



aqua

Aqua CSPM Auto Generate Tokens

Overview

The purpose of this document is to provide guidance on how to leverage **Aqua CSPM API Keys** to **generate tokens** that enable internal programmatic tasks, as well as provide guidance for customers with sub-accounts enabled within their instances.

Prerequisites

In order to proceed with utilizing the endpoint that will be defined later on, there are a few tasks to complete:

- Create a **permission sets** within Aqua
- Create an **Aqua Role** and assign the permission sets and determine if the tasks requires **Global** or specific **Application Scope**
- CSPM API Key and Secret

The items mentioned above can be found below in the reference section for more explicit detail. In this document the permission set will enable all objects in read only capacity, the Aqua Role will map to that permission set and the scope will be global.

Permission Set

To create a new **permission sets** navigate to the top left of the browser and click on the **Menu** > **Account Management** > **Permission Sets** > click on **Add Permission Sets**



Aqua Hub NEW

Context aware risk management of cloud and Kubernetes resources

Supply Chain Security NEW

Protect your software supply chain and source code

CSPM

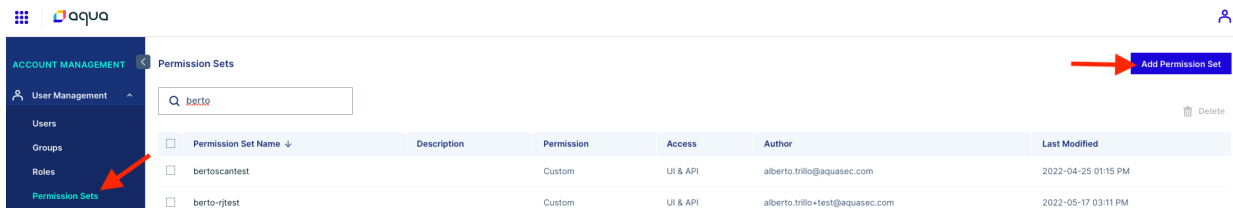
Monitor cloud infrastructure security and compliance risks

Workload Protection

Runtime protection for cloud native applications

Account Management

Manage users, roles, permissions, and billing



The screenshot shows the Aqua Account Management interface. On the left is a sidebar with a menu containing 'User Management', 'Users', 'Groups', 'Roles', and 'Permission Sets'. The 'Permission Sets' item is highlighted with a red arrow. The main content area is titled 'Permission Sets' and contains a search bar with the text 'berto'. Below the search bar is a table with the following data:

<input type="checkbox"/>	Permission Set Name ↓	Description	Permission	Access	Author	Last Modified
<input type="checkbox"/>	bertoscantest		Custom	UI & API	alberto.brillo@aquasec.com	2022-04-25 01:15 PM
<input type="checkbox"/>	berto-rjtest		Custom	UI & API	alberto.brillo+test@aquasec.com	2022-05-17 03:11 PM

In the top right corner of the main content area, there is a red arrow pointing to a blue button labeled 'Add Permission Set'.

In this example, the **permission sets** that will be created will have **view only** permissions to the following:

- Policies
- Assets
- Compliance
- System

In the image below, we enable all components with **View Only** permissions

Permission Set			
4 Categories			
<div>> Policies</div> <div>> Assets</div> <div>> Compliance</div> <div>> System</div>	<div>Edit</div> <div></div> <div>0/5</div>	<div>View Only</div> <div></div> <div>5/5</div>	<div>Not Set</div> <div></div> <div>0/5</div>
	0/7	9/9	0/9
	0/2	2/2	0/2
	0/5	10/10	0/10



Once the desired role is created, the **Aqua Role** can be created.

Aqua Role

The Aqua Role can be used to assign specific permissions to a user or a token in this case. To create an Aqua Role, navigate to the top left of the browser and click on the **Menu > Account Management > Roles** > click on **Add Role**. Enter the following:

- Name
- Permission Sets
- Application Scopes

The role can be scoped to many **Application Scopes**, for the purpose of this document it will be set to **Global**



