Event Monitoring

VIII

Novell® ZENworks® 7 Linux Management includes a Message Logger component that tracks and logs significant system events. Administrators can use this information to monitor events related to devices, policies, and bundles. Specifically, event monitoring allows you to

- Monitor problems associated with devices, policies, and bundles
- Track successful events
- Log events and run reports
- View a summary of problems on a hot list

This section contains the following topics:

- Chapter 30, “Event Monitoring Overview,” on page 367
- Chapter 31, “Working with Event Logs,” on page 371
- Chapter 32, “Message Logger,” on page 377
- Chapter 33, “Configuring Message Logger Settings,” on page 379

Event Monitoring Overview

30

Event monitoring allows you to manage your environment by taking messages from the Message Logger and displaying them in various event logs, making it easy to track errors, problems, and successful events for your devices, policies, and bundles.

You can capture and store specific events related to devices, policies, and bundles that you or your organization's help desk can analyze and use to monitor problems without visiting the server or workstation, which can reduce problem resolution times and increase productivity. The captured information includes a description, time stamp, severity status, and message ID.

To keep your environment running at its maximum efficiency, you can use the event logs to stay abreast of critical errors and help you to troubleshoot and fine-tune your environment.

The following sections provide additional information:

- Section 30.1, "Event Monitoring Terminology," on page 367
- Section 30.2, "Monitoring Device Events," on page 367
- Section 30.3, "Monitoring Policy Events," on page 368
- Section 30.4, "Monitoring Bundle Events," on page 368
- Section 30.5, "Using the Hot List," on page 368

30.1 Event Monitoring Terminology

Event: Something that happens, such as a successful installation, that triggers a message to be created and sent.

Local Log: A list of the event messages generated by the ZENworks Agent that resides on the server or workstation.

System Log: A list of event messages displayed only for servers that are functioning as primary or secondary ZENworks Servers. The log lists the system event messages generated by the ZENworks Server for activities that it performs on behalf of all managed devices in its Management Zone.

Message: A detailed description of an event. A message explains an exception such as an error or warning, provides information to a user, or includes a debug statement used for debugging the module.

Community String: The protocol password for SNMP. Applications use community strings for access control. You can use the trap receiver console to define the set of community strings to accept the trap. The agent, in turn, accepts or rejects the operation. When none of the community string matches, the trap is discarded.

30.2 Monitoring Device Events

When you use Novell® ZENworks® Linux Management to remotely install applications, you need feedback on the success and failure of certain events so you can keep your systems working at an optimal level. With event monitoring, you can track things such as software installation on client

devices, whether or not a device has been refreshed, whether or not sessions were started, and so on. These messages are logged into a database and the information displayed in the event logs.

30.3 Monitoring Policy Events

Novell ZENworks Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. The Message Logger tracks problems with setting policies and displays them in the event logs. The resulting messages alert you to any problems that arise, such as failed connections and the inability to create schedules.

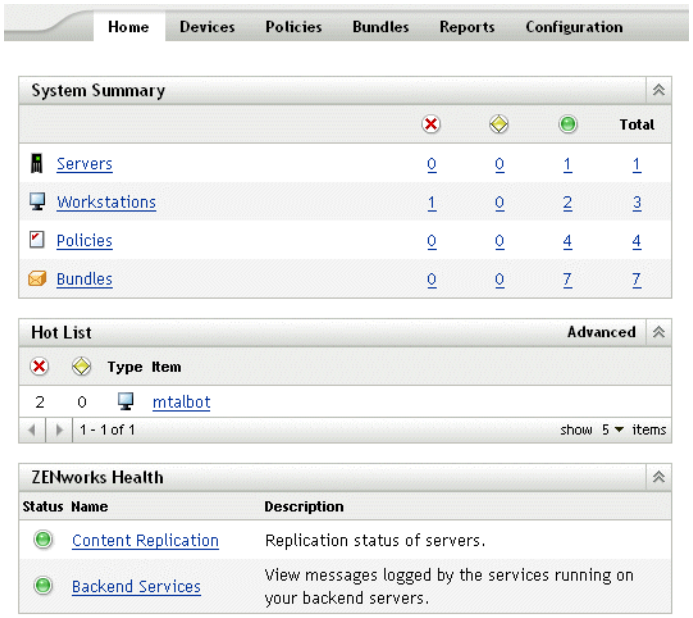
30.4 Monitoring Bundle Events

Novell ZENworks Linux Management enables you to create bundles and catalogs to distribute RPM packages to managed devices. In the process of pushing the bundles to managed devices, problems can arise, such as a bundle failing to install or problems with removing a bundle. These events are logged in the event log so you can address them.

