F5® DISTRIBUTED CLOUD SERVICES
User Guide

Table of Contents

About the F5® DISTRIBUTED CLOUD SERVICES

F5® Distributed Cloud Bot Defense provides protection for applications from malicious bots and unwanted automation attacks.

General Workflow

Installation

Preconditions:

1. Installed Magento EE/CE
2. https://devdocs.magento.com/guides/v2.4/install-gde/composer.html
3. https://devdocs.magento.com/guides/v2.4/config-guide/varnish/config-varnish.html
4. Install F5_DistributedCloudConnector extension.

F5_ DistributedCloudConnector Installation guide:

1. Download archive.
2. Copy archive files to MAGE_ROOT/app/code/F5/DistributedCloudConnector
3. Execute php bin/magento set:up
4. Execute php bin/magento s:d:c
5. Execute php bin/magento setup:static-content:deploy (if magento in developer mode add "-f" argument)

The extension version:
The version of the extension can be found in the "*composer.json*" file.

The "Developer Mode":
Please note that the developer mode is not supported in the extension.

Extension Configuration

To find the F5 Extension configurations, please proceed to the:
Admin Panel > STORES > Configuration > F5® DISTRIBUTED CLOUD SERVICES

There are such modules available for configurations:

1. Bot Defense;
2. Account Protection;
3. Authentication Intelligence;

Bot Defense

The Bot Defense module contains such configuration sections:

1. General;
2. JS Insertion;
3. Login Protection;
4. Protected Endpoints;
5. Web Scraping;
6. Allow List;

General

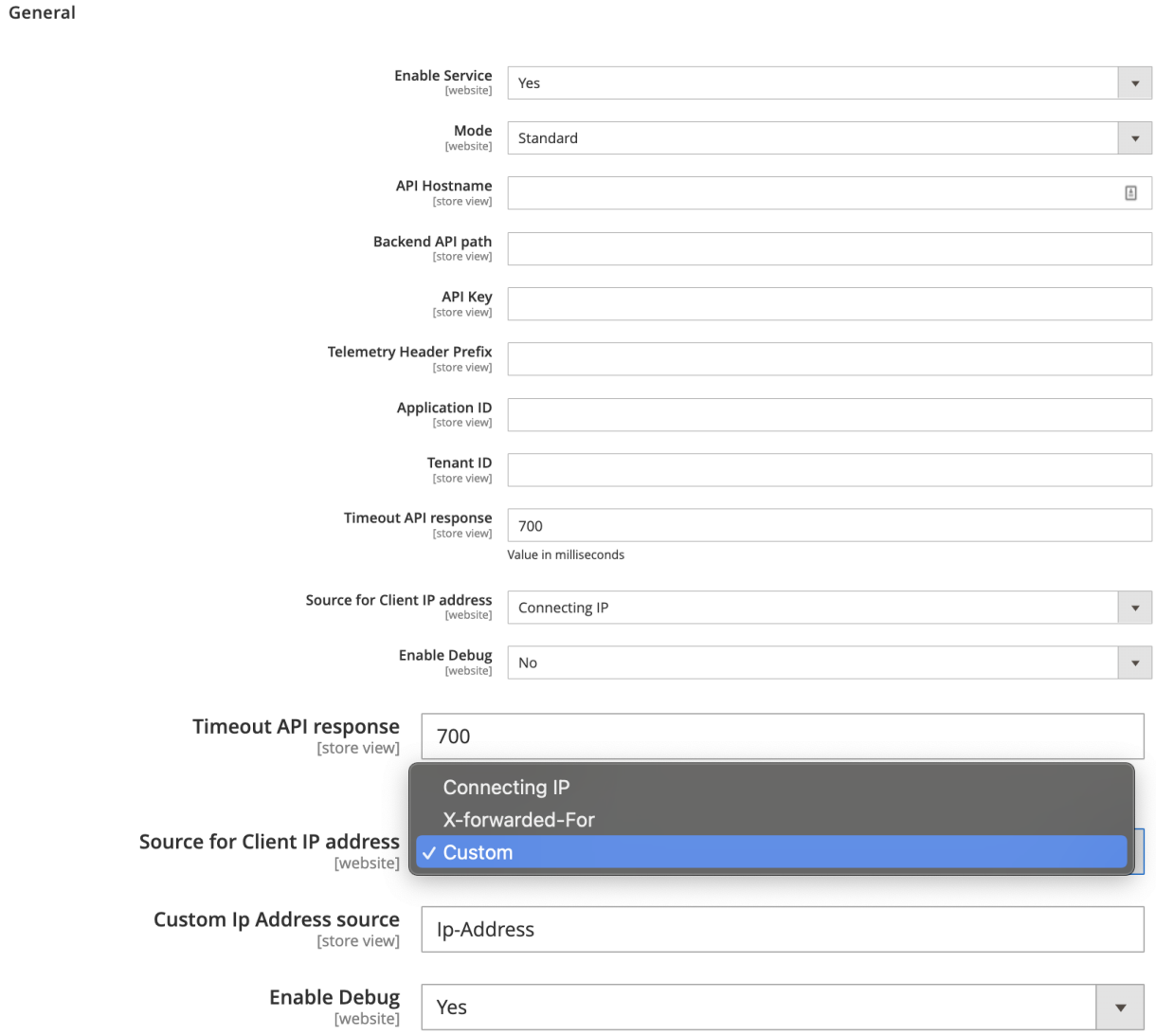
The “General” section contains options to enable and configure the connection of the “Bot Defense” module with the F5 Service.

