Logging Mechanism

Cisco ISE Logging Mechanism

Cisco 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.

You can configure a Cisco ISE node to collect the logs in the local systems using a virtual loopback address. To collect logs externally, you configure external syslog servers, which are called targets. Logs are classified into various predefined categories. You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

Note If the Monitoring node is configured as the syslog server for a network device, ensure that the logging source sends the correct network access server (NAS) IP address in the following format: *<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>*

Otherwise, this might impact functionalities that depend on the NAS IP address.

Configure Local Log Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.

Step 1 Choose **Administration** > **System** > **Logging** > **Local Log Settings**.

Step 2 In the **Local Log Storage Period** field, enter the maximum number of days to keep the log entries in the configuration source.

Step 3 Click **Delete Logs Now** to delete the existing log files at any time before the expiration of the storage period.

Step 4 Click **Save**.

Cisco ISE System Logs

In Cisco ISE, system logs 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. Cisco ISE has the following default targets, which are dynamically configured in the loopback addresses of the local system:

- LogCollector—Default syslog target for the Log Collector.
- ProfilerRadiusProbe—Default syslog target for the Profiler Radius Probe.

By default, AAA Diagnostics subcategories and System Diagnostics subcategories logging targets are disabled during a fresh Cisco ISE installation or an upgrade to reduce the disk space. You can configure logging targets manually for these subcategories but local logging for these subcategories are always enabled.

You can use the default logging targets that are configured locally at the end of the Cisco ISE installation or you can create external targets to store the logs.

Local Store Syslog Message Format

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.

Field	Description
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

You can use the web interface to configure logging category messages so that they are sent to remote syslog server targets. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP.

A message is generated when an event occurs. An event may be one that displays a status, such as a message displayed when exiting a program, or an alarm. There are different types of event messages generated from different facilities such as the kernel, mail, user level, and so on. An event message is associated with a severity level, which allows an administrator to filter the messages and prioritize it. Numerical codes are assigned to the facility and the severity level. A Syslog server is an event message collector and collects event messages from these facilities. The administrator can select the event message collector to which messages will be forwarded based upon their severity level. Refer to the Logging Category Settings section for the severity levels in 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 YYYY 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. See Set Severity Levels for Message Codes for security levels. 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)

Field	Description
time	Date of the message generation, according to the local clock of the originating Cisco ISE server, in the format YYYY Mmm DD hh:mm:ss. Possible values are: • YYYY = Numeric representation of the year. • 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 device 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.
cat_name	Logging category name preceded by the CSCOxxx string.

Field	Description
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.

Configure Remote Syslog Collection Locations

You can create external locations to store the syslogs.

The UDP SysLog (Log Collector) is the default remote logging target. When you disable this logging target, it no longer functions as a log collector and is removed from the Logging Categories page. When you enable this logging target, it becomes a log collector in the Logging Categories page.

Step 1 Choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Step 2 Click **Add**.

Step 3 Configure the field as necessary.

Step 4 Click **Save**.

Step 5 Go to the Remote Logging Targets page and verify the creation of the new target.
After you have created the syslog storage location on logging target page, you should map the storage location to the required logging categories, to receive the logs.

Cisco ISE Message Codes

A logging category is a bundle of message codes that describe a function, a flow, or a use case. In Cisco ISE, each log is associated with a message code that is bundled with the logging categories according to the log message content. Logging categories help describe the content of the messages that they contain.

Logging categories promote logging configuration. Each category has a name, target, and severity level that you can set, as per your application requirement.

Cisco ISE provides predefined logging categories for services, such as Posture, Profiler, Guest, AAA (authentication, authorization, and accounting), and so on, to which you can assign log targets.

Set Severity Levels for Message Codes

You can set the log severity level and choose logging targets where the logs of selected categories will be stored.

Step 1 Choose **Administration** > **System** > **Logging** > **Logging Categories**.

Step 2 Click the radio button next to the category that you want to edit, and click **Edit**.

Step 3 Modify the required field values.

Step 4 Click **Save**.

Step 5 Go to the Logging Categories page and verify the configuration changes that were made to the specific category.

Cisco ISE Message Catalogs

You can use the Message Catalog page 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.

Debug Logs

Debug logs capture bootstrap, application configuration, runtime, deployment, monitoring, reporting, and public key infrastructure (PKI) information. Critical and warning alarms for the past 30 days and info alarms for the past 7 days are included in the debug logs.