30.5 Using the Hot List

When a device, policy, or bundle has been identified as having a critical or warning event (non-system) that has not been acknowledged or cleared, it is displayed in the Hot List. You can use this list as a summary of problems that need attention. Events on the Hot List are ordered by severity: first are those devices, policies, or bundles with critical events, then those with warning events. Those with the most problems are listed first. With the Hot List, you can see at a glance which device, policy, or bundle needs the most attention.

Figure 30-1 *Summary Page and Hot List*



To view the Hot List, click *Home* on the toolbar. This page shows the System Summary and the Hot List. The System Summary page shows the various categories-servers, workstations, policies, and bundles-and their respective status counts. In this example, there are four policies and none have had a warning or critical event; one server that has not had any warning or critical events; and seven bundles that haven't had any warnings or critical events. In the workstation category, one workstation has had at least one critical event. You can click the workstation name to view a summary, which includes details of the problem events.

Working with Event Logs

31

Event logs are automatically created for important events, such as successful installations or critical errors.

The following sections provide additional information:

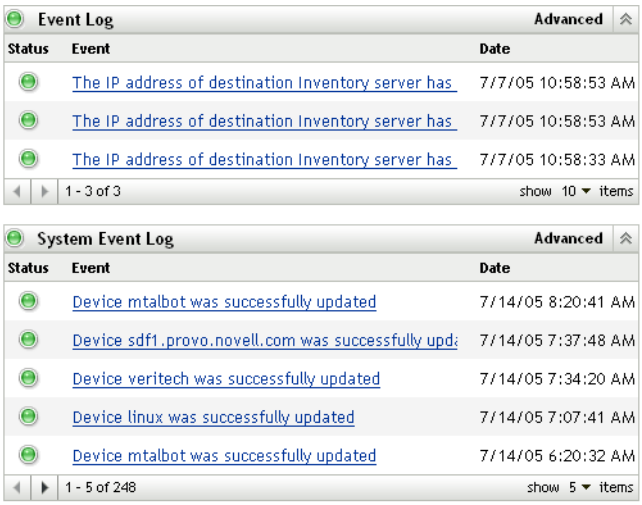
- Section 31.1, “The Event Log Page,” on page 371
- Section 31.2, “Working with the Log Pages,” on page 372

31.1 The Event Log Page

The Event Log page gives you an overview of the recorded events. The Event Log lists the event messages generated by the ZENworks® Agent that resides on the server or workstation. The list is ordered by date, with the latest date first. Each event listed includes the following information:

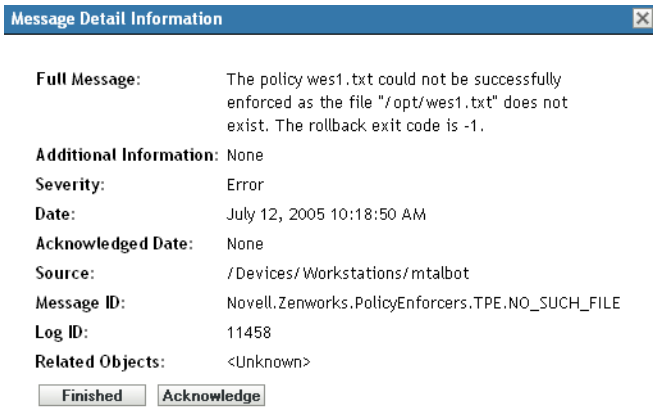
- **Status:** An indication of the event’s severity:
  - The icon indicates an event has executed successfully.
  - The icon indicates an exception condition that might cause problems but that might not need immediate attention.
  - The icon indicates that an action could not be completed because of a user or system error, and it needs immediate attention.
- **Event:** Something that happens, such as a successful installation, that triggers a message to be created and sent. Click the event message to display additional details. You can use the message details window to acknowledge the message, which causes the message to be cleared from the event log.
- **Data:** The date and time the event occurred.
- **Advanced:** A page showing you both acknowledged and unacknowledged events. You can sort events by status, date, or whether an event has been acknowledged or not. You can also acknowledge events from this page.

