aws marketplace

Implementation Guide:

Integrating Aqua CSPM with AWS Control Tower

Table of Contents

Foreword **3**

Solution Overview **4**

Architecture Diagram **4**

Pre-requisites **5**

Deploying the Solution **5**

Step 1.1: Register with Aqua Wave 6

Step 1.2: Generate API key and Secret 7

Step 1.3: Create a new Group in Aqua CSPM 8

Step 2: Create the StackSet for this integration 9

Step 3: Verify the automated onboarding of newly enrolled accounts into Aqua CSPM 9

FAQs **10**

Solution Estimated Pricing **10**

Additional Resources **10**

Partner contact information **11**

Foreword

Aqua Security is an Advanced APN member with Container Competency, helping customers unleash the full potential of their cloud native transformation and accelerate innovation with the confidence that all cloud native applications are secured from start to finish, at any scale.

Aqua Cloud Security Posture Management (CSPM) integration for AWS Control Tower is a multi-account security solution that continually audits your cloud accounts for security risks and misconfigurations across hundreds of configuration settings and compliance best practices, enabling consistent, unified multi-account security. It also provides self-securing capabilities to ensure your cloud accounts don't drift out of compliance by leveraging a policy-driven approach.

The purpose of this AWS Implementation Guide is to enable the customers to seamlessly activate, deploy and configure Aqua CSPM for environments managed by AWS Control Tower. Furthermore, it allows them to take full advantage of the resources pre-configured by AWS Control Tower as part of the initialization, for a smooth onboarding experience.

Solution Overview

The Aqua CSPM integration enables automated onboarding of AWS accounts created via AWS Control Tower, by leveraging the inherent account provisioning workflow. This will ensure that any newly created account will automatically be audited and monitored according to best practices and compliance standards for AWS. Through this integration, you will gain a multi-account security framework that will ensure that all your AWS accounts are always in conformance with cloud infrastructure best practices.

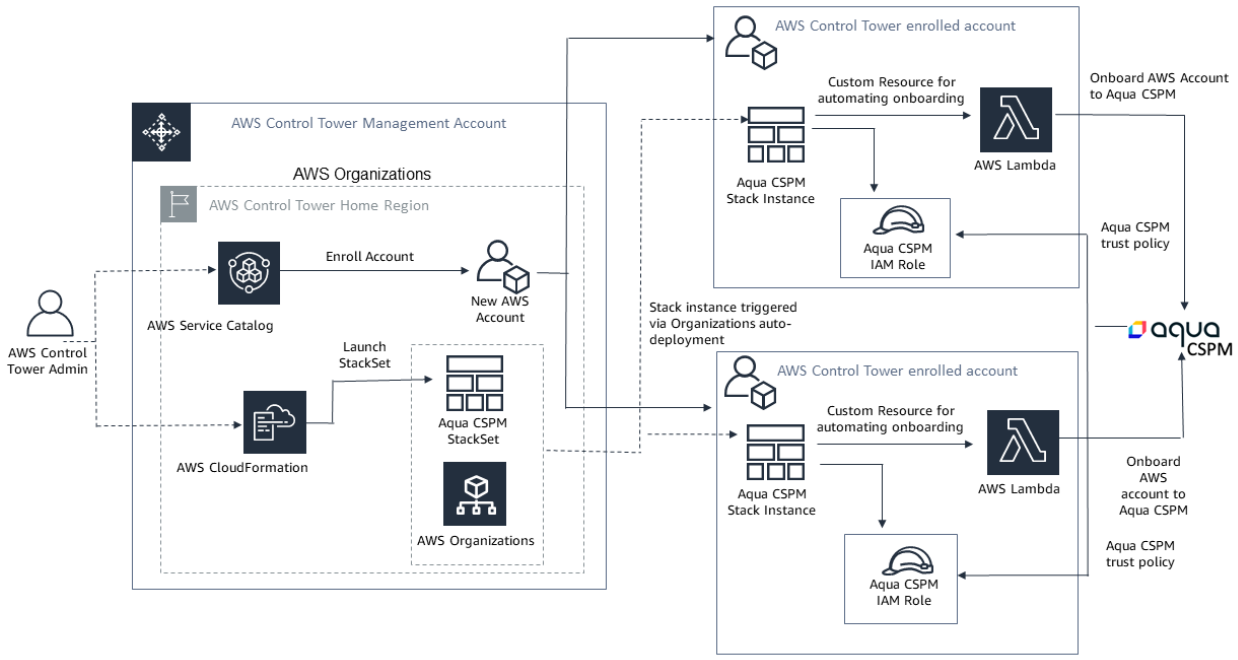
Aqua CSPM makes sure enterprises are using the cloud securely, continuously monitoring and alerting on any identified risks – either accounts out of compliance or exposed to vulnerabilities. It examines a vast array of misconfigurations across user roles and privileges, certificates, and multi-factor authentication (MFA), specific service configurations, data encryption, networking, auditing features, usage trends and conducts anomaly detection. Additionally, it also provides extensive reporting for Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), AWS Well-Architected Framework, General Data Protection Regulation (GDPR), and supports custom compliance requirements.

