Integrating Cequence Bot Defense SaaS with Akamai

Contents

About Cequence Bot Defense SaaS and Akamai ***2***

Step 1: Configure Application Availability **2**

Step 2: Configure Bot Defense SaaS Origin and Traffic Forwarding **3**

Step 2: Configure Bot Defense SaaS Origin and Traffic Forwarding - Loopback **5**

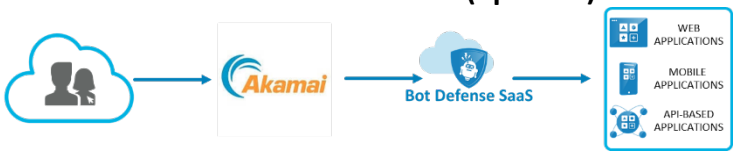
Pre-Shared Key Configuration 7

About Cequence Bot Defense SaaS and Akamai

Bot Defense SaaS uses an agentless, ML-based approach to eliminate avenues of fraud caused by account takeovers and API business logic abuse. When integrated with Akamai, traffic is directed to Bot Defense SaaS where it is analyzed by the CQAI ML-based automation indicators to determine malicious or benign intent. CQAI findings are then used to enforce policy or exported via a REST-based API to an existing component of your security infrastructure.

Traffic flow without Bot Defense SaaS:

Traffic flow with Bot Defense SaaS (option 1):



Traffic flow with Bot Defense SaaS in a loopback architecture (option 2):

The steps required to integrate Bot Defense SaaS with Akamai are relatively straightforward. All traffic that terminates on Akamai will be routed to Bot Defense SaaS first for inspection and then forwarded to the application origin (option 1) or forwarded back to Akamai from where it will be routed to the application origin (option 2).

Step 1: Configure Application Availability

Application availability must be ensured with the addition of Bot Defense SaaS to the traffic flow between Akamai and Application Origin.

In the rare event where Bot Defense SaaS becomes unavailable (determined via a health check), a fail-open must kick in and all application traffic from Akamai must get routed directly to the Application Origin, bypassing Bot Defense SaaS completely.

Such a fail-open scenario can be configured with a failover routing policy configuration. To create a failover routing policy, either one of the below solutions can be leveraged:

- Akamai Traffic Manager products - Global Traffic Management (GTM) or Application Load Balancer (ALB) Cloudlet
- Bot Defense SaaS Traffic Manager (for customers that don't use Akamai Traffic Manager products)

The failover routing policy will create a DNS hostname that will set two CNAME records pointing at the Bot Defense SaaS origin as the Primary, while the application origin acts as the Secondary.

This DNS hostname will be set as the origin hostname for forwarding application traffic to Bot Defense SaaS on the Akamai configuration.

Step 2: Configure Bot Defense SaaS Origin and Traffic Forwarding

To configure forwarding of all application traffic from Akamai to Bot Defense SaaS, modify the Origin Server Behavior along with the respective Origin SSL configuration.