Figure 31-1 *Event Logs*



When you click the description of an event, the following page appears:

Figure 31-2 *Detailed Information Concerning the Event*



This page can be used to acknowledge the event. Acknowledging an event removes it from the main event log, but you can still see it in the Advanced page. Clicking *Finished* closes the window.

There are two log lists, the Event Log and the System Event Log. The Event Log lists the event messages generated by the ZENworks Agent that resides on the server or workstation; the System Event Log is displayed only for servers that are functioning as primary or secondary ZENworks Servers. The System Event Log lists the system event messages generated by the ZENworks Server for activities that it performs on behalf of all managed devices in its management zone.

31.2 Working with the Log Pages

After an event has been logged, you can view and acknowledge it.

The following sections provide additional information:

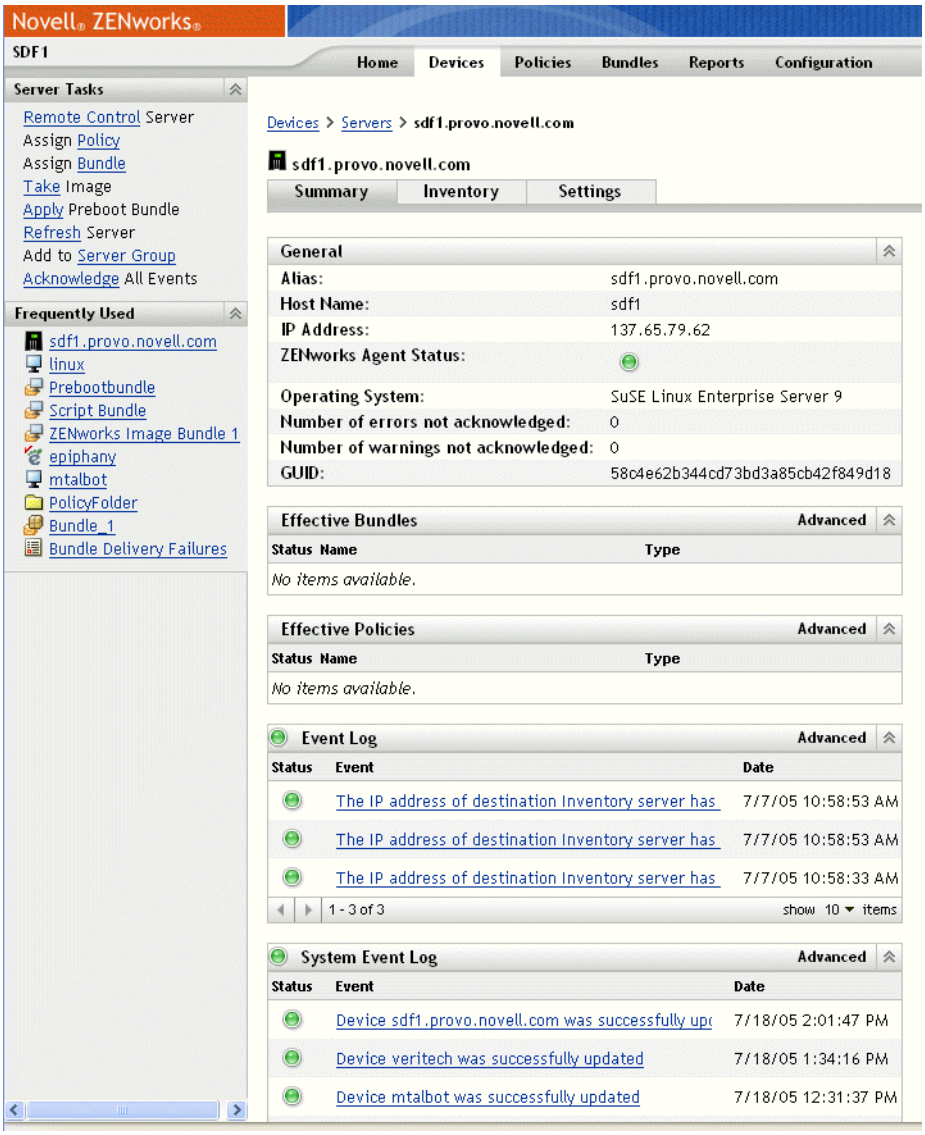
- Section 31.2.1, “Viewing an Event Log,” on page 372
- Section 31.2.2, “Acknowledging an Event,” on page 373
- Section 31.2.3, “Using the Advanced Page,” on page 375
- Section 31.2.4, “Clearing the Event Log,” on page 375

