Introduction to Cisco ISE Syslogs

Cisco ISE Message Catalog

Cisco Identity Services Engine (ISE) provides a logging mechanism that is used for auditing, fault management, and troubleshooting. The logging mechanism helps you to identify fault conditions in deployed services and troubleshoot issues efficiently. It also produces logging output from the monitoring and troubleshooting primary node in a consistent fashion.

In Cisco ISE, system logs (syslogs) are collected at locations called logging targets. Targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can use the FTP facility to transfer them to an external server.

You can use the Message Catalog page of the Cisco ISE dashboard to view all possible log messages and the descriptions. Choose **Administration** > **System** > **Logging** > **Message Catalog**.

The Log Message Catalog page appears, from which you can view all possible log messages that can appear in your log files. The data available in this page are for display only. If you are using Cisco ISE 2.3 and greater releases, choose **Export** to export all the syslog messages in the form of a CSV file .

For more information on the Cisco ISE logging mechanism, configuring syslog purge, configuring remote syslog collection locations, and other tasks, see the Chapter Maintain and Monitor in the *Cisco ISE Administrator Guide* for your release.

Local Store Syslog Message Format

Cisco ISE log messages are sent to the local store with this syslog message format:

timestamp sequence_num msg_ode msg_sev msg_class msg_text attr =value

Field	Description
timestamp	Date of the message generation, according to the local clock of the originating the Cisco ISE node, in the following format : *YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm*. Possible values are: • YYYY = Numeric representation of the year. • MM = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number. • DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number. • hh = The hour of the day—00 to 23. • mm = The minute of the hour—00 to 59. • ss = The second of the minute—00 to 59. • xxx = The millisecond of the second—000 to 999. • +/-zh:zm = The time zone offset from the Cisco ISE server's time zone, where zh is the number of offset hours and zm is the number of minutes of the offset hour, all of which is preceded by a minus or plus sign to indicate the direction of the offset. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
sequence_num	Global counter of each message. If one message is sent to the local store and the next to the syslog server target, the counter increments by 2. Possible values are 0000000001 to 999999999.
msg_ode	Message code as defined in the logging categories.
msg_sev	Message severity level of a log message. See **Administration** > **System** > **Logging** > **Logging Categories**.
msg_class	Message class, which identifies groups of messages with the same context.
msg_text	English language descriptive text message.
attr=value	Set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair. Attribute names are as defined in the Cisco ISE dictionaries. Values of the Response direction AttributesSet are bundled to one attribute called Response and are enclosed in curly brackets {}. In addition, the attribute-value pairs within the Response are separated by semicolons. For example, Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00;}

Remote Syslog Message Format

Cisco ISE log messages are sent to the remote syslog server with this syslog message header format, which precedes the local store syslog message format:

pri_num Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

Field	Description
pri_num	Priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value* 8) + severity value. Refer the relevant Cisco ISE Administrator Guide for your release to set security levels for message codes. The facility code valid options are: • LOCAL0 (Code = 16) • LOCAL1 (Code = 17) • LOCAL2 (Code = 18) • LOCAL3 (Code = 19) • LOCAL4 (Code = 20) • LOCAL5 (Code = 21) • LOCAL6 (Code = 22; default) • LOCAL7 (Code = 23)
time	Date of the message generation, according to the local clock of the originating Cisco ISE server, in the format Mmm DD hh:mm:ss. Possible values are: • Mmm = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number. • hh = The hour of the day—00 to 23. • mm = The minute of the hour—00 to 59. • ss = The second of the minute—00 to 59. Some devices send messages that specify a time zone in the format -/+hhmm, where - and + identifies the directional offset from the Cisco ISE server's time zone, hh is the number of offset hours, and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
xx:xx:xx:xx/host_name	IP address of the originating Cisco ISE node, or the hostname.

Field	Description
cat_name	Logging category name preceded by the CISExxx string.
msg_id	Unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.
total_seg	Total number of segments in a log message. Long messages are divided into more than one segment. **Note** The *total_seg* depends on the Maximum Length setting in the remote logging targets page. See *Remote Logging Target Settings*.
seg_num	Segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

The syslog message data or payload is the same as the Local Store Syslog Message Format. The remote syslog server targets are identified by the facility code names LOCAL0 to LOCAL7 (LOCAL6 is the default logging location.) Log messages that you assign to the remote syslog server are sent to the default location for Linux syslog (/var/log/messages), however; you can configure a different location on the server.