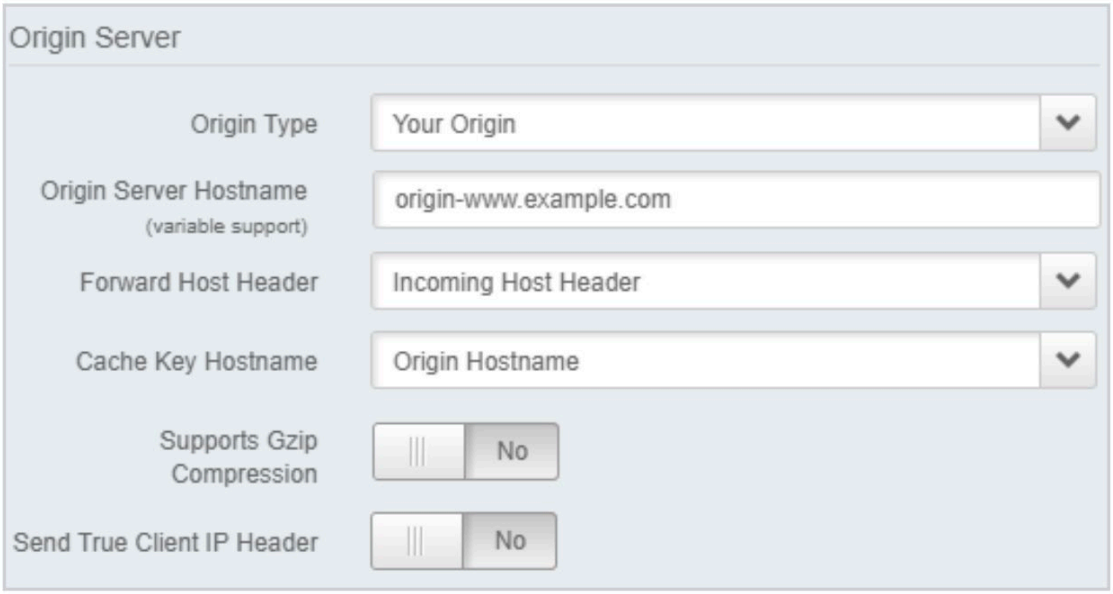


Image 1: Modify the Origin Server Behavior

- Under Akamai Property Manager, select the property configuration to be modified and go to the Behaviors section of the Default Rule.
- Select **Your Origin** in the Origin Type field.
- In the Origin Server Hostname field, enter the **DNS hostname created in Step 1**
- Select **Origin Hostname** in the Cache Key Hostname field.
- Choose **Yes** in the Supports Gzip Compression field.

- Choose **Yes** in the Send True Client Header field depending on whether you want to send the True Client IP header that Akamai sets.

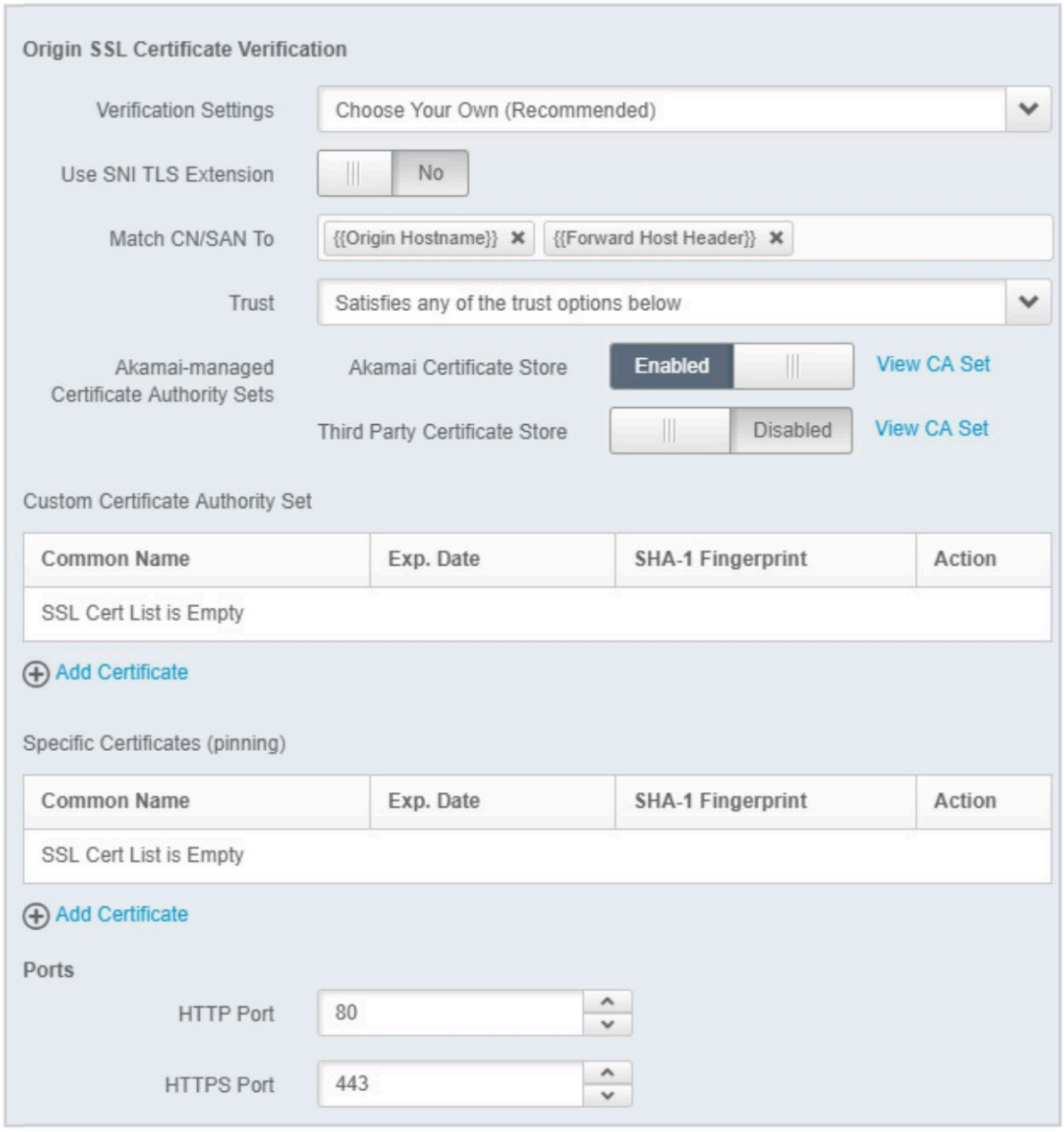


Image 2: Modify the Origin SSL Configuration

- In the **Verification Settings** field of the Origin SSL Certificate Verification section.