31.2.1 Viewing an Event Log

You can view event logs for devices, policies, and bundles. To view an event log, start with the appropriate tab in the ZENworks Control Center: Devices, Policies, or Bundles. For example, to view the event log for a server, do the following:

1. Click the *Devices* tab on the ZENworks Control Center page to display a list of managed devices.
2. Click *Servers* to display a list of servers.

3 Click the server you want to check. A summary page appears that includes the event logs. To view additional details, click the event.



31.2.2 Acknowledging an Event

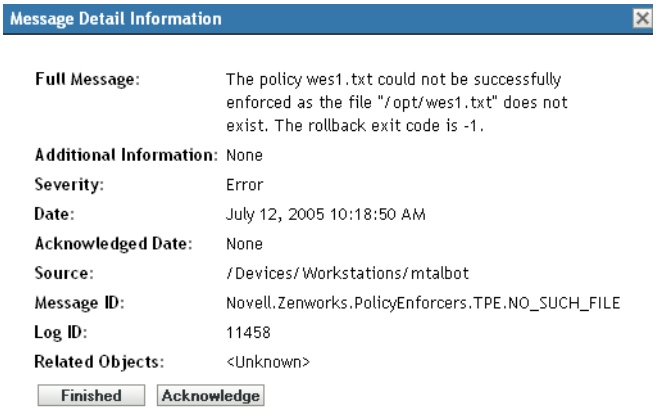
After you view the logs and identify a problem, you can acknowledge it. To acknowledge an event means you've seen it and either fixed it or decided to take care of the problem later. When you acknowledge an event, it is removed from the event and system log lists but kept in the database and on the Advanced page. You can view acknowledged events either by running a report or using the Advanced page.

There are three ways to acknowledge an event. You can acknowledge a single event, acknowledge multiple events, or acknowledge all events.

To acknowledge a single event:

1 Open the Summary page. (For information, see Section 31.2.1, “Viewing an Event Log,” on page 372.)

2 Click the event you want to acknowledge.



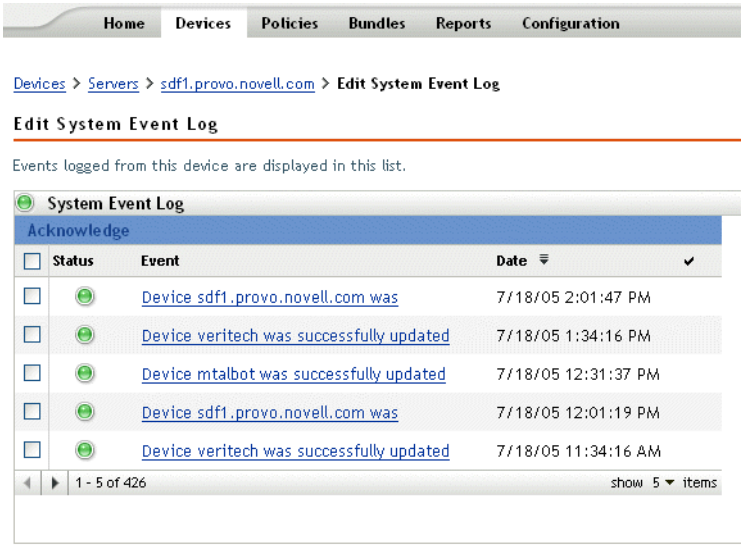
3 Click *Acknowledge*.

