CHAPTER 3

Installing and Running Security Software

This chapter provides instructions for downloading, installing, and running the Solaris Security Toolkit software and other security-related software. Included are instructions for configuring your environment for either standalone or JumpStart mode, and obtaining support. Also in this chapter is a fast-track approach for users who want to quickly install and run the Solaris Security Toolkit software.

This chapter contains the following topics:

Obtaining Support

The configurations for Sun systems implemented by the Solaris Security Toolkit software are Sun supported configurations. Support calls to Sun's support services are handled the same as other cases.

Note – The Solaris Security Toolkit software itself is not a supported Sun product. Sun's support services cannot accept calls about the Solaris Security Toolkit's scripts.

To obtain Solaris Security Toolkit software assistance and to submit bug reports, questions, suggestions, and feedback, please use the Solaris Security Toolkit Support Forum at the following Web site:

```
http://supportforum.sun.com/cgi-bin/WebX.cgi?/
security.jass.toolkit
```

Feedback on how the Solaris Security Toolkit software works and words of encouragement to the developers are appreciated.

Taking the Recommended Track

We *highly* recommend that you follow the instructions and process provided in this section to install, configure, and execute the software. By following the recommended approach, you'll be guided through the process, including downloading additional security software, with detailed instructions, helpful examples, and useful recommendations.

Although the Solaris Security Toolkit software is a standalone product, it is most effective when used with the additional security software we recommend and provide for downloading. This software includes the latest Recommended and Security Patch Cluster from SunSolve OnLine, Secure Shell software for Solaris OE releases that do not include it, permission and ownership modification software to tighten Solaris OE and third-party software permissions, and integrity validation binaries to validate the integrity of Sun files and executables.

This section contains the following tasks:

Perform Planning and Pre-Installation Tasks

Proper planning is key to successfully using the Solaris Security Toolkit software to secure systems. Refer to Chapter 2 for detailed information about planning and other tasks recommended before you install the software.

If you are installing the software on a deployed system, refer to Chapter 2, "Perform Pre-Installation Tasks" on page 33, for information about performing pre-installation tasks to install the software on deployed systems.

Determine Which Mode to Use

We recommend that you harden systems either during or immediately after installation, to limit the period a system might be exposed to attack while in an unsecured state. Before using the Solaris Security Toolkit software to secure a system, configure the Solaris Security Toolkit software to run properly in your environment.

The Solaris Security Toolkit software has a modular framework. For customers not yet using the JumpStart product, the flexibility of the Solaris Security Toolkit software's framework allows them to efficiently prepare for using JumpStart later. Customers with existing JumpStart installations benefit from the Solaris Security Toolkit software's ability to integrate into existing JumpStart architectures.

The following sections describe each mode.

Standalone Mode

The Solaris Security Toolkit software runs directly from a Solaris OE shell prompt in standalone mode. The standalone mode allows you to use the Solaris Security Toolkit software on systems that require security modifications or updates, yet cannot be taken out of service to re-install the OS from scratch. Ideally, however, we recommend that systems be reinstalled from scratch to secure them.

Standalone mode is particularly useful when hardening a system after installing patches. You can run the Solaris Security Toolkit software multiple times on a system with no ill effects. Patches might overwrite or modify files the Solaris Security Toolkit software has modified; by rerunning the Solaris Security Toolkit software, any security modifications undone by the patch installation can be reimplemented.

Note – In production environments, we recommend that patches always be staged in test and development environments before installation in live environments.

The standalone mode is one of the best options to harden a deployed system as quickly as possible. No special steps are required to integrate the Solaris Security Toolkit software into a non-JumpStart architecture, other than those provided in the downloading and installing instructions provided in "Download Security Software" on page 43.

JumpStart Mode

JumpStart technology, which is Sun's network-based Solaris OE installation mechanism, can run Solaris Security Toolkit scripts during the installation process. This book assumes that the reader is familiar with JumpStart technology and has an existing JumpStart environment available. For more information about JumpStart technology, refer to the Sun BluePrints book *JumpStart™ Technology: Effective Use in the Solaris™ Operating Environment*.

For use in a JumpStart environment, the Solaris Security Toolkit source in either the `JASS_HOME_DIR` (for `tar` downloads) or `/opt/SUNWjass` (for `pkg` downloads) has to be copied into the base directory of the JumpStart server. Typically, this is `/jumpstart` on the JumpStart server. After this task is done, `JASS_HOME_DIR` becomes the base directory of the JumpStart server.

Only a few steps are required to integrate the Solaris Security Toolkit software into a JumpStart architecture. Refer to Chapter 5 for instructions on how to configure a JumpStart Server.

