



Tenable and Microsoft Intune Mobile Device Management Integration Guide

Last Revised: April 16, 2025



Table of Contents

Tenable Vulnerability Management for Microsoft Intune	3
Tenable Security Center for Microsoft Intune	8



Tenable Vulnerability Management for Microsoft Intune

Before you begin:

- You must have an active Microsoft Entra ID subscription.
- [Create an App Registration](#) in the Microsoft Entra ID.
- [Create a User Account](#) with a **Cloud Device Administrator** or **Intune Administrator** role.
- If using the “user” authentication type, create a user account
- Add API permissions in Entra ID.

Note: Tenable supports two types of authentication, “user” authentication and “application” authentication. User authentication uses a “delegated” access scenario and requires an app registration as well as a user account. Application authentication uses the “app-only” access scenario and only requires an app registration. For more information, refer to the [Microsoft Entra ID Documentation](#).

To configure Microsoft Entra ID:

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. Open **Entra admin center**.
2. In the left navigation panel, click **Microsoft Entra ID**.

The **Microsoft Entra ID** menu appears.

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

The **Register an application** page appears.

6. Enter a **Name** .



7. Select the **Support account types**.
8. (Optional) Provide a **Redirect URI**.

Note: The Redirect URI should be left empty.

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 following permissions. If using user authentication, these should be the “Delegated” type. If using application authentication, they should be the “Application” type.

User Authentication:

Permission	Type
DeviceManagementConfiguration.Read.All	Delegated
DeviceManagementManagedDevices.Read.All	Delegated

Application Authentication:

Permission	Type
DeviceManagementConfiguration.Read.All	Application
DeviceManagementManagedDevices.Read.All	Application

4. Click **Grant admin consent for <tenant>**.

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.

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

If using user authentication, create a user account. Otherwise, you may skip this section.

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

The **New User** section appears.

2. Type the required information for the new user.
3. Grant the user role-based access for the required API permissions.

Note: This can be done by giving the user the directory role of “Cloud Device Administrator” or “Intune Administrator”. It can also be done using a custom role, for more on custom roles please refer to the Microsoft Role Based Access Control (RBAC) documentation.

Note: If using user authentication, please note that Multi Factor Authentication (MFA) is not supported.

To configure Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
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
Authentication Type	Authenticate using application authentication or user authentication.
Tenant	The Microsoft Entra ID Directory (tenant) ID visible in your App registration.
Client	The Microsoft Entra ID Application (client) ID generated during your App registration.
Secret	The secret key generated when you created your client secret key in Microsoft Entra ID.
Username	If using user authentication, the username for the account you want Tenable Vulnerability Management to use to authenticate to Intune.
Password	If using user authentication, the password for the account you want Tenable Vulnerability Management 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.



Tenable Security Center for Microsoft Intune

Before you begin:

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

To configure Microsoft Entra ID:

Create an App Registration

Create an App Registration to generate an Application (client) ID and Directory (tenant) ID. You need this information for the Tenable integration.

1. Create an **App Registration**.
2. In the left navigation panel, click **Microsoft Entra ID**.

The **Microsoft Entra ID** menu appears.

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

The **Register an application** page appears.

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

Note: The Redirect URI should be left empty.

9. Click **Register**.



10. Under **Apps registrations**, click on the **App registration** you 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 **DeviceManagementConfiguration.Read.All** and **DeviceManagementManagedDevices.Read.All** permissions.

Note: When you add the **DeviceManagementConfiguration.Read.All** and **DeviceManagementManagedDevices.Read.All** API permissions, you must select a Microsoft Graph API permission type of **Delegated**. Otherwise, you cannot collect any data.

4. Click **Grant admin consent for <tenant>**.

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.

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. Go through the steps again to generate another client secret.

Create a User Account



You need the username 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 Microsoft Entra ID account with a **Directory role** of **Intune Administrator**.

To configure Tenable Security Center

1. Log in to Tenable Security Center as an administrator via the user interface.
2. Click **Repositories**.

The **Repositories** page appears.

3. Click **Add**.

The **Add Repository** page appears.

4. Select **Mobile** as a repository type.

The **Mobile Repository Configuration** page appears.

5. Select **Microsoft Intune** from the **Type** drop-down box.
6. Configure the options for your repository type:

Option	Description	Default
Intune Tenant	(Required) The Microsoft Entra ID Directory value in your Microsoft Intune registration.	--
Intune Client	(Required) The Microsoft Entra ID Application value generated during your Microsoft Intune registration.	--



Option	Description	Default
Intune Secret	(Required) The Microsoft Entra ID client secret key.	--
Intune Username	(Required) The username for the Microsoft Intune user account Tenable Security Center uses to authenticate Microsoft Intune.	--
Intune Password	(Required) The password for the Microsoft Intune user.	--
Scanner	(Required) Specifies which Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 -04:00

7. Click **Submit**.

Tenable Security Center saves your configuration.

What to do next:

- If you added an offline repository, export one or more repositories from your other Tenable Security Center as described in [Export a Repository](#).
- If you added an offline repository, import one or more exported repository files as described in [Import a Repository](#).



For more information on Tenable Security Center scans, see [Tenable Security Center Scanning Overview](#).