



## System Log Management

---

In an open distributed system, there are generally multiple applications running on a number of machines of different types. Cisco Syslog Analysis streamlines the management of such systems by providing a common administrative interface for all log messages received from the applications.

The result is an orderly presentation of information which assists in the diagnosis and troubleshooting of system problems.

### The System Log Management Process

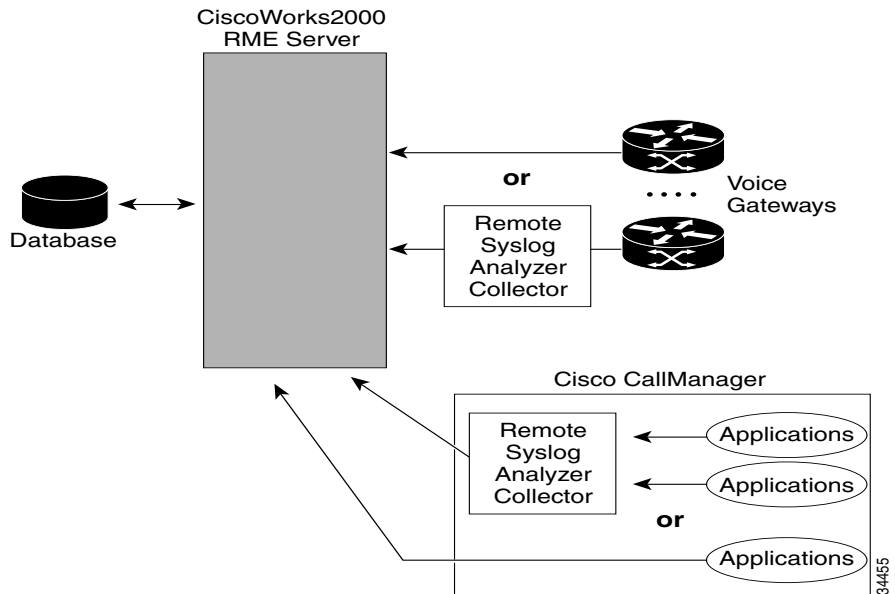
Although it can be adapted to other network management systems, Cisco syslog (system log) messages are best managed with Cisco Syslog Analysis, which is packaged with CiscoWorks2000 Resource Manager Essentials.

Cisco Syslog Analyzer is the component of Cisco Syslog Analysis that provides a common storage and analysis of the system log for multiple applications. The role of the other major component, Cisco Syslog Collector, is to gather log messages from Cisco CallManager servers.

These two Cisco applications work together to provide a centralized system logging service for Cisco IP Telephony Solutions.

A diagram of the system (Figure 8-1) shows how the Cisco Syslog Analyzer and Syslog Cisco Collector function within the syslog analysis process.

**Figure 8-1 Functional Components of the System Logging Service**



## CiscoWorks2000

Using CiscoWorks2000, you can easily configure and produce reports on the log messages collected from each Cisco CallManager device and other IP telephony devices.

CiscoWorks2000 provides a common system log for applications in the multi-host and multi-platform Cisco IP Telephony Solutions environment. In addition, with help from Simple Network Management Protocol (SNMP), CiscoWorks2000 can also provide additional information on each device from which the log messages originate.

Each time a device is added to the CiscoWorks2000 device inventory, a new database is created. Once the device is added to the list, CiscoWorks2000 gathers some device information via SNMP. You can easily read and use this information for system maintenance and problem-solving.

For information on setting up CiscoWorks2000, see the “Reporting and Analyzing Data with CiscoWorks2000” section on page 8-10.

## Cisco Syslog Collector

The function of Cisco Syslog Collector is to collect log messages from a Cisco CallManager server, or a cluster of servers, at any network installation (as shown in Figure 8-1). The service collects a wide range of significant event messages which reflect system status. It is configured on your web browser using the Cisco CallManager Administration application (see Figure 8-3).

After validating the events or error messages collected, Cisco Syslog Collector passes them to the Syslog Analyzer. When this process is complete, you can use Cisco Syslog Analyzer to analyze the log messages.

You can stop and start the Cisco Syslog Collector service from the Windows 2000 Service Control Manager.