Aqua Hub NEW

Context aware risk management of cloud and Kubernetes resources

Supply Chain Security NEW

Protect your software supply chain and source code

CSPM

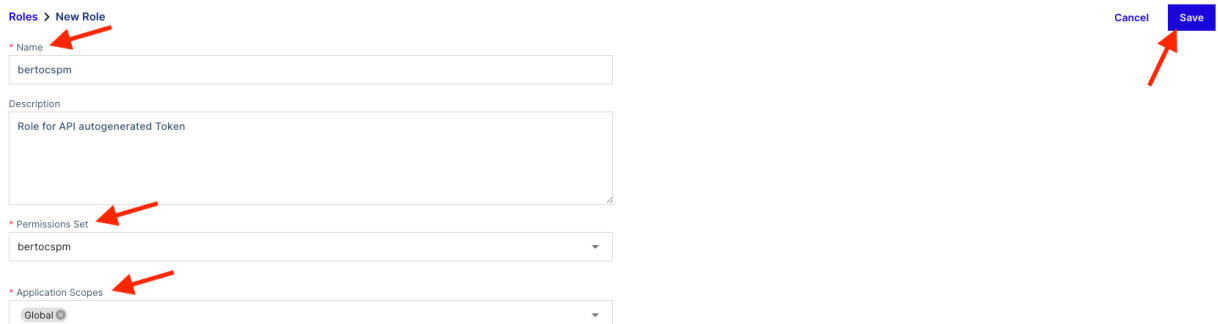
Monitor cloud infrastructure security and compliance risks

Workload Protection

Runtime protection for cloud native applications

Account Management

Manage users, roles, permissions, and billing



Roles > New Role

* Name

Description

* Permissions Set

* Application Scopes

Cancel Save

Once the **Aqua Role** is completed, click **Save** and proceed to generating the **CSPM API Keys**.

CSPM API Key and Secret

When generating an **API Key** in CSPM, copy the key immediately to proceed with the steps later on in the document

To generating an **API Key** navigate to the **Aqua Menu** > **CSPM** > **Settings** > **API Keys** and click **Generate Key**



Aqua Hub NEW

Context aware risk management of cloud and Kubernetes resources

Supply Chain Security NEW

Protect your software supply chain and source code

CSPM

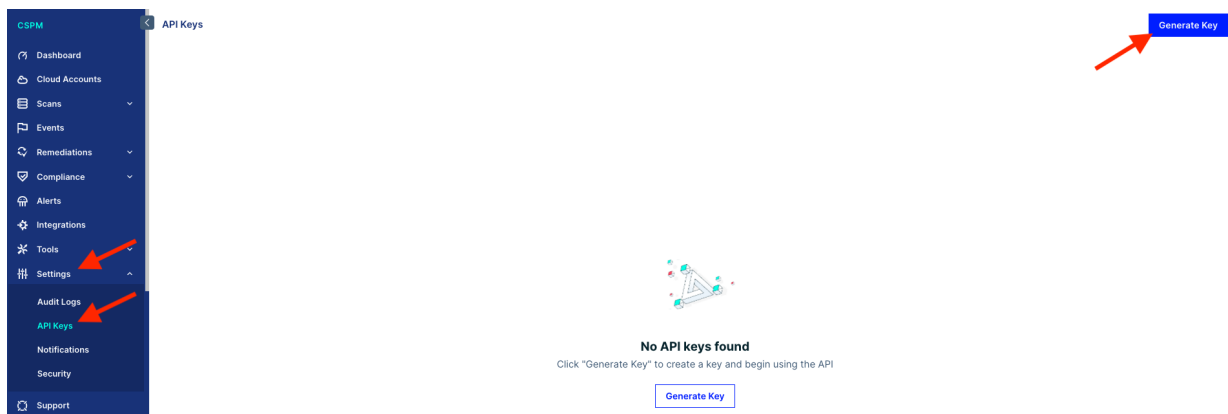
Monitor cloud infrastructure security and compliance risks

Workload Protection

Runtime protection for cloud native applications

Account Management

Manage users, roles, permissions, and billing



The screenshot shows the Aqua CSPM interface. On the left is a dark blue sidebar with a menu. The 'API Keys' option is highlighted in green. In the main content area, there is a message 'No API keys found' with a sub-message 'Click "Generate Key" to create a key and begin using the API'. A blue button labeled 'Generate Key' is visible in the top right corner of the main content area. Red arrows point to the 'API Keys' menu item and the 'Generate Key' button.

This will present both the **API Key** and **API Secret**, copy both values immediately

New API Key



Be sure to save the following secret; once you close this window it will no longer be accessible.

