



ALTMAN TECHNOLOGIES

LT Auditor+ for NetWare

Quick Start Guide

Documentation issue: 5.1

Copyright © Blue Lance Inc.

Distributed by: -

Altman Technologies Ltd

LT Auditor+ for NetWare: Overview

LT Auditor+ is a security software application that provides surveillance of user activity for Novell NetWare & Microsoft Windows servers and security activity for Novell eDirectory/NDS & Microsoft Active Directory/NT Domains to produce an enterprise-wide audit trail.

LT Auditor+ monitors, records, alerts on & reports on key user-generated events across your network servers, providing consolidated reporting of security-sensitive activity. LT Auditor+ meets the requirements of auditors by providing detailed reporting of who did what, where and when.

LT Auditor+ for NetWare can be configured to monitor Novell NetWare Directory Services (eDirectory/NDS) activity, file/directory activity, login activity and system activity on the network in real-time. Filters can be configured as per user-defined security policies to collect logs for auditing. Audit logs collected on individual servers can be sent to a single server for enterprise-wide consolidated reporting.

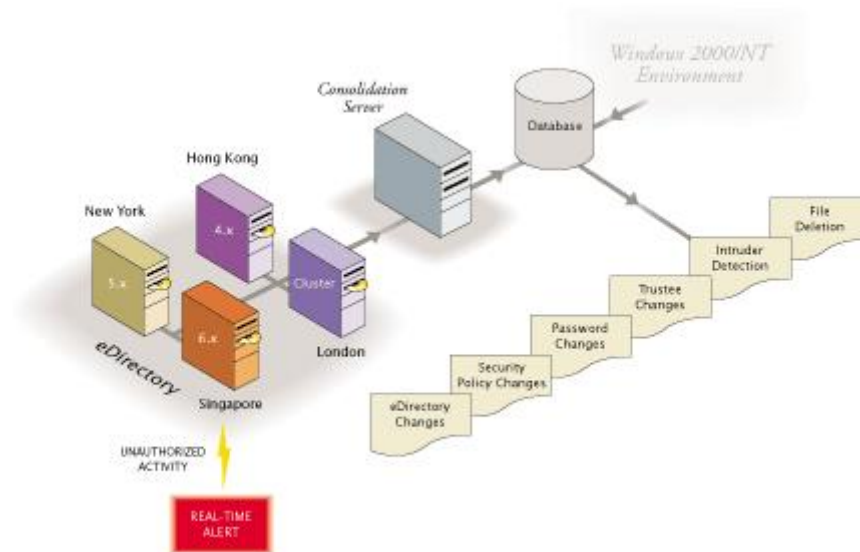
SUPPORTED FEATURES

- Unobtrusively monitors and audits users, files and system activity
- Tracks sensitive files and directories using powerful filtering technology
- Immediate notification of security breaches via optional real-time alerts
- Alerts deliverable via SNMP, SMTP or network broadcasts
- Granular reporting for faster and easier forensic analysis
- Monitors all eDirectory/NDS changes
- Supports NetWare 6.x, NetWare 5.x, NetWare 4.11 (& above) & all eDirectory/NDS versions on these platforms
- Powerful event filtering at collection and/or reporting stage
- Consolidated repository; multi-server and cross-platform (Windows/NetWare)
- Supports MS-SQL & Oracle databases as well as Pervasive Btrieve
- Pre-defined audit exception reports and customisable options
- “Drill-down” for more extensive forensic reporting

All trademarks contained in this document are the properties of their respective owners.

Concept

- LT Auditor+ management console installed on Windows
- NetWare servers are remotely installed from this console



- Agent NLM's run on every NetWare server monitoring events *directly* (including the consolidation server)
- Data collected according to configured filters
- Optional alerts according to configured filters
- Daily archive & data transfer to the consolidation server
- Daily consolidation to database (Btrieve only)
- Reports run from database using the LT Auditor+ Btrieve Report Generator

Cross-platform consolidation to Windows or to use a SQL database:

- Requires a Windows server running LT Auditor+ for Windows
- Consolidation server becomes gateway server from NetWare to Windows
- Data is transferred via IP from gateway to LT Auditor+ Windows

1. Getting Started

For further information - or if you encounter any problems installing - please see the files:

README.TXT in the unzip folder or NetWare folder of the CD,

LT Auditor+ for Novell Netware User Guide.PDF (Adobe Acrobat) in the Manuals folder,

LTA.CHM (Compiled Help) in the "Program Files\BlueLance, Inc\LT Auditor+ for NetWare" folder.

