

# Configure Youtube Traffic Optimization with Akamai Connect

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Akamai Connect and WAAS](#)

[Configure](#)

[Step 1. You need an SSL certificate signed by your internal/public CA.](#)

[Step 2. You need to trust your the intermediary and/or root Certificate Authority \(CA\) across your organization.](#)

[Step 3. Create an SSL accelerated Service on WAAS device using WAAS Central Manager GUI.](#)

[Step 4. Configure the SSL Accelerated Service.](#)

[Step 5. Upload certificate and private key.](#)

[Step 6. Verify the uploaded certificate information.](#)

[Step 7. Click the SUBMIT button and this is the end result.](#)

[Step 8. Enable Akamai Connect.](#)

[Step 9. Enable the SSL Interposer on the branch WAAS \(Required only for Single Side Setup\).](#)

[Verify](#)

[Step 1. You need to have Akamai Connect enabled on branch WAAS.](#)

[Step 2. Verify Youtube Acceleration on Client.](#)

[Step 3. Verify on WAAS.](#)

[Troubleshoot](#)

[Problem: Traffic is not accelerated by SSL AO.](#)

[Problem: The browser cannot connect to Youtube and there is no certificate pushed.](#)

[Problem: Traffic hits Akamai Connect Engine but there is no Cache hit.](#)

[Problem: Akamai Cache breaks HTTPS connection when going through a proxy with Authentication.](#)

## Introduction

This document describes the required steps for configuring Youtube Acceleration on Cisco Wide Area Application Services (WAAS) using Akamai Connect feature.

**Note:** Throughout this article, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE (Wide Area Application Engineer) refers to WAE and WAVE appliances, SM-SRE modules running WAAS, and vWAAS instances.

# Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco WAAS
- Public Key Infrastructure
- Secure Sockets Layer (SSL) Certificate

## Components Used

The information in this document is based on these software versions:

- Cisco WAAS version 5.5.1
- Cisco WAAS version 6.2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Background Information

## Akamai Connect and WAAS

The Akamai Connect feature is an HTTP/S object cache component added to Cisco WAAS. It is integrated into the existing WAAS software stack and is leveraged via the HTTP Application Optimizer. Akamai Connect helps reduce latency for HTTP/S traffic for business and web applications and can improve performance for many applications including POS (Point of Sale), HD video, digital signage, and in-store order processing. It provides significant and measurable WAN data offload and is compatible with existing WAAS functions such as DRE (deduplication), LZ (compression), TFO (Transport Flow Optimization), and SSL acceleration (secure/encrypted) for first and second pass acceleration.

These terms are used with Akamai Connect and WAAS:

- Akamai Connect - Akamai Connect is an HTTP/S object cache component added to Cisco WAAS, integrated into the existing WAAS software stack and leveraged via the HTTP Application Optimizer. WAAS with Akamai Connect helps to reduce latency for HTTP/S traffic for business and web applications.
- Akamai Connected Cache - Akamai Connected Cache is a component of Akamai Connect, which allows the cache engine (CE) to cache content that is delivered by an Edge server on the Akamai Intelligent Platform.

# Configure

## **Step 1. You need an SSL certificate signed by your internal/public CA.**

The certificate needs to include the following SubjectAltName:

\*.youtube.com

\*.googlevideo.com

\*.ytimg.com

\*.ggpht.com

youtube.com

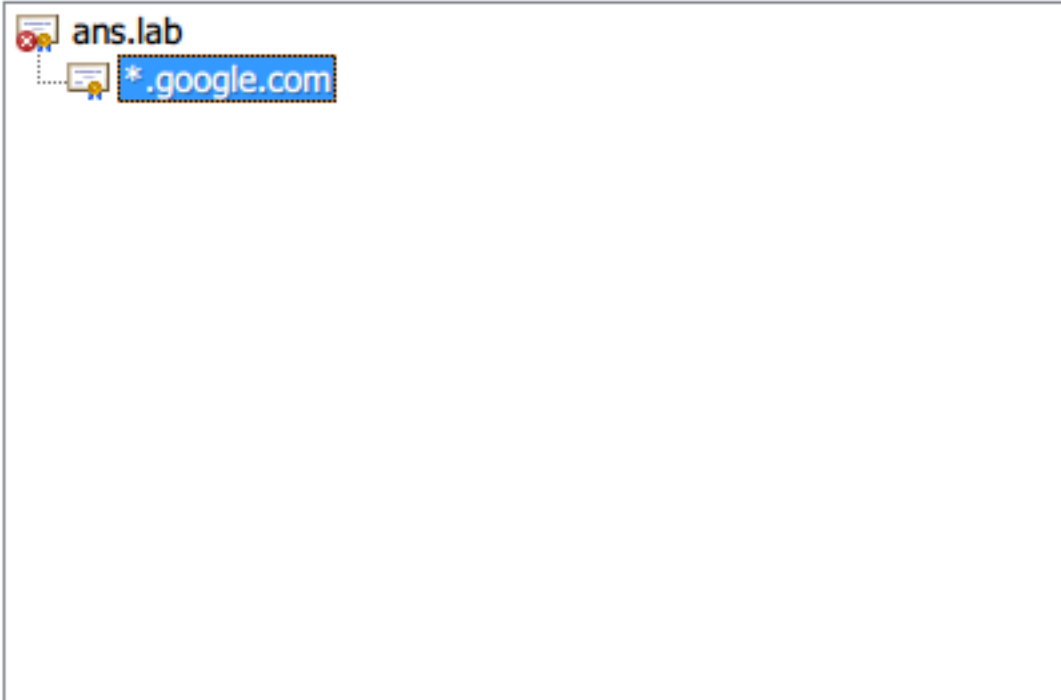
This is an example certificate:

Certificate



General Details Certification Path

Certification path



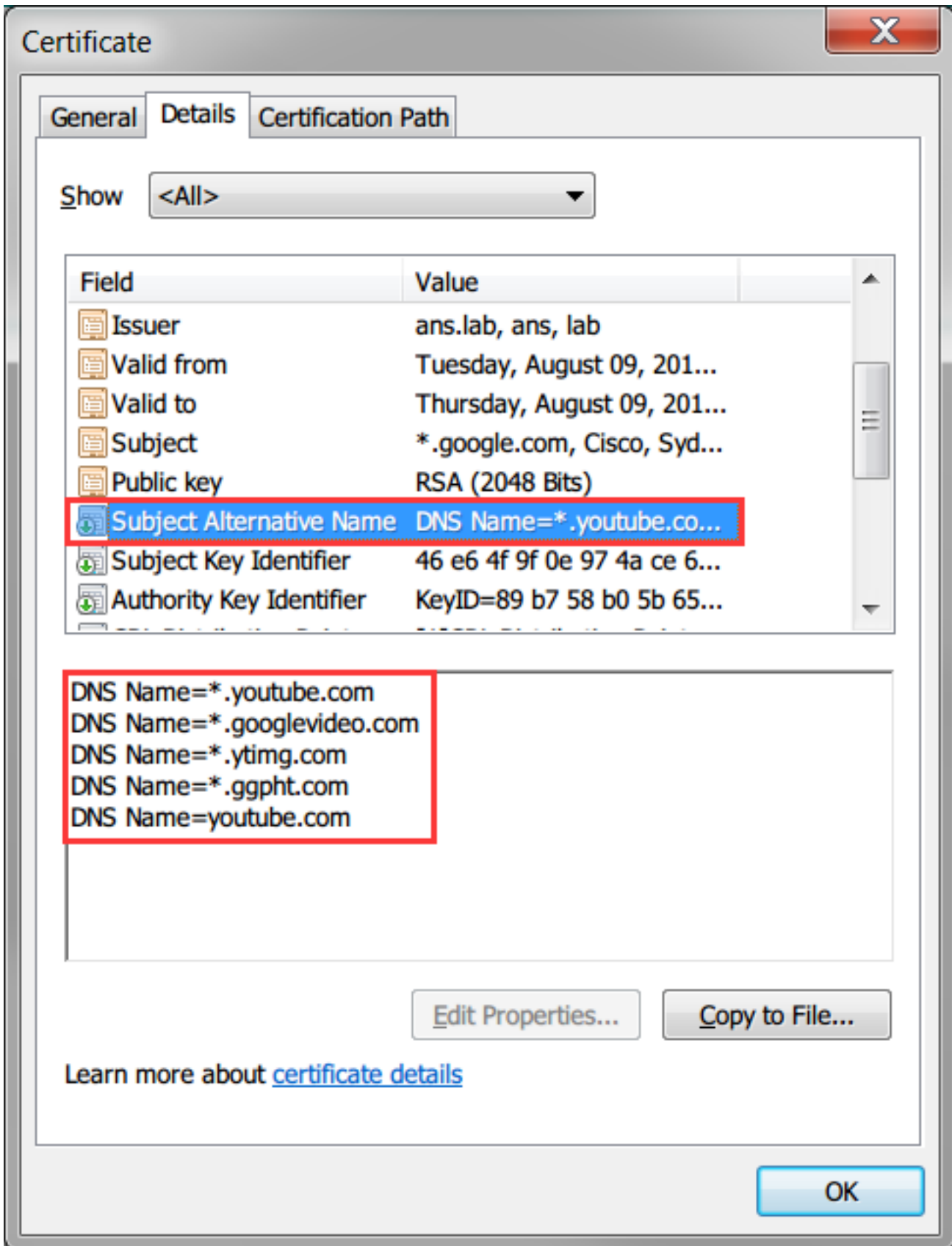
View Certificate

Certificate status:

This certificate is OK.

Learn more about [certification paths](#)

OK



**Step 2. You need to trust your the intermediary and/or root Certificate Authority (CA) across your organization.**

This can be achieved by using Group Policy across the Active Directory domain.

If you are testing this setup in a lab, you can install the intermediary and/or root CA in the client device as a Trusted CA.