With a cross-account security auditor Identity and Access Management (IAM) role, Aqua CSPM can only see the infrastructure configurations and provides useful insights into the security posture of your cloud services. The Aqua CSPM integration automates the creation of this IAM role when a new account is enrolled, ensuring that your AWS accounts are always in audited for conformance right out the gate.

The integration comes in the form of a CloudFormation template that is extremely easy to deploy in your AWS Control Tower management account in the home region. The home region is the AWS Region where the Landing zone is set up. The solution involves a one-time deployment of the CloudFormation StackSet, which gets automatically triggered as a part of the account provisioning workflow.

Architecture Diagram

Enterprises today are faced with the challenge of using the cloud securely and continuously monitoring for any identified risks, which can be either accounts out of compliance or exposed to vulnerabilities. Compounding that fact are the research challenges of implementing new cloud-aware security solutions that can provide pre-emptive protection for complex and ever dynamic Cloud infrastructure followed by remediations -- all of which has to be translated into a security strategy to fight against the emerging security threats.



Pre-requisites

1. AWS Control Tower
   The solution doesn't require any additional resources to be enabled outside of the ones already enabled by AWS Control Tower, which involve identity management and federated access to accounts. This guide assume you already have AWS Control Tower deployed and leverages the automated account provisioning workflows for this integration. To get started with AWS Control Tower, check out the Getting Started documentation. You also need administrator privileges in the AWS Control Tower management account.

2. Register with Aqua Wave
   An active subscription with Aqua Wave for Developer or any higher pricing tier plan. Don't have an account yet? Subscribe to Aqua Wave on AWS Marketplace

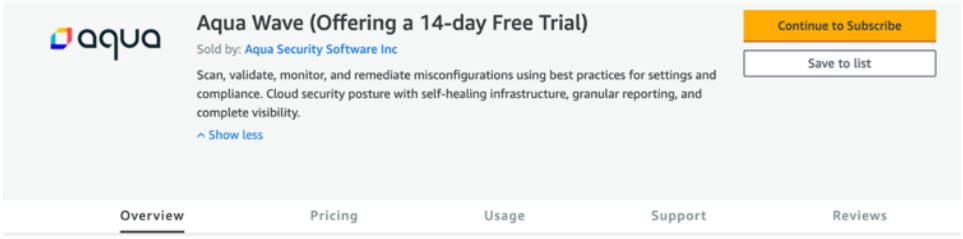
Deploying the Solution

The Aqua CSPM integration is completely automated end-to-end and can be deployed in three simple steps:

1. Register with Aqua Wave and generate the application programming interface (API) key
2. Deploy the CloudFormation StackSet in the Control Tower Management account, and providing API key and Secret as the input
3. Verify the automated onboarding of newly enrolled accounts into Aqua CSPM

Step 1.1: Register with Aqua Wave

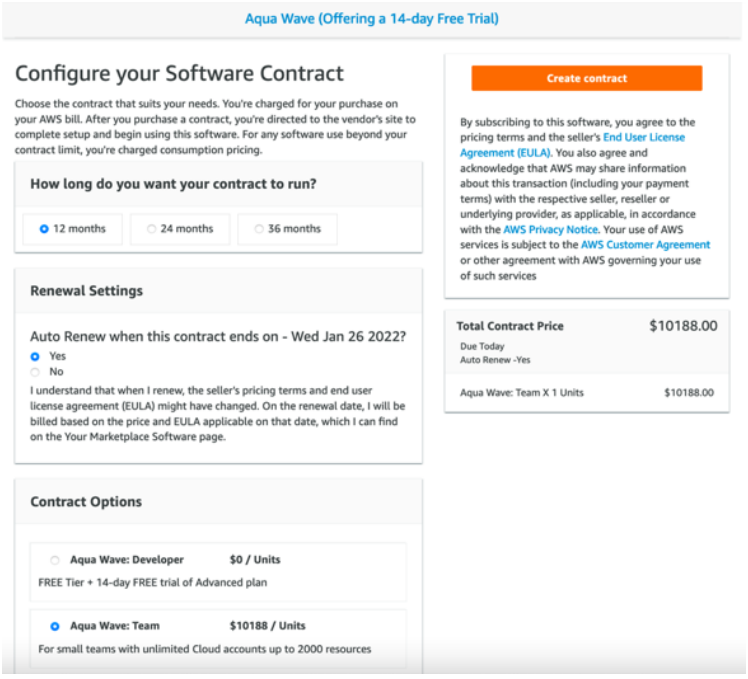
Ensure that you have an active subscription with Aqua Wave with Developer or higher plan. You can subscribe to the Aqua Wave listing on AWS Marketplace. It comes with a 14-day free trial of our Advanced tier and a perpetually free Developer edition as well.



