

Setting Client for authorization

The screenshot displays the configuration page for an RMMClient. The left sidebar shows navigation options like 'Configure', 'Manage', and 'Groups'. The main content area is titled 'RMMClient' and includes a 'Settings' tab. The settings are organized into several sections:

- Client Information:** Client ID (RMMClient), Name, and Description.
- Enabled:** A toggle switch set to 'ON'.
- Consent Required:** A toggle switch set to 'OFF'.
- Client Protocol:** A dropdown menu set to 'openid-connect'.
- Client Template:** A dropdown menu, highlighted with a red box.
- Access Type:** A dropdown menu set to 'confidential', highlighted with a red box.
- Standard Flow Enabled:** A toggle switch set to 'ON'.
- Implicit Flow Enabled:** A toggle switch set to 'OFF'.
- Direct Access Grants Enabled:** A toggle switch set to 'OFF'.
- Service Accounts Enable:** A toggle switch set to 'ON', highlighted with a red box.
- Authorization Enable:** A toggle switch set to 'ON', highlighted with a red box.
- Root URL:** An empty text input field.
- * Valid Redirect URIs:** A list of URIs including 'https://www.rmm.wise-paas.com/*' and 'http://preview-rmm40.eastasia.cloudapp.azure.com/*'.
- Base URL:** An empty text input field.
- Admin URL:** An empty text input field.
- Web Origins:** A list of origins including 'https://www.rmm.wise-paas.com' and 'http://preview-rmm40.eastasia.cloudapp.azure.com'.

Get Client's secret

The screenshot shows the AD-ANTECH Keycloak administration interface. On the left is a dark sidebar with the AD-ANTECH logo and a navigation menu. The main content area is titled 'Clients > RMMClient' and shows the configuration for the 'RMMClient'. The 'Credentials' tab is selected, and a red box highlights the 'Client Authenticator' dropdown menu (set to 'Client Id and Secret') and the 'Secret' text input field containing the value 'a1179a01-c7bd-4776-a6f0-2b93c7941667'. A 'Regenerate Secret' button is located to the right of the secret field. Below this, the 'Registration access token' field is visible with its own 'Regenerate registration access token' button.

AD-ANTECH

RMM

Configure

- Realm Settings
- Clients**
- Client Templates
- Roles
- Identity Providers
- User Federation
- Authentication

Clients > RMMClient

RMMClient

Settings **Credentials** Roles Mappers ? Scope ? Authorization Revocation Sessions ? Offline Access ? Clustering

Client Authenticator ? Client Id and Secret

Secret a1179a01-c7bd-4776-a6f0-2b93c7941667 **Regenerate Secret**

Registration access token ? **Regenerate registration access token**

Set Client's role

Client's role

The screenshot shows the ADVANTAGE console interface. On the left is a dark sidebar with the 'RMM' menu expanded to show options like 'Configure', 'Realm Settings', 'Clients', 'Client Templates', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'. The main content area is titled 'Clients > RMMClient' and shows the configuration for the 'RMMClient'. The 'Roles' tab is selected, displaying a table of roles. The 'devicemanager' role is highlighted with a red box.

Role Name	Composite
devicemanager	False
uma_protection	False

Set Resource's permission

ADIANTECH Admin

RMMClient

Settings Credentials Roles Mappers Scope **Authorization** Revocation Sessions Offline Access Clustering Installation Service Account Roles

Settings **Resources** Authorization Scopes Policies Permissions Evaluate

Filter: Name Type URI Owner Scope Create

Name	Type	URI	Owner	Scopes	Permissions	Actions
Default Resource	urn:RMMClient:resources:default	/*	RMMClient	No scopes assigned.	Default Permission	Create permission
device	No type defined.	/*	RMMClient	No scopes assigned.	Device Permission	Create permission

Set Permission mapping with policy

The screenshot displays the ADAMTECH RMM interface. On the left is a dark sidebar with the ADAMTECH logo at the top. Below the logo, the sidebar is divided into sections: 'RMM' (with a dropdown arrow), 'Configure' (containing 'Realm Settings', 'Clients', 'Client Templates', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'), and 'Manage' (containing 'Groups', 'Users', and 'Sessions'). The 'Clients' option is currently selected.