For additional information, please try our web support page (www.altman.co.uk/support), which has a Frequently Asked Questions (FAQ) section; if this does not help, contact **Altman Technologies** (see front-sheet for contact details).

The software is available as a download from the web or can be supplied on CD. The zip file you are provided with specifies the version number in its name & needs to be unzipped.

Please read this entire document before starting the installation. The installation process involves:

- Installing the LT Auditor+ Management Console on a workstation along with the Set-up files needed to remotely install LT Auditor+ on NetWare servers
- Remotely installing LT Auditor+ from this workstation, on all NetWare servers to be monitored and audited; this installs the NLM's (i.e. agents) that need to be loaded on all servers to allow LT Auditor+ to start collecting data

It is recommended that the user installing LT Auditor+ should have administrative rights (i.e. Admin equivalent on eDirectory/NDS & Administrator equivalent on the Windows workstation). However, if not, the user should have NetWare trustee rights to the following folders on every server where LT Auditor+ is to be installed:

- SUPERVISOR rights to the folder where LT Auditor+ is to be installed
- READ, WRITE, CREATE and MODIFY rights to the SYS:SYSTEM folder

System Requirements

Server	Workstation
NetWare 4.11 (or above), NetWare 5.x or NetWare 6.x	Windows NT4 (SP6a), Windows 2000 (SP2 or above), Windows XP (SP1 or above), Windows 2003
4MB available RAM	Novell Client32 4.8 or above (English)
100MB hard drive space on agent servers	128MB RAM
1GB hard drive space on consolidation server	100MB free hard drive space
BTRIEVE.NLM version 6.10c or later on consolidation server	

2. Workstation Installation

Setup

To install LT Auditor+, perform the following steps:

1. Insert the LT Auditor+ CD into the CD drive of the workstation or go to the unzip folder.
2. If Autorun is enabled, select *Install Products _LT Auditor+ for NetWare*. If Autorun is not enabled, execute *Setup.exe* from the NetWare folder on the CD or unzip folder.
3. The Install Wizard displays a welcome message. Follow the instructions to install LT Auditor+.
4. When the customer information window displays, enter your user name, company name, and serial number. If you are installing a trial version of LT Auditor+, enter *Trial* in the Key Number field. Click *Next* and follow the instructions to continue the installation process.
5. When the Install Wizard complete window displays, click *Finish* to exit.

This completes the installation of the LT Auditor+ Management Console as well as the Set-up files required to install LT Auditor+ on servers.

3. Remote Server Installation

Before you install LT Auditor+ on a server, ensure:

- You are logged into the eDirectory/NDS tree for that server
- You have valid connection along with the necessary trustee assignments on that server

To install LT Auditor+ on a server, follow these steps:

1. Select *Start _Programs _LT Auditor+ _LT Auditor+ for NetWare _Remote Install*. The LT Auditor+ Remote Setup window displays. Click *Next* and follow the instructions to install LT Auditor+. Read the licence information & click *Yes* to accept.
2. When the install option window displays, select one of the following options:
 - Update AUTOEXEC.NCF (the original file will be renamed AUTOEXEC.LTA)
 - Manually update AUTOEXEC.NCF later

Under the LT Auditor+ configuration files section, select one of the following:

- Use default configuration files
- Use configuration files from server

3. Click *Next* to continue.
4. Click *Add* to select a NetWare server or servers, on which to install LT Auditor+. Users can browse for servers if required.
5. If you have more than one volume on your NetWare servers, we suggest you pick the largest upon which to install LT Auditor+ & avoid SYS: in case the filling up of that volume should affect server performance. To do this, click the grey icon with “...” on it, to the right of the server’s entry on the Select Remote Machines window & browse-to or specify the desired volume.
6. Click *Install* to install on all selected servers.

