SIA Integration

Microsoft Intune

31st August 2022

Table of Contents

Overview

This document covers the Intune integration supported on SIA Mobile. They are intended for UI users. API documentation is available online on developer.securemobi.net

Microsoft Endpoint Manager (Intune)

Introduction

This integration allows you to connect your account to an Intune account and sync intune device attributes with your device platform attributes. It also allows you to define groups mapping to automatically move devices between policy groups based on their device mapping.

Prerequisite

Here is a summary of steps on how to prepare the client credentials. Please review Microsoft official guides if you come across any difficulty from below steps.

1. Sign in to the **Microsoft Endpoint Manager** admin center using administrative credentials.
2. Select **All services** > **M365 Azure Active Directory** > **Azure Active Directory** > **App registrations**.
3. Choose **New registration** to create a new application.
4. In the **Register an application** pane, specify the following:
   - A **Name** for the application.
   - The **Supported account types.** This value can be default.
   - A **Redirect URI** value. This value is an option.
5. After registered, from the **application** pane:
   - Note the **Application (client) ID** value.
   - Note the **Directory (tenant) ID** value.
6. From the **API permissions** pane, choose **Add a permission** > **Microsoft APIs** > **Microsoft Graph**. Then, select the type of **Application permissions** we require:
   - DeviceManagementManagedDevices.Read.All

    - DeviceManagementConfiguration.Read.All
    - DeviceManagementApps.Read.All
    - Group.Read.All
    - Directory.Read.All
    - User.Read.All

7. From the same panel, select **Grant admin consent for your organization** to apply the permissions (you need to be assigned the Global administrator)

8. From the **Certificates & secrets** pane, choose **Client secrets** > **New client secret.**

    - Note the **Secret value**.

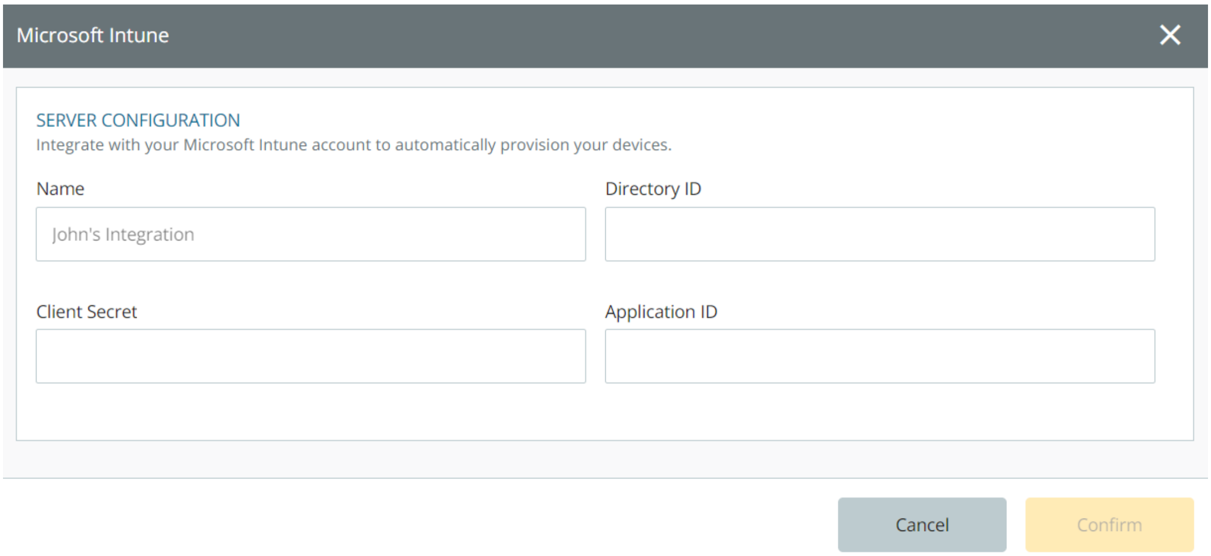
Integration setup

Create Intune Integration

To create an Intune integration, simply navigate to **Integrations**, then click on (+) **Create Integration**.

Choose **Microsoft Endpoint Manager (Intune)** under UEM integrations. Then provide the values gathered in the Prerequisite step:

- Application ID
- Directory ID
- Client Secret



Microsoft Intune

SERVER CONFIGURATION

Integrate with your Microsoft Intune account to automatically provision your devices.

Name: John's Integration

Directory ID:

Client Secret:

Application ID:

After this is created, you have connected your account to Intune, your devices will start syncing from Intune and their details will start getting updated, to see what details are being pulled from Intune, you can check the default device mappings of this integration.