Download Security Software

The first stage in hardening a system requires downloading additional software security packages onto the system you want to secure. This section covers the following tasks:

- "Downloading Solaris Security Toolkit Software" on page 44
- "Downloading Recommended Patch Cluster Software" on page 45
- "Downloading FixModes Software" on page 47
- "Downloading OpenSSH Software" on page 48
- "Downloading the MD5 Software" on page 50

Note – Of the software described in this section, the Solaris Security Toolkit software, Recommended and Security Patch Cluster, FixModes, and MD5 software are strongly recommended. Instead of OpenSSH, you can substitute a commercial version of Secure Shell, available from a variety of vendors. We strongly recommend that you install and use a Secure Shell product on all systems. With the release of Solaris 9 OE, a version of Solaris Secure Shell is included. If using Solaris 9 OE, we strongly recommend using this Secure Shell version.

Downloading Solaris Security Toolkit Software

The Solaris Security Toolkit software must be downloaded first, then installed on either the server on which you are using the Solaris Security Toolkit software in standalone mode or on a JumpStart server for JumpStart mode.

The primary function of the Solaris Security Toolkit software is to automate and simplify building secured Solaris OE systems based on the recommendations contained in this guide and security-related Sun BluePrints OnLine articles.

Note – The following instructions use filenames that do not reference the version number. Always download the latest version available from the Web site.

Throughout the rest of this guide, the `JASS_HOME_DIR` environment variable refers to the root directory of the Solaris Security Toolkit software. When the Solaris Security Toolkit software is installed from the `tar` archive, `JASS_HOME_DIR` is defined to be the path up to, and including, `jass-`*`n.n`*. If you install the `tar` version of the distribution in the `/opt` directory, the `JASS_HOME_DIR` environment variable is defined as `/opt/jass-`*`n.n`*.

The Solaris Security Toolkit software is distributed in Solaris OE package format, in addition to the traditional compressed `tar` archive. The same software is included in both archives.

Choose the format most appropriate for your situation. Typically, the `pkg` format is best for clients and the `tar` is best for JumpStart systems and for developing custom packages.

Procedures for downloading and installing these two different archive types are provided in the following sections.

▼ To Download the `tar` Version

1. **Download the software distribution file** (`jass-`*`n.n`*`.tar.Z`)**.**

   The source file is located at the following Web site:

   `http://www.sun.com/security/jass`

2. **Extract the software distribution file into a directory on the server using the** `zcat` **and** `tar` **commands as shown**:

```
# zcat jass-n.n.tar.Z | tar xvf -
```

   Where *`n.n`* is the most current version that you are downloading.

Executing this command creates the `jass-n.n` subdirectory in the current working directory. This subdirectory contains all the Solaris Security Toolkit directories and associated files.

▼ To Download the pkg Version

1. **Download the software distribution file (`SUNWjass-n.n.pkg.Z`).**

   The source file is located at:

   ```
   http://www.sun.com/security/jass
   ```

Note – If you encounter difficulty downloading the software, use your browser's integrated Save As option.

---

2. **Extract the software distribution file into a directory on the server by using the `uncompress` command**:

```
# uncompress SUNWjass-n.n.pkg.Z
```

3. **Install the software distribution file into a directory on the server using the `pkgadd` command as shown:**

```
# pkgadd -d SUNWjass-n.n.pkg SUNWjass
```

Where *n.n* is the most current version that you are downloading.

Executing this command creates the `SUNWjass` directory in `/opt/jass-n.n`. This subdirectory contains all the Solaris Security Toolkit directories and associated files.

Downloading Recommended Patch Cluster Software

Patches are released by Sun to provide Solaris OE fixes for performance, stability, functionality, and security. It is critical to the security of a system that the most up-to-date patch cluster is installed. To ensure that the latest Solaris OE Recommended and Security Patch Cluster is installed on your system, this section describes how to download the latest patch cluster.

Note – Apply standard best practices to all patch cluster installations. Before installing any patches, evaluate and test them on nonproduction systems or during scheduled maintenance windows.

▼ To Download Recommended Patch Cluster Software

Before you install a patch cluster, we recommend that you review individual patch README files and other information provided. The information often contains suggestions and information helpful to know before installing a patch cluster.

1. **Download the latest patch cluster from the SunSolve OnLine Web site at:**

   `http://sunsolve.sun.com`

2. **Click on the Patches link at the top of the left navigation bar.**

3. **Click on the Recommended and Security Patches link.**

   The license agreement is displayed.

4. **Select the appropriate Solaris OE version in the Recommended Solaris Patch Clusters box.**

   In our example, we select Solaris 8 OE.

5. **Select the best download option, either HTTP or FTP, with the associated radio button, then click Go.**

   A Save As dialog box is displayed in your browser window.