Such options are available:

1. **Enable Service** - allows to enable service by selecting the “Yes” option and to disable it service by selecting the “No” option;
2. **Mode** - there are two options available:
    - **“Enterprise”** - the dedicated mode of usage where the “Application ID” and “Tenant ID” fields are not required;
    - **“Standard”** - the multi-tenant mode of operation;
3. **API Hostname** - the hostname provided by the F5 should be used here;
4. **Backend API path** - the path to the Bot Defense script file on the website backend;
5. **API Key** - this key is used for authentication of the API calls to the F5 system. The value for this field can be obtained from the F5 Distributed Cloud console;
6. **Telemetry Header Prefix** - the value for this field should be provided by the F5;
7. **Application ID** - the value for this field can be obtained from the F5 Distributed Cloud console (field is available only when the “Standard” mode is selected);
8. **Tenant ID** - the value for this field can be obtained from the F5 Distributed Cloud console (field is available only when the “Standard” mode is selected);
9. **Timeout API response** - the time (defined in milliseconds) that the module will wait for response from the F5 server. After that - the customer’s request will be processed by the Adobe Commerce backend. The default value is 700 milliseconds;
10. **Source for Client IP address** - this option allows to select what source to use for getting the customer’s IP address:
    - ***Connecting IP*** - the IP address will be gathered from the customer’s connection information;
    - ***X-Forwarded-For*** - the IP address will be gathered from the X-forwarded-For header;

- ***Custom*** - this option allows to define the custom header name to use for customer's IP address gathering;
  - ***Custom IP address source*** - the custom header name for gathering a customer's IP address. Please note that In the configured header, the first character of each word should be in upper case.

11. **Enable Debug** - the requests and responses to/from the F5 service will be recorded into the log file on the website server, when the option is enabled.



JS Insertion

In this section the JS tag insertion can be configured

1. **JS Path** - it is possible either enter https://<FQDN+JS_Location> (absolute JS tag) or just the URL path (relative JS tag) in the box.
   - The "absolute" JS tag or "relative" tag can be entered into the pages

- https://<FQDN+JS_Location> (Sample: https://www.foo.com/abc.js) <JS_Location> (Sample: /abc.js)
- If using “absolute” tag insertion, ensure the JS requests are routed to the F5 Bot Defense service.

2. **Insert JS option** - the option that allows to place the JS tag into the page structure in the different ways:
   - Before <script>
   - After </title>
   - After <head>
3. **JavaScript load mode** - select the load mode of the JavaScript on the page:
   - Async with caching
   - Async no caching
   - Sync with caching
   - Async with caching and defer XHR
4. **Insert JS to specific web pages** - allows to display or hide the “Specific pages list” field by selecting one of the options described below:
   - **When “Yes”** - the “Specific pages list” field shows:
     i. **Specific pages list** - the list of the pages that should have the JS tag should be defined in this field:
        1. *Only the path to the page should be defined (for ex. /about-us);*
        2. *Each new page starts from the new line;*
        3. *Wildcard can be used for page path definition; (“*”, “.” etc)*
        4. *To insert the JS tag to all pages - put the only “*” (asterix symbol) to the field*
        5. *The JS tag will not be present on any page while this field is empty*
   - ***When “No” - the*** “Specific page list” field is hidden and the JS tag is displayed on all available pages that are not defined in the “Excluded pages list” field.
5. **Exclude JS from specific web pages** - allows to display or hide the “Excluded pages list” field by selecting one of the options described below:
   - **When “Yes” -** the “Excluded pages list” field shows:
     i. **Excluded pages list** - the list of the pages that should be excluded from the JS tag insertion:
        1. *Only the path to the page should be defined (for ex. /about-us);*
        2. *Each new page starts from the new line;*
        3. *Wildcard can be used for page path definition; (“*”, “.” etc)*

