

Oracle CPQ with Akamai Integration Guide

TABLE OF CONTENTS

Revision History	2
Introduction	2
Considerations	2
Akamai Reference Links	2
Prerequisites	2
Setup Overview	3
Certificate Provisioning	4
Oracle CPQ Application Setup	8
Akamai Property Template Setup	8
Akamai Rule Creation	9
Akamai Rule Behavior Settings	12
Default Rule	14
Compression Rule	19
Old IE Browsers Rule	19
Old Mozilla Browsers Rule	20
Redirect to HTTPS	21
Dynamic Content	21
Disable Chunk for Migration	22
Static Content	23
Pre-WAF Rule	24
Embargoed Country Blocking	24
Splash Assets	25
Non-Splash Assets	25
Image Manager	27
Add UA to Cache Key	28
Save the Template Property	29
Akamai Property Clone Setup	29
Testing in Staging Environment	35
Edit hosts file	35
DNS Change	36
Purging Akamai Cache	36
Deactivation and Activation of Property	37
Handling Site Changes	37
Troubleshooting	38
Log Delivery Service	39

REVISION HISTORY

This document will continue to evolve as existing sections change and new information is added. All updates appear in the following table:

DATE	WHAT'S CHANGED	NOTES
NOV 2020	Embargoed Country Blocking	Updated list of embargoed countries
JUN 2020		Initial Document Creation

INTRODUCTION

Akamai is a content delivery network that primarily acts as a proxy between the browser (other clients) and the Oracle CPQ Site (origin server). When a browser makes a request to the Oracle CPQ site, the request is routed through Akamai servers (edge servers) that sit between the origin server and the end user. This routing helps cache and serve the content based on the property setup in Akamai.

This document provides an overview of how to configure Oracle CPQ for use with Akamai. This integration was introduced by Oracle CPQ release 19D. It is intended solely to help you assess the business benefits of upgrading to 19D and to plan your IT projects

Considerations

Implementing this functionality requires the skills of an experienced Akamai administrator. Oracle does not warranty any of the included code snippets; Oracle cannot certify these against future versions of Akamai or Oracle CPQ.

As with all changes to your CPQ application and associated integrations, administrators are strongly encouraged to work in a sandbox/test site prior to making any changes to a production environment. Any changes should be thoroughly documented and commented to enable future changes or troubleshooting.

Akamai Reference Links

Akamai Control Center: <https://control.akamai.com>

Akamai Documentation: <https://learn.akamai.com>

Prerequisites

The following are the prerequisites to perform the Oracle CPQ and Akamai integration:

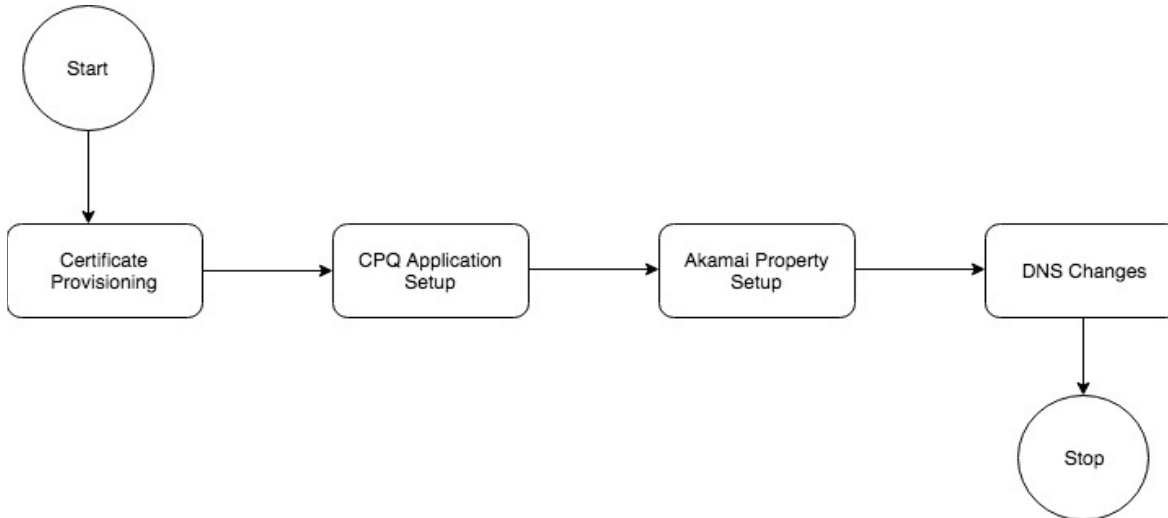
- Current customer contract with Oracle for CPQ.
- Oracle CPQ Site must have a vanity domain. This should be a domain that matches one owned by the customer. So, instead of megacorp.bigmachines.com, it can be cpq.megacorp.com. This will route all customer domain requests to Akamai edge.
- SSL certificate for your company's online presence. Identify the point of contact in your organization who manages the SSL certificate for your company's online presence. This point-of-contact will need to provide information from the SSL certificate during this process.
- Current customer contract with Akamai including:
 - Access to Akamai Control Center associated with Akamai account
 - Access to provision certificates
 - Access to create Akamai property

SETUP OVERVIEW

The setup activities are organized into the following areas within this document:

1. Certificate Provisioning
2. CPQ Application Setup
3. Akamai Property Template Setup
4. DNS Change

The following diagram shows the typical flow for integrating Akamai for a new customer.

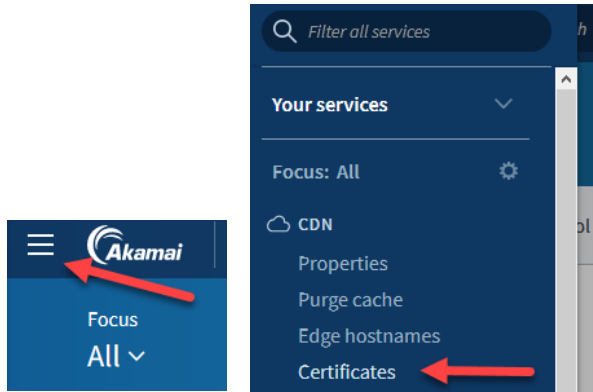


The first step is to create a new SSL Certificate. This usually takes time as the Certificate Signing Request (CSR) needs to be generated and approved by the Certificate Authority (CA). Once the certificates are provisioned, then CPQ Application Setup needs to be performed. Once the CPQ site is ready then Akamai property needs to be configured, tested, and deployed to the production network. The final step to taking this live is to make the DNS Changes.

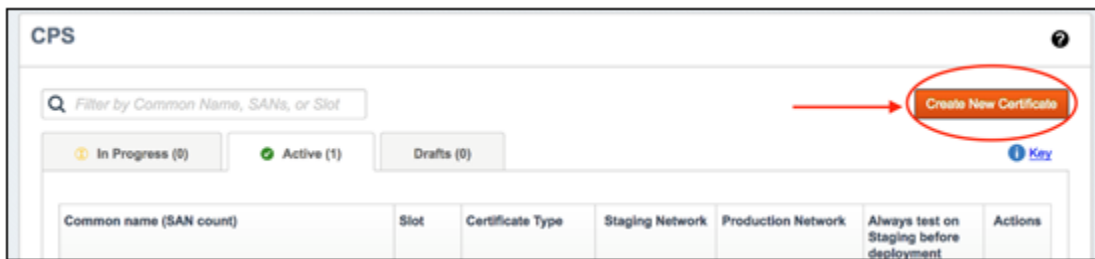
Note: Akamai may alter its administration interfaces from those represented in this document. However, even with an interface change, the goals documented in these steps remain the same.

CERTIFICATE PROVISIONING

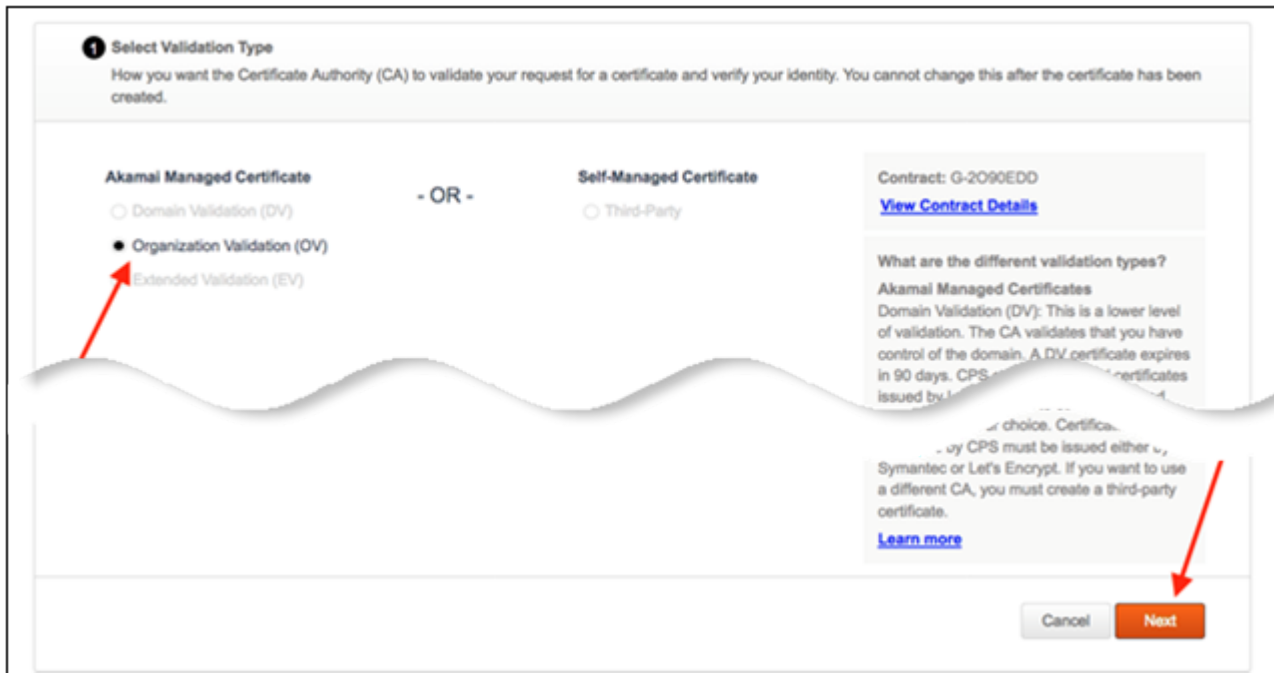
In the Akamai Control Center menu, navigate to **Certificates**.



1. Click **Create New Certificate**. The Step 1: Select Validation Type page opens.



2. Select **Organization Validation (OV)** under Akamai Managed Certificate.



3. Click **Next**. The Step 2: Select Certificate Settings page opens.

4. Select **Subject Alternative Names (SAN)** for Certificate Type.

2 Select Certificate Settings
Select the type of certificate and the certificate authority that will be used for this certificate. You cannot change this after the certificate has been created.

Certificate Type ● **Subject Alternative Names (SAN)**
 Single
 Wildcard
 Wildcard SAN

What are the different types of certificate?
SAN certificate: Uses Subject Alternative Names and allows you to secure up to 100 property hostnames with one certificate.
Single certificate: Associates a property hostname with a certificate.
... is DV certificate...
... and OV and EV certificates ...
from Symantec. If you want to use a different CA, you need to create a third-party certificate.
[Learn more](#)

Cancel **Next**

5. Click **Next**. The Step 3: Enter Certificate Information page opens.

6. Using the SSL certificate for your organization's online presence as a reference, enter the following:

- **Common Name (CN)**
- **SANs (optional)**
- **Company Information**

3 Enter Certificate Information
The hostnames and organization information to be included in the certificate issued by the Certificate Authority.

Common Name (CN)
 Skip CN FQDN Validation

What do I enter for common name (CN)?
Enter the common name (CN) you want to use for the certificate in the Common Name field. The company entered in the Company Information field must have the legal rights to use the domain in this certificate. You can also enter custom data in the Common Name field (CN). In these cases, you can skip this option. The CN field is always required.

SANs (optional)
[Clear All](#)

What is a SAN?
A SAN is a Subject Alternative Name. This field allows you to enter alternate or additional hostnames that you are using this certificate for. SAN validation is required.

