

# Using AuditLogin v3.2

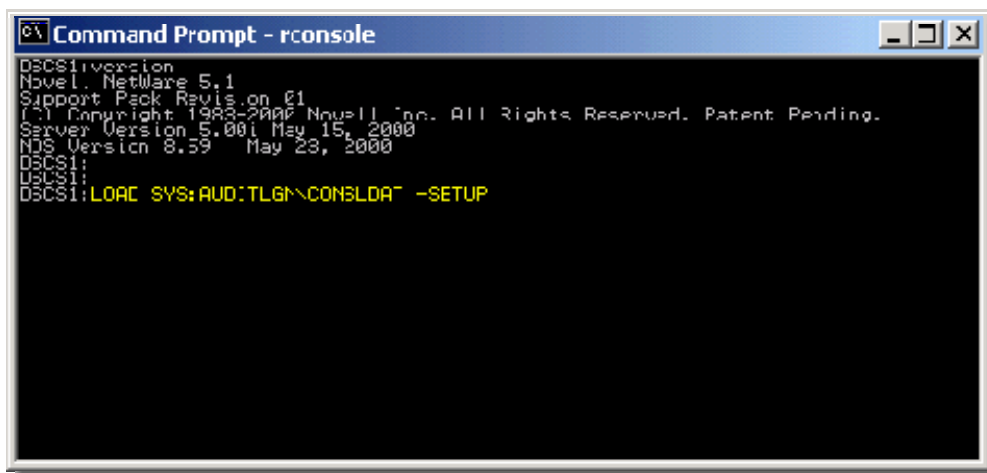
## Install

### Cookbook Installation:

This installation is designed to not take more than 5 minutes, even if you have never seen AuditLogin before.

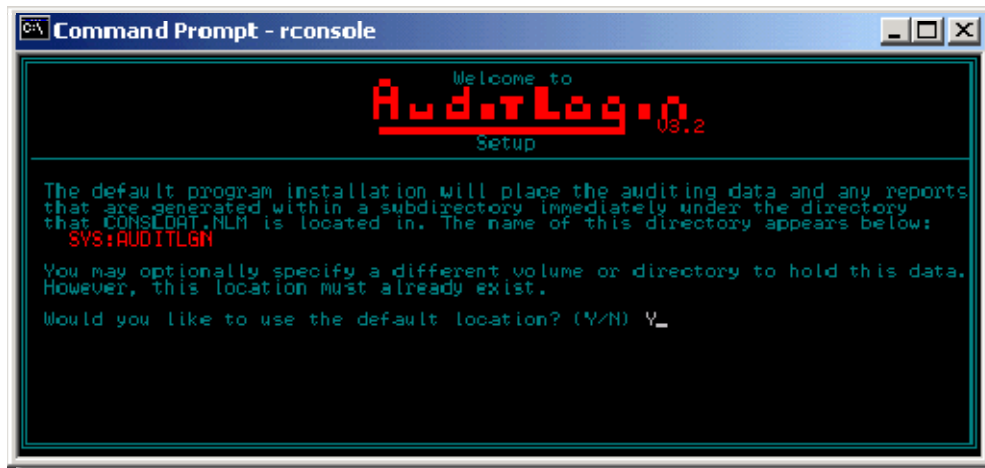
1. Select a server to serve as the consolidator. This will run the consolidation NLM named CONSLDAT.NLM. If you are unsure as to what this is, see the [component overview page](#). This server does not need to be very high in power, especially if you are going to be auditing fewer than 20 servers with a moderate amount of activity.
2. Create a directory to hold the NLMs. This is referred to as the distribution directory. Rules for this directory are:
  - o You must select a volume that is present on all servers that you might want to audit (ex: SYS). The directory takes very little disk space and you have to option of storing the auditing data on a different volume. Take a moment to review the section on [AuditLogin Version 3.2 Directory Placement](#).
  - o To maintain compatibility across NetWare versions, Long filenames in the path are not currently supported so do not use them. (Example: SYS:AUDITLGN)
3. Unzip the distribution package into the directory that you just created. The following are the principle files in the distribution:
  - o CONSLDAT.NLM - the consolidation NLM.
  - o AUDITLGN.NLM - the system monitoring NLM.
  - o AUDITADM.EXE - Win32 administrator tool.
4. On the server console, load the consolidator with the -SETUP option.

Example: "LOAD SYS:AUDITLGN\CONSLDAT.NLM -SETUP")



```
Command Prompt - rconsole
DSCSIversion
Novel. NetWare 5.1
Support Pack Revision 01
© Copyright 1988-2000 Novell, Inc. All Rights Reserved. Patent Pending.
Server Version 5.00i May 15, 2000
NDS Version 8.39 May 23, 2000
DSCSI:
DSCSI:
DSCSI:LOAD SYS:AUDITLGN\CONSLDAT.NLM -SETUP
```

