CHAPTER 13

Logging

This chapter describes the logging mechanism implemented in the Cisco Identity Services Engine (ISE), including steps to configure logging targets, edit logging categories, and configuring logging settings. The following topics are covered:

Understanding Logging

The Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting of the services provided by Cisco ISE. 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 your 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, called targets. Logs are classified into various predefined categories, which are discussed in Understanding Logging Categories. You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

In the ISE administration interface, navigate to **Administration > System > Logging** to perform the following logging related tasks:

- To configure local log settings, see Configuring Local Log Settings, page 13-2
- To understand and create remote logging targets, see Understanding Remote Logging Targets, page 13-2
- To understand and edit logging categories, see Understanding Logging Categories, page 13-5
- To view message catalog, see Viewing Message Catalog, page 13-8
- To understand and configure debug logs, see Understanding Debug Log Configuration, page 13-8
- To view log collection status, see Viewing Log Collection Status, page 13-10

Configuring Local Log Settings

Use this process to set the local log storage period and to delete the local logs.

To configure the logging settings, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Local Log Settings**.

Step 2 Configure the following fields:

a. Local Log Storage Period—The maximum number of days to keep the log entries in the configuration source.

Note To avoid wasting disk space, logs can be deleted during the specified local log storage period. Click the **Delete Logs Now** button to delete the existing log files at any time before the expiration of the storage period.

Step 3 Click **Save**.

Understanding Remote Logging Targets

Logging targets are locations where the system logs are collected. In Cisco ISE, targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can FTP 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.

Configuring Remote Logging Targets

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

This section contains the following topics:

Viewing Remote Logging Targets

You can view the predefined and user-defined remote logging targets. You can also search for a particular target using the filter.

To view remote logging targets, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Remote Logging Targets page appears with a list of existing logging targets.

Step 2 Click Filter and choose one of the following options:

- Quick Filter
- Advanced Filter

To perform a quick filter, enter search criteria in one or more of the following attribute fields:

- Name
- IP Address
- Type
- Description

To perform an Advance filter, create a matching rule by performing the following:

- In the Filter drop-down list, select one of the following options:
  - Name
  - IP Address
  - Type
  - Description
- In the second drop-down list, select one of the following options:
  - Contains
  - Does not contain
  - Does not equal
  - Ends with
  - Is empty
  - Is exactly (or equals)
  - Is not empty
  - Starts with
- In the text box, enter your desired search value.
- Click Go to launch the filter process, or click plus (+) to add additional search criteria.
- Click Clear Filter to reset the filter process.

The desired remote logging targets are displayed.

Creating Remote Logging Targets

To create an external logging target, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Remote Logging Targets page appears.

Click **Add**.

Step 2 The Log Collector page appears.

Step 3 Configure the following fields:

a. Name—Enter the name of the new target.

b. Target Type—By default it is set to Syslog. The value of this field cannot be changed.

c. Description— Enter a brief description of the new target.

d. IP Address—Enter the IP address of the destination machine where you want to store the logs.

e. Port—Enter the port number of the destination machine.

f. Facility Code—Choose the syslog facility code to be used for logging. Valid options are Local0 through Local7.

g. Maximum Length— Enter the maximum length of the remote log target messages. Valid options are from 200 to 1024 bytes.

Step 4 Click **Save**.

Step 5 Go to the Logging Targets page and verify the creation of the new target.

Editing Remote Logging Targets

To edit a remote logging target, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Remote Logging Target page appears.

Click the radio button next to the logging target name that you want to edit and click **Edit**.

The Log Collector page appears.

Step 2 Modify the following field values as necessary:

- Name
- Target Type
- Description
- IP Address
- Port
- Facility Code
- Maximum Length

Step 3 Click **Save**.

The updating of the selected Log Collector is completed.

Deleting Remote Logging Targets

To edit a remote logging target, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Log Collector page appears.

Step 2 Click the radio button next to the logging target that you want to delete and click **Delete**.

Step 3 Click **OK** in the confirmation dialog box to confirm that you want to delete the logging target.

Understanding Logging Categories

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.

Table 13-1 lists the Cisco ISE predefined categories that are available in Cisco ISE by default:

Table 13-1 Logging Categories

Parent Category	Category
AAA Audit	• AAA Audit • Failed Attempts • Passed Authentication
AAA Diagnostics	• AAA Diagnostics • Administrator Authentication and Authorization • Authentication Flow Diagnostics • Identity Store Diagnostics • Policy Diagnostics • Radius Diagnostics • Guest
Accounting	• Accounting • Radius Accounting
Administrative and Operational Audit	• Administrative and Operational Audit

Table 13-1 Logging Categories (continued)

Parent Category	Category
Posture and Client Provisioning Audit	• Posture and Client Provisioning Audit
Posture and Client Provisioning Diagnostics	• Posture and Client Provisioning Diagnostics
Profiler	• Profiler
System Diagnostics	• System Diagnostics • Distributed Management • Internal Operations Diagnostics
System Statistics	• System Statistics

See Available Reports, page 23-41 for more information on the relevant troubleshooting reports per category.

This section contains the following topics:

- Searching Logging Categories, page 13-6
- Editing Logging Categories, page 13-7

Searching Logging Categories

You can use Filter to search for a particular category.

To search a category, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Logging Categories**.

The Logging Categories page appears with a list of existing categories.

