

Allow/Deny Rules for Headers

<https://campus.barracuda.com/doc/20645728/>

You can enforce strict limitations on incoming headers intended for a service using the **WEBSITES > Allow/Deny Rules > Header : Allow/Deny Rules** section. You can sanitize HTTP headers that carry sensitive information identifying the client and some application-specific state information passed as one or more HTTP headers. A header ACL can be configured to prevent attack types and stop potentially malicious metacharacters and keywords from being allowed in a header.

To create a Header ACL rule:

1. Go to the **WEBSITES > Allow/Deny Rules** page.
2. In the **Header : Allow/Deny Rules** section, identify the service which needs a header ACL rule.
3. Click **Add** next to the service. The **Create Header ACL** window appears.
4. Specify appropriate values for the given fields and click **Save**.

For more information, click **Help** in the web interface. Also, see [Allow/Deny/Redirect Rules for URLs](#).

© Barracuda Networks Inc., 2024 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.