# Installing a Release of LTS/OnGuard™ Release 7.0

**Transaction Design, Inc.**

Notice

The information contained in this document is subject to change without notice.

Transaction Design, Inc. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Transaction Design, Inc., shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

This document is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Transaction Design, Inc.

Transaction Design, Inc.
542 San Pedro Cove
San Rafael, CA 94901
USA
1-415-256-8369 Voice
1-415-256-1844 Fax
lts@transactiondesign.com
www.transactiondesign.com

© 1996-2016 by Transaction Design, Inc. All rights reserved.

LTS/OnGuard™ is a trademark of Transaction Design, Inc. Stratus, VOS, and OpenVOS are registered trademarks of Stratus Technologies.

Manual number: OG002
Printing date: January 2016
LTS/OnGuard release: 7.0

# Contents

**INTRODUCTION** ..... **4**

*The purpose of this manual* ..... *4*
*Audience* ..... *4*
*Revision information* ..... *4*
*Manual organization* ..... *4*
*Notation* ..... *4*
*Format for commands* ..... *5*
Purpose ..... 5
CRT Form ..... 5
Lineal Form ..... 5
Arguments ..... 5
Explanation ..... 6
Examples ..... 6
*Online documentation* ..... *6*
*A note on the use of this manual* ..... *6*

**INSTALLATION PROCEDURES** ..... **7**

BACKGROUND INFORMATION ..... 7
SOFTWARE LICENSE ..... 7
THE LTS/ONGUARD DIRECTORY STRUCTURE ..... 7
*Administrator Commands* ..... *9*
*User Commands* ..... *11*
THE FULL INSTALLATION PROCEDURE ..... 12
A NOTE TO EXISTING USERS WHO ARE UPGRADING ..... 18
Moving of database files ..... 18
Overwriting of existing files ..... 18
INSTALLATION STEPS ..... 19
THE SERVICE PACK INSTALLATION STEPS ..... 21

**INSTALLATION COMMANDS** ..... **23**

*install_lts Privileged, SysAdmin or System* ..... *24*
*install_lts_sp Privileged, SysAdmin or System* ..... *26*
*lts_verify_license Privileged, SysAdmin or System* ..... *28*

# Figures

Figure 1. The LTS/OnGuard Directory Structure ..... 8

# Introduction

## The purpose of this manual

This manual *Installing a Release of LTS/OnGuard [OG002]* documents the installation procedures for installing the LTS/OnGuard software for security audit and control.

## Audience

This manual is intended for users who must install LTS/OnGuard on their system, such as Security Administrators and System Administrators.

The manual assumes that you can use the system. It also assumes that you are familiar with LTS/OnGuard itself (see the *LTS/OnGuard Reference Manual [OG001]*).

## Revision information

This manual is a revision. It describes the installation procedures for LTS/OnGuard.

## Manual organization

This manual is divided into two sections:

Section 1 describes the installation procedure.

Section 2 describes the installation commands.

## Notation

This manual uses *italics* to introduce or define new terms. For example:

The *external* commands have access rights and ACLs just like any other files.

*Computer font* is used to represent text that would appear on your terminal. This might be the name of a command or its options, or it might be a pathname on disk. For example:

```
audit_access_lists -detail
```

*Slanted font* is used to represent general terms which must be replaced by an actual value at execution time. In this example, the user would type a value to replace the term in slanted font:

```
-report_file report_file_path
```

*Printer font* is used to show output from LTS/OnGuard reports. For example:

```
There are no files with non-empty ACLs in this directory
```

*Boldface* is used for emphasis. For example:

Do **not** add this directory to the default search paths for commands.

## Format for commands

This manual uses these conventions to describe commands

`command_name`

The name of the command is at the beginning of the command description.

*Privileged*

If this appears after the name of the command, the command can only be issued by a privileged user.

*SysAdmin or System*

If this appears after the name of the command, the command can only be issued by someone logged in under one of these group names.

### Purpose

This explains briefly what the command does.

