Novell

ZENworks® 10 Configuration Management with SP1

10.0.3.

1

MESSAGE LOGGING REFERENCE

Novell®

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This *Novell ZENworks 10 Configuration Management Message Logging Reference* includes information about Message Logger features and procedures to help you configure and maintain your Novell® ZENworks® system. The information in this guide is organized as follows:

- Chapter 1, "Overview," on page 9
- Chapter 2, "Configuring Message Logger Settings," on page 11
- Chapter 3, "Managing Messages," on page 19

Audience

This guide is intended for ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

ZENworks 10 Configuration Management with SP1 is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 10 Configuration Management documentation (http://www.novell.com/documentation/zcm10/index.html)ZENworks 10 Configuration Management with SP1 documentation (http://www.novell.com/documentation/zcm101/index.html).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux*, should use forward slashes as required by your software.

Overview

1

The Message Logger component of Novell® ZENworks® 10 Configuration Management with SP1 lets the other ZENworks components such as zenloader and webservices, ZENworks Management Daemon (ZMD), Remote Management, and Policy Enforcers log messages to different output targets. The output targets includes the system log, local log, database, SMTP, SNMP trap, and UDP.

The following sections provide additional information on the Message Logger component:

- Section 1.1, "Functionalities of Message Logger," on page 9
- Section 1.2, "Message Severity," on page 9
- Section 1.3, "Message Format," on page 10

1.1 Functionalities of Message Logger

Message Logger performs the following functions:

- Writes messages to local log files.
- Writes messages to system log or event log.
- Writes messages to the Management console.
- Sends messages to the Management server.
- Sends messages as SMTP mail to SMTP servers from the Primary Server.
- Sends messages as SNMP traps to remote or local machines from the Primary Server.
- Sends messages as UDP packets to UDP destinations.
- Writes messages to the ZENworks database.
- Automatically purges database entries from the ZENworks database.
- Automatically acknowledges the messages in the ZENworks database.

1.2 Message Severity

A message is an event that is generated by different components and modules. These events can be exceptions such as errors, warnings, information to a user, or a debug statement to debug a module.

Messages are classified based on the following severity levels:

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

Warning: Indicates 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.

Debug: Provides debug information to troubleshoot and solve problems that might occur. The debug messages are stored only in the local file.

1.3 Message Format

Messages are logged in different formats depending on the output targets. For more information on message formats see, .

Configuring Message Logger Settings

<div style="text-align: right; font-size: 3em;">2</div>

The following sections provide information on configuring the settings of the Message Logger component of Novell® ZENworks® 10 Configuration Management with SP1.

2.1 Configuring the Message Logger Settings at the Zone Level

The following sections contain information to help you configure the settings in the Management Zone to enable message logging:

2.1.1 Local Device Logging

In ZENworks Control Center, the Local Device Logging page lets you configure the message logging to a local drive and the system log file of the managed device.

To enable and configure local logging for messages:

1 In ZENworks Control Center, click *Configuration*.

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

3 Configure the following options in the Local File panel.

Field	Details
Log Message to a Local File if Severity Is	◆ **Error:** Stores messages with a severity of Error.
	◆ **Warning and Above:** Stores messages with a severity of Warning and Error.
	◆ **Information and Above:** Stores messages with a severity of Information, Warning, and Error.
	◆ **Debug and Above:** Stores messages with a severity of Debug, Information, Warning, and Error.
	If you need to troubleshoot a ZENworks® Adaptive Agent issue on an individual device, you can change the severity setting so that additional information is logged. To do so, on the device, double-click the Z icon in the system tray; click *Logging* in the left navigation pane; then select an option from the *Log Messages if Severity Is* drop-down list.
Rolling Based on Size	Closes the current log file and starts a new file based on the file size:
	◆ **Limit File Size to:** Specify the maximum size of the log file, in either kilobytes (KB) or megabytes (MB). The log file is closed after the size of the file reaches the specified limit and a new file is started.
	◆ **Number of Backup Files:** Specify the number of closed files to be backed up. The maximum number of backup files is 13.
Rolling Based on Date	Closes the current log file and starts a new file based on the following schedules:
	◆ **Daily Pattern:** Starts a new file daily.
	◆ **Monthly Pattern:** Starts a new file monthly.

