LOGZILLA DOCUMENTATION

Cisco

LogZilla App Store application: Cisco

LogZilla App Store · Generated May 3, 2026 · logzilla.ai/docs/logzilla-appstore/cisco

Overview

Cisco IOS (Internetwork Operating System) is the operating system used on most Cisco routers and switches. IOS devices generate syslog messages for routing protocol events, interface state changes, configuration modifications, hardware alerts, and security violations. The base Cisco parser handles all IOS-based products including routers, switches, and wireless controllers.

App Function

- Parse Cisco IOS syslog messages and extract the `cisco_mnemonic` field
- Remove embedded timestamps to enable proper event deduplication
- Extract network metadata (IP addresses, interfaces, VLANs, users)
- Categorize events by Event Class for cross-vendor analysis
- Provide triggers for high-impact network and system events

Vendor Documentation

- Cisco IOS and NX-OS Software (https://www.cisco.com/c/en/us/support/ios-nx-os-software/index.html)

Device Configuration

Configure the Cisco device to send syslog messages to LogZilla:

Access the device CLI via SSH or console

Enter configuration mode:

```
configure terminal
```

Configure the syslog destination:

```
logging host <logzilla-ip>
logging trap informational
service timestamps log datetime msec
```

Save the configuration:

```
write memory
```

Verification

Generate a configuration change or wait for a routing event, then verify events appear in LogZilla by selecting the User Tags menu for `Vendor` -> `Cisco`.

Incoming Log Format

Cisco IOS syslog messages follow this format:

```
<timestamp>: %<facility>-<severity>-<mnemonic>: <message>
```

- **timestamp** - Date and time of the event
- **facility** - Cisco subsystem generating the message (e.g., LINK, BGP, OSPF)
- **severity** - Numeric severity level (0-7)
- **mnemonic** - Event identifier (e.g., UPDOWN, ADJCHANGE)
- **message** - Event description with variable data

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Cisco`	Vendor identifier
`Event Class`	`network`	Cross-vendor event classification
`SrcIP`	`192.168.1.1`	Source IP address from ACL and login events
`DstIP`	`10.0.0.1`	Destination IP address from ACL events
`Interface`	`GigabitEthernet0/1`	Network interface name
`Neighbor IP`	`10.0.0.254`	Routing protocol neighbor IP address
`VLAN`	`100`	VLAN ID from switching events
`User`	`admin`	Username from configuration and login events

Log Examples

BGP Neighbor Down

```
%BGP-5-ADJCHANGE: neighbor 10.0.0.1 Down BGP Notification sent
```

Interface State Change

```
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
```

Configuration Change

```
%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:interface vlan 100
```

OSPF Adjacency

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.2 on Vlan100 from FULL to DOWN
```

Port Security Violation

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation on port Gi0/1
```

Triggers

Routing Protocols

Trigger	Description
Cisco: BGP Session Change	BGP neighbor state change or notification
Cisco: OSPF Adjacency Change	OSPF neighbor state change
Cisco: EIGRP Neighbor Change	EIGRP neighbor up/down or stuck-in-active

Trigger	Description
Cisco: IS-IS Adjacency Change	IS-IS adjacency state change

High Availability

Trigger	Description
Cisco: HSRP State Change	HSRP state transition
Cisco: VRRP State Change	VRRP state transition
Cisco: Redundancy/SSO Event	SSO switchover or standby lost
Cisco: Stack Member Change	Stack member added, removed, or election

Interface/Link

Trigger	Description
Cisco: Interface State Change	Interface or line protocol up/down
Cisco: Port Channel Issue	Port channel bundle failure or LACP issue
Cisco: Error Disabled Port	Port error-disabled or recovered
Cisco: Duplex Mismatch	CDP detected duplex mismatch

Spanning Tree

Trigger	Description
Cisco: Spanning Tree Event	Topology change, root change, or BPDU guard

Security

Trigger	Description
Cisco: Port Security Violation	MAC address violation on secure port
Cisco: Authentication Failure	Login or 802.1X authentication failure
Cisco: DHCP Snooping Violation	Untrusted DHCP packet detected
Cisco: Dynamic ARP Inspection Violation	Invalid ARP packet detected

VPN/Crypto

Trigger	Description
Cisco: IPSec/IKE Failure	IPSec or IKE negotiation failure

Hardware

Trigger	Description
Cisco: Power Supply Issue	Power supply failure or RPS event
Cisco: Fan/Temperature Alert	Fan failure or temperature threshold
Cisco: Memory/CPU Issue	Memory allocation failure or CPU threshold
Cisco: Transceiver Issue	Unsupported or failing transceiver
Cisco: Linecard/Module Failure	Linecard crash or failure

System

Trigger	Description
Cisco: System Reload	System reload or restart
Cisco: Configuration Change	Configuration modification detected

Trigger	Description
Cisco: PoE Event	PoE device connect/disconnect
Cisco: Object Tracking State Change	Tracked object state transition
Cisco: SNMP Queue Full	SNMP input queue overflow