Altiris™ Log Viewer User Guide

Symantec™
A Division of Broadcom

Altiris™ Log Viewer User Guide

Legal Notice

For more information, please visit https://www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Broadcom
1320 Ridder Park Drive
San Jose, California
95131

https://www.broadcom.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Contents

Chapter 1

Introducing the Altiris™ Log Viewer

This chapter includes the following topics:

About the Altiris Log Viewer

The Altiris Log Viewer (also known as NS Log Viewer) lets you monitor several log locations for different components like IT Management Suite, Symantec Management Agent and Symantec Installation Manager. The Altiris Log Viewer is a `WinForms` executable that lets you view the Notification Server logs.

The Altiris Log Viewer is installed by the **Diagnostics** package during the initial installation of the Symantec Management Platform. The `altiris_diagnostics_`*`[product-version]`*`_x64.msi` is located at …`\Program Files\Altiris\Symantec Installation Manager\Installs\Altiris`.

The Log Viewer lets you perform the following tasks:

- View error, warning, informational, trace, and verbose messages.
- Search the logs and view the results.
- Bookmark the log items.
- Filter the logs to display a subset of messages.
- Save the filter definitions for later use.
- Perform search in log files without loading them into Log Viewer.

Log Viewer automatically detects whether a component is installed to custom location and monitors the custom path. Log Viewer lists the real-time events, errors and warnings. These messages help you monitor and troubleshoot your Notification Server.

You can use the Log Viewer to determine the problems and their cause. After you identify errors or warnings in the Log Viewer, you can use the error messages to search the Symantec Knowledge Base for the articles that help you correct the error. You can also raise the issue to the technical support team.

Altiris Log Viewer User Interface

The following figure and table describe the sections of the Altiris Log Viewer user interface.

Figure 1-1 Sections of the Altiris Log Viewer user interface

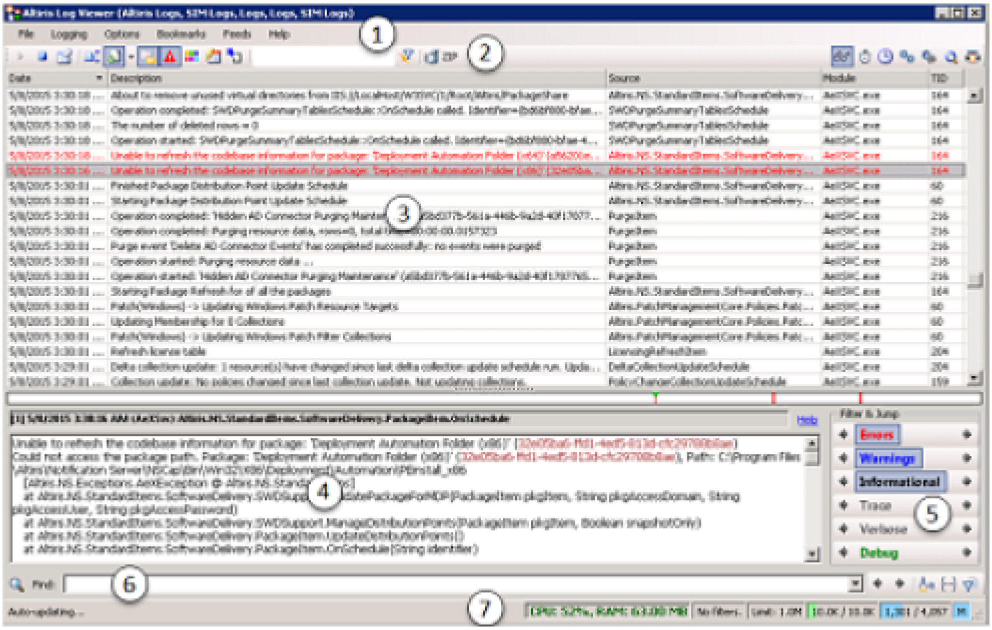


Table 1-1 Sections of the Altiris Log Viewer user interface

Section	Description
Top menu (1)	The top menus let you specify the settings of the Log Viewer and use different ways of analyzing the logs. For example, under **File > Watch Folders**, you can manage the list of folders containing logs that the Log Viewer monitors. You can add or remove the folders and reset to the default logging folders. The Log Viewer Filters under **Options > Filters** help you include or exclude certain types of messages to analyze the NS Logs or Agent Logs. While troubleshooting errors on your Symantec Management Platform, you may have a lot of messages that can cause additional noise on the actual issue. You can then exclude the messages that you already know about or only include the messages that contain a specific word. After you enter the include filters as a list of items separated with semicolons, the grid only shows the log entries that contain these values. You can save the defined filter for later use. The **Item Browser** under **Options > Item Browser** lets you view the details of an item that you have selected in the data grid. You can also search for a specific GUID and see its details. Under **Options > SMP Verbose Levels**, you can adjust the SMP verbosity.
Frequent action icons (2)	The frequent action icons let you quickly start or stop auto-updating, monitor recent files, apply quick filter, and perform other frequently used tasks.