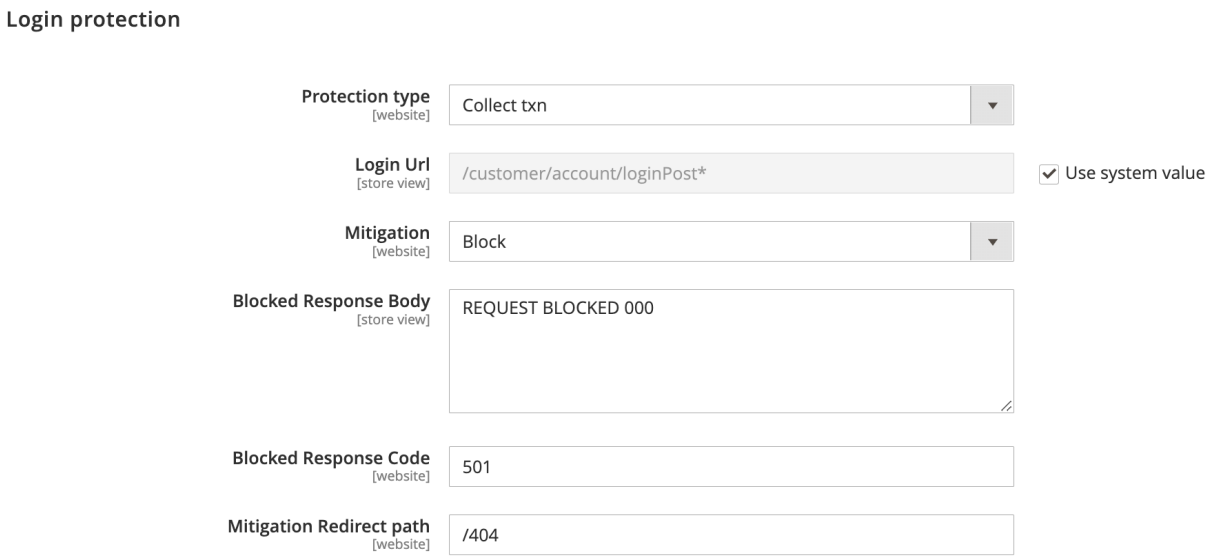
- ***When "No"*** *- the* "Excluded pages list" field is hidden and the JS tag is displayed according to the "Insert JS to specific web pages" configurations.

Login Protection

The "Login Protection" functionality allows to configure the Bot Defense for the Login action directly.
There are such options available for configuration:

1. **Protection type:**
    a. **Disable** - in this state, the Login Protection is disabled.
    b. **Collect txn** - the customer's verification will be performed after sending the login request to the origin destination.
    c. **Ignore txn** - the customer's verification will be performed right after clicking the "Login" button on the storefront, but before the Login request will be performed to the origin destination. The login transaction will not be sent to the F5 service.
2. **Login Url** - this field allows to define the login action URL, that should be protected by the "Bot Defense". By default it set to the - "/customer/account/loginpost*" destination, that is used by the Adobe Commerce platform by default. But it can be customized in cases when the non-default login functionality is using on the website.
3. **Mitigation** - the mitigation action type can be selected using this field. There three options available:
    a. **Continue** - no action will be performed and customer will be allowed to visit the destination page;
    b. **Block** - customer will be blocked from the destination page by the blank page with the content defined in the "**Blocked Response Body**" field and the response code defined in the "**Blocked Response Code**" field;

c. **Redirect** - the customer will be redirected to the page which path is defined in the “**Mitigation Redirect path**”.