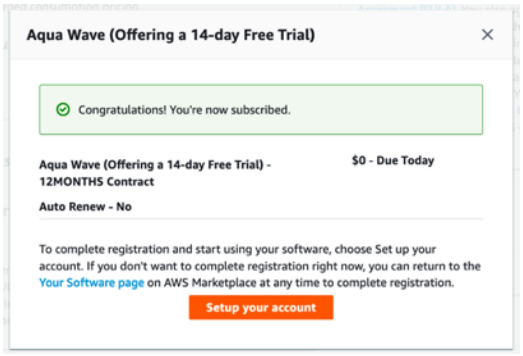
Click on **Continue to Subscribe** button.

Configure your Contract according to your requirements. Make sure to select the **Contract Duration** and **Renewal** preference.

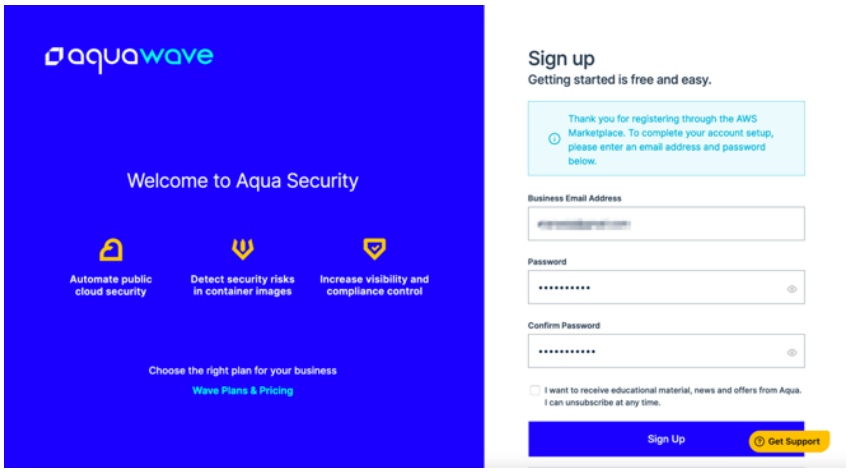
Click on **Create Contract** to purchase Aqua Wave from Marketplace



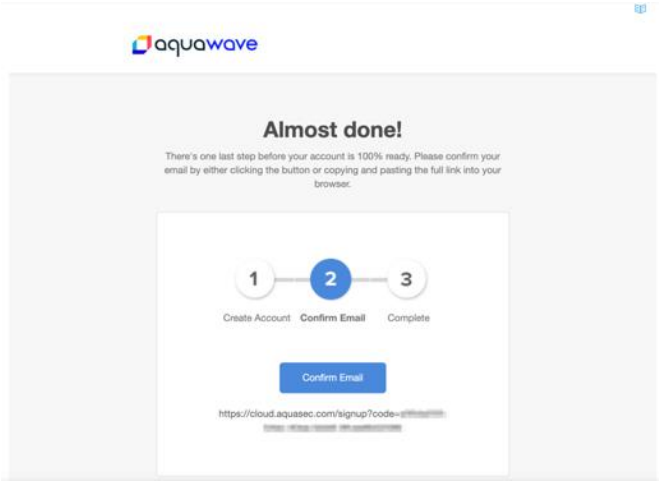
After you purchase the subscription, you will see a welcome screen that will enable you to sign up for Aqua Wave



When you click on **Setup your Account**, you will be redirected to the Aqua Wave Sign Up page where you can provide your email address for registration.



