LOGZILLA DOCUMENTATION

Microsoft

LogZilla App Store application: Microsoft

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/microsoft

© LogZilla Corporation · logzilla.ai

Overview

Microsoft Windows produces log events from various services and programs but does not natively support forwarding events to external log collectors. The LogZilla Windows Event Forwarder reads local Windows events and forwards them to LogZilla in JSON format.

App Function

Windows events forwarded by the LogZilla Windows Event Forwarder are processed to extract security-relevant metadata including:

- Event IDs and descriptions
- Usernames and domain information
- Source IP addresses
- MITRE ATT&CK technique mappings
- Process creation details for suspicious activity detection

Vendor Documentation

- Microsoft Windows (https://www.microsoft.com/en-us/windows/)
- Event Logging (https://docs.microsoft.com/en-us/windows/win32/eventlog/event-logging)

Prerequisites

Required: The LogZilla Windows Event Forwarder (https://github.com/logzilla/extras/tree/master/winagent) must be installed on each Windows system. Without the agent, no Windows events will be forwarded to LogZilla.

Device Configuration

Download the agent from the LogZilla extras repository (https://github.com/logzilla/extras/tree/master/winagent)
Install the agent on each Windows system to monitor
Configure the agent with the LogZilla server address and ingest token
Select which Event Logs to forward (Security, System, Application, etc.)
Start the LogZilla Windows Event Forwarder service
The agent configuration interface allows selection of specific Event Logs and filtering options.

Incoming Log Format

The Windows Syslog Agent converts native Windows events into JSON format for LogZilla processing.

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Microsoft	Vendor name for cross-vendor filtering
Product	Windows	Product name for cross-vendor filtering
Event Class	auth, security, system	Cross-vendor event classification
Event Type	login_failure	Specific event type (login_failure, login_success, account_created)
MSWin EventID	4625	Windows Event ID
MSWin EventLog	Security	Windows Event Log name
MSWin Category	Logon/Logoff	Windows event category
MSWin Sub Category	Logon	Windows event sub-category
Criticality	High, Medium, Low	Event criticality level
MSWin Description	An account failed to log on	Human-readable event description
MitreId	T1110	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic category
User	jsmith	Target username for auth events
User Domain Name	CORP	Target user domain name
SrcIP	192.168.1.100	Source IP address

© LogZilla Corporation · logzilla.ai

Tag Name	Example	Description
`MSWin Failed Login User`	`admin`	Username for failed login (4625)
`MSWin Failed Login Source Network`	`192.168.1.100`	Source IP for failed login (4625)
`MSWin New Process`	`C:\Windows\System32\cmd.exe`	New process path (4688)
`MSWin Process Args`	`powershell.exe -enc ...`	Process arguments (4688)
`MSWin Parent Process`	`C:\Windows\explorer.exe`	Parent process (4688)
`MSWin Suspicious Indicator`	`Encoded Command`	Suspicious activity indicator

MITRE ATT&CK Mapping

The app maps security-relevant Windows events to MITRE ATT&CK techniques:

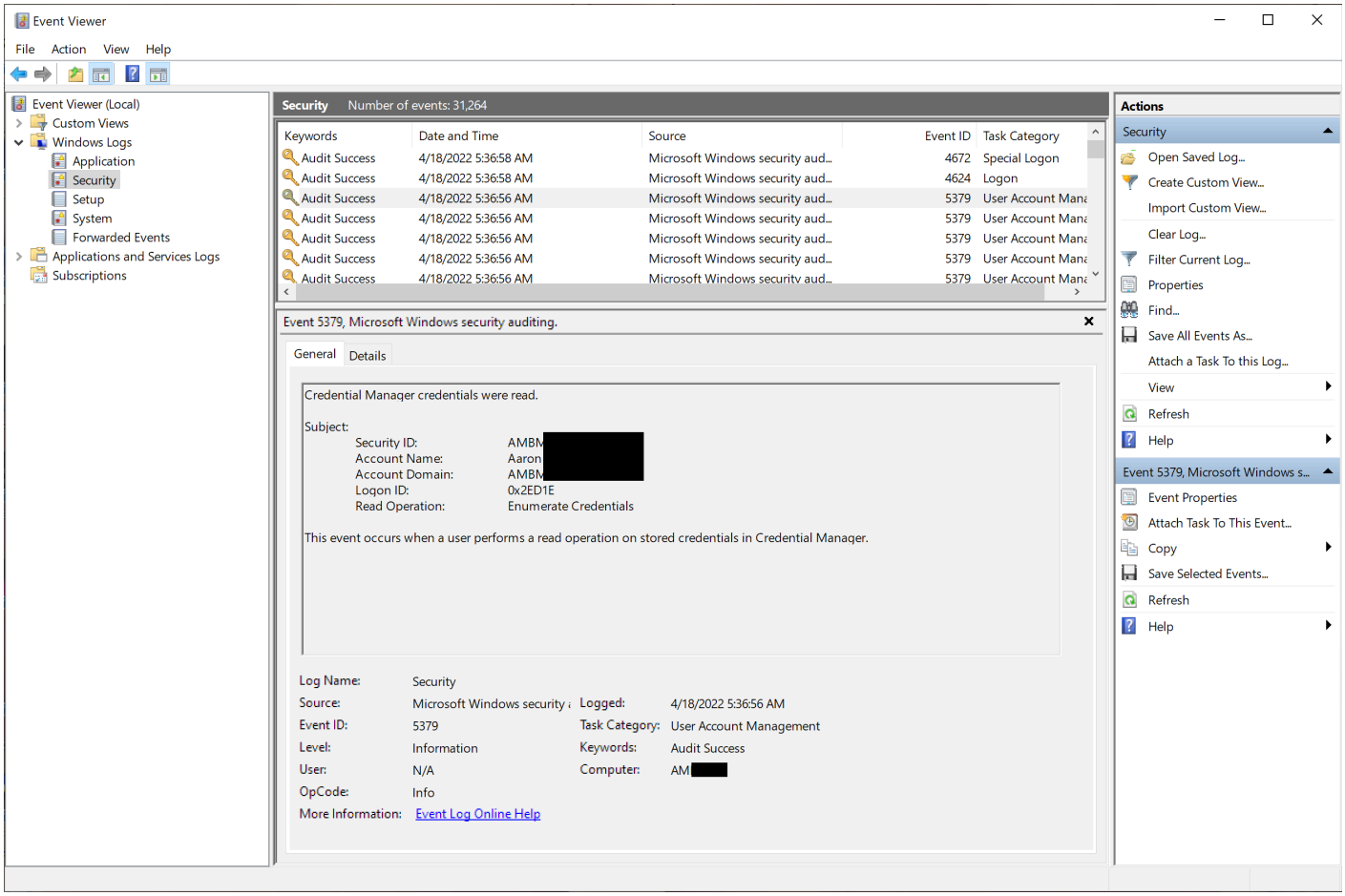
Event ID	Technique	Tactic	Description
4625, 4740, 4776	T1110	Credential Access	Brute Force
4771, 4768, 4769	T1558	Credential Access	Kerberos Tickets
4720	T1136.001	Persistence	Create Account
7045, 4697	T1543.003	Persistence	Windows Service
4672, 4728, 4732, 4756	T1078	Privilege Escalation	Valid Accounts
1102	T1070.001	Defense Evasion	Clear Event Logs
4624	T1021	Lateral Movement	Remote Services
4688 (suspicious)	T1059	Execution	Command Interpreter

