07-12-2026

Web proxy data

Web proxy data refers to the information generated, collected, or analyzed by a web proxy server as it intermediates communication between client devices and web servers. A web proxy acts as a gateway, forwarding client requests to the internet and retrieving responses on their behalf. Web proxy data includes logs, metadata, and analytics that capture details about web traffic, such as requested URLs, user IP addresses, access times, and filtering decisions.

This data is valuable for monitoring internet activity, enforcing security policies, filtering web content, and analyzing user behavior. It is commonly used in enterprise environments, schools, and other organizations to ensure safe and efficient internet usage.

Web proxy data typically includes:

- **Request data:** This refers to information about web requests sent by clients through the proxy
- **Response data**: This includes details about responses received from the requested web servers
- **User and device metadata**: This includes data about the users or devices that made the requests
- **Bandwidth and traffic usage**: This includes information about the amount of data transferred through the proxy
- **Filtering and security data**: This includes data about blocked or filtered web traffic
- **Time-based data**: This includes information related to the timing and frequency of requests
- **Authentication and access control data**: This includes details about user authentication, access policies, and permissions
- **Real-time threat intelligence data**: This includes data related to detected threats or suspicious activities
- **Cache data**: This includes details about cached web content to improve performance and reduce bandwidth usage
- **Performance metrics**: This includes information about the performance of the proxy server

The Splunk Common Information Model (CIM) add-on contains a Web data model with fields that describe web server and/or proxy server data in a security or operational context.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Add-ons and apps

- Splunk Add-on for Squid Proxy
- Splunk Add-on for NGINX
- Splunk Add-on for Check Point Log Exporter
- Splunk Add-on for McAfee Web Gateway
- Add-on for McAfee/SkyHigh Web Gateway (MWG/SWG/MWGCS)
- Splunk Add-on for Symantec Blue Coat ProxySG
- Splunk Add-on for Palo Alto Networks
- Splunk Add-on for Fortigate
- Splunk Add-on for HAProxy
- Fortinet FortiGate Add-On for Splunk
- Cisco Umbrella Connector
- PAVO Web Proxies App for Splunk
- Zscaler
  - Zscaler Technical Add-On for Splunk
  - Zscaler Splunk App
  - Zscaler Connector
  - Atlas ITSI Content Pack for ZScaler

Splunk Lantern articles for the Splunk platform

- Configuring Splunk add-on for McAfee/Skyhigh Web Gateway
- Monitoring NIST SP 800-53 rev5 control families
- Running common General Data Protection Regulation compliance searches
- Finding large web uploads
- Detecting malicious activities with Sigma rules
- Automating threat operations and threat hunting with the Recorded Future App for Splunk

Splunk Lantern articles for Splunk security products

- Monitoring for indicators of ransomware attacks
- Detecting Log4j remote code execution