Table 1-1 Sections of the Altiris Log Viewer user interface *(continued)*

Section	Description
Data grid (3)	The data grid on the upper section of the Log Viewer window displays the log file entries. Note that by default only Error, Warning and Information level events are captured. Under **Options > Log Options**, you can specify the severity levels to be logged. You can drag and drop the log files (or folders containing log files) to the data grid to display their content. For each log entry, the following data is displayed: ■ **Date** - The date and time the log entry was made in the log. ■ **Description** - The description of the log entry. ■ **Source** - The name of the source that generated the log entry. ■ **Module** - The module that generated the log entry. ■ **TID** - The ID of the thread within the process that generated the log entry. The right-click menu in the data grid lets you copy, bookmark or filter the log entries. The log entries are colored according to their severity as follows: ■ Errors - red. ■ Warnings - blue. ■ Informational messages - black. ■ Trace and Verbose messages - grey. ■ Debug messages - green.

Table 1-1 Sections of the Altiris Log Viewer user interface *(continued)*

Section	Description
Log entry details (4)	The left section of the bottom pane displays the full details of the log entry that is currently selected in the data grid. The details section displays the following data: ■ **Description** - The description of the log entry. If the description contains a dynamic link, you can click it and open the **Item Browser** to view the details of the current item. ■ **Date** - The date and time the log entry was generated. ■ **Tick Count** - The tick count that the log entry was generated. ■ **Host Name** - The name of the host machine that the log entry was generated on. ■ **Size** - The size of the log entry. ■ **Process** - The name of the process that generated the log entry. ■ **Thread ID** - The ID of the thread within the process that generated the log entry. ■ **Module** - The name of the module within the process that generated the log entry. ■ **Priority** - The severity of the log entry (1 = error, 2 = warning, 4 = informational, 8 = trace, 16 = verbose). ■ **Source** - The name of the source that generated the log entry. ■ **File** - The path and the name of the log file that contains the log entry.
Filters section (5)	The **Filters** section lets you quickly switch on and off the types of the log messages that are displayed in the data grid. The arrows let you jump to the next or the previous log message of this type in the data grid.
Find section (6)	The **Find** section at the bottom of the Log Viewer window lets you search and highlight specific log entries based on the text or a regular expression. All matching items are highlighted in the data grid. The following options let you manage your search: ■ **Search up** - lets you select the next log message that matches the search text. ■ **Search down** - lets you select the previous log message that matches the search text. ■ **Case sensitive search** - lets you specify that the search should be case sensitive. ■ **Use text as regular expression** - lets you specify that the search text is a .NET regular expression. ■ **Text is a set of filters with +/- operators** - lets you add several operators.
Status bar (7)	The status bar at the bottom of the Log Viewer window displays the CPU and RAM usage, allocated buffers, the number of rows, the Log Viewer activity, etc.

Chapter 2

Working with the Altiris™ Log Viewer

This chapter includes the following topics:

Opening the Log Viewer

The 7.5 release of IT Management Suite introduced a new Log Viewer with enhanced usability and functionality.

To open the Log Viewer

- On the Notification Server computer, click **Start**, and then click **All Programs > Symantec > Diagnostics > Altiris Log Viewer**.

  The `LogViewer2.exe` file is located at the following path:

  ```
  …\Program Files\Altiris\Diagnostics
  ```

Configuring the logging severity settings

The Log Viewer lets you specify the types of messages that you want to be logged for your system. After you specify the message severities that you want to log, the Symantec Management Platform is automatically configured to collect the appropriate information and the registry setting for the error logging configuration is changed. Alternatively, you can change the **Severity** regkey value manually in the Registry Editor.

Additionally, you can adjust the amount of **Verbose** level messages that are written into the log for Notification Server or Task Server. Sometimes, if Notification Server has a lot of active client computers, the amount of **Verbose** level messages can be very large. It may then be hard to find particular **Verbose** level messages that you need, such as, for example, the messages related to the schedules. In this situation, you can reduce the amount of **Verbose** level messages that are collected for Notification Server.

To configure the general logging severity settings

1. In the Log Viewer, click **Options > Log Options**.
2. In the **Log Options** dialog box, on the **NS Settings** tab, under **Loggable Severities**, check the severities that you want to log.

   You can also specify if you want to log the information about Symantec Management Platform, about Symantec Management Agent, or both.
3. Click **OK**.

To adjust the amount of Verbose level messages for Notification Server

1. In the Log Viewer, click **Options > SMP Verbose Levels**.
2. In the **SMP Verbose Levels** dialog box, on the tabs, edit the severity levels.
3. Click **Apply**.

To adjust the amount of Verbose level messages for Task Server

1. In the Log Viewer, click **Options > TM Extended Settings**.
2. In the **TM Extended Settings** dialog box, on the tabs, edit the severity levels.
3. Click **Apply**.

To configure the general logging severity settings in the Registry Editor

1. Open the Registry Editor and go to the following location:

   `HKEY_Local_Machine\SOFTARE\Altiris\eXpress\Event Logging\LogFile`.
2. Change the **Severity** regkey value manually.

   By default, the Altiris Log Viewer logs options for the **Severity** regkey with the value of 7. You can change the logging option to value `f` or `ff` in hexadecimal or `255` in decimal, which will log every message option allowed in the Altiris Log Viewer.