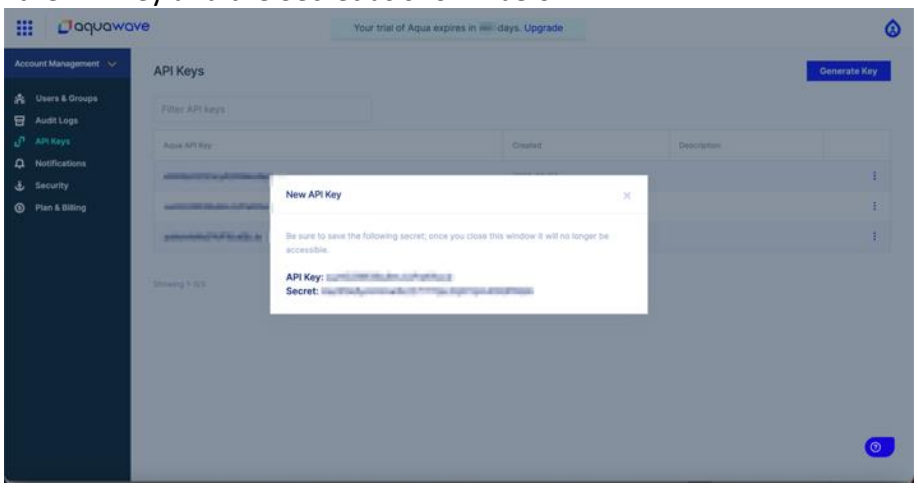
You will receive a verification email within minutes of completing the subscription, following which you can start using the Aqua CSPM functionality.



Step 1.2: Generate API key and Secret

Once registered, you can sign into the Aqua Wave portal and generate the API key by navigating to **Account Management > API Keys** and clicking on **Generate Key** button.

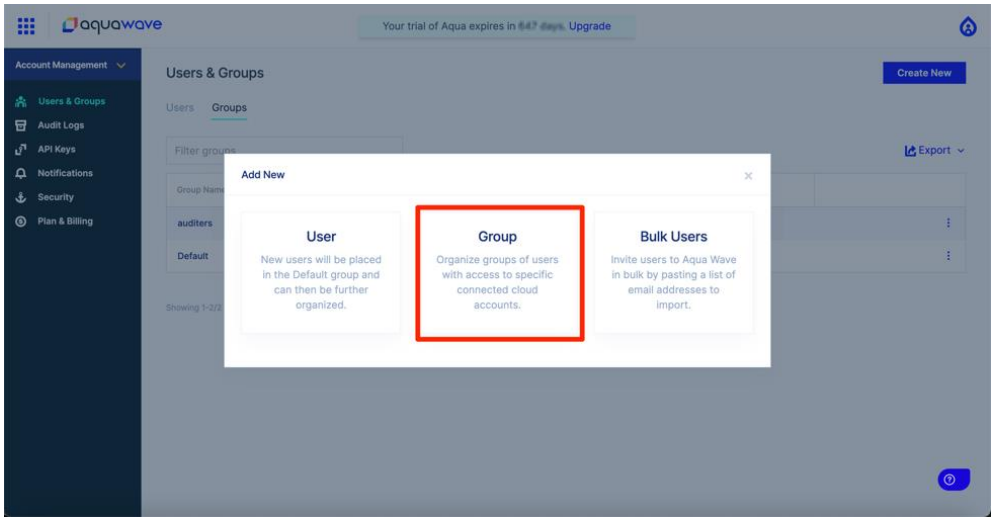
Make note of the API Key and the Secret as shown below



Step 1.3: Create a new Group in Aqua CSPM

Aqua CSPM comes with a Default group and can be used to add the newly provisioned accounts. Additionally, you can create a new Group and provide it as a parameter to CloudFormation StackSet.

For creating a new group, navigate to **Account Management > Users & Groups.** In the **Groups** tab, click on **Create New**.



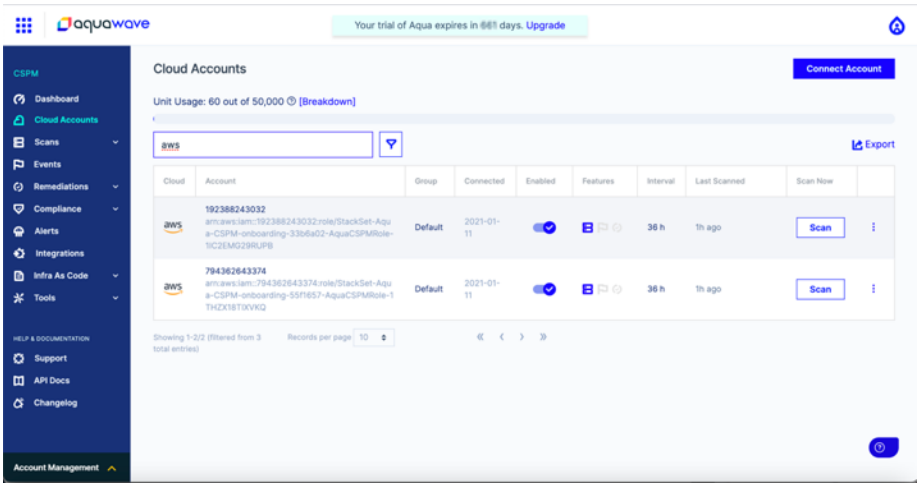
Note: Ideally, you will want to maintain group parity between the AWS Control Tower Organization Unit and the Aqua CSPM groups. It is recommended to name the Groups based on Business Unit or Organization Unit names. (E.g.: R&D, Sales etc.)

