LOGZILLA DOCUMENTATION

Cisco ISE

Rules, dashboards, and triggers for Cisco Identity Services Engine

LogZilla App Store · Generated June 11, 2026 · logzilla.ai/docs/logzilla-appstore/cisco—ise

Overview

Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to organizational routers and switches. ISE simplifies identity management across diverse devices and applications.

App Function

Step translation improves log readability. Cisco ISE log messages contain authentication and authorization events composed of multiple processing steps. These steps are represented as numeric `Step=` fields with associated `StepData=` values in the original logs.

Numeric step references are transformed into human-readable step names with associated data. The numeric `Step=` and `StepData=` fields are removed from the message text and replaced with an ordered sequence of descriptive step names with their corresponding data, making the logs substantially more readable and comprehensible.

Vendor Documentation

- Cisco Identity Services Engine (https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html)
- Logging (Cisco Identity Services Engine) (https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_logging.html)
- Introduction to Cisco ISE Syslogs (https://www.cisco.com/c/en/us/td/docs/security/ise/syslog/Cisco_ISE_Syslogs/m_IntrotoSyslogs.html)

Device Configuration

To send logs to LogZilla, configure the Cisco ISE:

Log in to the Cisco ISE admin console
Navigate to **Administration** > **System** > **Logging** > **Remote Logging Targets**
Add a new remote logging target with the LogZilla server IP
Configure the log categories to send
Save the configuration
Refer to the Cisco ISE documentation for detailed configuration options.

Incoming Log Format

Cisco ISE logs use syslog format with fixed header fields (date-timestamp, numeric IDs, and event summaries) followed by extensive key/value pairs. Each key and value is separated by =, and pairs are separated by commas and spaces.

Parsed Metadata Fields

Global Tags

Tag	Example	Description
Vendor	Cisco	Vendor identifier for cross-vendor filtering
Product	ISE	Product identifier
Event Class	auth	Cross-vendor event classification

Standardized Tags

Tag	Example	Description
DstIP	10.42.7.63	Destination IP address (HC)
User	jsmith	Username from authentication request (HC)

Cisco ISE-Specific Tags

Tag	Example	Description
Cisco ISE Category	Failed Attempts	ISE event category
Cisco ISE Action	Admin Login	Specific action type
Cisco ISE Device IP	10.34.150.68	Network device IP address (HC)
Cisco ISE Device	switch-01	Network device name

Tag	Example	Description
Cisco ISE Failure Reason	24408 User authentication failed	Reason for failure (HC)
Cisco ISE Policy	Building_SJC14_WNBU	ISE policy set name (HC)
Cisco ISE Failed User	jdoe	Username with failed password attempt (HC)