Certificate



General Details Certification Path



### Certificate Information

**This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.**

**Issued to:** ans.lab

**Issued by:** ans.lab

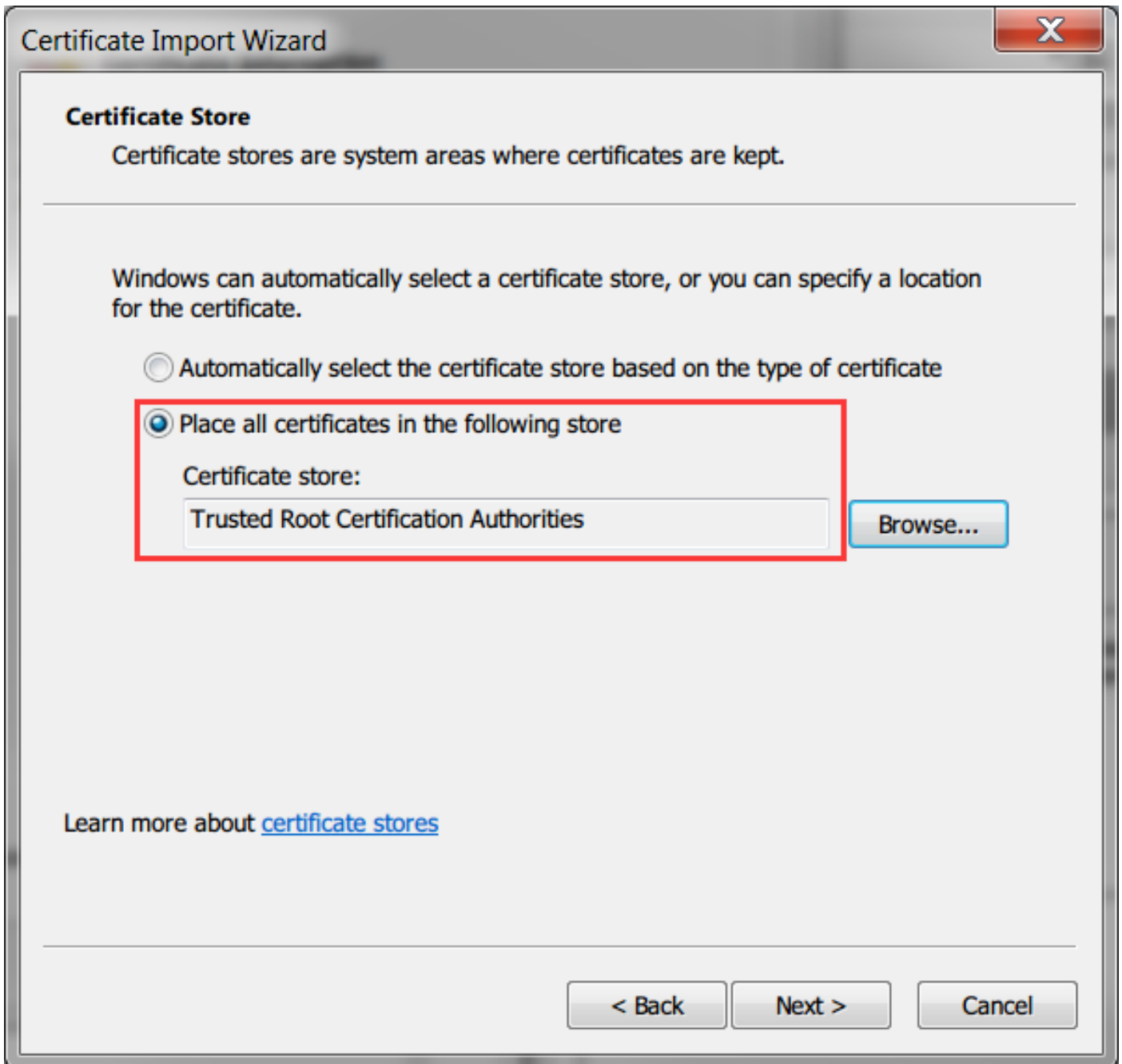
**Valid from** 8/ 8/ 2016 **to** 8/ 8/ 2021

**Install Certificate...**

Issuer Statement

Learn more about [certificates](#)

OK



### Step 3. Create an SSL accelerated Service on WAAS device using WAAS Central Manager GUI.

On dual sided Akamai (pre WAAS 6.2.3) configure the SSL accelerated service on the core WAAS. For single sided Akamai (WAAS 6.2.3 or later) configure the SSL accelerated server on the branch WAAS and enable the SSL interposer. This is the only difference between dual side setup and single side setup.

**Note:** WAAS running software release prior to 6.2.3 needs a dual sided Akamai setup to accelerate Youtube Traffic The core WAAS proxies the SSL connection going to Youtube. WAAS running software release 6.2.3 or later supports SSL AO v2 (SAKE). This allows the branch WAAS to proxy the SSL connection when the branch sends traffic directly to the internet without being directed through the datacentre infrastructure.

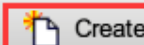


Navigate to **Devices > Configure > Acceleration > SSL Accelerated Service**, as shown in the image:

Devices | AppNav Clusters | Locations

Configure | Monitor | Admin

- AppNav Cluster**
  - AppNav Cluster
- Interception**
  - Interception Configuration
  - Interception Access List
- Acceleration**
  - Enabled Features
  - Accelerator Threshold
  - TCP Settings
  - TCP Adaptive Buffering Settings
  - DRE Settings
  - HTTP/HTTPS Settings
  - SMB Settings
  - SMB Preposition Settings
  - MAPI Settings
  - ICA Settings
  - Optimization Class-Map
  - Optimization Policies
  - SSL Accelerated Services**
- File Services**
  - SMB Dynamic Shares
- Caching**
  - Akamai Connect
  - Device Profile
- Storage**
  - Disk Encryption
- Security**
  - Secure Store
  - Windows Domain
  - SSL
  - Peering Service
  - Management Service
  - AAA
- Peers**
  - Peer Settings
- Network**
  - Network Interfaces
  - Default Gateway
  - Management Interface Settings
  - Jumbo MTU
  - Port Channel
  - TCP/IP Settings
  - CDP
  - DNS
  - Network Services
  - Console Access
- Monitoring**
  - Alarm Overload Detection
  - Flow Monitor
  - SNMP
  - Log Settings
- Date/Time**
  - NTP
  - Time Zone