Company Information

What do I enter for company name?
Enter the name of the company or organization requesting this certificate. Enter the name as it appears in all legal documents and as it appears in the legal entity filing. The organization or company you specify here must own or have legal rights to use the hostnames in the Common Name (CN) and SAN fields.
[Learn more](#)

What do I enter for main business phone number?
The main phone number of the company. For OV and EV certificates, the Certificate Authority will use this phone number to contact the Administrator. This phone number should match what is published by third-party.

- Verify that the information matches the reference SSL certificate **exactly** then click **Next**. The Step 4: Enter Company Information page opens.
- Accept the default for Company Information, if applicable, and click **Next**. The Step 5: Enter Contact Information page opens.

- Enter the following information:
 - Administrator Contact Information**
 - Akamai Technical Contact Information**

Note: Contact Akamai for the technical contact associated with your account.

- Click **Next**. The Step 6: Select Network Settings page opens.

11. Accept the defaults for the following:

- **Deployment Network**
- **Geographical Deployment**
- **SNI-Only**

6 Select Network Settings
These settings allow you to specify how your certificate deploys to the Akamai Secure CDN, most cannot be changed after the certificate has been created.

Deployment Network Standard TLS Enhanced TLS

Geographical Deployment Excludes China & Russia

SNI-Only On Off

How do the deployment networks differ?
Standard TLS: Provides a rich set of TLS and HTTPS functionality architected to provide high-performance, and massively scalable delivery of media assets and website content using customer branded certificates supporting SNI compatibility.

Why can't I change Geographical Deployment?
If you leave...

What is SNI-Only?
Server Name Indication (SNI) is an extension of the Transport Layer Security (TLS) networking protocol.

Cancel Review

12. Click **Review**.

13. Review the data and then click **Submit**. Once submitted, you receive a confirmation message.

CPS > Create New Certificate

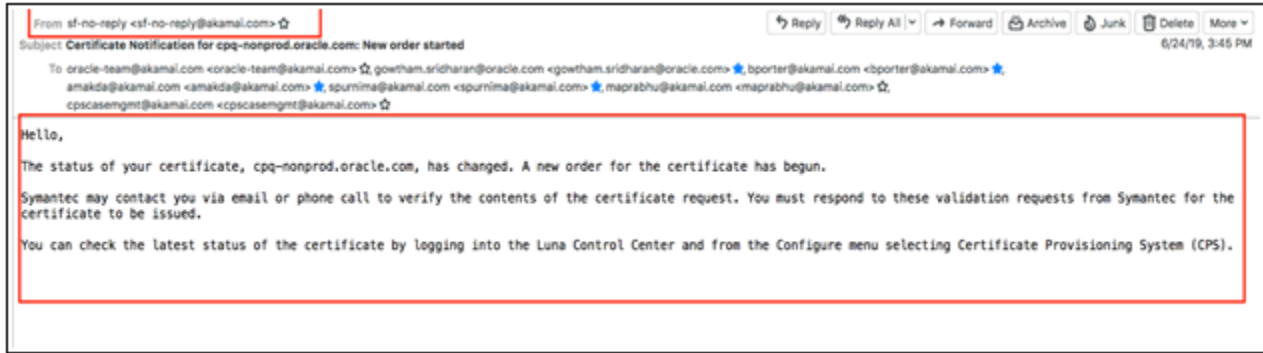
Success!
Your certificate request has been successfully submitted.

Next Steps
CPS is generating a certificate signing request (CSR), and will send it to the CA for signing. The CA will compare the information on the certificate to data in Whois and call the admin contact to verify the certificate request. It may take a few days to receive the signed certificate back from the CA.

Done

14. Click **Done**.

Status updates for the certificate throughout the process will be sent via email.



ORACLE CPQ APPLICATION SETUP

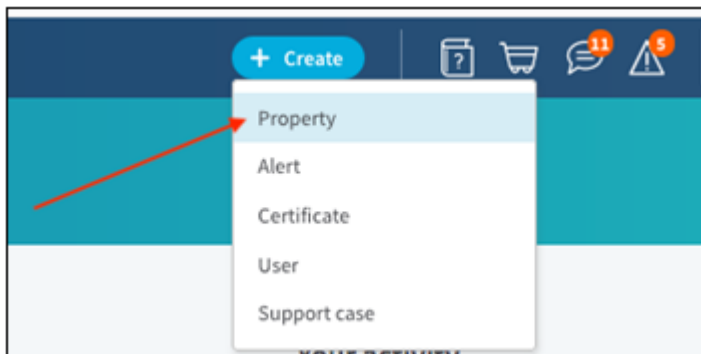
In [My Oracle Support](#), log a Technical Service Request (SR) with the instructions: "Please enable Akamai for CPQ environment <your CPQ environment>."

The SR is routed to the CPQ Operations team, who will deploy a test html file to the CPQ application for testing Akamai connectivity.

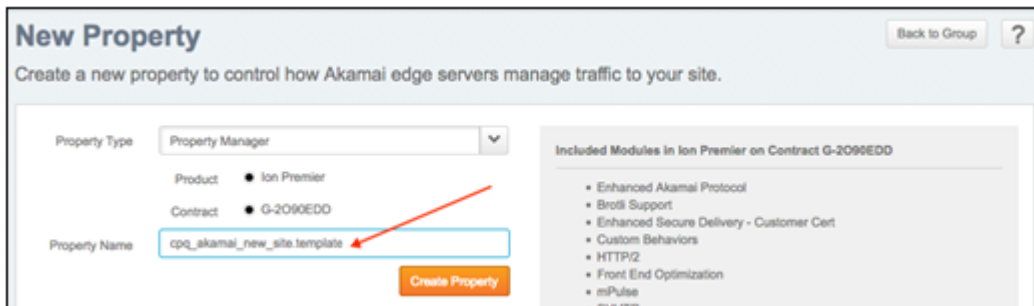
Akamai Property Template Setup

A property is a unique file with customizable rules that control how Akamai servers deliver CPQ content, and where caching behavior is configured.

1. Create a template from the properties home page by navigating to **+ Create** → Property. The New Property page opens.

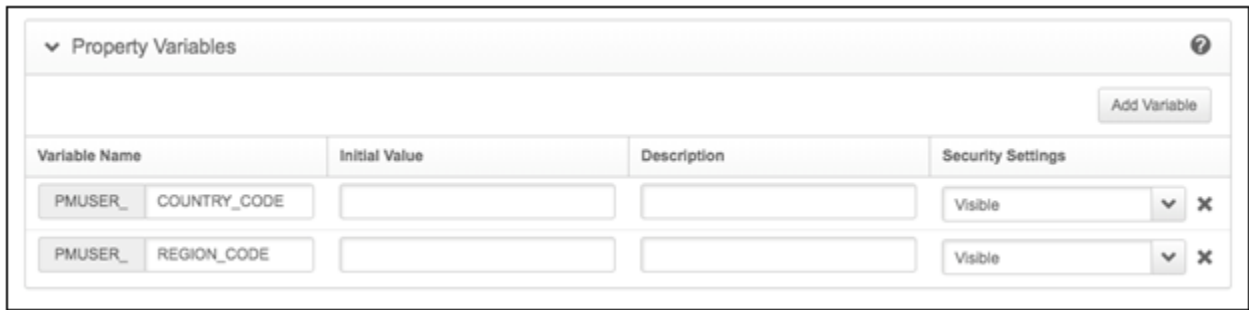


2. Enter **cpq_akamai_new_site.template** for the Property Name.



3. In Property Variables, click **Add Variable**.

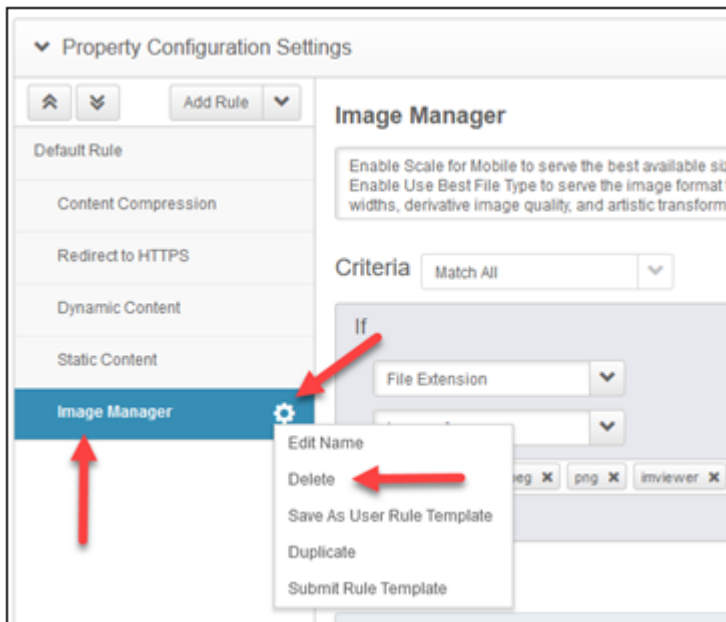
4. Add **COUNTRY_CODE** and **REGION_CODE** variables under Variable Name within the Property Variables section.



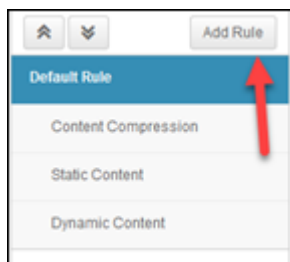
Akamai Rule Creation

Note: The following steps walk you through creating rules that are specific to Oracle CPQ environments and continue from [Akamai Property Template Setup](#).

5. In Property Configuration Settings section, delete any default rules under Default Rule except for Content **Compression**, **Static Content**, and **Dynamic Content**, as follows:
 - a. Click on the name of the rule to select it.
 - b. Click the rule's gear icon.
 - c. Click **Delete**.

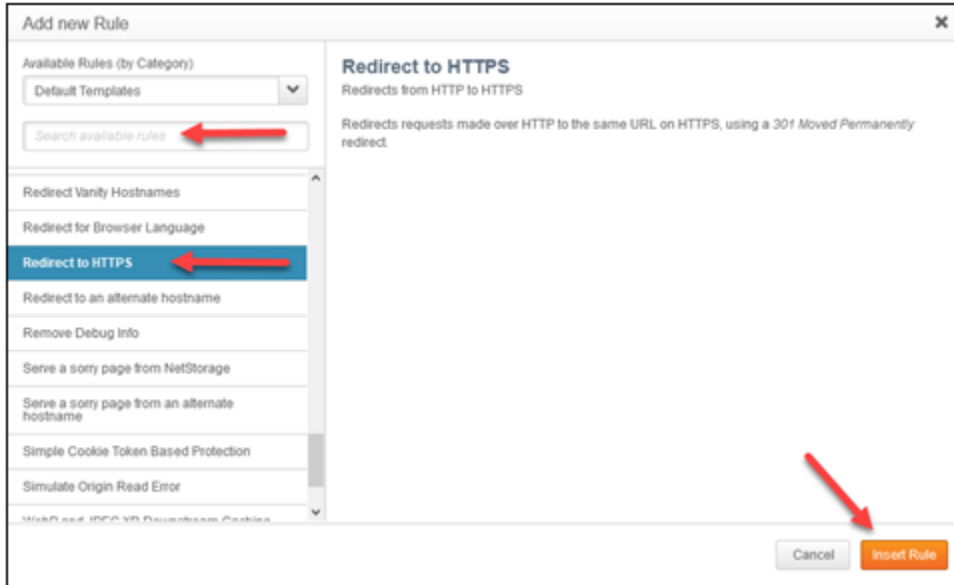


6. Add **Redirect to HTTPS** and **Image Manager** by selecting them from the available rules as follows:
 - a. Click **Add Rule**.

