Getting Started with Audit

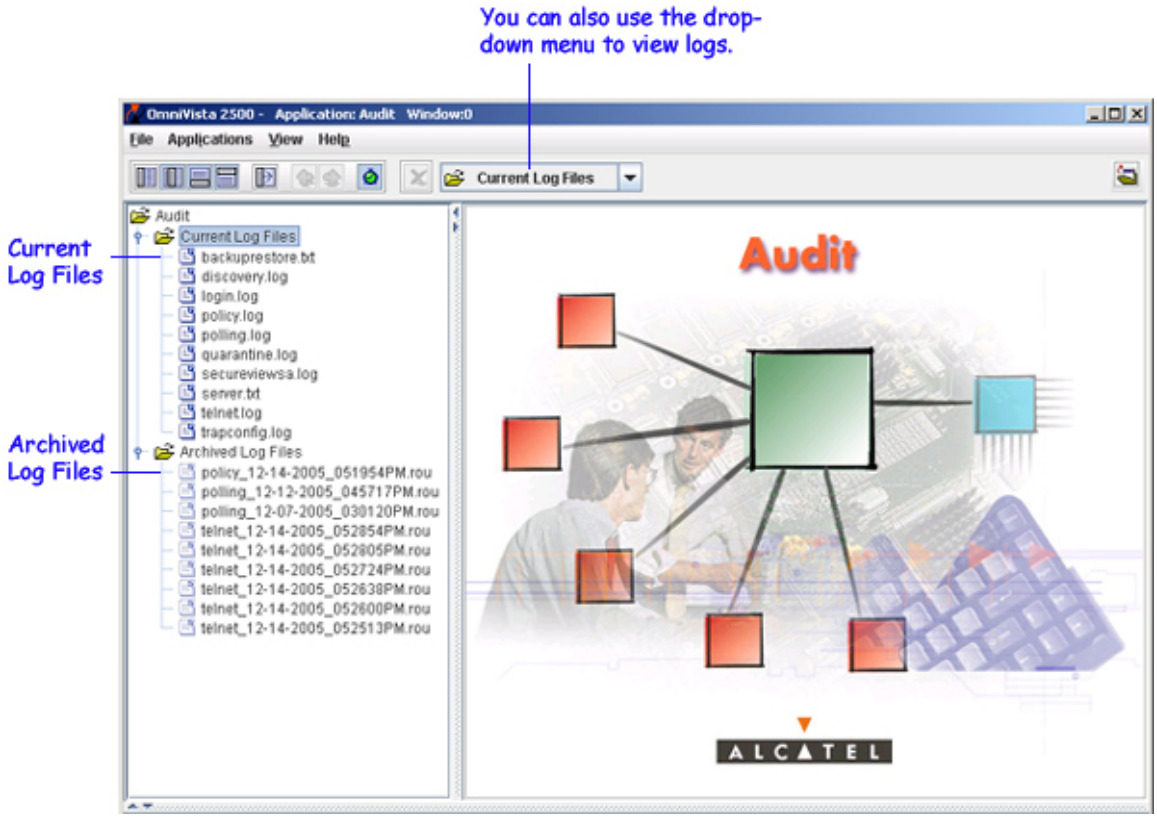
Use the Audit application to monitor client and server activity, such as the date and time when a user logged into OmniVista, when an item was added to the discovery database, when a configuration file was saved, when a particular application was launched, etc. OmniVista organizes this information and stores it in the following log files:

- **accounting.log** - a record of all accounting activity
- **appaccess.log** - time and day users accessed a particular application
- **backuprestore.txt** - a record of all backup and restore activity
- **config.log** - a record of all save configuration activity
- **discovery.log** - a record of all discovery activity
- **login.log** - time and day users logged into OmniVista and whether or not login attempts were successful
- **policy.log** - a record of all policy activity
- **polling.log** - a record of all switch polling activity
- **quarantine.log** - a record of all Quarantine Manager activity
- **secureviewsa.log** - a record of all authentication server configuration activity
- **server.txt** - a record of all server activity
- **statistics.log -** a record of all Statistics activity
- **syslog.log -** a record of system events
- **telnet.log** - a record of all telnet activity
- **trapconfig.log** - a record of all trap configuration activity
- **trap.txt -** a record of all traps received
- **vlan.log -** a record of all VLAN activity.