Devices > DC-WAVE-7571 > Configure > Acceleration > **SSL Accelerated Services**

SSL Accelerated Services for WAE, DC-WAVE-7571  Create  Refresh  Print

Current applied settings from WAE, DC-WAVE-7571

**SSL Accelerated Services**

#### Step 4. Configure the SSL Accelerated Service.

If you use an explicit proxy, Protocol Chaining needs to be enabled. HTTP AO must be applied to the TCP port used for proxying the traffic (for example, 80 or 8080).

**Match Server Name Indication** needs to be checked. In this setup, when the core WAAS receives SSL traffic, it compares the SNI field in the Client Hello with the SubjectAltName in uploaded certificate. If the SNI field matches the SubjectAltName the core WAAS proxies this SSL traffic.





When the **Match Server Name Indication** field is checked, use **Any** for IP Address and **443** for Server Port. Click **Add** to add this entry.

- └─ TLSv1 Record Layer: Handshake Protocol: **Client Hello**
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 198
  - └─ Handshake Protocol: Client Hello
    - Handshake Type: Client Hello (1)
    - Length: 194
    - Version: TLS 1.2 (0x0303)
    - Random
      - Session ID Length: 0
      - Cipher Suites Length: 28
    - Cipher Suites (14 suites)
    - Compression Methods Length: 1
    - Compression Methods (1 method)
    - Extensions Length: 125
    - Extension: renegotiation\_info
    - └─ Extension: server\_name
      - Type: server\_name (0x0000)
      - Length: 20
      - └─ Server Name Indication extension
        - Server Name list length: 18
        - Server Name Type: host\_name (0)
        - Server Name length: 15
        - Server Name: **www.youtube.com**

*Server Name Indication (SNI)*

## Step 5. Upload certificate and private key.

You need to provide a certificate and private key. The example shown in the image uses PEM format:

[Generate self-signed certificate and private key](#)

[Import existing certificate and optionally private key](#)

**i** It is recommended to use certificates of 1024 bit key size and avoid using certificate chains if you plan to configure more than 128 accelerated services(up to 512).

Mark private key as exportable

Upload file in PKCS#12 format

Upload file in PEM format

Paste certificate and key in PEM-format

Passphrase to decrypt private key:

Upload key:  Google.com.key

Upload certificate:  Google.com.cer

[Export certificate and key](#)

[Generate certificate signing request](#)

Optional Client Certificate and private key

[Import existing client certificate and optionally private key](#)

## Step 6. Verify the uploaded certificate information.

**Certificate Info**

Certificate in PEM encoded form

### Issued To

Common Name: \*.google.com

Email:

Organization:

Organization Unit: Cisco

Locality: Sydney

State: NSW

Country: AU

Serial Number: 199666714554801961566220

### Issued By

Common Name: ans.lab

Email:

Organization:

Organization Unit:

Locality:

State:

Country:

### Validity

Issued On: Mon Aug 08 14:58:06 GMT 2016

Expires On: Wed Aug 08 15:08:06 GMT 2018

### Fingerprint

SHA1: 0A:A3:69:A2:5D:91:5F:66:1E:F2:59:76:A0:A8:DB:21:E3:AE:68:84


Base64: CqNpol2RX2Ye8ll2oKjbIeOuaIQ=

### Key

Type: SHA1WITHRSA

Size (Bits): 2048

## Step 7. Click the SUBMIT button and this is the end result.

SSL Accelerated Services for WAE, DC-WAVE-7571							Create	Refresh	Print
Current applied settings from WAE, DC-WAVE-7571				- Go to the SSL Global Settings page to modify selection.					
SSL Accelerated Services			Items 1-1 of 1		Rows per page: 25	Go			
<input type="checkbox"/>	Name ▲	Service Address/Port	Issued To	Issuer	Expiry Date	Service Status			
<input type="checkbox"/>	 Youtube-OTT	Any:443		ans.lab	Aug 08 2018	Enabled			

## Step 8. Enable Akamai Connect.

Navigate to **Devices > Configure > Caching > Akamai Connect**.