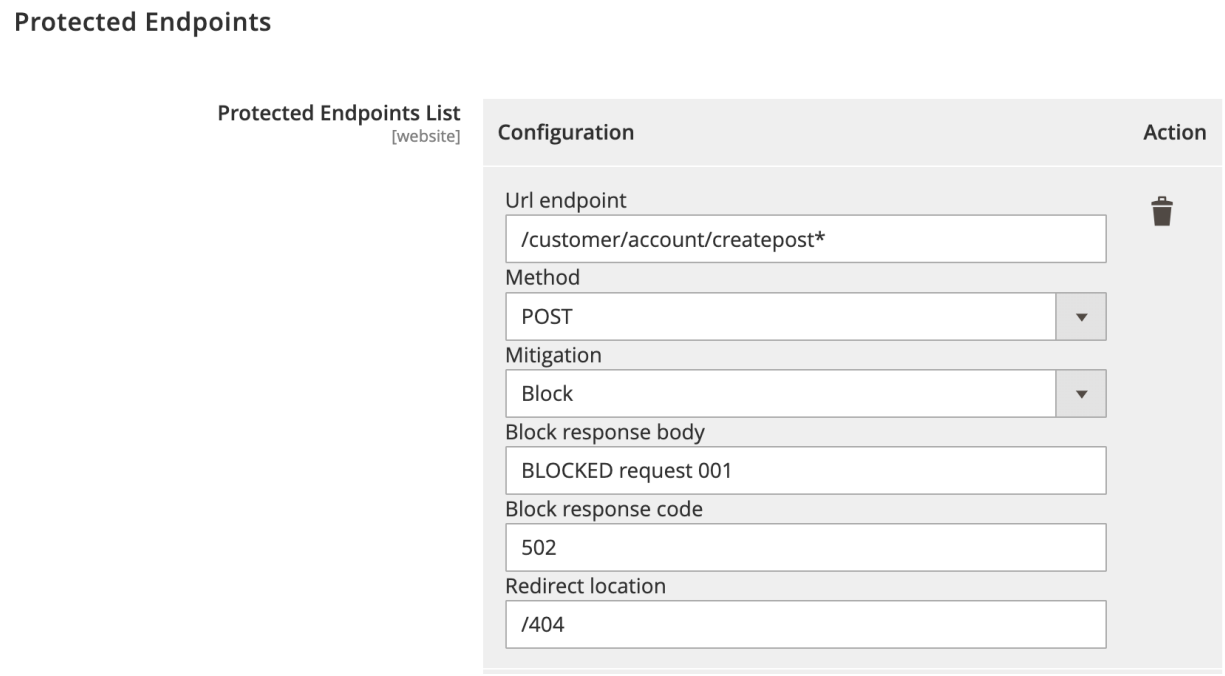


Protected Endpoints

The Protected Endpoints functionality allows to define pages and sources on the website that should be protected by the “Bot Defense”.

There are such options available for configuration:

1. **URL endpoint** - the path to the page or action that should be protected. Wildcards can be used to define complex URLs (“*”, “.” etc).
2. **Method** - the type of the request method that is performing to the defined page or action. These types of request methods are supported:
    a. GET;
    b. POST;
    c. PUT;
3. **Mitigation** - the mitigation action type can be selected using this field. There three options available:
    a. **Continue** - no action will be performed and customer will be allowed to visit the destination page;
    b. **Block** - customer will be blocked from the destination page by the blank page with the content defined in the “**Block Response Body**” field and the response code defined in the “**Block Response Code**” field;
    c. **Redirect** - the customer will be redirected to the page which path is defined in the “**Redirect location**”.



