How to Mask Sensitive Data in Logs

https://campus.barracuda.com/doc/22118831/

- Masking cannot be applied to sensitive data in custom parameters or custom headers.
- After data is masked, it cannot be retrieved, recovered, or restored.
- Note that the "SECURITY" module is available only in the 540 and above models

You can configure the Barracuda Load Balancer ADC to mask sensitive data before logging it. Sensitive data such as credit card information, U.S. Social Security numbers (SSNs), or other proprietary data in the URL parameters of a request can be masked. Data masking is configured for an application using parameter names to specify sensitive data.

To configure data masking:

1. Go to the **SECURITY > Advanced Security** page.
2. In the **Mask Sensitive Data** section, click **Edit** in the row for the virtual service that requires data masking.
3. In the **Mask Sensitive Data** window, enter the names of the parameters to mask. You can provide multiple parameter names separated by commas with no spaces between them. (For example: `cardId,securityNumber,password`).
4. Click **Save** .

On the **BASIC > Access Logs** page, the sensitive data will be overwritten by Xes.

© 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.