Cache Settings
Cache Prepositioning

Enable Akamai Connect

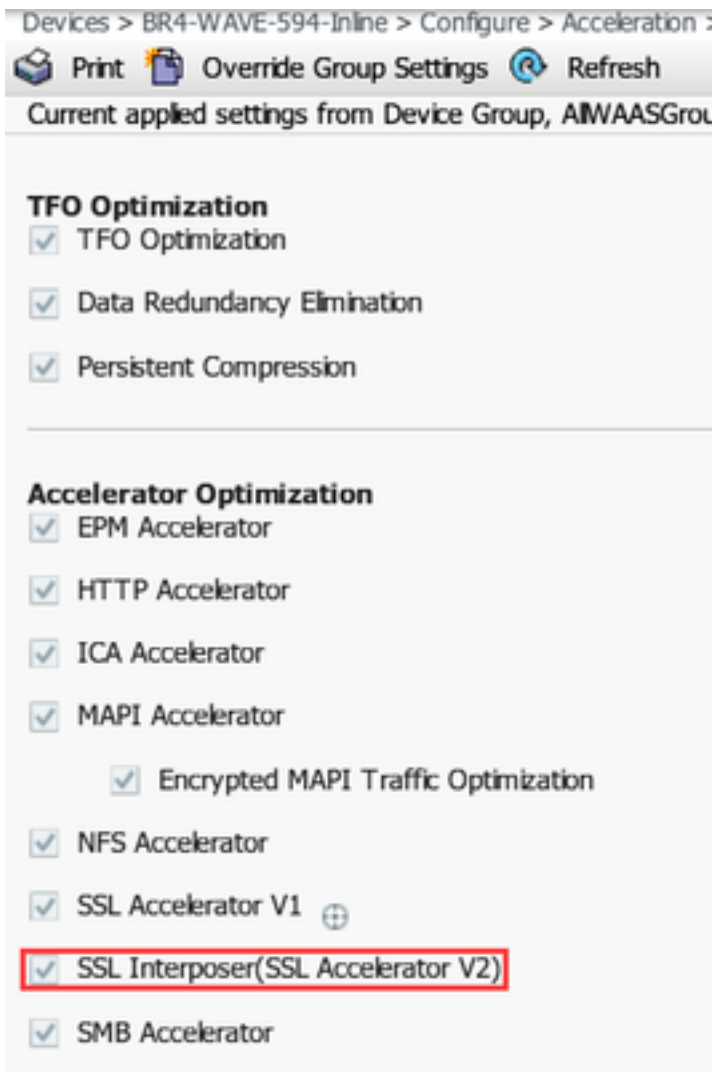
---

▼ **Edit Settings**

Akamai Connected Cache

Over the top Cache

**Step 9. Enable the SSL Interposer on the branch WAAS (Required only for Single Side Setup).**



## Verify

**Step 1. You need to have Akamai Connect enabled on branch WAAS.**

WAAS-BRANCH# show accelerator http object-cache

```

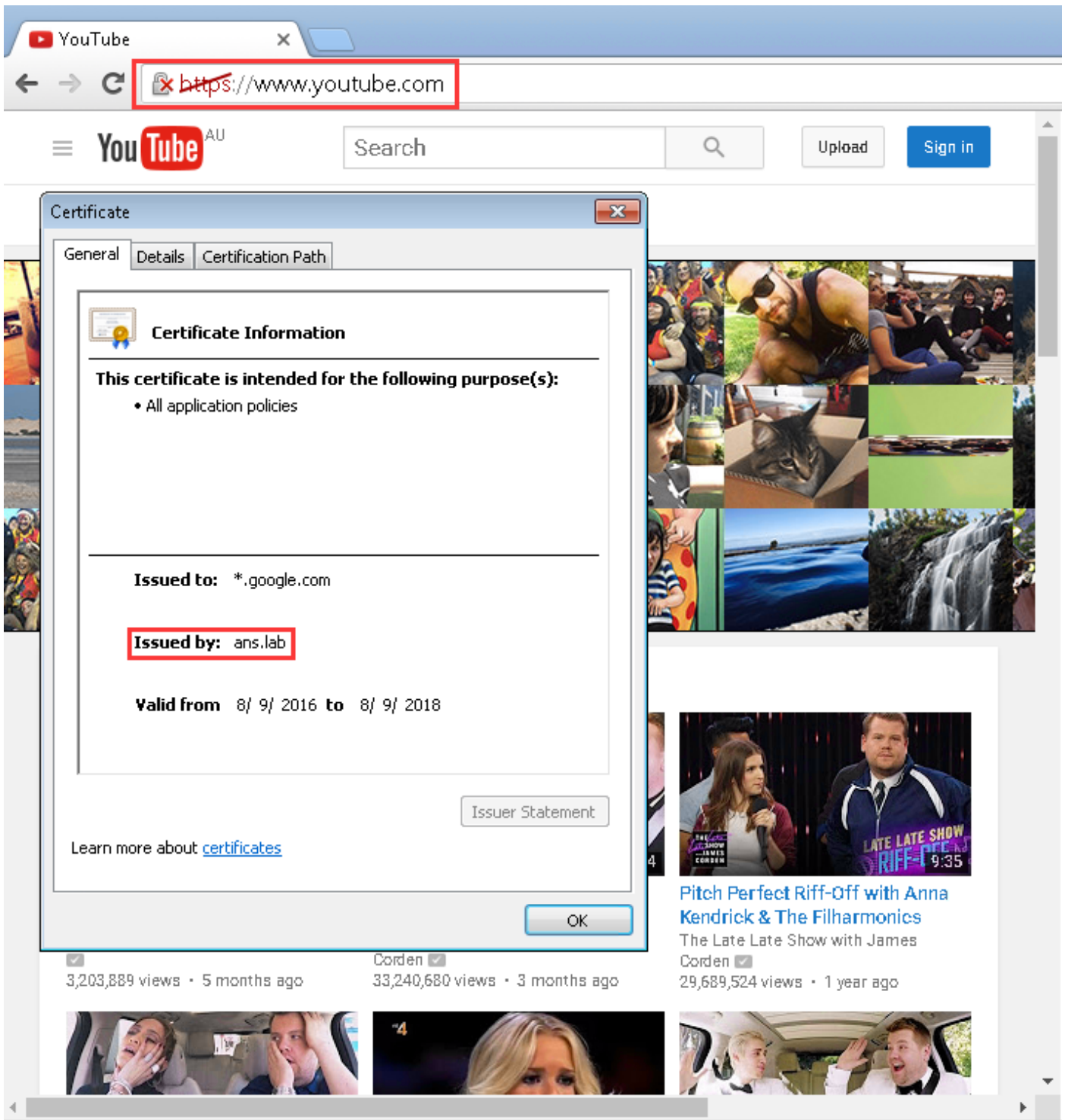
HTTP Object-cache
.....
Status
-----
                Operational State
                -----
                Running Akamai Connected Cache State ----- Connected

