

LOGZILLA DOCUMENTATION

Microsoft IIS

Rules, dashboards, and triggers for Microsoft IIS W3C access logs forwarded by NXLog or another file shipper

LogZilla App Store · Generated October 31, 2026 · logzilla.ai/docs/logzilla-appstore/microsoft-iis

Overview

Microsoft Internet Information Services (IIS) is the web server built into Windows Server. It hosts ASP.NET and static sites, and many Microsoft products such as Exchange and SharePoint run on top of it. IIS records every request in a per-site log file in the W3C Extended Log File Format, its default format, which carries the client address, request, status, substatus, Win32 status and processing time of each request. Monitoring those logs shows traffic volume per site, error rates, slow responses and attack probes against public-facing applications.

App Function

- Parse IIS access log lines in the W3C Extended format delivered by NXLog or another file shipper under the program name `Microsoft-IIS`
- Recognize the default and the full IIS field selections, and the usual variations between them, from the shape of each line, without depending on the `#Fields` header line
- Extract the site, server and client addresses, port, user, method, status code, IIS substatus, Win32 status, protocol version, user agent and a response-time bucket
- Classify every request as `Event ClassWeb` and flag path traversal, SQL injection, command injection, Log4Shell and exploit-probe requests with MITRE ATT&CK techniques and compliance frameworks
- Rewrite the stored message to the request, status, client, user, site and user agent so that cookies, referrers, byte counts and opaque query tokens no longer defeat deduplication
- Provide the `Microsoft IIS: Web Traffic` dashboard and feed the WebOps dashboard
- Alert on server errors, detected attacks and forbidden requests

Vendor Documentation

- [IIS Log File Settings \(logFile element\)](https://learn.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/sitedefaults/logfile/) (https://learn.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/sitedefaults/logfile/)
- [IIS Central Logging \(log element\)](https://learn.microsoft.com/en-us/iis/configuration/system.applicationhost/log/) (https://learn.microsoft.com/en-us/iis/configuration/system.applicationhost/log/)
- [W3C Logging Fields and Order \(HTTP Server API\)](https://learn.microsoft.com/en-us/windows/win32/http/w3c-logging) (https://learn.microsoft.com/en-us/windows/win32/http/w3c-logging)
- [NXLog Community Edition Reference Manual: im_file](https://docs.nxlog.co/ce/current/index.html#im_file) (https://docs.nxlog.co/ce/current/index.html#im_file)
- [NXLog: Microsoft IIS \(written for NXLog Agent\)](https://docs.nxlog.co/integrate/microsoft-iis.html) (https://docs.nxlog.co/integrate/microsoft-iis.html)

Device Configuration

IIS writes its access logs to disk and does not send syslog. A file shipper on the Windows host tails the log files and forwards each line to LogZilla. The steps below cover the IIS logging settings and NXLog Community Edition as the shipper.

IIS logging settings

The defaults are correct; verify them in **Internet Information Services (IIS) Manager -> server or site -> Logging**:

Format: W3C.

One log file per: Site. Each site then logs under %SystemDrive%\inetpub\logs\LogFiles\W3SVC<site id>\ and starts a new u_exYYMMDD.log file every day.

Log Event Destination: Log file only (or Both log file and ETW event). ETW event only writes no file and nothing is forwarded.

Select Fields: keep the default selection. To tag requests with the site name, also select **Host (cs-host)**; the full selection is supported as well.

When **One log file per** is set to Server (central W3C logging), all sites share one directory and the shipper's file pattern points at that directory instead.

NXLog Community Edition

Install NXLog Community Edition on the IIS host and replace C:\Program Files\nxlog\conf\nxlog.conf with the following, changing logzilla.example.com to the LogZilla server address and the W3SVC directory numbers to the site ids listed in IIS Manager under **Sites**. NXLog Community Edition accepts wildcards in the file name but not in a directory name, so each site gets its own <Input> block:

```
Panic Soft

define ROOT C:\Program Files\nxlog
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Extension _syslog>
    Module xm_syslog
</Extension>

<Input iis_site_1>
    Module im_file
    File 'C:\inetpub\logs\LogFiles\W3SVC1\u_ex*.log'
    SavePos TRUE
    ReadFromLast TRUE
    PollInterval 1
```

```

# Do not forward the W3C header lines (#Software, #Version, #Date, #Fields).
Exec if $raw_event =~ /^#/ drop();

# Value that appears in LogZilla's "program" field.
Exec $SourceName = "Microsoft-IIS";
</Input>

<Input iis_site_2>
  Module      im_file
  File        'C:\inetpub\logs\LogFiles\W3SVC2\u_ex*.log'
  SavePos      TRUE
  ReadFromLast TRUE
  PollInterval 1
  Exec if $raw_event =~ /^#/ drop();
  Exec $SourceName = "Microsoft-IIS";
</Input>

<Output logzilla>
  Module om_tcp
  Host    logzilla.example.com
  Port    514
  Exec    to_syslog_ietf();
</Output>

<Route iis_to_logzilla>
  Path iis_site_1, iis_site_2 => logzilla
</Route>