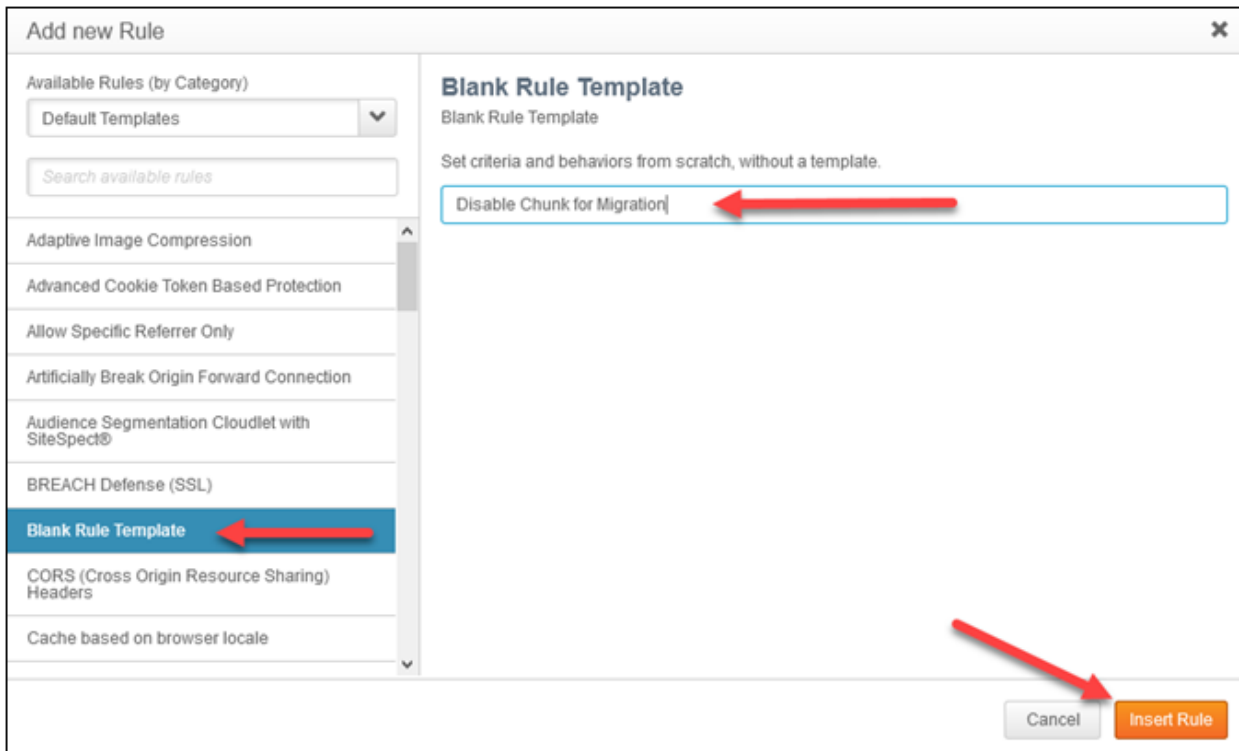


- b. (Optional) In the Add new Rule window, type the rule name in Search available rules to filter the list.

- c. Click the rule to select it from the list of available rules.
- d. Click **Insert Rule**.



- 7. Add **Old IE browsers, Old Mozilla browsers, Disable Chunk for Migration, Pre-WAF, Embargoed Country Blocking, Splash Assets, Non-Splash, Add UA to Cache Key, and Remove Vary Header** by creating them from blank rule templates as follows:
 - a. Click **Add Rule**.
 - b. Select **Blank Rule Template** in the Add new Rule window.
 - c. For each rule, type its name in the field under Blank Rule Template.
 - d. Click **Insert Rule**.



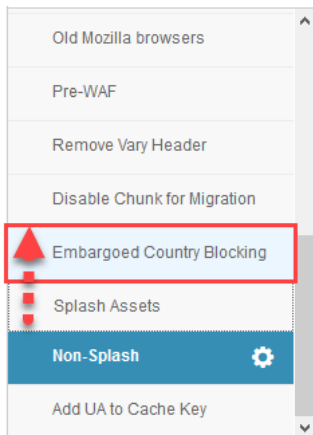
8. Re-order rules to match the hierarchy below:

Default Rule

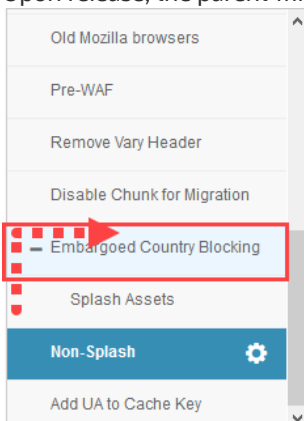
- └Content Compression
 - └Old IE Browsers
 - └Old Mozilla Browsers
- └Redirect to HTTPS
- └Dynamic Content
- └Disable Chunk for Migration
- └Static Content
- └Pre-WAF
 - └Embargoed Country Blocking
 - └Splash Assets
 - └Non-Splash
- └Image Manger
- └Add UA to Cache Key
 - └Remove Vary Header

Default Rule
└ Content Compression
Old IE browsers
Old Mozilla browsers
Redirect to HTTPS
Dynamic Content
Disable Chunk for Migration
Static Content
└ Pre-WAF
└ Embargoed Country Blocking
Splash Assets
Non-Splash
Image Manager
└ Add UA to Cache Key
Remove Vary Header

- To change a rule's position, click and drag the rule a new position and release the rule when its predecessor is highlighted.



- To place a rule as a child of another rule, drag it to the right before releasing.
 - The child rule name will be indented
 - Upon release, the parent will display an 'expanded' icon (-)



- To remove a child from its parent, click the child and drag left.

Akamai Rule Behavior Settings

- For each rule, you need to define Criteria and Behaviors.
The following are general editing instructions:
 - To specify a Criteria, click **Add Match**.
 - To specify a Behavior, click **Add Behavior**.

Example Rule View Rule JSON

Add a comment...

Criteria Match All Add Match

Click on the "Add Match..." button to specify a criteria

Behaviors Add Behavior

Click on the "Add Behavior..." button to specify a behavior

- For Behaviors, filter the list by typing in the search field (optional), select a Behavior, and then click **Insert Behavior**.

Add a Behavior for this Rule

Available Behaviors (By Category)

All

allow

Allow All Methods on Parent Servers

Allow DELETE

Allow OPTIONS

Allow PATCH

Allow POST

Allow PUT

Allow DELETE

Allow use of the DELETE HTTP request method. By default, GET or HEAD are the only methods honored, and others are denied with a 403. With this behavior enabled, DELETE requests pass to the origin, and do not cache.

Allow DELETE

Behavior Allow

Allow Body Deny

Cancel Insert Behavior

- To remove a Criteria or Behavior, hover over its block and click (X).

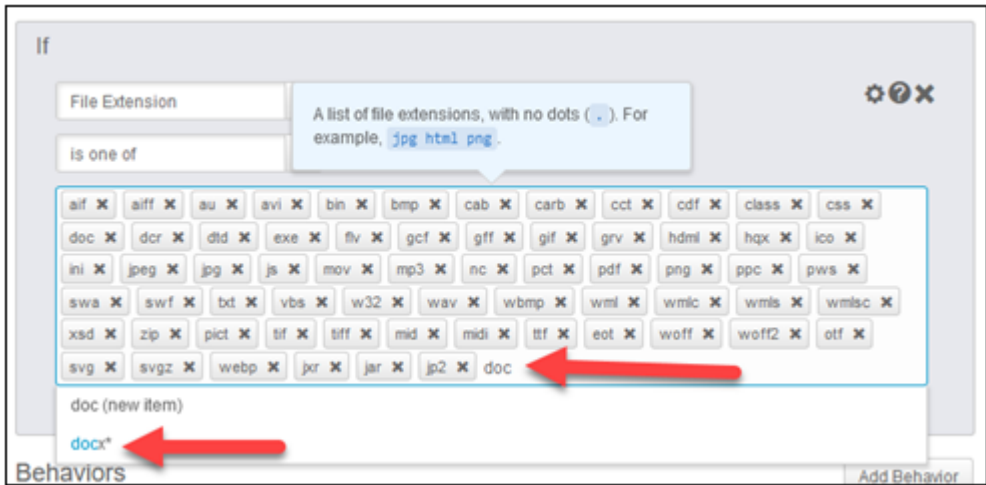
If

Hostname

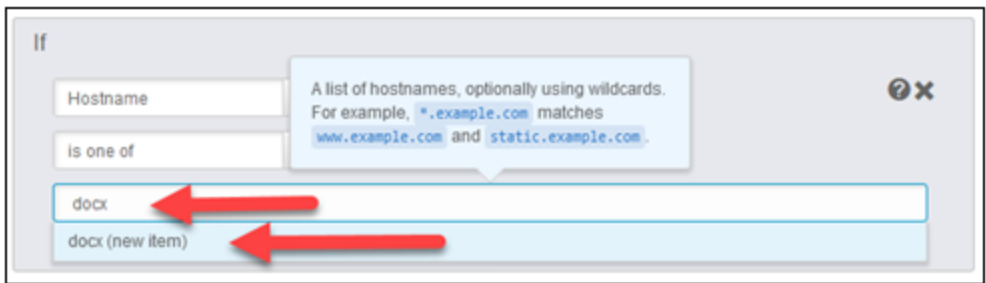
is one of

abc

- To add a Criteria value, click in its value field.
 - If a list of values is available, begin typing to filter the list, then click a value to select it. An informational balloon may be shown to guide you to expected values.



- If no list of values is available, type the value and click on <value> (new item) in the list to add it.



- To delete a value, click on the (X) to delete it.



- To re-order Behaviors, click and drag the behavior's block to move it.

DEFAULT RULE

Default Rule is applied to all requests, depending upon the Akamai contract.

Set indicated values for the following behaviors, adding any as necessary. Other default values for behaviors should be left as-is.

Origin Server

- **Origin Server Hostname:** Enter the CPQ Application server i.e. myCompany.bigmachines.com
- **Send True Client IP Header:** Yes
- **Verification Settings:** Choose Your Own
- **Match CN/SAN To:** *.bigmachines.com (Delete any other values)

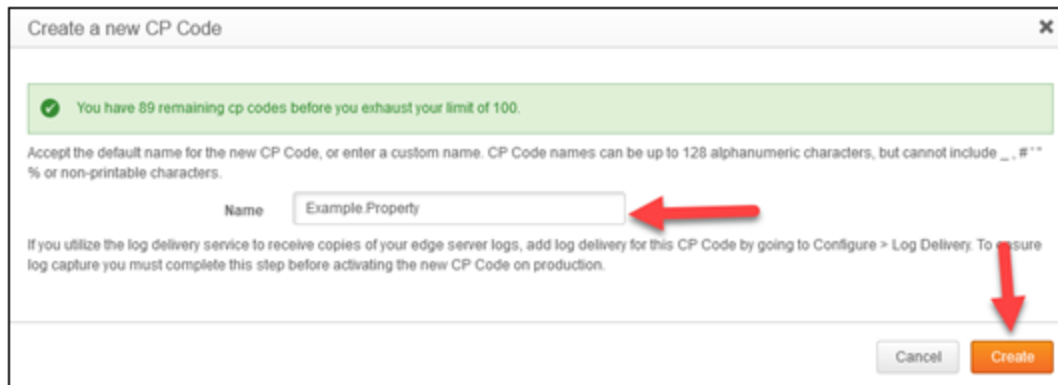
Origin Server

Origin Type	<input type="text" value="Your Origin"/>
Origin Server Hostname <small>(variable support)</small>	<input type="text"/>
Forward Host Header	<input type="text" value="Origin Hostname"/>
Cache Key Hostname	<input type="text" value="Incoming Host Header"/>
Supports Gzip Compression	<input checked="" type="checkbox"/>
Send True Client IP Header	<input checked="" type="checkbox"/>
True Client IP Header Name	<input type="text" value="True-Client-IP"/>
Allow Clients To Set True Client IP Header	<input type="checkbox"/> No
Origin SSL Certificate Verification	
Verification Settings	<input type="text" value="Choose Your Own"/>
Use SNI TLS Extension	<input checked="" type="checkbox"/>
Match CN/SAN To	<input type="text" value="*.bigmachines.com"/>
Trust	<input type="text" value="Akamai-managed Certificate Authorities Sets"/>
Akamai-managed Certificate Authority Sets	Akamai Certificate Store <input checked="" type="checkbox"/> View CA Set
	Third Party Certificate Store <input type="checkbox"/> Disabled View CA Set
Ports	
HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>

Content Provider Code

Content provider codes identify CPQ Site requests for logging, clearing cache etc.

1. Click **Create new...**
2. In the Create a new CP Code window, accept the default name value proposed.
3. Click **Create**.



Create a new CP Code

✔ You have 89 remaining cp codes before you exhaust your limit of 100.

Accept the default name for the new CP Code, or enter a custom name. CP Code names can be up to 128 alphanumeric characters, but cannot include `_`, `#`, `%` or non-printable characters.

Name

If you utilize the log delivery service to receive copies of your edge server logs, add log delivery for this CP Code by going to Configure > Log Delivery. To ensure log capture you must complete this step before activating the new CP Code on production.

Caching

- **Caching Option:** No Store (default). This will be overridden later in our subsequent configuration.