## Cisco Syslog Analyzer

Cisco Syslog Analyzer, which resides on a CiscoWorks2000 server, receives the messages collected from multiple applications by the Cisco Syslog Collector.

When a collection of data is received, the Cisco Syslog Analyzer parses and stores the results in the CiscoWorks2000 database. This interface allows you to access and manage whatever data is collected from the system's managed devices.

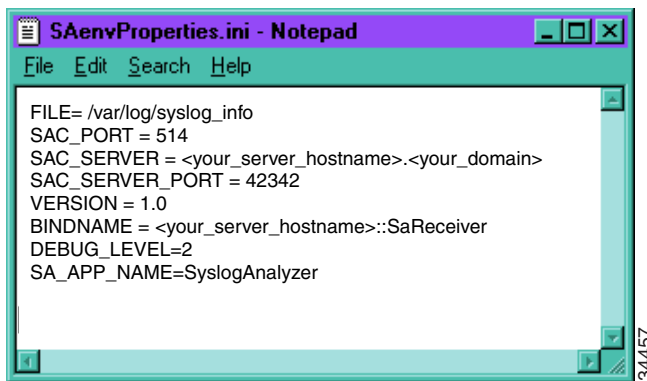
# Configuring Cisco CallManager Syslog Components

In order to work with the CiscoWorks2000 management system, you must provide a configuration file (see Figure 8-2) so the Cisco Syslog Collector can establish the location of your CiscoWorks2000 server. That server can then begin receiving messages from the Cisco Syslog Collector.

## Editing the Configuration File

Currently, you can change the CiscoWorks2000 server name only by editing the SAenvproperties.ini file manually, then restarting the Cisco Syslog Collector service.

**Figure 8-2** Sample Configuration File



If you enter the name of the CiscoWorks2000 server correctly during the installation process, the hostname will be set automatically in the SAenvproperties.ini configuration file. It will not be necessary to edit the file manually.

**Note**

Future releases will provide an administrative interface to enable a server name change. Refer to the *Release Notes for Cisco CallManager Release 3.0(1)* for details.

## Enabling the SNMP Agent

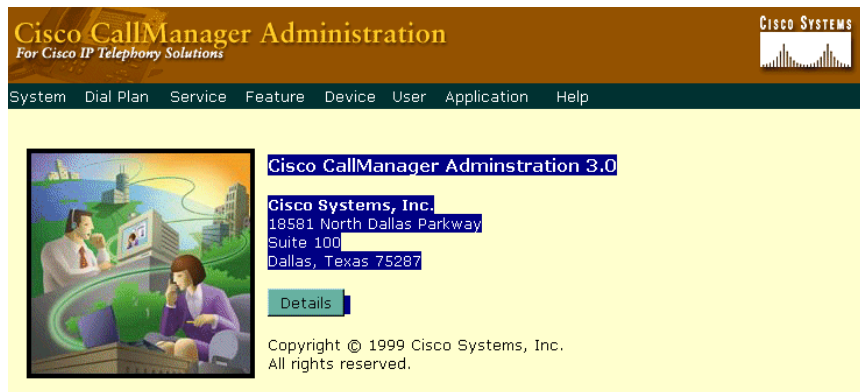
Because CiscoWorks2000 sends SNMP requests to query for device information, you must enable the Microsoft Windows 2000 SNMP service at the time that Cisco CallManager 3.0 is installed.

Device databases are added to the CiscoWorks device list each time a system is added, and SNMP requests are used to retrieve that information. See Chapter 9, “SNMP Instrumentation” for more information.

## Setting Up Trace Configuration

The web-based Cisco CallManager Administration interface defines configuration services, directs the syslog output, and initiates the logging activity.

**Figure 8-3** Cisco CallManager 3.0 Administration



- Step 1** To access the Cisco CallManager Administration interface, pull down the **Service > Trace** menu from the main Administration page (see Figure 8-3).
- Step 2** Use the Trace Configuration interface (see Figure 8-4) to set the trace properties.
  - a.** Turn on trace by checking the **Trace On** box.



**Note** Using the Trace Configuration interface, you can enable certain debug traces with particular masks, and the data generated will migrate to whatever component is enabled.