Note: The **traps.txt** file will not be listed under **Current Log Files**. It will be located in installation directory/data/logs.

All logs are dynamically updated; and, with the exception of the **server.txt** file, each of the log files can be archived, exported to a .txt file, or deleted.

The Audit tree control displays two types of log files: **Current Log Files** and **Archived Log Files**.

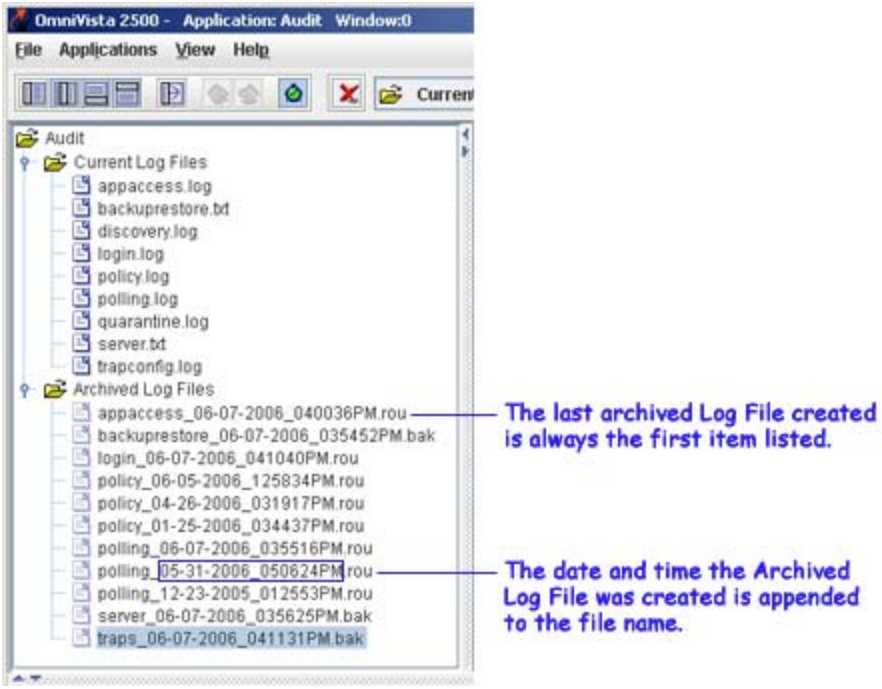


Current Log Files

Current Log Files record current user activity, such as the date and time when a user logged in, when a configuration file was saved, when a discovery item was added , etc. If a supported log file type does not appear under Current Log Files, then no activity has occurred for that particular feature since the last time the file was archived or since OmniVista was first installed. For example, if the **vlan.log** file is not listed under Current Log Files, then no OmniVista VLANs application activity has occurred since the last time the **vlan.log** file was archived. In addition, a log file does not exist for applications that are not included in the current OmniVista installation.

Archived Log Files

When a Current Log File is archived, an Archived Log File is created that is a copy of the Current Log File (log files are appended with a ".rou" extension, text files are appended with a ".bak" extension) . The Archived Log File has the same filename as the Current Log File but the date and time the file was archived is appended to the filename. For example, if you archive the **appaccess.log** file, a copy of this log is created and saved under the name **appaccess_06-07-2006_040036PM**, as shown in the diagram below.