6. **Save the file locally.**

7. **Move the file securely to the system being hardened by using the `scp` command, or another method that provides secure file transfer.**

   The `scp` command used should be similar to the following:

```
# scp 8_Recommended.zip target01:
```

8. **Move the file to the** `/opt/SUNWjass/Patches` **directory and uncompress it.**

   For example:

CODE EXAMPLE 3-1 Moving a Patch File to `/opt/SUNWjass/Patches` Directory

```
# cd /opt/SUNWjass/Patches
# mv /<directory in which file was saved>/8_Recommended.zip .
# unzip 8_Recommended.zip
Archive:     8_Recommended.zip
   creating: 8_Recommended/
  inflating: 8_Recommended/CLUSTER_README
  inflating: 8_Recommended/copyright
  inflating: 8_Recommended/install_cluster
[. . .]
```

Later, the patch cluster software is installed automatically after downloading all the other security packages and executing the Solaris Security Toolkit software.

Note – If you do not place the Recommended and Security Patch Cluster software into the `/opt/SUNWjass/Patches` directory, a warning message displays when you execute the Solaris Security Toolkit software. You can safely ignore this message if no patch clusters apply, as is often the case with new releases of the OS.

Downloading FixModes Software

FixModes is a software package that tightens the default Solaris OE directory and file permissions. Tightening these permissions can significantly improve overall security. More restrictive permissions make it even more difficult for malicious users to gain privileges on a system.

Note – With the Solaris 9 OE release, changes were made to improve the default permissions of objects previously altered by the FixModes software. However, the FixModes software is still necessary, because third-party and unbundled software typically requires tightening of file and directory permissions.

▼ To Download FixModes Software

1. **Download the FixModes precompiled binaries from:**

   `http://www.sun.com/blueprints/tools/FixModes_license.html`

   The FixModes software is distributed as a precompiled and compressed package version file formatted for Solaris OE systems. The file name is `SUNBEfixm.pkg.Z`.

2. **Once downloaded, move the file securely to the system being hardened by using the `scp` command, or another method that provides secure file transfer.**

   The `scp` command used should be similar to the following command:

```
# scp SUNBEfixm.pkg.Z target01:
```

3. **Save the file, `SUNBEfixm.pkg.Z`, in the Solaris Security Toolkit `Packages` directory in `/opt/SUNWjass/Packages`, with the following commands:**

```
# cd /opt/SUNWjass/Packages
# mv /<directory in which file was saved>/SUNBEfixm.pkg.Z .
```

   Later, the FixModes software is installed automatically after downloading all the other security packages and executing the Solaris Security Toolkit software.

4. **Uncompress the `pkg` file with the following command:**

```
# uncompress SUNWBEfixm.pkg.Z
```

Downloading OpenSSH Software

In any secured environment, the use of encryption in combination with strong authentication is required to protect user-interactive sessions. At a minimum, network access must be encrypted.

The tool most commonly used to implement encryption is Secure Shell software, whether a version bundled with the Solaris OE, a third-party commercial, or freeware version. To implement all the security modifications performed by the Solaris Security Toolkit software, you must include a Secure Shell software product.

Note – With the release of Solaris 9 OE, a version of Secure Shell is included. If using Solaris 9 OE, we strongly recommend using this Secure Shell version due to its integration with other Solaris OE security features such as the Basic Security Module (BSM) as well as its support by Sun's support organization.

Information on where to obtain commercial versions of Secure Shell is provided in the Preface under "Related Resources" on page xxix.

The Solaris Security Toolkit software disables all nonencrypted user-interactive services and daemons on the system, in particular daemons such as `in.telnetd`, `in.ftpd`, `in.rshd`, and `in.rlogind`.

Access to the system can be gained with Secure Shell similarly to what is provided by Telnet and FTP.

▼ To Download OpenSSH Software

Note – If the server is running Solaris 9 OE, you can use the bundled Secure Shell software and skip the OpenSSH installation steps in this section.

- **Obtain the following Sun BluePrints OnLine article, and use the instructions in the article for downloading the software.**

A Sun BluePrints OnLine article about how to compile and deploy OpenSSH titled "Building and Deploying OpenSSH on the Solaris Operating Environment" is available at:

```
http://www.sun.com/blueprints
```

Or, obtain the Sun BluePrints publication *Secure Shell in the Enterprise*, which is available at book stores.

Later, the OpenSSH software is installed automatically after downloading all the other security packages and executing the Solaris Security Toolkit software.

Caution – Do not compile OpenSSH on the system being hardened and do not install the compilers on the system being hardened. Use a separate Solaris OE system—running the same Solaris OE version, architecture, and mode (for example, Solaris 8 OE, Sun4U™ (`sun4u`), and 64-bit)—to compile OpenSSH. If you implement a commercial version of SSH, then no compilation is required. The goal is to limit the availability of compilers to potential intruders. Understand, however, that refraining from installing compilers locally on a system does not provide significant protection against determined attackers, because they can still install pre-compiled tools.