The following are the values in decimal for each message type:

- 1 = error
- 2 = warning
- 4 = informational
- 8 = trace
  Note that enabling **Trace** on your NS Logs provides extra information but it is recommended to disable this option after troubleshooting. If the **Trace** option is enabled, the trace entries overwrite the NS Logs very fast and other valuable data might get lost.
- 16 = verbose
- 32 = debug
  The debug messages are the system messages that are not part of the log files. In the Log Viewer process, a special “listener” runs to catch such messages. Note that if you use other tools to catch the debug messages in your system, you should run only one listener at once. If several tools are active at the same time and catching the debug messages, the result for both tools will be inaccurate, because some messages get collected by one tool and some messages by another.

For example:

- Severity = 7 (1 + 2 + 4)
- Severity = 15 (1 + 2 + 4 + 8)

For more information about configuring the logging, see the following Knowledge Base Article: How to configure logging on the Notification Server and an Altiris Agent computer.

Finding the log files

The NS Log files are named `a.log` and the name of the files is incremental: `a1.log`, `a2.log`, etc. The most recent file is `a.log`. The file size can be up to 2000 KB. When the file size reaches this limit, the previous file is automatically archived and renamed to `a1.log`. There can be 200 log files. Once this limit is reached, the oldest log file is overwritten. By default, when the Log Viewer opens, it opens the `a.log` file.

You can change the NS Log settings in the Registry Editor, at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\Event Logging\LogFile
```

The Agent Log files are named `agent.log` and the name of the files is incremental: `agent1.log`, `agent2.log`, etc. The most recent file is `agent.log`. The file size can be up to 200 KB and there can be 50 log files.

You can change the Agent Log settings in the Registry Editor, at the following location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Event Logging\LogFile`

Depending on the version of the Symantec Management Platform that you use, the NS Log files and the Agent Log files are stored in different locations.

Table 2-1 Log types and locations

Log type	SMP version	Location
NS Log	NS 6.0/SMP 7.0	`…\Program Files\Altiris\Notification Server\Logs`
NS Log	SMP 7.x and later	`…\ProgramData\Symantec\SMP\Logs`
Agent Log	NS 6.0	`…\Program Files\Altiris\Altiris Agent\Logs`

Agent Log	SMP 7.x and later	Due to enhanced security in Windows Vista and later operating systems, where the processes that run with User credentials do not have elevated rights to modify files in the `Program Files` location, this path cannot be used.
		Instead, Windows mirrors this location to a virtual store, which appears in `C:\Program Files` for the Log Viewer. The path is specific to the User account under which the process runs, and the created entries are stored under this User profile, at the following location:
		`%UserProfile%\AppData\Local\VirtualStore\Program Files\Altiris\Altiris Agent`
		Because of this security model, in SMP 7.x and later, the default Agent Log path is already in the **User** folder. You can find it in the Registry at `HKLM\SOFTWARE\Altris\Altiris Agent\Event Logging\LogFile`, under the `FilePath` entry. The logs are stored at the following location:
		`C:\Users\Public\Public Documents\Altiris\Altiris Agent\Logs\`

Filtering the log messages

The filtering option lets you search for the log messages in the Log Viewer according to the criteria that you specify. You can filter the messages that contain or do not contain the specified tokens.

The **Exclude** option filters out the log entries that do not contain the tokens that you specify. For example, if you enter **"w3wp;container"**, the log content will display the entries that do not have these tokens in **Description**, **Source**, or **Module** field.

After you remove the irrelevant messages from the log, you can set up additional filtering using the **Include** option. For example, you enter **"operation;delta"**. After you also apply the **Include** tokens to the filter, you get the list of the log messages that do not contain **"w3wp;container"** tokens, and contain **"operation;delta"** tokens in the **Description**, **Source**, or **Module** field.

See “Using advanced filtering” on page 14.

To filter log messages

1. In the Log Viewer, click **Options > Filters**.
2. In the **Log Viewer Filters** dialog box, do the following:
   - In the **Exclude** box, type the tokens that the log messages should not contain.
     If you want to enter multiple tokens, use semicolon to separate the values.
     Note that the more tokens you add in the **Exclude** box, the fewer messages are displayed.
   - (Optional) To see the messages that do not contain the tokens that you entered, click **Apply**.
   - In the **Include** box, type the tokens that the remaining log messages should contain.
     If you want to enter multiple tokens, use semicolon to separate the values.
     Note that the more tokens you add in the **Include** box, the more messages are displayed.
   - Click **Apply**.

   Note: Note that if you apply the **Include** and **Exclude** tokens to the log messages, and close the **Log Viewer Filters** dialog box, the filter still applies to the log. To remove the filter, you must empty the **Include** and **Exclude** boxes, and then click **Apply** once more.

   - (Optional) To save the filter for using it later, click **Save** on the toolbar, specify the name of the file, and then click **Save**.

Using advanced filtering

Simple filtering lets you search for the messages that contain or do not contain the specified tokens in **Description**, **Source**, or **Module** field.

See “Filtering the log messages” on page 13.

Advanced filtering lets you specify more log entry fields where you want to perform the search. The operators and various comparison values let you create a very flexible custom filter.

To define the logical operators, enter the following syntax in the **Include** or **Exclude** sections of the **Log Viewer Filters** dialog box:

```
<Operator1>{

<SmartFilter1>

<Operator2>{

<SmartFilter2>

}

}
```

The syntax supports **AND**, **OR**, and **NOT** operators.

To define the smart filter, use the following syntax:

```
$<Field><Comparison><Value>
```

Table 2-2 Supported values for the filter syntax

Filter item	Supported values
Field	**Field** is a short name of the data field of the log entry. The following short names are supported: ■ **PID** - process ID (numeric) ■ **TID** - thread ID (numeric) ■ **DT** - date time ■ **TM** - time value that is part of the date time ■ **PIN** - process name (text) ■ **SRC** - source (text) ■ **MOD** - module (text) ■ **MSG** - part of the message or description (text) ■ **TXT** - all text fields of the log entry (text) ■ **SEV** - severity level of the log entry (numeric: 1 - error, 2 - warning, 4 - info, 8 - Trace, 16 - Verbose) ■ **SZ** - size of the log entry (numeric)

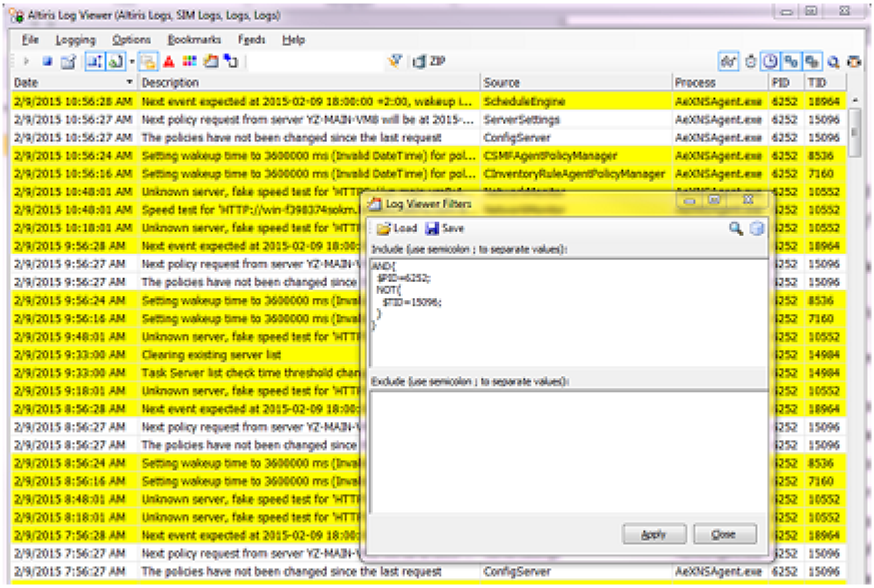
Table 2-2 Supported values for the filter syntax *(continued)*

Filter item	Supported values
Comparison	The following comparisons are supported: ■ **= (==)** equal ■ **~ (~=)** around (partial equality, for text fields it's going to be "contains") ■ **! (!=)** not equal ■ **>** greater ■ **>=** greater or equal ■ **<** less ■ **<=** less or equal ■ **? (?=)** equal to value as a regular expression ■ **?! (?!=)** not equal to value as a regular expression ■ **& (&=)** bitwise AND provide non-zero result ■ **^ (^=)** bitwise AND provide zero result
Value	The value that is used for the comparison. Note that some fields use text values, some numeric values, and some date/time values.

Note: The syntax of the filters is very strict. The operators and the short names of the fields must be uppercase and no extra spaces are allowed in the filter definition.

For example, `$TID=125` is a correct statement, while `$Tid = 125` is not applied as a filter for the **TID** field.

Figure 2-1 Example 1



Altiris Log Viewer (Altiris Logs, SIM Logs, Logs, Logs)
File Logging Options Bookmarks Feeds Help
ZIP
Log Viewer Filters
Load Save
Apply Close

Date	Description	Source	Process	PID	TID
2/9/2015 10:56:28 AM	Next event expected at 2015-02-09 18:00:00 +2:00, wakeup i...	ScheduleEngine	AeXNSAgent.exe	6252	18964
2/9/2015 10:56:27 AM	Next policy request from server YZ-MAIN-VM8 will be at 2015-...	ServerSettings	AeXNSAgent.exe	6252	15096
2/9/2015 10:56:27 AM	The policies have not been changed since the last request	ConfigServer	AeXNSAgent.exe	6252	15096
2/9/2015 10:56:24 AM	Setting wakeup time to 3600000 ms (Invalid DateTime) for pol...	CSMFAgentPolicyManager	AeXNSAgent.exe	6252	8536
2/9/2015 10:56:16 AM	Setting wakeup time to 3600000 ms (Invalid DateTime) for pol...	CInventoryRuleAgentPolicyManager	AeXNSAgent.exe	6252	7160
2/9/2015 10:48:01 AM	Unknown server, fake speed test for 'HTTP			6252	10552
2/9/2015 10:48:01 AM	Speed test for 'HTTP://win-f398374sokm.			252	10552
2/9/2015 10:18:01 AM	Unknown server, fake speed test for 'HTTI			252	10552
2/9/2015 9:56:28 AM	Next event expected at 2015-02-09 18:00:			252	18964
2/9/2015 9:56:27 AM	Next policy request from server YZ-MAIN-V			252	15096
2/9/2015 9:56:27 AM	The policies have not been changed since			252	15096
2/9/2015 9:56:24 AM	Setting wakeup time to 3600000 ms (Inval			252	8536
2/9/2015 9:56:16 AM	Setting wakeup time to 3600000 ms (Inval			252	7160
2/9/2015 9:48:01 AM	Unknown server, fake speed test for 'HTTI			252	10552
2/9/2015 9:33:00 AM	Clearing existing server list			252	14984
2/9/2015 9:33:00 AM	Task Server list check time threshold chan			252	14984
2/9/2015 9:18:01 AM	Unknown server, fake speed test for 'HTTI			252	10552
2/9/2015 8:56:28 AM	Next event expected at 2015-02-09 18:00:			252	18964
2/9/2015 8:56:27 AM	Next policy request from server YZ-MAIN-V			252	15096
2/9/2015 8:56:27 AM	The policies have not been changed since			252	15096
2/9/2015 8:56:24 AM	Setting wakeup time to 3600000 ms (Inval			252	8536
2/9/2015 8:56:16 AM	Setting wakeup time to 3600000 ms (Inval			252	7160
2/9/2015 8:48:01 AM	Unknown server, fake speed test for 'HTTI			252	10552
2/9/2015 8:18:01 AM	Unknown server, fake speed test for 'HTTI			252	10552
2/9/2015 7:56:28 AM	Next event expected at 2015-02-09 18:00:			252	18964
2/9/2015 7:56:27 AM	Next policy request from server YZ-MAIN-V			252	15096
2/9/2015 7:56:27 AM	The policies have not been changed since the last request	ConfigServer	AeXNSAgent.exe	6252	15096

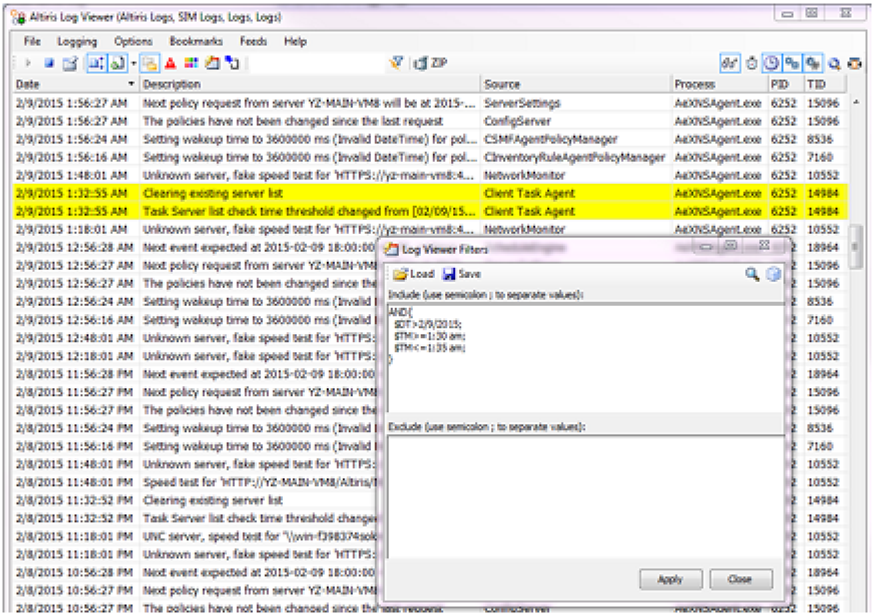
Include (use semicolon ; to separate values):