```

Ensure Operational State is **Running** and Connect State is **Connected**.

**Step 2. Verify Youtube Acceleration on Client.**

When you access Youtube you must see the certificate signed by your own CA:



### Step 3. Verify on WAAS.

Verify if SSL AO is correctly applied to the traffic:

Example Output from the CLI when running WAAS software prior to 6.2.3 (SSL AO v1 and Dual Site Setup)

WAAS-BRANCH# **show statistics connection**

ConnID	Source IP:Port	Dest IP:Port	PeerID	Accel	RR
6859	10.66.86.90:13110	10.66.85.121:80	00:06:f6:e6:58:56	THSDL	51.9%
6839	10.66.86.90:13105	10.66.85.121:80	00:06:f6:e6:58:56	THSDL	16.6%
6834	10.66.86.90:13102	10.66.85.121:80	00:06:f6:e6:58:56	THSDL	93.5%
6733	10.66.86.90:13022	10.66.85.121:80	00:06:f6:e6:58:56	THSDL	72.7%

6727 10.66.86.90:13016 10.66.85.121:80 00:06:f6:e6:58:56 THSDL 03.9%

## Example Output from the CLI when running WAAS software 6.2.3 or later (SSL AO v2 and Single Site Setup)

### WAAS-BRANCH# show statistics connection

ConnID	Source IP:Port	Dest IP:Port	PeerID	Accel	RR
3771	10.66.86.66:60730	58.162.61.183:443	N/A	THs	50.9%
3770	10.66.86.66:60729	58.162.61.183:443	N/A	THs	52.1%
3769	10.66.86.66:60728	58.162.61.183:443	N/A	THs	03.0%
3752	10.66.86.66:60720	208.117.242.80:443	N/A	THs	54.8%
3731	10.66.86.66:60705	203.37.15.29:443	N/A	THs	13.8%
3713	10.66.86.66:60689	58.162.61.142:443	N/A	THs	40.4%
3692	10.66.86.66:60669	144.131.80.15:443	N/A	THs	10.4%

Check the ce-access-errorlog on the branch WAAS. Log entries for optimized traffic have a code of 10000 associated with them (Indicate classified as OTT-Youtube) and h - - 200 indicates that the object cache is hit and traffic is served locally. The most acceleration is expected on googlevideo. You can open multiple browsers on the test machine and play the same video at the same time to test the setup:

### Sample output from ce-errorlog:

```
08/09/2016 01:49:26.612 (fl=5948) 10000 0.002 0.033 1356 - - 148814 10.66.86.90 10.66.85.121
2905 h - - 200 GET https://r5---sn-uxanug5-
ntqk.googlevideo.com/videoplayback?dur=703.721&ei=ozapV8jrGdWc4AKytYaYBQ&fexp=3300116%2C3
300131%2C3300161%2C3312739%2C3313265%2C9422596%2C9428398%2C9431012%2C9433096%2C9433223%2C9433946
%2C9435526%2C9437
066%2C9437552%2C9438327%2C9438662%2C9438804%2C9439580%2C9442424%2C9442920&requiresssl=yes&initcwn
dbps=6383750&gir=
yes&sparams=clen%2Cdur%2Cei%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Ckeepalive%2Clmt%2Cmi
me%2Cmm%2Cmn%2Cms
%2Cmv%2Cpl%2Crequiresssl%2Csource%2Cupn%2Cexpire&signature=34635AFA02C12695F90E50E067E6BD4B7E5821
32.DEB68217D77D25
F02925B272C6B3F032D3764535&ipbits=0&ms=au&mt=1470706873&pl=22&mv=m&mm=31&mn=sn-uxanug5-
ntqk&keepalive=yes&key=yt6
&ip=64.104.248.209&clen=10444732&sver=3&source=youtube&itag=251&lmt=1466669747365466&upn=1700mSa
Uqq4&expire=14707 28963&id=o-ABXm_M_rqaPqauN_rtx9jNvU4NPYMD-wx-
oJw0mAUclg&mime=audio%2Fwebm&cpn=YsB-Jmb04EU-BeHl&alr=yes&ratebypass
=yes&c=WEB&cver=1.20160804&range=136064-284239&rn=4&rbuf=8659 - - 08/09/2016 01:49:26.899
(fl=5887) 10000 0.003 0.029 1357 - - 191323 10.66.86.90 10.66.85.121 2905 h - - 200 GET
https://r5---sn-uxanug5-
ntqk.googlevideo.com/videoplayback?dur=703.721&ei=ozapV8jrGdWc4AKytYaYBQ&fexp=3300116%2C3
300131%2C3300161%2C3312739%2C3313265%2C9422596%2C9428398%2C9431012%2C9433096%2C9433223%2C9433946
%2C9435526%2C9437
066%2C9437552%2C9438327%2C9438662%2C9438804%2C9439580%2C9442424%2C9442920&requiresssl=yes&initcwn
dbps=6383750&gir=
yes&sparams=clen%2Cdur%2Cei%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Ckeepalive%2Clmt%2Cmi
me%2Cmm%2Cmn%2Cms
%2Cmv%2Cpl%2Crequiresssl%2Csource%2Cupn%2Cexpire&signature=34635AFA02C12695F90E50E067E6BD4B7E5821
32.DEB68217D77D25
F02925B272C6B3F032D3764535&ipbits=0&ms=au&mt=1470706873&pl=22&mv=m&mm=31&mn=sn-uxanug5-
ntqk&keepalive=yes&key=yt6
&ip=64.104.248.209&clen=10444732&sver=3&source=youtube&itag=251&lmt=1466669747365466&upn=1700mSa
Uqq4&expire=14707 28963&id=o-ABXm_M_rqaPqauN_rtx9jNvU4NPYMD-wx-
oJw0mAUclg&mime=audio%2Fwebm&cpn=YsB-Jmb04EU-BeHl&alr=yes&ratebypass
=yes&c=WEB&cver=1.20160804&range=284240-474924&rn=6&rbuf=17442 - -
```