Downloading the MD5 Software

The MD5 software generates MD5 digital fingerprints on the system being hardened. Generate the digital fingerprints, then compare them with what Sun has published as correct, to detect system binaries that are altered or *trojaned* (hidden inside something that appears safe) by unauthorized users. By modifying system binaries, attackers provide themselves with backdoor access onto a system; they hide their presence and could cause systems to operate in unstable manners.

▼ To Download the MD5 Software

1. **Download the MD5 binaries from the following web site:**

   `http://www.sun.com/blueprints/tools/md5_license.html`

   The MD5 programs are distributed as a compressed package version file.

2. **Move the file** `SUNBEmd5.pkg.Z` **securely to the system being hardened with the** `scp` **command, or another method that provides secure file transfer.**

   The `scp` command used should be similar to the following command:

```
# scp SUNBEmd5.pkg.Z target01:
```

3. **Move the file,** `SUNBEmd5.pkg.Z`**, to the Solaris Security Toolkit** `Packages` **directory in** `/opt/SUNWjass/Packages` **with a command similar to the following:**

```
# cd /opt/SUNWjass/Packages
# mv /<directory in which file was saved>/SUNWBEmd5.Z .
```

   After the MD5 software is saved to the `/opt/SUNWjass/Packages` directory, the execution of the Solaris Security Toolkit software installs the software.

   After the MD5 binaries are installed, you can use them to verify the integrity of executables on the system through the Solaris fingerprint database. More information on the Solaris fingerprint database is available in the Sun BluePrints OnLine article titled “The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files.”

4. **(Optional) Download and install Solaris Fingerprint Database Companion and Solaris Fingerprint Database Sidekick software from the Sun BluePrint Web site at:**

   `http://www.sun.com/blueprints/tools`

We strongly recommend that you install these optional tools and use them with the MD5 software. These tools simplify the process of validating system binaries against the database of MD5 checksums. Use these tools frequently to validate the integrity of the Solaris OE binaries and files on a secured system.

These tools and instructions for downloading them are in the Sun BluePrints OnLine article titled “The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files.”

The integrity of the security tools downloaded should be verified. On the download page of the Solaris Security Toolkit, MD5 checksums are available for this purpose. Before installing and running the Solaris Security Toolkit software and additional security software, validate integrity through the use of MD5 checksums.

Customize Security Profiles

A variety of security profile templates are included with the Solaris Security Toolkit software distribution as drivers. As mentioned in the previous chapter, the default security profile and changes made by these drivers may not be appropriate for your systems. Typically, the security profiles implemented by these drivers are “high-water” marks for security. By this, we mean that they disable services that are not required, and they enable optional security features disabled by default.

Before running the Solaris Security Toolkit software, review and customize the default security profiles for your environment, or develop new ones. Techniques and recommendations for customizing security profiles are provided in Chapter 10.

Install and Execute the Software

It is important that the following preliminary tasks be completed prior to executing the Solaris Security Toolkit software. Most of the hardening is done automatically when you execute the Solaris Security Toolkit software.

- Download the additional security software and the Solaris Security Toolkit software on the system you want to harden or on the JumpStart server. (Refer to “Download Security Software” on page 43.)
- Configure your system for standalone or JumpStart mode. (Refer to “Determine Which Mode to Use” on page 42.)
- If applicable, customize the Solaris Security Toolkit software for your environment.
- Before installing and running the Solaris Security Toolkit software and additional security software, validate integrity through the use of MD5 checksums.

You can execute the Solaris Security Toolkit software directly from the command line or a JumpStart server.

For command line options and other information about executing the software, refer to one of the following:

- "Executing the Software in Standalone Mode" on page 52
- "Executing the Software in JumpStart Mode" on page 60

Executing the Software in Standalone Mode

Example command line usage in standalone mode:

```
# jass-execute [-r root_directory -p os_version ] [ -q | -o
output_file ] [ -m e-mail_address ] -d driver
```

TABLE 3-1 lists the command line options available and describes each.

TABLE 3-1 Using Command Line Options With `jass-execute`

Option	Description
`-a`	Determines if a system is in compliance with its security profile.
`-d`	Specifies the driver to be run in standalone mode.
`-h`	Displays the `jass-execute` help message, which provides an overview of the available options.
`-H`	Provides a simple mechanism to determine how many times the Solaris Security Toolkit software has been run on a system.
`-l`	Provides a mechanism to determine the most recent run.
`-m`	Mails output to an email address.
`-o`	Directs output to a file.
`-q`	Prevents the display of output to the screen. Also known as the quiet option.
`-r`	Specifies the root directory used during `jass-execute` runs.
`-u`	Runs undo option with interactive prompts that ask you what action you want to take when exceptions are encountered.