The event disappears from the list but remains in the database and is listed on the Advanced page.

To acknowledge several events:

1 Open the Summary page. (For information, see Section 31.2.1, “Viewing an Event Log,” on page 372.)

2 Click *Advanced* on the toolbar in the Event Log section.



3 Select the check box for each message you want to acknowledge.

4 Click *Acknowledge*.

To acknowledge all events:

1 Open the Summary page.

2 Click *Acknowledge All Events* in the upper-left corner.

   Clicking *Acknowledge All Events* acknowledges *all* system events, not just those in a single category.

31.2.3 Using the Advanced Page

You can open the Advanced page by clicking *Advanced* in the upper-right corner of the event log part of the page. In the Advanced page, you can acknowledge events, view acknowledged events, and click the description of an event for more details.

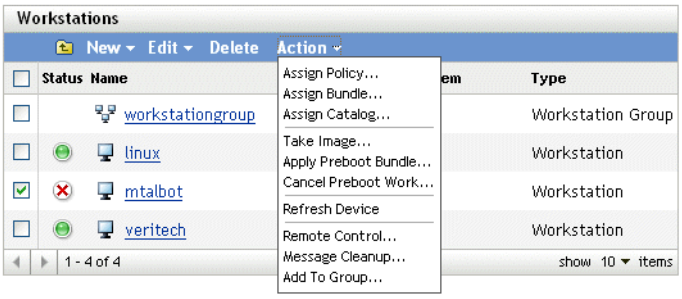
31.2.4 Clearing the Event Log

After you acknowledge an event, you have two options for cleaning up the logs. You can clear the events, which deletes the events from all the lists, including the Advanced window. Once cleared, the event is only available through reports. You can also permanently delete the event, which deletes the event from both the logs and the database. You can clear events associated with servers, workstations, policies, and bundles. For each, the process is the same.

To clear the event log for a workstation:

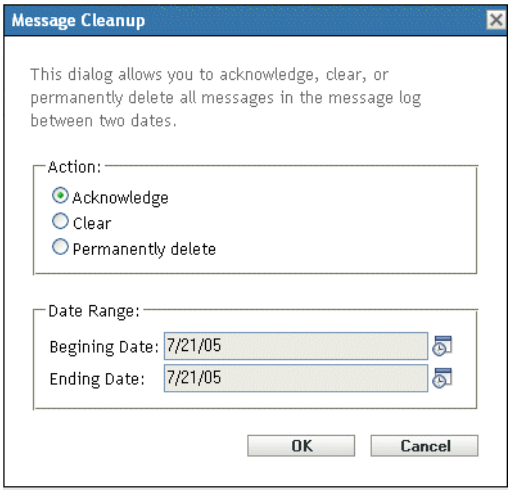
1 Open the Devices page, then click *Workstations*.

2 Click the check box of the workstation you want cleared of events.



3 Click *Action* on the toolbar.

4 Click *Message Cleanup*.



From here you can do the following:

- Acknowledge all event messages for the device. This acknowledges all events within a specified date range and deletes them from the Hot List, event log, and system event log.
- Clear all event messages. This clears all events within a specified date range from the event log, system event log, advanced event log, and advanced system event log.
- Permanently delete all event messages. This deletes all events within a specified date range from all the log lists and the database.

5 When you have selected the option you want and set a date range, click *OK* to clear the messages.

Message Logger

32

You can use the Message Logger component of Novell® ZENworks® 7 Linux Management to log the messages on managed devices and servers.

The following sections provide information to help you understand the functionality of the Message Logger component:

- Section 32.1, "What Is Message Logger?," on page 377
- Section 32.2, "Message Severity," on page 377
- Section 32.3, "Message Format," on page 377

32.1 What Is Message Logger?

Message Logger is the component responsible for logging the messages to different output targets. Several components of ZENworks 7 Linux Management use Message Logger to log messages, including zenloader and webservices on the server and the ZENworks management daemon (ZMD), Remote Management, and Policy Enforcers on the client. For more information about ZENworks services, see Section 3.1, "ZENworks Services," on page 23.

Message Logger logs the messages in different output targets, such as e-mails, SNMP traps, writes to the database, local and system log files, and the central log file.