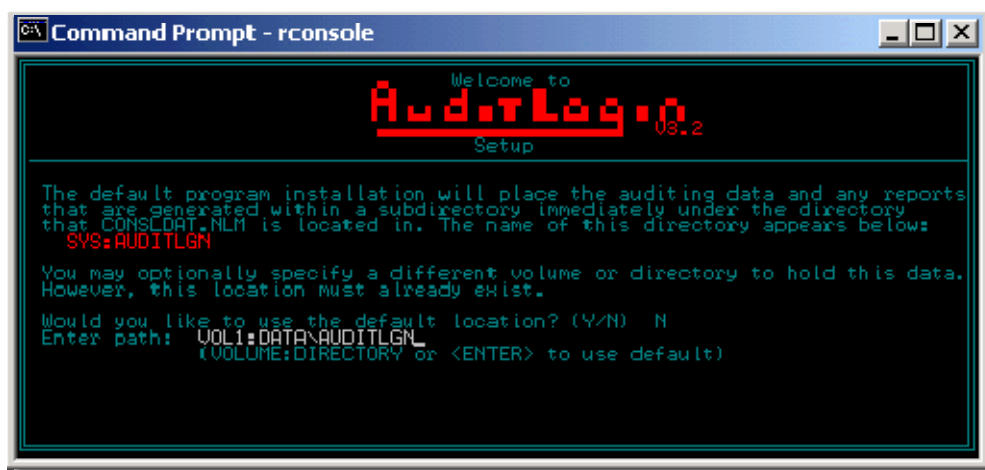
5. You will be asked to select a location on the server in which to store the auditing data files.



If Yes is selected, the auditing data will be placed in a subdirectory of the master directory and you will proceed to step 6 below.

If you want to change the location of these files later, you may do so using the Admin tool. For more information, see the section on [AuditLog Version 3.2 Directory Placement](#).

If No is selected, you will be prompted to enter the path of the directory (which must already exist):



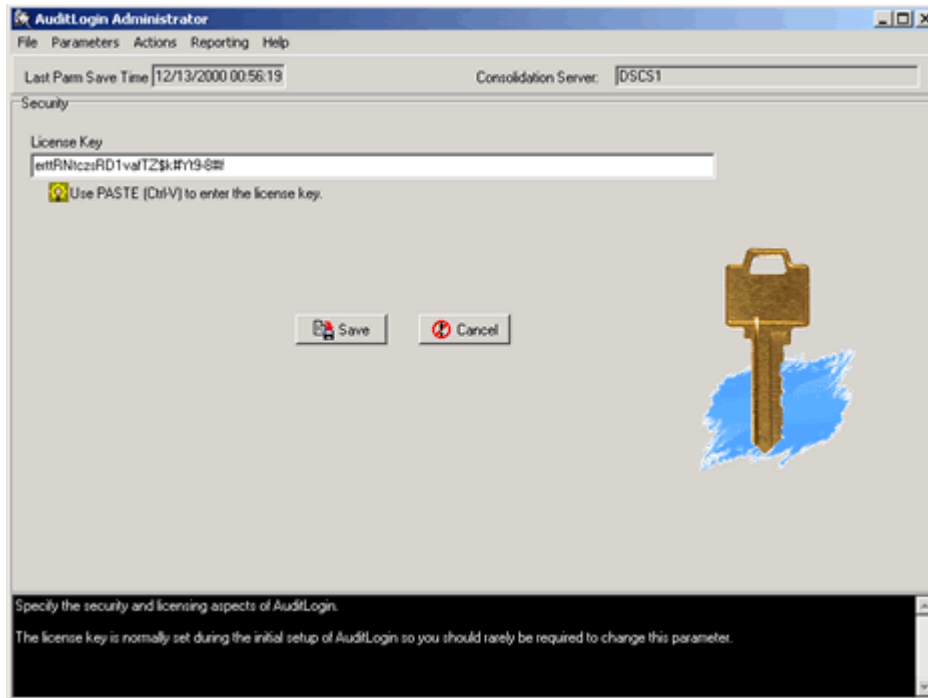
6. You will be prompted to agree to complete the installation.

```
Command Prompt - rconsole
Welcome to
AuditLog V3.2
Setup
Setup will perform operations to complete the installation.
1. Creating AuditLogin V3 initialization file.
2. Creating AUDITLOG directory to contain consolidated auditing logs.
3. Creating batch file to start Win32 Administrator application.
4. Creating STATS directory to contain consolidated statistics logs.
5. Creating REPORTS directory to contain customized reports.
Perform above actions? (Y/N) Y_
```

If you agree, the following actions will be taken:

- The system parameter file will be created to allow for further product installation. This file is named AUDITLGN.INI and will be placed in the *master directory*. All system parameter defaults will be set and a special license key "Initialize" will be set.
  - A subdirectory named AUDITLOG will be created in the log directory. This is where the system will place auditing data that is sent in from all servers running the system monitoring NLM (AUDITLGN.NLM).
  - A DOS batch file named GOADMIN.BAT will be created to allow you to continue the installation by starting the Win32-based Administration program. The batch file will start the Admin tool with the required -S option to specify the name of consolidation server.
  - A subdirectory named STATS will be created in the log directory. This is where the system will place statistical information that is sent in from servers running the system monitoring NLM.
  - A subdirectory named REPORTS will be created in the log directory. When someone requests that a report be generated, this is where the report will be stored.
7. After completing the initial setup, the consolidation NLM will finish initialization in setup mode. Until you use the Administrator to set the license key, the Consolidator will not be able to receive auditing data from any servers. Here is a screen shot of the consolidator in this state:

8. Now you will need to set the license key and other operating parameters. To do this you will need to start the Win32-based Admin tool. You can do this a number of ways:
  - o Click on the GOADMIN.BAT file.
  - o Start->Run with the required -S option specifying the name of the server running the consolidation NLM.
  - o Create a NetWare Application Launcher application object that specified the above parameter.
9. When the tool starts, you should be shown the Security page where you can PASTE in the product license key.