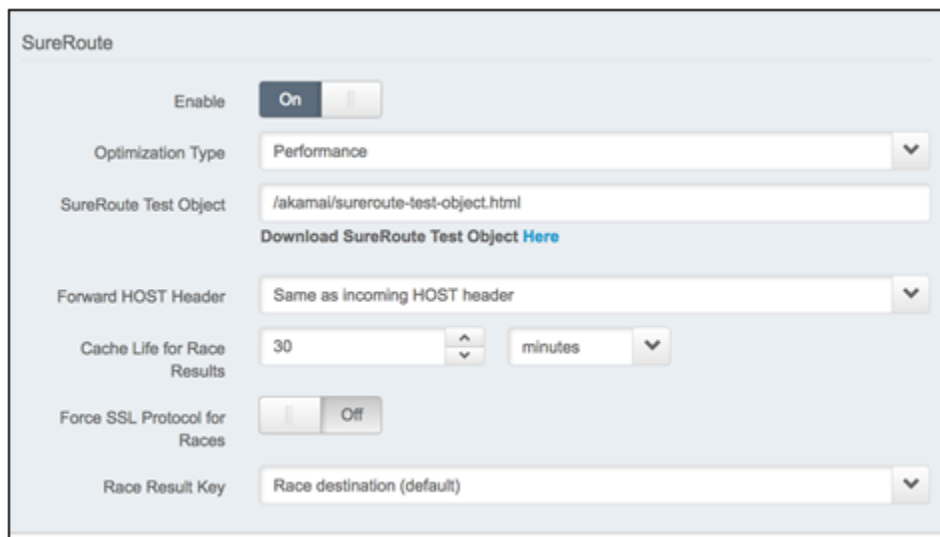
Caching

Caching Option

SureRoute

SureRoute provides the path to the test object that is used by Akamai edge servers to find the optimized path.

- **SureRoute Test Object:** Enter `/akamai/sureroute-test-object.html`



SureRoute

Enable On

Optimization Type

SureRoute Test Object
[Download SureRoute Test Object Here](#)

Forward HOST Header

Cache Life for Race Results

Force SSL Protocol for Races Off

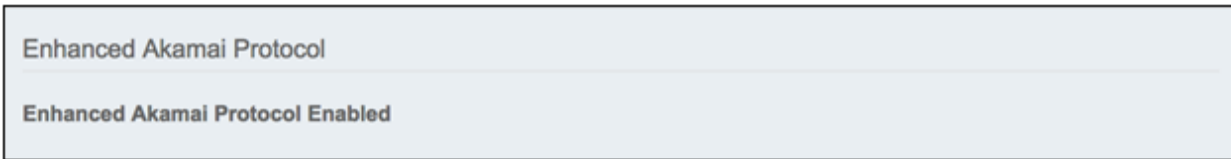
Race Result Key

Tiered Distribution and Prefetch Objects

- If present, delete **Tiered Distribution** and **Prefetch Objects** behaviors.

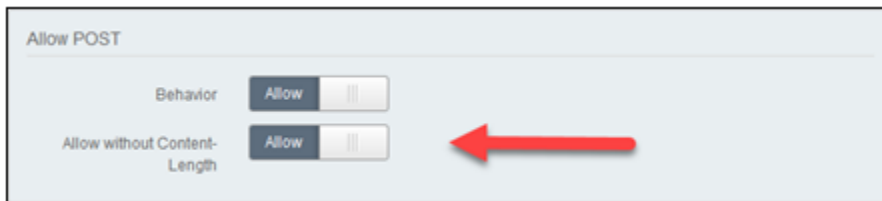
Enhanced Akamai Protocol

- **Enhanced Akamai Protocol:** Optional, availability depends on the contract. No user settings required.



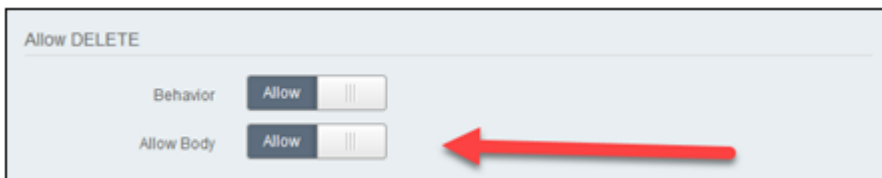
Allow POST

- **Allow without Content-Length:** Allow



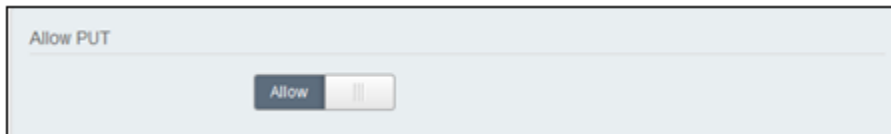
Allow DELETE

- **Allow Body:** Allow



Allow PUT

- No changes required



Log Request Details

- **Log Host Header:** On
- **Log User-Agent Header:** Off
- **Include Custom Log Field:** On
- **Custom Log Field:** Enter `{{user.PMUSER_COUNTRY_CODE}}|{{user.PMUSER_REGION_CODE}}|{{builtin.AK_GHOST_IP}}`

Log Request Details

Log Host Header On

Log Referrer Header Off

Log User-Agent Header Off

Log Accept-Language Header Off

Cookie Mode

Include Custom Log Field On

Custom Log Field (variable support)

mPulse

- If present, delete mPulse behavior.

Set Variable

Depending on the contract, you may optionally create two instances for Set Variable.

- **Variable:** PMUSER_COUNTRY_CODE / PMUSER_REGION_CODE
- **Create Value From:** Extract
- **Get Data From:** Edgescape Data

Set Variable

Variable

Create Value From

Get Data From

Edgescape Field

Operation

Set Variable

Variable

Create Value From

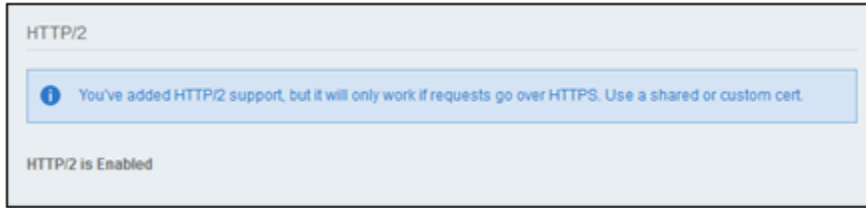
Get Data From

Edgescape Field

Operation

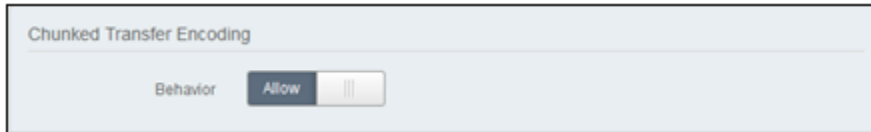
HTTP/2

- No user settings required.



Chunked Transfer Encoding

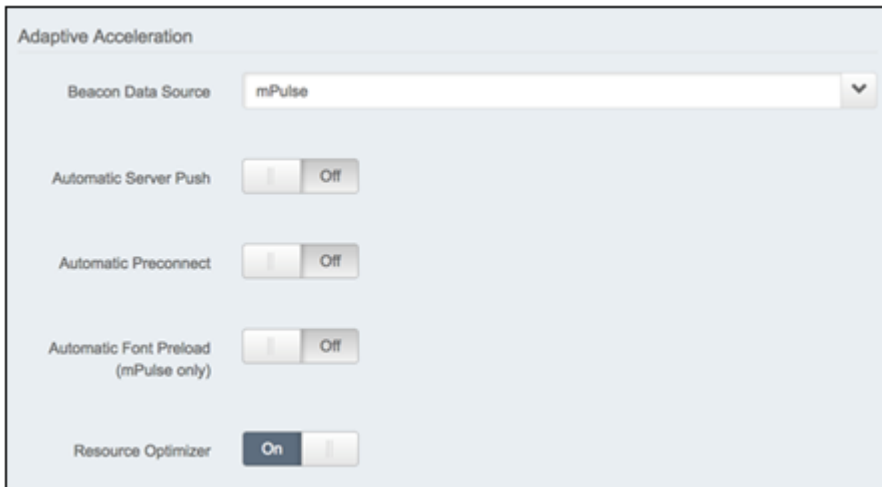
- No changes required.



Adaptive Acceleration

Adaptive Acceleration settings are optional. Adaptive Acceleration can improve HTML page load performance by repositioning content. When it receives an HTML page request, Adaptive Acceleration augments the response using unobtrusive techniques to provide content to the browser as needed. This reduces the load and render time for web pages based on information from navigation and resource timing data.

- **Beacon Data Source:** mPulse
- **Automatic Server Push:** Off
- **Automatic Preconnect:** Off
- **Automatic Front Preload (mPulse only):** Off
- **Resource Optimizer:** On

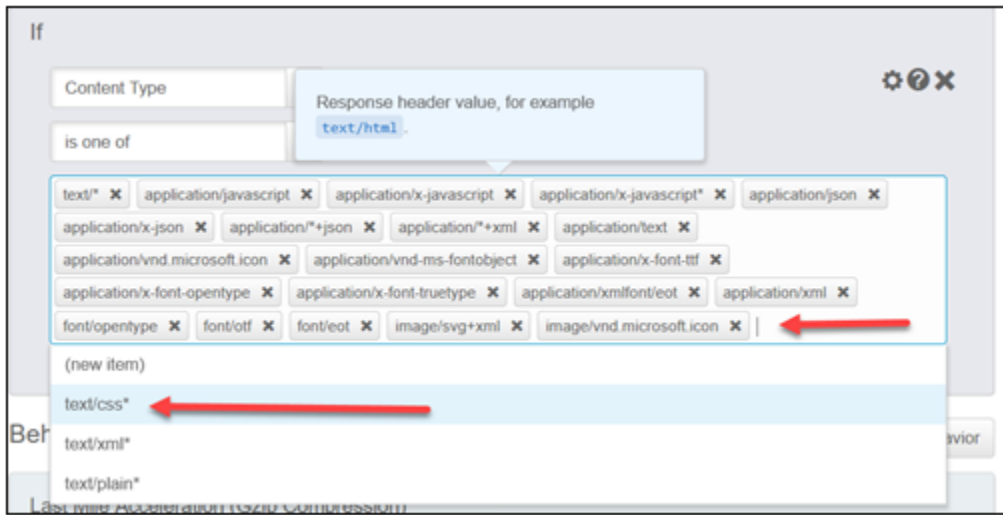


COMPRESSION RULE

Content Compression applies GZIP to content sent to the browser for compressible content-types.

Criteria

- Add text/css* to the default list by clicking in the value area and selecting it from the list.

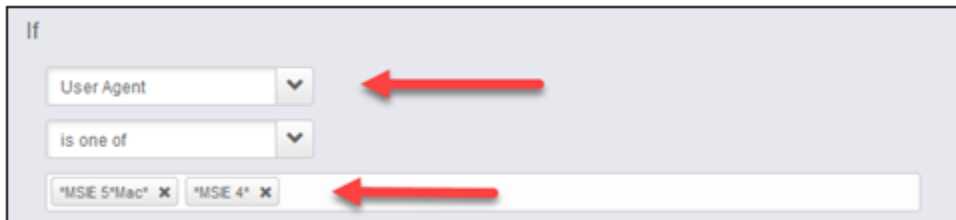


OLD IE BROWSERS RULE

Old IE Browsers disables last mile compression for old versions of Internet Explorer (IE) browsers.

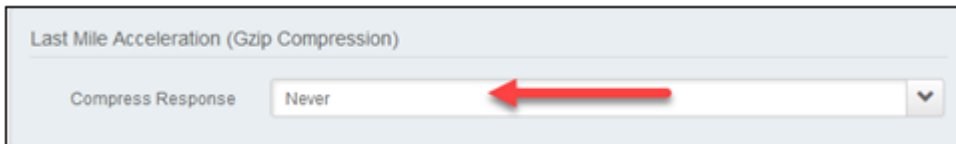
Criteria

- If User Agent is one of *MSIE 5*Mac* or *MSIE 4*



Last Mile Acceleration (Gzip Compression)

- **Compress Response:** Never



OLD MOZILLA BROWSERS RULE

Old Mozilla Browsers disables last mile compression for old versions of Mozilla browsers.