**Figure 8-4 Trace Configuration Interface**

### Trace Configuration

172.20.71.248

**Current Service: CallManager**  
**Current Server: 172.20.71.248**  
 Status: Ready

Configured Services: CallManager

Trace On

Mask:   Show Time

Level: ERROR  Show Date

User Mask:

0  1  2  3  4  5  6  7  
 8  9  10  11  12  13  14  15

Event: DEBUG

Components:

EventLog

Output Debug String

File Name:

# of Files:   
 # of Lines:   
 # of Minutes:

System Log

Debug Enabled

System Server:

34456

- b. Activate the output components by checking the boxes defining event logs, debug traces, or syslog output files.

**Caution**

---

In Cisco CallManager Release 3.0, you can use Cisco Syslog Collector to collect the debug trace from applications. However, enabling too many debug traces at the same time may impose too heavy a burden on the network and on the system—so define only a few specific tracing levels at any given time.

Enable the debug trace message option only when there is not much activity in the system. Use the local file output option of the debug trace at all other times.

---

- c. If a server other than the Cisco Syslog Analyzer is used, type in the name of the syslog server.
  - If the CiscoWorks2000 server name has been properly configured during the installation, the local collector file will start forwarding syslog messages to the CiscoWorks2000 server as soon as the system log component is enabled.
  - The single exception is the syslog component, which must have the “Debug Enabled” box checked. When this box is unchecked, the service sends only significant events (such as alarms and errors) to the syslog component.

**Note**

---

You must configure the Syslog server name only when a syslog daemon other than CiscoWorks2000 is used as the syslog server. If CiscoWorks2000 is being used, leave this box blank, and the syslog messages will be directed to a local syslog collector by default.

---

When the System Log component is enabled, Trace Configuration tells the configured services to automatically direct syslog messages to a local syslog collector process, which forwards them to a CiscoWorks2000 server, where you can view them.

# Administering Your System

When you use Cisco Syslog Analyzer, you will be able to examine the event log reports from each Cisco CallManager system. In addition to a cluster of Cisco CallManager systems, a network installation may also have some voice equipment, routers, gateways and other devices generating log messages. After you have set up your system, you can access all of this information through one server.

## Enabling Your Web Browser

You can access CiscoWorks2000 through any web browser, provided that your browser has Java and JavaScript enabled and is configured to accept cookies. You can see the configuration status displayed in the main window on the CiscoWorks2000 web page, as in Figure 8-5.

**Figure 8-5** CiscoWorks2000 Web Interface



## Using the CiscoWorks2000 Interface with Cisco CallManager

To examine syslog output sent from a particular device, you must open the CiscoWorks2000 web interface and point to the relevant managed device. (See the “Running Standard Reports” section on page 8-10 and Figure 8-6.) In addition to syslog reports, you can also view some system information on the managed devices that generate the syslog messages.

The CiscoWorks2000 server you designate gets device information by querying the SNMP agent on each device, including the Cisco CallManager system. The SNMP agent is enabled at the time you install Cisco CallManager.

## Defining Managed Devices

You must define managed devices on the CiscoWorks2000 device inventory list (e.g. Figure 8-6). Devices managed may include Cisco CallManager itself as well as other devices, such as routers, voice gateways, and firewalls. Define each device that will be managed on the target network (see CiscoWorks2000 online help under **Resource Management Essentials > Inventory**).

You must configure each managed device to send and report syslog messages to a CiscoWorks2000 server, which then generates reports for all of the devices on the network.

**Note**

---

Each managed device requires a different configuration, and because there are many different types of Cisco hardware that may be in use, there are many possible configurations.

---

**Note**

---

Cisco routers are routinely configured for system logging. Consult your Cisco documentation for information on router system logging.

---

## Reporting Managed Device Messages

You can access syslog messages from managed devices in the Standard Reports section (see the “Running Standard Reports” section on page 8-10).

Syslog messages received from unexpected device—those that have not been added in the Device Lists—are made available in a single table (see the “Running Reports on Unexpected Devices” section on page 8-13 and Figure 8-8).