10. Paste in the license key and click "Save". If the license key is invalid, you will be informed at this point. Contact [support](#) if you have problems with the license key.
11. (optional) Add the LOAD command for the consolidator to the AUTOEXEC.NCF file for the consolidation server. (Ex: "LOAD SYS:AUDITLGN\CONSLDAT.NLM")
12. You now need to enable auditing on one or more servers by selecting "[Audited Servers...](#)" under the "Parameters" menu option.
13. At this point, AuditLogin is setup in a base configuration.
14. Refer to the configuration section for information on other parameters or configuring other servers to run the system monitoring NLM (AUDITLGN.NLM)

# AuditLogin v3.2

## Upgrade

### Upgrading from Version 2.x

V3 is much easier to deal with than V2 was. The NLMs are named the same, but that is where the similarities end. Use the following procedure to remove V2:

1. Shutdown the V2 CONSLDAT NLM and remove the consolidator LOAD command (if present) from AUTOEXEC.NCF.
2. Shutdown the V2 AUDITLGN NLM on all servers and remove the LOAD AUDITLGN or NCF invocation commands from AUTOEXEC.NCF.
3. If desired, save your V2 auditing logs somewhere else.
4. Remove the entire V2 installation directory.
5. Follow the instructions for a "New Install" for V3.

### Upgrading from Version 3.0

The name of the NCP extension has changed from 3.0, so you will need to upgrade AUDITLGN NLM on the servers as quickly as possible after upgrading the distribution and restarting the CONSLDAT NLM.

Perform the following steps:

1. Ensure that all servers running the AUDITLGN NLM are indicating that the consolidator NLM is up and communication is occurring correctly.
2. Expand the ZIP file into your 3.0 distribution directory on your consolidation server.
3. Re-load the consolidation NLM (CONSLDAT.NLM). On startup, it will perform all upgrade tasks necessary for V3.1 on the consolidation server.
4. Start the V3.1 Admin win32 application and click on "Parameters" and "Audited Servers..". Highlight all servers being audited and click on "Upgrade NLM".
5. Verify that the V3.1 AUDITLGN NLM is running correctly on all audited servers.

### Upgrading from Version 3.1

Upgrading from Version 3.1 is very simple since there are no interoperability issues between the NLMs from version 3.1 to 3.2. Follow the normal process for applying maintenance to AuditLogin:

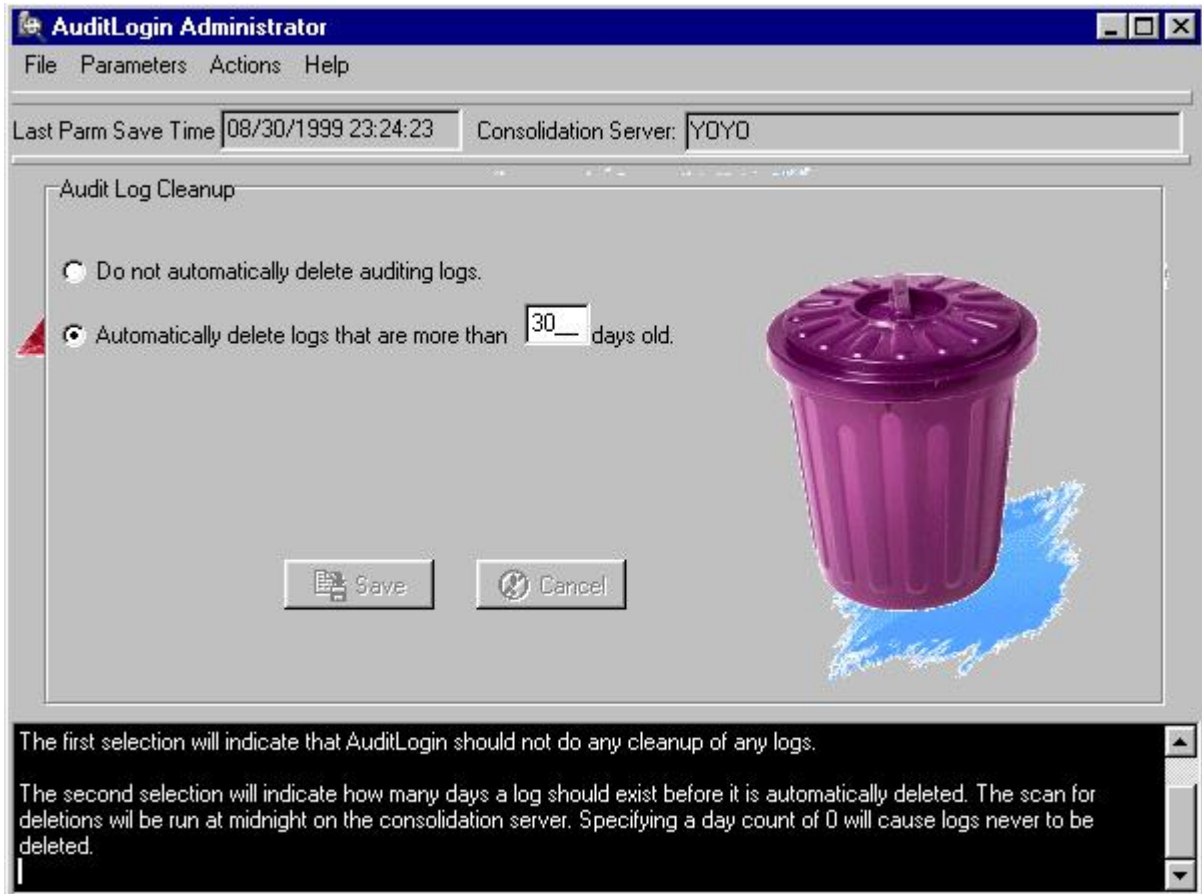
1. Unzip the 3.2 in the master directory on your consolidation server. (ex: SYS:AUDITLGN)
2. Restart CONSLDAT.NLM on the consolidation server.

