Request Control Cloudlet

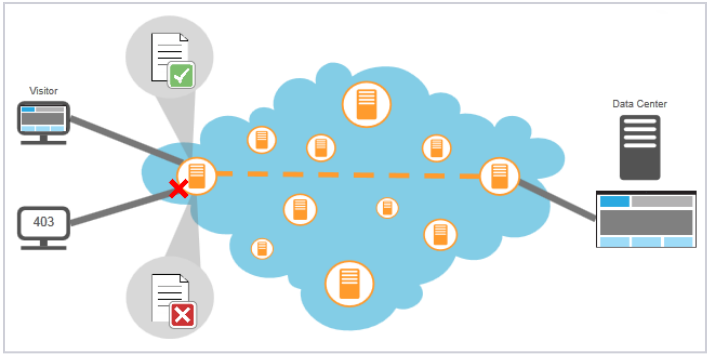
Request Control is an Akamai Cloudlet, a value-added application which complements Akamai's core delivery solutions to solve specific business challenges. Cloudlets bring a site's business logic closer to the end user by placing it on the "edge" of the content delivery platform.

The Request Control Cloudlet allows you to provide conditional access to your website or application by defining and managing whitelists and blacklists based on a number of match criteria, including the IP address and/or geography associated with incoming requests. In addition, you can have a branded 403 (Forbidden) page display when a user is denied access.

Request Control provides:

- **Self-Service:** Request Control comes with an easy-to-use user interface (UI) and an OPEN API that provide self-service capabilities.
- **Flexible Rule Creation:** Using either the Cloudlets Policy Manager or the OPEN API, you can create access rules that meet your business needs.
- **Faster Propagation Times:** The Cloudlets Policy Manager allows you to make changes to your configurations on the fly and then propagate those changes quickly.

How Request Control Works



This diagram shows how Request Control works when creating a whitelist. In this case, when a visitor requests a page from an IP address or geography for which access is *allowed* based on the rule(s) configured, that visitor will be able to view the page.

However, if the visitor's IP address or geography is not included in the rules, that visitor will receive a 403 (Forbidden) error.

Note: You have the option of displaying a branded 403 page to users who are denied access.

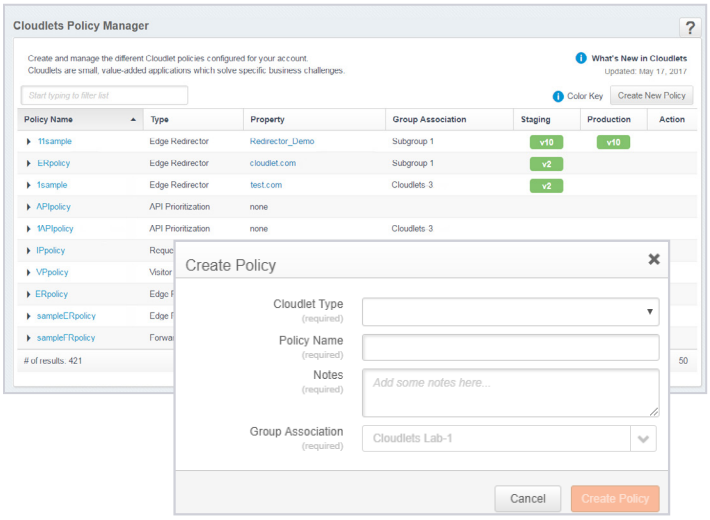
Conversely, for a blacklist, if a visitor requests a page from an IP address or geography for which access is denied based on the rule(s) configured, that visitor will receive a 403 error. All other visitors who do not match the blacklist rule(s) will be able to view the page.

Request Control Configuration Overview

Once the Request Control Cloudlet has been added to your contract and, if desired, your branded 403 page is ready, you have to complete these tasks:

1. In the Cloudlets Policy Manager, configure a Request Control policy and rules, then activate the policy version. See the *Cloudlets Quick Reference* for activation information.
2. In Property Manager, select the appropriate property, set up the Request Control behavior, and then activate the property.