```

Add an `<Input>` block for every further site and list it in the `Route`. To follow every site with one input, including sites created later, point the file pattern at the `LogFiles` directory and let NXLog search its subdirectories:

```

<Input iis>
  Module      im_file
  File        'C:\inetpub\logs\LogFiles\u_ex*.log'
  Recursive    TRUE
  SavePos      TRUE
  ReadFromLast TRUE
  PollInterval 1
  Exec if $raw_event =~ /^#/ drop();
  Exec if file_name() =~ /FTPSVC/ drop();
  Exec $SourceName = "Microsoft-IIS";
</Input>

<Route iis_to_logzilla>
  Path iis => logzilla
</Route>

```

The `file_name()` line keeps the IIS FTP logs out; the FTP service writes them to `FTPSVC<id>` directories under the same root with the same file name pattern.

Restart the `nxlog` service after saving the configuration.

Other file shippers work the same way: forward each line unchanged as the syslog message and set the program (syslog tag) to `Microsoft-IIS`, `IIS`, `W3SVC` or `iis_access`.

Verification

Open a page on one of the sites, then search LogZilla for events with `Vendor` set to `Microsoft` and `Product` set to `IIS`. The message reads as the request, for example `GET /Dashboard 200 client=203.0.113.10 site=www.example.com ua="..."`, and the `Microsoft IIS: Web Traffic` dashboard populates.

Incoming Log Format

Each request is one line of space-separated fields. IIS writes the selected fields in this fixed order and leaves out the ones that are not selected:

```
date time s-sitename s-computername s-ip cs-method cs-uri-stem
cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie)
cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes
cs-bytes time-taken
```

- **date, time** - Request time in UTC (LogZilla records its own arrival time)
- **s-sitename** - Site id (`W3SVC1`); used as `Site` when `cs-host` is not logged
- **s-computername** - Server name; the syslog host already carries it
- **s-ip, s-port** - Server address and port (`DstIP`, `DstPort`)
- **cs-method, cs-uri-stem, cs-uri-query** - Request verb, path and query string
- **cs-username** - Authenticated user, – for anonymous (`User`)
- **c-ip** - Client address, IPv4 or IPv6 (`SrcIP`)
- **cs-version** - Protocol version (`HTTP Version`)
- **cs(User-Agent)** - Browser string with spaces replaced by + (`User Agent`, decoded)
- **cs(Cookie), cs(Referer)** - Not tagged and left out of the stored message
- **cs-host** - Host header (`Site`)
- **sc-status, sc-substatus** - HTTP status (`HTTP Status Code`) and IIS substatus (`IIS Substatus` when not 0)
- **sc-win32-status** - Windows status code (`Win32 Status` when not 0)
- **sc-bytes, cs-bytes** - Byte counts, not tagged
- **time-taken** - Processing time in milliseconds (`Response Time`)

The default IIS selection omits s-sitename, s-computername, cs-version, cs(Cookie) and cs-host; the byte counters are part of the default since the February 2026 Windows update. Custom fields appended after time-taken are ignored. Every new log file starts with four header lines (#Software, #Version, #Date, #Fields); when a shipper forwards them they are tagged with Vendor and Product only.

The stored message is rewritten as `<method> <stem>[?<query>] [<status>[.<substatus>]] [client=<c-ip>] [user=<user>] [site=<site>] [ua="<user agent>"]`; each bracketed part is present when its field is logged and not empty. The query string is kept when it is 64 characters or shorter and replaced by ? . . . otherwise, except for a detected attack, whose query is kept up to 1024 characters because it is the evidence. The W3C timestamp, cookie, referrer and byte counts are dropped so that repeated requests deduplicate.