The main content area shows a breadcrumb trail: 'Clients > RMMClient > Authorization > Permissions > Device Permission'. Below this is the title 'Device Permission' with a trash icon. The configuration form includes the following fields:

- Name ***: Device Permission
- Description**: (empty)
- Apply to Resource Type**: OFF
- Resources ***: device (highlighted in a red box)
- Apply Policy ***: Default Policy (highlighted in a red box)
- Decision Strategy**: Unanimous (dropdown menu)

At the bottom of the form are 'Save' and 'Cancel' buttons.

Set Realm's role

Realm's role

The screenshot shows the ADI ANTECH management console. The left sidebar contains a navigation menu with the following items: RMM, Configure (Realm Settings, Clients, Client Templates, Roles, Identity Providers, User Federation, Authentication), and Manage (Groups). The main content area is titled 'Roles' and has two tabs: 'Realm Roles' (selected) and 'Default Roles'. Below the tabs is a search bar with the placeholder text 'Search...'. A table displays the following data:

Role Name	Composite	Description
offline_access	False	`\${role_offline-access}`
RealmDeviceManager	False	
uma_authorization	False	`\${role_uma_authorization}`

Set account to map with Roles

The screenshot displays the Advantech user management interface. On the left is a dark sidebar with the Advantech logo and a navigation menu. The main content area shows the user profile for Jonathan.lin@advantech.com.tw, with the 'Role Mappings' tab selected. The interface is divided into two sections: 'Realm Roles' and 'Client Roles'. Each section contains an 'Available Roles' list, an 'Assigned Roles' list (highlighted with a red box), and an 'Effective Roles' list. In the 'Realm Roles' section, 'offline_access' is available and 'RealmDeviceManager' and 'uma_authorization' are assigned. In the 'Client Roles' section, 'uma_protection' is available and 'devicemanager' is assigned. The 'Effective Roles' lists show the roles currently active for the user in each context.

Advantech

RMM

Configure

- Realm Settings
- Clients
- Client Templates
- Roles
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import

Users > jonathan.lin@advantech.com.tw

Jonathan.lin@advantech.com.tw

Details Attributes Credentials **Role Mappings** Groups Consents Sessions

Realm Roles

Available Roles ⓘ

offline_access

Add selected >

Assigned Roles ⓘ

RealmDeviceManager
uma_authorization

<< Remove selected

Effective Roles ⓘ

RealmDeviceManager
uma_authorization

Client Roles

RMMClient

Available Roles ⓘ

uma_protection

Add selected >

Assigned Roles ⓘ

devicemanager

<< Remove selected

Effective Roles ⓘ

devicemanager

Test whether the setting is workable or not

The screenshot displays the ADAMTECH user interface. On the left is a dark sidebar with a navigation menu. The main content area shows the configuration for the 'RMMClient' under the 'Authorization' tab, specifically the 'Policy Evaluation' section. The evaluation results for the 'device' are shown below.

ADAMTECH

RMMClient

Settings Credentials Roles Mappers Scope **Authorization** Revocation Sessions Offline Access

Settings Resources Authorization Scopes Policies Permissions **Evaluate**

[New Evaluation](#) | [Re-Evaluate](#) | [Show Authorization Data](#)

device

Result	PERMIT
Scopes	No scopes available.
Policies	<ul style="list-style-type: none">• Device Permission decision was PERMIT by UNANIMOUS decision.<ul style="list-style-type: none">• Default Policy voted to PERMIT .

Test whether the setting is workable or not

Configure

- Realm Settings
- Clients
- Client Templates
- Roles
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import

Settings Credentials Roles Mappers ? Scope ? **Authorization** Revocation Sessions ? Offline Access ? Clustering Installation ? Service Account Roles ?

Settings Resources Authorization Scopes Policies Permissions **Evaluate**

Identity Information ?

Client ? RMMClient

User * ? jonathan.lin@advantech.com.tw

Roles ? Any role...

Contextual Information ?

Contextual Attributes ?

Key	Value	Actions
		Add

Permissions ?

Apply to Resource Type ?

OFF

Resources * ?

Select a resource...

Scopes ?

Select a scope...

Add

Resource	Scopes	Actions
device	Any scope.	Delete

Evaluate Reset