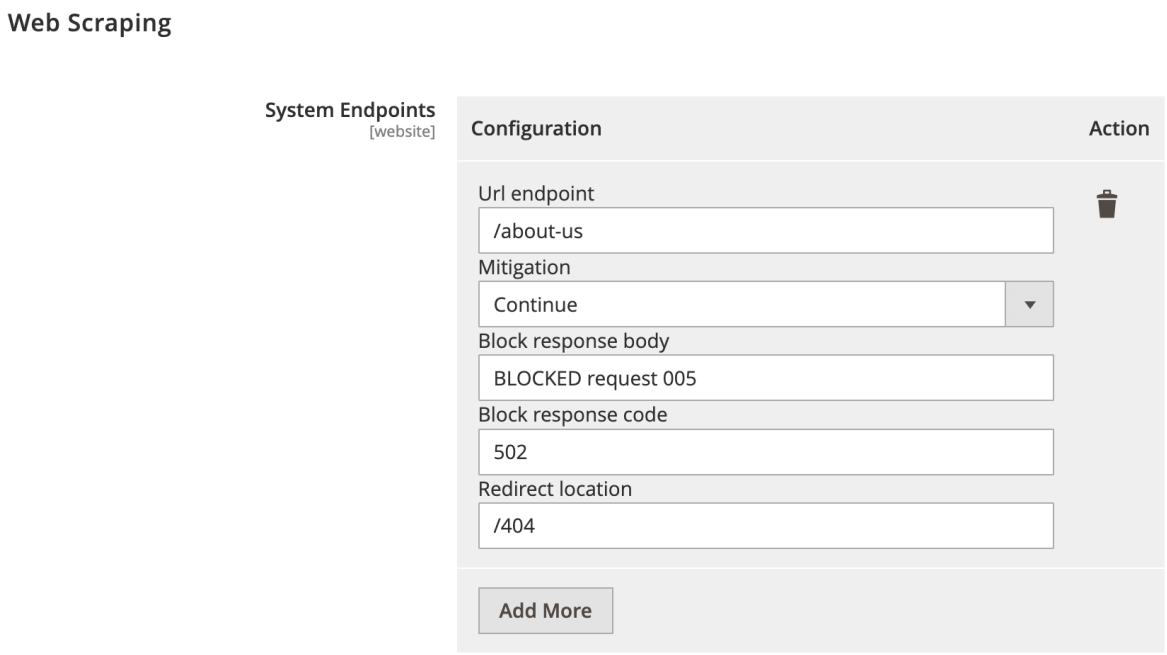
Web Scraping

The Web Scraping functionality allows to define pages and sources on the website that should be protected by the “Bot Defense”.

This option allows to protect the documents and pages that are accessible by the GET XHR requests.

The System Endpoints have such option and configurations:

1. **URL endpoint** - the path to the page or action that should be protected. Wildcards can be used to define complex URLs (“*”, “.” etc).
2. **Mitigation** - the mitigation action type can be selected using this field. There three options available:
    a. **Continue** - no action will be performed and customer will be allowed to visit the destination page;
    b. **Block** - customer will be blocked from the destination page by the blank page with the content defined in the “**Block Response Body**” field and the response code defined in the “**Block Response Code**” field;
    c. **Redirect** - the customer will be redirected to the page which path is defined in the “**Redirect location**”.

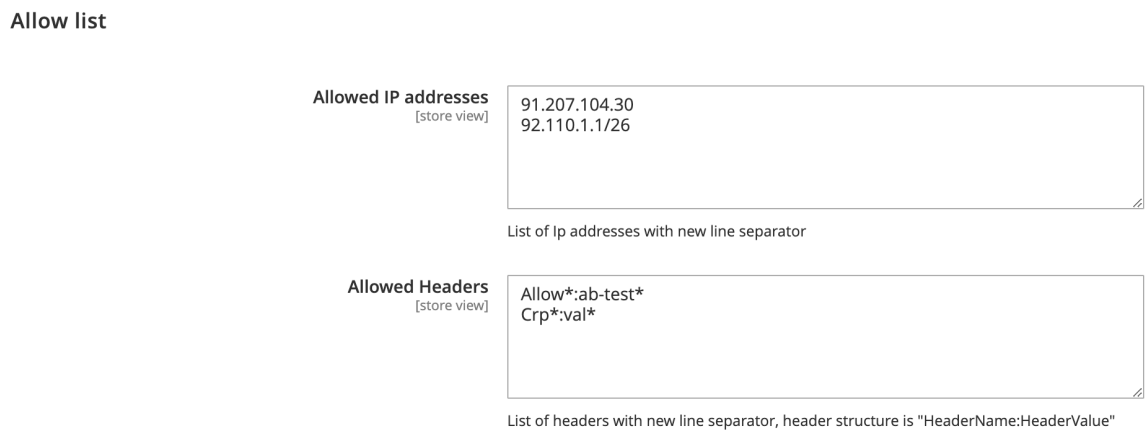


Allow List

The “Allow List” functionality allows the users or requests to get to the origin destination without performing verification by the Bot Defense.
There are two options that give this possibility: allow listing by the IP Address and by the request headers.

Allowed IP addresses:
The requests that are sent from the IP addresses defined in the “Allowed IP addresses” field will get to the endpoint without performing verification. (*Each new IP address should be defined in the new line. CIDR format is supported*).