## Reporting and Analyzing Data with CiscoWorks2000

The CiscoWorks2000 menu bar provides opportunities for you to get reports and set up analysis of your data. Currently, reports on both standard and unexpected devices can be run for Cisco IP Telephony devices.

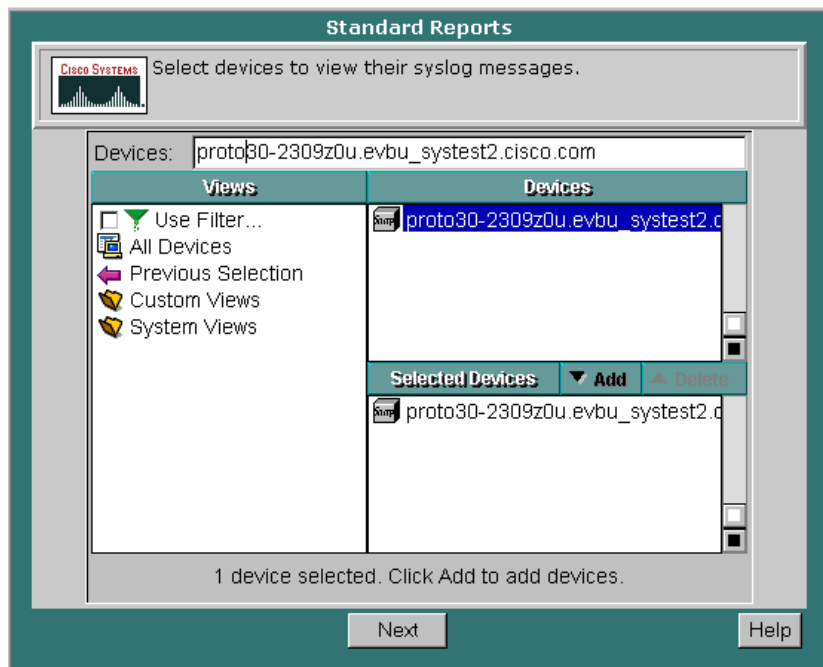
However, customized report formats and advanced analysis parameters for these devices will soon be available to extend the usability of your syslog data.

### Running Standard Reports

You can use the standard report forms included under the CiscoWorks2000 Syslog Analysis menu to retrieve data according to device, severity, date or type.

Selected information collected from the network devices being managed is gathered and displayed in the Standard Reports system log.

Figure 8-6 Standard Reports



Use the Standard Report interface to identify the devices for which event and trace data are needed. Figure 8-6 shows a selected device on the Standard Report form.

Next, select one of three types of report you want and the dates for which you want information (Figure 8-7). The resulting report will reflect these choices.

**Figure 8-7** *Select Dates and Report Type*

**Select Dates and Report Type**

**CISCO SYSTEMS** Select the report type and dates to include.

Report Type	Dates
<input type="radio"/> All Messages	<input checked="" type="checkbox"/> Today
<input checked="" type="radio"/> Messages by Severity Level	<input checked="" type="checkbox"/> All
<input type="radio"/> Messages by Alert Type	<input checked="" type="checkbox"/> Mar 9 (Thursday)
	<input checked="" type="checkbox"/> Mar 8 (Wednesday)
	<input checked="" type="checkbox"/> Mar 7 (Tuesday)
	<input checked="" type="checkbox"/> Mar 6 (Monday)
	<input checked="" type="checkbox"/> Mar 5 (Sunday)
	<input checked="" type="checkbox"/> Mar 4 (Saturday)

Back Next Help

34460

## Running Reports on Unexpected Devices

You can use the Unexpected Device Report form included under the CiscoWorks2000 Syslog Analysis menu to retrieve data on devices which have not been rolled into the CiscoWorks2000 device list.

Syslog messages are detectable even from unmanaged devices. The information collected is displayed in the Unexpected Device Report.

**Figure 8-8** Unexpected Device Report

**Select Dates**

**Cisco SYSTEMS** Select dates to include in the Unexpected Device Report.

**Dates**

- Today
- All
- Mar 9 (Thursday)
- Mar 8 (Wednesday)
- Mar 7 (Tuesday)
- Mar 6 (Monday)
- Mar 5 (Sunday)
- Mar 4 (Saturday)

Finish Help

34464