### CRT Form

This shows the form which is displayed on the CRT when the `DISPLAY-FORM` key is pressed or the `-form` option is given for the command. The values displayed are the default values for the command.

### Lineal Form

This shows the syntax of the command with its arguments as it is used in a lineal form on the command line, similar to giving the `-usage` option for the command.

| | |
|---|---|
| `argument` | required argument |
| `[argument]` | optional argument (NOTE: do **not** type in the brackets) |

### Arguments

This describes each of the arguments for the command. You may see the following descriptors on a command argument:

| | |
|---|---|
| **REQUIRED** | You cannot enter this command without supplying a value for this argument. |
| **CYCLE** | Only certain predefined values are allowed for this argument. For a switch, these values are “yes” and “no” on the CRT form. For certain options, there is a list of values which will be described in the text for this argument. |

### Explanation

This part explains how to use the command and may give other information about it.

### Examples

This part gives you some examples of how to invoke the command with various arguments. Not every command will have an examples section (particularly those that do not accept arguments).

## Online documentation

The LTS/OnGuard commands use the same online help convention as system commands. To get a brief description of what a command does, type

```
help command_name
```

Whenever you have the CRT form of the command on the screen (by using the `DISPLAY-FORM` key or the `-form` argument), you can press the `HELP` key to obtain information about the field where the cursor is currently positioned.

## A note on the use of this manual

This manual documents all commands and files which are part of the user interface. Any other commands or files which are shipped as part of the software product are intended solely for internal use in the product and may change without warning.

This manual documents all of the directory structure which is part of the user interface. Any other directories which are created by the software product are intended solely for internal use in the product and may change without warning.

# Section 1: Installation Procedures

## Background Information

This manual describes the installation of LTS/OnGuard™ security utilities for audit and control. It also describes the commands provided for installation.

You should be familiar with using the system, including executing commands, and navigating the directory hierarchy before trying to install this software. You should also be familiar with LTS/OnGuard software itself.

You should read through this entire manual before attempting to install LTS/OnGuard.

**Note: Release 7.0 will run under OpenVOS 17.0 and later releases on V-series machines. Release 7.0 will run on VOS 14 on Continuum.**

## Software License

This release of the LTS/OnGuard™ security utilities constitutes a major release. In order to successfully execute this new software on a computer module, the user must have valid keys for release 7 enabling the software on that module. The keys will be supplied with the release.

## The LTS/OnGuard Directory Structure

LTS/OnGuard creates its own directory structure to avoid interfering with standard system files and directories. Most files are under a directory named `lts` which is created under `(master_disk)>system`. A number of files for non-privileged users will be placed in a "user library" which will be specific to your site.

Access rights to the directories and files in and under `lts` are set to the appropriate values by the installation and run-time software. You should not change access lists within this directory structure.