32.2 Message Severity

Messages are classified in the following three categories:

Error: Indicates that an action cannot be completed because of a user or system error. These messages require immediate attention from an administrator.

Warning: Calls attention to an exception condition. These messages might not be an error but can cause problems if not resolved. These messages do not require immediate attention from an administrator.

Information: Provides feedback about something that happened in the product or system that is important and informative for an administrator.

32.3 Message Format

Messages are logged on the managed device and primary server in the following format:

```
Severity: [time] Component_Name Message_ID Message_String
Additional_Info:Value_for_Additional_Info
```

For example, ERROR: [3/15/05 3:28:45 PM] PolicyEnforcers Novell.Zenworks.PolicyEnforcers.EPE.NO_SUCH_FILE The Text File policy could not be successfully enforced as the file `abc.txt` does not exist.

Additional Info: PolicyEnforcer Exception: file does not exist.

Configuring Message Logger Settings

33

You can perform the following activities by configuring Message Logger settings:

- Write messages to a local log file
- Write messages to a system log file
- Send messages as SNMP traps
- Send messages as SMTP mail
- Purge the database entries

NOTE: The Message Logger does not log the messages with severity levels other than error, warning, information, and debug.

There are two ways to configure Message Logger settings:

- Section 33.1, "Configuring Message Logger Settings for the Primary Server," on page 379
- Section 33.2, "Configuring Message Logger Settings for a Managed Device," on page 382

33.1 Configuring Message Logger Settings for the Primary Server

The following settings of the Message Logger can be configured to log messages on the primary server:

- Section 33.1.1, "Configuring Database Maintenance Settings," on page 379
- Section 33.1.2, "Configuring Centralized Log Settings," on page 380
- Section 33.1.3, "Configuring SMTP Settings," on page 380
- Section 33.1.4, "Configuring SNMP Settings," on page 381

33.1.1 Configuring Database Maintenance Settings

These settings allow you to configure the database maintenance settings for purging the database log messages.

1. In the ZENworks® Control Center, click *Configuration*.
2. In *Management Zone Settings*, click *Centralized Message Logging*.
3. Under *Central Server*, specify the name of the server that is responsible for purging message log entries from the database.

   You can also select a server by clicking .

   The ZENworks servers that are displayed here are the ones that are registered with Novell® ZENworks Linux Management Server.

4 In the *Purge Log Entries After* field, select a value from the drop-down list. The available options are *30, 60,* and *90*.

   Log entries older than the selected number of days are purged. Purging is done every midnight and 5 minutes after zenloader starts.

5 Click *OK* or *Apply*.

33.1.2 Configuring Centralized Log Settings

These settings allow you to use a log file to log the messages of a server and all the managed devices that are connected to this server. The name of this log file is `central-message.log`, and it is located in `/var/opt/novell/log/zenworks`.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Under *Centralized File Log*, select the *Log Message to a Centralized File if Severity Is* check box to enable the settings.

4 In the *Log Message to a Centralized File if Severity Is* field, select a value from the drop-down list.

   - Select *Error* to store the messages that have an Error severity.
   - Select *Warning and Above* to store the messages that have a severity of Warning and Error.
   - Select *Information and Above* to store the messages that have a severity of Information, Warning, and Error.

5 In the *Limit File Size To* field, specify the size of a file in KB or MB.

   The message file is backed up after reaching the specified size.

6 In the *Number of Backup Files* field, specify the number of backup files to take.

   The maximum number of backup files is 99. The most recent backup file is named `central-message.log.1`, the second most recent file has the number 2, and so on. When the maximum file size is reached, the oldest file is deleted.

7 Click *Apply* or *OK*.

33.1.3 Configuring SMTP Settings

These settings allow you to send error messages through e-mail by configuring SMTP settings.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Under *E-mail Notification*, select the *Send Log Message via E-mail If Severity Is* check box to enable the settings.

4 In the *SMTP Server Address* field, specify the SMTP server address.

   You can specify a DNS name or IP address as a server address.

5 Select *SMTP Server Requires Authentication* to authenticate to the SMTP server.

6 Specify the username to use to authenticate to the SMTP server.

7 Specify the password to use to authenticate to the SMTP server.

IMPORTANT: For security considerations, you should create a separate e-mail account and password to send ZENworks messages.