Device Mappings

Device mappings define what fields from an intune device you want to persist your platform device. Here are the default device mappings for this integration:

External Device Attribute	Platform Device Attribute
deviceName	name
managedDeviceName	name
operatingSystem	os
managedDeviceOwnerType	metadata.intune.managedDeviceOwnerType
serialNumber	metadata.intune.serialNumber
osVersion	metadata.intune.osVersion
model	metadata.intune.model
id	metadata.intune.managedDeviceId
azureADDeviceId	metadata.intune.azureADDeviceId

Here we have defined 2 mappings with the same `platform_device_attribute`, this means that the system will get the `deviceName`, if it is not available it will use the `managedDeviceName` field and set the `name` of the Platform device to its value.

Metadata attributes are additional information enriching the device platform information.

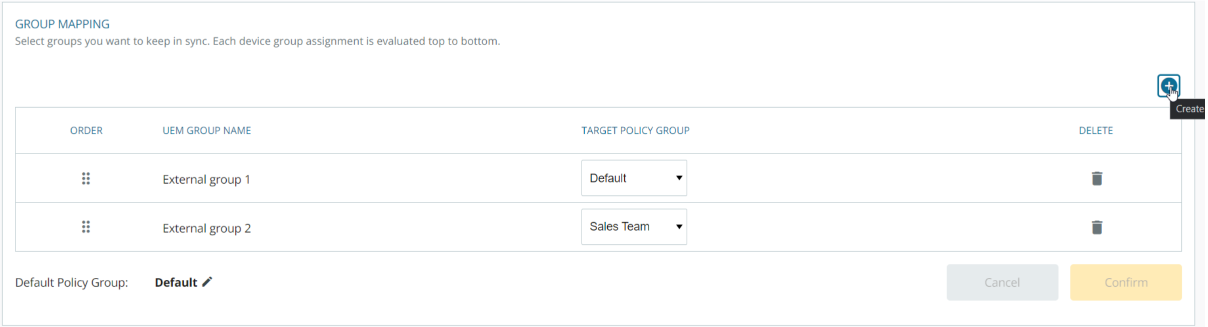
Group Mappings

Group mappings will update the Policy Group of your Devices based on their Intune groups.

Create a Group mapping list

To create group mappings, we need to know what Intune Groups you are going to map to your Policy Groups.

Under GROUP MAPPING, simply **select the (+) icon** and search for an Intune group using its name or ID. **Select the Intune group** you want to map and select **Add.**



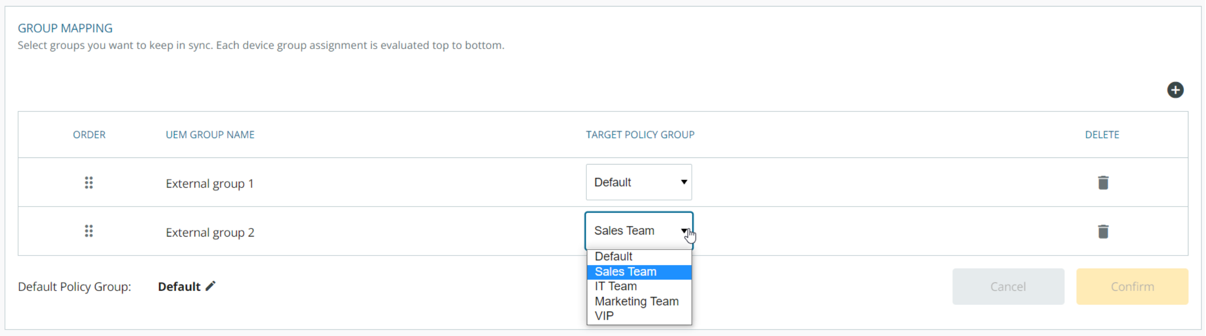
GROUP MAPPING

Select groups you want to keep in sync. Each device group assignment is evaluated top to bottom.

ORDER	UEM GROUP NAME	TARGET POLICY GROUP	DELETE
⠿	External group 1	Default	🗑
⠿	External group 2	Sales Team	🗑

Default Policy Group: **Default**

A new entry will appear under the GROUP MAPPING section. Under TARGET POLICY GROUP, select the desired existing Policy Group you want to map to this Intune group.



GROUP MAPPING

Select groups you want to keep in sync. Each device group assignment is evaluated top to bottom.

ORDER	UEM GROUP NAME	TARGET POLICY GROUP	DELETE
⠿	External group 1	Default	🗑
⠿	External group 2	Sales Team	🗑

Default Policy Group: **Default**

You can add multiple entries and sort them by priority (top to bottom), or delete any entry you do not need anymore. When you are done, do not forget to save your group mapping list.

How does Group mapping works

Once you have defined a group mapping list, if you have a device in "Intune group 1" and the device exits in our platform, it will be assigned to the Default Group, if you move that device in Intune to "Intune group 2", that device will be moved to "My other policy group".

If the device is in both groups in Intune, then the mapping higher in the list will determine where the device will go, in this case it will go to "Default Group"

iOS/iPadOS App distribution with auto-registration

This deployment option for iOS/iPadOS allows to shorten the user on-boarding process by enabling auto-registration.