The output from **show statistic acceleration http object-cache** must also show ott-youtube hits increasing:

WAAS-BRANCH# **show statistics accelerator http object-cache**

..... Object Cache Caching Type: ott-youtube Object cache transactions served from cache:  
52 Object cache request bytes for cache-hit transactions: 68079 Object cache response bytes for  
cache-hit transactions: 14650548 .....

## Troubleshoot

### **Problem: Traffic is not accelerated by SSL AO.**

Solution:

Check if SSL AO matches the SNI on the core WAAS with these debug command:

This is an example of a successful output from ssl-errorlog:

```
WAAS# debug accelerator ssl sni
08/09/2016 01:33:23.721sslao(20473 4.0) TRCE (721383) SNI(youtube.com) matched with certificate
SNA youtube.com [c2s.c:657] 08/09/2016 01:33:23.962sslao(20473 6.0) TRCE (962966)
SNI(youtube.com) matched with certificate SNA youtube.com [c2s.c:657]
```

This is an example of an unsuccessful output from ssl-errorlog:

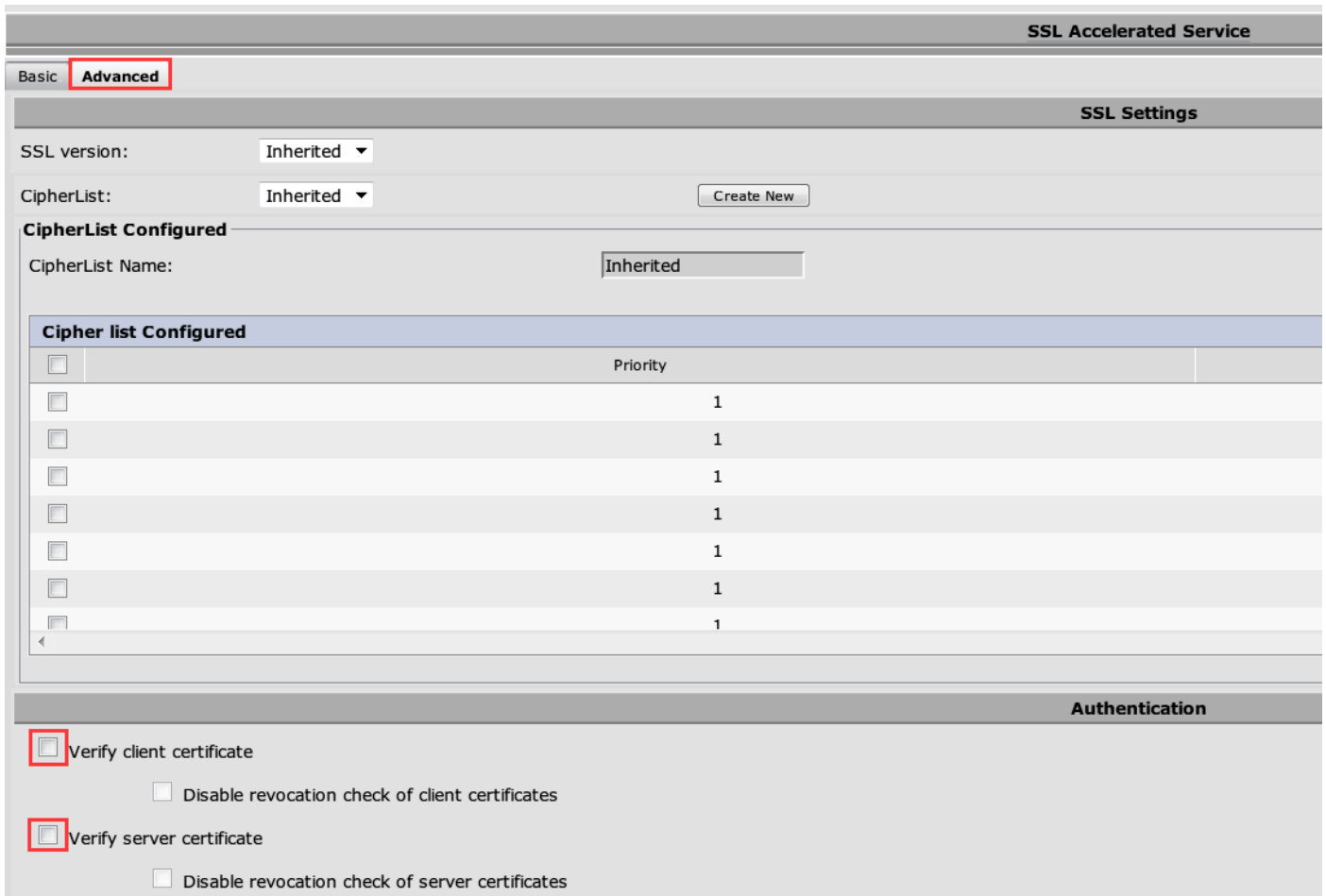
```
WAAS# debug accelerator ssl sni
08/09/2016 01:19:35.929sslao(20473 5.0) NTCE (929983) Unknown SNI: youtube.com [sm.c:4312]
08/09/2016 01:20:58.913sslao(20473 3.0) TRCE (913804) Pipethrough connection unknown
SNI:youtube.com IP:10.66.85.121 ID:655078 [c2s.c:663]
```