Criteria

- If User Agent is one of *Mozilla/4*
–AND–
- If User Agent is not one of *(compatible;*

The screenshot shows a rule configuration interface with two conditions. The first condition is under the heading "If" and consists of a dropdown menu set to "User Agent", a second dropdown menu set to "is one of", and a text input field containing "*Mozilla/4*" with a small "x" icon to its left. A red arrow points to the "User Agent" dropdown, another red arrow points to the "is one of" dropdown, and a third red arrow points to the "*Mozilla/4*" text field. Below this is a separator line with the word "AND" in the center. The second condition also starts with a "User Agent" dropdown, followed by a dropdown menu set to "is not one of", and a text input field containing "*(compatible;*" with a small "x" icon to its left. Red arrows point to the "User Agent" dropdown, the "is not one of" dropdown, and the "*(compatible;*" text field.

Last Mile Acceleration (Gzip Compression)

- **Compress Response:** Never

The screenshot shows a configuration box titled "Last Mile Acceleration (Gzip Compression)". Inside the box, there is a label "Compress Response" followed by a dropdown menu. The dropdown menu currently displays the value "Never". A red arrow points to the dropdown menu.

REDIRECT TO HTTPS

Redirect to HTTPS redirects HTTP traffic to HTTPS and requires no changes to default values.

If

Request Protocol

HTTP

Behaviors Add Behavior

Redirect

i The Redirect behavior may be better served by the Edge Redirector Cloudlet, which manages large numbers of redirects, and allows non-IT staff, like those in marketing, to set up redirects.

Redirect Type

Destination Protocol

Destination Hostname

Destination Path

Include Query String

Redirect Status Code

DYNAMIC CONTENT

Dynamic Content bypasses the caching for dynamic content (non-cacheable) and requires no changes to default values.

If

Response Cacheability

is not

Behaviors Add Behavior

Downstream Cacheability

Caching Option

DISABLE CHUNK FOR MIGRATION

Disable Chunk for Migration disables the Accept-Encoding protocol for Migration Download URL's.

Criteria

- If Path matches one of /migration/receiver*
 - AND -
- Request Method is POST
 - AND -
- Request Header mReqType is one of catXmlDown

The screenshot shows an 'If' configuration form with three conditions connected by 'AND' operators. The first condition is 'Path matches one of /migration/receiver*'. The second condition is 'Request Method is POST'. The third condition is 'Request Header mReqType is one of catXmlDown'.

Modify Outgoing Request Header (2 Instances)

- **Action:** Remove
- **Select Header Name:** Other...
- **Custom Header Name:** Accept-Encoding / TE

The screenshot shows two identical 'Modify Outgoing Request Header' configuration forms. The first form has 'Action' set to 'Remove', 'Select Header Name' set to 'Other...', and 'Custom Header Name' set to 'Accept-Encoding'. The second form has 'Action' set to 'Remove', 'Select Header Name' set to 'Other...', and 'Custom Header Name' set to 'TE'.

STATIC CONTENT

Static Content sets the default caching for static file extensions.

Criteria

- Criteria requires no changes to default values.
- If present, remove **Prefetch Objects** and **Prefetchable Object** behaviors.

The screenshot shows a configuration panel titled "If". It features a "File Extension" dropdown menu and a "is one of" dropdown menu. Below these are several rows of buttons, each representing a file extension with a small 'x' icon to its right. The extensions listed are: aif, aiff, au, avi, bin, bmp, cab, carb, cct, cdf, class, css, doc, dcr, dtd, exe, flv, gcf, gff, gif, grv, hdml, hqx, ico, ini, jpeg, jpg, js, mov, mp3, nc, pct, pdf, png, ppc, pws, swa, swf, txt, vbs, w32, wav, wbmp, wml, wmlc, wmls, wmlsc, xsd, zip, pict, tif, tiff, mid, midi, ttf, eot, woff, woff2, otf, svg, svgz, webp, jxr, jar, and jp2.

Downstream Cacheability

- **Caching Option:** Don't send cacheability headers; client browser defaults apply

The screenshot shows a configuration panel titled "Downstream Cacheability". It contains a "Caching Option" dropdown menu with the selected value "Don't send cacheability headers; client browser defaults apply".

Caching

- Caching should require no changes to default values.

The screenshot shows a configuration panel titled "Caching". It contains three settings: "Caching Option" set to "Cache", "Force Revalidation of Stale Objects" set to "Serve stale if unable to validate", and "Max-age" set to "1" days.

Tiered Distribution

- Tiered Distribution should require no changes to default values.

The screenshot shows a configuration panel titled "Tiered Distribution". It contains two settings: "Enable" set to "On" and "Tiered Distribution Map" set to "Global (ch2)".

PRE-WAF RULE

Pre-WAF is an optional group of rules forming a firewall-like web application to prevent access from specific countries. It contains no Criteria or Behaviors itself.

EMBARGOED COUNTRY BLOCKING

Criteria

Criteria : Match Any

- If User Location Data Country is one of Cuba (CU), North Korea (KP), Syrian Arab Republic (SY), Iran (IR), Venezuela (VE)
- OR -
- Request Header X-Debug-Embargo is one of true

If

User Location Data

Country is one of

Cuba (CU) North Korea (KP) Syrian Arab Republic (SY) Iran (IR) Venezuela (VE)

AND

Request Header

X-Debug-Embargo is one of

true

Modify Outgoing Response Header

- **Select Header Name:** Other...
- **Custom Header Name:** X-Debug-Embargo
- **Header Value:** true

Modify Outgoing Response Header

Action Add

Select Header Name Other...

Custom Header Name X-Debug-Embargo
(variable support)

Header Value true
(variable support)

SPLASH ASSETS

Criteria

- If Path matches one of /ak-splash/*

The screenshot shows an 'If' configuration box. It contains a dropdown menu set to 'Path', another dropdown menu set to 'matches one of', and a text input field containing the regex pattern '/ak-splash*' with a small 'x' icon to its right.

Site Failover

- **Action:** Use alternate hostname on provider network
- **Alternate Hostname on Provider Network:** embargo.splash.oracle.com
- **Request Path:** Same

The screenshot shows the 'Site Failover' configuration interface. At the top, there is a yellow warning box with a triangle icon and the text: 'To ensure the Site Failover behavior works correctly, you should use it within a match such as Response Status Code or Origin Timeout.' Below this, the 'Enable' toggle is set to 'On'. The 'Action' dropdown is set to 'Use alternate hostname on provider network'. The 'Alternate Hostname on Provider Network' text input field contains 'embargo.splash.oracle.com'. The 'Request Path' dropdown is set to 'Same'.

NON-SPLASH ASSETS

Criteria


- If Path does not match one of /ak-splash/*

The screenshot shows an 'If' configuration box. It contains a dropdown menu set to 'Path', another dropdown menu set to 'does not match one of', and a text input field containing the regex pattern '/ak-splash*' with a small 'x' icon to its right.

Site Failover

- **Action:** Use alternate hostname on provider network
- **Alternate Hostname on Provider Network:** embargo.splash.oracle.com
- **Request Path:** Other
- **Modified Path:** /embargoed.html
- **Include Query String:** No

Site Failover

 To ensure the Site Failover behavior works correctly, you should use it within a match such as Response Status Code or Origin Timeout.

Enable On

Action

Alternate Hostname on Provider Network (variable support)

Request Path

Modified Path (variable support)

Include Query String No

IMAGE MANAGER

The Image Manager provides image optimizations when rendering in the browser and should require no changes to default values.

If

File Extension

is one of

Caching

Caching Option

Force Revalidation of Stale Objects

Max-age

Image Manager

Image Optimization Settings

Enable

Scale for Mobile

Use Best File Type

Region

Traffic Settings

Pristine Images CP Code
The Pristine Images CP Code option in Image Manager must not be empty.

Derivative Images CP Code
The Derivative Images CP Code option in Image Manager must not be empty.

Policy Set (API Key)

Policy Set Type

Policy Set Name (API Key)

ADD UA TO CACHE KEY

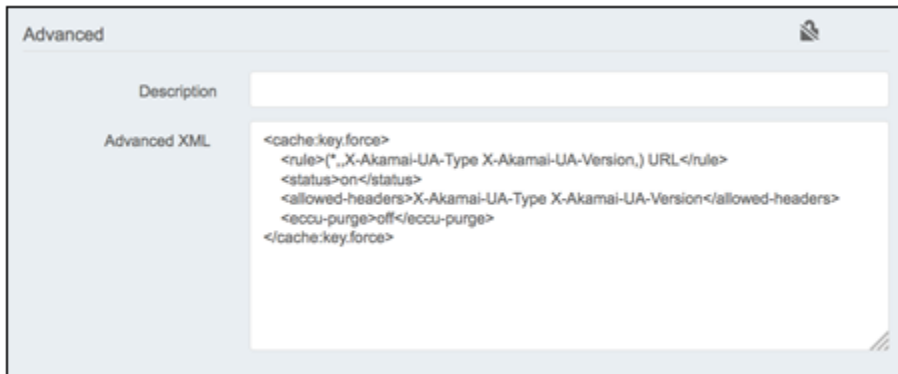
Criteria

- **Criteria:** None

Advanced

- **Advanced XML:** Contact your Akamai representative to add the following XML.

```
<cache:key.force>  
  <rule>>(*,,X-Akamai-UA-Type X-Akamai-UA-Version,) URL</rule>  
  <status>on</status>  
  <allowed-headers>X-Akamai-UA-Type X-Akamai-UA-Version</allowed-headers>  
  <eccu-purge>off</eccu-purge>  
</cache:key.force>
```



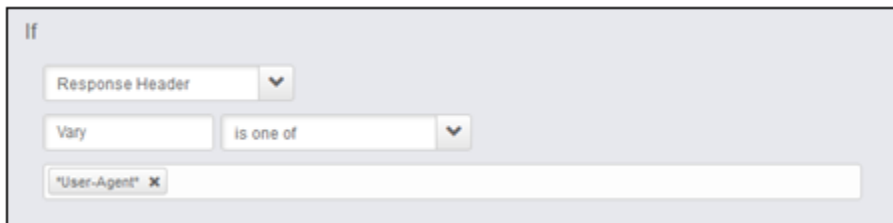
The screenshot shows a configuration window titled "Advanced". It has a "Description" field which is empty. Below it is the "Advanced XML" field, which contains the XML code: `<cache:key.force>
<rule>>(*,,X-Akamai-UA-Type X-Akamai-UA-Version,) URL</rule>
<status>on</status>
<allowed-headers>X-Akamai-UA-Type X-Akamai-UA-Version</allowed-headers>
<eccu-purge>off</eccu-purge>
</cache:key.force>`

Remove Vary Header

Remove Vary Header removes the caching of responses that are dependent on the user-agent.

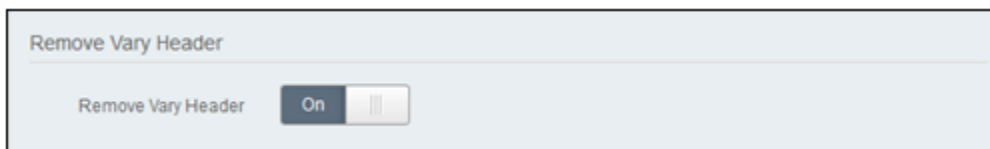
Criteria

- If **Response Header Vary** is one of *User-Agent*



The screenshot shows a configuration window titled "If". It has a dropdown menu set to "Response Header". Below that is a "Vary" field and an "is one of" dropdown menu. The "is one of" dropdown menu is set to "*User-Agent*" with a close button (X).

- **Remove Vary Header:** should require no change to the default value.

