



Tenable and Microsoft Intune Mobile Device Management Integration Guide

Last Revised: May 22, 2021



Table of Contents

Tenable.io for Microsoft Intune	3
Nessus for Microsoft Intune	7



Tenable.io for Microsoft Intune

Before you begin:

- You must have an active Microsoft Azure subscription.
- [Create an App Registration](#) in the Azure active directory.
- [Create a User Account](#) with a **Directory role** of **Intune Administrator**.
- Add API permissions in Microsoft Azure.
- You must have an active Microsoft Intune subscription.

To configure Microsoft Azure:

Create an App Registration

You must create an App Registration to generate an Application (client) ID and Directory (tenant) ID. This information is needed for the Tenable integration.

1. Create an **App Registration**.
2. In the left navigation panel, click **Azure Active Directory**.

The **Azure Active Directory** menu appears.

3. Click **App Registrations**.
4. The **App Registrations** page appears.
5. Click the **New registration** tab.

The **Register an applicant** page appears.

6. Enter a **Name** .
7. Select the **Support account types**.
8. Provide a **Redirect URI**.

Note: The Redirect URI is required, but has no effect for this configuration; therefore, it doesn't have to be a real URI, i. e., <https://example.com>.



9. Click **Register**.
10. Under **Apps Registrations**, click on the **App registration** you just created.
11. In the **Overview** section, copy and save the **Application (client) ID** and **Directory (tenant) ID**.

Select API permissions

In the newly created App Registration, add permissions in the **Add API Permissions** section.

1. Click **API permissions**.
The API permissions page appears.
2. Click the **Add a Permission** button.
3. Select the **DeviceManagementManagedDevices.Read.All** and **DeviceManagementConfiguration.Read.All** permissions.
4. Click **Grant admin consent for Tenable, Inc.**

Create a Client Secret

1. In the **Certificates and Secrets** section, click the **New client secret** button.
The **Add a client secret** window appears.
2. Enter a **Description**.
3. In the **Expires** section, select an expiration time.

Note: If you select **1 year** or **2 years**, you have to create a new client secret at that time. Selecting **Never** alleviates renewal.

4. Click **Add**.
5. Immediately, copy the client secret value.

Caution: Once you navigate away from this page the client secret value becomes hidden. There is no way to retrieve it once it becomes hidden. You must go through the steps again to generate another client secret.

Create a User Account

You need the user name and password to set up the Microsoft Intune account.



1. Click the **New User** button.

The **New User** section appears.

2. Type the required information for the new user.
3. In the **Directory role** option, select **Intune Administrator**.

Note: The user must have an Azure active directory account with a **Directory role** of **Intune Administrator**. You cannot use a domain account.

To configure Tenable.io:

1. Log in to Tenable.io.
2. At the top of the screen, click **New Scan**.

The **Scan Templates** page appears.

3. Click the **Mobile Device Scan** template.

The **New Scan/Mobile Device Scan** page appears.

4. In the **Name** field, enter a name for your scan.
5. (Optional) Add a description for the scan.
6. Select a **Folder**.
7. Select a **Scanner**.
8. Click the **Credentials** tab.
9. Select **Intune**.

The **Intune** configuration fields appear.



10. Provide the scan information described in the table below.

Option	Description
Tenant	The Microsoft Azure Directory (tenant) ID visible in your App registration.
Client	The Microsoft Azure Application (client) ID generated during your App registration.
Secret	The secret key generated when you created your client secret key in Microsoft Azure.
Username	The username for the account you want Nessus to use to authenticate to Intune.
Password	The password for the account you want Nessus to use to authenticate to Intune.

11. Click **Save to Managed Credentials**.

A **Save Credential** window appears.

12. In the **Credential Name** field, type a name for the credential.

13. Click **Save**.

The **My Scans** page appears.

14. To verify the integration works, click the **Launch** button next to your newly created scan.

15. Once the scan completes, click the scan to view the results.



Nessus for Microsoft Intune

Before you begin:

- You must have an active Microsoft Azure subscription.
- [Create an App Registration](#) in the Azure active directory.
- [Create a User Account](#) with a **Directory role** of **Intune Administrator**.
- Add API permissions in Microsoft Azure.
- You must have an active Microsoft Intune subscription.

To configure Microsoft Azure:

Create an App Registration

You must create an App Registration to generate an Application (client) ID and Directory (tenant) ID. This information is needed for the Tenable integration.

1. Create an **App Registration**.
2. In the left navigation panel, click **Azure Active Directory**.

The **Azure Active Directory** menu appears.

3. Click **App registrations**.
4. The **App Registrations** page appears.
5. Click the **New registration** tab.

The **Register an applicant** page appears.

6. Enter a **Name**.
7. Select the **Support account types**.
8. Provide a **Redirect URI**.

Note: The Redirect URI is required, but has no effect for this configuration; therefore, it doesn't have to be a real URI, i. e., <https://example.com>.

9. Click **Register**.



10. Under **Apps registrations**, click on the **App registration** you just created.
11. In the **Overview** section, copy and save the **Application (client) ID** and **Directory (tenant) ID**.

Select API permissions

In the newly created App Registration, add permissions in the **Add API permissions** section.

1. Click **API permissions**.

The API permissions page appears.

2. Click the **Add a Permission** button.
3. Select the **User.Read**, **Device.Read**, **Device.ReadWrite.All**, **DeviceManagementApps.Read.All**, **DeviceManagementConfiguration.Read.All**, **DeviceManagementManagedDevices**, **DeviceManagementRBAC.Read.All**, **DeviceManagementServiceConfig.Read.All**, and **UserRead.All** permissions.
4. Click **Grant admin consent for Tenable, Inc.**

Create a Client Secret

1. In the **Certificates and Secrets** section, click the **New client secret** button.

The **Add a client secret** window appears.

2. Enter a **Description**.
3. Select a time for **Expires**.

4. **Note:** If you select **1 year** or **2 years**, you have to create a new client secret at that time. Selecting **Never** alleviates renewal.

5. Click **Add**.
6. Immediately, copy the client secret value.

Caution: Once you navigate away from this page the client secret value becomes hidden. There is no way to retrieve it once it becomes hidden. You must go through the steps again to generate another client secret.

Create a User Account

You need the user name and password to set up the Microsoft Intune account.



1. Click the **New User** button.

The **New User** section appears.

2. Type the required information for the new user.
3. In the **Directory role** option, select **Intune Administrator**.

Note: The user must have an Azure active directory account with a **Directory role** of **Intune Administrator**. You cannot use a domain account.

To configure Nessus

1. Log in to Nessus.
2. At the top of the screen, click **New Scan**.

The **Scan Templates** page appears.

3. Click the **Mobile Device Scan** template.

The **New Scan/Mobile Device Scan** page appears.

4. In the **Name** field, enter a name for your scan and (optional) description.
5. Select a **Folder** and **Scanner**.
6. Click the **Credentials** tab.
7. Select **Intune**.

The **Intune** configuration fields appear.



8. Provide the scan information described in the table below.

Option	Description
Tenant	The Microsoft Azure Directory (tenant) ID visible in your App registration.
Client	The Microsoft Azure Application (client) ID generated during your App registration.
Secret	The secret key generated when you created your client secret key in Microsoft Azure.
Username	The username for the account you want Nessus to use to authenticate to Intune.
Password	The password for the account you want Nessus to use to authenticate to Intune.

9. Click **Save**.

The **My Scans** page appears.

10. To verify the integration works, click the **Launch** button next to your newly created scan.

11. Once the scan completes, click the scan to view the results.