoft Graph – Calendars.Read
   - Microsoft Graph – DeviceManagementConfiguration.Read.All
   - Azure Service Management – user_impersonation

Scanning Microsoft 365 environment:
   - Microsoft Graph – SecurityEvents.Read.All

Scanning Microsoft Intune:
   - Microsoft Graph – DeviceManagementApps.Read.All
   - Microsoft Graph – DeviceManagementManagedDevices.Read.All

<table>
<thead>
<tr>
<th>API / Permissions name</th>
<th>Type</th>
<th>Description</th>
<th>Admin consent req...</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Service Management (1)</td>
<td></td>
<td></td>
<td></td>
<td>***</td>
</tr>
<tr>
<td>user_impersonation</td>
<td>Delegated</td>
<td>Access Azure Service Management as organization use...</td>
<td>-</td>
<td>☑ Granted for Bob Corp</td>
</tr>
<tr>
<td>Microsoft Graph (7)</td>
<td></td>
<td></td>
<td></td>
<td>***</td>
</tr>
<tr>
<td>Calendars.Read</td>
<td>Application</td>
<td>Read calendars in all mailboxes</td>
<td>Yes</td>
<td>☑ Granted for Bob Corp</td>
</tr>
<tr>
<td>DeviceManagementApps.Read</td>
<td>Application</td>
<td>Read Microsoft Intune apps</td>
<td>Yes</td>
<td>☑ Granted for Bob Corp</td>
</tr>
<tr>
<td>DeviceManagementConfiguration</td>
<td>Application</td>
<td>Read Microsoft Intune device configuration and policies</td>
<td>Yes</td>
<td>☑ Granted for Bob Corp</td>
</tr>
<tr>
<td>Directory.Read.All</td>
<td>Application</td>
<td>Read directory data</td>
<td>Yes</td>
<td>☑ Granted for Bob Corp</td>
</tr>
<tr>
<td>Policy.Read.All</td>
<td>Application</td>
<td>Read your organization’s policies</td>
<td>Yes</td>
<td>☑ Granted for Bob Corp</td>
</tr>
<tr>
<td>Reports.Read.All</td>
<td>Application</td>
<td>Read all usage reports</td>
<td>Yes</td>
<td>☑ Granted for Bob Corp</td>
</tr>
<tr>
<td>User.Read.All</td>
<td>Application</td>
<td>Read all users’ full profiles</td>
<td>Yes</td>
<td>☑ Granted for Bob Corp</td>
</tr>
</tbody>
</table>

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

What to do next:

Create an audit scan in either Tenable.io or Nessus:

- [Audit Microsoft Azure in Tenable.io](#)
- [Audit Microsoft Azure in Nessus](#)
Audit Microsoft Azure in Tenable.io

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

For more information on the Microsoft Azure audit, see 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.io:

1. Log in to Tenable.io.
2. Click **New Scan**.
   
The **My Scans** page appears.

3. Select the **Audit Cloud Infrastructure** template.
4. In the **Name** box, type a descriptive name for the scan.

5. (Optional) In the **Description** box, enter information to describe your scan.

6. Click **Compliance**.

7. 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 [Microsoft Azure Audit Compliance Reference](#) in the [Nessus Compliance Checks Reference Guide](#).

8. Click each compliance check you want to add to the scan.
9. If you choose to add a custom audit file, click **Add File** and select the file to upload.

10. Click **Credentials**.

11. Click **Microsoft Azure**.

   **Note:** See the Required User Privileges section in the Nessus User Guide for the required Microsoft Azure privileges.

12. 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:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant ID</td>
<td>The <a href="#">Tenant ID</a> or Directory ID for your Azure environment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Application ID</td>
<td>The application ID (also known as client ID) for your registered application.</td>
<td>Yes</td>
</tr>
<tr>
<td>Client Secret</td>
<td>The secret key for your registered application.</td>
<td>Yes</td>
</tr>
<tr>
<td>Subscription IDs</td>
<td>List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.</td>
<td>No</td>
</tr>
</tbody>
</table>

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

13. 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.io scans, refer to the [Tenable.io User Guide](#).
Audit Microsoft Azure in Nessus

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

For more information on the Microsoft Azure audit, see 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 Nessus:

1. Log in to Nessus.
2. Click **Scans**.
   
   The **My Scans** page appears.
3. Click **+ New Scan**.
   