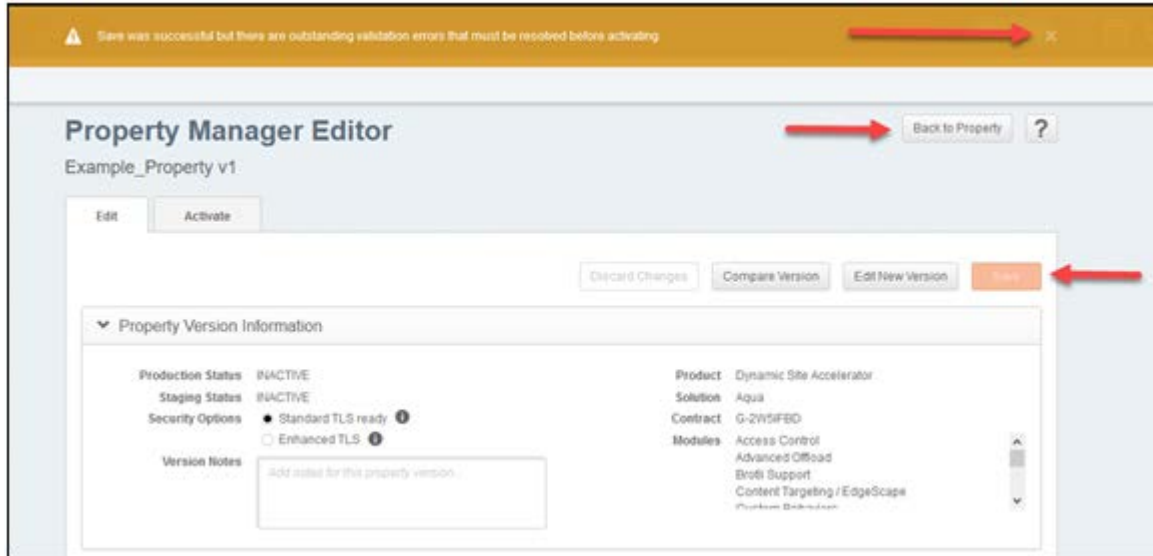


The screenshot shows a configuration window titled "Remove Vary Header". It has a toggle switch labeled "Remove Vary Header" which is currently set to "On".

Save the Template Property

The template property is now complete.

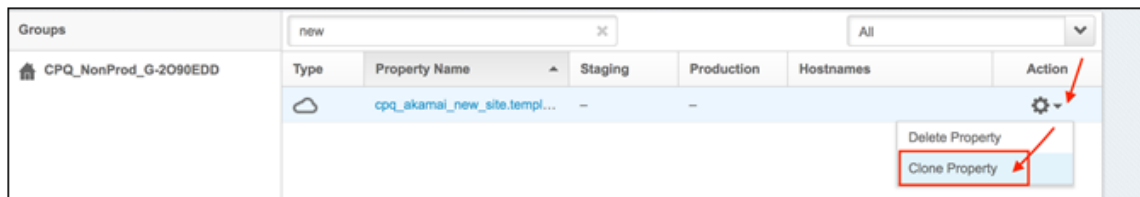
1. Click **Save** at the top or bottom of the page. An error banner "Save was successful but there are outstanding validation errors that must be resolved before activating" will be shown.
2. Click **(X)** to close the banner.
3. Click **Back to Property**.



Akamai Property Clone Setup

Create the property to be used in production by cloning the template.

1. Hover over the property named **cpq_akamai_new_site.template** in the Property Group page.
2. Click the gear icon in the **Action** column.
3. Click **Clone Property**. The Clone Property page opens.



4. Enter a **Property Name**. We recommend you use the vanity domain name so that it's easy to correlate.

5. Click **Clone Property**. The Property Manager Editor page opens.

The screenshot shows the 'Clone Property' form. At the top, it says 'Create a new property by cloning another.' Below this, there are several fields: 'Property Type' (Property Manager), 'Property Version' (Version 1), 'Product' (Ion Premier), and 'Contract' (G-2090EDD). The 'Property Name' field contains 'e.g. example.com' and has a red border with a red arrow pointing to it. Below the name field is the text 'Name must be at least 3 characters'. There is a 'Copy Hostnames?' checkbox which is unchecked. At the bottom right, there is an orange 'Clone Property' button with a red arrow pointing to it.

6. Click **Enhanced TLS** for Security Options within the Property Version Information section.

The screenshot shows the 'Property Manager Editor' page for 'den01scy.us.oracle.com v1'. It has 'Edit' and 'Activate' tabs. At the top right are buttons for 'Cancel', 'Compare Version', 'Edit New Version', and 'Save'. The main section is 'Property Version Information'. On the left, there are 'Production Status' (INACTIVE) and 'Staging Status' (INACTIVE). Under 'Security Options', there are two radio buttons: 'Standard TLS ready' (unselected) and 'Enhanced TLS' (selected), with a red arrow pointing to the 'Enhanced TLS' option. Below this is a 'Version Notes' text area. On the right, there is a list of details: 'Product' (Ion Premier), 'Solution' (Aqua), 'Contract' (G-2090EDD), and 'Modules' (Access Control, Adaptive Acceleration, Advanced Offload, Akamai Instant, Built Content).

7. In Property Hostnames section, click **Add**. The Step 1: Add Hostnames – Hostnames page opens.

The screenshot shows the 'Property Hostnames' section. At the top, there is a red error message: 'At least one property hostname is required.' Below this is a search filter 'Filter by Hostname or Edge Hostname'. To the right are buttons for 'Edit Selected', 'Delete Selected', and 'Add', with a red arrow pointing to the 'Add' button. Below the buttons is a table with columns: 'Status', 'Property Hostname', 'Certificate', 'Slot', 'Edge Hostname', and 'IP Type'. At the bottom left, there is a red information icon and the text 'Add a property hostname by clicking Add'.

8. Enter the vanity domain name in the **Add Hostname(s)** field.

9. Click **Next**. Step 2: Add Hostnames – IP Version page opens.

10. Select the applicable **IP Version**.

11. Click **Next**. The Step 3: Add Hostnames – Certificates page opens.

12. Select the vanity domain's certificate in the **Select Certificate** field.

Note: Hostname must match the certificate's domain name exactly.

13. Click **Next**. The Step 4: Add Hostnames – Edge Hostnames page opens.

14. Click **Submit**.

Note: If the edge hostname is not auto-populated, click on the drop-down and select an edge hostname. The edge hostname should follow the convention `<hostname>.edgekey.net` where `<hostname>` is the vanity domain.

Each property hostname listed below routes through the Akamai server using the edge hostname next to it. The edge hostname is not visible to users accessing your website or application.

Property Hostname	Edge Hostname	IP Version
tier3-176a.bigmachines.com	tier3-176a.bigmachines.com-v3.edgekey.net	IPv4 + IPv6

Items: 1 < 1 > Items Per Page: 10 25 50

Cancel Previous Submit

15. You should see a success message. Click **Close**.

Success!
Congratulations! You successfully modified the property hostname to edge hostname associations for your website or application. Any newly created edge hostnames will go live when you activate your configuration in either staging or production.

If you associated your property hostnames to new edge hostnames, remember to update your CNAME record. Be sure to follow these steps:

1. Activate your configuration in staging, and wait for confirmation that the new edge hostname has been created.
2. Test your configuration.
3. Activate your configuration in production.
4. Change the CNAME record of your property hostname to point to the new edge hostname.

Important! Traffic will not be directed to edge servers until this property has a complete configuration activated in the production environment. Do not update your DNS record before completing those steps. See [Activating](#) and [Edge Hostnames](#) for more information.

Close

16. Navigate to the Property Configuration Settings and click **Default Rule**.

17. Set the Origin Server values as follows:

- **Origin Server Hostname:** <Oracle CPQ Hostname i.e. myCompany.bigmachines.com>
- **Verification Settings:** Choose Your Own
- **Match CN/SAN To:** *.bigmachines.com

Origin Server

Warning: If you are changing your Origin Server SSL Certificate Verification settings it is strongly recommended that you test on Staging before activating on Production. Failure to test on Staging may result in a service outage.

Origin Type: Your Origin

Origin Server Hostname (variable support): tier3-176.bigmachines.com

Forward Host Header: Origin Hostname

Cache Key Hostname: Incoming Host Header

Supports Gzip Compression: Yes

Send True Client IP Header: Yes

True Client IP Header Name: True-Client-IP

Allow Clients To Set True Client IP Header: No

Origin SSL Certificate Verification

Verification Settings: Choose Your Own

Use SNI TLS Extension: Yes

Match CN/SAN To: *.bigmachines.com

Trust: Akamai-managed Certificate Authorities Sets

Akamai-managed Certificate Authority Sets: Akamai Certificate Store (Enabled), Third Party Certificate Store (Disabled)

18. In the Content Provider Code section, click **Create new....**

Content Provider Code

Content Provider Code: [input field]

Create new...

19. You should see a default name (usually the template name). Click **Create**.

Create a new CP Code

You have 14988 remaining cp codes before you exhaust your limit of 15000.

Accept the default name for the new CP Code, or enter a custom name. CP Code names can be up to 128 alphanumeric characters, but cannot include _ , # * % or non-printable characters.

Name: den02scy.us.oracle.com

If you utilize the log delivery service to receive copies of your edge server logs, add log delivery for this CP Code by going to Configure > Log Delivery. To ensure log capture you must complete this step before activating the new CP Code on production.

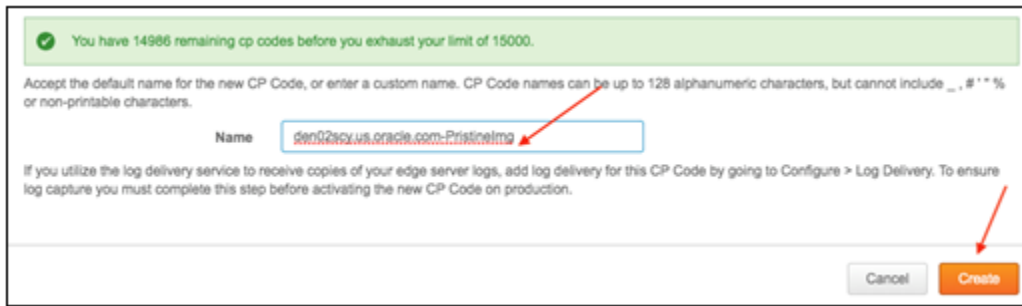
Cancel Create

20. Navigate to the Property Configuration Settings and click **Image Manager**.

21. Click **Create new...** to create a new **Pristine Images CP Code** within the Traffic Settings section.

22. Add the suffix **-PristineImg** to the default template name, as specified in step 19.

23. Click **Create**.



You have 14986 remaining cp codes before you exhaust your limit of 15000.

Accept the default name for the new CP Code, or enter a custom name. CP Code names can be up to 128 alphanumeric characters, but cannot include `_`, `#`, `^`, `%` or non-printable characters.

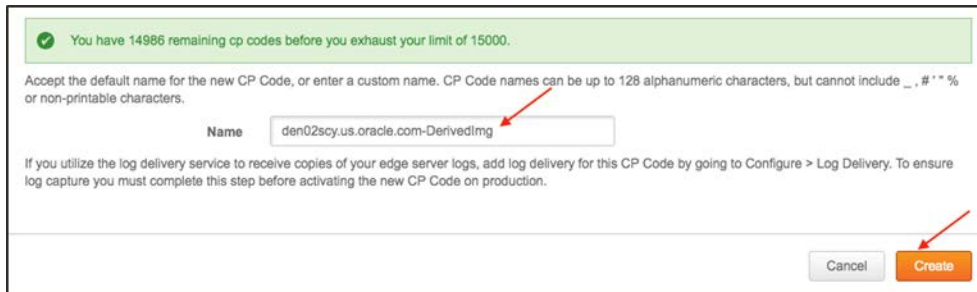
Name

If you utilize the log delivery service to receive copies of your edge server logs, add log delivery for this CP Code by going to Configure > Log Delivery. To ensure log capture you must complete this step before activating the new CP Code on production.

24. Click **Create new...** to create a new **Derivative Images CP Code** within the Traffic Settings section.

25. Add the suffix **-DerivedImg** to the default template name specified in step 19.

26. Click **Create**.



You have 14986 remaining cp codes before you exhaust your limit of 15000.

Accept the default name for the new CP Code, or enter a custom name. CP Code names can be up to 128 alphanumeric characters, but cannot include `_`, `#`, `^`, `%` or non-printable characters.

Name

If you utilize the log delivery service to receive copies of your edge server logs, add log delivery for this CP Code by going to Configure > Log Delivery. To ensure log capture you must complete this step before activating the new CP Code on production.

27. Click **Save** at the top or bottom of the Property Manager Editor page.

28. Once ready for activation, click on the **Activate** tab. Each property file is versioned, and you can only overwrite the highest version that is not activated.