- Select **Choose Your Own (Recommended**) in the Verification Setting field of the Origin SSL Certificate Verification section.

- Select **Satisfies any of the trust options below** in the Trust field.

- Enable **Akamai Certificate Store** and **Third Party Certificate Store** in the Akamai-managed Certificate Authority Sets field. This represents Akamai's collection of trusted root certificates.

- [Optional] Add the certificates to the **Custom Certificate Authority Set** section and the **Specific Certificates (pinning)** section only if there is a need to pin either the intermediate or the leaf certificates.

Step 2: Configure Bot Defense SaaS Origin and Traffic Forwarding - Loopback

To configure forwarding of all application traffic from Akamai to Bot Defense SaaS, **add** the Origin Server Behavior along with the respective Origin SSL configuration.

Please note that in the case of **Loopback** traffic flow, the existing Application Origin configuration does not need to get modified. However, a conditional will need to be added to forward traffic to the application origin (see section Pre-Shared Key below); since all application traffic is forwarded to Bot Defense SaaS, by default.

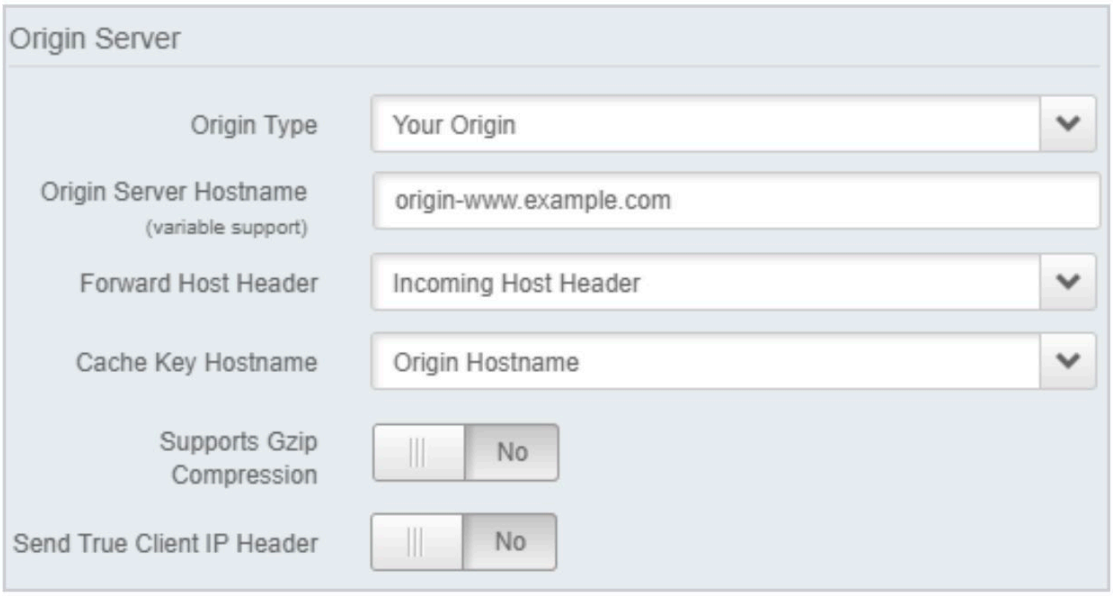


Image 3: Add the Origin Server Behavior

- Under Akamai Property Manager, select the property configuration to be modified and go to the Behaviors section of the Default Rule.

- Select **Your Origin** in the Origin Type field.

- In the Origin Server Hostname field, enter the **DNS hostname created in Step 1**

- Select **Origin Hostname** in the Cache Key Hostname field.

- Choose **Yes** in the Supports Gzip Compression field.

- Choose **Yes** in the Send True Client Header field depending on whether you want to send the True Client IP header that Akamai sets.