3. Use the Windows Admin tool to distribute and restart AUDITLGN.NLM on all audited servers.

# AuditLogin v3.2

## Log Cleanup

The logs of auditing data compiled by AuditLogin can be automatically managed by the system.

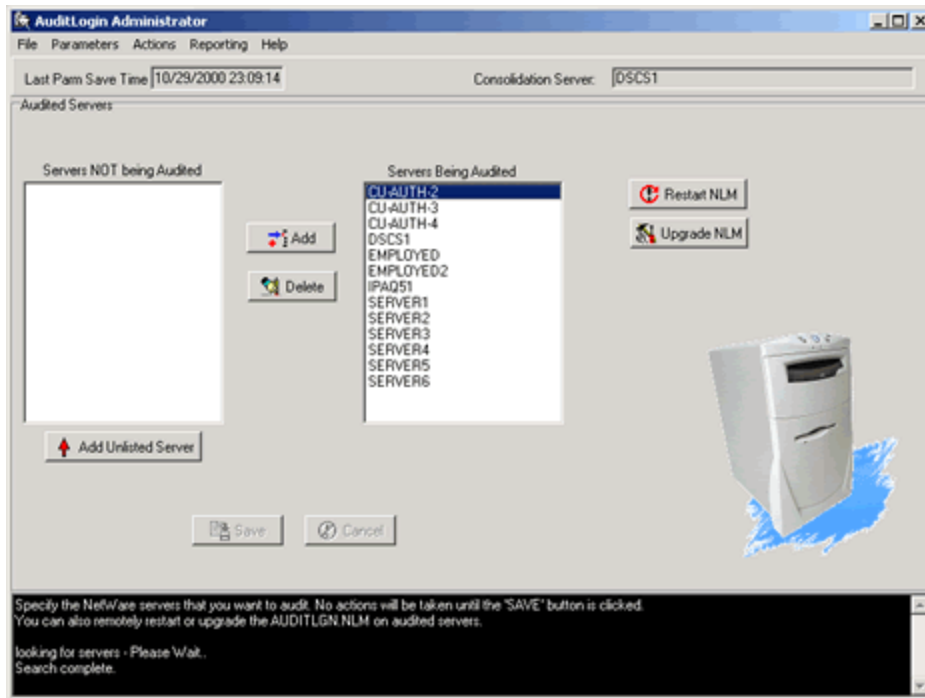


At your discretion, the logs can be cleaned up (deleted) by the consolidator after a specified period of time. Log file names are of the form YYYYMMDD.00x. The deletion is done based on the name of the file and not based on time stamps on the files themselves. If enabled, the search for and deletion of old auditing files is done each time a scheduled file sort is done.

# AuditLogin v3.2

## Audited Servers

While not merely a configuration parameter, the names of the servers running the system monitoring NLM (AUDITLGN.NLM) is maintained by the Admin tool. The servers are not only named here, but the servers are actually remotely configured to run the NLM.