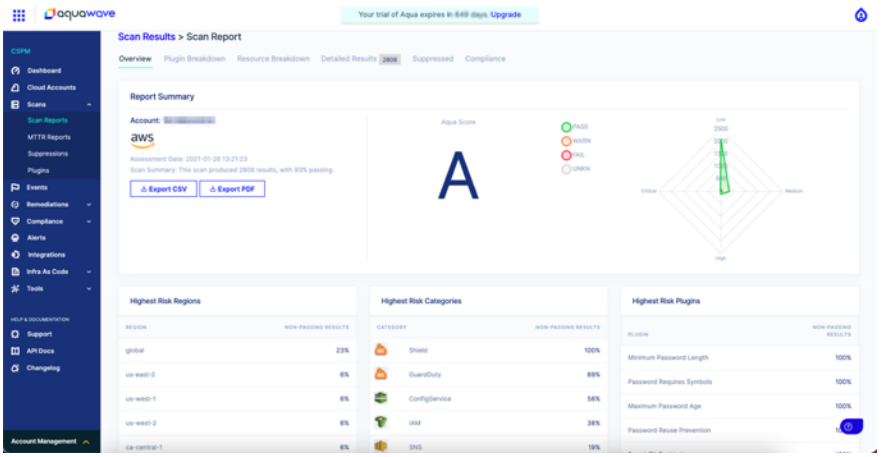
Step 2: Create the StackSet for this integration

1. Retrieve the CloudFormation template for the solution from our GitHub repository.
2. Log into your Management account and navigate to AWS Control Tower home region
3. Navigate to the AWS CloudFormation console
4. On the left navigation bar, select **StackSets** and click on **Create StackSet**
5. In the **Choose a template** step, either upload the YAML template or paste in the S3 URL for the template.
6. In the **Specify StackSet details** section, enter the **StackSet name** and input the **AquaCSPMAPIKey** and **AquaCSPMSecretKey that you captured in Step 1.2** along with the **AquaGroupName** from Step 1.3. Click **Next.**
7. On the **Configure StackSet options** page under **Permissions** section, select **Service-managed permissions**. Click **Next**.
8. On the **Set deployment options** page
    a. Under **Deployment targets** select **Deploy to organizational units (OUs)** and input the appropriate AWS Organization Unit ID.
    Note: Selecting an Organizational Unit (OU) allows you to create a mapping to a corresponding Group in Aqua CSPM for better management. You can choose deploying to Organization as well but that will lead to all the accounts being onboarded to the same Aqua CSPM Group.
    b. For **Automatic deployment**, select **Enabled**.
    c. For **Account removal behavior**, select **Delete stacks**.
    d. For **Specify regions**, select the home region.
    e. Leave the deployment options as default
    f. Click **Next**
9. Review the StackSet details and **acknowledge the creation of IAM resources** by clicking the checkbox.
10. Click **Submit**
11. You will be taken to “StackSet details” page, under the “Operations” tab, where you can monitor the progress of the stack set that you just attempted to create. Wait until you make sure, the Status reads SUCCEEDED

Step 3: Verify the automated onboarding of newly enrolled accounts into Aqua CSPM

1. Once a new account is enrolled from AWS Control Tower, it is automatically set up to allow your Aqua CSPM to scan, monitor and audit the account for compliance standards.
2. You can log into your Aqua Wave account and verify that the new account has been registered.





3. You can then go ahead and enable the Real-time events and Remediations for the accounts as per your need.

FAQs

https://wave-support.aquasec.com/support/solutions/16000060942

Solution Estimated Pricing

This solution can be deployed at no additional cost apart from the Aqua Wave plan that you registered for. Aqua Wave offers flexible pricing plans to fit your scale. Visit the Aqua Wave pricing page for more information.

Additional Resources

https://wave-support.aquasec.com/support/solutions

Partner contact information

For any questions or issues please reach out to us here.