For detailed information about the options available with `jass-execute` command in standalone mode, refer to the following sections:

- "Audit Option" on page 54
- "Display Help Option" on page 55
- "Driver Option" on page 55
- "Email Notification Option" on page 56
- "Execute History Option" on page 57
- "Most Recent Execute Option" on page 57
- "Output File Option" on page 58
- "Quiet Output Option" on page 58
- "Root Directory Option" on page 59
- "Undo Option" on page 59

For a complete listing of available drivers, refer to the Drivers directory. Newer versions of the software may contain additional drivers.

▼ To Execute the Software in Standalone Mode

1. **Execute the** `secure.driver` **(or a product specific script such as** `sunfire_15k_sc-secure.driver`**) as follows.**

CODE EXAMPLE 3-2 Executing the Software in Standalone Mode

```
# cd /opt/SUNWjass
# ./jass-execute -d secure.driver
[NOTE] Executing driver, secure.driver

============================================================
secure.driver: Driver started.
============================================================

============================================================
JASS Version:  4.0
Node name:     ufudu
Host ID:       8085816e
Host address:  10.8.31.115
MAC address:   8:0:20:85:81:6e
OS version:    5.9
Date:          Tue Dec 31 16:28:24 EST 2002
============================================================
[...]
```

For a complete listing of available drivers, refer to the Drivers directory. Newer versions of the software may contain additional drivers.

2. **After running the Solaris Security Toolkit software on a system, reboot the system to implement the changes.**

   During hardening, a variety of modifications are made to the configuration of the client. These modifications could include disabling startup scripts for services, disabling options for services, and installing new binaries or libraries through patches. Until the client is restarted, these modifications might not be effective.

3. **After rebooting the system, verify the correctness and completeness of the modifications. (Refer to "Validate the System Modifications" on page 61.)**

4. **If any errors are encountered, fix them and run the Solaris Security Toolkit software again in standalone mode.**

Audit Option

Through the `-a` option, the Solaris Security Toolkit software can perform an audit run to determine if a system is in compliance with its security profile. This run validates not only if system file modifications made are still active, but also if previously disabled processes are running or removed software packages are reinstalled. For more information on this function, refer to Chapter 6.

Example usage to audit a system against a security profile:

```
# jass-execute -a driver [ -V verbosity ] [ -q | -o output_file ]
[ -m e-mail_address ]
```

Display Help Option

The `-h` option displays the `jass-execute` help message, which provides an overview of the available options.

The `-h` option produces output similar to the following:

CODE EXAMPLE 3-3 Sample `-h` Option Output

```
# ./jass-execute -h

To apply this Toolkit to a system, using the syntax:
   ./jass-execute [-r root_directory -p os_version ]
[ -q | -o output_file ] [ -m e-mail_address ] -d driver

To undo a previous application of the Toolkit from a system:
   ./jass-execute -u [ -n ] [ -q | -o output_file ]
[ -m e-mail_address ]

To audit a system against a pre-defined profile:
   ./jass-execute -a driver [ -V verbosity ]
[ -q | -o output_file ] [ -m e-mail_address ]

To display the history of Toolkit applications on a system:
   ./jass-execute -H

To display the last application of the Toolkit on a system:
   ./jass-execute -l

To display this help message:
   ./jass-execute -h
```

Driver Option

The `-d` <*`driver`*> option specifies the driver to be run in standalone mode.

You must specify a driver with the `-d` option. The Solaris Security Toolkit software prepends `Drivers/` to the name of the script added. You need to enter only the script name on the command line.

Note – You cannot use the `-d` option with the `-u, -H, -h, or -a` options.

A `jass-execute` hardening run using the `-d <driver>` option produces output similar to the following:

CODE EXAMPLE 3-4 Sample `-d <driver>` Option Output

```
# ./jass-execute -d secure.driver
[NOTE] Executing driver, secure.driver

============================================================
secure.driver: Driver started.
============================================================

============================================================
JASS Version:  4.0
Node name:     ufudu
Host ID:       8085816e
Host address:  10.8.31.115
MAC address:   8:0:20:85:81:6e
OS version:    5.9
Date:          Tue Dec 31 16:28:24 EST 2002
============================================================
[...]
```

Email Notification Option

The `-m <email address>` option provides a mechanism by which standalone hardening and undo output can be emailed automatically by the Solaris Security Toolkit software when the run completes. The email report is in addition to any logs generated on the system using other options.

A Solaris Security Toolkit run calling `sunfire_15k_sc-config.driver` using the email option would be similar to the following:

```
# ./jass-execute -m root -d sunfire_15k_sc-config.driver
[...]
```

Execute History Option

The `-H` option provides a simple mechanism to determine how many times the Solaris Security Toolkit software has been run on a system. All runs are listed regardless of whether they have been undone.