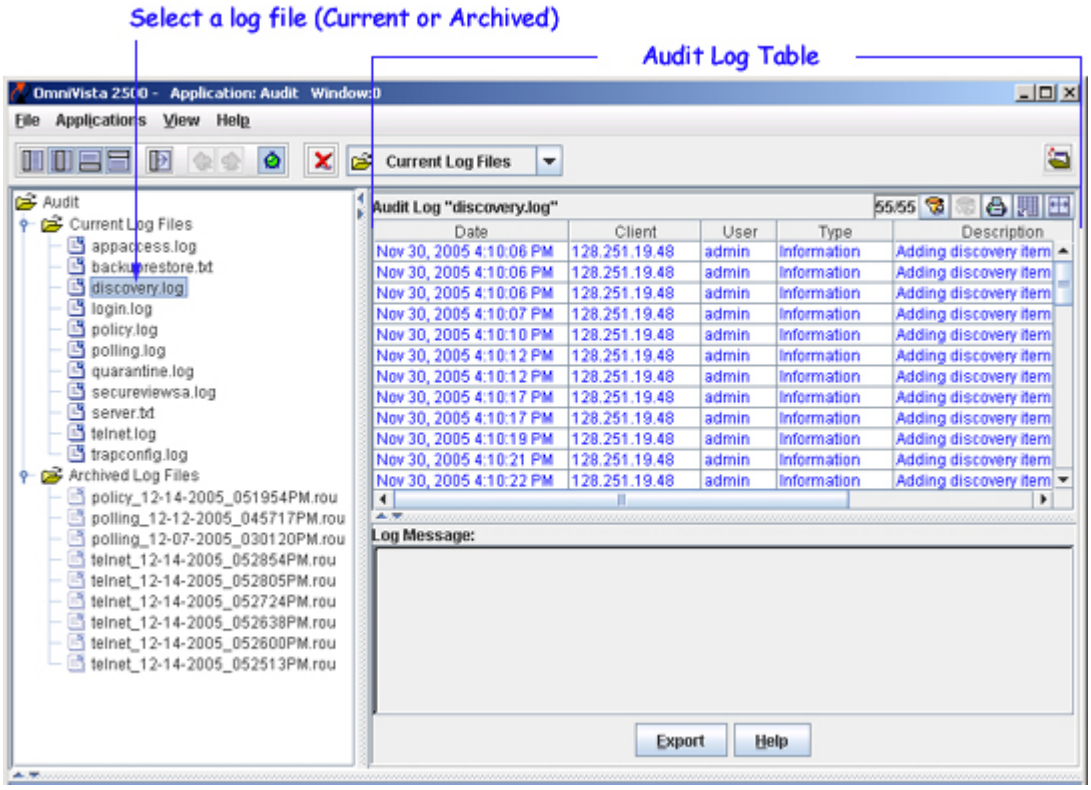


To learn how to archive a Current Log File, see Archiving Log Files.

You can set the maximum number of entries that can exist in the log files, and also set the maximum size of the **server.txt** file. Click on the **File** menu, select **Preferences,** and then click **Audit Log Size** to access the Audit Preferences panel. The maximum number of entries that you configure applies to all log files. When a Current Log File reaches the configured maximum number of entries, OmniVista automatically archives a copy of the file to the Archived Log Files folder.

Viewing Log Files

To view either a Current Log File or an Archived Log File, select the file from the tree control or the drop-down menu, then view the information in the adjacent window. The example below shows how to view a Current Log File. See Field Definitions for a description of each of the log file fields.



Field Definitions

Date. The date and time when the event occurred. For example, the date and time when the user logged in, the date and time when a configuration file was saved, etc.

Client. The IP address of the OmniVista client that initiated this action.

User. The login name of the user associated with this entry. OmniVista's pre-defined user names include **admin**, **netadmin**, **user**, and **writer**.

Type. Three message types are available: **Information**, **Warning**, and **Error**.

- **Information**. Indicates that an action was initiated or successfully completed (e.g., "Begin saving configuration").
- **Warning**. Indicates that a user action was unsuccessful, or that there was a change to the system (e.g., "Failed login attempt).
- **Error**. Indicates a system or application problem (e.g., a log message telling you that a device went down, or that that there was no response from the device).