This completes the installation of LT Auditor+ agents (NLM’s) on servers to be audited.

4. Loading LT Auditor+ Agents or NLM's

LT Auditor+ NLM's must be loaded on the server to begin the auditing process.

To load LT Auditor+ server modules, use the LT Auditor+ Management Console, NetWare Module Controller and click *LTASTART* (or from the server System Console, enter *LTASTART* and press Enter). The following NLM's are loaded:

- LTMERGE.NLM — Consolidation Module
- LTTRANS.NLM — Transfer Module
- LTSECURE.NLM — LT Auditor+ Security Module
- LTAUDIT.NLM — Auditing Engine
- LTASNMP.NLM — LT Auditor+ SNMP Module

These NLM's reside in the LT Auditor+ directory on the server. If the loader does not load these modules successfully, an error message will display on the server screen stating the problem and a possible solution. If you need to unload the NLM's, enter *LTASTOP* and press *Enter*.

Loader Switches

For further control and configuration, switches can be used with the loader. The LTAIP.NLM for cross-platform transfer on the gateway server must be loaded using the loader switch */IP*.

For more information on loading switches, refer to the *Installing LT Auditor+* chapter in the manual.

Configuring LT Auditor+

To monitor network activity, use the following as a guideline for using LT Auditor+:

1. Select *Start _Programs _LT Auditor+ _LT Auditor+ for NetWare _Management Console* to bring up the LT Auditor+ Management Console.
2. Select a server to configure as a “template” for others.
3. Create new filter policy statements on that server. The default policies from the install audit all Login and eDirectory/NDS activity. File deletions and modifications are also audited. Please configure your filters according to your organisation's security policies.
4. Set up archive and data transfer settings on the server. Archive files contain all the audit trail data collected by LT Auditor+ on the server. The transfer settings define how archived files are transferred to the consolidation server.
5. Export these policies to other servers in the environment.
6. Change to the consolidation server and create consolidation jobs to consolidate archived files to a Btrieve database.
7. Use the LT Auditor+ Report Generator to run enterprise-wide reports from the consolidated Btrieve database. Refer to the “LTABtrRep8_Start_Up.pdf” Quick Start guide for more information on installing & running this software on your workstation.

Notes:

- The consolidation server *does not* require any data transfer settings.
- If you are only testing on one server it will be the consolidation server & still needs to run a consolidation to convert the compressed archive files into the readable Btrieve format.
- The gateway server for cross-platform consolidation requires IP data transfer to the LT Auditor+ Windows Manager.

Assigning authorised users to manage LT Auditor+

By default, the user installing LT Auditor+ is the only user authorised to manage LT Auditor+. To allow other users to manage LT Auditor+ they need to be included into the authorised users list.

All authorised users must have the following NetWare trustee rights on all servers they manage:

- SUPERVISOR rights to the folder where LT Auditor+ is installed
- READ rights to the SYS:SYSTEM folder

Uninstalling

Uninstalling the software from your workstation desktop does not automatically uninstall the servers.

First uninstall the NetWare server(s). To do this, delete the whole of the directory structure under LTAUDIT and the four files beginning within LTA*.* in SYS:SYSTEM.

Finally, run uninstall for the LT Auditor+ NetWare software from the Control Panel, Add/Remove programs on the workstation.

Registering

LT Auditor+ comes with a fully functional, 30-day evaluation licence. Before the end of this evaluation, if you wish to buy, we will supply you with a serial number to turn the evaluation into a full licensed version, enabling you to keep all the data & filters you have collected and customised.

Updating versions

There is no need to uninstall first. New versions can safely be installed over previous versions as long as you are within maintenance.

You need to run Setup on a workstation, run *LTASTOP* on a server, update the server NLM's from the Remote Install, run *LTASTART* and then use Export from the Management Console to update all other servers.

For more detailed instructions on how to upgrade, please see the Upgrade Start_Up document that accompanies each new version.

Testing

To test everything is running correctly, we recommend you set up filters & jobs as above, then leave the server NLM's collecting for a day. You should then be able to report from the data collected using the (separately installed) LT Auditor+ Report Generator.