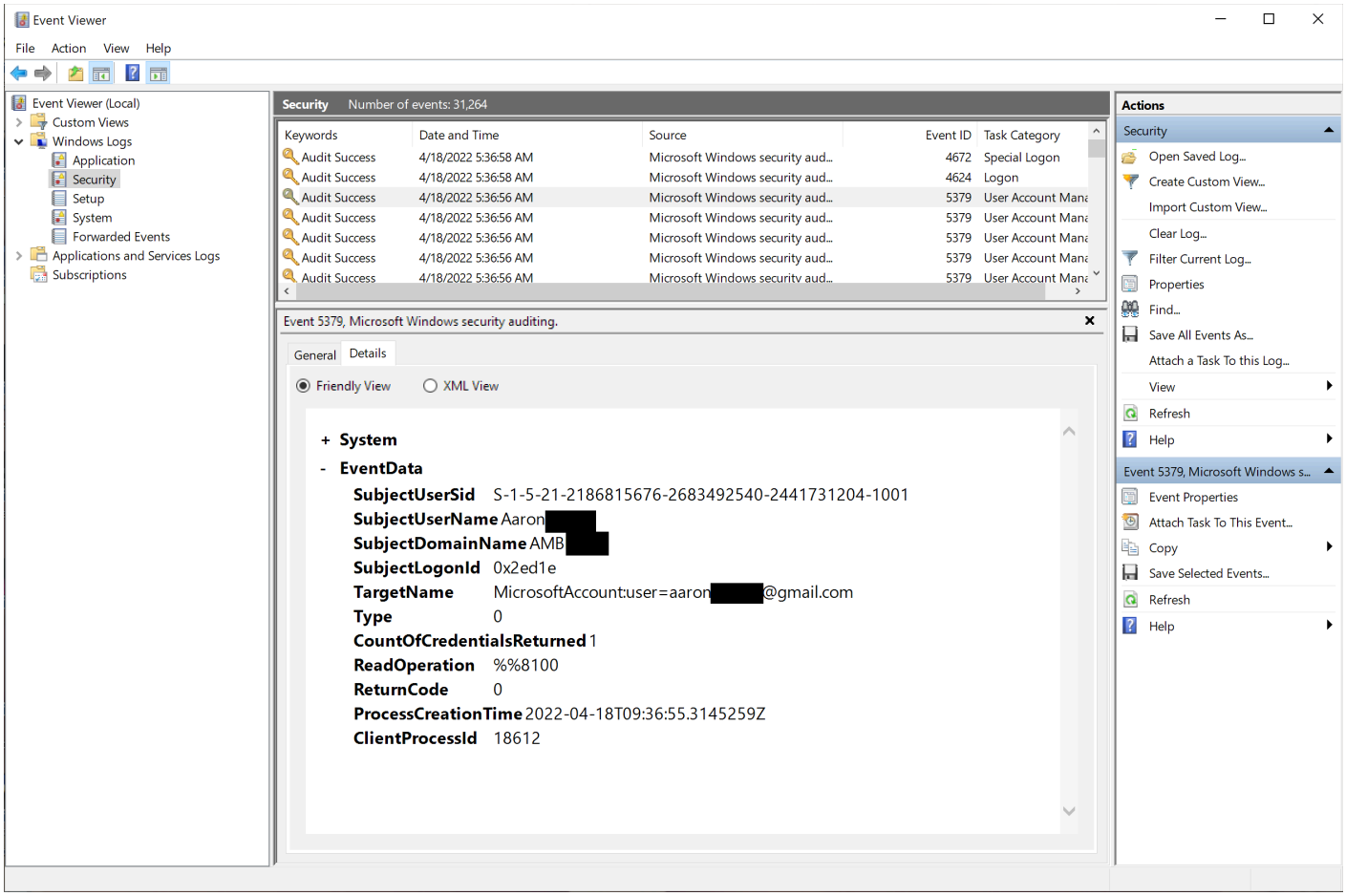
Process creation events (4688) are only flagged when suspicious patterns are detected, such as encoded PowerShell commands, LOLBins, or execution from temporary directories.