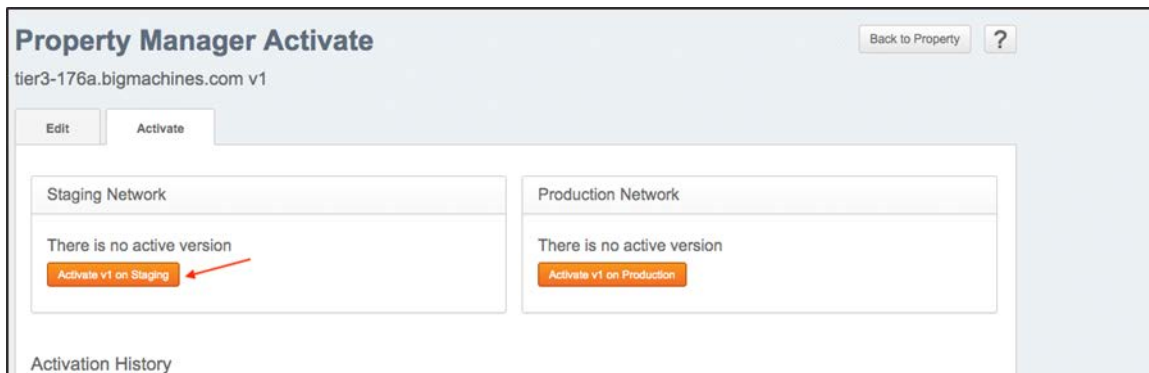


Property Manager Editor

tier3-176a.bigmachines.com v1

Property Version Information

29. Activate the property in the Staging Network by clicking on **Activate v1 on Staging**.



Property Manager Activate

tier3-176a.bigmachines.com v1

Staging Network

There is no active version

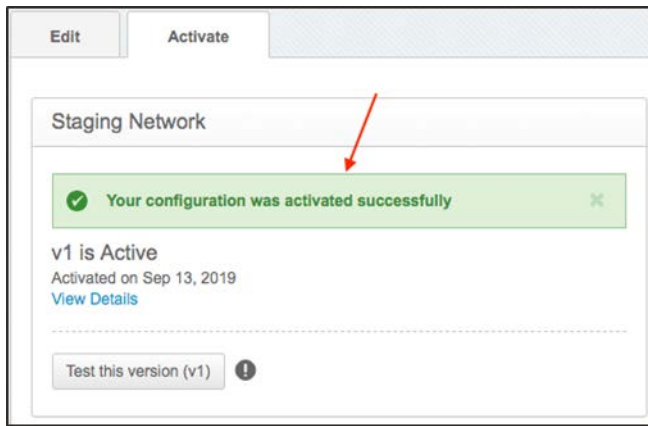
Production Network

There is no active version

Activation History

30. (Optional) Add notes as desired.

31. Click **Activate**. A confirmation message displays.



32. Test the site in the staging environment. See [Testing in Staging Environment](#). Once all the tests are successful, then proceed to activate the property in production.

Testing in Staging Environment

When you activate a property to the staging environment, Akamai deploys the property file to its staging network. The staging network can be identified by replacing `<hostname>.edgekey.net` with `<hostname>.edgekey-staging.net`.

For example: if the edge hostname is `vanity-domain.mySite.com.edgekey.net`, then the staging network will be located at `vanity-domain.mySite.com.edgekey-staging.net`.

Follow the steps described below.

1. In a Windows command window, enter `nslookup <hostname>.edgekey-staging.net`. The IP Address returned here is an Akamai Staging Network edge server that will have the new configuration deployed.

Example:

```
nslookup vanity-domain.mySite.com.edgekey-staging.net

Non-authoritative answer:
Name:      e36883.dscb.akamaiedge-staging.net
Addresses: 2600:1407:21:383::9013
           2600:1407:21:380::9013
           23.50.52.35
           23.50.52.32
Aliases:  vanity-domain.mySite.com.edgekey-staging.net
Address:  23.206.156.158 <===== Resolved Staging Edge Server
```

2. Create a new `/etc/hosts` entry on your local server/workstation, for example:
`23.206.156.158 vanity-domain.mySite.com.edgekey-staging.net.`

EDIT HOSTS FILE

Windows 7 or higher:

1. Click **Start -> All Programs -> Accessories**
2. Right-click **Notepad** and select **Run as administrator**.
3. Click **Continue** on the "Windows needs your permission" UAC window.
4. When Notepad opens, click **File -> Open**
5. In the filename field, type `C:\Windows\System32\Drivers\etc\hosts`.
6. Click **Open**.

7. Add the line specified on step 2 above.
8. Save and Exit.

MAC/Linux

1. Open a terminal.
2. Type `sudo vi /etc/hosts`.
3. Enter required password.
4. Add the line specified on step 2 above.
5. Save and Exit (:wq).

DNS Change

1. Add a new CNAME record to the hostname DNS entry, to point the vanity domain name to the Akamai edge server that is configured in the property.

Example: `vanity-domain.mySite.com CNAME to vanity-domain.mySite.com.edgekey.net`

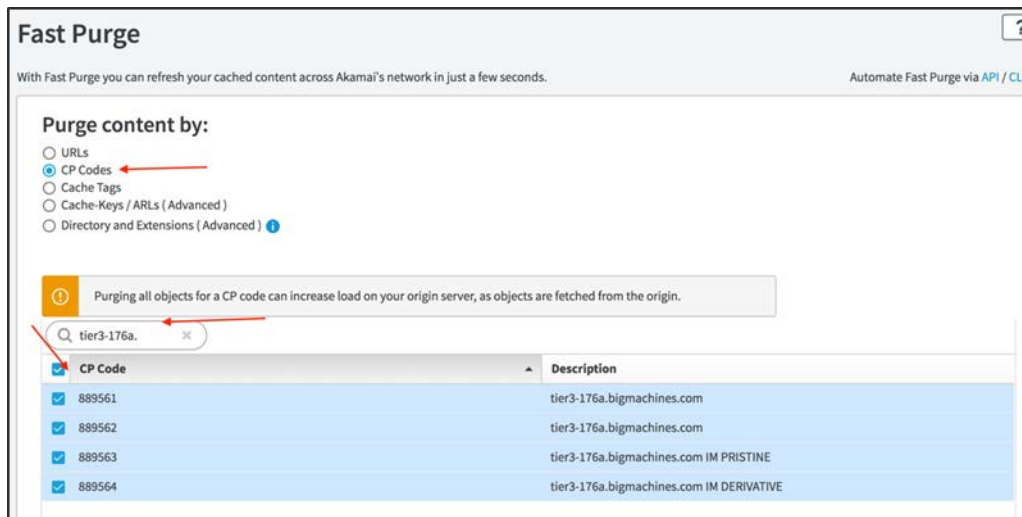
2. Run a `dig` command to verify the DNS routing.

PURGING AKAMAI CACHE

Akamai cache needs to be cleared whenever a property is activated.

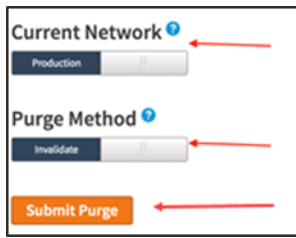
To purge Akamai cache, perform the following steps:

1. In the Akamai Control Center, navigate to $\equiv \rightarrow$ **Purge cache**. The Fast Purge page opens.
2. Select **CP Codes** for Purge content by.
3. In the search field, enter the hostname to filter the list.
4. Click in the Select All check box to select all CP Codes from the filtered list.



5. Depending on the need, set the Current Network to either **Production** or **Staging**.
6. Set the Purge Method to **Invalidate**.

- Click **Submit Purge**. This action will take a couple of seconds to complete.



DEACTIVATION AND ACTIVATION OF PROPERTY

To deactivate or activate a property, perform the following steps:

- Hover over the property to be deactivated/activated in the Property Group page.
- Click the gear icon in the **Action** column.
- Click on the **Activate** or **Deactivate** action.

Type	Version	Based On	Last Edited	Author	Notes	Staging	Production	Actions
Cloud	Version 4	Version 3	Sep 13, 2019	gowtham.sridharan@oracle.com		Inactive	Inactive	
Cloud	Version 3	Version 2	Sep 12, 2019	gowtham.sridharan@oracle.com	invalid domain ssl	Deactivated	Inactive	
Cloud	Version 2	Version 1	Sep 12, 2019	gowtham.sridharan@oracle.com	Testing SSL Verification	Deactivated	Inactive	
Cloud	Version 1	-	Sep 12, 2019	gowtham.sridharan@oracle.com		Active	Inactive	⚙️

HANDLING SITE CHANGES

Whenever the static content changes in the CPQ Site, the Akamai will refresh its cache based on the rule “Static Content” in the Akamai property. Currently it will refresh after one day. If cache needs to refresh sooner, then it needs to be purged manually. Refer to [Purging Akamai Cache](#).

The static content can change in many ways. Below are example scenarios:

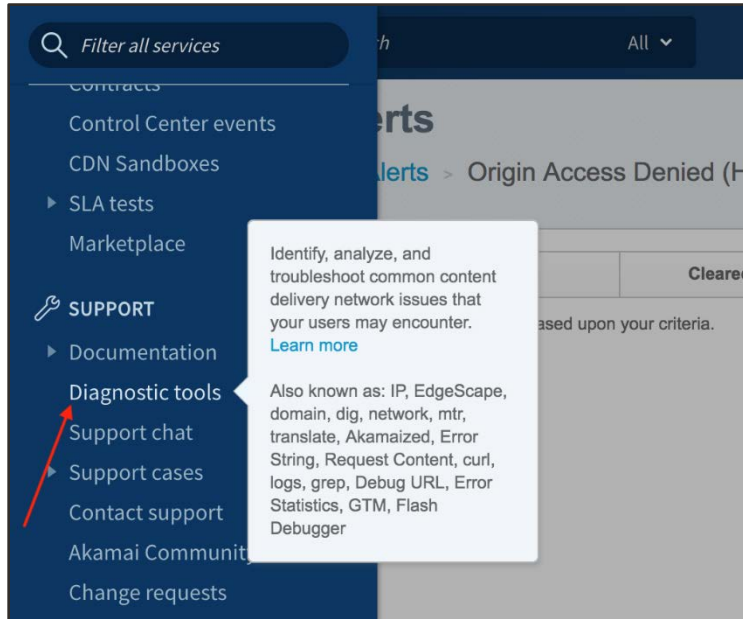
- CPQ Admins can change the static content.
- A fix/patch can be applied.
- The Site can be upgraded during the release window.

TROUBLESHOOTING

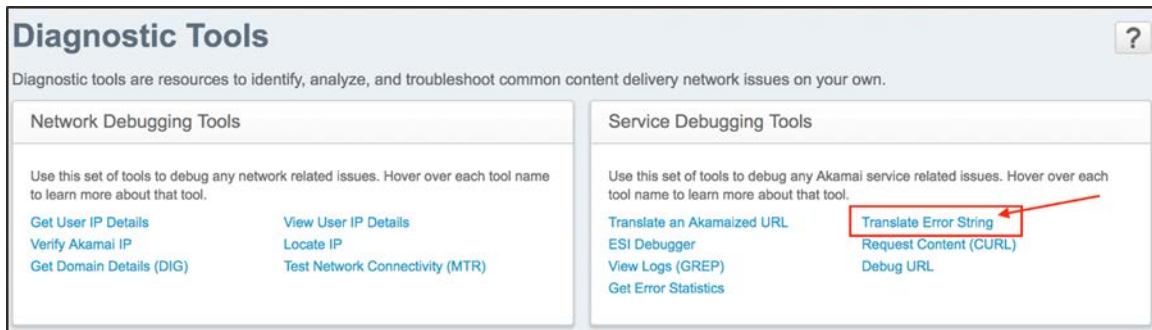
If the Akamai setup causes an issue, the Akamai server will send an error string. Use this string as a starting point for troubleshooting. For example, end users/clients will see errors similar to: **Reference #9.6f321cb8.1568339219.1181952b**.