The `-H` option produces output similar to the following:

CODE EXAMPLE 3-5 Sample `-H` Option Output

```
# ./jass-execute -H
Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 0.3.

The following is a listing of the applications of the Solaris
Security Toolkit on this system.  This list is provided in
reverse chronological order:

1.   December 31, 2002 at 12:20:19 (20021231122019) (UNDONE)
2.   December 31, 2002 at 12:10:29 (20021231121029)
3.   December 31, 2002 at 12:04:15 (20021231120415)
```

From the output, it is clear that the Solaris Security Toolkit software was run on this system three times and that the last run was undone.

Most Recent Execute Option

The `-l` option provides a mechanism to determine the most recent run. This is always the last run listed by the `-H` option as well.

The `-l` option provide outputs similar to the following:

CODE EXAMPLE 3-6 Sample `-l` Option Output

```
# ./jass-execute -l

Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 0.3.

The last application of the Solaris Security Toolkit was:

1.   December 31, 2002 at 12:20:19 (20021231122019) (UNDONE)
```

Output File Option

The `-o <output_file>` option redirects the console output of `jass-execute` runs to a separate file, `output_file`.

This option has no effect on the logs kept in the `JASS_REPOSITORY` directory. This option is particularly helpful when performed over a slow terminal connection, because there is a significant amount of output generated by a Solaris Security Toolkit run.

This option can be used with either the `-d`, `-u`, or `-a` options.

The `-o` option produces output similar to the following:

CODE EXAMPLE 3-7 Sample `-o` Option Output

```
# ./jass-execute -o jass-output.txt -d secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to jass-output.txt
```

Quiet Output Option

The `-q` option disables Solaris Security Toolkit output to standard input output (stdio) stream during a hardening run.

This option has no effect on the logs kept in the `JASS_REPOSITORY` directory. Similar to the `-o` option, this option is particularly helpful when running the Solaris Security Toolkit software through a cron job or over slow network connections.

This option can be used with either the `-d`, `-u`, or `-a` options.

The `-q` option produces output similar to the following:

CODE EXAMPLE 3-8 Sample `-q` Option Output

```
# ./jass-execute -q -d secure.driver
[NOTE] Executing driver, secure.driver
```

Root Directory Option

The `-r <root directory>` option is for specifying the root directory used during `jass-execute` runs. Using the `-r` option also requires using the `-p` option to specify the platform (OS) version. The format of the `-p` option is equivalent to that produced by `uname -r`.

By default, the root filesystem directory is `/`. This root directory is defined by the Solaris Security Toolkit environment variable `JASS_ROOT_DIR`. The Solaris OE being secured is available through `/`. For example, if you want to secure a separate OS directory, temporarily mounted under `/mnt`, then use the `-r` option to specify `/mnt`, and all the scripts are applied to that OS image.

Undo Option

Through the `-u` option, the Solaris Security Toolkit software can undo system modifications performed during hardening. Each finish script can be undone with the `-u` option. In addition, the Solaris Security Toolkit's undo ability is tightly integrated with the checksums generated during each run. For more information on this capability, refer to Chapter 4.

Example command line usage of an undo command:

```
# jass-execute -u [ -f | -b | -k] [ -q | -o output_file ] [ -m e-
mail_address ]
```

Executing the Software in JumpStart Mode

The JumpStart mode is controlled by the Solaris Security Toolkit driver inserted in the `rules` file on the JumpStart server.

If you have not configured your environment to use JumpStart mode, refer to Chapter 5.

For more information on the JumpStart technology, refer to the Sun BluePrint book *JumpStart™ Technology: Effective Use in the Solaris™ Operating Environment*.

▼ To Execute the Software in JumpStart Mode

To execute the Solaris Security Toolkit software in JumpStart mode, it must be integrated into your JumpStart environment and called as part of the finish scripts associated with a JumpStart installation. For information about how to integrate the Solaris Security Toolkit software into your environment, refer to Chapter 5.

1. **After making all of the required modifications to the drivers, install the client using the JumpStart infrastructure.**

   This task is done using the following command from the client's `ok` prompt.

   ```
   ok> boot net - install
   ```

   Once the installation is completed, the system is rebooted by the JumpStart software.

   The system should be in its correct configuration. During hardening, a variety of modifications are made to the configuration of the client. These modifications could include disabling startup scripts for services, disabling options for services, and installing new binaries or libraries through patches. Until the client is restarted, these modifications might not be effective.

2. **After the system is rebooted, verify the correctness and completeness of the modifications. (Refer to "Validate the System Modifications" on page 61.)**

3. **If any errors are encountered, fix them and reinstall the client's OE.**

Validate the System Modifications

After rebooting the system, validate the correctness and completeness of the modifications as described in the following sections.

Performing QA Checks of Services

One of the significant challenges involved in securing systems is determining what OE services must be left enabled for the system to function properly. Solaris OE services might be needed because they are used directly, such as Secure Shell to log into a system. Or, they could be used indirectly, such as the Remote Procedure Call (RPC) daemon for the graphical user interface of third-party software management tools.

