

Configuring Global ACLs

<https://campus.barracuda.com/doc/4259851/>

Global ACLs (URL ACLs) are strict allow/deny rules shareable among multiple services configured on the Barracuda Web Application Firewall. They are associated with configured Security Policies.

Steps To Configure Global ACLs

1. Go to the **SECURITY POLICIES > Global ACLs** page.
2. Select the policy from the **Policy Name** drop-down list.
3. In the **Create Global ACL** section, specify values for the following:
 1. **URL ACL Name** - Enter a name for the URL ACL.
 2. **URL Match** - Enter a URL to be matched against the URL in the request. The URL should start with a "/" and can have at most one "*" anywhere in the URL. Examples:
/Bank/Forms/*, /images/*.
 3. **Extended Match** - Define an expression that consists of a combination of HTTP headers and/or query string parameters. This expression is used to match against special attributes in the HTTP headers or query string parameters in the requests. Use '*' to denote "any request", that is, do not apply the Extended Match condition. For information on how to write extended match expression, see [Extended Match Syntax Help](#).
 4. **Extended Match Sequence** - Enter a number to indicate the order in which the extended match rule must be evaluated in the requests.
 - **Range:** 1 to 1000
 - **Default:** 1
 5. **Action** - Select the action from the drop-down list to be taken on the request matching this URL.
 1. *Process* - Processes any request matching this ACL.
 2. *Allow* - Allows the request by disabling all security checks on an incoming request that matches the ACL. It also disables Data Theft on such responses.
 3. *Deny and Log* - Denies any request matching this ACL and also logs the event. The request is not subjected to any security policies. This is an unconditional Deny. When a request is denied, the Barracuda Web Application Firewall sends a cryptic error response.
 4. *Deny with no Log* - Same as Deny, but the event is not logged.
 5. *Temporary Redirect* - Redirects the denied request with the 302 status code to the URL specified in the **Redirect URL** field.
 6. *Permanent Redirect* - Redirects the denied request with the 301 status code to the URL specified in the **Redirect URL** field.
 6. **Redirect URL** - Specify a URL to which a user should be redirected if **Action** is set to *Redirect*.
 7. **Follow Up Action** - Select the required follow up action to be taken whenever the request is denied.
 8. **Follow Up Action Time** - Specify the time (sec) to block the client IP if Follow Up Action is set to Block Client-IP. The time can range between 1 to 600000 seconds.
4. Click **Add**.

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.