   The **Scan Templates** page appears.
4. In the **Compliance** section, select the **Audit Cloud Infrastructure** template.
   
   The **Audit Cloud Infrastructure** page **Settings** tab appears.
5. In the **Name** box, type a descriptive name for the scan.
6. (Optional) In the **Description** box, enter information to describe your scan.
7. Click the **Credentials** tab.
8. In the **Categories** section, click **Microsoft Azure**.
   
   The **Microsoft Azure** options appear.
9. Click the **Authentication Method** drop-down menu to select your preferred authentication method: **key** or **password**.

10. Configure the credentials for your selected authentication method.

   To configure key authentication:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant ID</td>
<td>The <a href="#">Tenant ID</a> or Directory ID for your Azure environment.</td>
<td>Yes</td>
</tr>
<tr>
<td>Application ID</td>
<td>The application ID (also known as client ID) for your registered application.</td>
<td>Yes</td>
</tr>
<tr>
<td>Client Secret</td>
<td>The secret key for your registered application.</td>
<td>Yes</td>
</tr>
<tr>
<td>Subscription IDs</td>
<td>List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.</td>
<td>No</td>
</tr>
</tbody>
</table>

   To configure password authentication:

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

11. Click **Compliance**.

12. 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 Microsoft Azure Audit Compliance Reference in the Nessus Compliance Checks Reference Guide.

13. Click each compliance check you want to add to the scan.

14. If you choose to add a custom audit file, click **Add File** and select the file to upload.

15. Click **Save**.

   The credential saves and the **My Scans** page appears.

**Note:** For additional information on configuring Nessus scans, refer to the Nessus 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.io and exports asset and vulnerability data from Tenable.io directly to Azure 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 Azure Sentinel, see the Microsoft documentation.

**Required User Role:** Administrator. For more information, see API Permissions.

Before you begin:

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

Configuration Steps

Create the data connector

1. Navigate to the Tenable.io Sentinel Solution on the Azure Marketplace and click Create.

   The Create Tenable.io Sentinel Solution page appears.
Important: This Azure Sentinel Solution is currently in public preview. This feature is provided without a service level agreement, and it’s not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see Supplemental Terms of Use for Microsoft Azure Previews.

Note: There may be known issues pertaining to this Solution, please refer to them before installing.

Tenable.io offers a comprehensive portfolio that helps prevent attacks by identifying the vulnerabilities, configuration issues, and malware that hackers could use to penetrate your environment. Use this solution to export data about your Assets and Vulnerabilities to Azure Sentinel.

Azure Sentinel Solutions provide a consolidated way to acquire Azure Sentinel content like data connectors, workbooks, analytics, and automations in your workspace with a single deployment step.

Data Connectors: 1, Parsers: 2

Learn more about Azure Sentinel | Learn more about Solutions

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

Subscription

Resource group

Product

TenableIOSentinellIntegration

Create new

Instance details
Workspace

TenableWorkspace

Review + create
2. Choose the **Resource Group** that contains your Logs Analytics Workspace with Azure Sentinel enabled, and select that **Workspace** from the dropdown list.

3. Click **Review + Create**. This adds a Tenable.io Data Connector and two Parsers to your Azure Sentinel environment.

4. Choose the supported account types for your environment.

5. Navigate to Azure Sentinel and select **Data Connectors**. Search for "Tenable."

6. Click **Open connector page** on the Tenable.io data connector.

   The **Data connectors** page appears.
Note: You will need the Azure Log Analytics Workspace ID and Workspace Key. The data connector installation page displays both values.

Note: You will need Tenable.io API credentials. See Generate API Keys to retrieve those credentials.

7. Read the included instructions on the data connector and click **Deploy to Azure** when you have the required credentials to deploy the data connector.

**Deploy the data connector**

Deploying the data connector creates a storage account, an applications insight resource, and several Azure functions within your Azure subscription.

Note: You are responsible for any charges these resources incur.