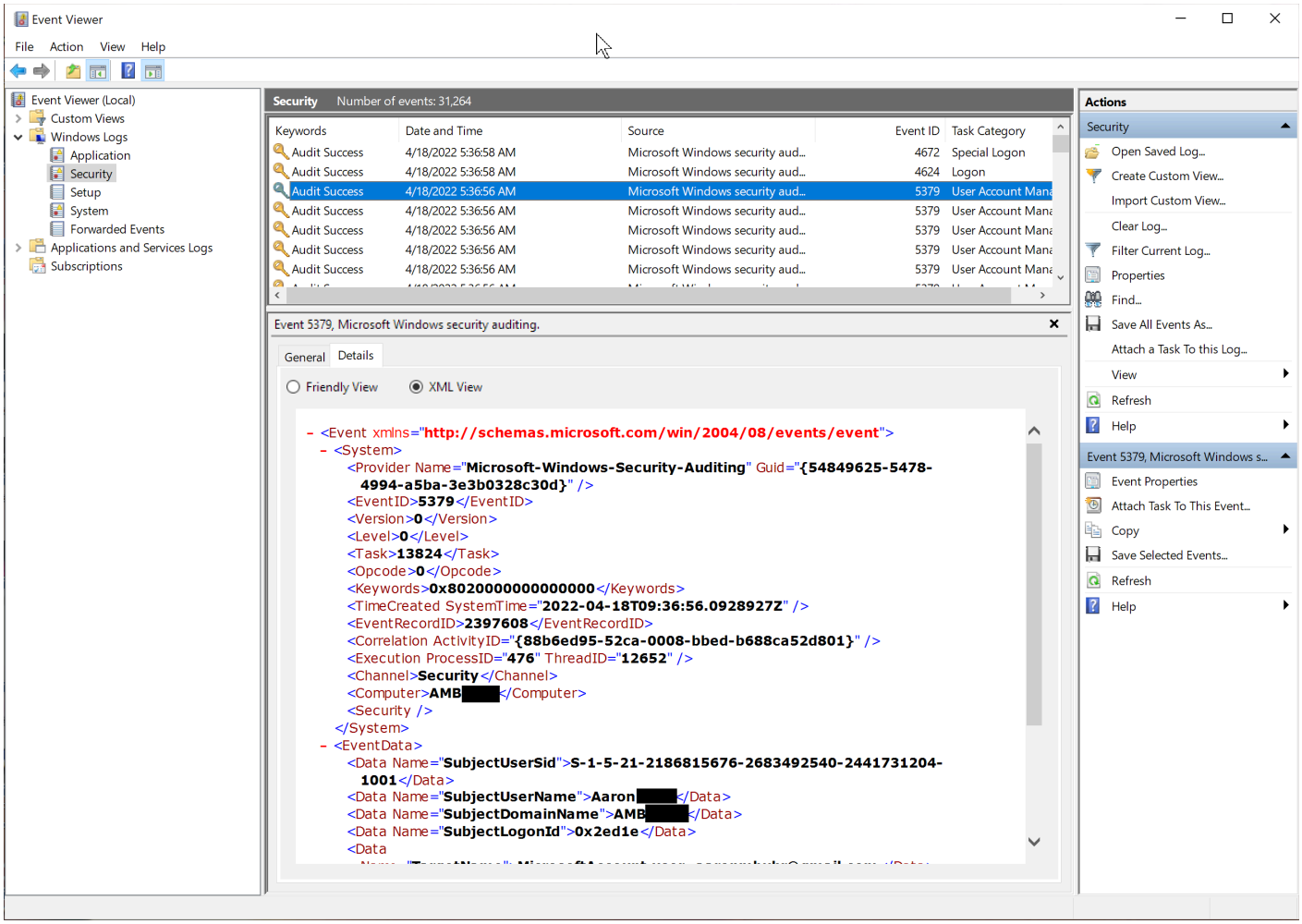
© LogZilla Corporation · logzilla.ai

Log Examples

Windows Event Viewer




Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions
Security Number of events: 31,264
Keywords Date and Time Source Event ID Task Category
Audit Success 4/18/2022 5:36:58 AM Microsoft Windows security aud... 4672 Special Logon
Audit Success 4/18/2022 5:36:58 AM Microsoft Windows security aud... 4624 Logon
Audit Success 4/18/2022 5:36:56 AM Microsoft Windows security aud... 5379 User Account Mana
Audit Success 4/18/2022 5:36:56 AM Microsoft Windows security aud... 5379 User Account Mana
Audit Success 4/18/2022 5:36:56 AM Microsoft Windows security aud... 5379 User Account Mana
Audit Success 4/18/2022 5:36:56 AM Microsoft Windows security aud... 5379 User Account Mana
Audit Success 4/18/2022 5:36:56 AM Microsoft Windows security aud... 5379 User Account Mana
Event 5379, Microsoft Windows security auditing.
General Details
Friendly View XML View
+ System
- EventData
SubjectUserSid S-1-5-21-2186815676-2683492540-2441731204-1001
SubjectUserName Aaron
SubjectDomainName AMB
SubjectLogonId 0x2ed1e
TargetName MicrosoftAccount:user=aaron@gmail.com
Type 0
CountOfCredentialsReturned 1
ReadOperation %%8100
ReturnCode 0
ProcessCreationTime 2022-04-18T09:36:55.3145259Z
ClientProcessId 18612
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 5379, Microsoft Windows s...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help



JSON Format (LogZilla Input)

The Windows Agent sends events via HTTP with metadata in `extra_fields`:

```
{
  "host": "WIN-SERVER01",
  "program": "Microsoft-Windows-Security-Auditing",
  "message": "EventID=\"4625\" EventLog=\"Security\" An account failed to log on",
  "extra_fields": {
    "_source_type": "WindowsAgent",
    "_log_type": "eventlog",
    "event_id": "4625",
    "event_log": "Security",
    "computer": "WIN-SERVER01",
    "event_user_name": "jsmith",
    "event_user_domain": "CORP",
    "SubjectUserSid": "S-1-5-21-1234567890-1234567890-1234567890-1001",
    "SubjectUserName": "WIN-SERVER01$",
    "SubjectDomainName": "CORP",
    "TargetUserName": "jsmith",
    "TargetDomainName": "CORP",
```

```
    "WorkstationName": "WORKSTATION01",
    "IpAddress": "192.168.1.100",
    "ProcessName": "C:\\Windows\\System32\\svchost.exe"
  }
}
```

Standard fields (`host`, `program`, `message`) are at the top level. Event-specific fields are in `extra_fields` and vary by Event ID.

Triggers

Trigger Name	Condition	Action
Windows: Suspicious Process Execution	4688 with suspicious indicator	Alert
Windows: MITRE ATT&CK Activity	Any event with MitreId	Alert
Windows: Failed Login Attempt	Event ID 4625	Alert
Windows: Account Locked Out	Event ID 4740	Alert
Windows: Audit Log Cleared	Event ID 1102	Alert
Windows: Account Created	Event ID 4720	Alert
Windows: Account Deleted	Event ID 4726	Alert
Windows: Security Group Changed	Event ID 4728, 4732, 4756	Alert
Windows: Special Privileges Assigned	Event ID 4672	Alert
Windows: New Service Installed	Event ID 7045	Alert
Windows: Unexpected Shutdown	Event ID 6008	Alert

© LogZilla Corporation · logzilla.ai