There are two action buttons which are active unless the contents of the "Servers Being Audited" window is changed:

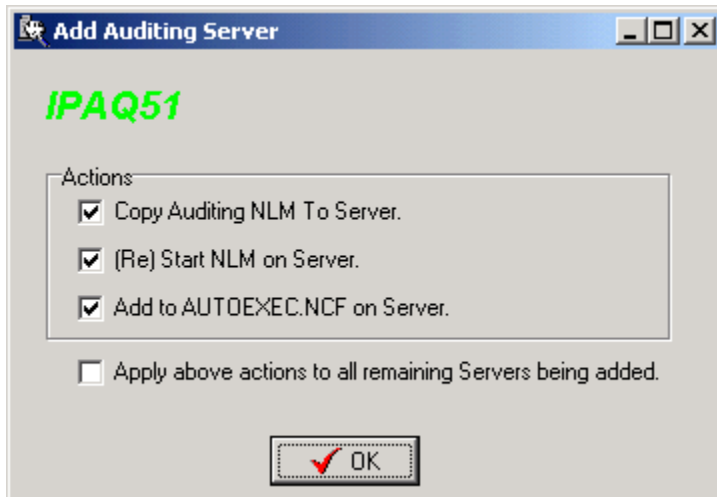
- **Restart NLM** - This will make a connection to the server(s) selected in the "Servers Being Audited" window and remotely attempt to UNLOAD and then LOAD AUDITLGN.NLM on each server. If the NLM is not already loaded, only the LOAD will occur.
- **Upgrade NLM** - This will copy AUDITLGN.NLM from the consolidation server master directory to the server(s) selected in the "Servers Being Audited" window and remotely attempt to UNLOAD and then LOAD AUDITLGN.NLM on each server. If the NLM is not already loaded, only the LOAD will occur.

There are two window panes:

- Servers Not Being Audited
- Servers Being Audited

You can select one or more servers from either window for transfer into the other column using the **Add** and **Delete** buttons. However, no action is taken until the **Save** button is clicked.

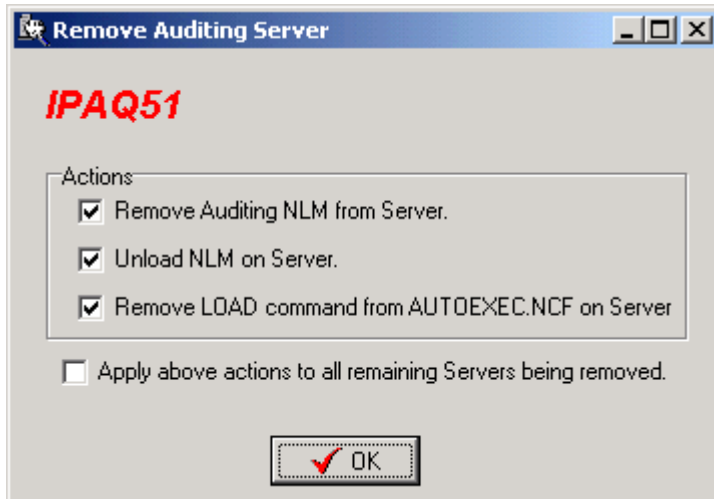
When the **Save** button is clicked, any servers that were not being audited prior to the operation are dealt with first.



Besides adding the server to the configuration, the Admin tool will optionally:

- Copy the NLM from the distribution on the consolidator to the remote server. The same directory path as the one containing the distribution will be created if it does not exist.
- Start the NLM on the remote server. If there is already a NLM called AUDITLGN.NLM running, it will be unloaded.
- Add the LOAD command (including the entire path) to the end of the AUTOEXEC.NCF file on the remote server.
- If you are adding multiple servers, you can apply your selections for the above options to the remainder of the servers.

After adding new servers to the configuration, any servers that have been removed from the configuration will be dealt with second.