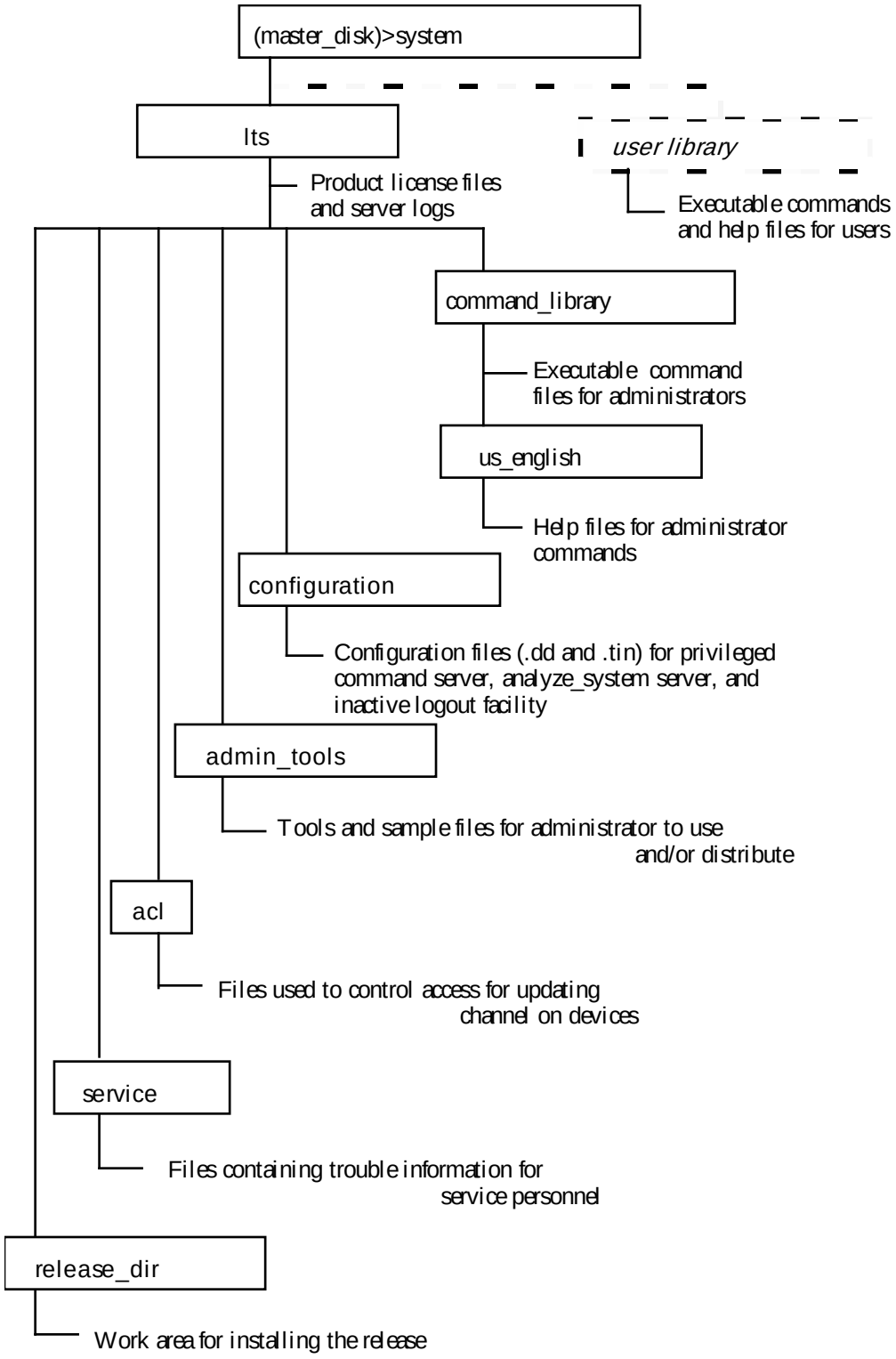


**Figure 1. The LTS/OnGuard Directory Structure.**

## Administrator Commands

All of the files for the administrator are under `(master_disk)>system>lts`. When you first install the software, `lts` itself will be empty. When the various commands run, they will place files into `lts`. The rest of the files are contained in subdirectories.

`lts>command_library`

This directory contains the executable commands for administrators. The auditing commands and the commands to set up and operate the privileged command and `analyze_system` request environments and the inactive logout facility are in this directory. The license file also exists in this directory.

`lts>command_library>us_english (obsolete)`

This directory contains the help files that support the commands in `command_library`. You can change these in the conventional way to customize help for your site. (obsolete)

`lts>configuration`

This directory contains the `.dd` and `.tin` files needed to create the `.table` files for the privileged command and `analyze_system` request servers. The `.tin` files which are installed contain the entries your non-privileged users need to execute all of the front-end requests which are shipped with this release.

If these files are already present during the installation process, the install command does not install `.tin` files from the release tape. Instead the install command installs `.new` files.

This directory also contains subdirectories for temporary files.

`lts>acl`

This directory contains any files used to control access to update channel on terminals through the privileged command environment.

`lts>service`

This directory contains any “trouble call” files created by commands which stop due to a fatal error. The information in these files will assist LTS personnel in solving problems.

`lts>admin_tools`

This directory contains tools for the administrator. Some such as abbreviations files may be installed for users, while others remain for

administrative use. This directory also contains the text of the current license agreement, and the report title file.