On a Windows* managed device, the local files are zmd-messages.log, loader-messages.log, and services-messages.log. The zmd-messages.log file is located in \novell\zenworks\logs\localstore. The loader-messages.log and services-messages.log are located in \novell\zenworks\logs.

On a Linux* managed device, the local files messages.log and services-messages.log are located in /var/opt/novell/ log/zenworks.

4 Configure the following options in the System Log panel.

Field	Details
Send Message to Local System Log if Severity Is	◆ **Error:** Stores messages with severity of Error.
	◆ **Warning and Above:** Stores messages with a severity of Warning and Error.
	◆ **Information and Above:** Stores messages with a severity of Information, Warning, and Error.

The system log file is Event log on Windows and is /var/log/messages on Linux devices.

2.1.2 Centralized Message Logging

In ZENworks Control Center, the Centralized Message Logging page lets you configure the settings related to message logging performed by the Primary Server.

1 In ZENworks Control Center, click *Configuration*.

2 In the Management Zone Settings panel, click *Event and Messaging*, then click *Centralized Message Logging.*

3 In the Automatic Message Cleanup panel, configure the settings to automatically acknowledge or remove the logged messages from the ZENworks server.The following table contains information on the options available:

Field	Details
Preferred Maintenance Server	Specify the IP address of the preferred server on which the Message Cleanup actions runs to acknowledge or delete the logged messages from database.
Information	Allows you to configure the following settings for the informational messages:
	◆ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are acknowledged when the message Clean up activity is scheduled to run. If you specify zero, then the informational messages dated until today are acknowledged. By default, all the informational messages older than 60 days are automatically acknowledged.
	◆ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are deleted when the message Clean up activity is scheduled to run. If you specify zero, then the informational messages dated until today are deleted. By default, all the informational messages older than 60 days are automatically deleted.
	If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

Field	Details
Warnings	Allows you to configure the following settings for the warning messages:
	◆ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are acknowledged when the message Clean up activity is scheduled to run. If you specify zero, then the warning messages dated until today are acknowledged. By default, all the warning messages older than 60 days are automatically acknowledged.
	◆ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are deleted when the message Clean up activity is scheduled to run. If you specify zero, then the warning messages dated until today are deleted. By default, all the warning messages older than 60 days are automatically deleted.
	If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.
Errors	Allows you to configure the following settings for the error messages:
	◆ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are acknowledged when the message Clean up activity is scheduled to run. If you specify zero, then the error messages dated until today are acknowledged. By default, all the error messages older than 60 days are automatically acknowledged.
	◆ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are deleted when the message Clean up activity is scheduled to run. If you specify zero, then error messages dated until today are deleted. By default, all the error messages older than 60 days are automatically deleted.
	If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.
Select the Days of the Week and the Time to Perform the Message Cleanup	Allows you to specify the time and the days of the week days to run the Message Cleanup action. The administrator can set a daily schedule for Message Cleanup action.

Field	Details
Use Coordinated Universal Time	Allows you to convert the specified time to GMT time. By default, this option is selected.

4 In the E-mail Notification panel, configure the settings to send the error messages to the administrators through e-mail. The following table contains information on the options available:

Field	Details
Send Log Message via E-mail if Severity Is	Allows you to select the severity of the message to send the log messages through e-mail.
From	Specify the sender's e-mail address.
To	Specify the e-mail address of the recipients. You can specify more than one e-mail address by separating them with commas.
Subject	Specify the subject to be included while sending the e-mail from the Primary Server. You can customize the subject field with macro values. For more information on customizing the subject field, see Section 3.1.2, "E-Mail Format," on page 20.

5 In the SNMP Traps panel, configure the SNMP traps on the ZENworks Server to send log messages.

Field	Details
Send as SNMP Trap if Severity Is	Sends SNMP trap if the logged message's severity is Error.
Trap Target	Specify the IP address or DNS name of the SNMP server.
Port	Specify the port number of the SNMP server configured for this operation. By default, the port number is 162.
Community String	Specify the community string of the SNMP trap that is to be sent.