1. From the **Custom deployment** page, select a **Resource Group** and enter the required credentials.
Custom deployment

Deploy from a custom template

Basics  Review + create

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 *

Resource group *

Create new

Instance details

Region *

Function Name

TenableIO

Workspace ID *

workspace-id

Workspace Key *

workspace-key

Tenable Access Key *

tenable-access-key

Tenable Secret Key *

tenable-secret-key

Tenable Export Schedule In Minutes

1440

Review + create  < Previous  Next : Review + create >
**Tip:** You can optionally configure the export schedule from Tenable.io. The value must be set in minutes and defaults to export assets and vulnerabilities from Tenable.io every 1440 minutes - meaning one export per 24 hour period.

2. Click **Review + create**.

Once the deployment succeeds, it can take up to an hour for the Data Connector to begin exporting data from Tenable.io.

3. **Azure Sentinel** will change the data connector status to **Connected** once data begins to flow from Tenable.io to Azure Sentinel.

4. Once the **Tenable.io Data Connector** is connected, navigate to the **Queries** resource within the data connector to see some sample queries to use for working with the exported data from Tenable.io.
Tenable.io Vulnerability Management

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

- **Connector**
  - 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**
- **Create Azure Application**
  - Audit Microsoft Azure in Tenable.io
Integration Requirements

To integrate Tenable.io with Microsoft Azure, you need the following:

- **Tenable.io account**
  
  To purchase a Tenable.io account or set up a free evaluation, visit [http://www.tenable.com/products/tenable-io](http://www.tenable.com/products/tenable-io)

- **Azure account**
  
  To create a free account, visit [https://azure.microsoft.com/en-us/free/](https://azure.microsoft.com/en-us/free/)

- **Internet connection**
  
  You must have a `<user>@<somedomain>.onmicrosoft.com` account.
Microsoft Azure Connector

The Microsoft Azure Connector provides real-time visibility and inventory of assets in Microsoft Azure accounts.

To import and analyze information about assets in Microsoft Azure, you must configure Azure to support connectors and then create an Azure connector in Tenable.io.

**Note:** If your Azure deployment includes Azure instances in the Azure China or Azure Government regions, Tenable.io cannot connect to those instances.

To assess Azure assets for vulnerabilities, Tenable recommends that you use Frictionless Assessment to assess for vulnerabilities in the cloud. Alternatively, you can run a Nessus scanner or agent scan, both of which run plugins locally on the host.

<table>
<thead>
<tr>
<th>Goal</th>
<th>Connector Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discover Microsoft Azure assets and assess for vulnerabilities using Frictionless Assessment</strong></td>
<td>Frictionless Assessment</td>
</tr>
<tr>
<td>The cloud connector discovers Azure assets, then assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the host.</td>
<td></td>
</tr>
<tr>
<td>For more information, see Frictionless Assessment for Azure.</td>
<td></td>
</tr>
<tr>
<td><strong>Discover Microsoft Azure assets</strong></td>
<td>Discovery Connector</td>
</tr>
<tr>
<td>The cloud connector discovers Azure assets without assessing them for vulnerabilities. Optionally, you can scan discovered assets later using a Nessus scanner or agent scan.</td>
<td></td>
</tr>
</tbody>
</table>

To analyze assets via a Microsoft Azure connector:

1. Configure your Azure account to support your connectors, as described in Configure Azure (Connector).
2. Create your Azure connector, as described in Create a Microsoft Azure Connector.
**Note:** To manage existing Microsoft Azure connectors, see [Manage Connectors](#) in the Tenable.io Vulnerability Management User Guide.

**Tip:** For common connector errors, see [Connectors](#) in the Tenable Developer Portal.
Configure Azure (Connector)

Before you can use Tenable.io Azure connectors, you must perform several steps in Microsoft Azure.

**Note:** If your Azure deployment includes Azure instances in the Azure China or Azure Government regions, Tenable.io cannot connect to those instances.

To configure Microsoft Azure:

1. [Create an Azure Application](#) if one does not already exist.
   
   **Note:** The Azure Application ID and Client Secret are obtained during this step.

2. [Obtain the Azure Tenant ID (Directory ID)](#).

3. [Obtain the Azure Subscription ID](#).

4. [Grant the Azure Application reader role permissions](#).

5. (Optional) [Link Additional Azure Subscriptions to your Azure Application](#).