`lts>release_dir`

This directory is a work area for the installation of this release. After a complete installation, this directory will be empty, with the possible exception of VOS save/restore logs.

If there are any files which could not be installed in the proper directory, they will be found here after the installation command finishes.

## User Commands

LTS/OnGuard has several commands that are for users: `execute_privileged_command`, `execute_as_request`, `lts_batch`, `lts_start_process`, `lts_registration_admin`, and `lts_uci`. These are the commands which pass requests to the controlled server environments for privileged commands and `analyze_system` requests.

In addition, there are a large number of "front-end" files for users. These are command macros or programs which provide the normal command line forms interface for the user, while passing the actual command or request to a server for processing. By using these, the non-privileged user is controlled and monitored by the server environments while the users see the operating system interface which they expect.

These commands should ***not*** be placed in administrative libraries (such as `lts>command_library`). To let users execute them, you would have to add the directories to the user command search paths and grant them sufficient access to see and execute the commands. Doing this would give the users access to more information than they need. Instead, these commands should be installed in a library that users normally have access to.

Some sites use `(master_disk)>system>applications_library` as a location for site-specific commands of all types. If you are already using this directory, you can add the LTS/OnGuard user commands there. If you prefer, you can create some other directory for this purpose such as `(master_disk)>system>lts_user`. If you are installing LTS/OnGuard for the first time and will be implementing security incrementally, we recommend that the front-end commands be placed in a separate library for a user-by-user roll-out of the LTS/OnGuard features.

When you install LTS/OnGuard, you will need to choose the library where these user commands can be placed.

## The Full Installation Procedure

The installation of a full release LTS/OnGuard software consists of three steps:

1. Bringing the installation package to the module.
2. Running the installation tools.
3. Performing any administrative customization.

**Step 1. Placing the installation tools and software on the module**

The LTS/OnGuard software files are provided as a 'bundled' VOS file.

**Step 2. Placing the installation tools and software**

The Transaction Design website contains news, manuals, and updates for the LTS/OnGuard software. The URL to get to our LTS/OnGuard™ news and updates page is: `http://www.transactiondesign.com`. Contact us for the link to the software download page.

You will need several files:

- `lts_*_man.pdf`: The LTS/OnGuard Reference Manual in Adobe PDF format;
- `lts_*_srb.pdf`: The LTS/OnGuard Software Release Bulletin in Adobe PDF format;
- `lts_*_install.pdf`: This document in Adobe PDF format;
- `lts*ia32.bun`: File containing LTS/OnGuard™ for the Stratus V-series (IA32) hardware type;
- `lts*cont.bun`: File containing LTS/OnGuard™ for the Stratus Continuum hardware type;

Unbundle the LTS/OnGuard software:

- On the Stratus, rename the lts*.bun file to lts*.save.evf.gz.

```
rename lts*.bun lts*.save.evf.gz
```

Unbundle the lts*.save.evf.gz file using the freeware utilities from the Stratus VOS FTP site. This should create or place the files in a temporary directory.

**Note**: There are multiple versions of the VOS tools containing 'unbundle.cm'. Please be sure to use the tool in such a way that all of the unbundled files are placed in the temporary directory under your home dir or another safe place, not under the >system directory. After installation this temporary directory may be deleted.

```
unbundle lts70aia32.save.evf.gz
```

This should create a directory named lts70aia32. Confirm that the directory contains install_lts.cm and the ship_files folder.

```
change_current_dir lts70aia32
list -all
```

Login as a privileged user in the SysAdmin group on the module where you wish to install the software. If you are not privileged and SysAdmin, you will not have sufficient authority to perform some of the steps in installation.

Note: You should not start logging the procedure to a file. The installation tool will provide a log for you.

**Step 3. Running the installation tools**

The installation tool is `install_lts`. This command will verify that the appropriate directory structure exists or will create it, move the files into the `lts>release_dir`, and moves the files to the appropriate final destination directories.