6 In the UDP Forwarder panel, configure the settings to send logged messages through the UDP services. The following table contains information on the options available:

Field	Details
Send Message via UDP	Sends messages to the UDP destinations if the logged message's severity is Error.

Field	Details
UDP Destinations	You can perform the following tasks with the *Add*, *Edit*, and *Remove* options:

- ◆ **Add a Server**
  1. Click *Add* to display the Add UDP Destination Address dialog box.
  2. Specify the server name and the UDP port number configured for this operation.
  3. Click *OK*.
- ◆ **Remove a Server**
  1. Select the check box in front of the server (or servers).
  2. Click *Remove*.
- ◆ **Edit Server Details**
  1. Select the check box in front of the server.
  2. Click *Edit* to display the Edit UDP Destination.
  3. Modify the settings as desired, then click *OK*.

2.2 Configuring the Message Logger Settings at the Folder Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging settings for all the devices within a folder:

1. In ZENworks Control Center, click *Devices*.
2. Click the folder (details) for which you want to configure the Message Logger settings.
3. Click *Settings*, then click *Device Management > Local Device Logging*.
4. Click *Override*.
5. Edit the logging settings as required.
6. To apply the changes, click *Apply.*

   or

   To revert to the Local Device Logging settings configured at the zone level, click *Revert*.
7. Click *OK*.

2.3 Configuring the Message Logger Settings at the Device Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging settings for the managed device:

1. In ZENworks Control Center, click *Devices*.
2. Click *Servers* or *Workstations* to display the list of managed devices.
3. Click the device for which you want to configure the Message Logger settings.

4 Click *Settings*, then click *Device Management > Local Device Logging*.

5 Click *Override*.

6 Edit the logging settings as required.

7 To apply the changes click *Apply*.

or

To revert to the Local Device Logging settings configured at the zone level, click *Revert*.

8 Click *OK*.

2.4 Turning on the Debug Messages

To turn on the logging of debug messages for all the components:

1 In ZENworks Control Center, click *Configuration*.

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

3 In the local file panel, select the *Log message to a local file if severity is* option, then select the severity as *Debug and above*.

4 Click *Apply,* then click *OK*.

Managing Messages

3

The Message Logger component lets you manage the messages logged by the other components of Novell® ZENworks® 10 Configuration Management with SP1.

3.1 Understanding Message Formats

Messages are logged in different formats depending on the output targets such as local log, e-mail notification, SNMP traps, and UDP notification.

All error messages log the component name on which the error is generated. To troubleshoot the error, refer to the component's Reference Guide.

Example 1: Error related to Policy Management.

```
[DEBUG] [7/22/2007 3:42:45 PM] [] [PolicyManager] [] [Name =
RM_dev, Guid = 271414163524d000190dbc6fa94272aa, Type = remote
management policy, Version = 2] [] [].
```

To troubleshoot this error, refer *ZENworks 10 Configuration Management Policy Management Reference*.

Example 2: Error related to Remote Management.

```
[ERROR] [15-07-2007 12:44:16] [] [Remote Management]
[RemoteManagement.VNCEVENT_CANNOT_OPEN_EVENT] [Unable to open the
<ZRMUserLoginEvent> event] [] [].
```

To troubleshoot this error, refer *ZENworks 10 Configuration Management Remote Management Reference*.

3.1.1 Local Log File Format

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

```
[severity] [loggingTime] [userGUID] [componentName] [MessageID]
[MessageString] [additionalInfo] [RelatedGUID].
```

For example, `[DEBUG] [1/22/2007 12:09:15 PM] [] [ZMD] [] [refreshing QuickTaskRefresh(GeneralRefresh)] [] [].`

3.1.2 E-Mail Format

An e-mail message consists of the message header and the message body:

Message Header: The subject field in the e-mail can be customized as required by using keyword substitution macros. The following table lists the possible keyword substitution macros:

Macro	Value
%s	Severity of the message.
%c	Name of the component.
%d	ID of the device at which the message is generated.
%t	Time of the message generation.
%a	Alias name of the device where the message is generated.