To troubleshoot Akamai error strings, perform the following steps:

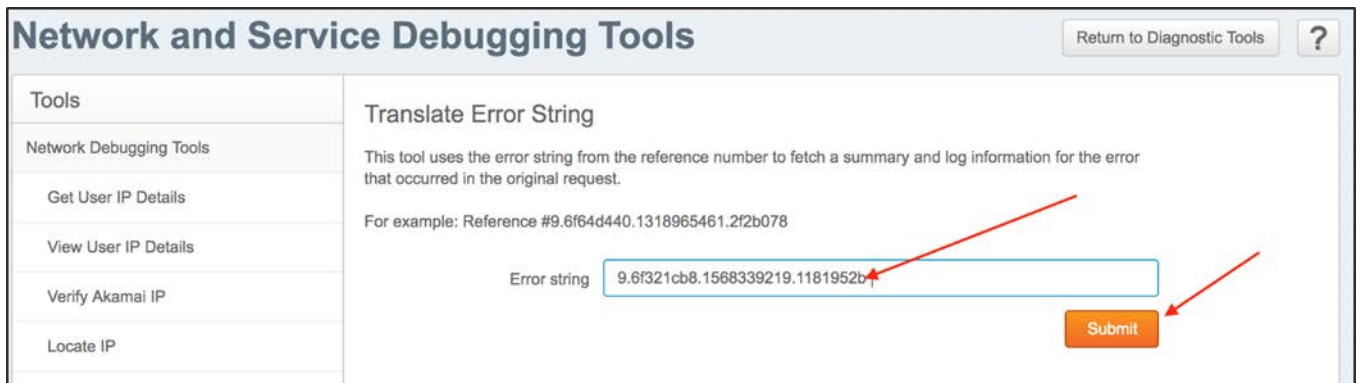
1. Copy the Reference # from the error page.
2. In the Akamai Control Center, navigate to **Support → Diagnostic Tools**. The Diagnostic Tools page opens.



3. Click **Translate Error String** under Service Debugging Tools.

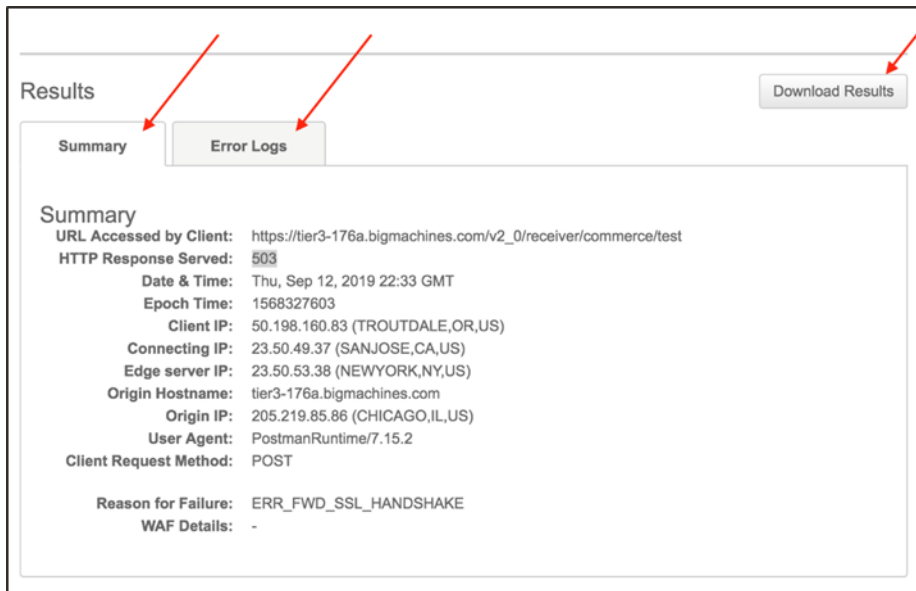


4. Past the error number (only include the string that follows the #) that was copied in step 1 into the Error string field.
5. Click **Submit**.



Results are shown in **Summary** and **Error Logs** tabs that you can use for analysis.

6. Click **Download Results** to save a local copy of the results.



LOG DELIVERY SERVICE

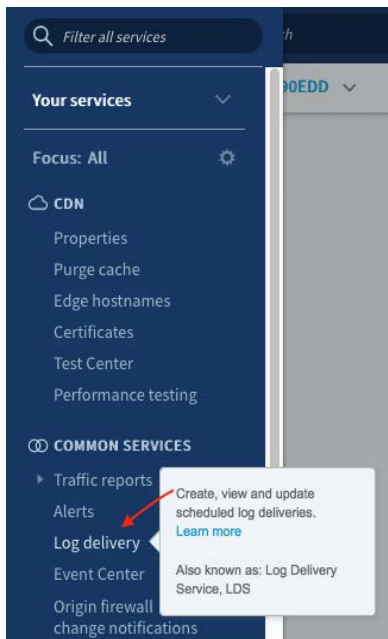
The Akamai Log Delivery Service (LDS) provides server logs through log delivery service.

Akamai's infrastructure is constantly gathering log entries from thousands of edge servers around the world. LDS creates a copy of these logs and delivers them based on a predetermined schedule.

Note: Log delivery usually takes a day or two from the date of setup.

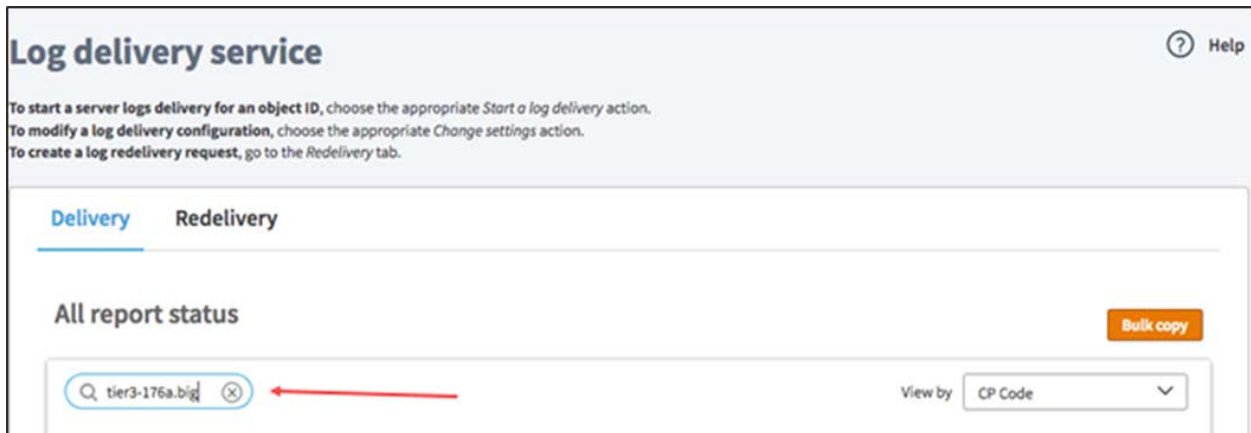
To set up the Akamai Log Delivery Service, perform the following steps:

1. In the Akamai Control Center, navigate to ☰ → **Common Services** → **Log delivery**.

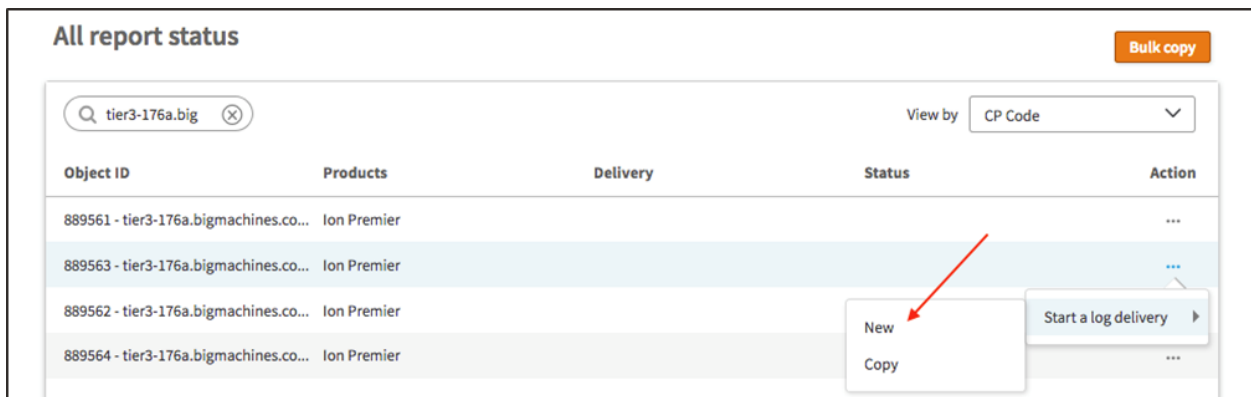


2. Click in the filter in the Delivery tab of the in the Log Delivery Service page.

3. Enter a CP Code to filter.



4. In the Action column, click on ... → **Start a log delivery** → **New**. The Step 1: Create a Configuration – Log configuration page opens.



5. Enter the date from when log entries need to be captured in the **Start date** field.
6. Select the **Indefinite end date** checkbox.
7. Select **combined** in the Log Format drop-down.
8. Enter a string to be the first token in the log filename, such as the domain name, for the **Log Identifier String**. For Pristine and Derived, use <domainname>-PristineImg, <domainname>-DerivedImg respectively.
9. Select **Aggregate by log arrival time** for the Aggregate Type.
10. Select the frequency desired from the **Delivery frequency** drop-down. Every 1 hour is a good selection to start with.

11. Click **Next**. Step 2: Create a Configuration - Delivery page opens.

The screenshot shows a dialog box titled "Create a configuration for: 889561 - tier3-176a.bigmachines.com". At the top, there are three steps: 1. LOG CONFIGURATION (highlighted), 2. DELIVERY, and 3. CONTACT DETAILS. The "Log configuration" section includes:

- Log details:**
 - Start date: 09/24/2019
 - Indefinite end date
 - Log format: combined
 - Log identifier string: tier3_176a
- Aggregation:**
 - Type: Aggregate by log arrival time
 - Delivery frequency: Every 1 hour
 - Aggregate by hit time

There are explanatory text blocks: "This string will be the first token of the log filename. For example, if the identifier string is acme, the log filename is in the format: acme_1.w3c_S.200301019999-9999-0.gpg." and "This option allows you to receive log data in the order that it arrives from the edge servers. This is the fastest way to get log data, but it is more difficult to process. For example, a delivery that covers a 24-hour period will usually contain some data from the previous several days." At the bottom, there are "Cancel", "Back", and "Next" buttons. Red arrows point to the "Next" button and several input fields.

12. Select **FTP** for the Delivery Type.

13. Enter **<your SFTP server>** in the Machine field.

14. Enter **<your SFTP username>** in the Login field.

15. Enter **< your SFTP password>** in the Password field.

16. Enter the directory for the logs, such as akamai_logs/<hostname>/ in the Directory field. Ensure the directory structure accurately indicates the hostname for the relevant logs.

17. Select the **Secure via Secure FTP** checkbox.

18. Select **2 MB (approx. 12 MB uncompressed logs)** in the Approximate message size drop-down. You may increase the size, if necessary.

19. Select **GZIP** in the Encoding drop-down.

20. Click **Next**. The Step 3: Create a configuration – Contact Details page opens.

The screenshot shows the "Delivery" configuration page. At the top, there are three steps: 1. LOG CONFIGURATION, 2. DELIVERY (highlighted), and 3. CONTACT DETAILS. The "Log delivery" section includes:

- Type: FTP
- Machine: SFTP.MySite.com
- Login: MyLogin
- Password: [masked]
- Directory: akamai_logs/domainName/
- Send via Secure FTP
- Akamai NetStorage 4
- Email
- Approximate message size: 2 MB (approx. 12 MB uncompressed logs)
- Encoding: GZIP

There is explanatory text: "To save logs in the FTP user's default directory, leave the directory field blank." At the bottom, there are "Cancel", "Back", and "Next" buttons. A red arrow points to the "Next" button.

21. Enter the email addresses for delivery of the logs. The specified email accounts will also receive alerts if logs are not delivered.

22. Click **Finish**.

1 LOG CONFIGURATION 2 DELIVERY 3 CONTACT DETAILS

Contact details

If we can't deliver the log files, we will send an email alert to the contact listed below. Make sure that this email address is checked on a daily basis. You may provide multiple addresses, delimited by commas.

Email address(es)

23. Navigate back to the Log delivery service and confirm that the status is **Active**.

Log delivery service Help

To start a server logs delivery for an object ID, choose the appropriate *Start a log delivery* action.
To modify a log delivery configuration, choose the appropriate *Change settings* action.
To create a log redelivery request, go to the *Redelivery* tab.

Delivery Redelivery

All report status

View by

Object ID	Products	Delivery	Status ↑	Action
866319 - cpq-nonprod.oracle.com	Ion Premier	SFTPU	Active	...

24. Repeat these steps for the other two CP Codes (Pristinelmg and Derivedlmg) with the appropriate log identifier strings.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.

Outside North America, find your local office at oracle.com/contact.



blogs.oracle.com



facebook.com/oracle



twitter.com/oracle

Copyright © 2020 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use.

Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

