How to Add a Bot to the Allow List

https://campus.barracuda.com/doc/98216316/

You can add a bot definition to the allow list of bots either by selecting a bot definition from the Barracuda Advanced Threat Intelligence (ATI) service or by adding a custom bot definition. To add a bot definition, perform the following configuration.

Add a Bot from the ATI Bot Library

1. Go to the **BOT MITIGATION > Libraries** page, **Allowed Bots** section.
2. Click **Add Bot**.
3. On the **Add Bot** window, specify values for the following:
   - **Bot Definition** – Select the **From Bot Library** option.
     - **Name** – Specify the bot name that you want to search, or select a bot category and bot class to list the bots associated with the selected options.
     - **Bot Category** – Select the required category from the **Select Category** drop-down list.
     - **Bot Class** – Select the required class from the **Select Class** drop-down list.
     - Click **Search** to view the list of bots associated with the selected bot category and class.
     - In the table, select the check boxes next to the bot names that you want to add to the allowed bots list.
4. Click **Save**.

Add a Custom Bot

1. Go to the **BOT MITIGATION > Libraries** page, **Allowed Bots** section.
2. Click **Add Bot**.
3. On the **Add Bot** window, specify values for the following:
   - **Bot Definition** – Select the **Custom** option.
   - **Parent Name** – Enter a name for the bot group.
   - **User Agent**: Define a user agent expression by clicking the widget. This expression is used to match against the User-Agent header in the requests. To build an expression, click the **Edit** button and specify values for the following fields:
     - **User Agent Expression** – Displays the defined expression.
     - **Element Type** – By default, the element type is set to **Header**.
     - **Element Name** – By default, the element name is set to **User-Agent**.
     - **Operator** – Select the operator from the drop-down list. For more information, see Operators.
     - **Value** – Enter the user agent name that needs to be matched with the User-Agent header in the request.

        - **Concatenate** – Select the **Add** button to add some more expressions to the existing match sequence. Select the **Or** button to replace the existing match sequence.
        - Click **Insert** and then click **Apply** to apply this expression. Click **Cancel** to cancel this expression.
4. **Bot Identifier** – Select the way you want the Barracuda WAF to identify the bot.
    - **Host**: – Identifies the bot through the hostname.
        - **Host** – Enter a host name that needs to be matched against the client. The client IP address will be resolved against the DNS server using the reverse DNS lookup mechanism. This can be either a specific host match or a wildcard host match with a single * anywhere in the host name. For example, with *.example.com, any client matching this host is allowed.
    - **IP Addresses** – Identifies the bot through the IP address.
        - Specify the IP addresses that needs to be matched against the client IP address. If the IP address is matched, the request is allowed.
    - **ASN Group Name** – Identifies the bot through the ASN group name.
        - **ASN Group Name** – Select an ASN group from the **Select ASN Group** drop-down list. The AS numbers listed in the **ASN Details** field are matched against the client AS number. If the AS number is matched, the request is allowed.
        - **ASN Details** – The table displays the list of ASN names and the associated IDs that are configured in the selected ASN group.
5. Click **Save**.

After a custom bot definition is added to the **Allowed Bots** list, it gets displayed under **Allowed Bots** in the Web Scraping policy in the **BOT MITIGATION > Bot Mitigation > Web Scraping** section. You can select the bot under **Allowed Bots** to ensure that the bot-related checks happen when the matching request is received.

Operators

The following are the possible operators in an element match. The operators are case insensitive. For example: eq, Eq and EQ all behave the same.

- **is equal to** – true if the operand is equal to the given value. A case-insensitive string comparison is performed, so a value of "01" does not equal the value "1", whereas the values "one" and "ONE" are equal.
- **not equal to** – true if the operand is not equal to the given value. A case-insensitive string comparison is performed.
- **contains** – true if the operand contains the given value.
- **doesn't contain** – true if the operand does not contain the given value.
- **regex contains** – true if the operand contains the given value, specified as a regular expression.
- **regex not contains** – true if the operand does not contain the given value, specified as a

regular expression.

- **regex equals** – true if the operand matches the given value, specified as a regular expression.
- **regex not equals** – true if the operand does not match the given value, specified as a regular expression.
- **exists** – true if the operand exists. A value is not required.
- **not exists** – true if the operand does not exist. A value is not required.