```
AND{
 $PID=6252;
 NOT{
  $TID=15096;
 }
}
```

Exclude (use semicolon ; to separate values):

The filter in Figure 1 shows to the log entries where the process ID (**PID**) is 6252 and the thread ID (**TID**) is not 15096.

Figure 2-2 Example 2



Date	Description	Source	Process	PID	TID
2/9/2015 1:56:27 AM	Next policy request from server YZ-MAIN-VM8 will be at 2015-...	ServerSettings	AeXNSAgent.exe	6252	15096
2/9/2015 1:56:27 AM	The policies have not been changed since the last request	ConfigServer	AeXNSAgent.exe	6252	15096
2/9/2015 1:56:24 AM	Setting wakeup time to 3600000 ms (Invalid DateTime) for pol...	CSMFAgentPolicyManager	AeXNSAgent.exe	6252	8536
2/9/2015 1:56:16 AM	Setting wakeup time to 3600000 ms (Invalid DateTime) for pol...	CInventoryRuleAgentPolicyManager	AeXNSAgent.exe	6252	7160
2/9/2015 1:48:01 AM	Unknown server, fake speed test for 'HTTPS://yz-main-vm8:4...	NetworkMonitor	AeXNSAgent.exe	6252	10552
2/9/2015 1:32:55 AM	Clearing existing server list	Client Task Agent	AeXNSAgent.exe	6252	14984
2/9/2015 1:32:55 AM	Task Server list check time threshold changed from [02/09/15...	Client Task Agent	AeXNSAgent.exe	6252	14984
2/9/2015 1:18:01 AM	Unknown server, fake speed test for 'HTTPS://yz-main-vm8:4...	NetworkMonitor	AeXNSAgent.exe	6252	10552
2/9/2015 12:56:28 AM	Next event expected at 2015-02-09 18:00:00			2	18964
2/9/2015 12:56:27 AM	Next policy request from server YZ-MAIN-VM8			2	15096
2/9/2015 12:56:27 AM	The policies have not been changed since the			2	15096
2/9/2015 12:56:24 AM	Setting wakeup time to 3600000 ms (Invalid			2	8536
2/9/2015 12:56:16 AM	Setting wakeup time to 3600000 ms (Invalid			2	7160
2/9/2015 12:48:01 AM	Unknown server, fake speed test for 'HTTPS:			2	10552
2/9/2015 12:18:01 AM	Unknown server, fake speed test for 'HTTPS:			2	10552
2/8/2015 11:56:28 PM	Next event expected at 2015-02-09 18:00:00			2	18964
2/8/2015 11:56:27 PM	Next policy request from server YZ-MAIN-VM8			2	15096
2/8/2015 11:56:27 PM	The policies have not been changed since the			2	15096
2/8/2015 11:56:24 PM	Setting wakeup time to 3600000 ms (Invalid			2	8536
2/8/2015 11:56:16 PM	Setting wakeup time to 3600000 ms (Invalid			2	7160
2/8/2015 11:48:01 PM	Unknown server, fake speed test for 'HTTPS:			2	10552
2/8/2015 11:48:01 PM	Speed test for 'HTTP://YZ-MAIN-VM8/Altiris/			2	10552
2/8/2015 11:32:52 PM	Clearing existing server list			2	14984
2/8/2015 11:32:52 PM	Task Server list check time threshold change			2	14984
2/8/2015 11:18:01 PM	UNC server, speed test for '\\win-f398374sok			2	10552
2/8/2015 11:18:01 PM	Unknown server, fake speed test for 'HTTPS:			2	10552
2/8/2015 10:56:28 PM	Next event expected at 2015-02-09 18:00:00			2	18964
2/8/2015 10:56:27 PM	Next policy request from server YZ-MAIN-VM8			2	15096
2/8/2015 10:56:27 PM	The policies have not been changed since the last request	ConfigServer	AeXNSAgent.exe	6252	15096

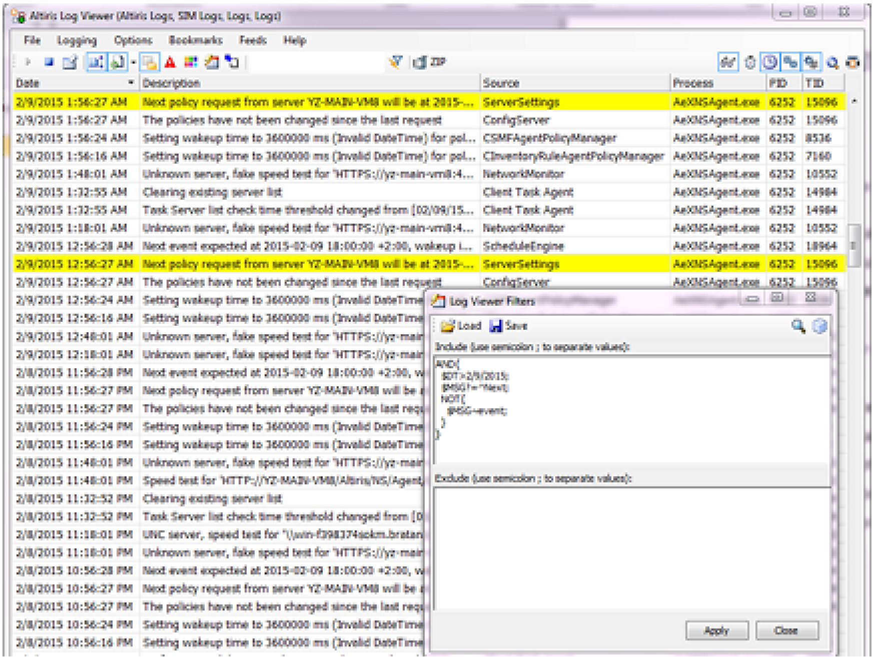
Include (use semicolon ; to separate values):