The `install_lts` command starts logging when it begins executing, so when the installation is done, you will have a log file in your home directory named `install_log_[module]_(date).txt`

By default, `install_lts` will move the command files to the appropriate directories, deleting any existing file of the same name which is already there. It will perform the same function for user and front-end files, moving them to the user library. **You may need to protect any front-end files which have been created or modified at your site.**

At the end of the installation process `lts>release_dir` should be empty. If there are any files left in `release_dir`, other than files left by the VOS restore process, then you should find an error message in the log file describing the problem.

**Step 4. License keys**

If supplied separately, the `tdi_config.txt` file must be placed in the `>system>lts>command` library before performing the next steps. If this is a major release of LTS/OnGuard with a new initial release number, i.e. 6.2 versus 7.0, new license document and report title files will have to be created for each computer module by running `lts_verify_license.pm`. Please refer to the detailed installation steps for further information.

**Step 5. Performing any administrative customization**

If you are installing LTS/OnGuard for the first time, you may wish to customize your installation.

- **Administrator abbreviations**

  You will want to create abbreviations for the LTS/OnGuard administrative commands for yourself and any other administrators. To simplify that task, there are files in the `admin_tools` directory (`abbrev_*`) that you can paste directly into your own `abbreviations` file in your home directory, if you wish.

- **Command libraries**

  LTS/OnGuard will use two libraries in your environment:

  - Front-end library, `>system>applications_library`, `>system>lts_user`, or some such. This library must exist before doing the installation. If you want LTS/OnGuard to be universally used, you should include this library in the default command_library paths. It must precede the `>system>command_library`. If you don't want it to be universal, it will need to be added to each user's start_up.cm macro, again preceding the `>system>command_library`.
  - Administrator's library, `>system>lts>command_library`. This library is used only by the administrators who will be starting or stopping the LTS/OnGuard server environment. It is not to be used by the typical user.

  The typical user will end up with library paths that look like:

  - `>system>lts_user or >system>applications_library`
  - …
  - `>system>command_library`

  The administrative user will end up with library paths that look like:

  - `>system>lts_user or >system>applications_library`
  - …
  - `>system>lts>command_library`
  - …

- >system>command_library

In the admin_tools directory is a file (add_to_administrator_start_up_cm) that you can paste into the start_up.cm file in your home directory.

- **User abbreviations**

  Any users who will be registered to use the privileged command environment or the analyze_system request environment may want abbreviations for the user commands. You can paste abbrev_users from the admin_tools directory into the abbreviations file of these users.

  A non-privileged user who is acting as an auditor on the system and must use the LTS/OnGuard auditing commands should be given the file abbrev_ltsadmin.

- **The restricted environments**

  Before non-privileged users can pass commands through the privileged command and analyze_system request environments, you must configure the tables correctly and then start the servers.

  There are several files shipped with this release to assist you in configuring your non-privileged users. The priv_cmd_commands.tin file contains entries for hundreds of privileged commands available through the server. Use install_priv_cmd_tables to configure this commands file and customize the priv_cmd_users.tin file to contain your local users. You can then use start_priv_cmd_server to begin processing.

  Similarly, use install_as_rqst_tables to configure the as_rqst_commands.tin file and customize the as_rqst_users.tin file to contain your local users. Use start_as_rqst_server to begin processing.

  If you wish to make more privileged commands and analyze_system requests available at a later time, there are two files, priv_cmd_commands.new and as_rqst_commands.new, which you can use with an editor to place new entries in your commands .tin files.

  If you wish to use the facility to control which devices can be updated through the privileged command server, you must first create the table and establish the access files.

  - First, change the link install_priv_cmd_tables.cm in lts>command_library to point to the file ipct_with_uci.cm. Then, execute install_priv_cmd_tables to create the correct settings in the priv_cmd_uci table.

  - You may then wish to add files to lts>acl and change their access lists.

If you wish to use the lts_registration_admin environment, you must register the users with appropriate class in the tables.