Allow Header:
The requests that contain the [header]:[value] pair will be able to get to the endpoint without verification by the Bot Defense. *(Each new [header]:[value] pair should be defined in the new line. Wildcards can be used for both Header name and Header Value (“*”, “.” etc))*



Account Protection

F5 Distributed Cloud Account Protection provides a converged solution for application security and fraud protection powered by a real-time, closed-loop engine and large-scale unified telemetry to reduce customer friction and stop fraud before it happens.

General

The configuration page of the “Account Protection” module can be found by this way:
Admin panel > STORES > Configuration > F5® DISTRIBUTED CLOUD SERVICES > Account Protection

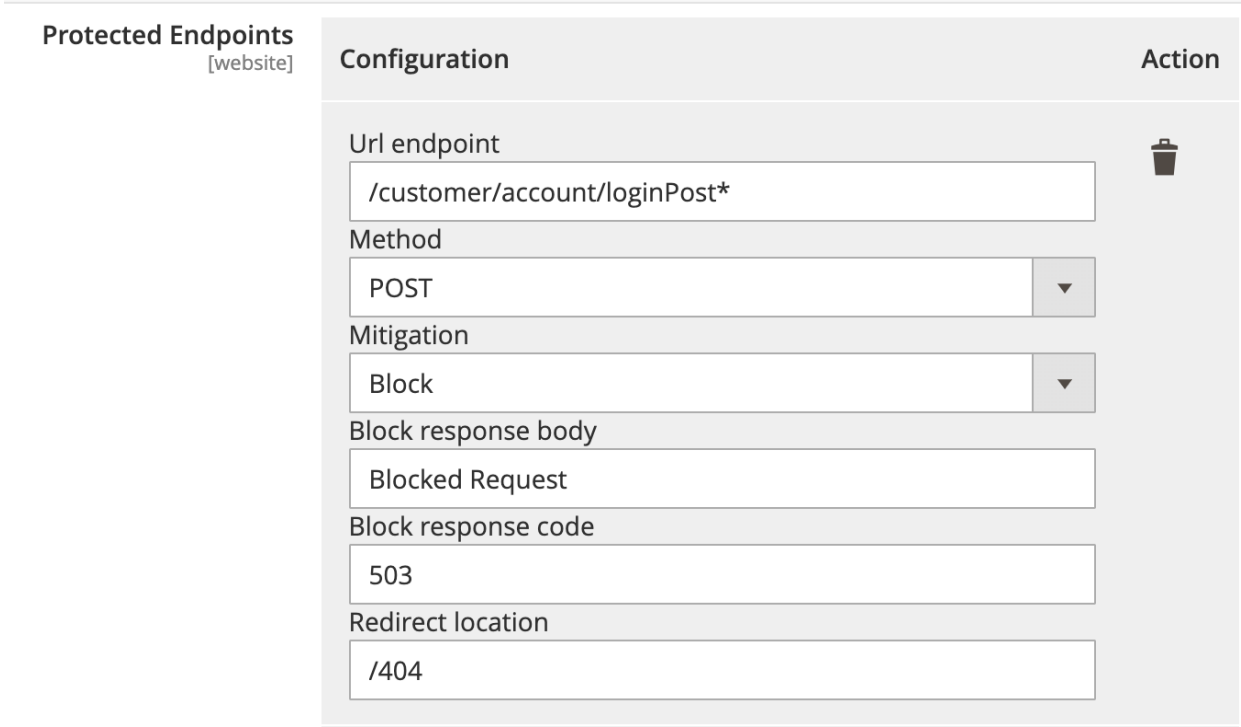
There are such configuration fields and options are available on the “General” section:

1. **Enable Service** - allows to enable service by selecting the “Yes” option and to disable it service by selecting the “No” option;
2. **API Hostname** - the host name of the Account Protection service;
3. **Script Tag** - path to the F5 Account Protection script;
4. **JS Path** - the path to the JS script file;
5. **Customer ID** - the customer identificator, can be obtained from the F5 Service;
6. **Cookie name** - the name of the cookie from the Account Protection service, that should be decrypted and processed;
7. **Decryption key** - the key that allows to decrypt the "fr" field's value in received cookie from the Account Protection;

Protected Endpoints

These options allow defining the endpoints that should be protected by the “Account Protection” functionality.