For example, if you want the subject line to display as "ERROR occurred on device Testifies at 4/1/07 5:31:01 PM", then specify "*%s occurred on device %a at %t*" in the *Subject* field.

Message Body: The message body consists of the following fields:

Field	Details
Device Alias	Name of the device where the message is generated.
Device IP Address	IP Address of the device where the message is generated.
Error	[Date] Component name Message ID localized message string.
Additional Information (Optional)	Additional Information if any.

3.1.3 SNMP Message Format

The SNMP messages consists of the following two parts:

SNMP Message Header The following table lists the fields contained in the header:

Field	Details
Version number	Specifies the version of SNMP used. ZENworks 10 Configuration Management with SP1 uses SNMPv1.
Community String	Defines an access environment for a group of network-management systems (NMS).

Protocol Data Unit (PDU) The following table lists the fields contained in the PDU:

Field	Details
Enterprise	Identifies the type of managed object generating the trap. ZENworks 10 Configuration Management with SP1 uses 1.3.6.1.4.1.23.2.80.100.
Agent address	Provides the IP address of the machine where the trap was generated.
Generic trap type	This has the integer value 6. Type 6 is an enterprise- specific trap type, which has no standard interpretation in SNMP. The interpretation of the trap depends upon the value in the specific trap type field, which is defined by Message Logger MIB.
Specific trap code	For enterprise-specific traps generated by ZENworks 10 Configuration Management with SP1, the values in the specific trap type field are as indicated below: ◆ For a severity level of MessageLogger.ERROR, the specific trap is 1. ◆ For a severity level of MessageLogger.WARN, the specific trap is 2. ◆ For a severity level of MessageLogger.INFO, the specific trap is 3.
Time stamp	The time stamp indicating when the trap occurred.
Variable bindings	Provides additional information pertaining to the trap. This field consists of the following name/value pairs: ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.1, the value is the device GUID. ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.2, the value is the device name. ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.3, the value is the component name. ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.4, the value is the time when the message was logged. ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.5 the value is the message ID. ◆ For trap ID 1.3.6.1.4.1.23.2.80.100.0.6 the value is the probable cause.

3.1.4 UDP Payload Format

The payload is a byte array with null-terminated delimiters such as "\0" or 0 x 00 (hexadecimal) for each element. Each element's data is presented as UTF-8 encoded strings and is explained below:

◆ The first element is the ZENworks version information. For example, 10.

◆ The second element is the value of severity of the message. The severity values are 4 for INFO, 6 for WARNING, and 8 for DEBUG messages.

◆ The third element is the message date. The date is not locally specific and is represented as UTF-8 string. For example, 09-Dec-2006 14:15:44.

◆ The fourth element is the user ID.

◆ The fifth element is the component name.

◆ The sixth element is the non-localized message ID.

◆ The seventh element is the localized message string.

◆ The eighth element is the additional information.

◆ The ninth element is the probable cause URL.

◆ The tenth element is the relatedGUID objects separated by commas.

NOTE: If the element does not have any data, then it is represented as \0\0.

3.2 Viewing the Message Status

In ZENworks Control Center, you can view the status of the logged messages in the following panels on the home page.

3.2.1 Message Summary

The Message Summary panel displays the number of critical, warning, and normal messages generated on the four main objects in the Management Zone namely: the servers, workstations, policies, and bundles.

Figure 3-1   *Message Summary*

Message Summary	⊗	◇	●	Total
Servers	3	0	5	8
Workstations	9	1	1	11
Policies	3	0	17	20
Bundles	2	0	5	7

In the Message Summary panel, you can do the following:

- ◆ Click an object type to display its root folder. For example, click *Servers* to display the Servers root folder.
- ◆ For any object type, click the number in one of its status columns (⊗ ◇ ●) to display a listing of all the objects that currently have that status. For example, to see the list of policies that have a normal status, click the number in the column of the *Policies*.
- ◆ For any object type, click the number in the *Total* column to display all of the objects of that type having critical, warning, or normal messages. For example, click the Total count for *Servers* to display a list of all servers having messages logged.