Most of these requirements should be determined before running the Solaris Security Toolkit software. (Refer to Chapter 2, “Determine Application and Service Requirements” on page 23.) However, the only definitive mechanism is to install and secure the system, then perform thorough testing of its required functionality through quality assurance (QA) testing. Ideally, there should be a QA plan in place for any new system being deployed. If so, this plan should be executed after the system is hardened. Similarly, for deployed systems being hardened, thorough testing must be performed to ensure that all required and expected functionality is present.

If the QA process uncovers any discrepancies, perform the following:

1. Determine the problem area, based on the recommendations in Chapter 2.
2. Validate that the application runs in the modified configuration.
3. Undo the Solaris Security Toolkit run.
4. Modify the security profile (driver), based on the problem resolution.
5. Run the Solaris Security Toolkit software again.

The end result should be a security profile that can be run on the system without adversely impacting any required functionality.

Performing Security Assessments of Configuration

While validating that the system performs all required functions, also evaluate the security configuration to determine if the system is secured to the desired level. Depending on what hardening or minimization was performed on the system, this may involve different aspects.

At a minimum, the configuration of the system should be reviewed in the following ways:

- Ensure that all appropriate Security and Recommended Patches are installed.
- Verify that only required and appropriate processes are running, and that they are running with the appropriate arguments.
- Ensure that only required daemons are running, and that they are running with the appropriate arguments.
- Verify that only required ports are open on the system by checking locally (for example, `netstat -a`) and remotely by using a port scanner such as Nmap, which can determine which ports are available on a network interface.
- Make sure that only required Solaris OE packages were installed if the system was minimized.

This review should be considered a minimum for newly built and secured systems. When hardening legacy systems, the underlying OE should be verified to determine if unauthorized modifications were made. Integrity checking of this nature is best done by mounting the system's file system in read-only mode and running integrity checking software from a known OE instance. The tools described in the Sun BluePrints OnLine article titled "The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files" are useful in these scenarios.

Validating Security Profile

After a system is secured and you validate its required services and capabilities, use the audit function to make sure that the security profile was applied properly and completely. This task is critical for two reasons. The first is to ensure that the system is hardened as required. The second is to ensure that the security profile defined for the system is properly reflected in the Solaris Security Toolkit configuration. This check is critical because the configuration information is used to maintain the security profile of the system over its entire deployed lifecycle.

For more information about the audit function, refer to Chapter 6.

Perform Post-installation Tasks

If you installed the software on a deployed system, refer to Chapter 2, “Perform Post-Installation Tasks” on page 34, for information about performing post-installation tasks on deployed systems.

Taking the Fast Track

This section provides a fast track approach to using the Solaris Security Toolkit software. Although we strongly recommend that you follow the standard methods presented in “Taking the Recommended Track” on page 41, we empathize with users who are terminally impatient and want to execute the Solaris Security Toolkit software immediately to see what happens. Review the following key considerations to determine if this characterization fits you:

- The approach in this section assumes that you are willing to break things and are able to fix them.
- Because there are potentially serious consequences that could result, it is important that you read and carefully consider the notes, cautions, and recommendations in this section.

Note – Only notes and cautions critical to successfully installing and configuring the Solaris Security Toolkit software are included in this section. Refer to “Taking the Recommended Track” on page 41 for complete information on configuring and executing the Solaris Security Toolkit software.

- Evaluate your security policy and requirements against the default drivers before executing the Solaris Security Toolkit software.
- We strongly recommend that you have console access.
- A reboot is required for the changes to take affect.
- If you run into problems with a hardening run, use the undo feature. For detailed information, refer to Chapter 4.

Note – The information in this section applies to using the Solaris Security Toolkit software in standalone mode only. For details on the differences between standalone mode and JumpStart mode, refer to “Determine Which Mode to Use” on page 42.

This section contains the following topics:

Download Software

Note – The following instructions use filenames that do not reference the version number. Always download the latest version available from the Web site.

▼ To Download the Solaris Security Toolkit Software

The Solaris Security Toolkit software is distributed in Solaris OE package format, in addition to the traditional compressed `tar` archive. The same software is included in both archives. Choose the format most appropriate for your scenario. Downloading and installing these two different archive types are addressed in the following procedures.

▼ To Download the `pkg` Version

1. **Download the software distribution file (**`SUNWjass-`*`n.n`*`.pkg.Z`**).**

   The source file is located at:

   `http://www.sun.com/blueprints/tools/license.html`

2. **Extract the software distribution file into a directory on the server by using the** `uncompress` **command**:

```
# uncompress SUNWjass-n.n.pkg.Z
```

3. **Install the software distribution file into a directory on the server using the** `pkgadd` **command as shown:**

```
# pkgadd -d SUNWjass-n.n.pkg SUNWjass
```

   Executing this command creates the `SUNWjass` directory in `/opt`. This subdirectory contains all the Solaris Security Toolkit directories and associated files.