Log Examples

Failed RADIUS Authentication

```
0001969854 1 0 2014-08-07 00:00:16.712 -07:00 0098649452 5434
NOTICE RADIUS: Endpoint conducted several failed authentications of the
same scenario, ConfigVersionId=133, Device IP Address=11.22.150.68,
Device Port=1645, DestinationIPAddress=11.22.7.63, DestinationPort=1812,
RadiusPacketType=AccessRequest, UserName=testuser, Protocol=Radius,
NetworkDeviceName=EXAMPLE, User-Name=anonymous, NAS-IP-Address=11.22.150.68,
NAS-Port=60000, Service-Type=Framed, Framed-MTU=1449,
State=37CPMSessionID=0a22964453e324d700000d64\\;42SessionID=jjj-kkkk-lll01/1\
95491152/2084868\\;, Called-Station-ID=3c-08-f6-59-0e-10:alpha_phone,
Calling-Station-ID=00-23-33-41-60-52, NAS-Port-Type=Wireless - IEEE 802.11,
NAS-Port-Id=Capwap7, EAP-Key-Name=, cisco-av-pair=service-type=Framed,
cisco-av-pair=audit-session-id=0a22964453e324d700000d64,
cisco-av-pair=method=dot1x, cisco-av-pair=cisco-wlan-ssid=alpha_phone,
Airespace-Wlan-Id=2, IsEndpointInRejectMode=false, AcsSessionID=jjj-kkkk-ll\
l01/195491152/2084868, AuthenticationIdentityStore=CiscoAD,
AuthenticationMethod=PAP_ASCII, SelectedAccessService=Default
Network Access, FailureReason=24408 User authentication against Active
Directory failed since user has entered the wrong password, Step=11001,
Step=11017, Step=15049, Step=15008, Step=15048, Step=15048, Step=15048,
Step=15048, Step=15048, Step=15004, Step=11507, Step=12300, Step=12625,
Step=11006, Step=11001, Step=11018, Step=12101, Step=12100, Step=12625,
Step=11006, Step=11001, Step=11018, Step=12102, Step=12800, Step=12175,
Step=12805, Step=12806, Step=12801, Step=12802, Step=12105, Step=11006,
Step=11001, Step=11018, Step=12104, Step=12804, Step=12816, Step=12132,
Step=12209, Step=12218, Step=12125, Step=11521, Step=12105, Step=11006,
Step=11001, Step=11018, Step=12104, Step=12220, Step=11522, Step=11806,
Step=12105, Step=11006, Step=11001, Step=11018, Step=12104, Step=12607,
Step=12606, Step=12611, Step=15041, Step=15006, Step=22072, Step=15013,
Step=12606, Step=12105, Step=11006, Step=11001, Step=11018, Step=12104,
Step=12610, Step=15041, Step=15004, Step=15006, Step=22072, Step=15013,
Step=24430, Step=24325, Step=24313, Step=24319, Step=24367, Step=24367,
Step=24367, Step=24367, Step=24367, Step=24367, Step=24367, Step=24367,
Step=24367, Step=24323, Step=24344, Step=24408, Step=22057, Step=22061,
```

```
Step=12610, Step=12105, Step=11006, Step=11001, Step=11018, Step=12104,
Step=12610, Step=12853, Step=11520, Step=12117, Step=22028, Step=12965,
Step=12105, Step=11006, Step=11001, Step=11018, Step=12104, Step=11504,
Step=11003, Step=5434, SelectedAuthenticationIdentityStores=CiscoAD,
SelectedAuthenticationIdentityStores=Internal Endpoints,
SelectedAuthenticationIdentityStores=Internal Users,
SelectedAuthenticationIdentityStores=Guest Users,
NetworkDeviceGroups=Location#All Locations#SJC#WNBU,
NetworkDeviceGroups=Device Type#All Device Types#Wireless#WLC#NGWC,
EapTunnel=EAP-FAST, EapAuthentication=EAP-GTC,
CPMSessionID=0a22964453e324d700000d64, EndPointMACAddress=00-23-33-41-60-52,
EapChainingResult=No chaining, ISEPolicySetName=Building_SJC14_WNBU,
AllowedProtocolMatchedRule=WNBU_SJC14_Wireless_Dot1x,
IdentitySelectionMatchedRule=Default, TotalFailedAttempts=12987,
TotalFailedTime=310509, AD-Domain=cisco.com,
AD-User-Candidate-Identities=testuser@cisco.com, StepData=4= DEVICE.Location,
StepData=5= Radius.Called-Station-ID, StepData=6= Radius.Service-Type,
StepData=7= Radius.NAS-Port-Type, StepData=8= Radius.NAS-IP-Address,
StepData=9=WNBU_SJC14_Wireless_Dot1x, StepData=59=EAP_TLS_BYOD,
StepData=60=CiscoAD, StepData=69=Default, StepData=71=EAP_TLS_BYOD,
StepData=72=CiscoAD, StepData=73=CiscoAD, StepData=74=testuser,
StepData=75=cisco.com, StepData=76=cisco.com,
StepData=77=icm.cisco.com\\,Domain trust direction is one-way,
StepData=78=sea-alpha.cisco.com\\,Domain trust direction is one-way,
StepData=79=partnet.cisco.com\\,Domain trust direction is one-way,
StepData=80=IL.TEST.COM\\,Domain trust direction is one-way,
StepData=81=UK.TEST.COM\\,Domain trust direction is one-way,
StepData=82=SN.local\\,Domain trust direction is one-way,
StepData=83=webex.local\\,Domain trust direction is one-way,
StepData=84=in.test.com\\,Domain trust direction is one-way,
StepData=85=US.TEST.COM\\,Domain trust direction is one-way,
StepData=87=STATUS_WRONG_PASSWORD\\,ERROR_INVALID_PASSWORD\\,testuser@cisco.com,
StepData=88=CiscoAD, Location=Location#All Locations#SJC#WNBU, Device
Type=Device Type#All Device Types#Wireless#WLC#NGWC,
Response={RadiusPacketType=AccessReject; },
```

Triggers

Trigger	Description
`Cisco ISE: Authentication Failed`	Failed authentication attempts (potential brute force)
`Cisco ISE: Admin Login`	Administrative login events (audit trail)
`Cisco ISE: Device Registration`	New devices joining the network
`Cisco ISE: Alarm`	ISE system alerts and alarms