3.2.2 Device Hot List

The Device Hot List displays a list of the devices that have generated a critical or warning message. The device remains in the hot list until you acknowledge its message (or messages). You can use this list as a summary of problems that need attention on the device.

The list is ordered based on the severity of the events. To display the events, do one of the following:

- ◆ Click the ⊗ icon in the column heading to display only the events with a critical status.
- ◆ Click the ◇ icon in the column heading to display only the events with a warning status.
- ◆ Click the device to display its message log.

To view the Device Hot List:

1 In ZENworks Control Center, click the *Home* tab.

Figure 3-2 *Device Hot List*

⊗	⊗	◇	Type	Item
3	45	22	🖥	blr-nrm-r6a
2	28	27	🖥	blr-nrm-r9a
2	25	23	🖥	blr-nrm-r5v2
2	0	0	🗄	blr-nrm-r3f
1	52	1	🖥	blr-nrm-r11d

Device Hot List   1 - 5 of 15   show 5 ▼ items

The list displays only five items at a time. To display the next set of the items, click the ▸ icon.

3.3 Viewing the Messages

In the ZENworks Control Center, you can view the logged messages as follows

3.3.1 Message Log

The Message Log displays all unacknowledged messages generated for the object such as device, bundle, or policy.

To view the message logs:

1 In ZENworks Control Center, click the *Device Hot List* on the home page, then click the device to view its message log.

You can also use the Devices menu to view the logs:

1 In ZENworks Control Center, click *Devices*.

2 Click *Servers* or *Workstations* to display the list of managed devices.

3 Click the name of a device, then click the *Summary* tab.

Figure 3-3 *Message Log*

Status	Message	Date
◇	The action local file rights policy (ID:local file rights policy	3:20 AM
⊗	The drive "d:" is not a local fixed drive. Files/folders on this	3:20 AM
◇	The action local file rights policy (ID:local file rights policy	3:14 AM
⊗	The drive "d:" is not a local fixed drive. Files/folders on this	3:14 AM
◇	The action grouppolicy (ID:grouppolicy) failed, but the action s	3:11 AM

Message Log   Advanced   1 - 5 of 91   show 5 ▼ items

The message log displays the following:

Field	Description
Status	Displays an icon indicating the type of message: ❌ Critical Message 🔶 Warning 🟢 Normal
Message	Displays a brief description of the event that occurred.
Date	Displays the date and time the event occurred.

To view the log messages in the advanced view:

1 Click *Advanced* on the right-hand corner of the Memory Log panel.
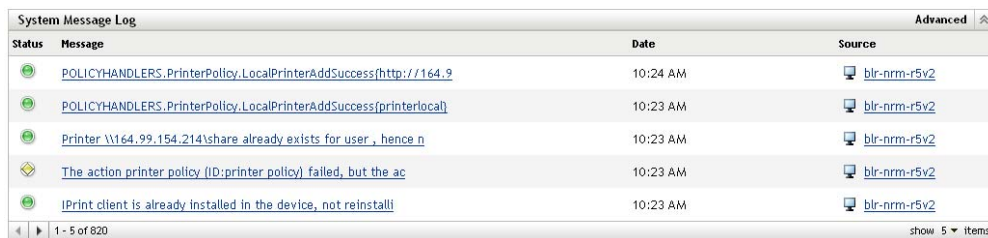
You can acknowledge or delete messages from the message log. For more information on acknowledging messages, see Section 3.4, "Acknowledging Messages," on page 25, and for information on deleting messages, see Section 3.5, "Deleting Messages," on page 27.

3.3.2 System Message Log

The System Message Log panel displays the unacknowledged messages generated by the ZENworks Servers and managed devices in the Management Zone.