8 In the *Message Settings* section, specify the sender's e-mail address in the *From* field. The error messages are sent from this e-mail address.

9 In the *To* field, specify the e-mail address of the recipients.

You can specify more than one e-mail address by separating the addresses with commas.

10 Specify a subject for the e-mail.

The following table describes how you can customize the subject field:

Format Specifiers	Value
%s	Severity of the message
%c	Component name
%d	Device ID
%t	Time when the message is generated
%a	Alias name of the device on which the message is generated.

Format specifiers are a special set of characters that are replaced with their associated values.

For example, if you want the subject line to be displayed as "ERROR occurred on device TestDevice at 4/7/05 5:31:01 PM," then in the subject line you should specify "%s occurred on device %a at %t."

11 Click *OK* or *Apply*.

33.1.4 Configuring SNMP Settings

These settings allow you to send messages as SNMP traps. The location of the MIB file is `/opt/novell/zenworks/share/loggermodule/messageloger.mib`.

NOTE: The MIB file should not be modified or deleted, or sending of traps does not work.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Under *SNMP Traps*, select the *Log to SNMP Trap if Severity Is* check box to enable all the fields.

4 In the *Log to SNMP Trap if Severity Is* field, select a value from the drop-down list.

- Select *Error* to forward on as traps the messages that have Error, Information, Warning, and Debug severity.
- Select *Warning and Above* to forward on as traps the messages with a severity of Warning and Error.
- Select *Information and Above* to forward on as traps the messages that have a severity of Information, Warning, and Error.

5 Specify a trap target.

You can specify the IP address or DNS name of the management console as a trap target.

6 Specify the port number of the SNMP server.

By default, the port number is 162.

7 Specify the community string of the SNMP trap that is to be sent.

The default value of the community string is Public.

8 Click *OK* or *Apply*.

33.2 Configuring Message Logger Settings for a Managed Device

The following settings of the Message Logger can be configured to log the messages on a managed device:

- Section 33.2.1, "Configuring Local Log Settings," on page 382
- Section 33.2.2, "Configuring System Log Settings," on page 383

33.2.1 Configuring Local Log Settings

These settings allow you to write messages into a local file. The name of the log file for ZMD logging is `zmd-message.log`; for ZENloader logging it is `loader-message.log`; and for ZEN server logging it is `services-message.log`. The path of the local log files is `/var/opt/novell/log/zenworks`.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Local Device Logging*.

3 Under *Local File*, select the *Log Message to a Local File if Severity Is* check box to enable the fields.

4 In the *Log Message to a Local File if Severity Is* field, select a value from the drop-down list.

- Select *Error* to store the messages that have Error, Information, Warning, and Debug severity.
- Select *Warning and Above* to store the messages with a severity of Warning and Error.
- Select *Information and Above* to store the messages that have a severity of Information, Warning, and Error.
- Select *Debug and Above* to store the messages that have a severity of Debug, Information, Warning, and Error

5 In the *Limit File Size To* field, specify the size of the file in MB or KB.

The messages are backed up after reaching the specified size and the file is reset.

6 In the *Number of Backup Files* field, specify the number of backup files to take.

The maximum number of backup files is 99. The most recent backup file is named central-message.log.1, the second most recent file has the number 2 and so on. When the maximum file size is reached, the oldest file is deleted.

7 Click *OK* or *Apply*.

33.2.2 Configuring System Log Settings

These settings allow you to insert messages into the system file. The path of the system log file is `/var/log/messages`.

1. In the ZENworks Control Center, click *Configuration*.
2. In *Management Zone Settings*, click *Local Device Logging*.
3. Under *System Log*, select the *Send Message to Local System Log if Severity Is* check box to enable the fields.
4. In the *Send Message to Local System Log if Severity Is* field, select a value from the drop-down list.
   - Select *Error* to store the messages with Error, Information, Warning, and Debug severity.
   - Select *Warning and Above* to store the messages with a severity of Warning and Error.
   - Select *Information and Above* to store the messages with a severity of Information, Warning, and Error.
5. Click *OK* or *Apply*.