Step 2 Click Filter and choose one of the following options:

- Quick Filter
- Advanced Filter

To perform a quick filter, enter search criteria in one or more of the following attribute fields:

- Parent Category
- Category
- Targets
- Severity
- Local Log Level

To perform an Advance filter, create a matching rule by performing the following:

- In the Filter drop-down list, select one of the following options:
  - Parent Category
  - Category
  - Targets

  - Severity
  - Local Log Level
- In the second drop-down list, select one of the following options:
  - Contains
  - Does not contain
  - Does not equal
  - Ends with
  - Is empty
  - Is exactly (or equals)
  - Is not empty
  - Starts with
- In the text box, enter your desired search value.
- Click Go to launch the filter process, or click plus (+) to add additional search criteria.
- Click Clear Filter to reset the filter process.

The desired remote logging categories are displayed.

Editing Logging Categories

This section shows you how to set the log severity level and choose logging targets where the logs of selected categories will be stored.

To edit the configuration of a specific logging category, complete the following steps:

Step 1 From the Cisco ISE Administration Interface, choose **Administration > System > Logging > Logging Categories**.

The Logging Categories page appears with a list of existing categories.

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

The edit page appears, showing the details of the selected category.

Step 3 Modify the following field values:

Note The Name field cannot be changed.

a. Log Severity Level— For diagnostic logging categories, use the drop-down list box to select the severity level. Valid options are:
   - FATAL—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately.
   - ERROR—This option indicates a critical or error condition.
   - WARN—This option indicates a normal but significant condition. This is the default condition.
   - INFO—This option indicates an informational message.
   - DEBUG—This option indicates a diagnostic bug message.

b. Target—This section contains two boxes: Available and Selected. The Available box contains the existing logging targets, both local (predefined) and external (user-defined). The Selected box, which is initially empty, contains the selected targets for the specific category. You can change the targets for a category by transferring the targets between the Available and the Selected boxes using the left and right icons.

Step 4 Click **Save**.

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

Viewing Message Catalog

You can use the Message Catalog page to view all possible log messages.

To view the message catalog, complete the following steps:

Step 1 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.

Each message contains the following fields:

- Category Name—The logging category to which a message belongs
- Message Class—The group to which a message belongs
- Message Code—A unique message code identification number associated with a message
- Message Text—Name of the message
- Severity—The severity level associated with a message

Understanding Debug Log Configuration

Debug logs capture bootstrap, application configuration, runtime, deployment, monitoring and reporting, and public key infrastructure (PKI) information.

Use this process to configure the log severity level for individual components, and store the debug logs in the local server so that you can export to Cisco technical support for evaluation and troubleshooting.

Note The debug log configuration is not saved upon backup and restore operation and this configuration is not saved upon upgrade.

Configuring Debug Log Level

To configure debug logs via the Cisco ISE user interface, complete the following steps:

Step 1 Choose **Administration > System > Logging > Debug Log Configuration**. The Node List page appears, which contains a list of nodes and their personas.

Note You can use the Filter button to search for a specific node, particularly if the node list is large.

Step 2 Select the node and click **Edit**.

The Debug Level Configuration page appears, which contains a list of components that is based on the services that are running in the selected node and the current log level that is set for individual components.

Each node contains the following components:

- Active Directory
- CacheTracker
- NotificationTracker
- ReplicationTracker
- cisco-mnt
- client
- com-cisco-nm
- epm-pap
- epm-pap-api.services
- epm-pdp
- epm-pip
- guest
- guestadmin
- guestauth
- guestportal
- identity-store-AD
- mnt-alert
- mnt-collector
- org-apache
- org-apache-cxf
- org-apache-digester
- org-displaytag
- pep-auth-manager-test
- posture
- profiler

- provisioning
- prrt-JNI
- runtime-AAA
- runtime-config
- runtime-logging
- sponsorportal
- swiss

Note You can use the Filter button to search for a specific component from the list.

Step 3 Do one of the following to adjust the log severity level:

- Click on a component name, choose the desired log level from the combo box, and click **Save**.

  Valid options are:

  - FATAL—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately.
  - ERROR—This option indicates a critical or error condition.
  - WARN—This option indicates a normal but significant condition. This is the default condition.
  - INFO—This option indicates an informational message.
  - DEBUG—This option indicates a diagnostic bug message.

- Choose a component name for which you want to configure the debug log level, and click **Edit**. In this page, choose the desired log level from the Log Level combo box, 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.

The debug log configuration for the selected component is complete.

Related Topics

- Downloading Support Bundles, page 22-40
- Downloading Debug Logs, page 22-42

Viewing Log Collection Status

You can obtain reports on the log collection status for all Cisco ISE nodes. In the Cisco ISE administration interface, choose **Monitor > System > Reports > Log Collection Status**. The Log Collection status page appears, which contains the following information:

- ISE Server: Name of the Cisco ISE node in which logs are collected
- Last Syslog Message: Arrival time of the most recent syslog message
- Last Error: Name of the most recent error message

- Last Error Time: Arrival time of the most recent error message

See System Reports, page 23-10, for information on how to generate the report on log collection status.

Viewing Log Collection Details

You can view server log details such as last syslog message, log configuration changes made, server errors, and so on using the Log Collection Details page. In the Cisco ISE administration interface, choose **Monitor > System > Reports > Log Collection Status**. The Log Collection status page appears. Select a node to view the Log Collection Details page, which contains the following information pertaining to the selected node:

- Log Name: Name of the log category under which the logs are collected
- Last Syslog Message: Arrival time of the most recent syslog message
- Last Error: Name of the most recent error message
- Last Error Time: Arrival time of the most recent error message

See System Reports, page 23-10 for information on how to generate the report on log collection status.