Description. For **login.log**, the description might be the status of the login ("Successful login") or the type of user change ("Update group"). For **discovery.log**, the description might be the name of the discovered switch, including its IP address and who has access privileges to it ("Writing discovery item [10.255.11.127 PR-5200 (-Everyone-)]").

Switch IP Address. The management IP address that identifies the switch on which the event occurred.

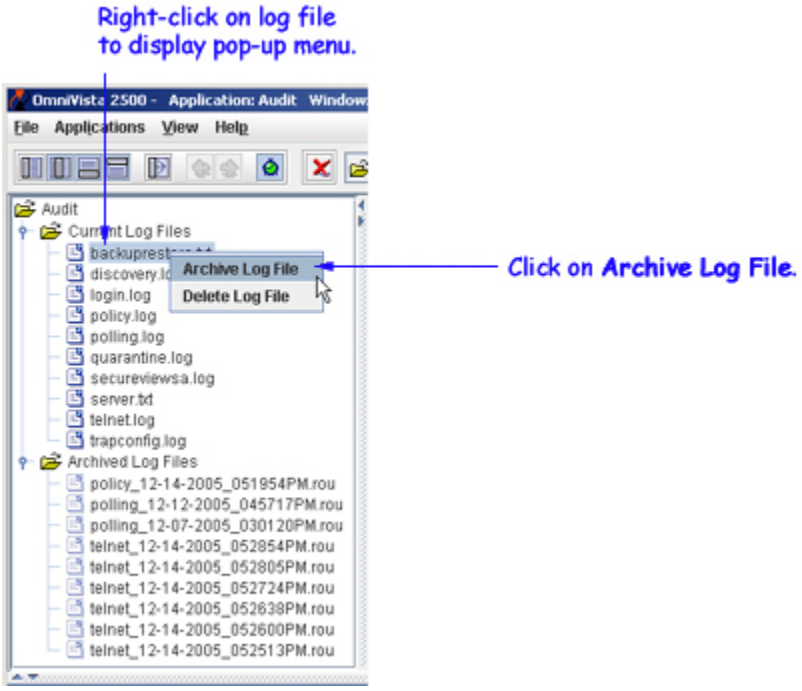
Archiving Log Files

Follow the steps below to archive a log file.

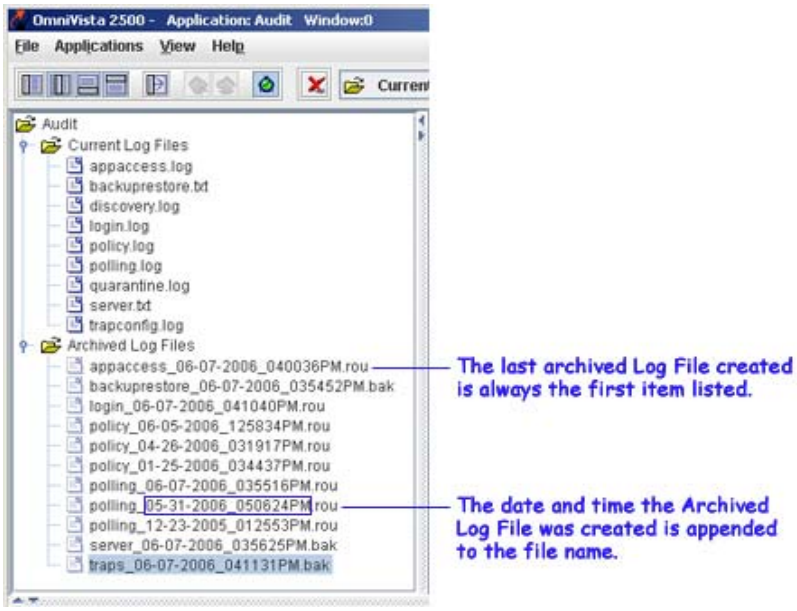
1. Select the log file you want to archive from the Current Log Files list.