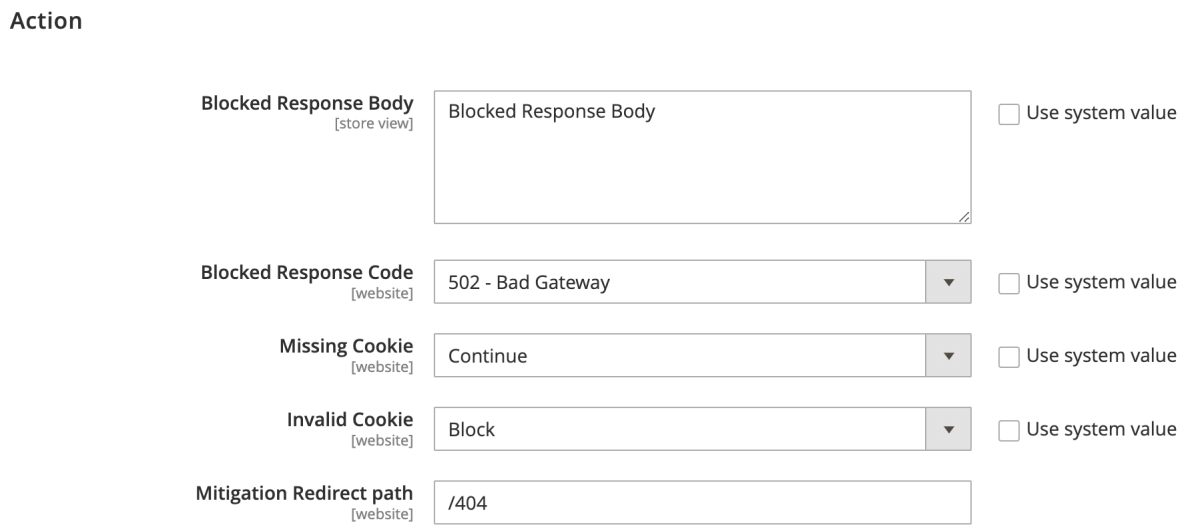
1. **URL endpoint** - the path to the page or action that should be protected. Wildcards can be used to define complex URLs (“*”, “.” etc).
2. **Mitigation** - the mitigation action type can be selected using this field. There three options available:
    a. **Continue** - no action will be performed and customer will be allowed to visit the destination page;
    b. **Block** - customer will be blocked from the destination page by the blank page with the content defined in the “**Blocked Response Body**” field and the response code defined in the “**Blocked Response Code**” field;
    c. **Redirect** - the customer will be redirected to the page which path is defined in the “**Mitigation Redirect path**”.
3. **Method** - the type of the request method that is performing to the defined page or action. These types of request methods are supported:
    a. GET;
    b. POST;
    c. PUT;
4. **Blocked Response Body** - the message that will be displayed on the blank page when the mitigation action “Block” is performing against malicious request;
5. **Blocked Response Code** - the status code that malicious user will get in response to the request to Protected Endpoint when the “Block” mitigation action is performed;
6. **Redirect location** - the path to the page where the malicious request will be redirected when the “Redirect” mitigation action is performed;



Action

The “Action” section contains the mitigation actions settings, such as:

1. **Missing Cookie** - this option allows the user to select the mitigation action for cases when the “Account Protection” cookie is missing. There are three options to select:
    a. Continue;
    b. Block;
    c. Redirect.
2. **Invalid Cookie** - this option allows the user to select the mitigation action for cases when the “Account Protection” cookie is invalid. There are three options to select:
    a. Continue;
    b. Block;
    c. Redirect.



Authentication Intelligence

Authentication Intelligence allows to extend the login session lifetime for the non-malicious users, after they were verified by F5 service.

General

There are such configuration fields and options are available on the “General” section:

1. **Enable Service** - allows to enable service by selecting the “Yes” option and to disable it service by selecting the “No” option;
2. **API Hostname** - the host name of the Authentication Intelligence service;
3. **Script Tag** - path to the F5 Authentication Intelligence script;
4. **JS Path** - the path to the JS script file;
5. **Customer ID** - the customer identificator, can be obtained from the F5 Service;
6. **Cookie name** - the name of the cookie from the Authentication Intelligence service, that should be decrypted and processed;
7. **Decryption key** - the key that allows to decrypt the "c" field's value in received cookie from the Authentication Intelligence service;

General

Enable Service [website]	Yes
API Hostname [store view]	
Script Tag [store view]	
JS Path [store view]	
Customer ID [store view]	
Cookie name [store view]	
Decryption key [store view]	