```
AND{
  $DT>2/9/2015;
  $TM>=1:30 am;
  $TM<=1:35 am;
}
```

Exclude (use semicolon ; to separate values):

The filter in Figure 2 shows to the entries that were logged on 2/9/2015 (**DT**), between 1:30 A.M. and 1:35 A.M. (**TM**).

Figure 2-3 Example 3


Altiris Log Viewer (Altiris Logs, SIM Logs, Logs, Logs)
File
Logging
Options
Bookmarks
Feeds
Help
ZIP
Log Viewer Filters
Load
Save
Include (use semicolon ; to separate values):
Exclude (use semicolon ; to separate values):
Apply
Close

Date	Description	Source	Process	PID	TID
2/9/2015 1:56:27 AM	Next policy request from server YZ-MAIN-VM8 will be at 2015-...	ServerSettings	AeXNSAgent.exe	6252	15096
2/9/2015 1:56:27 AM	The policies have not been changed since the last request	ConfigServer	AeXNSAgent.exe	6252	15096
2/9/2015 1:56:24 AM	Setting wakeup time to 3600000 ms (Invalid DateTime) for pol...	CSMFAgentPolicyManager	AeXNSAgent.exe	6252	8536
2/9/2015 1:56:16 AM	Setting wakeup time to 3600000 ms (Invalid DateTime) for pol...	CInventoryRuleAgentPolicyManager	AeXNSAgent.exe	6252	7160
2/9/2015 1:48:01 AM	Unknown server, fake speed test for 'HTTPS://yz-main-vm8:4...	NetworkMonitor	AeXNSAgent.exe	6252	10552
2/9/2015 1:32:55 AM	Clearing existing server list	Client Task Agent	AeXNSAgent.exe	6252	14984
2/9/2015 1:32:55 AM	Task Server list check time threshold changed from [02/09/15...	Client Task Agent	AeXNSAgent.exe	6252	14984
2/9/2015 1:18:01 AM	Unknown server, fake speed test for 'HTTPS://yz-main-vm8:4...	NetworkMonitor	AeXNSAgent.exe	6252	10552
2/9/2015 12:56:28 AM	Next event expected at 2015-02-09 18:00:00 +2:00, wakeup i...	ScheduleEngine	AeXNSAgent.exe	6252	18964
2/9/2015 12:56:27 AM	Next policy request from server YZ-MAIN-VM8 will be at 2015-...	ServerSettings	AeXNSAgent.exe	6252	15096
2/9/2015 12:56:27 AM	The policies have not been changed since the last request	ConfigServer	AeXNSAgent.exe	6252	15096
2/9/2015 12:56:24 AM	Setting wakeup time to 3600000 ms (Invalid DateTime				
2/9/2015 12:56:16 AM	Setting wakeup time to 3600000 ms (Invalid DateTime				
2/9/2015 12:48:01 AM	Unknown server, fake speed test for 'HTTPS://yz-main				
2/9/2015 12:18:01 AM	Unknown server, fake speed test for 'HTTPS://yz-main				
2/8/2015 11:56:28 PM	Next event expected at 2015-02-09 18:00:00 +2:00, w				
2/8/2015 11:56:27 PM	Next policy request from server YZ-MAIN-VM8 will be a				
2/8/2015 11:56:27 PM	The policies have not been changed since the last requ				
2/8/2015 11:56:24 PM	Setting wakeup time to 3600000 ms (Invalid DateTime				
2/8/2015 11:56:16 PM	Setting wakeup time to 3600000 ms (Invalid DateTime				
2/8/2015 11:48:01 PM	Unknown server, fake speed test for 'HTTPS://yz-main				
2/8/2015 11:48:01 PM	Speed test for 'HTTP://YZ-MAIN-VM8/Altiris/NS/Agent/				
2/8/2015 11:32:52 PM	Clearing existing server list				
2/8/2015 11:32:52 PM	Task Server list check time threshold changed from [0				
2/8/2015 11:18:01 PM	UNC server, speed test for '\\win-f398374sokm.bratan				
2/8/2015 11:18:01 PM	Unknown server, fake speed test for 'HTTPS://yz-main				
2/8/2015 10:56:28 PM	Next event expected at 2015-02-09 18:00:00 +2:00, w				
2/8/2015 10:56:27 PM	Next policy request from server YZ-MAIN-VM8 will be a				
2/8/2015 10:56:27 PM	The policies have not been changed since the last requ				
2/8/2015 10:56:24 PM	Setting wakeup time to 3600000 ms (Invalid DateTime				
2/8/2015 10:56:16 PM	Setting wakeup time to 3600000 ms (Invalid DateTime				