2. Right-click on the log file to display the Audit control tree pop-up menu, as shown below.

3. Click on **Archive Log File**.



When a Current Log File is archived, an Archived Log File is created that is a copy of the Current Log File (log files are appended with a ".rou" extension, text files are appended with a ".bak" extension) . The Archived Log File has the same filename as the Current Log File but the date and time the file was archived is appended to the filename. For example, if you archive the **appaccess.log** file, a copy of this log is created and saved under the name **appaccess_07-22-2004_035519PM**, as shown in the diagram below.



When you archive a log file, the file is removed from the Current Log Files folder and archived to the Archived Log Files folder. A new log file will be created in the Current Log Files Folder when any logging activity occurs. For example, a new "appaccess.log" file will be created the first time you access another OmniVista application.

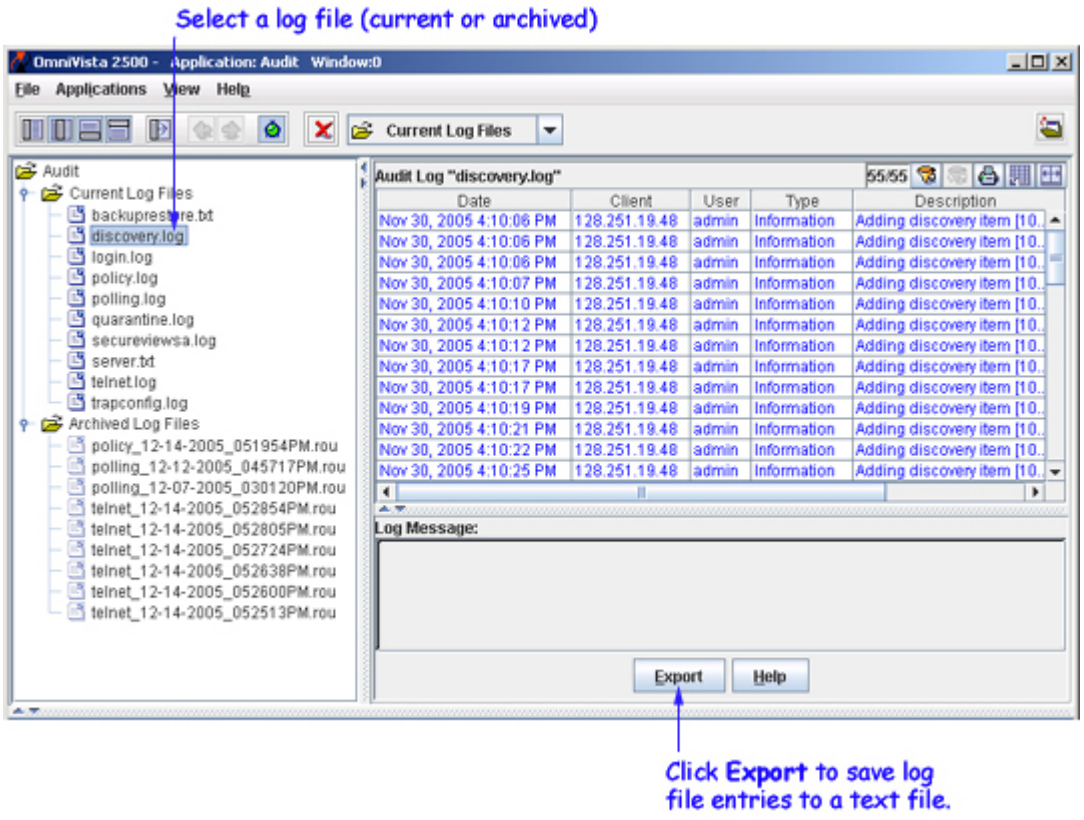
You can set the maximum number of entries that can exist in the log files, and also set the maximum size of the server.txt file. Click on the **File** menu, select **Preferences,** then click on **Audit Log Size** to access the Audit Preferences window. The maximum number of entries that you configure applies to all log files. When a Current Log File reaches the configured maximum number of entries, OmniVista automatically archives a copy of the file to the Archived Log Files folder.