- **Security Standards Reporting**

  audit_security_info has the ability to compare current settings with predefined tables holding a set of standard settings. The user may wish to install these tables. To do so, issue the install_security_standards command. This will create these tables and move them to >system>lts:

  - standard_forbidden_pwds.table
  - standard_network_access.table
  - standard_restricted_users.table
  - standard_security.table
  - standard_posix.table
  - standard_ssh_services.table
  - standard_stcp_services.table

- **The inactive logout facility**

  If you wish to use the facility for logging out inactive users (LTS/Terminator), you must first create and install the table describing the terminals to be monitored. You can use install_terminator_table to do this.

- **The module_start_up.cm**

  If you wish to have the privileged command or analyze_system server environments start automatically when the module is rebooted, you can place the start commands in your module_start_up.cm file. In the admin_tools directory, there is a file (add_to_module_start_up) which you can customize and paste into your module_start_up.cm file. Be sure to place these commands **after** any system commands.

  As discussed earlier you may wish to add the LTS/OnGuard front-end library to the default library paths.

  If users are likely to submit requests for privileged command execution or analyze_system requests through batch, make sure that you do not start batch processing on that queue until after you have started the servers.

  If you wish to have inactive terminal monitoring start automatically when the module is rebooted, you can place the start command in module_start_up.cm. The command for this is also in the add_to_module_start_up_file in admin_tools. In the file as shipped, the command is commented out so it will not execute. To activate it, edit the file and remove the “&” at the beginning of the line.

  Also shipped is a feature with the capability for a non-privileged user to start the privileged command and analyze_system servers. If you wish to have the restarter process start automatically when the module is

rebooted, you can place the start_lts_restarter command in `module_start_up.cm`.

**Note. Log and temporary file cleanup**

As part of your daily system log cleanup or "garbage collection" you will want to schedule automatic cleanup of the following:

```
>system>lts
     LTS_as_rqst_log.(date)  - log of as_rqst_server
     LTS_priv_cmd_log.(date)- log of priv_cmd_server
     *_rpt.(date).*          - reports created by –file parameter
>system>lts>configuration>lts_sf
     *.*                     - temp files
>system>lts>configuration>lts_temp_files
     *.*                     - temp files
>system>lts>db
     rah*(date)*      - un-processed registration_admin history file
     raf*(date)*      - un-processed registration_admin update file
```

**Note. Trouble reports**

If a portion of LTS/OnGuard experiences a problem, it will place one or more trouble reports in `>system>lts>service`. This folder should be examined periodically for trouble reports. These reports are required when opening a trouble ticket with the Status Customer Assistance Center or with Transaction Design.

## A Note to Existing Users who are Upgrading

### Moving of database files

As part of the installation, databases which by default had been in >system>lts will be moved to >system>lts>db.

### Overwriting of existing files

As part of the installation, files in the user directory will be overwritten by new files from the install with the same name. There are front-end files included for privileged commands and `analyze_system` requests. If you have created or modified front-end files in the user directory, they will be overwritten during the installation. You should either move these files to another location during the installation procedure or give a different user library name to the installation command. Front-end files you received as part of an earlier release and have not changed may be safely overwritten by the installation process.

The installation will also overwrite files in the `>system>lts>command_library` directory. If you have modified any files in this directory, the changes would be lost. Typically, the only changes here are to the tape handling commands, such as `lts_scmd.cm` to set tape defaults. The installation tool will rename `.cm` files in this directory to *`macro_name.LTS`* instead of deleting the old files. If you have modified any `.cm` files, they will still be in the directory after installation, but with the new name. You may then apply your changes to the new `.cm` files. When you no longer need the old versions of the `.cm` files, you may delete any files from `lts>command_library` with the suffix `.LTS`.

## Installation Steps

You install an LTS/OnGuard release by following these steps:

1. Receive the software from the website or via email.

2. Unbundle the file on the Stratus using the freeware utility tools from the Stratus FTP site.

3. Login as a privileged user in the SysAdmin group on the module where you wish to install the software.

4. Execute the installation command install_lts

Perform these steps in this order:

Step 1. Unbundle the LTS/OnGuard software.