What to do next:

- [Create an Azure connector](#).
Create Azure Application

To create an Azure Application for an Azure Tenable.io connector:

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **Azure Active Directory**.
3. Click **App registrations**.
4. To add a new application, click **New registration**.
5. In the **Name** box, enter a descriptive name for the application.

6. In the **Supported Account types** section, choose one of the three options to specify the type of accounts that can access the API.

7. (Optional) In the **Redirect URI** section, select either **Web** or **Public client (mobile & desktop)** from the drop-down, and then enter the URI in the text box.

8. Click **Register** to finalize the settings and create the application.

A success message appears at the top of the page stating that the new application has been created, and the page is redirected to the **Overview page** for the application.
9. Copy the **Application (client) ID**. This information is used to configure a connector with Tenable.io.
10. In the **Manage** section for the application, click **Certificates & secrets**.

![Image of Microsoft Azure interface](image)

11. In the **Client Secrets** section, click **+ New client secret**.

12. In the **Description** box, type a description for the client secret.

13. For the **Expires** option, select an expiration date.

14. Click the **Add** button.

   The new client secret is added.

15. Copy or make a note of the client secret value.

   Later, you will need this client secret to configure a connector with Tenable.io.

What to do next:

- **Obtain the Azure Tenant ID (Directory ID)**
Obtain Azure Tenant ID (Directory ID)

To obtain your Tenant ID for an Azure Tenable.io connector:

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **Azure Active Directory**.
   - The **Directory Overview** page appears.
3. In the **Manage** section, click **Properties**.
   - The **Directory properties** page appears.
4. Copy the **Directory ID**.

**Note:** The Tenant ID and Directory ID are the same.

What to do next:

- [Obtain the Azure Subscription ID](#).
Obtain Azure Subscription ID

To obtain your Subscription ID for an Azure Tenable.io connector:

1. Log in to the Microsoft Azure portal.

2. In the left-hand menu, click **All Services**.
3. In the **General** section, click **Subscriptions**.

4. Copy the **Subscription ID** for the applicable subscription.

**What to do next:**

- **Grant the Azure Application reader role permissions.**
Grant the Azure Application Reader Role Permissions

To grant an Azure application reader role permissions for an Azure Tenable.io connector:

**Note:** For more information, see the Microsoft Azure documentation: Manage access to Azure resources using RBAC and the Azure portal.

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click All Services.
3. In the General section, click **Subscriptions**.

4. In the subscription table, click the applicable subscription.

   The **Overview** page for the subscription appears.

5. In the menu for the subscription, click **Access control (IAM)**.

   The **Access control (IAM)** page appears.

6. Click the **+Add** button.

   A pop-up menu appears.
7. Click **Add role assignment.**
8. In the **Add role assignment** plane, in the **Role** drop-down, select **Reader**.
9. In the Assign access to drop-down, select Azure AD user, group, or service principal.
10. In the **Select** drop-down, select your Azure Application.

11. Click the **Save** button.

**What to do next:**

Do one of the following:

- (Optional) **Link Additional Azure Subscriptions to your Azure Application.**
- **Create an Azure connector.**
Link Azure Subscriptions

Before you begin:

- Record the name of the application you created for your primary Azure subscription.

To configure linked Azure subscriptions:

Grant the secondary subscription reader role permissions for the application you created for your primary Azure subscription.

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click All Services.
3. In the **General** section, click **Subscriptions**.

4. In the subscription table, click the applicable subscription.

   The **Overview** page for the subscription appears.

5. In the menu for the subscription, click **Access control (IAM)**.

   The **Access control (IAM)** page appears.

6. Click the **+Add** button.

   A pop-up menu appears.
7. Click **Add role assignment**.
8. In the **Add role assignment** plane, in the **Role** drop-down, select **Reader**.
9. In the **Assign access** to drop-down, select **Azure AD user, group, or service principal.**
10. In the **Select** drop-down, select your Azure Application.

11. Click the **Save** button.

**What to do next:**

- [Create an Azure connector](#)
Create a Microsoft Azure Connector

**Required User Role:** Administrator

Before you begin:

- Complete the required Microsoft Azure configuration steps.
- Update your plugin set to 2018-12-19 or later.