Exporting Log Files

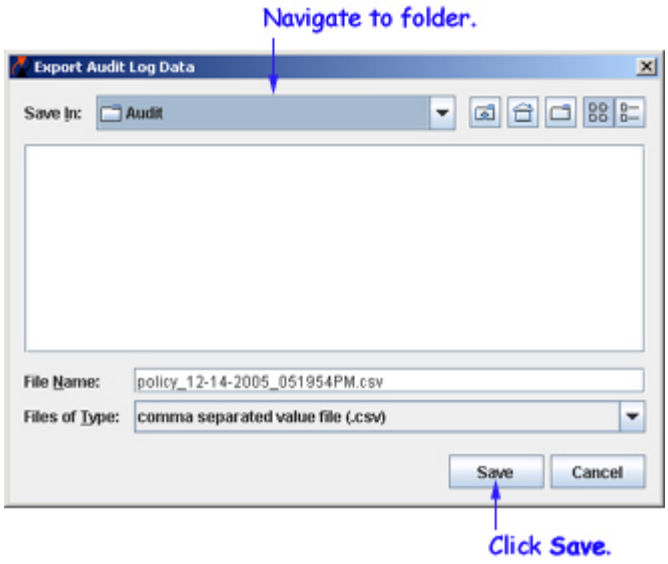
Log file information can be saved and made available for viewing at a later time by exporting it to a .txt file. You can export both Current Log Files and Archived Log Files. After the information is exported, it can be viewed through any text processor. When viewed through a spreadsheet program, the data can also be sorted and filtered as needed. Follow the steps below to export a log file.

1. Select the log file you want to export.

2. Click on the **Export** button, as shown below.



After you click on the **Export** button, the Export Audit Log Data window appears.



3. Navigate to the drive and folder where you want to save the log file, accept the default filename or enter a new filename, then click **Save**.

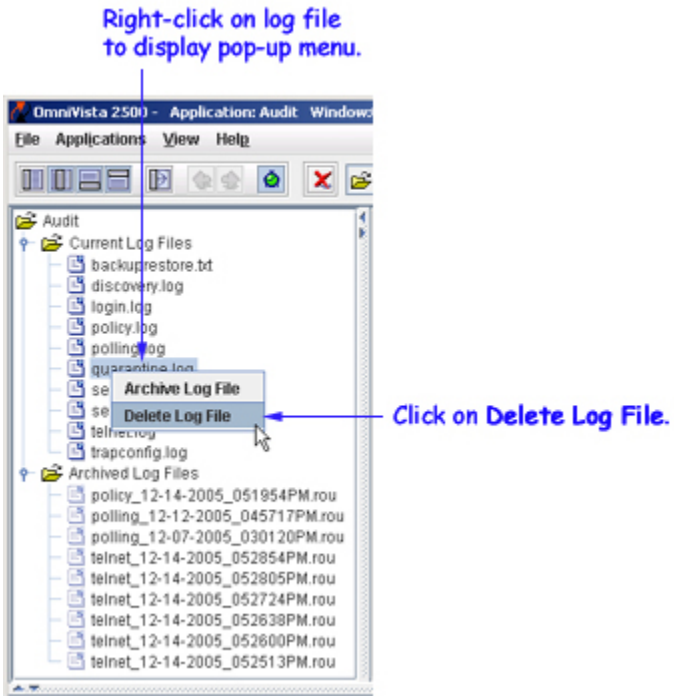
Deleting Log Files

Follow the steps below to delete a log file.

1. Select the log file you want to delete.

2. Right-click on the log file to display the Audit control tree pop-up menu, as shown below.

3. Click on **Delete Log File**. A confirmation box will display, giving you the opportunity to confirm or cancel your action.



In the above example, a Current Log File was selected. However, you can delete Current Log Files and Archived Log Files.

To delete more than one file at a time, use the **Shift** or **Ctrl** keys to select multiple files.