API Key: NPL1yqPA8z5L3cAF2KPKQM

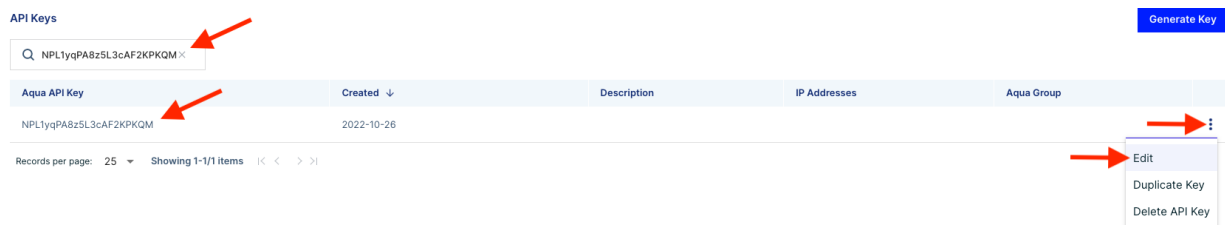
Secret: fW4imEZoMynxOt1qbZtV2qd2rJvbzOolNnC

Close

API Permissions

With the newly created **API Key**, permissions must be assigned to leverage **role assignment** and **token creation**.

If there are many **API Keys** in the environment, grab the value of the newly created key and enter it in the **search**. Once that is completed, click on the **vertical ellipses** on the far right and click **Edit**



By default, the key has **Global Permissions**, turn the slider to the left to disable it

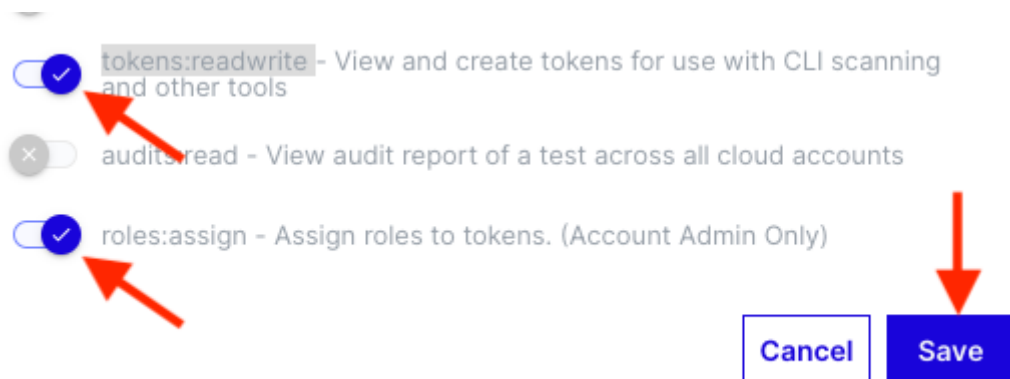
Global Permissions

Selecting an Aqua Group limits this API key to access resources belonging only to this group. An empty group makes the API key an account admin with access to all groups.

☒ Enable global admin permission

Scroll all the way to the **bottom** of the edit pop up box > enable the following two permissions **below** and click **Save**

- **roles:assign**
- **tokens:readwrite**



The API Keys used in this document have since been deleted

API Payload

In order to generate tokens that are assigned the correct permissions, the **payload** must contain the **Aqua Role** that was created earlier in this document. Below is the example of the payload that will need to be passed through.

```
{
  "validity":240,
  "allowed_endpoints":["API ACTION"],
  "csp_roles":["rolename"]
}
```

Definition of the keys listed above:

- **validity** - Length of time for the token to **expire**
- **allowed_endpoints** - The endpoints the token has access to, examples are **DELETE GET HEAD OPTIONS PATCH POST PUT ANY**
- **csp_roles** - The **Aqua Role** to be assigned to the token (The role created earlier in the document)

To compile a script, please visit [CSPM API Docs](#), linked is the tokens endpoint used to **generate tokens**

Sub-Account Usage

Customers that have **sub-accounts** enabled can also take advantage of this feature. The same [prerequisites](#) apply and the [API Key](#) steps would need to be created in **each** (if multiple sub-accounts) sub-account. Once the keys are created correctly in each sub-account, the documentation and the [payload](#) can be used to automate **Cloud Workload Protection Platform (CWPP)** endpoints.

Not all of the endpoints are supported at this time. If there is an endpoint needed, contact your CSM or support@aquasec.com

The environment is now enabled to automatically create tokens with fine tuned permissions!

References

- [Permission Sets](#)
- [Aqua Role](#)
- [CSPM API Documentation](#)
- [CSPM Code Examples](#)
- [RBAC Overview](#)