To create a Microsoft Azure connector:

1. In the upper-left corner, click the button.  
   The left navigation plane appears.
2. In the left navigation plane, click Settings.  
   The Settings page appears.
3. Click the Cloud Connectors tile.  
   The Cloud Connectors page appears and displays the configured connectors table.
4. In the upper-right corner of the page, click the Create Connector button.  
   The Select a Connector plane appears.
5. In the Connectors section, click Microsoft Azure.  
   The Microsoft Azure settings plane appears.
6. In the Connector Name box, type a name to identify the connector.
7. In the Application ID box, type the Azure application ID that you obtained when configuring Microsoft Azure.
8. In the Tenant ID box, type the Azure Tenant ID obtained when configuring Microsoft Azure.
9. In the Client Secret box, type the client secret obtained when configuring Microsoft Azure.
10. Use the Auto Account Discovery toggle to enable or disable automatic discovery of Azure subscription ID(s).
Note: Auto account discovery is enabled by default. The Azure connector automatically discovers your subscription ID and any linked subscription ID(s).

11. (Optional) If Auto Account Discovery is disabled, manually add one or more subscription IDs:
   a. In the Subscription IDs section, click the + button next to Subscription IDs.
      The Add Subscription IDs plane appears.
   b. In the Subscription ID box, type the subscription ID obtained when configuring Microsoft Azure.
   c. (Optional) Click the + button next to Add Another Subscription ID to add additional linked Azure accounts.
   d. In the Subscription ID box, type the subscription ID for the Azure account that you want to link. For information about configuring linked subscriptions, see Link Azure Subscription.
   e. To add the Subscription ID(s), click Add.
      Tenable.io displays the Microsoft Azure settings plane, and the Subscription ID(s) you linked are listed under Subscription IDs.

12. In the Select or Create Network drop-down box, select an existing network for your connector or click the + button to create a new network.

Note: Networks help to avoid IP address collisions between cloud assets and Nessus-discovered assets. Tenable recommends creating a network for each connector type in use to prevent asset records in different cloud environments from overwriting each other. For more information about the network feature, see Networks.

13. Use the Schedule Import toggle to enable or disable scheduled imports.

Note: By default, Tenable.io requests new and updated asset records every (1) days.

When enabled:
• In the **Import** text box, type the frequency with which Tenable.io sends data requests to the Azure server.

• In the drop-down box select **Minutes**, **Hours**, or **Days**.

14. Do one of the following:

• To save the connector, click **Save**.

• To save the connector and import your assets from Azure, click **Save & Import**.

**Note:** There may be a short delay before your assets appear in Tenable.io.
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.
Create a Scan

Create a Tenable.io Scan

For instruction on creating a scan, see the Create a Scan steps in the Tenable.io User Guide.

Create an Agent Scan

For instruction on creating an Agent scan, see the Create an Agent Scan steps in the Tenable.io 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.io or 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.io 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.io 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.io or Nessus Manager.

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

For more information on installing and configuring Nessus Agents, refer to the Nessus User Guide.
Tenable.io Web Application Scanner

View the following sections for steps on how to configure Tenable.io Web Application Scanner with Microsoft Azure.

- [Provision Tenable Core Web Application Scanner (BYOL) in Azure Marketplace](#)
- [Create a Web Application Scan](#)
Provision Tenable Core Web Application Scanner (BYOL)