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Microsoft	Always Microsoft
Product	IIS	Always IIS
Event Class	Web	Web, or Web, Security for a detected attack
Event Type	Web Security	Set for detected attacks only
Site	www.example.com	Host header, or the site id when the host is not logged
DstIP	10.0.0.5	Server address (HC)
DstPort	https	Server port as a service name
SrcIP	203.0.113.10	Client address (HC)
User	user1	Authenticated user (HC)
HTTP Method	GET	Request verb
HTTP Status Code	404 Not Found	HTTP status with its name
HTTP Version	HTTP/2	Protocol version the client used

Tag Name	Example	Description
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) ...	Browser string with spaces restored (HC)
IIS Substatus	401.2	Status and IIS substatus, when the substatus is not 0
Win32 Status	64 Client Disconnected	Windows status code when not 0, with its name for the common codes and as a bare number otherwise
Response Time	100-500ms	Processing time bucket: <100ms, 100-500ms, 500ms-1s, 1-5s, >5s
IIS Attack Type	SQL Injection	Path Traversal, SQL Injection, Command Injection, Exploit Probe or Log4Shell
MitreId	T1190	MITRE ATT&CK technique of a detected attack
MITRE Tactic	Initial Access	MITRE ATT&CK tactic of a detected attack
Compliance - <framework>	1	Applied to detected attacks, one tag per framework

Log Examples

Request with the full field selection

```
2026-01-01 12:00:00 W3SVC1 WEB-1 10.0.0.5 GET /Dashboard - 443 - 203.0.113.10 HTTP/2 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36 ASP.NET_SessionId=abc123 https://www.example.com/www.example.com 200 0 0 101964 3534 82
```

Stored as:

```
GET /Dashboard 200 client=203.0.113.10 site=www.example.com ua="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
```

Request with the default field selection

```
2026-01-01 12:00:01 10.0.0.5 POST /login - 443 - 198.51.100.20 Mozilla/5.0+
(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36 https://www.example.com/login 401 0 0 1535 1201 106
```

Server error with substatus and Win32 status

```
2026-01-01 12:00:03 W3SVC2 WEB-1 10.0.0.5 GET /api/report - 443 user1 203.0.113.10 HTTP/1.1
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36 - https://www.example.com/
api.example.net 500 19 5 1234 567 6000
```

SQL injection probe

```
2026-01-01 12:00:05 W3SVC1 WEB-1 10.0.0.5 GET /search q=%27+UNION+SELECT+1%2C2-- 443 - 203.0.113.10
HTTP/2 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36 - - www.example.com 200 0 0 512
300 40
```

Log file header

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2026-01-01 12:00:00
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent)
cs(Referer) sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken
```

Dashboards

- **Microsoft IIS: Web Traffic** - request counts and rate, 4xx, 5xx and attack badges, status trend, top sites, clients, user agents, response time distribution, IIS substatus and Win32 status breakdowns, attack types and MITRE techniques, and a live request stream.

IIS requests also appear on the **WebOps: Overview** dashboard together with the other web servers.

Triggers

Trigger	Description
Microsoft IIS: Server Error (5xx)	A request ended in a 5xx status
Microsoft IIS: Attack Detected	A request matched an attack pattern
Microsoft IIS: Access Forbidden (403)	A request was refused with 403

The 403 trigger fires on every 403, including the routine 403.4 (SSL required) and 403.14 (directory listing refused) substatus; disable it or narrow its filter where those are expected.

Caveats

- The LogZilla Windows agent forwards Windows Event Log records, not log files, so it is not a path for IIS logs. Use NXLog or another file shipper that follows the daily `u_ex*.log` files by wildcard.
- The parser places the fields around `s-port` and `c-ip`, both IIS defaults. With `s-port` turned off, the client address and user are still found. With `c-ip` turned off, only the server address, port, method, path, status, substatus, Win32 status and response time are tagged; keep `c-ip` selected.
- `Response Time` requires `time-taken`, and `IIS Substatus` and `Win32 Status` require their fields; all three are IIS defaults. When exactly four numbers follow the status (both byte counters without `time-taken`, or one byte counter with it), the last one is not read as `time-taken` and `Response Time` is not set.
- LogZilla stamps each line with its arrival time, not with the W3C `date` and `time` fields, so a backlog replayed after a shipper restart carries the replay time.
- The HTTP.sys error log (`HTTPERR`), the IIS native and NCSA formats, and IIS FTP logs are not parsed.