On the Stratus, rename the `lts70*.bun` file to `lts70*.save.evf.gz`.

```
rename lts70aia32.bun lts70aia32.save.evf.gz
```

Unbundle the `lts70aia32.save.evf.gz` file using the freeware utilities from the Stratus VOS FTP site. This should create a directory named `lts70aia32`. The directory should contain `install_lts.cm` and the `ship_files` directory.

```
unbundle lts70aia32
change_current_dir lts70aia32
list -all
```

Step 2. Login as a privileged user in the SysAdmin group on the module where you wish to install the software.

If you are not privileged and SysAdmin, you will not have sufficient authority to perform some of the steps in installation.

You can be in **any** directory on the target module containing the previously loaded files to perform the installation. There is no special location you need to change to.

Note: You should not start logging the procedure to a file – the installation tool will provide a log for you.

Step 3. Execute the installation command

a. Issue the `install_lts` command with the `-form` option.

   To install the user commands you will need to give the pathname of the (existing) directory.

b. Confirm that the installation of the files was successful.

Step 4. If this is a new installation, or a major upgrade such as going from LTS/OnGuard release 6 to 7, perform these steps:

a. If supplied separately, copy the `tdi_config.txt` license file into `>system>lts>command_library`.
b. Install the new license document and report title file for LTS/OnGuard. This is accomplished by running `lts_verify_license.pm` as SysAdmin. Be sure to run the ".pm" instance of the command.
c. Add the LTS/OnGuard library paths to your personal start_up.cm, and execute the macro and confirm that the paths were added properly. They should be:

`(master_disk)>system>applications_library`
…or whatever directory you have selected as the directory to hold the front-end commands This must come before the directory below in the list of your library paths.
`(master_disk)>system>lts>command_library`
This must come before `>system>command_library` in the list of your library paths.

d. Run `list_library_paths command` to confirm that the paths are in the correct order. Then run `start_process 'list_library_paths command'` Then examine the `*.out` file and again confirm that the paths are in the correct order.

Step 5. Install or update the tables for the priv_cmd server:

a. Execute `install_priv_cmd_tables.cm` and make the appropriate edits to the `priv_cmd_commands.tin` and `priv_cmd_users.tin` files. This step is required when going from release 6 to 7. If this is an upgrade, access the `priv_cmd_commands.new` file and merge it into the `priv_cmd_commands.tin` to update the table properly. Note that this step may be required if installing an incremental release, if commands have been added.

Step 6. Install or update the tables for the as_rqst server:

a. Execute `install_as_rqst_tables.cm` and make the appropriate edits to the `as_rqst_commands.tin` and `as_rqst_users.tin` files. Note that this step may be required if installing an incremental release, if commands have been added.

Step 7. Start (or bounce) the servers

a. Execute `start_priv_cmd_server` and confirm that the server is up.
b. Execute `start_as_rqst_server` and confirm that the server is up.
c. Execute `set_site_preferences`.

## The Service Pack Installation Steps

You install an LTS/OnGuard service pack by following these steps:

1. Receive the software from the website or via email.

2. Unbundle the file on the Stratus using the freeware utility tools from the Stratus FTP site.

3. Login as a privileged user in the SysAdmin group on the module where you wish to install the software

4. Execute the installation command install_lts_sp

Perform these steps in this order:

Step 1. Unbundle the LTS/OnGuard service pack

On the Stratus, rename the `lts*.bun` file to `lts*.save.evf.gz`.

```
rename lts*sp.bun lts*sp.save.evf.gz
```

Unbundle the `lts*.save.evf.gz` file using the freeware utilities from the Stratus VOS FTP site. This should create a directory named `lts*`. The directory should contain `install_lts_sp.cm` and the updated software modules.

```
unbundle lts70aia32sp
```

This should create a directory named `lts70aia32sp`. Confirm that the directory contains `install_lts_sp.cm` and additional modules.

```
change_current_dir lts70aia32sp

list -all
```

Step 2. Login as a privileged user in the SysAdmin group on the module where you wish to install the software.

If you are not privileged and SysAdmin, you will not have sufficient authority to perform some of the steps in installation.