Tenable Core Web Application Scanner Bring Your Own License (BYOL) is an instance of a Tenable.io 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Details</strong></td>
<td><strong>Subscription</strong> The account through which resources are reported and services are billed.</td>
</tr>
<tr>
<td><strong>Resource Group</strong></td>
<td>The collection of resources that share the same lifecycle, permissions, and policies.</td>
</tr>
<tr>
<td><strong>Instance Details</strong></td>
<td><strong>Virtual machine name</strong> The name used for both, the virtual machine and host name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Region</strong> The regional location most suitable for you and your customers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Some virtual machine sizes are not available in certain regions.</td>
</tr>
<tr>
<td></td>
<td><strong>Availability options</strong> (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.</td>
</tr>
<tr>
<td></td>
<td><strong>Image</strong> The base operating system or application for the virtual machine.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>The virtual machine size to support the workload you want to run.</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td><strong>Administrator Account</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>The type of authentication the administrator uses - SSH or password.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>The administrator username for the virtual machine.</td>
</tr>
</tbody>
</table>
| **SSH Key** | (Only available when you select SSH for Authentication Type) The single-line RSA public key or multi-line PEM certificate. 
For additional information on setting up your SSH account, see Create a Password for the Initial Administrator User Account. |
| **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.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>(Optional) Enable to capture the serial</td>
</tr>
<tr>
<td>Boot diagnostics</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OS guest diagnostics</td>
<td>(Optional) Enable to receive metrics for your virtual machine.</td>
</tr>
<tr>
<td>Diagnostic storage account</td>
<td>The account used to store your metrics.</td>
</tr>
<tr>
<td>Identity</td>
<td></td>
</tr>
<tr>
<td>System assigned managed identity</td>
<td>(Optional) Enable to grant permissions using the Azure role-based access control.</td>
</tr>
<tr>
<td>Azure Active Directory</td>
<td></td>
</tr>
<tr>
<td>Login with AAD credentials (preview)</td>
<td>(Optional) Enable to use your corporate Active Directory credentials to log in to the virtual machine, enforce MFA, and enable access via RBAC roles.</td>
</tr>
<tr>
<td>Auto-shutdown</td>
<td></td>
</tr>
<tr>
<td>Enable auto-shutdown</td>
<td>(Optional) Enable to automatically shut-down your virtual machine daily.</td>
</tr>
</tbody>
</table>

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.io Web Application Scanning in Microsoft Azure** in the **Tenable Core for Tenable.io Web Application 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.io Web Application Scanning User Guide.
Deploy a Nessus Scanner

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

- [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 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Details</strong></td>
<td></td>
</tr>
<tr>
<td>Subscription</td>
<td>The account through which resources are reported and services are billed.</td>
</tr>
<tr>
<td>Resource Group</td>
<td>The collection of resources that share the same lifecycle, permissions, and policies.</td>
</tr>
<tr>
<td><strong>Instance Details</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual machine name</td>
<td>The name used for both, the virtual machine and host name.</td>
</tr>
<tr>
<td>Note:</td>
<td>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.</td>
</tr>
<tr>
<td>Region</td>
<td>The regional location most suitable for you and your customers.</td>
</tr>
<tr>
<td>Note:</td>
<td>Some virtual machine sizes are not available in certain regions.</td>
</tr>
<tr>
<td>Availability options</td>
<td>(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.</td>
</tr>
<tr>
<td>Image</td>
<td>The base operating system or application for the virtual machine.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>The virtual machine size to support the workload you want to run.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Administrator Account</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>The type of authentication the administrator uses - SSH or password.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>The administrator username for the virtual machine.</td>
</tr>
<tr>
<td><strong>SSH Key</strong></td>
<td>(Only available when you select SSH for Authentication Type) The single-line RSA public key or multi-line PEM certificate. For additional information on setting up your SSH account, see <a href="#">Create a Password for the Initial Administrator User Account</a>.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>(Only available when you select Password for Authentication Type) The administrator password for the virtual machine.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>(Only available when you select Password for Authentication Type) Verification for the administrator password for the virtual machine.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Boot diagnostics</td>
<td>(Optional) Enable to capture the serial</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Console output and screenshots</td>
<td>console output and screenshots of the virtual machine running on a host.</td>
</tr>
<tr>
<td>OS guest diagnostics</td>
<td>(Optional) Enable to receive metrics for your virtual machine.</td>
</tr>
<tr>
<td>Diagnostic storage account</td>
<td>The account used to store your metrics.</td>
</tr>
<tr>
<td>Identity</td>
<td></td>
</tr>
<tr>
<td>System assigned managed identity</td>
<td>(Optional) Enable to grant permissions using the Azure role-based access control.</td>
</tr>
<tr>
<td>Azure Active Directory</td>
<td></td>
</tr>
<tr>
<td>Login with AAD credentials (preview)</td>
<td>(Optional) Enable to use your corporate Active Directory credentials to log in to the virtual machine, enforce MFA, and enable access via RBAC roles.</td>
</tr>
<tr>
<td>Auto-shutdown</td>
<td></td>
</tr>
<tr>
<td>Enable auto-shutdown</td>
<td>(Optional) Enable to automatically shut-down your virtual machine daily.</td>
</tr>
</tbody>
</table>

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 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.
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 ten-able.com.