### **Problem: The browser cannot connect to Youtube and there is no certificate pushed.**

Solution:

This can be caused by the core WAAS not trusting the certificate pushed by Youtube.

Uncheck this on SSL accelerated service.



**Problem: Traffic hits Akamai Connect Engine but there is no Cache hit.**

Solution:

This can be caused by enforcing the If-Modified-since (IMF) check on the branch WAAS. The IMS option may check the enforced logging of users activity to a proxy server or usage analysis device. When IMS check is enabled, in the current OTT version, Youtube always requests the client to fetch the latest copy from the origin server.

This can be observed in ce-access-errorlog:

```
07/20/2016 00:41:49.420 (fl=36862) 10000 2.511 0.000 1312 1383 4194962 4194941 10.37.125.203
10.6.76.220 2f25 l-s s-ims-fv - - 200 GET https://r3---sn-jpuxj-
coxe.googlevideo.com/videoplayback?signature=AACC537F02B652FEA0600C90
0B069CA3063C15CD.58BA962C80C0E7DFA9A6664ECDCE6404A3E2C65&clen=601694377&pl=24&mv=m&mt=146897480
1&ms=au&ei=a8ioV- HZG4u24gL-hpu4BQ&mn=sn-jpuxj-
coxe&mm=31&key=yt6&sparams=clen%2Cdur%2Cei%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2C
itag%2Ckeepalive%2Clmt%2Cmime%2Cmm%2Cmn%2Cms%2Cmv%2Cpl%2Crequiressl%2Csource%2Cupn%2Cexpire&sver
=3&gir=yes&fexp=9
416891%2C9422596%2C9428398%2C9431012%2C9433096%2C9433221%2C9433946%2C9435526%2C9435876%2C9437066
%2C9437553%2C9437
742%2C9438662%2C9439652&expire=1468996811&initcwndbps=9551250&ipbits=0&mime=video%2Fmp4&upn=B-
BbHfjKlaI&source=yo utube&dur=308.475&id=o-ABCCH12_QzDMemZ8Eh7hbsSbhXZQ7yt325a-
xfqNRok1&lmt=1389684805775554&itag=138&requiressl=yes&
ip=203.104.11.77&keepalive=yes&cpn=4cIAF7ZEwNbfV7Cr&alr=yes&ratebypass=yes&c=WEB&cver=1.20160718
&range=193174249- 197368552&rn=68&rbuf=23912 - -
```

Uncheck these on the branch WAAS to disable IMS checking:

Navigate to **Configure > Caching > Akamai Connect.**



Enable Akamai Connect[▶ Edit Settings](#)

### ▼ Advanced Cache Settings

Default Transparent Caching Policy: \*

Standard

#### Site Specific Transparent Caching Policy

[Add Site Specific Transparent Caching Policy](#) [Edit](#) [Delete](#)

	<input type="checkbox"/>	Hostname/IP	Transparent Caching Policy
1	<input type="checkbox"/>	broomenorthp...	Bypass

 Force IMS DIA ? Force IMS Always ? Use HTTP Proxy for connections to Akamai network ?

This issue is expected to be fixed in WAAS 6.3 and beyond.

### **Problem: Akamai Cache breaks HTTPS connection when going through a proxy with Authentication.**

Solution:

When you need to go through a proxy before going to the internet and the proxy requires authentication, WAAS may break the HTTPS connection. Packet capture taken on branch WAAS shows the response of HTTP 407 from the server site. However, the capture stops after the first packet. Subsequent packets are not sent and the response is incomplete.

This is tracked in defect [CSCva26420](#) and is likely to be fixed in WAAS 6.3 release.