Data Theft Protection

https://campus.barracuda.com/doc/45026293/

Data theft protection prevents unauthorized disclosure of confidential information such as social security number, passwords, credit card information, etc.

To Create a Data Theft Element

URL: /v1/security_policies/{policy_id}/data_theft_protection			
Method: POST			
Description: Adds a data theft element with the given values.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
name	Alphanumeric	Yes	A name for this data theft element.
enabled	String	Optional	Use this data theft element to be matched in the server response pages. The values include: • yes • no
identity_theft_type	Enumeration	Yes	The identity theft pattern to which the element mentioned in “name” belongs to. The enumerated values include: • directory_indexing • credit_cards • social_security_numbers • custom
custom_identity_theft_type	Enumeration	Conditional	The identity theft pattern defined on the ADVANCED > Libraries page (if any). **Note**: Required ONLY when **identity_theft_type** is *custom*.
action	Enumeration		The action to be enforced on any page sent by the server containing this data type. The enumerated values include: • cloak • block
initial_characters_to_keep	Numeric	Optional	The number of initial characters to be displayed to the user. **Note**: Required ONLY when **action** is *cloak*.
trailing_characters_to_keep	Numeric	Optional	The number of trailing characters to be displayed to the user. **Note**: Required ONLY when **action** is *cloak*.

Example:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/data_theft_protection -u 'eyJldCI6IjEzODAxNDk3ODMiLCJwYXNzd29yZCI6ImVhZWYxNzBhNThhN2Y0MjBjM2IwYjYxYmMy\nMTJkZTJkIiwidXNlciI6ImFkbWluIn0=\n:' -X POST -H Content-Type:application/json -d '{"name":"element_1","identity_theft_type":"social_security_numbers"}'

Response:

{"id":"element_1","token":"eyJldCI6IjEzODAxNTAxNDkiLCJwYXNzd29yZCI6IjRmMGNhYTFlYWQzZTFiNDRkNDYyNWVjMDUx\nZTMxZGZjIiwidXNlciI6ImFkbWluIn0=\n"}

To Retrieve Data Theft Elements

URL: /v1/security_policies/{policy_id}/data_theft_protection /v1/security_policies/{policy_id}/data_theft_protection/{data_theft_protection_id}			
Method: GET			
Description: Lists all data theft elements if “data_theft_protection_id” is not specified.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
parameters	Alphanumeric	Optional	Any specific parameter name that needs to be retrieved. See *Example 2*.

Example 1:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/data_theft_protection/element_1 -u 'eyJldCI6IjEzODAxNDk3ODMiLCJwYXNzd29yZCI6ImVhZWYxNzBhNThhN2Y0MjBjM2IwYjYxYmMy\nMTJkZTJkIiwidXNlciI6ImFkbWluIn0=\n:' -X GET

Response:

{"initial_characters_to_keep":"0","name":"element_1","custom_identity_theft_type":"","identity_

theft_type":"social_security_numbers","trailing_characters_to_keep":"4","action":"block","id":"element_1","token":"eyJldCI6IjEzODAxNTAzODUiLCJwYXNzd29yZCI6IjVkZGI4YTJiMTdkNzkwZDg5NjIyM2Y0MTM1\nZjM2YzlmIiwidXNlciI6ImFkbWluIn0=\n","enabled":"1"}

Example 2:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/data_theft_protection/element_1 -u 'eyJldCI6IjE1MDE5MDUxMzkiLCJwYXNzd29yZCI6IjUwN2I1ZDRhMTc3Mzc4Zjc5NGY2ZmM3NTNh\nYTczM2IxIiwidXNlciI6ImFkbWluIn0=\n:' -X GET -G -d parameters=action,identity_theft_type

Response:

{"action":"block","id":"element_1","token":"eyJldCI6IjE1MDQzMTYyMTAiLCJwYXNzd29yZCI6ImVhZWRmMTQ2YTkwNmZiOWFiZDhiNDNkMGZl\nNzFlMmE0IiwidXNlciI6ImFkbWluIn0=\n","identity_theft_type":"social_security_numbers"}

To Update a Data Theft Element

URL: /v1/security_policies/{policy_id}/data_theft_protection/{data_theft_protection_id}			
Method: PUT			
Description: Updates the values of given parameters in the given data theft element.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
enabled	String	Optional	Use this data theft element to be matched in the server response pages. The values include: • yes • no

identity_theft_type	Enumeration	Optional	The identity theft pattern to which the element mentioned in “name” belongs to. The enumerated values include: • directory_indexing • credit_cards • social_security_numbers • custom
custom_identity_theft_type	Enumeration	Optional	The identity theft pattern defined on the ADVANCED > Libraries page (if any). **Note**: Required ONLY when **identity_theft_type** is *custom*.
action	Enumeration	Optional	The action to be enforced on any page sent by the server containing this data type. The enumerated values include: • cloak • block
initial_characters_to_keep	Numeric	Optional	The number of initial characters to be displayed to the user. **Note**: Required ONLY when **action** is *cloak*.
trailing_characters_to_keep	Numeric	Optional	The number of trailing characters to be displayed to the user. **Note**: Required ONLY when **action** is *cloak*.

Example:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/data_theft_protection/element_1 -u 'eyJldCI6IjEzODAxNDk3ODMiLCJwYXNzd29yZCI6ImVhZWYxNzBhNThhN2Y0MjBjM2IwYjYxYmMy\nMTJkZTJkIiwidXNlciI6ImFkbWluIn0=\n:' -X PUT -H Content-Type:application/json -d '{"trailing_characters_to_keep":"2","action":"cloak"}'

Response:

{"id":"element_1","token":"eyJldCI6IjEzODAxNTA3NjgiLCJwYXNzd29yZCI6IjdjZDZiMmUzMzMxN2E1ZGY2ZDEyMWRjYmY3\nMzJjNmU0IiwidXNlciI6ImFkbWluIn0=\n"}

To Delete a Data Theft Element

URL: /v1/security_policies/{policy_id}/data_theft_protection/{data_theft_protection_id}
Method: DELETE
Description: Deletes the given data theft element.

Example:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/data_theft_protection/element_1 -u 'eyJldCI6IjEzODAxNDk3ODMiLCJwYXNzd29yZCI6ImVhZWYxNzBhNThhN2Y0MjBjM2IwYjYxYmMy\nMTJkZTJkIiwidXNlciI6ImFkbWluIn0=\n:' -X DELETE

Response:

{"msg":"Successfully deleted","token":"eyJldCI6IjEzODAxNTA4MzgiLCJwYXNzd29yZCI6IjgwM2IxOTVmYzVlYzc0YjZkYzA1MjEzM2Nl\nZjBkYjI3IiwidXNlciI6ImFkbWluIn0=\n"}