1 In ZENworks Control Center, click *Configuration*.

2 Click *System Information.*

Figure 3-4 *System Message Log*

The system message log displays the following:

Field	Description
Status	Displays an icon indicating the type of message: ❌ Critical Message 🔶 Warning 🟢 Normal
Message	Displays a brief description of the event that occurred
Date	Displays the date and time the event occurred

To view the log messages in the advanced view:

1 Click *Advanced* on the right-hand corner of the System Memory Log panel.

You can acknowledge or delete messages from the system message log. For more information on acknowledging messages, see Section 3.4, "Acknowledging Messages," on page 25, for information on deleting messages, see Section 3.5, "Deleting Messages," on page 27.
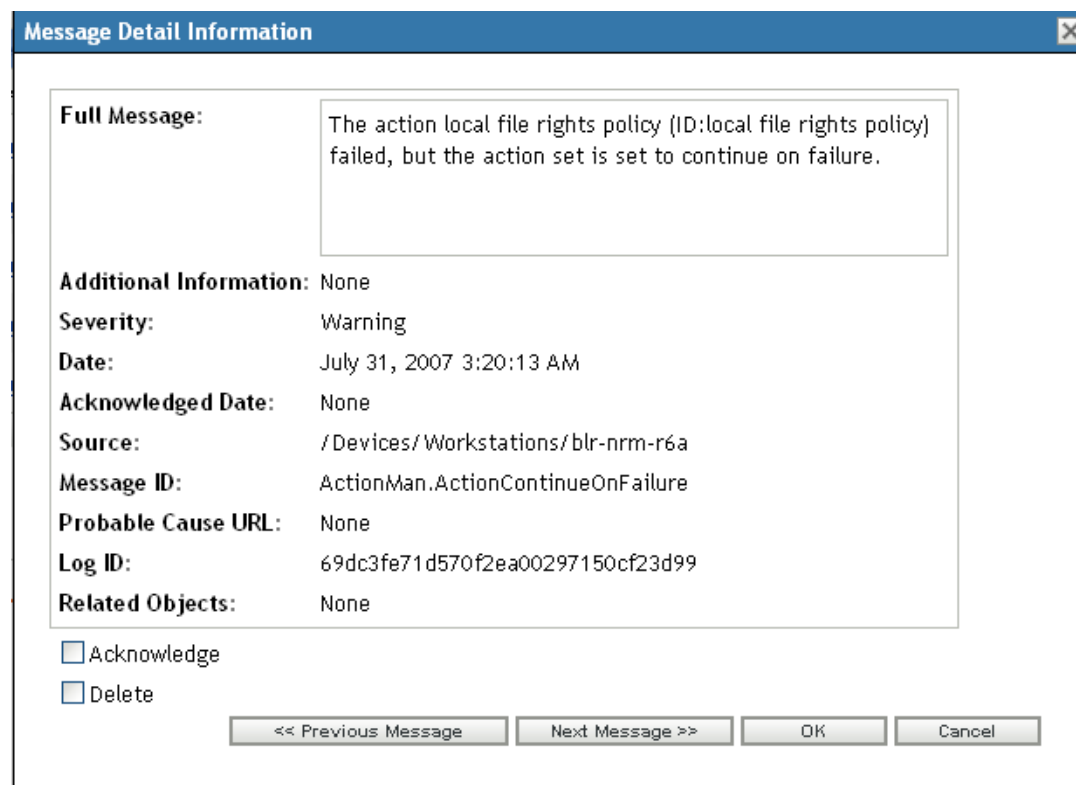
3.4 Acknowledging Messages

An acknowledged message is one that you have reviewed and marked as acknowledged(✔).

- ◆ Section 3.4.1, "Acknowledging a Message," on page 25
- ◆ Section 3.4.2, "Acknowledging Multiple Messages," on page 26
- ◆ Section 3.4.3, "Acknowledging Messages Logged During a Specified Time," on page 26

3.4.1 Acknowledging a Message

1 In the Message Log panel or the System Message Log panel, click the message you want to acknowledge.

2 In the Message Detail Information dialog box, select the *Acknowledge* option, then click *OK*.

Figure 3-5 *Message Detail Information*

The acknowledged messages are removed from the Message Log panel or the System Message Log panel depending on which panel you selected in Step 1.

The acknowledged messages continue to be listed in the Advanced view of these logs, marked with a check mark (✔).

