Configuring Data Theft Protection

https://campus.barracuda.com/doc/17106004/

Data theft protection prevents unauthorized disclosure of confidential information. Configuring data theft protection requires two steps:

- Specify any at risk data elements handled by the web application by configuring a Security Policy.
- Enable protection of these elements where needed by configuring a URL Policy.

Sensitive data elements might require masking to prevent their unauthorized disclosure or requests containing sensitive data might be blocked altogether. You can configure a Security Policy to protect any sensitive data elements. These settings can then be used by any service associated with the security policy. URL policies applied to narrowly defined URL spaces requiring this protection can be individually enable as needed. Other URL spaces operate without unnecessarily incurring the processing hit. To optimize performance, enable data theft protection only for the parts of the website that are known to carry sensitive information.

Specifying at Risk Data Elements

To configure Data Theft Protection, navigate to the **SECURITY > Security Policies** page. Click the **New Security Policy** button. Give the new policy a name and click **Create**. Select this new policy under **Custom Policies**. Scroll to the **Data Theft Protection** section and click **Configure**. From here, you can configure new Identity Theft data types.

Enable URL Protection

You can enable protection for specific URLs using the **SECURITY > Advanced Security** page. Security Policy Data Theft settings are then enforced only for configured URLs. While, Barracuda Energize Updates provides a set of default protected patterns such as credit card and social security numbers, these can be expanded or customized, using **SECURITY > Libraries**, to include other web application specific data patterns needing protection from disclosure. Any configured pattern can be masked, or the response blocked altogether, if a protected pattern occurs in the server response.

When Data Theft Protection is enabled, the Barracuda Load Balancer ADC intercepts the response from the server and matches with the pattern listed in the **SECURITY > View Internal Patterns** page and **SECURITY > Libraries** page (if any custom identity theft patterns). If the response matches any of the defined patterns, it is blocked or cloaked based on the **Action** (**Block** or **Cloak**) set. If action is set to **Block**, the response sent by the server is blocked. If set to **Cloak**, a part of the data is cloaked that is, overwritten with "X"s.

The default identity theft elements provided by the Barracuda Load Balancer ADC are:

- Credit Cards (credit-cards)

- Directory Indexing (directory-indexing)
- Social Security Numbers (ssn)

Credit Cards and Social Security Numbers

To prevent exposure of personal data, such as Credit Card number or a Social Security Number (SSN), select **Block** to block the response from the server or **Cloak** to overwrite the characters based on values defined in the **Initial Characters to Keep** and **Trailing Characters to Keep** parameters. By default, the credit-card and ssn Protected Data Types are set to **Cloak**.

Directory Indexing

If a web server is configured to display the list of all files within a requested directory, it may expose sensitive information. The Barracuda Load Balancer ADC prevents exposure of valuable data by blocking the response from the server. By default, directory indexing is set to Block.

To configure data theft protection, select a policy from the **Policy Name** list and click **Configure...** under **Data Theft Protection** in the **Security Policies** section.