Creating a Policy for Request Control



To create a policy for Request Control:

1. From the Luna Control Center, select **Configure** ▸ **Cloudlets** ▸ **Cloudlets Policy Manager**.
2. On the Cloudlet Policies page, select **Create New Policy**.
3. Complete the following fields:

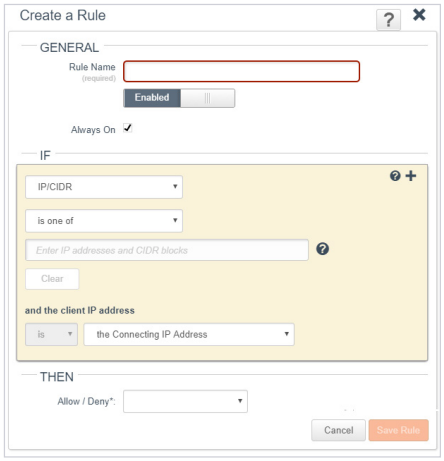
Field	Entry
Cloudlet Type	Select **Request Control**.
Policy Name	Enter the name of the policy.
Notes	Enter a meaningful description for the policy.

4. Click **Create Policy**. The Policy Details page displays for new policy.

Configuring Rules for Request Control

To configure rules for API Prioritization:

1. From the Luna Control Center, select **Configure** ▸ **Cloudlets** ▸ **Cloudlets Policy Manager**.
2. Click the name of the policy you want to add a rule to.
3. Click the number of the policy version you are adding rules to.
4. Select **Add Rule**.

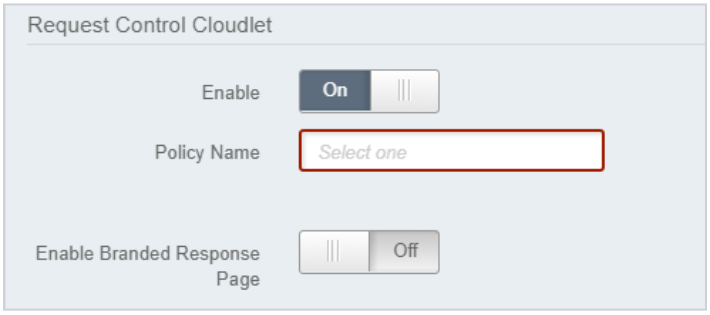


5. Complete the following fields:

Field Name/ Type	Entry
Rule Name	Enter a descriptive name for this rule.
Always On	Select if the rule is always applied. If deselected, start and end date fields display.
Start Date/Time	If the rule is for a fixed time, enter the start date and time.
End Date/Time	If the rule is for a fixed time, enter the end date and time.
Match Type	Select the type of match to use for this rule. **Note:** While the primary match types for this Cloudlet are IP address/CIDR list (IP/CIDR) and geography, other match types, like request header, are also available.
Operator	Select whether to use positive match criteria or negative match criteria.
Match Criteria	Enter the match criteria for this rule.
Case Sensitive	Select if the match criteria is case sensitive.
Allow/Deny	Select to either allow or deny access to the website or application. If denying access, you have the option of using a branded 403 page.

6. Click **Save Rule** once all changes are complete, then click **Save Changes** on the Version Details page.

Enabling Request Control in Property Manager



To enable Request Control in Property Manager:

1. From the Luna Control Center, select **Configure** ▸ **Manage Properties** (under **Property Manager**).
2. Navigate to the property you will be adding Request Control to.
3. Open the version of the property configuration, then select the default rule you want to add Request Control to.
4. Click **Add Behavior**, then select **Request Control** from the list of available behaviors.
5. On the Create Rule page, complete the following fields:

Field	Entry
Enable	Set to **On** to enable Request Control.
Policy Name	Specify the name of the appropriate policy.
Enable Branded 403 Page	Select whether to enable a branded 403 (Forbidden) page for this instance of the Request Control Cloudlet.
NetStorage	If using a branded 403 page, select the NetStorage domain that contains the branded 403 page.
Branded 403 Path and File Name	If using a branded 403 page, enter the full path of the branded 403 page, excluding the NetStorage CP code. You must include the file name in the path.

6. Save your changes to the rule, then activate the newly-updated property.