3.4.2 Acknowledging Multiple Messages

1 In the Message Log panel or the System Message lLog panel, click *Advanced* on the right-hand corner of the panel.

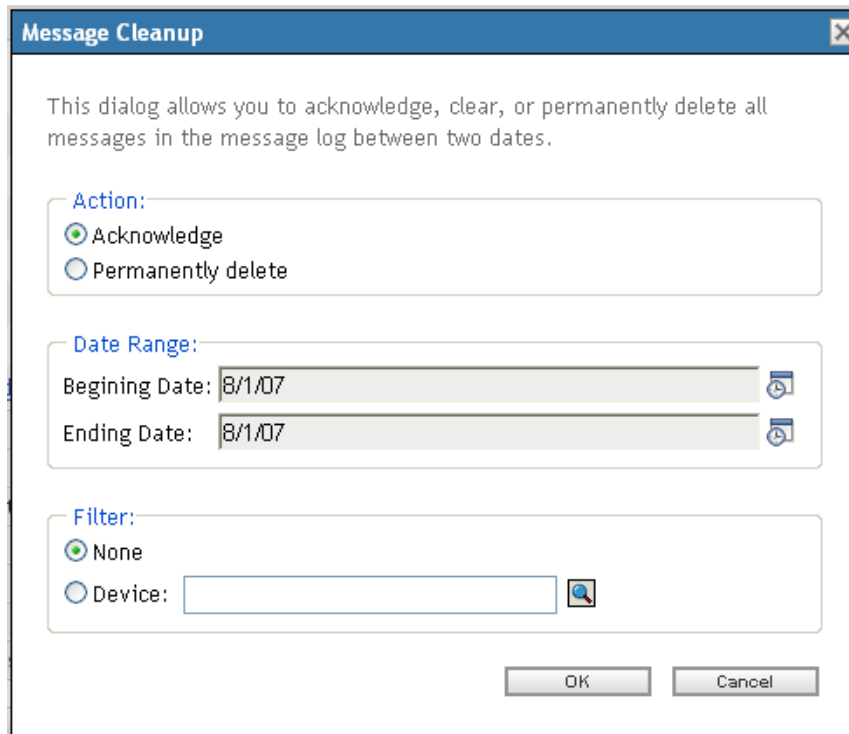2 Select the messages to acknowledge, then click *Acknowledge*.

Figure 3-6   *Edit Message Log*

The acknowledged messages are marked with a check mark(✔).

3.4.3 Acknowledging Messages Logged During a Specified Time

1 In ZENworks Control Center, click *Configuration*.

2 In the *Configuration Tasks*, click *Message Cleanup*.

3 In the Message Cleanup dialog box, select *Acknowledge*.

4 In the *Date Range* option, select the *Beginning Date* and the *Ending Date*.

5 Select the *Filter* option:

    *None***:** Cleans up the messages in selected date range from all the devices.

    *Device***:** Cleans up the messages in selected date range from the selected device.