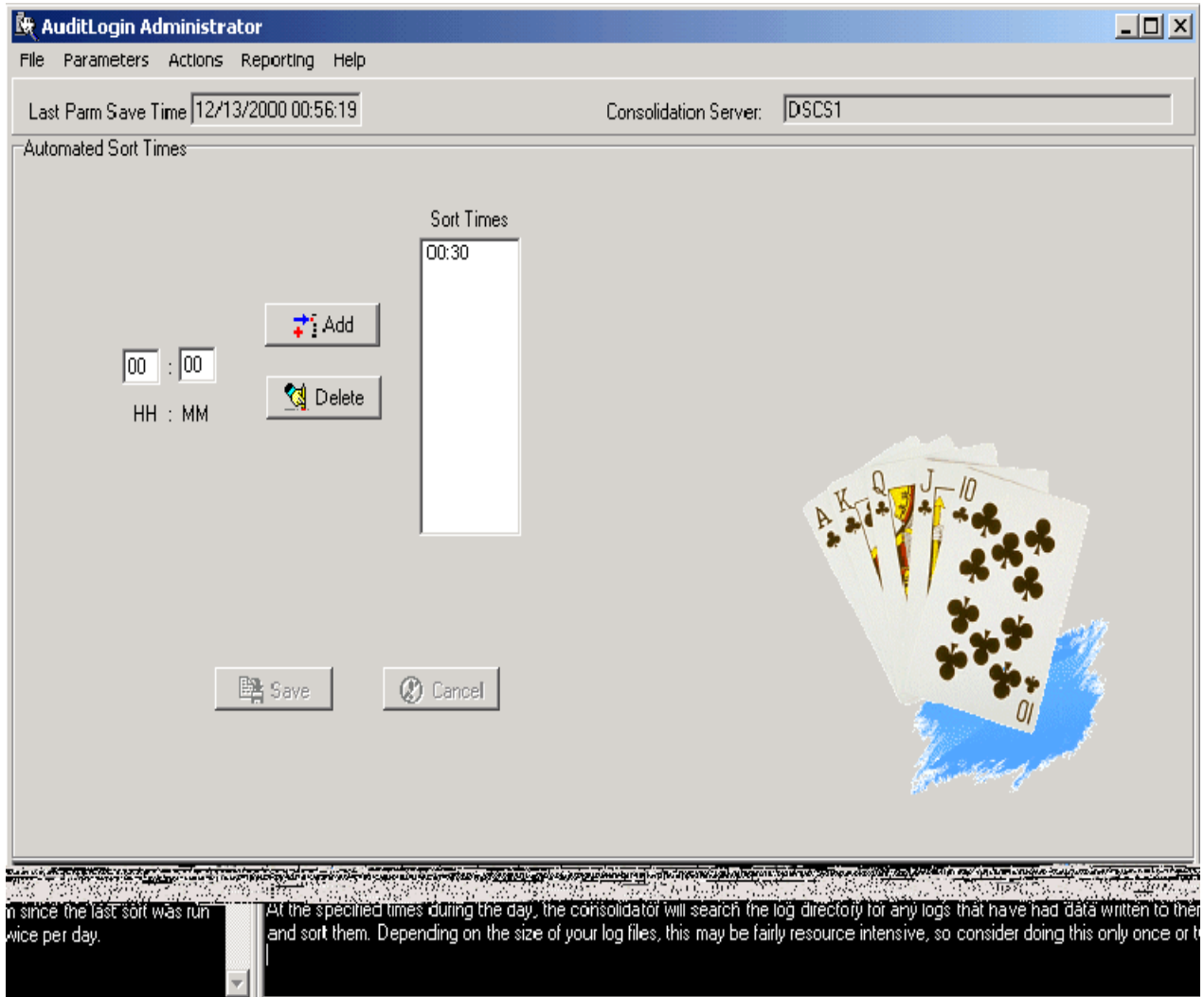
Besides removing the server from the configuration, the Admin tool will optionally:

- Remove the AUDITLGN.NLM file from the server.
- Unload the NLM remotely. This should always be selected since the consolidator will ignore any data sent to it from servers that are not in the audited servers list.
- Remove the LOAD command from the AUTOEXEC.NCF file on the remote server. This should always be selected, especially if you have removed the NLM from the server.
- If you are removing multiple servers, you can apply your selections for the above options to the remainder of the servers.

# AuditLogin v3.2

## Automated Sort

The Admin tool allows you to specify at what times of the day it should sort data files.




(Click on Image to Expand)

There is one auditing file kept per day. It's name is of the form YYYYMMDD.00x where x is either 0 or 1. The distinction is:

- .001 files have had data written to them by the consolidator since the last sort took place.
- .000 files have had no data written to them by the consolidator since the last sort took place.

Normally, data is sent in by the system monitoring NLM as the events occur on that server. However, if the consolidator is down or is otherwise unreachable due to network or server problems, the data is staged on the server running the system monitoring NLM. When the server detects that the consolidation NLM is reachable, all data in the staging file is sent in. This means that the data in the auditing files can be in an unsorted state.