```
AND{
  $DT>2/9/2015;
  $MSG!=^Next;
  NOT{
    $MSG~event;
  }
}
```

The filter in Figure 3 shows the entries that were logged on 2/9/2015 (**DT**) and where the description field (**MSG**) of the log entry contains the token "Next", and does not contain the token "event".

Working with the bookmarks

Bookmarks let you quickly find the items that you have saved for later use. You can toggle bookmarks in the log that you currently view. You can also export the bookmarks and view them later.

To set the bookmarks

- In the Log Viewer, right-click the log message in data grid, and then click **Toggle Bookmark**.

  The log message that is set as a bookmark has a red triangle in the upper left corner of the **Date** field.

To work with the bookmarks

- In the Log Viewer, do one of the following:

To move to the next bookmark.	Right-click the log message in data grid, and then click **Go to next Bookmark**. You can also use the keyboard shortcuts to jump between the bookmarks. See “Altiris Log Viewer keyboard shortcuts” on page 23.
To export the bookmarks.	■ Set the bookmarks for the log entries that you want to export. ■ On the top menu, click **Bookmarks > Export**. ■ In the **Save As** dialog box, specify the location and the name of the file, and then click **Save**. The file is saved with the `.lvbm` extension.
To import the bookmarks.	■ On the top menu, click **Bookmarks > Import**. ■ In the **Open** dialog box, locate the bookmarks file with the `.lvbm` extension, and then click **Open**.
To clear the bookmarks.	Right-click the data grid area, and then click **Clear all bookmarks**.

Viewing the remote log feed

Altiris Log Viewer lets you view the log feeds of the remote computers. To view the log of a computer remotely, you must start the remote log feed on this computer.

To view the remote log feed

1. On the computer for which you want to view the log remotely, open the Log Viewer, and then do the following:
   - Click **Feeds > Start Remote Log Feed**.
   - In the **Start Remote Log Feed** dialog box, specify the necessary options, and then click **Start**.
     Note that you can also use the command line options to start the remote log feed.
     See “Command line options” on page 24.
2. On the computer where you view the remote log, open the Log Viewer.
3. In the Log Viewer, click **Feeds > Remote Log Feeds**.
4. In the **Remote Log Feeds** dialog box, do the following:

To add a new remote computer.	■ Click **Add**. ■ In the **New feed** dialog box, specify the data of the remote computer and the severity level of the log messages that you want to collect. You must enter the same port and password that you specified on the remote computer when starting the remote log feed in step 1. ■ Click **Connect**.
To view the remote log feed of a previously defined computer.	Select the remote computer from the list, and then click **OK**.

5 (Optional) To solve the GUID-s in the remote log messages, do the following:

- In the Log Viewer, click **Options > Log Options**.
- In the **Log Options** dialog box, on the **Remote DB** tab, specify the details for connecting to the remote database.
- Click **OK**.

Walking the log files

The **Walk Log Files** feature lets you browse through the multiple log files and search for specific tokens.

To walk the log files

1 In the Log Viewer, click **File > Walk Log Files**.

2 In the **Walk Log Files** dialog box, click **Get Files**.

This option loads the log files from the default location only.

3 (Optional) To add files from custom locations, click **+Folders** or **+Files**.

4 (Optional) Check the boxes for the following options:

Only selected files Lets you search within the selected files only.

Match case Lets you search for the items with matching token case.

Regex Lets you search for the items by regular expression.

Prescan If this option is checked, the file that is currently scanned is entirely loaded into the memory in text format and quick search is performed. If the token is not found, the next file is loaded.

Lookaround +/- entries for fetch When the token you are looking for is found, the messages before and after this log entry are shown in the result window. Check this box if you want to see the context of this log entry.

5 In the **Find** box, type the token that you want to find, and then click the **Search** icon.

Keyboard Shortcuts

This appendix includes the following topics:

- Altiris Log Viewer keyboard shortcuts

Altiris Log Viewer keyboard shortcuts

Altiris Log Viewer provides you with a set of keyboard shortcuts.

Table A-1 Keyboard shortcuts

Shortcut	Description
Home	Lets you jump to the first (latest) line and enables auto-scroll.
ALT+Q	Lets you automatically resize column widths.
CTRL + F2	Lets you toggle bookmarks.
F2	Lets you walk through the bookmarks.
CLTR + SHIFT + F2	Lets you clear all bookmarks.

Appendix B

Command line options

This appendix includes the following topics:

- Command line options

Command line options

Using the command line options, you can open the Log Viewer in the following modes:

- `-v` opens the Log Viewer in log viewer mode. (Default.)
- `-f` opens the Log Viewer in log feed source mode.
  If you open the Log Viewer on Notification Server in log feed source mode, it will monitor the log and send the information to peers. The peers are the Log Viewers that run on the external computers. These computers can securely connect to Notification Server and receive the log content from the source Log Viewer.

The supported command line options for each mode are as follows:

```
LogViewer [ -v ] [ -a | -r | -c | -i ]* [ <folder> | <file> ]*
```

```
LogViewer -f [ -e | -q | -l <port> | -p <password> ]* [ <folder> ]*
```

Table B-1 Log Viewer Mode Options

Option	Description
`-a`	Start with auto-scroll on.
`-r`	Start with recursive (sub-folder) monitoring on.
`-c`	Clear persistent data store on load.
`-i`	Start with auto-updating off (idle).

Table B-2 Log Feed Source Mode Options

Option	Description
`-e`	Use encryption to protect the feed.
`-q`	Quiet mode.
`-l <port>`	Listen on the specified port instead of the default.
`-p <password>`	Require the given password to access the feed.

The following examples explain the usage of the command line options:

- `LogViewer -a -i C:\Temp\Logs`

  This command starts the Altiris Log Viewer in log viewer mode, with auto-scroll on and auto-updating off. The given folder (C:\Temp\Logs) is monitored instead of the default NS log folder.

- `LogViewer -f -p PasswordHere`

  This command starts the Altiris Log Viewer in log feed source mode, with the password **PasswordHere**. The specified password must be provided to access the log feed.

- `LogViewer -f -e C:\Temp\Logs`

  This command starts the Altiris Log Viewer in log feed source mode for the given folder (C:\Temp\Logs). Encryption is used to protect the log feed, but no password is required.

FAQ

This appendix includes the following topics:

- Altiris Log Viewer FAQ

Altiris Log Viewer FAQ

What do I do with the information in the Log Viewer?

After you identify the errors or warnings in the Log Viewer, copy the main part of the error message from the bottom window and search the Knowledge Base for any articles on how to correct the error. Sometimes, an error might appear in the log, but it does not cause any problems in your environment. However, if you have a problem, the error in the log helps you identify it. The Warning messages provide information that help you avoid problems that may develop if no action is taken.

The following examples show you different messages:

- **Unable to open a handle to Service 'Altiris Agent for Mac Service'. Error 424.**
  This is an error message and appears in red. However, if you have no Mac computers in you environment, the error message does not really indicate a problem.
- **The server is currently paused and will not process any create resource requests.**
  This is a warning message and is displayed in blue. This could cause problems if the server does not start soon. The requests would continue to back up, and the network and the server would start to slow down and could affect the whole network.

How do I know if the information in the Log Viewer is valid?

The only way to know if the information is valid is to search for the error/warning message in the Symantec Knowledge Base and see if the results indicate that you need to take some action. The first priority should be the error messages, and then the warnings. If you have problems with the Altiris environment and cannot find an article in the Knowledge Base, you need to open an incident with the support.