You can configure the debug log severity level for individual components.

You can store the debug logs in the local server.

Note Debug log configuration is not saved when a system is restored from a backup or upgraded.

Configure Debug Log Severity Level

You can configure the severity levels for the debug logs.

Step 1 Choose **Administration** > **System** > **Logging** > **Debug Log Configuration**.

Step 2 Select the node, and then click **Edit.**
The Debug Log Configuration page displays a list of components based on the services that are running in the selected node and the current log level that is set for the individual components.

Step 3 Select the component for which you want to configure the log severity level, and then click **Edit**. Choose the desired log severity level from the **Log Level** drop-down list, and click **Save.**

Note Changing the log severity level of runtime-AAA component changes the log level of its subcomponent prrt-JNI as well. A change in subcomponent log level does not affect its parent component.

Endpoint Debug Log Collector

To troubleshoot issues with a specific endpoint, you can download debug logs for that particular endpoint based on its IP address or MAC address. The logs from the various nodes in your deployment specific to that particular endpoint get collected in a single file thus helping you troubleshoot your issue quickly and efficiently. You can run this troubleshooting tool only for one endpoint at a time. The log files are listed in the GUI. You can download the logs for an endpoint from a single node or from all the nodes in your deployment.

Download Debug Logs for a Specific Endpoint

To troubleshoot issues related to a specific endpoint in your network, you can use the Debug Endpoint tool from the Admin portal. Alternatively, you can run this tool from the Authentications page. Right-click the Endpoint ID from the Authentications page and click **Endpoint Debug**. This tool provides all debug information for all services related to the specific endpoint in a single file.

Before You Begin

You need the IP address or MAC address of the endpoint whose debug logs you want to collect.

Step 1 Choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Endpoint Debug**.

Step 2 Click the **MAC Address** or **IP** radio button and enter the MAC or IP address of the endpoint.

Step 3 Check the **Automatic disable after *n* Minutes** check box if you want to stop log collection after a specified amount of time. If you check this check box, you must enter a time between 1 and 60 minutes.
The following message appears: "Endpoint Debug degrades the deployment performance. Would you like to continue?"

Step 4 Click **Continue** to collect the logs.

Step 5 Click **Stop** when you want to manually stop the log collection.

Collection Filters

You can configure the Collection Filters to suppress the syslog messages being sent to the monitoring and external servers. The suppression can be performed at the Policy Services Node levels based on different attribute types. You can define multiple filters with specific attribute type and a corresponding value.

Before sending the syslog messages to monitoring node or external server, Cisco ISE compares these values with fields in syslog messages to be sent. If any match is found, then the corresponding message is not sent.

Configure Collection Filters

You can configure multiple collection filters based on various attribute types. It is recommended to limit the number of filters to 20. You can add, edit, or delete a collection filter.

Step 1 Choose **Administration** > **System** > **Logging** > **Collection Filters**.

Step 2 Click **Add.**

Step 3 Choose the **Filter Type** from the following list:

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

Step 4 Enter the corresponding **Value** for the filter type you have selected.

Step 5 Choose the **Result** from the drop-down list. The result can be All, Passed, or Failed.

Step 6 Click **Submit.**

Event Suppression Bypass Filter

Cisco ISE allows you to set filters to suppress some syslog messages from being sent to the Monitoring node and other external servers using the Collection Filters. At times, you need access to these suppressed log messages. Cisco ISE now provides you an option to bypass the event suppression based on a particular attribute such as username for a configurable amount of time. The default is 50 minutes, but you can configure the duration from 5 minutes to 480 minutes (8 hours). After you configure the event suppression bypass, it takes effect immediately. If the duration that you have set elapses, then the bypass suppression filter expires.

You can configure a suppression bypass filter from the Collection Filters page in the Cisco ISE user interface. Using this feature, you can now view all the logs for a particular identity (user) and troubleshoot issues for that identity in real time.

You can enable or disable a filter. If the duration that you have configured in a bypass event filter elapses, the filter is disabled automatically until you enable it again.

Cisco ISE captures these configuration changes in the Change Configuration Audit Report. This report provides information on who configured an event suppression or a bypass suppression and the duration of time for which the event was suppressed or the suppression bypassed.