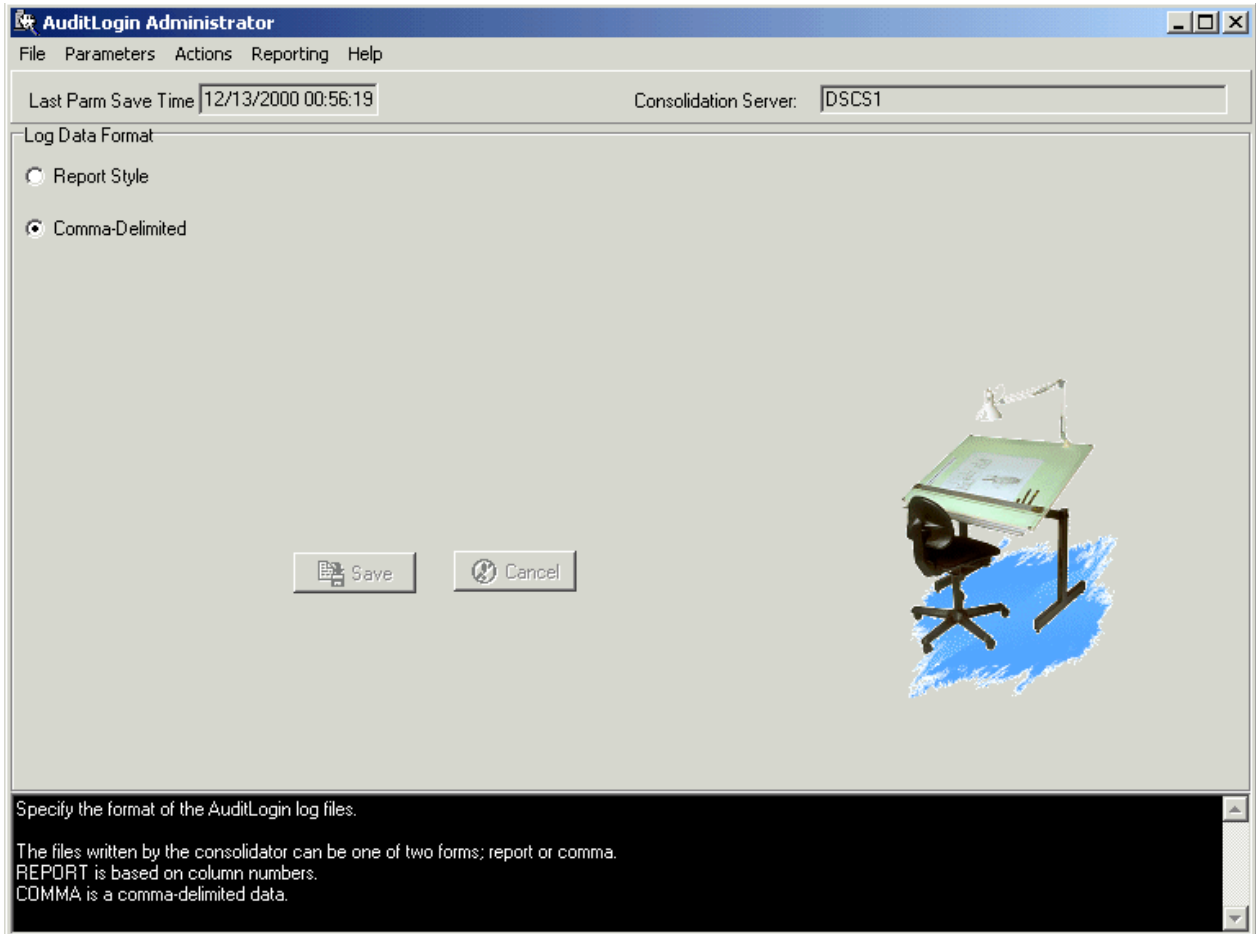
At the times specified, the consolidator will look for all .001 files and sort them; renaming each to .000 after sorting it. The sort is based on the quicksort algorithm and does not require that the entire file be in memory during the sort process. It uses intermediary files to ease memory allocation requirements for files with more than 10,000 records.

 If you have more than 10,000 login/logout records per day, you should consider marking the AUDITLOG directory as Immediate Purge.

# AuditLogin v3.2


## File Format

The auditing logs used with Version 3 of AuditLogin can be one of several formats that can be selected with the Admin tool.



(Click on Image to Expand)

- The REPORT format is mostly compatible with the logs generated by AuditLogin V2.
- The COMMA-DELIMITED format is new and is the default. It is useful for importing data into spreadsheets or database programs. It also takes less disk space than REPORT.

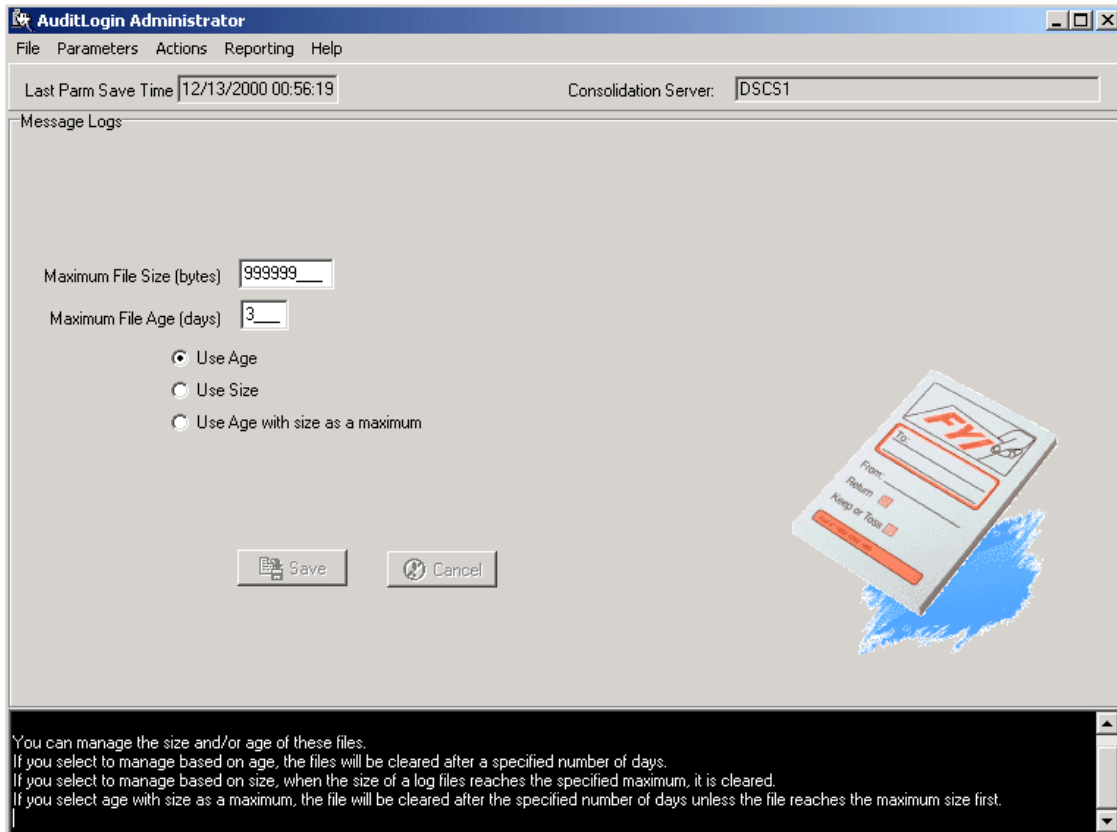
 **NOTICE:** With the initial release of V3 of AuditLogin, there is no tool provided to convert log data between the two formats. Therefore you should choose wisely. A tool is in development and will be introduced in a maintenance release.