▼ To Download the tar Version

1. **Download the software distribution file** (jass-*n.n*.tar.Z)**.**

   The source file is located at the following Web site:

   http://www.sun.com/security/jass

2. **Extract the software distribution file into a directory on the server using the** zcat **and** tar **commands as shown**:

```
# zcat jass-n.n.tar.Z | tar xvf -
```

   Where *n.n* is the most current version that you downloaded.

   Executing this command creates the jass-*n.n* subdirectory in the current working directory. This subdirectory contains all the Solaris Security Toolkit directories and associated files.

   Throughout the rest of this document, the JASS_HOME_DIR environment variable refers to the root directory of the Solaris Security Toolkit software. When the Solaris Security Toolkit software is installed from the tar archive, JASS_HOME_DIR is defined to be the path up to, and including, jass-*n.n*.

   If you invoke the command from the /opt directory, then the JASS_HOME_DIR variable is defined as /opt/jass-*n.n*, where *n.n* is the Solaris Security Toolkit version.

▼ To Download Additional Security Software

In "Taking the Recommended Track" on page 41, we provide instructions for downloading other security software. Of the software described, the Recommended and Security Patch Cluster, FixModes, and MD5 software are required. We strongly recommend that you use a Secure Shell product on the internal servers to protect user and administrative network traffic from disclosure, modification, and hijacking.

- **Refer to "Taking the Recommended Track" on page 41 for instructions if you want to download the additional security software at this time.**

Install and Execute the Software

After you download the Solaris Security Toolkit software, install it on the server you are hardening in standalone mode.

The Solaris Security Toolkit software provides a default driver named `secure.driver` for automating the implementation of Solaris OE modifications and installation of security software. This default driver implements Solaris OE security modifications based on the recommendations in Sun BluePrint OnLine articles. Also, if you downloaded the additional security software, it performs the following tasks:

- Installs the Recommended and Security Patch Cluster software
- Installs and executes the FixModes software to tighten file system permissions
- Installs the MD5 software

Note – During the modifications implemented in this section, all nonencrypted access mechanisms to the system being hardened—such as Telnet and FTP—are disabled. The hardening steps do not disable console access over serial ports, or directly attached video cards, monitors, and keyboards.

In addition to the default `secure.driver` driver, we provide product-specific drivers. You can use the default driver, use any of the product-specific drivers, or customize and create your own drivers. For more information, refer to Chapter 10.

▼ To Install Downloaded Software and Implement Changes

Caution – A Solaris Security Toolkit standalone run, on a pre-existing system, should only be performed after the machine has been backed up and rebooted to verify that it is in a known, working, and consistent configuration. Any errors or warnings detected during this preliminary reboot should be corrected or noted.

---

1. **From the list of hardening drivers, choose the one that applies to your system and purpose.**

   For a complete and up-to-date listing of available drivers, download the most recent version of the Solaris Security Toolkit software from the following Web site:

   `http://www.sun.com/security/jass`

   Refer to Chapter 10 for information about standard and product-specific drivers. For the most current listing of drivers, refer to the `Drivers` directory.

Caution – The following command executes all of the hardening scripts included in `secure.driver`. This action might not be appropriate for all environments. Evaluate which security modifications are required for your system before executing the Solaris Security Toolkit software.

---

2. **Execute the `secure.driver` (or a product-specific such as `sunfire_15k_sc-secure.driver`) as follows.**

CODE EXAMPLE 3-9 Executing a Driver

```
# cd /opt/SUNWjass
# ./jass-execute -d sunfire_15k_sc-secure.driver
[NOTE] Executing driver, sunfire_15k_sc-secure.driver

============================================================
sunfire_15k_sc-secure.driver: Driver started.
============================================================

============================================================
JASS Version:  4.0
Node name:     ufudu
Host ID:       8085816e
Host address:  10.8.31.115
MAC address:   8:0:20:85:81:6e
OS version:    5.9
Date:          Tue Dec 31 16:28:24 EST 2002
============================================================
[...]
```

Note – The `secure.driver` disables all remote access capabilities, such as Telnet, RSH, and RLOGIN, with the exception of Secure Shell in the Solaris 9 OE. Do not reboot the system without at least one of those services being enabled, having serial or console access to the system, or having an alternate remote access mechanism available such as Secure Shell.

---

3. **After running the Solaris Security Toolkit software on a system, reboot the system to implement the changes.**

   During hardening, a variety of modifications are made to the configuration of the client. These modifications could include disabling startup scripts for services, disabling options for services, and installing new binaries or libraries through patches. Until the client is restarted, these modifications might not be effective.

4. **After rebooting the system, verify the correctness and completeness of the modifications. (Refer to “Validate the System Modifications” on page 61.)**

5. **If any errors are encountered, fix them and run the Solaris Security Toolkit software again.**