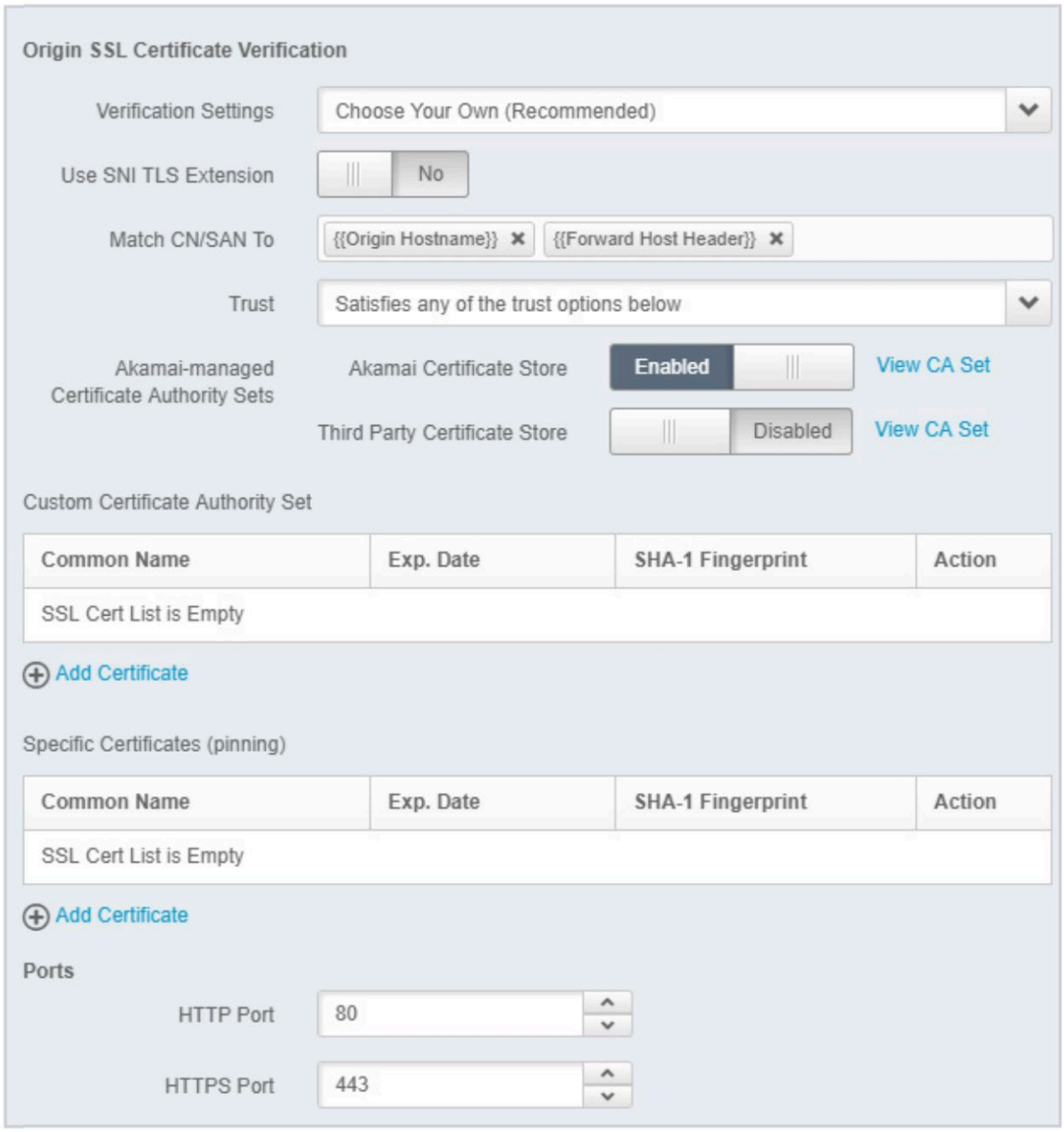


Image 4: Add the Origin SSL Configuration

- In the **Verification Settings** field of the Origin SSL Certificate Verification section.

- Select **Choose Your Own (Recommended**) in the Verification Setting field of the Origin SSL Certificate Verification section.

- Select **Satisfies any of the trust options below** in the Trust field.

- Enable **Akamai Certificate Store** and **Third Party Certificate Store** in the Akamai-managed Certificate Authority Sets field. This represents Akamai's collection of trusted root certificates.

- [Optional] Add the certificates to the **Custom Certificate Authority Set** section and the **Specific Certificates (pinning)** section only if there is a need to pin either the intermediate or the leaf certificates.

Pre-Shared Key Configuration

- As shown in the loopback architecture traffic flow diagram (option 2 on page 2), Akamai forwards all application traffic to Bot Defense SaaS, by default.

- Bot Defense SaaS then adds a pre-shared key in a specialized request header to all the application traffic it processes and forwards to Akamai.

- When this traffic hits Akamai again, placing a match on the presence of the pre-shared key in the specialized request header, Akamai makes the determination to no longer forward traffic to Bot Defense SaaS, and instead forwards it to the application origin.