# AuditLogin v3.2

## Message Logs

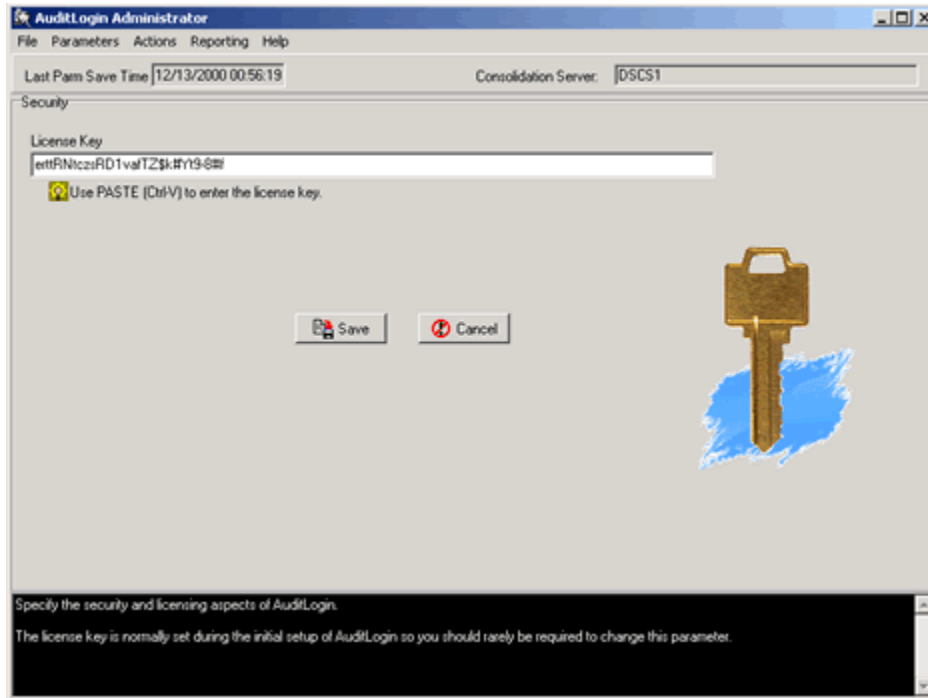
Besides the auditing files, the NLMs write operational logs that can be used to determine problems or inefficiencies in the operation of AuditLogin V3. The Admin tool will allow us to manipulate parameters relating to the size and/or age of these log files:




# AuditLogin v3.2

## Security

The license key can be changed at any time using the Security window of the Admin tool.



 **NOTICE:** Normally the license key will need to be changed after licensing the product. After that, no changes to the key should be required.

## Troubleshooting AuditLogin

For the most up to date issues please visit the [AuditLogin Support Forum](#).

If you have an issue with the product and do not see it addressed here or on the forum, please send a message to [support](#) or post a question on the forum. Technical support is initiated with email and is used as the primary medium of communication. Every problem is different. If we can answer your question quickly with a reply email, that is what will occur. Sometimes we may feel that a telephone conversation may be in order for the sake of clarity and expediency. Either way, we will be back with you quickly.

### Version 3.2

- [FIX: Timing-related Semaphore Abend in the AuditLogin NLM.](#)

If the server running AUDITLGN does not hold a NDS replica of it's own server object, it must make an unlicensed connection to a remote server that does hold a replica. If this connection is lost (ex: router problem), the connection is redriven to another server. During this reconnection, if a login or logout event occurred during this reconnection period, the semaphore abend would occur. This abend has been remedied by the AUDITLGN.NLM V3.23 release (May 11, 2001).

- [FIX: AUTOEXEC.NCF update does not ensure that the new LOAD command is on a new line.](#)

This problem has been remedied by the AuditAdm.EXE V3.23 release (May 11, 2001).

- [FIX: Memory consumption in AUDITLGN.NLM.](#)

AUDITLGN.NLM failed to free memory in certain circumstances related to timing, Client32 version, and replica location. This problem has been remedied by the AUDITLGN.NLM V3.23 release (May 11, 2001).

- [FIX: Report Header problem.](#)

A report type of "Session Length" would result in a problem with the report header. This problem has been remedied by the CONSLDAT.NLM V3.23 release (May 11, 2001).

- **ENHANCEMENT:** AuditLogin logs NDS "Workstation Object" logins and logouts. Customers have asked to ignore those transactions.

This change has been made with the AUDITLGN.NLM V3.23 release (May 11, 2001).