6 Click *OK*.

A message cleanup action is initiated and a system message is logged after the cleanup action is completed. For more information on viewing system logs, see Section 3.3.2, "System Message Log," on page 24.
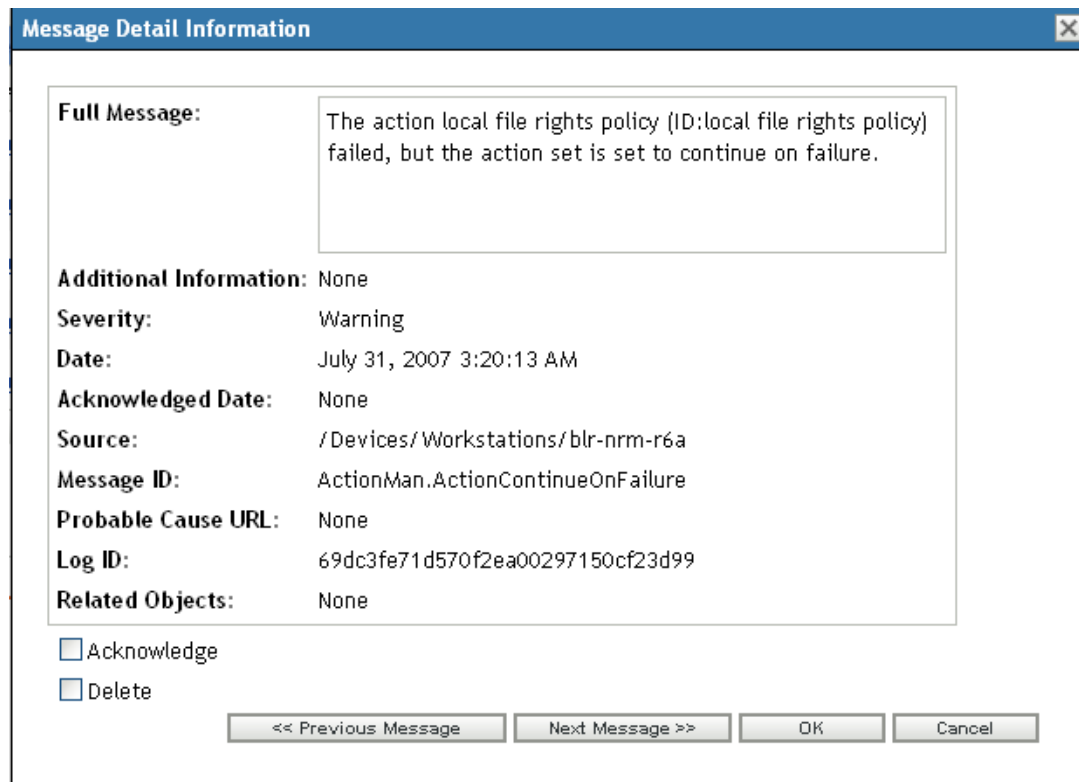
3.5 Deleting Messages

Deleting a message completely removes the message from your ZENworks system.

3.5.1 Deleting a Message

1 In the Message Log panel or the System Message Log panel, click the message you want to delete.

2 In the Message Detail Information dialog box, select the *Delete* option, then click *OK*.

Figure 3-7 *Message Detail Information*
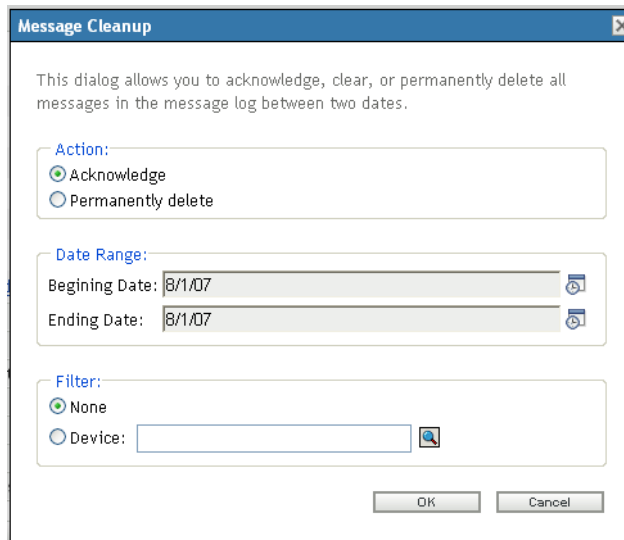

3.5.2 Deleting Multiple Messages

1 In the Message Log panel or the System Message lLog panel, click *Advanced* on the right-hand corner of the panel.

2 Select the messages to delete, then click *Delete*.

3.5.3 Deleting Messages Logged During a Specified Time

1 In ZENworks Control Center, click *Configuration*.

2 In the *Configuration Tasks*, click *Message Cleanup*.

3 In the Message Cleanup dialog box, select *Permanently Delete*.

4 In the *Date Range* option, select the *Beginning Date* and the *Ending Date*.

5 Select the *Filter* option:

   None: Cleans up the messages in selected date range from all the devices.

   Device: Cleans up the messages in selected date range from the selected device.

6 Click *OK*.

7 In the Confirm Delete Dialog box, click *OK* to delete the message.

   A system message is logged after the cleanup action is completed. For more information on viewing the system log see, Section 3.3.2, "System Message Log," on page 24.