Add the iOS/iPadOS store app

In your Intune Portal.

Go to Client Apps>Apps

1. Click on **+ Add**
   a. Under *App Type*, select **iOS/iPadOS store app**
   b. Click on **Select**
2. Under *App information*, click on the link **Search the App Store**
   a. Search for the **service mobile app** (tip: you can find in your account under Account Settings>Mobile Apps), and **select it**
   b. Click on **Select**
   c. Adjust the App information and then click on **Next**

Under *Assignments*, do not assign this app yet, click on **Next**

Under *Review + create*, select **Create**

Add and Assign the iOS/iPadOS app configuration

Go to **Client Apps>App Configuration policies**

Click on **+ Add** and **Managed devices**

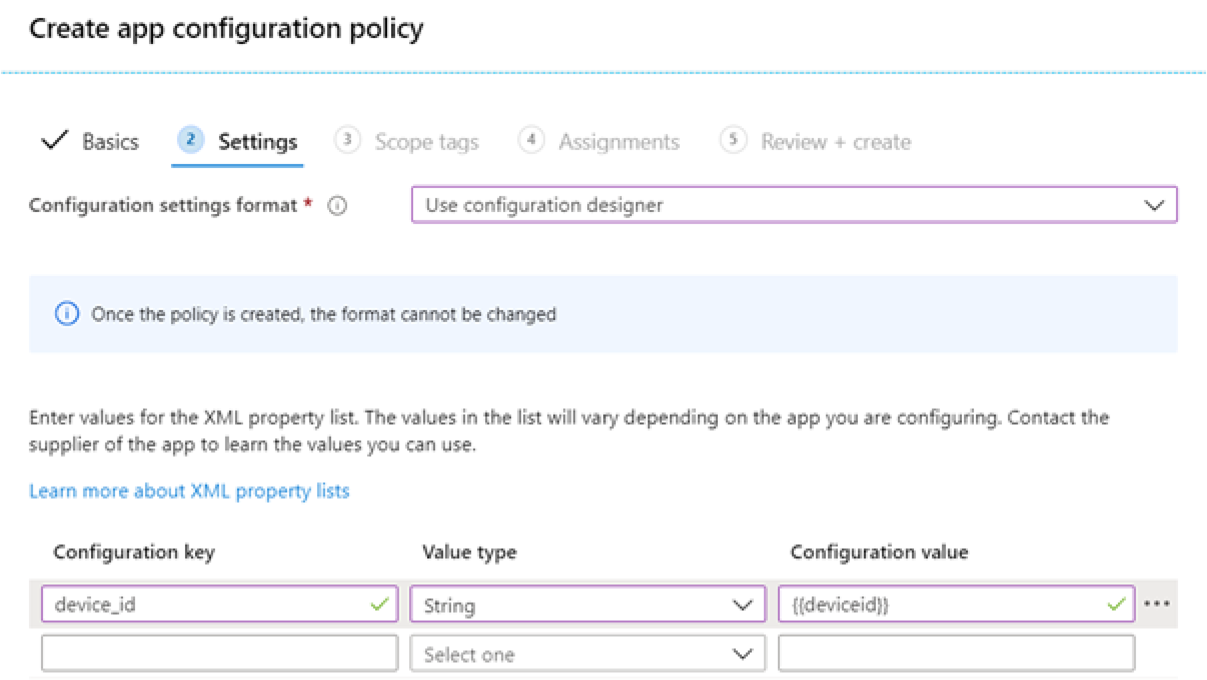
Under *Basics*

1. Give a **Name**
2. Select the **iOS/iPadOS** platform
3. Click on **Select App** and **add the service iOS/iPadOS store app**, click **OK**
4. Click on **Next**

Under *Settings*, choose in the drop-down **Use Configuration designer**

1. *Configuration key* is **device_id**
2. *Value Type* is **String**
3. *Configuration Value* is **{{deviceid}}**

4. Click on **Next**



Create app configuration policy

✓ Basics | 2 Settings | 3 Scope tags | 4 Assignments | 5 Review + create

Configuration settings format *: Use configuration designer

Once the policy is created, the format cannot be changed

Enter values for the XML property list. The values in the list will vary depending on the app you are configuring. Contact the supplier of the app to learn the values you can use.

Learn more about XML property lists

Configuration key	Value type	Configuration value
device_id	String	{{deviceid}}
	Select one	

Under *Assignments,* **define the groups** you want to select, then click on **Next**

Under *Review + create*, click on **Create**

Assign the iOS/iPadOS store app

Go back to **Client Apps>Apps**

Select the service iOS/iPadOS store app from the list

Under *Properties*, select **Edit** next to Assignments

You can now assign the app to the groups you want the app distributed to.

Under *Review + Save***,** then **Save**