You can be in **any** directory on the target module containing the previously loaded files to perform the installation. There is no special location you need to change to.

Note: You should not start logging the procedure to a file – the installation tool will provide a log for you.

Step 3. Execute the installation command

a. Issue the `install_lts_sp` command

If you have decided to install the user commands in a command directory other than `(master_disk)>system>applications_library`, you will need to give the pathname of the directory.

b. Confirm that the installation was successful.

# Installation Commands

This section documents the commands used in the installation of LTS/OnGuard software.

## install_lts *Privileged, SysAdmin or System*

**Purpose**

The `install_lts` command installs the LTS/OnGuard software from the unbundled directory structure on disk.

It is a privileged command, and you must also be in the “SysAdmin” or “System” group to execute this command.

**CRT Form**

```
-------------------------------- install_lts --------------------------------
user_library:
-verbose: no
```

**Lineal Form**

```
install_lts
            [user_library]
            [-verbose]
```

**Arguments**

`user_library, required`

The path name of a directory where the user commands are to be installed.

The user commands are all of the front-end commands which mimic the VOS commands, `execute_privileged_command, execute_as_request, lts_batch, lts_start_process, and lts_uci` and associated files.

`-verbose` **CYCLE**

If this switch is off or if it is omitted, the command installs files silently.

If the switch is on, the command displays the name of each file as it installs it.

**Explanation**

The `install_lts` command:

- Starts logging in your home directory to a file named `install_log_[module]_(date).txt`
- Creates any missing directories in the hierarchy under `(master_disk)>system>lts`

- Sets appropriate access rights on the `lts` directories
- Restores the product files into `release_dir`
- Moves the new files to the appropriate `lts` directories
- Moves database files from `>system>lts` to `>system>lts>db`

**Examples**

This command will perform a normal installation on a module, deleting any old files as it executes.

```
install_lts (master_disk)>system>lts_user
```

## install_lts_sp *Privileged, SysAdmin or System*

### Purpose

The install_lts_sp command updates the LTS/OnGuard software from a “service pack” directory on disk.

It is a privileged command, and you must also be in the “SysAdmin” or “System” group to execute this command.

### CRT Form

```
------------------------------ install_lts_sp ------------------------------
user_library:
-verbose: no
```

### Lineal Form

```
install_lts
            [user_library]
            [-verbose]
```

### Arguments

`user_library, required`

The path name of a directory where the user commands are to be installed.

The user commands are all of the front-end commands which mimic the VOS commands, `execute_privileged_command, execute_as_request, lts_batch, lts_start_process, and lts_uci` and associated files.

`-verbose` **CYCLE**

If this switch is off or if it is omitted, the command installs files silently.

If the switch is on, the command displays the name of each file as it installs it.

### Explanation

The `install_lts_sp` command:

- Starts logging in your home directory to a file named `install_log_[module]_(date).txt`
- Confirms access to the directories in the hierarchy under `(master_disk)>system>lts`

- Moves the new files to the appropriate `lts` directories

**Examples**

This command will perform an update on a module, deleting any old files as it executes.

```
install_lts_sp (master_disk)>system>lts_user
```

## lts_verify_license *Privileged, SysAdmin or System*

**Purpose**

The lts_verify_license command confirms that the encrypted license is valid, and that the report title and license document files are in their proper positions. If not, it will lead the user through steps to create them.

It is a privileged command, and you must also be in the "SysAdmin" or "System" group to execute this command.

**CRT Form**

```
------------------------------ lts_verify_license ----------------------
-verbose: yes
```

**Lineal Form**

```
lts_verify_license
             [-verbose]
```

**Arguments**

`-verbose` **CYCLE**

If the switch is yes, the command displays the name of the module, the RSN site id for the module, the duration of the license, and the current contents of the `report_company_name.txt` file which resides in `>system>lts>admin_tools`.

**Explanation**

The `lts_verify_license` command:

- Examines the encrypted license file and compares it with the module name, RSN site id, and the current date to determine if the software is properly licensed for the module.
- Looks for the license document and report title file. If they don't exist, the user will be lead through a dialogue which creates them.